NUOVA EDIZIONE
SETTEMBRE 2016

Rapporto

2016

sulla sicurezza ICT
in Italia

Indice

ASTREA Advanced Security, Training Research, Events Agency
Via Nicolò Copernico, 38 - 20125 Milano

Prefazione

Il rapporto CLUSIT che leggerete è stato steso da un team di lavoro che ha dedicato tempo e sforzi nell'analisi di una serie di fonti dalle quali è possibile trarre una conclusione semplice e chiara: il cybercrime è una realtà che fa parte della nostra vita quotidiana con la quale occorre fare necessariamente i conti.

Non è più possibile fare finta di nulla sperando che non tocchi mai a noi.
Ci toccherà eccome, sia nella vita privata che nella vita lavorativa.

Il cybercrime è cresciuto nell'ultimo anno, e molto. Le nostre stime parlano di circa il 30% per non parlare dello spionaggio che, secondo le risultanze del rapporto CLUSIT, crescono di quasi il 40% a testimonianza che siamo davanti a una vera e propria strategia.

Le infrastrutture critiche, e forse questo è il dato più preoccupante, sono oggetto di attacco costante se si considera che le nostre stime parlando di un aumento degli attacchi di oltre il 150%!

E poi c'è la modalità di attacco che più di ogni altro ha fatto parlare del tema nel corso del 2015: i *ransomware*. Vera e propria estorsione informatica la cui diffusione, e la conseguente capacità di generare denaro, non conosce limiti.

Stiamo quindi davanti a uno scenario che si potrebbe definire da incubo.
Attacchi alla vita quotidiana delle persone, attacchi alle infrastrutture che permettono alla società civile di continuare a essere tale, attacchi alle attività che permettono alle aziende di funzionare e alle pubbliche amministrazioni di erogare i servizi essenziali ai cittadini.

Questo scenario, che nel corso del 2015 si è materiarializzato nei casi di cronaca italiani e internazionali che tanto hanno fatto discutere, è per fortuna controbilanciato da un livello di attenzione che pian piano sta salendo. Aziende e pubbliche amministrazioni parlano della sicurezza e delle modalità e tecnologie per combattere il cybercrime come mai prima d'ora.

Anche i fatti di cronaca, seppur negativi se non drammatici per chi ne è stato coinvolto, aiutano. Vedere cosa succede agli altri ha effetto meno solo del subire noi stessi un attacco. E allora quali sono i settori dove si sono registrati maggiori attacchi: i servizi cloud, dalle webmail ai social network (con ciò dando ragione alle stime e previsioni del Rapporto CLUSIT dello scorso anno), siti di e-commerce e piattaforme cloud pubbliche, con un aumento del'81% degli attacchi rispetto all'anno 2014. E poi l'informazione e il gioco, se si considera che piattaforme di blogging e gaming hanno subito nel 2015 un numero di attacchi di quasi l'80% in più rispetto all'anno 2014.

Molto colpito anche il settore automotive (+67%) e il mondo della ricerca e della educazione (+50%) a dimostrazione che come sempre non ci sono limiti: ogni settore è a rischio.

Preoccupante anche che le tecniche di attacco utilizzate in oltre la metà dei casi gravi registrati nel 2015 siano state di livello banale, con sfruttamento di vulnerabilità note a dimostrazione che l'aumento di attenzione sul cybercrime ancora non si accompagna a un aumento rilevante della capacità di difesa.

Infine il darkweb: vero e proprio buco nero dove droga, terrorismo, armi e pedo-pornografia sembrano convivere in un ecosistema del tutto a sé stante.

E allora vi lascio alla lettura del Rapporto CLUSIT che avete fra le mani sperando che anche quest'anno la nostra ricerca serva ad aumentare la consapevolezza della necessità di una maggiore e sempre più efficace sicurezza.

2.500 copie cartacee, oltre 60.000 copie in elettronico e più di 200 articoli pubblicati nel 2015, sono l'evidenza della rilevanza del Rapporto CLUSIT ed è quindi importante diffonderlo, leggerlo, farlo conoscere, perché solo dalla consapevolezza può derivare la conoscenza del problema, la capacità di adottare scelte idonee e quindi la sicurezza nostra e di tutti.

Buona lettura

Gabriele Faggioli
Presidente CLUSIT

Introduzione al rapporto

Il Rapporto Clusit 2016 sulla sicurezza ICT in Italia è frutto del lavoro di un centinaio di esperti e della collaborazione di un gran numero di soggetti pubblici e privati, che hanno condiviso con Clusit informazioni e dati di prima mano e condiviso le proprie esperienze sul campo.
Il Rapporto inizia con una panoramica degli eventi di cyber-crime e incidenti informatici più significativi del 2015. Si tratta di un quadro estremamente aggiornato della situazione globale, con particolare attenzione all'Italia. In numero assoluto gli attacchi gravi di dominio pubblico sono aumentati, raggiungendo i 1.012 (erano 873 nel 2014).

In percentuale, rispetto al 2014, crescono Cybercrime (+30%) ed Espionage (+40%). In aumento, rispetto al 2014, gli attacchi verso i settori: Entertainment / News + 79% ; Research / Edu + 50%; Online Services (record di sempre in valori assoluti) + 80%; Critical Infrastructures + 150%. Stabili o in leggera crescita gli attacchi noti verso gli altri settori. Abbiamo inserito la nuova categoria Ospitalità perché abbiamo rilevato circa 40 attacchi contro alberghi e simili (tipicamente per colpirne i clienti).
Ci siamo avvalsi anche quest'anno dei dati relativi agli attacchi rilevati dal Security Operations Center (SOC) di FASTWEB, che ha analizzato la situazione italiana sulla base di oltre 8 milioni di eventi di sicurezza.
L'analisi degli attacchi è poi completata da due contributi tecnici di grande interesse: "Alcuni elementi sul cyber-crime in ambito finanziario con focus sull'Europa", a cura di IBM, e il "Rapporto 2015 sullo stato di Internet ed analisi globale degli attacchi DDoS", a cura di Akamai.

Quest'anno si sono aggiunte le rilevazioni e segnalazioni del CERT Nazionale e del CERT-PA e un contributo su "L'ecosistema criminale nel Dark Web".
Una delle chicche di questa edizione del Rapporto è lo "Speciale Milano EXPO 2015", che racconta l'esperienza di coloro che si sono occupati della gestione della sicurezza e degli attacchi avvenuti durante l'EXPO: Cisco Systems, il CERT di Poste Italiane e il C.N.A.I.P.I.C. (nucleo speciale in seno alla Polizia Postale).
Altra novità del Rapporto Clusit 2016 è un'analisi del mercato italiano della sicurezza IT, realizzata appositamente da IDC Italia.

Questi infine sono i temi trattati nella sezione FOCUS ON: Assicurare il rischio informatico (con il contribuito di CHUBB e Margas); E-Commerce (a cura di @Mediaservice.net e Netcomm); Il furto di credenziali (a cura di Microsoft); Nuovi modelli di prevenzione e di gestione degli incidenti (a cura di Hewlett Packard Enterprise); Le nuove sfide nel campo della Robotica (a cura del Tech and Law Center); La Sicurezza del Database (a cura di Oracle); Le prospettive per la Mobile Security nel 2016 (a cura di G DATA).

Panoramica dei cyber attacchi più significativi del 2015 e tendenze per il 2016

La punta dell'iceberg

In questa prima sezione del Rapporto CLUSIT 2016, giunto ormai al suo quinto anno di pubblicazione[1], analizziamo i più gravi attacchi informatici noti avvenuti a livello globale negli ultimi 11 semestri e l'impatto che questi hanno avuto, tentando di fornire un'interpretazione ragionata di quanto sta succedendo sul fronte della (in)sicurezza cibernetica[2], di individuarne le cause e di delineare le tendenze in atto.
Come da tradizione questa analisi, pur basandosi sull'attenta valutazione di tutte le informazioni disponibili in merito a ciascuno degli oltre 5.200 attacchi di dominio pubblico da noi classificati come gravi tra il gennaio 2011 e il giugno 2016 (dei quali 521 occorsi nel primo semestre 2016), è volutamente espressa con un linguaggio non-tecnico, in modo da risultare fruibile al maggior numero possibile di lettori.
Va sottolineato che le conclusioni presentate di seguito sono relative all'analisi di un campione ragionevolmente significativo ma certamente limitato degli incidenti più eclatanti, ovvero alla "punta dell'iceberg" di tutti gli attacchi informatici particolarmente gravi, avvenuti in Italia e nel mondo dal 2011, sia perché *la maggior parte* di tali aggressioni non diventano di dominio pubblico (mancando ancora una normativa che renda obbligatorio renderli noti[3], salvo alcuni ristretti settori regolamentati), sia perché spesso le conseguenze più gravi si evidenziano ad anni di distanza (p.es. nel caso di furto di proprietà intellettuale con finalità di spionaggio economico, o di compromissione preventiva di sistemi critici per ragioni geopolitiche).
Tipicamente in questo campione sono ben rappresentate quelle tipologie di attacchi in cui, per varie ragioni, l'aggressore non è riuscito a rimanere nascosto ed a muoversi silenziosamente (oppure non ha voluto nascondersi), mentre rispetto alla realtà dei fatti percepibile "sul campo" dagli addetti ai lavori sono meno rappresentate le aggressioni condotte lentamente, con tecniche sofisticate e senza destare sospetti nelle vittime.
Ciò premesso, confidando che anche questa edizione aggiornata del Rapporto CLUSIT 2016 possa apportare un utile contributo al crescente dibattito nazionale in merito alla Cyber Security[4], e che possa in particolare supportare il corretto inquadramento delle numerose dimensioni del problema (unica strada percorribile per definire celermente soluzioni concrete e sostenibili), auguriamo a tutti una buona lettura!

---

1 Ovvero alla decima edizione, considerando anche gli aggiornamenti semestrali

2 https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/principi-strategici-delle-politiche-di-cyber-security.html

3 https://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/dbn

4 https://www.youtube.com/watch?v=FbEMFyKoX8s

2016, il rischio "cyber" diventa inaccettabile

Nella seconda edizione del Rapporto CLUSIT, completata nel gennaio 2013, in merito all'impreparazione dell'Italia nei confronti delle crescenti minacce cibernetiche scrivevamo: *Mancano una adeguata consapevolezza da parte di tutti gli attori interessati, le competenze tecniche, il coinvolgimento delle parti sociali, della scuola, delle istituzioni e della politica, mancano gli investimenti e soprattutto manca la visione prospettica necessaria ad affrontare un problema tanto complesso, che richiede tempi di reazione rapidissimi e soluzioni multidisciplinari, coordinate, sofisticate, a fronte di un assalto continuo, su tutti i fronti, che va avanti 24 ore su 24 e che ormai costa alla nazione miliardi di euro all'anno di danni diretti ed indiretti. Riducendo sostanzialmente queste perdite si potrebbe recuperare quasi un punto di PIL: possiamo permetterci di non farlo?*

A oltre 48 mesi di distanza dobbiamo rilevare due fenomeni contrastanti, i quali introducono timide ragioni di ottimismo in uno scenario che purtroppo, generalmente parlando, appare assai poco attraente, essendo nel frattempo sensibilmente peggiorato.

Da un lato proprio a partire dal 2013 l'Italia si è dotata di un valido "Quadro strategico nazionale per la sicurezza dello spazio cibernetico"[5], quindi di un articolato "Piano nazionale per la protezione cibernetica e la sicurezza informatica"[6]. Segnaliamo inoltre la pubblicazione, nel febbraio 2016 di un primo "Framework Nazionale di Cyber Security"[7], frutto di un'inedita partnership tra pubblico e privato, per una volta anticipando analoghe iniziative europee[8].

Dall'altro lato però in questi ultimi 48 mesi l'insicurezza cibernetica a livello globale (e pertanto anche in Italia) è cresciuta in modo significativo, le tipologie di aggressori si sono moltiplicate (pensiamo non solo al braccio "digitale" dell'Islamic State ma anche ad altri gruppi di spionaggio e information warfare) e le perdite economiche sono aumentate di 4 volte[9]. Contestualmente si è assistito ad un fenomenale incremento della *superficie di attacco* esposta dalla nostra società digitale, sempre più iper-connessa, anche in conseguenza della massiccia adozione di nuove tecnologie "facili", a basso costo, che sono intrinsecamente poco o per nulla sicure se confrontate con le capacità di nuocere degli avversari.

E' innegabile che l'impiego spesso congiunto di queste tecnologie (in particolare Social Media, Cloud, Mobile ed Internet of Things) stia dando luogo ad una rivoluzione rapidissima dei processi produttivi, degli stili di vita e dei rapporti socio-economici.

La velocità e l'intensità di questa rivoluzione sono però determinate principalmente da esigenze contingenti di business, che quasi mai includono la Cyber Security tra le reali priorità di progetto ed esercizio di un processo produttivo o di un servizio; ciò avviene per ragioni

---

5 http://www.agid.gov.it/sites/default/files/leggi_decreti_direttive/quadro-strategico-nazionale-cyber_0.pdf

6 https://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/la-cyber-strategy-italiana.html

7 http://www.cybersecurityframework.it/

8 https://ec.europa.eu/digital-agenda/en/news/public-consultation-public-private-partnership-cybersecurity-and-possible-accompanying-measures

9 http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/

culturali, economiche e perché non sussistono obblighi particolari in tal senso.
D'altra parte le organizzazioni sono da anni alle prese con tagli di budget volti ad ottimizzare la spesa ICT: la risultante di questi due dinamiche è che le innumerevoli, crescenti applicazioni delle nuove tecnologie sono *inevitabilmente soggette a rischi sempre maggiori*, malamente o per nulla gestiti, gli impatti dei quali naturalmente ricadono sui loro gestori, sui loro utenti e potenzialmente, per effetto-domino, sull'intera collettività.
Pur rallegrandoci quindi per l'oggettivo miglioramento della situazione nazionale, quantomeno in prospettiva, dobbiamo rilevare con forte preoccupazione che la velocità e la determinazione con le quali si stanno muovendo Istituzioni, imprese e cittadini rispetto alla dimensione ed alle possibili conseguenze dell'attuale minaccia cibernetica non sono ancora in grado di fare la differenza.
Le risorse, le competenze e gli investimenti necessari non sono ancora disponibili in misura sufficiente: per dare un'idea, pur fatte le debite proporzioni, il budget 2016 per il Cybersecurity National Action Plan (CNAP) recentemente sottoposto dal Presidente Obama al Congresso USA è di 19 miliardi di dollari[10], cifra che non include le "cyber" spese militari e di intelligence. Da noi invece non si è ancora raggiunto il necessario equilibrio tra investimenti, stimoli (p.es. agevolazioni fiscali o di altro tipo per le organizzazioni virtuose) ed oneri (p.es. sanzioni e conseguenze legali per quelle non virtuose). Tutta la questione in Italia galleggia ancora in un limbo dal quale è essenziale che si esca al più presto, essendosi nel frattempo esaurito il tempo per le tattiche, il lobbying sterile, le burocrazie e le manovre politiche.
Soprattutto da parte dell'Esecutivo, pur rilevando segnali di un rinnovato interesse[11] del Governo per la materia, stimolato anche dall'approvazione da parte del Parlamento Europeo, il 6 luglio 2016, della Network and Information Security (NIS) Directive europea[12], non è stata ancora messa a regime una operatività univoca e condivisa tra i vari elementi che costituiscono l'architettura istituzionale di sicurezza cibernetica, il che determina impatti deteriori non solo sulla sicurezza ma anche sulla credibilità complessiva del Paese[13] nei confronti di alleati ed avversari, che ci osservano attentamente, misurandoci ogni giorno sul campo.
Va detto pertanto a chiare lettere, come si evincerà anche dai dati presentati più avanti, che negli ultimi 3 anni il divario tra percezione dei rischi "cyber" e realtà, e la forbice tra la gravità di questi rischi e l'efficacia delle contromisure poste in essere *si sono ulteriormente allargati, non ridotti*.
Sintetizzando, nella situazione attuale i crescenti rischi "cyber" non sono ancora gestiti in modo efficace, ovvero sono fuori controllo, ed in quanto tali, per la stessa definizione di rischio, devono essere considerati inaccettabili.

---

10 https://www.whitehouse.gov/blog/2016/02/09/presidents-national-cybersecurity-plan-what-you-need-know

11 https://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/normativa-di-riferimento/direttiva-1-agosto-2015.html

12 https://ec.europa.eu/digital-agenda/en/news/network-and-information-security-nis-directive

13 http://www.repubblica.it/tecnologia/sicurezza/2016/01/20/news/sicurezza_informatica_lettera_aperta_renzi-131683869/

In cosa consiste la Cyber Security?

Sui giornali, ai convegni, nelle presentazioni commerciali si evidenzia una notevole confusione in merito al significato dell'espressione "Cyber Security". Il Generale americano Michael Hayden (ex-direttore della CIA e della NSA) ha detto: "Raramente nella storia abbiamo avuto a che fare con una questione così importante ed allo stesso tempo così poco definita e compresa"[14].
In alcuni casi sembra che si tratti solo di un nuovo nome accattivante per la sicurezza informatica, riverniciata e riproposta tale e quale, come se fossimo ancora nel lontanissimo 2010. In altri casi questo termine viene ripetuto come una sorta di mantra, usato per invocare una qualche forma di magia, in grado di scacciare i demoni e di controllare il Genio digitale sfuggito dalla Lampada.

In realtà l'espressione Cyber Security indica un gruppo di attività e competenze multidisciplinari, complesse e sofisticate, molte delle quali *non informatiche*, che sono oggettivamente di difficile integrazione con le prassi esistenti di gestione dell'ICT e di allocazione dei budget relativi, poiché la loro implementazione richiede di superare paradigmi tecnologici e silos organizzativi costruiti negli anni a partire da esigenze di compliance e da metodi e strumenti propri della sicurezza informatica "tradizionale".
Il modello di sicurezza oggi più diffuso, evolutosi nel tempo per presidiare un perimetro molto più definito e semplice di quello attuale, a fronte di minacce molto più contenute, essendo reattivo agisce dopo che l'incidente si è già verificato (ovvero, nel migliore dei casi, durante). Alla luce delle nuove minacce questo approccio non costituisce più una forma di mitigazione del rischio significativa ed anzi mostra di possedere un'efficacia residuale e decrescente. Pertanto, interpretando in questo senso restrittivo la Cyber Security, essa non potrà mai risultare adeguata, diventando nel tempo un costo insostenibile a fronte di risultati scarsi, e/o costringendo ad accettare rischi eccessivi, certamente maggiori di quanto sarebbe ragionevole desiderare.
Per quanto ad oggi non esista una definizione esaustiva ed accettata di Cyber Security (nessuno ha osato finora formularla, e non saremo noi a provarci), possiamo senz'altro enunciare lo scopo complessivo di questo insieme di discipline: *proteggere tutti quegli asset materiali ed immateriali che possono essere aggrediti tramite il "cyberspazio" ovvero che dipendono da esso, garantendo allo stesso tempo la governance, l'assurance e la business continuity di tutta l'infrastruttura digitale a supporto.*
Di conseguenza, data l'enormità del suo ambito di applicazione, la Cyber Security in primo luogo non può che basarsi su logiche di *prevenzione, riduzione e trasferimento del rischio* e su processi di *Risk Governance*[15], applicati però ad un dominio caotico, dai confini e dalle dinamiche sempre cangianti, il quale pertanto va presidiato costantemente, 24x7, da per-

[14] http://www.darkreading.com/attacks-breaches/former-director-of-nsa-and-cia-says-us-cybersecurity-policy-mia/d/d-id/1323888

[15] https://en.wikipedia.org/wiki/Risk_governance

sonale qualificato dotato di metodologie di *Risk Management*[16] e strumenti adeguati (p. es. tool di analisi comportamentale, big data analytics, intelligenza artificiale, etc), capaci di operare *in tempo reale*.
In secondo luogo, per definire puntualmente la componente esogena del rischio, ovvero la probabilità che una minaccia esterna si realizzi, è necessario impiegare metodologie e strumenti di *Cyber Intelligence* capaci di osservare, tramite un monitoraggio continuo, l'esterno e l'interno con altrettanta attenzione, e di correlare i due domini. Anche in questo caso si tratta di sviluppare competenze sofisticate e di implementare processi nuovi, diversi rispetto alle prassi consolidate, considerando che oggi, nel migliore dei casi, le organizzazioni sono strutturate solo per osservare ciò che avviene nell'ambito di propri confini prestabiliti (i quali peraltro stanno ormai diventando sempre più porosi, a causa delle nuove tecnologie).

In terzo luogo è necessario definire e costantemente aggiornare il proprio *modello di minaccia*, ovvero individuare quale tra le diverse tipologie di attaccanti vorrà aggredire quale asset, perché, sfruttando quale vulnerabilità, con quali strumenti, atteggiamento, risorse etc. Anche questa attività di *Threat Modeling*[17] non può che essere continuativa ed integrarsi opportunamente con i processi di Risk Management e Cyber Intelligence, per fornire al primo delle metriche precise ed aggiornate su cui ragionare, ed alla seconda indicazioni in merito a quale ago cercare nel pagliaio del cyberspazio.
Tutte queste attività di difesa preventiva, costante, a 360°, si potranno realizzare solo grazie ad un forte impegno da parte di tutti gli stakeholders interessati, ed avranno successo esclusivamente nell'ambito di un ampio e snello coordinamento tra pubblico e privato, tra imprese e cittadini, tra amministrazioni centrali e locali, tra dipendenti e clienti, coinvolgendo nella formazione e nella prevenzione tutti i collaboratori ed i partner (inclusi i non-tecnici), dal momento che l'iper-connessione della civiltà digitale ed i costi della Cyber Security non consentono di giocare questa partita in solitario, o solo tra specialisti. Questo perché l'insicurezza cibernetica è di fatto ormai un problema di "salute pubblica", come una pandemia, che come tale va indirizzato e gestito, con il coinvolgimento e la collaborazione di tutti.
Mitigare gli inevitabili impatti di questa pandemia è l'obiettivo primario al quale si deve tendere, cominciando quanto prima con l'individuare e recuperare i gap più pericolosi, tenendo presente che il tempo a disposizione per intervenire in modo strutturato sui rischi "cyber", in particolare su quelli di natura sistemica (per il Paese) ed esistenziale (per le singole organizzazioni), è ormai sostanzialmente esaurito.

[16] https://en.wikipedia.org/wiki/Risk_management

[17] https://en.wikipedia.org/wiki/Threat_model

Analisi dei principali cyber attacchi noti a livello globale del primo semestre 2016

Nel precedente Rapporto CLUSIT 2015, alla luce dei trend individuati scrivevamo:
"dunque la vera questione per i difensori (con riferimento ai dati, alle infrastrutture informatiche ed a tutti quei servizi, molti dei quali critici, oggi realizzati tramite l'ICT) non è più "se", ma "quando" si subirà un attacco informatico (dalle conseguenze più o meno dannose), e quali saranno gli impatti conseguenti".
Questa tendenza si è ulteriormente consolidata nell'anno passato e nel 2016 il principale problema non è tanto che si verrà attaccati (tutti lo sono ormai costantemente, per lo più tramite sistemi automatizzati, nella sfera personale e professionale, per i motivi più disparati), ma quali saranno gli impatti degli attacchi andati a buon fine sulla sicurezza di organizzazioni, utenti, clienti e partner, e come impedire al maggior numero possibile di incidenti di verificarsi.
Per contribuire alla comprensione dell'evoluzione degli scenari, anche quest'anno l'aggiornamento pubblicato ad ottobre del Rapporto CLUSIT propone una dettagliata panoramica degli incidenti di sicurezza più significativi avvenuti a livello globale nel primo semestre dell'anno, confrontandoli una serie storica quinquennale.
Lo studio si basa su un campione complessivo di oltre 5.200 incidenti noti di particolare gravità, ovvero che hanno avuto un impatto particolarmente significativo per le vittime in termini di perdite economiche, di reputazione, di diffusione di dati sensibili (personali e non), o che comunque prefigurano scenari particolarmente pericolosi, avvenuti nel mondo (inclusa l'Italia) dal primo gennaio 2011 al 30 giugno 2016, di cui 1.012 registrati nel 2015 e 521 nel primo semestre 2016.
Anche quest'anno, per definire un cyber attacco come "grave" abbiamo impiegato gli stessi criteri di classificazione già applicati ai dati del 2014, più restrittivi rispetto agli anni precedenti, dal momento che nell'arco di questi 72 mesi si è verificata una sensibile evoluzione degli scenari, e che alcune categorie di attacchi, che potevano essere ancora considerati "gravi" nel 2011-2013, sono oggi diventati *ordinaria amministrazione*.

A parità di criteri, nel primo semestre 2016 abbiamo classificato come gravi un numero di attacchi superiore rispetto al secondo semestre 2015, pur avendo scartato una grandissima quantità di incidenti "minori" per evitare di confrontare, nell'ambito dello stesso campione, situazioni che hanno causato la perdita di milioni di euro o il furto di milioni di account con, per fare un esempio tra molti, un attacco DDoS di lieve entità verso una banca o un sito web istituzionale. Ciò non significa che questo genere di attacchi ad impatto minore non sia a sua volta in rapida crescita.

Dieci attacchi rappresentativi del 2015

Prima di analizzare quanto avvenuto nel corso dell'anno passato, quest'anno vogliamo partire da dieci incidenti del 2015 a nostro avviso particolarmente significativi, selezionati non tanto per la loro gravità in termini assoluti (per quanto alcuni siano stati particolarmente gravi), quanto piuttosto per rappresentare la varietà di situazioni che si stanno verificando.

Vittima	Attaccante	Tecniche usate
Anthem[18]	Cyber Espionage (Deep Panda)?	APT, Custom Malware

L'attacco a questa primaria compagnia di assicurazione sanitaria, iniziato ad aprile 2014 ma scoperto solo a gennaio 2015, ha provocando il furto di circa 80 milioni di record contenenti i dati personali dei clienti e degli impiegati (CEO compreso) compresi nomi, date di nascita, indirizzi email, dati sul reddito e altro ancora.
La stima dei danni è ancora in corso, ma si preannuncia molto pesante sia in termini di immagine che di risarcimenti agli utenti.
Alcuni sospettano che il gruppo responsabile sia lo stesso dell'attacco all'Office of Personnel Management (vedi più sotto), il che getterebbe una luce ancora più preoccupante sull'intera vicenda (dal momento che Anthem assicura la maggior parte dei dipendenti federali, militari inclusi).

Vittima	Attaccante	Tecniche usate
Ashley Madison[19]	Impact Team (per vendetta?)	Vulnerabilities / SQL Injection

Un gruppo sconosciuto di hackers denominato "Impact Team" è riuscito a compromettere da remoto il database dei 37 milioni di utenti di Ashley Madison, servizio web di incontri per adulti espressamente dedicato alle avventure extraconiugali, minacciando la sua casa madre (Avid Life Media) di pubblicarlo qualora il sito non fosse stato messo offline.
L'azienda ha rifiutato, pertanto l'intero database è stato reso pubblico, causando un notevole scandalo ed importanti disagi per milioni di persone.
Il gruppo ha proseguito pubblicando anche numerose email interne e documenti riservati di Avid Life Media, alcuni dei quali particolarmente scottanti, causando tra l'altro le dimissioni dell'amministratore delegato Noel Biderman.

[18] http://www.theguardian.com/us-news/2015/feb/05/millions-of-customers-health-insurance-details-stolen-in-anthem-hack-attack
[19] http://fortune.com/2015/08/26/ashley-madison-hack/

Alcuni utenti del servizio si sono suicidati per la vergogna (per esempio il pastore John Gibson)[20], in molti altri casi sono intervenute cause di separazione, e sono state attivate diverse class-action per il risarcimento dei danni, che si preannunciano miliardari.

Vittima	Attaccante	Tecniche usate
Oltre 100 Istituti bancari[21]	Cyber Crime organizzato	Phishing / Custom Malware

La più grande cyber-rapina del 2015, e probabilmente di tutti i tempi, è stata compiuta ai danni di oltre 100 istituti bancari appartenenti a più di 30 paesi del mondo, Italia inclusa con un danno stimato di almeno 1 miliardo di dollari.
Fin dalla fine del 2013 i cyber criminali responsabili dell'operazione "Carbanak" (così denominata da alcuni investigatori, in altre varianti detta "Anunak") hanno infiltrato con tecniche di phishing diverse organizzazioni finanziarie, infettandole con malware realizzato ad-hoc.
Grazie a questo malware i criminali hanno studiato attentamente le procedure ed i flussi interni delle banche colpite, riuscendo a sottrarre ingenti quantità di denaro tramite operazioni apparentemente lecite ed autorizzate. Pur essendo stata scoperta nel 2015, l'operazione "Carbanak" risulta essere ancora in corso[22], questa volta mirata oltre alle banche anche a società finanziarie, di trading online, catene alberghiere e casinò.

Vittima	Attaccante	Tecniche usate
Hacking Team[23]	Ignoto (insider ?)	Sconosciute

L'azienda italiana Hacking Team, specializzata nella produzione di software dedicato all'infiltrazione di device digitali (PC e mobile) con finalità investigative e di intelligence, è stata colpita da ignoti, che hanno copiato e pubblicato online una impressionante quantità di informazioni sensibili (oltre 400 Gigabyte).
In questo modo sono state rese pubbliche milioni di email, codici sorgenti, segreti industriali (inclusi alcuni exploit "zero-day", che sono stati prontamente riciclati da organizzazioni cyber criminali)[24] e informazioni riservate relative ai clienti dell'azienda, in molti casi molto delicate. Oltre al danno economico e di immagine per l'azienda, l'attacco ha aperto uno squarcio inquietante su un area piuttosto *borderline* della Cyber Security, che richiederebbe maggiore attenzione e supervisione.

---

20 http://www.seattletimes.com/opinion/editorials/elegy-for-john-gibson-an-average-guy-caught-in-the-ashley-madison-mess/

21 https://securityintelligence.com/carbanak-how-would-you-have-stopped-a-1-billion-apt-attack/

22 http://www.net-security.org/secworld.php?id=18831

23 http://www.corriere.it/tecnologia/cyber-cultura/cards/hacking-team-spioni-milanesi-hackerati-rubati-400-gb-documenti/furto-dati_principale.shtml

24 http://www.computerworld.com/article/2945495/security/cybercriminals-start-using-flash-zero-day-exploit-leaked-from-hacking-team.html

Vittima	Attaccante	Tecniche usate
Dipartimento di Stato USA[25]	**Cyber Espionage (russo ?)**	APT / Custom Malware

A pochi mesi di distanza dalla scoperta di una seria compromissione della rete non classificata della Casa Bianca (ottobre 2014), che aveva consentito agli aggressori di accedere a email ed agenda del Presidente americano e dei suoi collaboratori, si è scoperto (marzo 2015) che lo stesso gruppo (molto probabilmente state-sponsored) è riuscito a penetrare anche il sistema di posta del Dipartimento di Stato, mantenendovi l'accesso per diversi mesi. Per bloccare l'attacco, definito da un portavoce "il peggiore di sempre", l'amministrazione è stata costretta a fermare i sistemi ed a re-installarli da zero.

Vittima	Attaccante	Tecniche usate
Experian / T-Mobile[26]	Cyber Crime	Sconosciute

Cyber criminali hanno aggredito la società di recupero crediti Experian, sottraendo i dati di quindici milioni di clienti dell'operatore di telefonia T-Mobile, che aveva affidato all'azienda un contratto per il loro screening finanziario.
Tra i dati delle vittime nome, indirizzo, data di nascita, email e codice fiscale. Questo genere di furti su larga scala viene solitamente realizzato per facilitare ulteriori crimini, quali il furto di identità, tramite il quale poi si realizzano truffe online di vario genere. L'incidente dimostra l'urgenza di gestire correttamente (su vari piani, da quello legale a quello tecnologico) l'affidamento a terze parti dei dati di propri utenti.

Vittima	Attaccante	Tecniche usate
Direttore CIA John Brennan[27]	CWA - "Crackas With Attitude" ?	Social Engineering

Un sedicente gruppo di hacker adolescenti (CWA) ha annunciato di aver violato una casella mail personale su America on Line (AOL), appartenente al capo della CIA John Brennan. I ragazzi hanno affermato che "ci sarebbe riuscito anche un bambino di 5 anni", spiegando di aver utilizzato banali tecniche di social engineering nei confronti di Verizon (ISP di Brennan) e AOL (provider del servizio di posta) per ottenere l'accesso. Per la natura particolare del target e per le modalità "professionali" della rivendicazione da parte di CWA, gli autori potrebbero non essere dei semplici adolescenti annoiati, come alcuni suppongono[28].

[25] http://edition.cnn.com/2015/03/10/politics/state-department-hack-worst-ever/index.html

[26] http://www.itgovernanceusa.com/blog/15-million-t-mobile-records-hacked-says-experian/

[27] https://www.rt.com/usa/hackers-cia-brennan-financial-records-334/

[28] https://motherboard.vice.com/read/hacker-publishes-personal-info-of-20000-fbi-agents

Wikileaks ha poi raccolto e pubblicato una "selezione" di email e documenti sottratti dall'account di Brennan, dal titolo "The CIA Files"[29].

Vittima	Attaccante	Tecniche usate
VTech – smart toys e gadgets[30]	Hacker "etico" ?	SQL Injection

Le informazioni personali di circa 5 milioni di genitori ed oltre 200.000 ragazzi sono state rubate a seguito della compromissione di un sito web della società VTech, azienda cinese da 2 miliardi di dollari di fatturato che vende giocattoli e gadgets "smart", ovvero connessi ad Internet (p.es. tablet per ragazzi, baby monitor per neonati, tastiere musicali, etc).
Cosa ancora più preoccupante, nel database del sito sono state reperite migliaia di fotografie dei bambini, scattate tramite i giocattoli, complete di nome, cognome, indirizzo, data di nascita etc. Fortunatamente l'hacker che ha scoperto la vulnerabilità non ha rivenduto i dati nell'underground né li ha diffusi integralmente.
L'azienda non si è accorta della compromissione finché i giornali non hanno pubblicato la notizia, informati dall'hacker[31].

Vittima	Attaccante	Tecniche usate
OPM - Office of Personnel Management[32]	Cyber Espionage (Deep Panda)?	Known Vulnerabilities

L'Agenzia USA incaricata di effettuare il controllo dei precedenti sugli impiegati governativi americani (civili e militari) è stata violata sfruttando vulnerabilità note di software obsoleti. Ciò ha consentito agli attaccanti di sottrarre informazioni molto sensibili, relative a tutti i dipendenti federali dal 2000 in avanti (oltre 4 milioni di dipendenti e complessivamente 22 milioni di persone soggette a screening)[33].
L'attacco, che le autorità USA attribuiscono al governo cinese (il quale ha prontamente smentito qualsiasi coinvolgimento), ed in particolare al gruppo "Deep Panda", ha anche consentito di sottrarre informazioni in merito ai livelli di "clearance" di ciascun dipendente federale, inclusi i livelli Secret e Top Secret, e di ottenere oltre 1 milione di impronte digitali[34].
Il direttore dell'Agenzia, Katherine Archuleta, ha dato le dimissioni.

29 https://www.hackread.com/wikileaks-cia-john-brennans-hacked-email/

30 http://www.techinsider.io/childrens-toymaker-vtech-hacked-kids-pictures-stolen-2015-11

31 http://motherboard.vice.com/read/one-of-the-largest-hacks-yet-exposes-data-on-hundreds-of-thousands-of-kids

32 http://arstechnica.com/security/2015/06/epic-fail-how-opm-hackers-tapped-the-mother-lode-of-espionage-data/

33 http://www.reuters.com/article/us-cybersecurity-usa-idUSKCN0PJ2M420150709

34 http://money.cnn.com/2015/07/10/technology/opm-hack-fingerprints/

Vittima	Attaccante	Tecniche usate
Ukraine Power Grid / Kiev Airport [35]	Information Warfare	APT / Custom Malware

A dicembre un attacco realizzato tramite malware (BlackEnergy ed altri) ha consentito agli attaccanti di alterare il funzionamento di alcune sottostazioni della rete elettrica ucraina, con il risultato di provocare un black-out che ha interessato circa 80.000 utenze[36]. È il primo caso noto al mondo di black-out provocato maliziosamente (ovvero non per guasto o per errore umano) con mezzi "cyber".

L'attacco è stato coordinato con grande precisione, e gli aggressori si sono addirittura premurati di rallentare le attività di ripristino fornendo dati falsi ai manutentori tramite le interfacce delle sottostazioni, e/o cancellando le configurazioni dei sistemi. Attacchi simili sono stati portati anche verso l'aeroporto di Kiev Boryspil[37], causando il blocco di alcuni sistemi IT per un intero week-end.

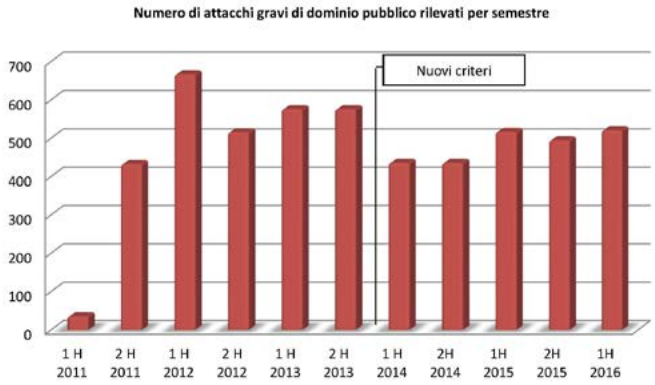
35 http://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid

36 http://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/

37 http://www.theregister.co.uk/2016/01/18/blackenergy_power_outage_malware_kiev_airport/

Analisi dei principali attacchi noti a livello globale

Dei 5.209 attacchi gravi di pubblico dominio che costituiscono il nostro database di incidenti degli ultimi 5 anni e mezzo, nel primo semestre 2016 ne abbiamo analizzati 521, contro i 495 del secondo semestre 2015 (+ 5%). Questa la distribuzione degli attacchi registrati nel periodo, suddivisi per semestre:



© Clusit - Rapporto 2016 sulla Sicurezza ICT in Italia - Aggiornamento Giugno 2016

Va tenuto presente che i dati di seguito sintetizzati rappresentano solo una frazione, per quanto significativa, del totale degli attacchi gravi presumibilmente andati a buon fine nel corso del primo semestre di quest'anno.
Questo campione infatti presenta ragionevolmente delle lacune, dovute al fatto che alcuni ambienti sono particolarmente efficaci nel minimizzare la diffusione pubblica di informazioni relative agli attacchi che subiscono, e risultano pertanto qui sotto-rappresentati.
Inoltre mentre ad oggi negli Stati Uniti è in vigore una normativa che obbliga le vittime a fare disclosure a seguito di un data breach, così non è nella maggior parte delle altre nazioni, Europa inclusa, di conseguenza gli attacchi noti contro bersagli americani risultano essere la maggioranza.
Infine alcuni tipi di attacchi (i più subdoli e silenziosi, per esempio quelli legati allo spionaggio industriale, o ad attività di Information Warfare) sono compiuti nell'arco di periodi piuttosto lunghi e dunque, sempre che diventino di dominio pubblico, emergono solo ad anni di distanza[38].

Le tre tabelle seguenti rappresentano una sintesi dei dati che abbiamo raccolto.
Come in passato abbiamo segnalato in arancio gli incrementi percentuali positivi, mentre abbiamo evidenziato nella colonna più a destra i trend osservati.

[38] https://www.securelist.com/en/blog/208216078/The_Careto_Mask_APT_Frequently_Asked_Questions

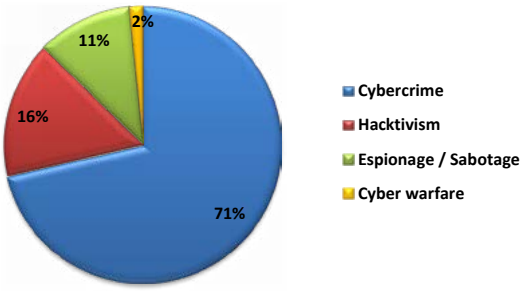
Distribuzione degli attaccanti per tipologia

ATTACCANTI per tipologia	2011	2012	2013	2014	2015	2H 2015	1H 2016	Variazioni 1H 2016 su 2H 2015	Trend 2016
Cybercrime	170	633	609	526	684	272,35%	-3,79%	9,41%	↑
Hacktivism	114	368	451	236	209	222,81%	22,55%	-4,60%	→
Espionage/ Sabotage	23	29	67	69	96	26,09%	131,03%	9,43%	↑
Cyber Warfare	14	43	25	42	23	207,14%	-41,86%	-46,67%	↓
TOTALE	469	1.183	1.152	873	1.012	495	521	5,25%	↑

© Clusit - Rapporto 2016 sulla Sicurezza ICT in Italia – *Aggiornamento al 30 giugno 2016*

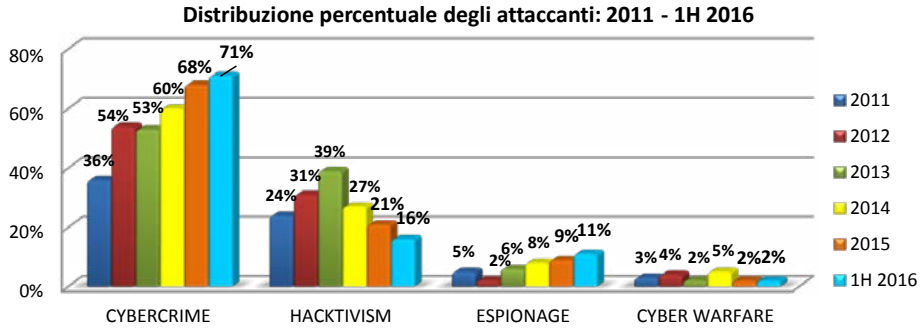
Complessivamente, rispetto al semestre precedente, il numero di attacchi gravi registrati cresce del 5%. Dal campione emerge chiaramente che, con l'esclusione delle attività riferibili ad attaccanti della categoria "Information Warfare" e "Hacktivism", dal punto di vista numerico nel primo semestre 2016 gli attacchi gravi di pubblico dominio compiuti per altre finalità sono in aumento rispetto al secondo semestre 2015, in particolare per quanto riguarda la categoria "Cybercrime", che presenta un tasso di crescita del +9% rispetto al periodo precedente.
Cresce anche la tipologia di aggressioni riferibile alla categoria "Espionage" (+9%). In termini assoluti nel primo semestre 2016 entrambe le categorie fanno registrare il numero di attacchi più elevato degli ultimi 6 semestri.

Tipologia e distribuzione degli attaccanti - 1H 2016



© Clusit - Rapporto 2016 sulla Sicurezza ICT in Italia - Aggiornamento Giugno 2016

Nel 2014 il Cybercrime si era confermato la prima causa di attacchi gravi a livello globale, attestandosi al 60% dei casi analizzati (era il 36% nel 2011). Nel 2015 tale percentuale era il 68%, che sale al 71% nel primo semestre 2016, mostrando un trend inequivocabile.
Va sottolineato che dal 2015 si è assistito alla diffusione ormai endemica di attività cybercriminali "spicciole" che in questo campione di incidenti gravi non sono rappresentate (per esempio le quotidiane campagne di estorsione realizzate tramite phishing e ransomware, che hanno colpito moltissime organizzazioni e cittadini italiani)[39], di conseguenza è lecito supporre che in generale questa crescita sia stata ancora maggiore



© Clusit - Rapporto 2016 sulla Sicurezza ICT in Italia - Aggiornamento Giugno 2016

.

Il Cybercrime passa dal 68% al 71% del totale, mentre l'Hacktivism diminuisce di 23 punti percentuali rispetto al suo picco del 2013, passando da oltre un terzo a meno di un quinto dei casi analizzati.
Per quanto riguarda le attività di Espionage, rispetto alla percentuale degli attacchi gravi registrati nel 2015 la quota di attacchi nel primo semestre 2016 è in crescita, mentre l'Information Warfare sembra essere in calo (probabilmente per mancanza di informazioni pubbliche in merito).

[39] http://www.repubblica.it/tecnologia/sicurezza/2016/02/05/news/malware_crescita_inarrestabile_17_a_dicembre-132773886/

Distribuzione delle vittime per tipologia

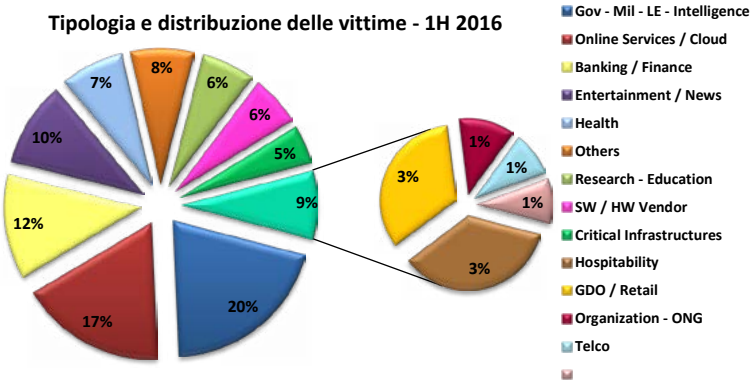
VITTIME PER TIPOLOGIA	2011	2012	2013	2014	2015	2H 2015	1H 2016	Variazioni 1H 2016 su 2H 2015	Trend 2016
Institutions: Gov - Mil - LEAs - Intelligence	153	374	402	213	223	109	105	-3,67%	→
Others	97	194	146	172	51	22	39	77,27%	↑
Entertainment / News	76	175	147	77	138	59	52	-11,86%	→
Online Services / Cloud	15	136	114	103	187	103	89	-13,59%	→
Research - Education	26	104	70	54	82	38	33	-13,16%	→
Banking / Finance	17	59	108	50	64	33	64	93,94%	↑
Software / Hardware Vendor	27	59	46	44	55	32	31	-3,13%	→
Telco	11	19	19	18	18	9	4	-55,56%	↓
Gov. Contractors / Consulting	18	15	2	13	8	3	2	-33,33%	↓
Security Industry	17	14	6	2	3	3	0	100,00%	↓
Religion	0	14	7	7	5	1	4	300,00%	↑
Health	10	11	11	32	36	16	39	143,75%	↑
Chemical / Medical	2	9	1	5	2	0	0	0,00%	→
Critical Infrastructures	-	-	37	13	33	13	24	84,62%	↑
Automotive	-	-	17	3	5	1	1	0,00%	→

continua >

VITTIME PER TIPOLOGIA	2011	2012	2013	2014	2015	2H 2015	1H 2016	Variazioni 1H 2016 su 2H 2015	Trend 2016
Org / ONG	-	-	19	47	46	21	5	-76,19%	↓
GDO / Retail	-	-	-	20	17	12	14	16,67%	↑
Hospitability / hotel industry					39	20	15	-25,00%	↓

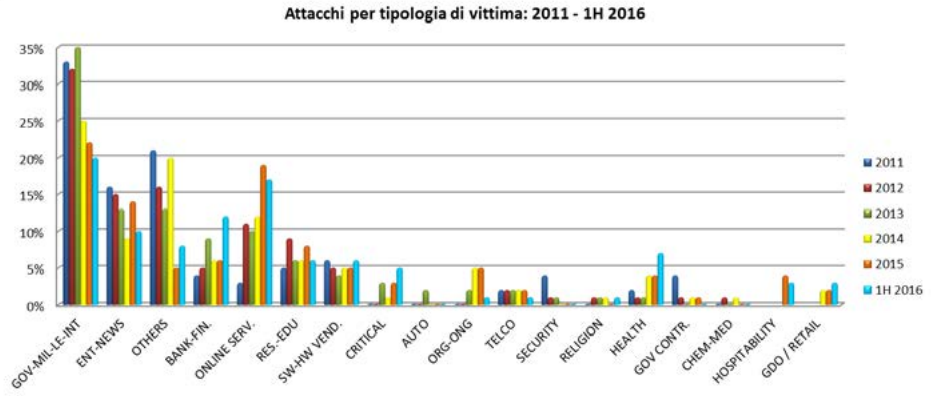
© Clusit - Rapporto 2016 sulla Sicurezza ICT in Italia – *Aggiornamento al 30 Giugno 2016*

Rispetto al secondo semestre 2015, nel primo semestre 2016 la crescita maggiore degli attacchi gravi si osserva verso le categorie "Banking / Finance" ed "Health", seguite da "Critical Infrastructures" e "GDO / Retail", oltre che verso l'ampia categoria "Others", che contiene tutte le organizzazioni non classificabili all'interno delle altre 17 categorie, a dimostrazione del fatto che ormai tutti sono diventati bersagli.
Rimangono stabili, sia pure con un leggero calo, gli attacchi verso i settori "Gov" (tipicamente con finalità di Espionage o di Hacktivism), "Entertainment / News", "Online Services / Cloud", e "Research / Education".
Nel 2015 abbiamo deciso di introdurre una nuova categoria, quella della "Ricettività" (Hospitability), dato che si sono presentati un certo numero di attacchi gravi verso organizzazione alberghiere, ristoranti, residence e collettività (tipicamente per colpirne gli utenti), che proseguono anche nel primo semestre 2016.
Complessivamente, su 18 categorie considerate, due rimangono invariate, 5 appaiono in calo ed altrettante rimangono sostanzialmente stabili, mentre 6 mostrano un aumento nel numero degli attacchi.



Al primo posto assoluto, in leggera diminuzione, ancora il settore governativo in senso esteso, con un quinto degli attacchi (20%). La categoria "Online Services / Cloud" si conferma al secondo posto (17%), per una maggiore concentrazione degli attacchi gravi verso i settori più esposti e più remunerativi. Al terzo posto, con una crescita importante rispetto al semestre precedente (+93%), la categoria "Banking / Finance", che nel primo semestre 2016 fa registrare il maggior numero di attacchi degli ultimi 11 semestri.

Rispetto al secondo semestre 2015 crescono anche la categoria "Health", (+143%) sempre più presa di mira da soggetti cyber criminali con finalità di furto di informazioni ed estorsione tramite Ransomware, e la categoria "Critical Infrastructures" (+84%). Cresce anche la categoria "Others" (+77%), che pur rappresentando solo l'8% del totale vede le aggressioni note aumentare sensibilmente.

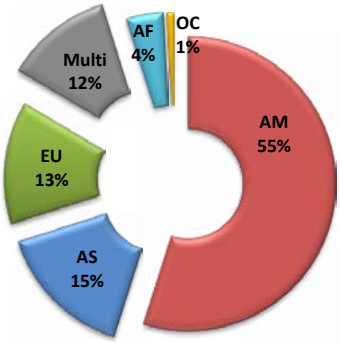


Rapporto 2016 sulla Sicurezza ICT in Italia - Aggiornamento Giugno 2016

Distribuzione delle vittime per area geografica

La classificazione delle vittime per nazione di appartenenza viene qui sintetizzata su base continentale.
Percentualmente aumentano le vittime di area americana (dal 47 al 55%) mentre mostrano leggere variazioni gli attacchi verso realtà basate in Europa ed in Asia.

Appartenenza geografica delle vittime per continente - 1H 2016



Rapporto 2016 sulla Sicurezza ICT in Italia - Aggiornamento Giugno 2016

Da notare che per la prima volta dal 2011 gli attacchi contro realtà asiatiche superano quelli contro realtà europee.
Cresce anche dal 9 al 12% la categoria "Multinational", ad indicare la tendenza a colpire bersagli sempre più importanti, di natura transnazionale.

Distribuzione delle tecniche di attacco per tipologia

TECNICHE DI ATTACCO PER TIPOLOGIA	2011	2012	2013	2014	2015	2H 2015	1H 2016	Variazioni 1H 2016 su 2H 2015	Trend 2016
SQL Injection	197	435	217	110	184	81	9	-88,89%	↓
Unknown	73	294	239	199	232	121	134	10,74	↑
DDoS	27	165	191	81	101	60	59	-1,67%	→
Known Vuln/ Misconfig	107	142	256	195	184	81	100	23,46	↑
Malware	34	61	57	127	106	52	118	126,92	↑
Account Cracking	10	41	115	86	91	35	15	-57,14	↓
Phishing/Social Engineering	10	21	3	4	6	3	48	1500,00%	↑
Multiple Techniques/APT	6	13	71	60	104	58	33	-43,10	↓
0-day	5	8	3	8	3	3	3		
Phone Hacking	0	3	0	3	1	1	2	100,00%	↑

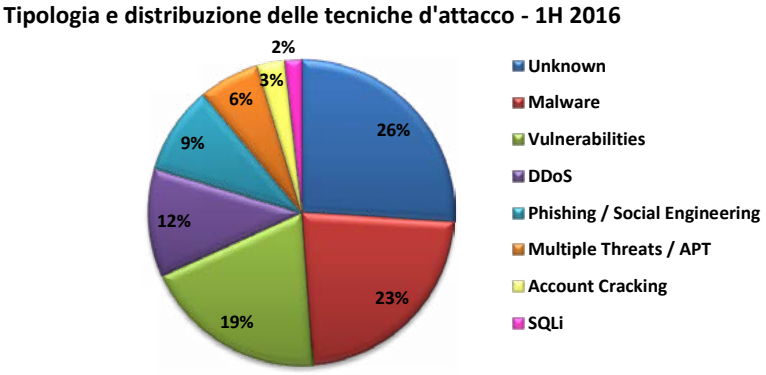
© Clusit - Rapporto 2016 sulla Sicurezza ICT in Italia – *Aggiornamento al 30 Giugno 2016*

Rispetto al secondo semestre 2015, tra le *root cause* degli attacchi gravi analizzati nel primo semestre 2016 ritornano ad aumentare il Malware comune (+129%) e le Vulnerabilità note (+23%), che erano risultate in forte diminuzione negli ultimi 2 anni, a dimostrazione del fatto che purtroppo oggi il costo sostenuto dagli attaccanti per realizzare i propri crimini tende a diminuire, dal momento che sono in grado di causare gravi danni anche utilizzando tecniche banali.

Il Malware (in particolare i c.d. Ransomware) è sempre più diffuso, e non solo per compiere attacchi "spiccioli" (tipicamente realizzati da cyber criminali poco sofisticati, dediti a generare i propri "margini" su grandissimi numeri). Anche l'Italia, come ogni economia avanzata, è pesantemente bersagliata da questo genere di minaccia[40].

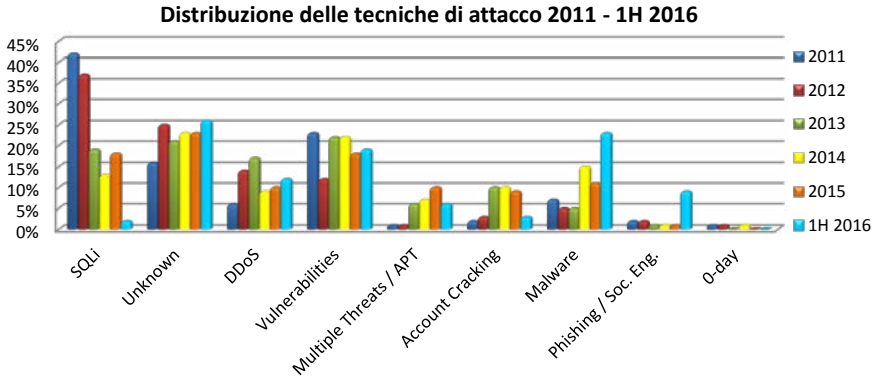
[40] http://www.repubblica.it/tecnologia/sicurezza/2016/02/05/news/malware_crescita_inarrestabile_17_a_dicembre-132773886/

Diminuiscono sensibilmente le SQLinjection, che in un semestre passano dal 18 al 2% del totale. Crescono invece fortemente gli attacchi realizzati a partire da attività di Phishing e Social Engineering (+1.500%), che passano dal 1% al 9% del totale. Sostanzialmente stabili gli attacchi DDoS.



Rapporto 2016 sulla Sicurezza ICT in Italia - Aggiornamento Giugno 2016

Tornano a crescere in modo apprezzabile le tecniche di attacco sconosciute, che purtroppo in termini assoluti rappresentano la prima categoria, con oltre un quarto del totale.



Rapporto 2016 sulla Sicurezza ICT in Italia - Aggiornamento Giugno 2016

Considerato che stiamo analizzando gli attacchi più gravi del periodo, compiuti contro primarie organizzazioni pubbliche e private, spesso di livello mondiale, il fatto che la somma delle tecniche di attacco più banali (SQLi, DDoS, Vulnerabilità note, malware "semplice") rappresenti ancora il 66% del totale (era il 57% nel 2015), dimostra senza dubbio che i difensori sono ancora in alto mare, e implica che gli attaccanti hanno sostanzialmente campo libero contro queste organizzazioni – forse la considerazione più preoccupante tra tutte quelle svolte fin qui.

Analisi Fastweb della situazione italiana in materia di cyber-crime e incidenti informatici

Introduzione e visione d'insieme

Negli ultimi 10 anni abbiamo continuato a connettere qualsiasi dispositivo ad internet ed abbiamo incominciato a basare tutti i nostri affari su computer e reti interconnesse, quasi sempre senza pensare a renderli sicuri a causa di una percezione falsata del rischio data da due principali pensieri "perché dovrebbero attaccare proprio me?" e "tanto non è mai successo".

Alla prima domanda è facile dare una risposta, i cyber criminali infatti attaccano tutti, indiscriminatamente, con script ed attività completamente automatizzate. Non si è attaccati solo se si hanno informazioni "preziose". Ogni informazione per loro è preziosa, ogni risorsa informatica può essere sfruttata per generare bitcoin, effettuare attacchi DDoS, inviare spam o sottrarre credenziali ed informazioni che solo in un secondo momento saranno vagliate oppure anche solo rivendute.

Alla seconda obiezione è ancora più semplice dare una risposta, in quanto non solo noi tutti veniamo continuamente attaccati ma anche tutte le nostre aziende vengono regolarmente compromesse. Chi sarebbe pronto a giurare di non aver mai avuto un computer infetto da un malware nella rete della propria azienda? Quello che un tempo si chiamava virus e faceva apparire popup con simpatiche donnine, oggi si chiama malware e mentre fa qualsiasi cosa pur di nascondersi, con ancor più ferocia, sottrae qualsiasi dato in nostro possesso.

È così che la scena italiana osservata da Fastweb durante il 2015 riflette ciò che si è visto anche nel resto del mondo: la crescita esponenziale dei malware e soprattutto quelli di tipo *ransomware, ad esempio Cryptolocker e simili. Questi eventi hanno scatenato grossi dibattiti sull'importanza della sicurezza informatica e di quanto sia necessario ormai, che ogni azienda investa risorse specifiche in questo campo. Oltre a questi sono sempre presenti le minacce rappresentate dagli attacchi di tipo DDoS, mirati all'interruzione dei servizi online: tutte le Aziende che offrono tali servizi possono essere possibili vittime di questi attacchi.*

Il Security Operations Center di Fastweb, attraverso l'evoluzione delle sue piattaforme, ha continuato a monitorare le principali minacce dirette verso i propri clienti, con l'intento di storicizzare e quindi studiare eventuali trend significativi.

Dati analizzati

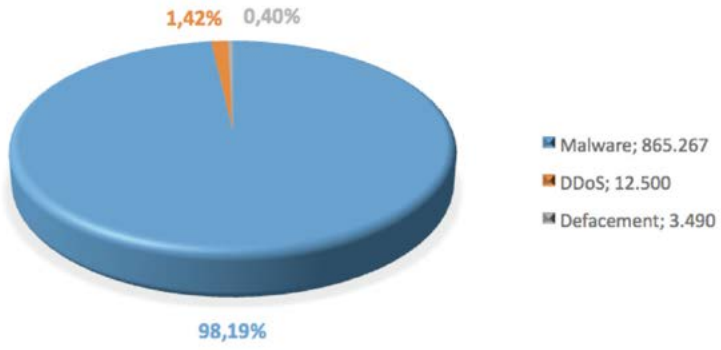
Quest'anno abbiamo analizzato oltre 8 milioni di eventi di sicurezza: aumentando la base dati di circa il 60% rispetto a quella dello scorso anno. Il dominio di analisi è costituito dai dati raccolti ed analizzati dal Security Operations Center, relativi agli indirizzi IP appartenenti all'AS Fastweb: oltre 6 milioni di indirizzi pubblici, dietro ognuno dei quali potrebbero celarsi decine o centinaia di computer / server.

I dati da noi raccolti sono stati arricchiti, analizzati e correlati con l'aggiunta di quelli forniti da organizzazioni come ad esempio la Shadowserver Foundation, che rappresenta una fonte

indicativa e molto dettagliata sull'evoluzione delle botnet e dei relativi malware.
I dati sugli attacchi di Distributed Denial of Service, sono stati ricavati da tutte le anomalie DDoS rilevate dalle tecnologie di Fastweb per il contrasto di questo tipo di attacchi.
È importante inoltre sottolineare che tutti i dati, prima di essere analizzati, sono stati automaticamente aggregati ed anonimizzati per proteggere la privacy e la sicurezza sia dei Clienti che di Fastweb stessa.

Le principali minacce

È evidente ormai che la principale minaccia è rappresentata dalla diffusione sempre crescente di malware: software malevolo che si installa volontariamente, perché l'utente clicca su qualche link malevolo, o involontariamente, perché sfrutta una qualche vulnerabilità dell'applicativo o del sistema operativo. Una volta avviato persegue le azioni per le quali è stato programmato: furto di informazioni sensibili, monitoraggio delle azioni dell'utente, codifica dei dati con l'intento di estorcere denaro e/o partecipazione alla formazione di botnet che, addirittura, è possibile usare, pagando, per effettuare campagne di spam, attacchi di tipo DDoS o altro genere di operazione malevola.
Il mercato dei malware si è evoluto in modo esponenziale adeguandosi a quelle che sono le grandi realtà dell'e-commerce odierno: è diventato molto semplice, nonché relativamente poco costoso, venire a contatto con i fornitori di questo tipo di software. È possibile, infatti, usufruire dei servizi di una botnet più o meno estesa (si parla pur sempre di decine di migliaia di computer zombie per le più piccole) e rimanere completamente anonimi, effettuando pagamenti con moneta elettronica (anche di tipo bitcoin e simili). Oltre al fatto che le compagnie che offrono questo genere di servizi, nella maggior parte dei casi, sono residenti in paesi in cui la legislazione non regola questo tipo di attività e diventa molto difficile, realmente impossibile, perseguirli.
Purtroppo gli strumenti di rilevazione (antivirus, antimalware) sono sempre più in difficoltà in quanto basati, per lo più, su rilevazione di signature. Quindi cambiando metodo di offuscamento si riesce a rendere un malware, perfettamente riconosciuto fino a quel momento, completamente e nuovamente invisibile.
Queste le motivazioni per cui la quasi totalità delle minacce provenga essenzialmente da malware. Gli attacchi di tipo DDoS, benché per loro stessa natura molto pericolosi e difficilmente evitabili, vengono mitigati efficacemente sottoscrivendo servizi di mitigation, che riescono a prevenire la totalità dei possibili disservizi. È importante sottolineare che quando ci si accorge di essere vittima di un attacco DDoS è essenzialmente troppo tardi: l'attacco potrebbe essere attivo da giorni, o addirittura mesi ed avrà già generato tutti i disservizi per i quali è stato concepito. Per questo è importante che il servizio di monitoraggio sia sempre attivo sugli apparati che forniscono connettività ai clienti.

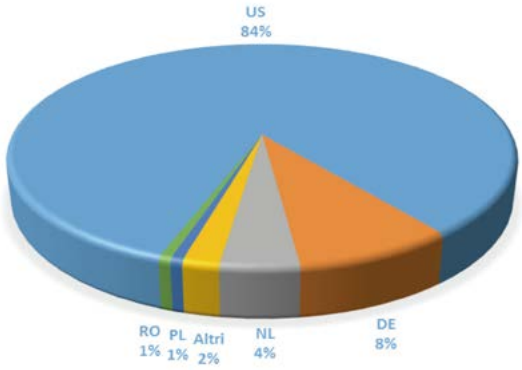


Dati FASTWEB relativi all'anno 2015

Figura 1 - Tipologie di attacchi rilevate

Distribuzione geografica dei centri di comando e controllo dei malware

I centri di comando e controllo (C&C) sono quegli host utilizzati per l'invio dei comandi alle macchine infette dal malware (bot) utilizzato per la costruzione della botnet. Anche quest'anno i dati continuano a mostrare che la quasi totalità dei centri di C&C relativi alle macchine infette appartenenti all'AS di Fastweb sono situate negli Stati Uniti.

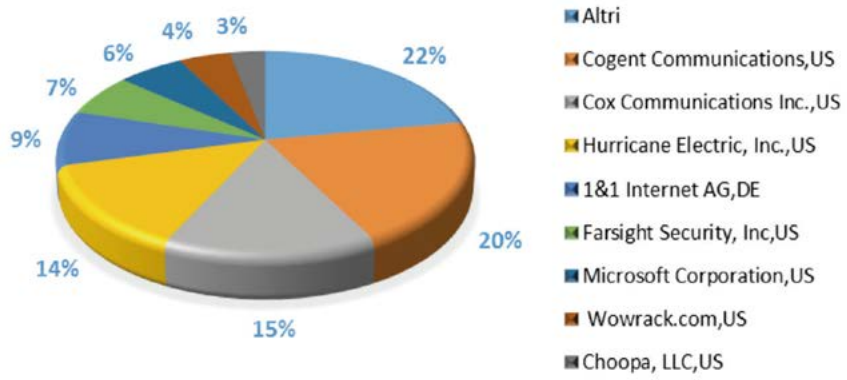


Dati FASTWEB relativi all'anno 2015

Figura 2 - Dislocazione dei Centri di Comando e Controllo

Gli AS che ospitano tali centri di comando e controllo cambiano rispetto allo scorso anno: sempre presente l'AS Cox Communications Inc. ma cambia nettamente la sua quota: dal

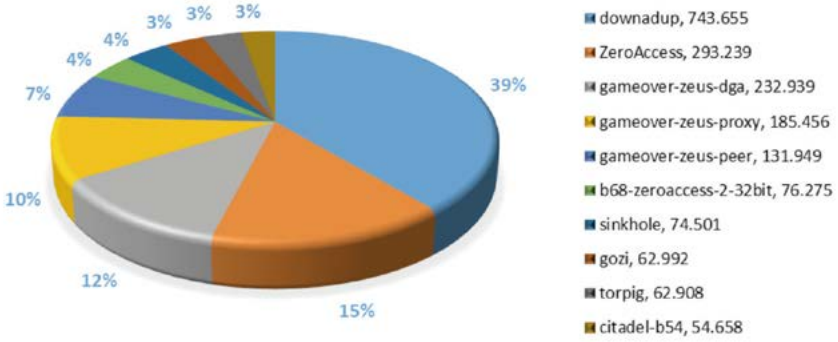
98% del 2014 passa quest'anno al 20%. È interessante notare che la quasi totalità degli AS americani si spartiscono, quasi in egual misura, i centri di comando e controllo. Si nota anche un nuovo AS, quello di Microsoft Corporation: non che questo ospiti veri centri di comando e controllo, ma è chiaramente l'effetto delle operazioni di botnet shutdown effettuate quest'anno dall'Azienda anche insieme alle forze dell'ordine come FBI e Interpol.



Dati FASTWEB relativi all'anno 2015

Figura 3 - AS ospitanti i Centri di Comando e Controllo

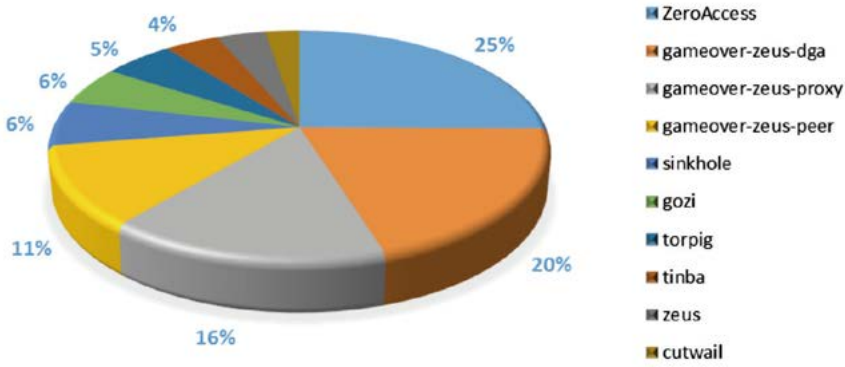
Tipologie di malware



Dati FASTWEB relativi all'anno 2015

Figura 4 - Tipologie di malware

I malware infestanti le macchine appartenenti all'AS di Fastweb si confermano essere sempre gli stessi. Le cause di questa situazione potrebbero essere sia dipendenti dalla scarsa manutenzione delle macchine, che restano infette per lunghi periodi di tempo, e quindi ciò rivela il mancato aggiornamento dei software di protezione o addirittura la sua totale assenza, sia la scarsa attenzione degli utenti che restano vittime delle campagne infezione generate dalle stesse botnet attraverso l'invio massivo di spam infetto.
A prova di quanto detto si evince che circa il 40% dei malware che abbiamo rilevato quest'anno trattasi di una variante del vecchio Conficker, benché ormai risalente al 2008 continua ad infestare, nell'arco di un anno, circa 750.000 host. Un gradino più in basso troviamo ZeroAccess ed il malware Gameover Zeus, le cui varianti hanno generato le più grandi infestazioni degli ultimi anni.
Se il 2015 vede il gradino più alto del podio dei malware più presenti sulla rete Fastweb dominio incontrastato di Conficker, sono due le botnet che invece si spartiscono la maggioranza degli host: la ZeroAccess e la GameOver Zeus, nelle sue varianti dga, proxy e peer.

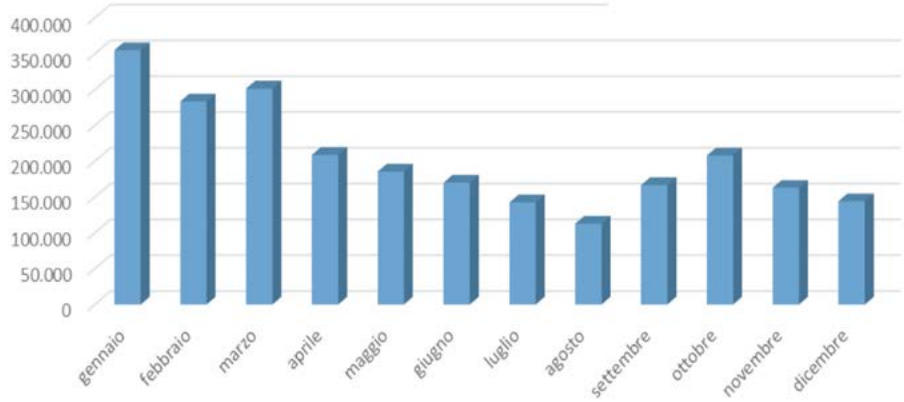


Dati FASTWEB relativi all'anno 2015

Figura 5 - Le botnet più diffuse

Andamento temporale

La diffusione temporale dei malware mostra un andamento piuttosto regolare durante il corso dell'intero anno. Come al solito il picco minimo ad agosto rispecchia il fermo delle attività lavorative ed il ridotto numero di host attivi sulla rete.

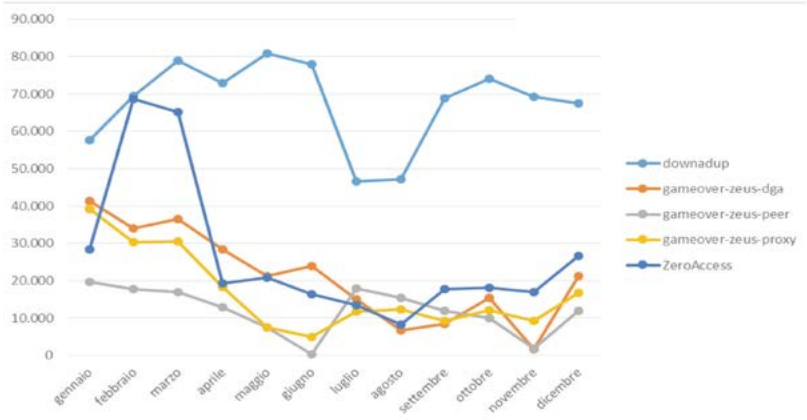


Dati FASTWEB relativi all'anno 2015

Figura 6 - Distribuzione mensile dei malware

Principali famiglie di malware

Di seguito l'andamento mese per mese delle principali famiglie di malware rilevate. È evidente la stragrande maggioranza del Conficker rispetto agli altri: durante il mese di agosto, suo picco di minimo, il malware si attesta su quasi 50.000 host.

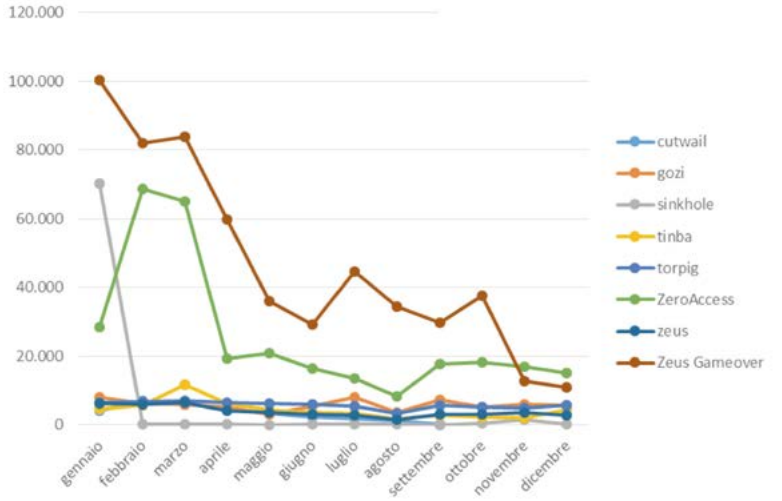


Dati FASTWEB relativi all'anno 2015

Figura 7 - Andamento dei principali malware

Principali famiglie di botnet

È molto interessante notare quanto invece la presenza di botnet all'interno dell'AS di Fastweb abbia avuto un trend continuamente decrescente. Ad esempio la Zeus Gameover a gennaio si attestava a ben 100.000 host per arrivare a neanche 20.000 host a dicembre.
È evidente che tali host abbiano beneficiato delle operazioni di shutdown operate durante l'anno.



Dati FASTWEB relativi all'anno 2015

Figura 8 - Andamento temporale delle botnet

Attacchi Distributed Denial of Service

Un attacco DoS (Denial of Service) è un attacco volto ad arrestare un computer, una rete o anche solo un particolare servizio offerto. Alcuni mirano solo ad un servizio, ad esempio Web, SMTP, FTP, etc., altri invece mirano a mettere fuori uso completamente il server o, addirittura, un'intera rete.
Un attacco DDoS (Distributed Denial of Service) è una variante del DoS ed impiega decine di migliaia di computer infetti, che formano una botnet, per portare a termine l'attacco. Il grande numero di macchine infette, involontariamente controllate dal centro di C&C, generano richieste verso l'obiettivo ed in poco tempo lo rendono indisponibile saturando tutte le sue risorse.
Gli attacchi di tipo DDoS sono molto più insidiosi da bloccare perché:

- La potenza dell'attacco (volume dei dati trasmessi, banda occupata, etc.) è maggiore, di vari ordini di grandezza, rispetto a quella possibile attraverso un DoS.
- È praticamente impossibile bloccare l'attaccante vista che sono decine di migliaia di computer infetti che perpetrano l'attacco se non sottoscrivendo un servizio di mitigation.
- È praticamente impossibile riconoscere il traffico autorizzato da quello non autorizzato, visto che i computer partecipanti alla botnet sono dislocati, praticamente in tutto il globo.

Quanti sono i DDoS?

Durante il 2015 abbiamo rilevato più di 12.500 anomalie riconducibili ad attacchi DDoS dirette verso i Clienti Fastweb, con un decremento rispetto all'anno precedente. Anche quest'anno l'andamento del primo semestre è leggermente più basso rispetto al secondo semestre.

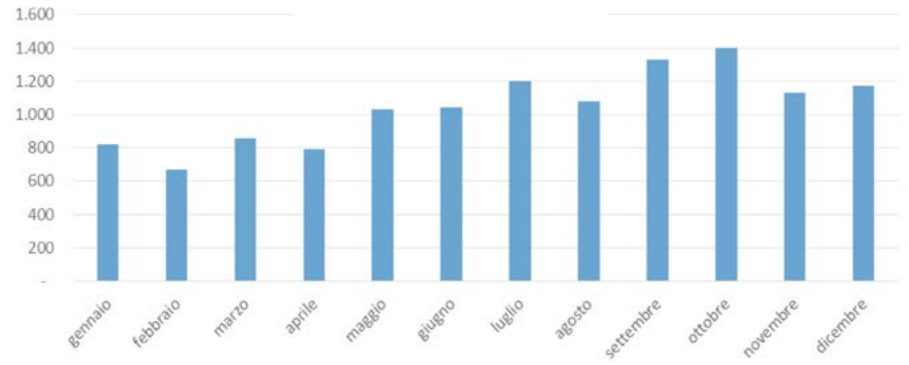
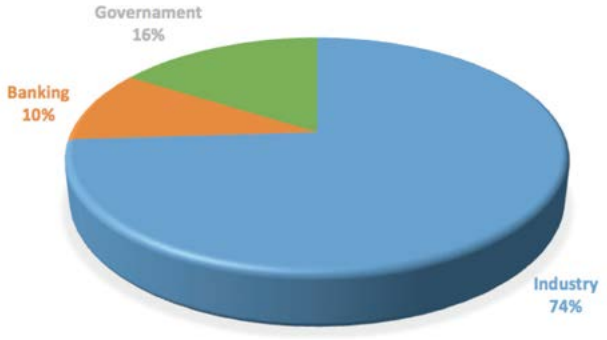


Figura 9 - Distribuzione mensile attacchi DDoS

Chi è vittima di un attacco ddos?

La rilevazione effettuata durante l'anno indica che i tre principali obiettivi degli attacchi DDoS sono le aziende private seguite dalle istituzioni governative (Ministeri, Pubbliche Amministrazioni locali e centrali, etc) ed il settore bancario che rappresenta il 10%.



Dati FASTWEB relativi all'anno 2015

Figura 10 - Target di possibili attacchi DDoS

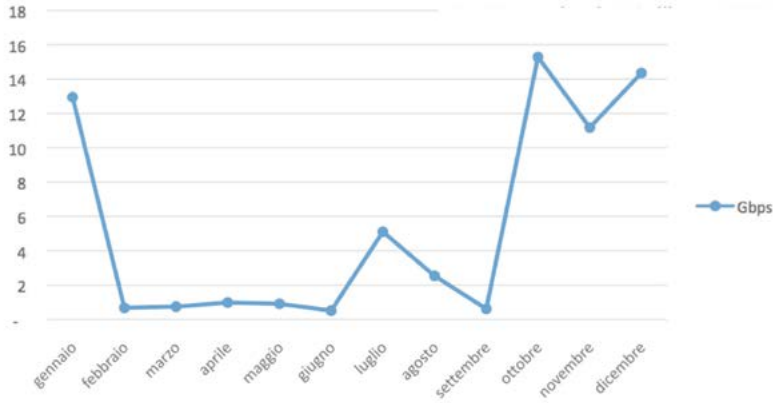
Il volume degli attacchi DDoS

Il volume degli attacchi, in termini di banda totale impiegata, seppur più alto, in media, rispetto a quello dello scorso anno, subisce dei sensibili spike a causa del peso dei mesi di marzo e luglio. Il volume delle anomalie registrate in questi due mesi rappresentano quasi il 50% di tutte le altre anomalie, riconducibili ad attacchi DDoS, dell'intero anno.

Dati FASTWEB relativi all'anno 2015

Figura 11 – Banda totale mensile impegnata dalle anomalie DDoS

La piattaforma di mitigation, che difende i clienti che hanno sottoscritto il servizio, mitiga mese per mese attacchi che occupano una banda che va da svariate centinaia di Mbps a picchi di decine di Gbps. La piattaforma è in grado di adattare autonomamente le sue soglie sulla base dei comportamenti e delle condizioni dei clienti. Le nostre analisi hanno rilevato che un attacco DDoS di potenza media si attesta a circa 6 Gbps.



Dati FASTWEB relativi all'anno 2015

Figura 12 – Picchi di traffico relativi ad attacchi DDoS

Dati FASTWEB relativi all'anno 2015

Figura 13 – Banda degli attacchi DDoS mitigati dalla piattaforma

Tecniche di attacco utilizzate

Abbiamo detto che l'attacco DoS più pericoloso è quello di tipo Distributed e cioè DDoS. Ci sono varie tecniche per portare a compimento un attacco di tipo denial of service, vediamone alcune:

- **ICMP flood**
  - **Smurf attack:** si invia un pacchetto con indirizzo ip sorgente forgiato verso apparati non correttamente configurati che ritrasmettono il pacchetto in modalità broadcast su tutta la rete interna andando velocemente a saturare tutta la banda disponibile.
  - **Ping flood:** banalmente si continua a pingare senza fine la vittima. Se migliaia e migliaia di computer, che fanno parte di una botnet, effettuano questa azione continuamente, la vittima esaurirà presto le sue risorse.
  - **Ping of Death:** si invia un pacchetto di ping non standard, forgiato in modo tale da mandare in crash lo stack di networking della macchina vittima.
- **SYN Flood**
  - L'attaccante manda un grande numero di pacchetti di tipo SYN alla vittima con indirizzo sorgente spoofato: il risultato è che la macchina vittima cercherà di rispondere con pacchetti di tipo SYN-ACK che non avranno mai risposta in quanto l'indirizzo di destinazione sarà inesistente. In un breve arco di tempo tutte le risorse della macchina vittima saranno esaurite.
- **HTTP POST DoS Attack**
  - Scoperto nel 2009 questo attacco sfrutta un difetto di progettazione di molti server web, ad esempio Apache. L'attaccante inizia una connessione http del tutto lecita verso un server web andando ad abusare del campo 'Content-Lenght': visto che la maggior parte dei server web accetta dimensioni del payload del messaggio anche di 2Gb, l'attaccante comincia ad inviare il corpo del messaggio ad un ridottissima velocità (anche 1byte ogni 110 secondi). Ciò comporta che il server web resta in ascolto per molto tempo, lasciando aperti i canali http (del tutto leciti) andando quindi a saturare tutte le sue risorse visto che le connessioni restano aperte.

Chiaramente questo tipo di tecniche possono essere utilizzate sia da attacchi semplici sia da quelli di tipo distribuito.
Nel corso degli anni gli attacchi DDoS si sono evoluti, aumentando in modo esponenziale la loro potenza, sfruttando bug di design di alcuni protocolli. Infatti sfruttando alcune vulnerabilità insite ai protocolli stessi, è possibile amplificare ulteriormente, di vari ordini di grandezza, il traffico diretto verso la macchina vittima.
Di seguito alcuni esempi dei fattori di amplificazione (rif. Wikipedia).

UDP-based Amplification Attacks

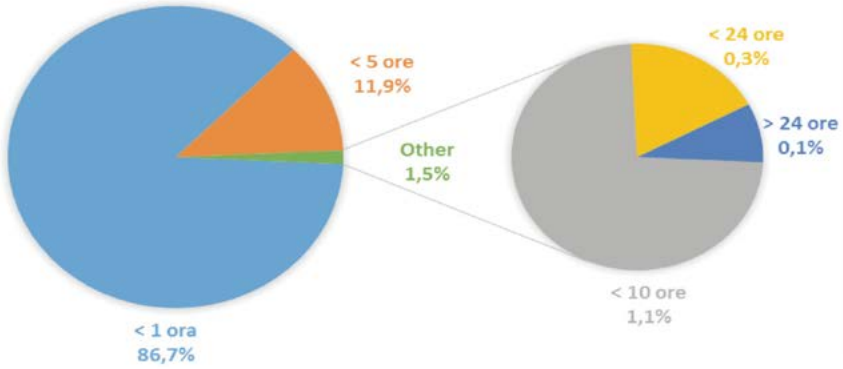
Protocol	Bandwidth Amplification Factor
NTP	556.9
CharGen	358.8
DNS	up to 179
QOTD	140.3
Quake Network Protocol	63.9
BitTorrent	4.0 - 54.3
SSDP	30.8
Kad	16.3
SNMPv2	6.3
Steam Protocol	5.5
NetBIOS	3.8

Dati FASTWEB relativi all'anno 2015

Figura 14 - Fattori di amplificazione degli attacchi DDoS

Quanto dura un attacco ddos?

L'evoluzione delle tecniche di attacco DDoS e la conseguente evoluzione delle tecniche di mitigation adottate dal SOC, hanno fatto sì che la durata della quasi totalità delle anomalie riconducibili ad attacchi DDoS duri meno di un'ora. Si rileva solo una piccolissima percentuale – circa 1,5% - di durata oltre le 5 ore. Un netto cambiamento rispetto allo scorso anno.



Dati FASTWEB relativi all'anno 2015

Figura 15 - Durata dei possibili attacchi DDoS

Attacchi al VOIP

Le principali minacce

VOIP è l'acronimo di 'Voice Over Internet Protocol', ed è una modalità di trasmissione della voce e traffico multimediale su reti di computer. La voce viene convertita, pacchettizzata e trasmessa come normale scambio di traffico dati.
I tre scenari classici di utilizzo del VOIP sono:

1 Computer – Computer
2 Telefono IP – Telefono IP
3 Telefono IP / PC – PSTN (rete telefonica classica)

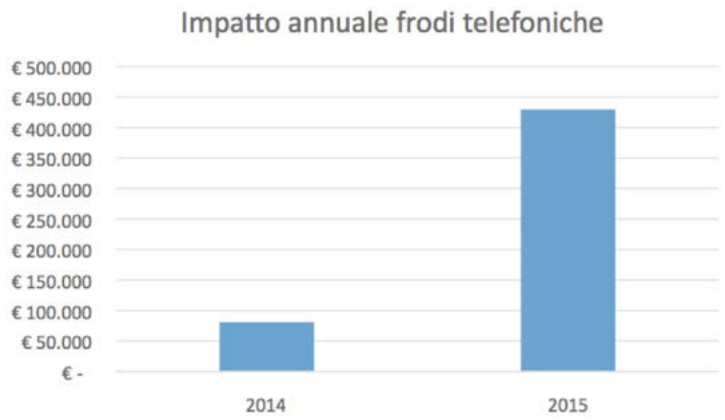
Il vantaggio maggiore delle comunicazioni VOIP è la sensibile riduzione dei costi che è possibile ottenere visto che sfrutta l'infrastruttura esistente delle reti di computer, ad esempio internet. Questo ha tuttavia portato con se nuove vulnerabilità ed ampliato la superficie di attacco delle Aziende che utilizzano questo tipo di tecnologia.
Essendo l'infrastruttura VOIP la stessa su cui girano i classici servizi come web, ftp, ssh, etc. soffre esattamente degli stessi rischi analizzati finora. Tuttavia, con l'introduzione di nuovi protocolli, sono state scoperte nuove vulnerabilità e quindi nuovi attacchi perpetrati contro aziende e organizzazioni.

La VOIPSA, Voice Over IP Security Alliance, ha categorizzato sei principali rischi associati al VOIP:

1. Social Threats: versione VOIP del furto d'identità, impersonare un utente e perpetrare azioni malevole con lo scopo di arrecare danni come, ad esempio, furto di informazioni aziendali riservate.
2. Eavesdropping: attacco del tutto simile al classico man-in-the-middle. L'attaccante si inserisce in una comunicazione tra due utenti con lo scopo di spiare, registrare e rubare informazioni.
3. Interception and Modification: si intercettano comunicazioni lecite tra utenti e le si modificano con lo scopo di arrecare disservizi come l'abbassamento della qualità delle conversazioni e/o l'interruzione completa e continua del servizio.
4. Service Abuse: si utilizza l'infrastruttura del rete VOIP della vittima per generare traffico verso numerazioni particolari a tariffazione speciale.
5. Intentional Interruption of Service: attacchi di tipo DoS e DDoS.
6. Others: attacchi di altro genere.

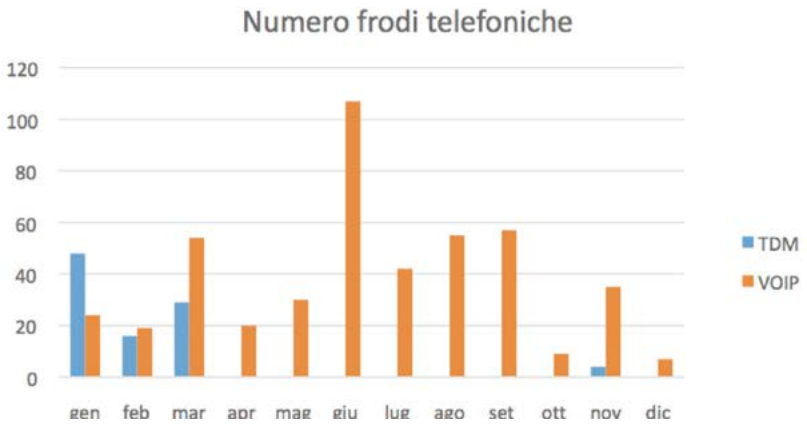
I dati Fastweb

Nell'ambito dello studio delle attività illecite condotte contro i nostri clienti quest'anno abbiamo analizzato gli attacchi verso l'infrastruttura VOIP dei nostri clienti innanzitutto confrontandolo con quanto accaduto nel 2014 e successivamente studiato il suo andamento mensile, comparandolo con quanto succede alla tecnologia tradizionale TDM.



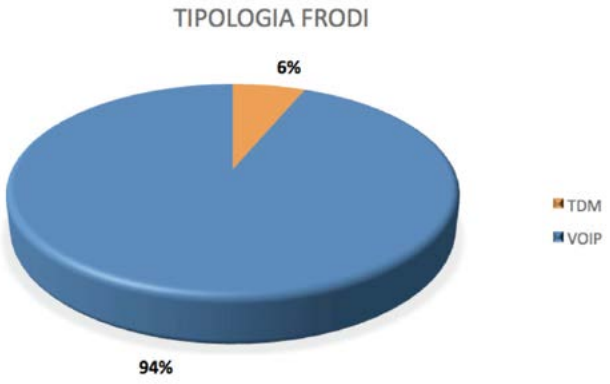
Dati FASTWEB relativi all'anno 2015

Figura 16 - Valore delle frodi



Dati FASTWEB relativi all'anno 2015

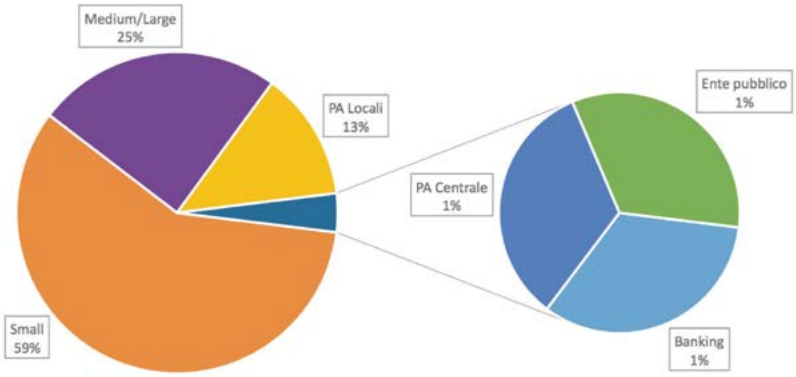
Figura 17 - Andamento delle frodi durante l'anno



Dati FASTWEB relativi all'anno 2015

Figura 18 - Truffe VOIP vs TDM

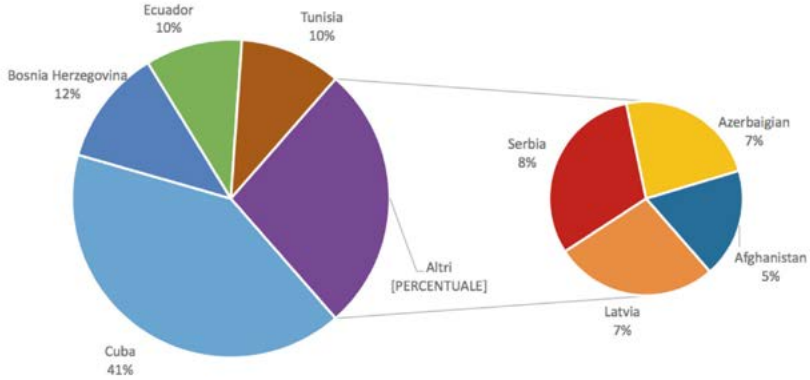
I dati osservati mostrano che più della metà degli attacchi all'infrastruttura VOIP è stata diretta verso clienti di tipo SMALL, probabilmente a causa del fatto che sempre più frequentemente, le piccole Aziende si rivolgono al VOIP per usufruire dei vantaggi legati ai suoi bassi costi. Questo potrebbe causare il fatto che vengano messi in produzione dispositivi non correttamente configurati, non gestiti né monitorati e dunque facili obiettivi di attività illecite. Come anche si è evidenziato che la stragrande maggioranza degli attacchi sono stati di tipo 'Service Abuse', attacchi volti a generare traffico illecito verso direttrici a tariffazione speciale.



Dati FASTWEB relativi all'anno 2015

Figura 19 - Vittime di truffe VOIP

Di seguito i principali paesi ospitanti le direttrici che hanno generato frodi del valore di almeno 1.000 €.



Dati FASTWEB relativi all'anno 2015

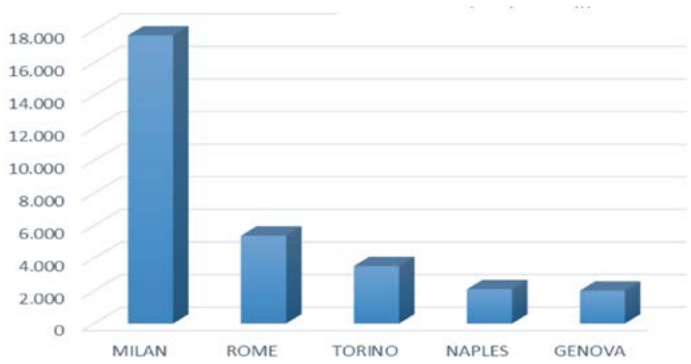
Figura 20 - Paesi ospitanti le direttrici dei principali attacchi

Ulteriori vulnerabilità

DNS Open Resolver

Purtroppo la scarsa attenzione verso le security best practice avuta in questi anni ha lasciato una pesante eredità: decine di migliaia di dispositivi esposti su internet con configurazioni troppo aperte o non configurati affatto.

Anche quest'anno la quantità di DNS Open Resolver è rimasta pressoché invariata, decine di migliaia di host, rispetto allo scorso anno, come anche la sua dislocazione sul territorio nazionale.



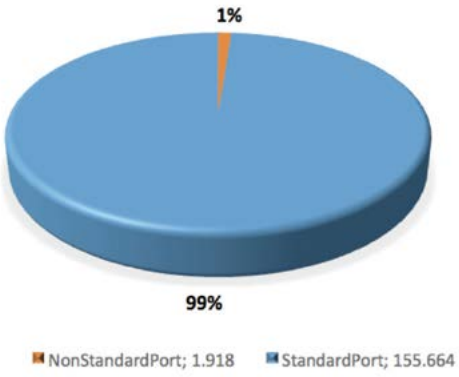
Dati FASTWEB relativi all'anno 2015

Figura 21 Dislocazione sul territorio nazionale degli open resolver

Servizi esposti pubblicamente

Quest'anno sono stati analizzati anche ulteriori potenziali rischi, come, ad esempio, il numero di server di backend esposti pubblicamente su internet. Questa situazione, benché non sia effetto di malware o di azioni malevole, rappresenta un grave rischio di sicurezza perché un server di questo tipo non dovrebbe mai essere esposto su internet, in quanto aumenta la potenziale superficie di attacco. In particolare le cause di queste potenziali vulnerabilità sono semplicemente errori di configurazioni dei dispositivi perimetrali e/o degli applicativi server.

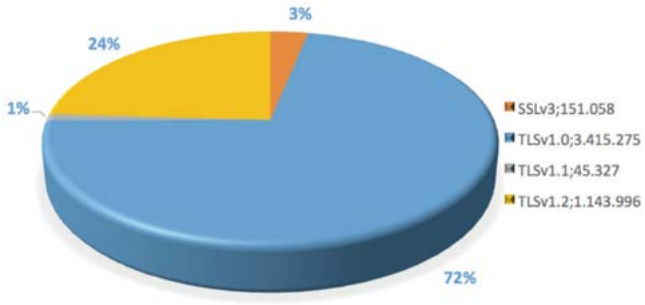
A peggiorare la situazione abbiamo rilevato che la quasi totalità dei servizi, in questo caso specifico server di database di tipo MSSQL, sono esposti con le porte di default. E chiaramente diventano vittime di attacchi di tipo brute-force.



Dati FASTWEB relativi all'anno 2015

Figura 22 - Server Microsoft SQL esposti su internet

Durante lo scorso anno, grande clamore hanno suscitato due attacchi al protocollo SSL: Heartbleed e POODLE. Questi due attacchi permettono di violare la sicurezza delle connessioni HTTPS rendendo di fatto vulnerabili tutte le connessioni sicure ad attacchi di tipo man in the middle. La gravità di questo tipo di attacco, ha di fatto, portato ad abbandonare la versione 3 del protocollo SSL ed in seguito – durante l'ultimo trimestre 2014 ed il primo trimestre 2015 – anche la versione 1.0 del protocollo TLS. Tuttavia la situazione sembra ancora qualche passo indietro rispetto alle best practice consigliate:



Dati FASTWEB relativi all'anno 2015

Figura 23 - Versioni dei protocolli SSL utilizzati

Se è pur vero che la versione 3 di SSL sembra ormai in dismissione, più del 70% degli host che espongono servizi sicuri usano ancora la versione 1.0 del protocollo TLS, vulnerabile a versioni evolute degli attacchi. La speranza è che questi siano migrati il prima possibile alla versione 1.2.

Considerazioni Finali

Alla luce di tutte queste analisi, possiamo affermare che il 2015 è stato un anno sicuramente particolare: le organizzazioni criminali hanno preso coscienza delle potenzialità dei malware andando a creare strutture commerciali efficientemente organizzate, capaci di generare sensibili profitti dalla vendita dei servizi che le botnet sono in grado di offrire. Tuttavia, questo tipo di evoluzione, del tutto simile a quella che può essere l'evoluzione di una normale azienda da start-up a multinazionale, ha presto dimostrato che manutenere infrastrutture delle dimensioni delle attuali botnet, richiede un deciso investimento sia in termini di tempo che di denaro.

Tale scenario ha comportato la nascita di un nuovo tipo di organizzazione, sicuramente di dimensione molto più piccole, in grado tuttavia di arrecare danni del tutto simili a quelli di una botnet di decine di migliaia di computer. Abbiamo cominciato ad osservare che anche piccoli agglomerati di server, ad esempio di qualche decina, ma con a disposizione considerevole larghezza di banda, possono generare attacchi DDoS tremendamente distruttivi, costando una piccolissima frazione del costo delle botnet tradizionali.

Per quanto riguarda le minacce portate invece agli utenti, siamo convinti che i malware di tipo ransomware continueranno a rappresentare una minaccia ancora molto forte, proprio perché mirata all'utilizzatore finale e non più all'infrastruttura informatica. In questo tipo di minaccia infatti, l'aspetto tecnico lascia il posto all'aspetto psicologico: si punta sfruttare i punti deboli umani, i cattivi comportamenti e/o la scarsa attenzione che, ancora oggi, la maggioranza degli utenti ripone nell'utilizzo degli strumenti informatici.

L'anno appena trascorso può essere considerato come l'anno delle estorsioni online e questo trend è, purtroppo, ancora in crescita. Il fatto che l'intero patrimonio Aziendale possa essere messo a rischio dal cattivo comportamento di un singolo dipendente, che magari apre un allegato di posta elettronica che sembra del tutto innocuo, ha sensibilizzato in modo molto deciso il management di molte Aziende, anche medio-piccole. Infatti sempre più spesso vengono organizzati dei test aziendali di sicurezza che puntano ad evidenziare quali siano i comportamenti da evitare e quali invece da osservare.

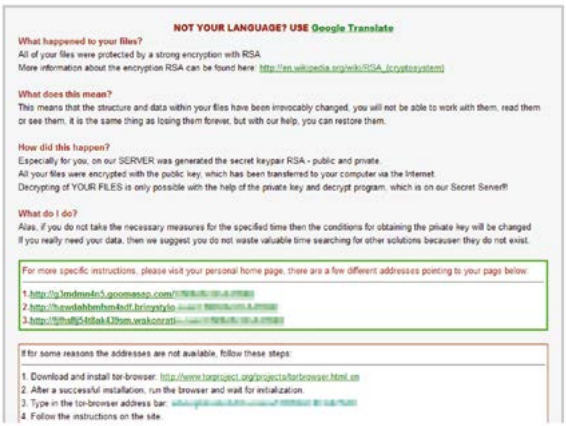
È sicuramente auspicabile che sempre più Aziende attuino processi di questo tipo, investano nella formazione e nella sensibilizzazione dei propri dipendenti, visto che, e ribadiamo, questo tipo di minacce devono essere considerate alla stessa stregua di quelle tradizionali, in quanto sono in grado di provocare danni che mettono seriamente in pericolo la vita dell'Azienda stessa.

Alcuni elementi sul cyber-crime in ambito finanziario con focus sull'Europa [a cura di IBM]

Temi principali dell'anno 2015

I dati IBM Security Trusteer per l'anno 2015 mostrano che il fenomeno del **malware bancario o malware specializzato in frodi finanziarie** si è sviluppato attorno a quattro principali codici malware: Neverquest, Bugat/Dridex, Dyre/Dyreza e Zeus 2, tutti basati su infrastrutture sofisticate, usati in numerose campagne di attacco nel corso dell'anno. L'attenzione si sta gradualmente spostando dall'utente casalingo agli utenti aziendali e corporate, con una conseguente massimizzazione degli importi frodati per ciascuna azione criminale.

Una lunga serie di altri malware (ad esempio Gozi, Tinba, Gootkit, Necurs, Ramnit ed altri) sono stati invece usati prevalentemente in campagne di attacco molto mirate verso istituzioni o soggetti specifici, e dal punto di vista strettamente numerico ciascuno ha costituito una presenza esigua.



Durante tutto il 2015 è cresciuta la diffusione dei **ransomware** (CryptoLocker, CryptoWall/Crowti, FakeBsod, Teslacrypt e altri) in particolare i **locker-ransomware**, che bloccano l'accesso all'intero dispositivo chiedendo il pagamento di una somma per riguadagnare il controllo del dispositivo, sono stati gradualmente soppiantati dai più insidiosi **crypto-ransomware**, codici che criptano i soli documenti lasciando però accesso al sistema che però risulterà vuoto e chiedendo un riscatto (generalmente nell'ordine delle centinaia di dollari) per riottenere i documenti in chiaro.

Questa particolare forma di malware è cresciuta di molto anche grazie alla diffusione di servizi di *ransomware as a service* gestiti da gruppi criminali che affittano servizi completi di ransomware a chi decide di gestire in proprio le campagne di estorsione informatica.

Già in passato il ransomware CryptoLocker e l'utilizzo della rete P2P (Peer-to-peer) Gameover ZeuS erano stati venduti o affittati come servizio. Il codice sorgente del malware ZeuS era apparso misteriosamente su Internet nel 2011 e questo aveva permesso a numerosi gruppi criminali di modificarne il codice per poi redistribuirlo, tanto che troviamo ancora

oggi molto malware di derivazione ZeuS. Le nuove varianti erano state in alcuni casi vendute o affittate, prima che l'operazione Tovar (Ottobre 2014) aveva bloccato l'infrastruttura di comunicazione di Gameover ZeuS.
In tempi più recenti alcune varianti del ransomware CryptoWall 3.1 e varianti di Dyre/Dyreza sono offerte nel dark web, offrendo veri e propri servizi di ***crimeware as a service*** chiavi in mano. Ai cyber criminali, acquistato il codice malware, rimane il compito di localizzare la messaggistica nella lingua nazionale, preparare il configuration file con gli obiettivi da attaccare e distribuire il malware, nella forma più semplice come allegato a mail di phishing o spear phishing.
Il crimeware as a service muove anche un piccolo indotto di servizi di supporto, come nel caso dei call centre operati da esperti in social engineering. Il servizio call-me-baby [PLR-100] recentemente individuato fornisce servizi di call centre nelle principali lingue Europee incluso l'Italiano. Il cyber criminale che vuole impossessarsi di credenziali di accesso sofisticate, ad esempio le OTP (One Time Password) o elementi di autenticazione out-of-band (ad esempio un SMS di verifica inviato dalla banca), può simulare attraverso il malware un problema temporaneo di operatività e indurre la vittima a chiamare il call-centre. Mentre molti utenti sono consapevoli del rischio phishing e quindi si guardano bene dal fornire elementi di autenticazioni in situazioni dubbie, pochi sono ancora consapevoli o preparati a fronteggiare un call-centre umano, specie se operato da soggetti particolarmente esperti in social engineering che parlano la nostra lingua.

Il cybercrime, e la relative azioni di contrasto, hanno visto una forte evoluzione dell'utilizzo delle **tecniche di encryption**. I cyber criminali hanno necessità di nascondere quanto più possibile le loro tracce, in particolare le comunicazioni con i server di C&C (Command-and-Control), mentre i prodotti antimalware o le organizzazioni di contrasto alla criminalità informatica, incluse le forze investigative e di Polizia, hanno necessità di decifrare codici e comunicazioni.
Tutti i più diffusi malware stanno spostando le comunicazioni con i server di C&C o le relative botnet sul dark web. CryptoWall 3.0, versione aggiornata del noto ransomware diffusasi a partire da Gennaio 2015, impone il pagamento del riscatto in BitCoin attraverso la rete di anonimizzazione Tor, istruendo le vittime all'installazione del Tor browser e rimandando per la procedura di pagamento ad un indirizzo sul dark web, con il chiaro obiettivo di evitare la localizzazione dei server di supporto e dei responsabili della frode operata dal ransomware. Inoltre CryptoWall 3.0 usa la rete I2P (The Invisible Internet Project) per anonimizzare le comunicazioni con i server di C&C.
La combinazione di Tor, I2P per le comunicazioni, assieme ai BitCoin per i pagamenti garantisce a CryptoWall e alla sua infrastruttura di supporto ancora lunga vita.

Anche il malware **Neverquest**, nelle sue versioni più recenti, basa buona parte delle proprie comunicazioni con i server di C&C sulla rete Tor, mentre il malware **Dyre/Dyreza** utilizza I2P per creare una dark net privata che collega tra di loro i nodi. Dyre si spinge oltre,

su ciascun computer infettato installa software che lo rende un nuovo nodo proxy di I2P, espandendo così la rete I2P di pari passo con la diffusione del malware, a tutto vantaggio della capacità di anonimizzazione e disponibilità.
La capacità di anonimizzazione di una dark net va di pari passo con la sua estensione e la conseguente difficoltà di controllare un numero sufficientemente alto di nodi. Con questo comportamento è come se ad ogni contagio Dyre si adoperasse per aumentare la complessità di individuazione della sua infrastruttura di comando e controllo.

Per comprendere l'impatto che sta avendo in Europa il tema delle comunicazioni attraverso le reti di anonimizzazione, sia originate dai malware che originate volontariamente dai navigatori per proteggere la propria privacy e anonimato, basta consultare i dati di Tor Metrics [PLR-101] che per l'intero anno 2015 riportano 7 paesi Europei tra i primi 10 paesi utilizzatori di Tor al mondo. L'Italia figura all'ottavo posto con una media di oltre 67.000 utenti giornalieri. Il progetto *the anonymous Internet* dell'Università di Oxford classifica l'Italia tra i più alti rapporti al mondo per utilizzatori medi giornalieri di Tor, con 1 utente Tor ogni circa 500 utenti Internet.

Numerosi progressi sono stati fatti durante l'anno nelle **tecniche di evasione dai prodotti Antivirus/Antimalware** e dai prodotti di analisi del codice eseguibile. Molti malware, ad esempio Dyre e alcuni altri di derivazione **Zeus**, utilizzano per la loro diffusione il downloader Upatre che nelle ultime versioni implementa tecniche di evasione da Windows Defender, Malwarebytes, AVG, Avira e ESET.
Una nuova variante del malware **Nemesis** [PLR-102], attiva nella seconda parte dell'anno, modifica il VBR (Volume Boot Record) di sistema, alterando il processo di boot e caricandosi in memoria prima della partenza del sistema operativo Windows. Il VBR è una piccola porzione di disco allocata all'inizio di ciascuna partizione che contiene codice per caricare in memoria e avviare il sistema operativo contenuto nella partizione. La particolare modalità di avviamento di Nemesis, prima e al di fuori del sistema operativo, lo rende particolarmente difficile da individuare con gli strumenti antivirus/antimalware tradizionali che girano all'interno del sistema operativo, e gli consente anche di sopravvivere in alcuni casi alla reinstallazione del sistema operativo.
Anche il malware **Rovnix** è un bootkit che installa parte del proprio codice nel VBR. Rovnix è attivo in Europa dal 2011, ma fortunatamente è poco diffuso e nel 2015 ha rappresentato poco più dell'1% di tutte le infezioni da malware in Europa.
Dyre ha implementato del 2015 anche nuove tecniche di randomizzazione del nome e del path del configuration file, rendendo molto più laborioso il lavoro degli antivirus che sono costretti a scandire l'intero disco prima di poterlo individuare. [PLR-103]

Abbiamo già citato il fenomeno dei call centre a supporto delle operazioni cyber criminali. La campagna denominata da IBM "Dyre Wolf" [PLR-104] [PLR-105] (il nome è stato ispirato dall'avidità del protagonista di *The Wolf of Wall Street*) ha **combinato assieme**

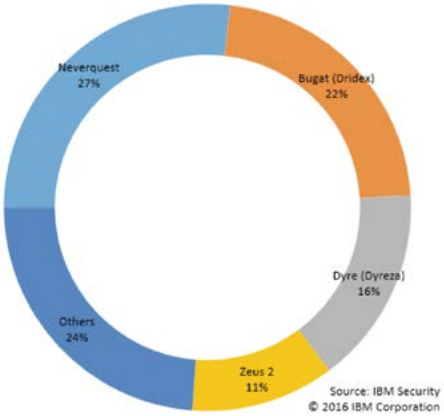
malware e tecniche di social engineering per indurre le vittime a chiamare un fantomatico call centre della banca attraverso il quale venivano indotte a rivelare importanti fattori di autenticazione, inclusa ogni forma di 2FA (Two-Factor Authentication) grazie ad un operatore umano che si presenta come operatore della banca e risponde al telefono nella lingua della vittima, ma in realtà abile e addestrato in tecniche di social engineering.
La seconda parte dell'anno ha visto uno spostamento dell'interesse verso gli account business e di grandi organizzazioni. La preferenza è sicuramente legata alla maggiore disponibilità di fondi su un conto business, e prova la capacità delle organizzazioni di cyber criminali di muovere ingenti quantità di capitali da una nazione all'altra lasciando pochissime tracce. Si ipotizza che il gruppo di Dyre e lo schema di attacco Dyre Wolf sia dietro un trasferimento elettronico fraudolento di 4.6 milioni di Euro ai danni della compagnia aerea Irlandese Ryanair. [PLR-106]

Tecniche più tradizionali, ma ancora remunerative, sono state usate durante tutto l'anno per estorcere denaro da banche e altre grosse istituzioni finanziarie per rimanere al sicuro da attacchi DDoS che avrebbero seriamente impattato, almeno nella minaccia, le operazioni Internet delle vittime.
È quello che hanno fatto gruppi criminali come i DD4BC (che sta per DDoS for BitCoin), attivo fin dal 2014, e il suo emulo Armada Collective comparso alla fine del 2015.
Ancora una volta il pagamento veniva richiesto in BitCoin per rendere più difficili le operazioni investigative.

Principali malware per frodi bancarie e finanziarie

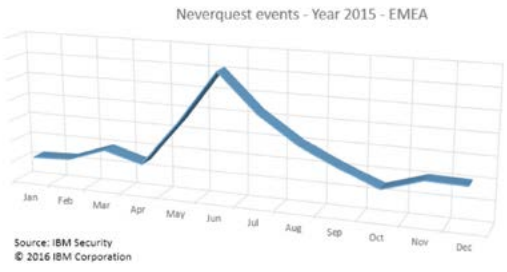
L'analisi che segue si concentra su malware specializzato per frodi finanziarie, perpetrate attraverso il furto di credenziali di accesso a siti di web banking e più in generale a sistemi di pagamento elettronico.

Dati IBM Security Trusteer per il 2015 in EMEA mostrano che il fenomeno malware si è concentrato attorno a quattro principali codici malware: Neverquest, Bugat (a.k.a. Dridex), Dyre (a.k.a. Dyreza) e Zeus 2. Questi - da soli - hanno costituito oltre il 75% di tutte le infezioni. Questi malware, basati su infrastrutture articolate, sono stati all'origine di numerose campagne di attacco nel corso dell'anno, orientate di volta in volta verso nazioni, istituzioni e soggetti diversi.
Una pletora di altri malware (Gozi, Tinba, Gootkit, Necurs, Ramnit, TDSS, Shifu, Rovnix, Zeus 1, BetaBot) sono stati rilevati nel



corso dell'anno, ma usati in campagne mirate di attacco verso istituzioni e soggetti di specifiche nazioni, e dal punto di vista numerico ciascuno ha costituito una presenza esigua.
Neverquest è indubbiamente il malware più diffuso in Europa. L'attività di Neverquest è stata particolarmente intensa tra Maggio ed Agosto, con un importante picco nel mese di Giugno. Bugat (Dridex) ha avuto un andamento altalenante, con un'importante diminuzione di attività nel mese di Settembre subito dopo l'arresto di Andrey Ghinkul [PLR-107], incriminato di frode informatica e di essere l'amministratore di una serie di botnet Bugat/Dridex, di cui la principale è stata parzialmente bloccata il 4 Settembre 2015 dalla National Crime Agency del Regno Unito in una operazione congiunta con autorità Statunitensi e numerosi partner tecnologici.

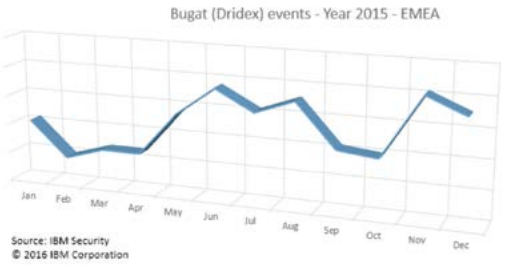
Andando più in dettaglio sull'evoluzione dei malware, l'andamento di **Neverquest** è stato particolarmente intenso tra Maggio ed Agosto e con un importante picco di attività nel mese di Giugno nel quale l'infrastruttura IBM Security Trusteer ha individuato eventi correlati a Neverquest pari ad oltre il doppio della media mensile sull'intero anno.



Neverquest è un malware scritto e usato prevalentemente per frodi bancarie, individuato per la prima volta nel 2013, ma che sembra in realtà l'evoluzione di una precedente famiglia di malware di cui in parte condivide l'infrastruttura dei server di C&C. Neverquest modifica la visualizzazione di alcuni siti bancari all'interno di browser compromessi, inserendo form e contenuti (web injects) con l'obiettivo di catturare le credenziali di accesso e inviandole verso l'esterno in forma criptata.
Il malware è veicolato attraverso diversi canali, inclusi *downloader* e *drive-by exploit kit*.
Uno dei downloader sfrutta la rete di anonimizzazione Tor per scaricare il nucleo principale del codice.

Il fenomeno dei drive-by exploit kit è particolarmente insidioso e si realizza inducendo l'utente a navigare su pagine web che nascondono attacchi, appunto gli exploit kit, per versioni vulnerabili di Java o dei plug-in del browser. Questi attacchi sono in grado di sfruttare macchine utente vulnerabili, impiantandovi malware, con la semplice navigazione sulle pagine malevole [PLR-108] anche in assenza di interazione dell'utente con la pagina. Nel corso del 2015 i *web browser exploit kit* hanno sfruttato la rara combinazione di portabilità del codice Java sia in termini di piattaforma che di browser, l'estrema diffusione di Java Runtime Environment su dispositivi di ogni tipo (inclusi i nuovi elementi costitutivi della Internet-of-Things), l'abbondante competenza specialistica nello scrivere codice Java, e il fiorente mercato underground per la vendita o il noleggio di exploit kit.

Bugat (o **Dridex**) è un malware specializzato nel furto di credenziali per l'accesso a siti bancari. Di Bugat si ha traccia fin dal 2009. Da allora gli sviluppatori di questo malware hanno gradualmente aggiunto funzionalità, fino alle più recenti tecniche di evasione dagli antivirus. Dal codice principale di Bugat sono state sviluppate varianti di codice con nomi diversi, i più comuni sono Dridex e Cridex.
Il vettore d'attacco sono email di *spear phishing* (phishing mirato verso specifici soggetti) che inducono la vittima ad aprire documenti Office allegati all'email, oppure raggiunti tramite un link. Questi documenti contengono macro o script, o a loro volta rimandano a siti web sul quale è ospitato codice che scandisce la macchina della vittima alla ricerca di eventuali vulnerabilità. Successivamente è scaricata la componente principale del malware che sfrutta proprio le vulnerabilità presenti sulla macchina e installa sul disco il malware.
Il furto delle credenziali avviene attraverso *web injects* ossia la capacità di inserire contenuti da far comparire nel browser e keyloggers che memorizzano le sequenze digitate sulla tastiera e le trasmettono verso l'esterno. Un codice così fatto può tenere sotto traccia la navigazione della vittima, e quando questa accede a siti bancari (elencati in un file di configurazione) comincia la sua attività, facendo comparire a schermo richieste di credenziali ed elementi addizionali di autenticazione, come il numero di carta di credito o i PIN dispositivi, facendoli apparire come legittima richiesta dal sito della banca e catturando poi quanto inserito.
Ciascun sistema infetto diventa elemento costituente di una botnet (o rete di computer compromessi) controllata dall'organizzazione criminale. A partire dal 2014 sono state osservate circa dieci distinte botnet Bugat/Dridex a livello mondiale. Una di queste, indentificata come EB120, controllava a Maggio 2015 oltre 100.000 computer. Per aumentare la resilienza dell'infrastruttura di botnet gli sviluppatori di Dridex hanno aggiunto capacità di comunicazione P2P tra peer di stesso livello, consentendo ai nodi di continuare ad avere una certa vitalità anche nel caso in cui la botnet principale dovesse essere bloccata.
In una imponente operazione di polizia internazionale, il 4 Settembre 2015 la National Crime Agency del Regno Unito, supportata da altre forze di Polizia e numerosi partner tecnologici, ha smantellato la rete dei server di C&C di Bugat/Dridex, arrestando a Cipro Andrey Ghinkul, ritenuto di essere a capo dell'organizzazione criminale responsabile di Bugat/Dridex. Poco prima dello smantellamento la botnet Dridex EB120 era diffusa principalmente in Europa, tra UK, Francia, Italia e Belgio.
L'attività di Bugat (Dridex) ha avuto un andamento altalenante, con un'importante decremento di attività nel mese di Settembre 2015 legato allo smantellamento della botnet EB120.
Il particolare meccanismo di resilienza realizzato combinando una classica botnet a comunicazioni P2P ha consentito alla rete di sopravvivere alla disattivazione di tutti i principali server C&C.

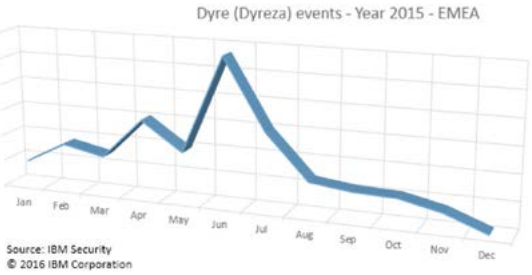


Un mese dopo alcuni nodi di secondo livello avevano riguadagnato la connessioni con nodi finali e a partire dal Ottobre 2015 nuove release di codice sono state iniettate nella botnet, segno che l'arresto del capo dell'organizzazione criminale responsabile di Bugat/Dridex e la disattivazione dei i server di C&C non era riuscita a fermare l'avanzata del malware, indubbiamente mantenuto da una importante organizzazione criminale.

Il malware **Dyre**, chiamato così per la stringa *"I am Dyreza"* trovata dentro il codice, è stato identificato per la prima volta nel Giugno 2014 con attacchi mirati verso banche negli Stati Uniti e Regno Unito [PLR-109]. La prima diffusione è stata verso siti di lingua Inglese, per poi spostarsi verso siti di web banking in Romania – Germania e la Svizzera di lingua Tedesca.
Il vettore di infezione delle prime versioni di Dyre sono documenti PDF allegati a email di spear phishing contenenti all'interno il downloader **Upatre**, che sfruttando codice Java-Script e un'immagine BMP appositamente malformata installano Upatre sulla macchina alla semplice apertura del PDF.
Upatre è un malware altamente specializzato nelle prime fasi dell'infezione (evasione o disattivazione dell'Antivirus, privilege escalation per acquisire i permessi amministrativi) e che poi scarica e attiva altri malware, tra cui anche Dyre. Il downloader Upatre scarica il malware Dyre da una rete di server di Command-and-Control dai quali riceve anche i file di configurazione che già dalle prime versioni di Dyre, contava oltre 100 siti di web banking [PLR-109] da monitorare.
Quando un computer infetto da Dyre naviga su uno dei siti descritti nel configuration file, ad esempio un sito di web banking, il codice si attiva e inietta nel web browser contenuti per ridirezionare tutto il traffico verso un sito replica, appositamente creato. L'utente continua a vedere nel proprio browser la URL della banca originaria, ma tutto quello che inserisce da tastiera viene ridirezionato verso gli attaccanti e non raggiunge mai il sito della banca, in questo ne l'utente ne la banca hanno modo di accorgersi che le credenziali di autenticazione sono state compromesse. Inoltre, il malware può inserire nel layout del sito bancario form con richieste addizionali, ad esempio credenziali addizionali o OTP (One Time Password).
Dopo essersi impossessati delle credenziali di autenticazione la rete di Dyre automaticamente si collega in tempo reale al vero sito della banca avendo pieno accesso al conto.

La vulnerabilità sfruttata dalle prime versioni di Upatre era una memory corruption risalente al 2013 e per la quale erano state rilasciate da tempo advisories e relativi aggiornamenti correttivi del Reader. Si sono quindi rivelati vulnerabili a Dyre i sistemi con Acrobat Reader non aggiornato da molto tempo, visto che Adobe aveva rilasciato gli aggiornamenti correttivi per questa vulnerabilità già nel Maggio 2013.
L'esempio di Dyre è eloquente, in quanto con il semplice aggiornamento periodico del Reader, ma più in generale di tutto il software installato, si sarebbero potuti contenere gli effetti di questo e di altri malware.
Dyre lavora per *campagne*, spesso legate a nazioni accomunate dalla stessa lingua. Una campagna di attacchi verso 17 siti di web banking spagnoli, nell'Aprile 2015, ha convolto

contemporaneamente anche alcuni siti di lingua spagnola in Cile, Colombia e Venezuela.
La grande diffusione di Dyre è iniziata con 2 campagne di phishing nell'Ottobre 2014, e dopo di allora ne sono seguite molte altre, sempre con la stessa modalità operativa.
La messaggistica viene tradotta in una specifica lingua, vengono create le definizioni dei siti di web banking di quella particolare nazione o gruppo linguistico e inserite nel configuration file, poi aggiornato su tutti i server di C&C. Sono stati contati oltre 300 server C&C a supporto di Dyre, alcuni condivisi anche con altri malware. Appena la configurazione è pronta vengono lanciate campagne di phishing, ciascuna campagna è contraddistinta da un CampaignID con data di inizio e la nazione target.



Un configuration file di Agosto 2015 riportava tra gli obiettivi circa 740 siti di web banking e pagamento online in 53 nazioni, incluse anche banche italiane. Anche in questo configuration file spicca la totale assenza di istituzioni in Russia e Ucraina.
Le nazioni europee colpite da Dyre nel corso del 2015 sono state, in ordine di eventi, il Regno Unito (che da sola ha totalizzato circa il 20% degli eventi mondiali), Germania, Francia, Spagna, Svizzera e Belgio.
Le ultime varianti di Dyre aggiungono supporto per **Windows 10**, e per il nuovo browser **Microsoft Edge**. Con questi aggiornamenti, Dyre è in grado di funzionare correttamente su tutti i sistemi operativi, da Windows Vista in poi, e su tutti i più diffusi browser.

Dyre Wolf

La campagna "Dyre Wolf" [PLR-104], [PLR-105] grazie alla **combinazione di sofisticato malware e di tecniche di social engineering** ha avuto pesanti conseguenze per alcune aziende corporate vittime di attacco. Dyre sembra essere operato da una vera e propria organizzazione criminale che prende di mira soprattutto vittime aziendali a cui invia, attraverso spear phishing, malware che intercetta le connessioni ai siti bancari usati normalmente per le transazioni commerciali. Le connessioni tra il browser della vittima e il sito bancario vengono intercettate e attraverso web injects vengono mostrati messaggi, all'interno del contesto del sito della banca, ad indicare che c'è un problema di operatività e invitano a chiamare l'operatore per continuare la transazione. A questo punto la vittima chiama l'operatore, convinto che si tratti della banca, invece al telefono risponde un membro dell'organizzazione criminale che chiede una serie di informazioni per proseguire la transazione, tra cui tutte le credenziali necessarie per effettuare una trasferimento elettronico di fondi. Proprio a questo punto l'organizzazione criminale si collega con il sito vero della banca, inserisce le

credenziali ed effettua il trasferimento, avendo anche la capacità di farsi dare al telefono dalla vittima eventuali codici di autorizzazione inviati per SMS o email.
Si ipotizza che questo schema di attacco sia dietro un trasferimento elettronico fraudolento di 4.6 milioni di Euro dalla compagnia aerea Irlandese Ryanair ad una banca Cinese. [PLR-106], [PLR-110], [PLR-111]
Campagne minori di malware si sono susseguite nel corso dell'anno. A Dicembre **Tinba v3** ha avuto come obiettivi clienti di online banking in Polonia, Italia, Olanda e Germania. Nel caso di queste nuove campagne di attacco la configurazione prendeva di mira prevalentemente account di grosse organizzazioni. La preferenza è sicuramente collegata alla maggiore disponibilità di fondi su un conto business in caso di successo dell'attacco, e prova la capacità delle organizzazioni di cyber criminali di muovere ingenti quantità di capitali attraverso i money mule.
Ancora a Dicembre 2015 il malware **GootKit** ha avuto come obiettivi siti di online banking di Francia, Italia e Regno Unito.

Pratiche minime di protezione

Alcune regole pratiche possono limitare la probabilità di compromissione dei nostri sistemi e delle proprie credenziali, riducendo l'impatto di potenziali azioni fraudolente:

- fare backup periodici dei propri dati (con frequenza quotidiana o almeno settimanale) su dispositivi di archiviazione esterni, multipli (almeno 2 diversi), alternati periodicamente e mantenuti in località diverse (ad esempio uno a casa e uno in ufficio). Inoltre il dispositivo di archiviazione deve essere disconnesso dal computer non appena terminato il backup. Non essendo possibile allo stato delle cose decriptare i dati, il ripristino da un backup è al momento l'unica strada perseguibile nel caso in cui si dovesse cadere vittima di un crypto-ransomware;
- diffidare da email non attese, o provenienti da mittenti sconosciuti o non credibili, specie se invitano ad aprire un allegato o cliccare su un link;
- attivare sull'antivirus la funzione di navigazione sicura e verifica dei link;
- attivare su tutti i browser le funzioni di navigazione sicura e verifica dei link (ad esempio il filtro SmartScreen di Internet Explorer o la protezione da phishing e malware presente in Firefox);
- verificare periodicamente il funzionamento delle funzioni di navigazione sicura e verifica dei link attraverso i siti di test messi a disposizione dai produttori dei browser;
- usare la massima cautela nell'aprire allegati, attendere comunque sempre che l'antivirus ne completi la scansione;
- invece di aprire direttamente l'allegato dalla mailbox, salvarlo su disco, scandirlo con l'antivirus e attendere il completamento della scansione prima di aprirlo;
- mantenere aggiornato il Sistema Operativo e tutto il software applicativo, abilitando i meccanismi di aggiornamento automatico e verificandone periodicamente il corretto funzionamento;
- ridurre la *superficie di attacco* verificando periodicamente i plug-in installati all'interno di

tutti i browser, rimuovendo quelli non necessari o non utilizzati recentemente, aggiornando quelli necessari e disabilitando i plug-in vulnerabili per i quali non esistono aggiornamenti (i browser più comuni hanno strumenti automatici di verifica);
- configurare il livello di sicurezza di Java su "Alto" o "Molto alto";
- aggiornare costantemente il Java Runtime Environment, configurando l'aggiornamento automatico;
- limitare l'esecuzione di applicazioni Java non firmate digitalmente o per le quali il certificato digitale non soddisfi i controlli operati dal browser;
- preferire eseguibili firmati digitalmente, per i quali il controllo del certificato operato dal sistema operativo consenta di verificare con certezza l'origine del software e che il codice non è stato alterato dopo la pubblicazione (integrità);
- verificare il corretto funzionamento dell'antivirus, in particolare relativamente agli aggiornamenti delle signature che devono essere quotidiani e andare sempre a buon fine in quanto alcuni malware cercano di sovvertire il meccanismo di aggiornamento dell'antivirus;
- accedere alle aree di memorizzazione in cloud (ad esempio dischi in cloud) solo per il tempo strettamente necessario, disconnettendosi non appena terminate le operazioni;
- iniziare quanto prima ad utilizzare soluzioni specifiche anti-malware che impediscano attacchi *man-in-the-browser* (MiTB) e proteggano la confidenzialità e l'integrità delle sessioni di navigazione ai siti di online banking;
- accertarsi sempre della fonte e dell'autorevolezza del software installato, specie quando si tratta di software gratuito cercato su Internet;
- attivare tutti i meccanismi di notifica di avvenuta transazione (SMS, email) forniti dalla nostra banca o Carta di Credito;
- controllare periodicamente le spese della carta di credito, segnalando prontamente alla banca eventuali addebiti anomali;
- vigilare con attenzione ogni volta che si presentano situazioni anomale nell'operatività della banca (ad esempio errori) e si viene invitati a proseguire l'operazione attraverso un operatore al telefono o in chat;
- di fronte a chiari segnali di phishing, anche se questi non coinvolgono noi o la nostra banca, segnaliamoli attraverso gli strumenti messi a disposizione dai browser (ad esempio il "Report unsafe website" di Internet Explorer)

Le grandi organizzazioni dovrebbero inoltre implementare strategie più articolate per evitare o limitare attacchi Corporate, come ad esempio:
- sensibilizzare i collaboratori sull'esistenza di attacchi mirati a specifiche organizzazioni, particolarmente convincenti e perpetrati attraverso schemi di *spear phishing* o *watering-hole;*
- utilizzare servizi di *IP address reputation* che consentano il blocco selettivo di IP, siti e URL ritenuti pericolosi;
- bloccare laddove consentito dai firewall perimetrali il traffico verso le reti di anonimizzazione, in quanto questo limita il meccanismo di comunicazione di molti malware;

- implementare soluzioni per la protezione dell'end-point, con verifica dell'integrità del browser e dell'intero sistema, protezione dell'integrità e confidenzialità del contenuto delle transazioni, prevenzione del riuso delle stesse password aziendali su siti esterni;
- implementare soluzioni per la verifica automatica della security posture di tutti i dispositivi aziendali indipendentemente dalla piattaforma e sistema operativo, bloccando l'attività di quelli che hanno settaggi insicuri o correggendo in automatico le configurazioni;
- introdurre soluzioni per il calcolo in tempo reale del fattore di rischio di ciascuna transazione, prendendo come base l'insieme di fattori di rischio costituiti dalle specifiche configurazioni del dispositivo, dell'applicazione, dei siti coinvolti e della sensitività della transazione;
- introdurre soluzioni per la cattura automatica di eventuale malware e trasmissione sicura verso i laboratori di analisi;
- addestrare il personale a riconoscere tentativi di phishing, anche attraverso simulazioni;
- implementare flussi approvativi con attori multipli e meccanismi di SoD (Segregation of Duties) nell'approvazione ed esecuzione di transazioni finanziarie.

Le istituzioni finanziare dovrebbero applicare livelli di protezione ancora più avanzata rispetto a quando appena elencato, come ad esempio:
- utilizzare soluzioni specifiche per la *fraud-detection* e *l'account take-over*;
- limitare l'accesso ai soli dispositivi che superino un livello considerato minimo di sicurezza;
- autenticazione a fattori multipli, autenticazione out-of-band (ad esempio SMS), utilizzo della geolocalizzazione del dispositivo mobile come ulteriore fattore di autenticazione;
- fornire ai propri clienti meccanismi di notifica in tempo reale di transazioni elettroniche.

Chi fornisce o sviluppa servizi sia sotto forma di web applications che di App per dispositivi mobili dovrebbe sempre avvalersi degli specifici SDK, testati e aggiornati e che forniscono già servizi completi di anti-malware, protezione delle sessioni di navigazione, identificazione di dispositivi rooted o jailbroken, protezione delle connessioni wifi pubbliche e insicure, limitando invece al minimo tutte le soluzioni che non abbiano subito rigorosi test e non siano aggiornate per inseguire costantemente l'evoluzione del malware.

Bibliografia

[PLR-100] *A Look Inside Cybercriminal Call* Centres - KrebsonSecurity, January 2016

[PLR-101] *Top-10 countries by directly connecting users* – The Tor project – Estrazione di dati dal 1-1-2015 al 31-12-2015

[PLR-102] D. Andonov, W. Ballenthin, N. Fraser, W. Matson, J. Taylor Thriving Beyond The Operating System: Financial Threat Group Targets Volume Boot Record - FireEye Threat Research, Dicembre 2015 - https://www.fireeye.com/blog/threat-research/2015/12/fin1-targets-boot-record.html

[PLR-103] O. Safran *Dyre Summer Renovation: Randomized Config File Names Keep Antivirus Engines Guessing* - SecurityIntelligence.com, August 2015 - https://securityintelligence.com/dyre-summer-renovation-randomized-config-file-names-keep-antivirus-engines-guessing/

[PLR-104] J. Kuhn *The Dyre Wolf Campaign: Stealing Millions and Hungry for More*, IBM X-Force, Aprile 2015 - https://securityintelligence.com/dyre-wolf/

[PLR-105] L. Kessem *Dyre Malware Takes Summer Holiday in Spain* – securityintelligence.com, July 2015 - http://securityintelligence.com/dyre-malware-takes-summer-holiday-in-spain/

[PLR-106] L. Kessem *2015: Cybercrime's Epic Year* - SecurityIntelligence.com, Dicembre 2015 - https://securityintelligence.com/2015-cybercrimes-epic-year/

[PLR-107] *Bugat Botnet Administrator Arrested and Malware Disabled* - U.S. Department of Justice, October 2015 - https://www.fbi.gov/pittsburgh/press-releases/2015/bugat-botnet-administrator-arrested-and-malware-disabled

[PLR-108] IBM Security Systems *IBM X-Force 2013 Mid-Year Trend and Risk Report*, September 2013

[PLR-109] *Protecting Against the Dyre Trojan: Don't Bring a Knife to a Gunfight* - SecurityIntelligence.com, December 2014 - http://securityintelligence.com/protecting-against-the-dyre-trojan-dont-bring-a-knife-to-a-gunfight/

[PLR-110] M. Cooter *Researchers blame Dyre Wolf malware for $5m Ryanair theft* – SC Magazine UK, Maggio 2015

[PLR-111] C. Hancock *Ryanair falls victim to €4.6m hacking scam via Chinese bank. CAB investigates after funds are taken from airline's account by electronic transfer* – The Irish Times, Aprile 2015

[PLR-112] L. Sutherland *2015 An Eventful Year in Cybersecurity* - IBM X-Force, Gennaio 2016 - https://securityintelligence.com/2015-an-eventful-year-in-cybersecurity/

Rapporto 2015 sullo stato di Internet e analisi globale degli attacchi DDoS [a cura di AKAMAI]

Analisi degli attacchi DDoS e trend emergenti

a. L'attività degli attacchi DDoS in forte aumento nel 2015

L'anno 2015 ha stabilito un record per il numero di attacchi DDoS osservati attraverso la rete con più del doppio del numero degli attacchi registrato nel 2014. Tuttavia, il profilo degli attacchi è cambiato. L'anno scorso gli attacchi ad alta larghezza di banda e attacchi di breve durata erano la norma. Ma nel 2015 il tipico attacco DDoS è stato inferiore a 10 gigabit al secondo (Gbps) con durata di meno di 24 ore. Ci sono stati diversi mega-attacchi nel 2015, ciascuno di ampiezza superiore a 100 Gbps: il più grande attacco DDoS osservato da Akamai ha raggiunto un picco a 240 Gbps.
Durante lo scorso anno 2015, i vettori degli attacchi DDoS sono mutati. Nel 2015 gli attacchi basati su Simple Service Discovery Protocol (SSDP) hanno rappresentato più del 20% dei vettori di attacco. SSDP viene abilitato di default su milioni di dispositivi per abitazioni ed uffici, tra cui router, server multimediali, web cam, televisori intelligenti e stampanti, in modo da permettere loro di scoprire l'altro su di una rete, stabilire la comunicazione e coordinare le attività. Se lasciati non protetti o mal configurati, questi dispositivi connessi a Internet possono essere sfruttati per l'uso come riflettori di attacchi DDoS (Internet-of-Things - IOT).
Durante il 2015 il settore del Gaming online è stato nuovamente il primo target per attacchi DDoS rispetto a qualsiasi altro settore. Quello del Gaming è rimasto il settore più colpito dal primo trimestre 2014, con più del 35% degli attacchi DDoS. Il settore Software e Tecnologia è stato il secondo più colpito nel 2015, con il 25% degli attacchi.

L'anno 2015 in sintesi:

> Aumento del numero totale degli attacchi DDoS
< Diminuzione degli attacchi DDoS a livello applicativo (Layer 7)
> Aumento degli attacchi DDoS a livello infrastrutturale (Layer 3 & 4)
< Diminuzione della durata degli attacchi
< Diminuzione del numero di attacchi superiori ai 100 Gbps
< Diminuzione della banda media degli attacchi DDoS
< Diminuzione dei picchi medi del volume degli attacchi DDoS
> Aumento degli attacchi di reflection

Anche se il numero di attacchi DDoS è aumentato, la percentuale di attacchi che aveva come obiettivo il livello di applicazione (Layer 7) è sceso nel corso dell'ultimo anno. Al contrario, gli attacchi DDoS diretti all'infrastruttura (Layer 3 e 4) sono aumentati rispetto al 2014. Mentre il numero di attacchi DDoS è aumentato nell'ultimo trimestre e nel corso

dell'ultimo anno, abbiamo osservato una diminuzione della durata media di attacco, così come del picco medio di banda (Mbps) e volume (Mpps).

b. La crescente minaccia dei siti di "Booter-stresser"

La diminuzione di durata della media degli attacchi può essere attribuita ad alcuni fattori. Il fattore principale è il crescente utilizzo di strumenti di tipo "Booter-Stresser". I siti che offrono strumenti di "Booter-Stresser" sono per definizione impostati per consentire agli amministratori di sistema di testare il carico di prova dei propri siti Web. Molti di questi siti sono semplicemente strumenti di "DDoS-for-hire" sotto mentite spoglie, basandosi sull'utilizzo di attacchi di tipo reflection per generare il loro traffico. Poiché la stragrande maggioranza di questi siti sono utilizzabili su abbonamento e di solito permettono solo attacchi per durata di 1.200 - 3.600 secondi (20-60 minuti), il loro crescente utilizzo è il motivo del calo della durata media degli attacchi osservata nel corso del 2015. In passato, gran parte degli attacchi DDoS erano basati su Botnet infette e sarebbero durati fino a quando l'attacco fosse stato mitigato, l'attaccante avesse rinunciato l'attacco o la botnet fosse stata neutralizzata. Infatti invece di spendere tempo e fatica per costruire e mantenere Botnet DDoS, è molto più facile per gli aggressori utilizzare gli strumenti "Booter-Stresser" per sfruttare dispositivi di rete e protocolli non correttamente posti in sicurezza.
Una revisione dei dati indica che gli strumenti di "Booter-Stresser" sono meno capaci di grandi attacchi, che al contrario le Botnet infette possono realizzare. Le pagine di login e di configurazione utente di questi strumenti sono quasi sempre ospitate dietro la protezione di una Content Delivery Network (CDN) gratuita o a basso costo. Questa collocazione fornisce agli attaccanti un livello percepito di anonimato e la capacità di lanciare i loro attacchi, almeno per un certo periodo di tempo, senza divulgare il loro punto di origine.
Un anno fa il picco di traffico usando queste tattiche da siti di "Booter-Stresser" generava una capacità misurata di 10-20 Gbps al secondo. Ora questi siti sono diventati più pericolosi, in grado di lanciare attacchi di oltre 100 Gbps. Con i nuovi metodi di attacco di tipo reflection che vengono aggiunti continuamente, come lo sfruttamento del protocollo SSDP, il danno potenziale da questi siti è destinato a crescere nel tempo.

c. L'adozione del protocollo IPv6 e i nuovi rischi di sicurezza

L'utilizzo di IPv6 DDoS non è ancora una prassi comune, ma ci sono indicazioni che gli attori maligni hanno iniziato la sperimentazione e la ricerca di metodi di attacco DDoS per l'IPv6. Una nuova serie di rischi e le sfide associate con la transizione a IPv6 stanno già interessando fornitori di servizi cloud così come fornitori di reti domestiche ed aziendali. Molti attacchi DDoS per l'IPv4 possono essere replicati utilizzando i protocolli IPv6, mentre alcuni nuovi vettori di attacco sono direttamente connessi con l'architettura IPv6. Molte delle caratteristiche del protocollo IPv6 potrebbero consentire agli aggressori di superare le protezioni basate su IPv4, creando una superficie di attacco DDoS più grande e forse più efficace.

d. Trend futuri

Ci aspettiamo di vedere un continuo trend di crescita di attacchi DDoS di lunga durata. Mentre il 2015 ha visto un attacco che misurava più di 240 Gbps e durato più di 13 ore, ci aspettiamo di vedere i futuri attacchi superare quei livelli.
Attori dannosi come DD4BC, Armada Collective e il Team OurMine continuano ad essere persistenti e creativi. Questi attacchi hanno ricevuto in alcuni casi successo e riteniamo che quindi gli stessi attori continueranno a spingersi avanti nella loro attività. Il loro numero e la varietà di strumenti di attacco probabilmente aumenteranno in futuro, rendendo inevitabile la minaccia di attacchi più grandi. Ci aspettiamo inoltre che i vettori SYN e SSDP rimangano molto popolari. La proliferazione di dispositivi connessi a Internet Home-Office non sicuri con protocollo Universal Plug and Play (UPnP) farà in modo che essi rimangano attraenti per l'utilizzo come riflettori di attacchi basati su SSDP.
Ci aspettiamo inoltre la continuazione degli attacchi al settore del Gaming online, spinti dalla continua ricerca dei giocatori di un vantaggio rispetto ai concorrenti e le vulnerabilità di sicurezza in piattaforme di gioco continueranno ad attirare gli aggressori in cerca di facili opportunità di sfruttamento delle vulnerabilità di sicurezza.
Il settore dei Servizi Finanziari rimarrà inoltre un obiettivo di rilievo, data la miriade di opportunità dei cyber criminali di estrarre e monetizzare i dati sensibili trafugati.
La collaborazione continua ad essere un imperativo per lo sviluppo del settore Software e Hardware, fornitori di servizi applicativi e cloud, e l'industria della sicurezza al fine di interrompere il ciclo di sfruttamento di massa, di costruzione di reti Botnet e per la monetizzazione. Nei prossimi mesi, ci aspettiamo un maggior numero di attacchi DDoS sulla rete, anche se i vettori e metodi di attacco continueranno a variare nel tempo.
Tra le nazioni maggiormente coinvolte negli attacchi, ci aspettiamo che gli Stati Uniti rimangano la fonte principale di traffico dannoso a causa del gran numero di dispositivi, vulnerabilità e utenti connessi a Internet, ed è probabile che i fornitori di servizi cloud rimarranno l'obiettivo più importante fino a che gli stessi non miglioreranno le loro procedure di sicurezza interne.

Attività DDoS nel 2015

a. Larghezza di banda, volumi e durata

Il numero di attacchi DDoS è stato in costante aumento trimestre su trimestre nel corso del 2015, anche se volume e larghezza di banda di picco media di attacco hanno continuato a scendere dal terzo trimestre del 2014. La larghezza di banda media di picco di attacco nel 2015 è stata di 7 Gbps, più bassa rispetto al picco medio di quasi 8 Gbps osservato nel 2014 e in lieve aumento rispetto alla media di 6 Gbps nel primo trimestre del 2015. Il volume medio degli attacchi è sceso in modo significativo rispetto al 2014, quando il record di picco medio è stato di 12 Mpps.
Le tendenze degli ultimi trimestri dimostrano che gli attori maligni stanno favorendo attacchi con larghezza di banda di picco più bassa, ma stanno lanciando attacchi più frequenti

rispetto a quanto realizzato un anno fa.

b. Mega attacchi DDoS

Nel 2015, 30 attacchi DDoS hanno registrato più di 100 Gigabit al secondo (Gbps). Questo è in leggero calo rispetto al 2014, quando abbiamo registrato un totale di 36 mega attacchi. Nel 2015 il più grande attacco registrato è stato di 240 Gbps, generati da un attacco volumetrico multi-vettore che ha utilizzato SYN flood insieme a UDP fragment flood e UDP flood. Tra i mega-attacchi, il settore del Gaming online ha ricevuto la quota maggiore di attacchi, anche se indirettamente.
Nel 2014, lo stesso tipo di attacco SYN flood, accoppiato a UDP fragment flood e UDP flood, ha prodotto un attacco DDoS record da 321 Gbps.
Nonostante nel 2015 il numero di mega attacchi sia diminuito, gli attacchi con picchi di oltre 50 Mpps sono estremamente pericolosi. Campagne di attacco di questo volume possono esaurire le risorse del contenuto della memoria indirizzabile (TCAM) nei router di frontiera, come quelli utilizzati dai fornitori di servizi Internet (ISP). Ciò può portare a perdita di pacchetti, andando a stressare la CPU - unità centrale di elaborazione - del router. Questo può causare danni collaterali in tutta la rete del provider di servizi Internet che gestisce il traffico di produzione per centinaia o migliaia di organizzazioni.
Il numero ridotto di mega attacchi DDoS, insieme con la mancanza di molti attacchi superiori a 150 Gbps, è una grande parte del motivo per cui la larghezza di banda di picco media di attacco diminuisce così drasticamente (25%) nel 2015. Abbiamo osservato inoltre una grande riduzione del numero di pacchetti negli attacchi più grandi. Il tasso di pacchetti (Mpps) ricevuti colpisce alcuni router e reti più che il numero di byte (Gbps) perché i pacchetti richiedono più memoria per la tracciabilità, impegnando risorse preziose.

c. I vettori DDoS in evidenza

Gli attacchi SYN e SSDP hanno rappresentato la maggioranza degli attacchi di tipo infrastrutturale. Solo nel terzo trimestre 2015, attacchi SYN e SSDP hanno rappresentato il 22,23% e il 24,01% di tutti gli attacchi, un aumento dal 14,62% rispetto al terzo trimestre del 2014. Lo sfruttamento del protocollo SSDP appare per la prima volta nel terzo trimestre 2014 e ancora non è stato soggetto agli stessi sforzi di pulizia come per NTP e DNS, dal momento che molte fonti di attacchi di reflection SSDP sfruttano dispositivi dell'Internet-of-Things (IoT). È improbabile che le vittime di abusi di tipo SSDP reflection si rendano conto che i loro dispositivi stanno partecipando ad attacchi DDoS. Anche se queste vittime osservano lentezza nelle loro reti, gli stessi non possono avere l'esperienza necessaria per risolvere completamente e mitigare la causa del problema.
In un quadro di visione più ampio, gli attacchi basati sull'infrastruttura hanno rappresentato la parte del leone nelle attività DDoS nel corso dell'anno 2015. Gli attacchi DDoS a livello di applicazione hanno rappresentato meno del 10% di tutte le attività, mentre il livello di infrastruttura ha sperimentato il 91% degli attacchi DDoS. Questa tendenza di attacchi per lo più a livello infrastrutturale continua da più di un anno, in quanto gli aggressori hanno

fatto affidamento sempre di più su vettori di reflection come principale metodo di attacco DDoS. Non solo questi attacchi di reflection sono più facili da lanciare, ma richiedono anche meno risorse da parte dell'attaccante.
Detto questo, gli script DDoS di attacco a livello di applicazione si sono spostati più verso l'uso delle risorse non basate su botnet, come gli script di attacco che sfruttano Proxy aperti su Internet. Questa tendenza, insieme con il continuo abuso di siti web basati su WordPress e Joomla come fonti di Flood, possono aprire la strada a un aumento degli attacchi DDoS basati sul livello applicativo per il futuro.
Anche se abbiamo scoperto ed analizzato due dozzine di vettori di attacco nel 2015, i primi 10 vettori sono stati responsabili per il 95% degli attacchi. Per comprendere meglio la natura ciclica degli attacchi, abbiamo analizzato questo sottogruppo di vettori di attacco nel corso degli ultimi cinque trimestri. La figura 1 mostra la frequenza di questi vettori di attacco all'interno di tale sottoinsieme. Ad esempio, la riduzione del traffico SSDP di attacco e il riemergere di attacchi frammento UDP come strumento primario riflettono la natura ciclica di strumenti e metodi del mondo degli attacchi DDoS. Abbiamo verificato un rapido aumento di strumenti utilizzanti reflection SSDP nel corso dell'ultimo anno, a dimostrazione di quanto facilmente questo protocollo possa essere oggetto di abusi.
Allo stesso modo abbiamo riscontrato un aumento degli attacchi NTP nel 2015, che probabilmente si ripresenterà all'inizio del 2016 dato che sono state recentemente rilevate nuove vulnerabilità nel Network Time Protocol. Detto questo, non tutte le vulnerabilità NTP producono risultati che possono essere usate per attacchi di Denial of Service. Finora l'unico metodo di abusi è il metodo Get Monlist nelle query NTP e alcuni server NTP sembrano avere ancora questa vulnerabilità. Questa tendenza di attacchi per lo più infrastrutturale ha continuato per più di un anno, in quanto gli aggressori hanno fatto affidamento sempre più sui vettori di attacco di reflection. Non solo gli attacchi reflection oscurano gli indirizzi IP veri dell'attaccante, ma richiedono anche meno risorse rispetto alle dimensioni dell'attacco.
Detto questo, gli script di attacco per gli attacchi DDoS a livello di applicazione si sono spostati verso l'uso di risorse non basate su botnet, ma di Open Proxy su Internet.

d. Attacchi DDoS al livello infrastrutturale e attacchi al livello applicativo

A livello di applicazione, gli attacchi HTTP GET sono attestati al 7% nel corso del 2015. HEAD, HTTP POST, e gli attacchi PUSH rappresentato meno dell'1% ciascuno. Molti degli attacchi flood GET sono stati basati su una combinazione di Joomla, WordPress e GET flood verso i proxy. Questi attacchi sono arrivati anche in forma di traffico reindirizzato dall'Asia. Altri attacchi a livello di applicazione sono stati utilizzati meno del 2% e l'utilizzo di HTTP GET Flood è stato costantemente favorito dagli attaccanti che hanno mirato al livello di applicazione.

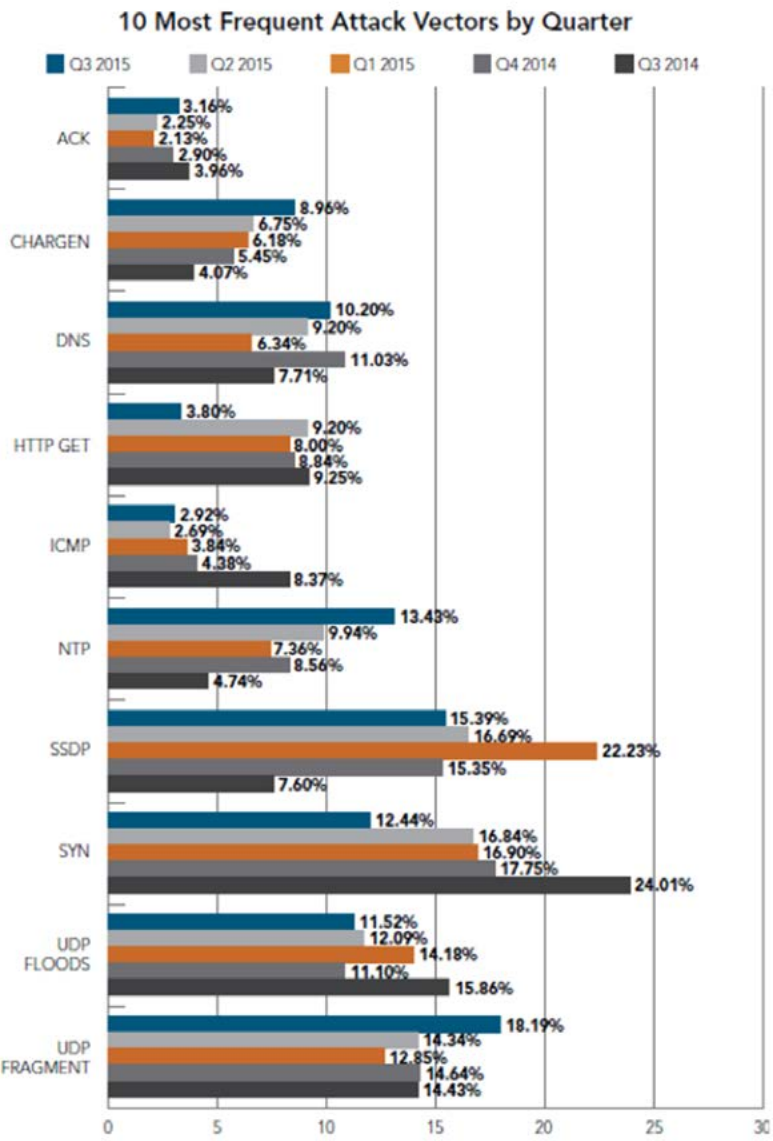


Figura 1: Frequenza dei 10 più comuni vettori di attacchi DDoS nel periodo Q3 2014 - Q3 2015. Fonte: Akamai

e. Le 10 nazioni fonti di attacchi DDoS

Guardando ai primi 10 paesi di origine per attacchi DDoS nel 2015, vediamo la Cina ancora una volta in cima alla lista, con circa il 23% del traffico DDoS. US, Germania, Brasile e Regno Unito seguono con circa il 45% del traffico, come mostrato nella Figura 2. Altri Paesi presenti nella relazione sono l'India, la Corea del Sud, Egitto, Taiwan, Australia, Russia, Spagna, Giappone e Messico.
Insieme, Cina, Stati Uniti e Regno Unito hanno rappresentato più del 50% degli IP fonte di attacco nel 2015. La Cina è rimasta il primo attore nel traffico di attacco DDoS non spoofing con il 30% rispetto al 23% dello scorso anno. I numeri mostrano un calo percentuale a partire dal 2014 riguardo i paesi di origine, quando gli Stati Uniti rappresentavano il 32% di tutto il traffico di attacco, seguiti dalla Cina e Regno Unito. Il calo percentuale non indica un calo di attacchi provenienti da questi paesi. Rispetto allo scorso anno, gli attacchi DDoS sono aumentati del 35% e hanno più che raddoppiato il numero dal primo trimestre 2014.
Alcune ragioni dell'aumento di fonti di attacco potrebbero essere attribuite all'aumento del traffico reindirizzato dall'Asia. Questo traffico reindirizzato è sembrato essere un attacco DDoS. La presenza dell'Australia nella lista è probabilmente dovuta all'incremento degli accessi a Internet ad alta velocità in tutta la regione e della connettività dei dispositivi IOT (Internet-of-Things).
È importante notare che la tracciabilità di un paese fonte di un attacco si basa principalmente sul traffico di un'applicazione che richiede una connessione completa. Il traffico di Infrastruttura, come l'UDP, è facilmente falsificabile, e quindi non è stato utilizzato in questa metrica.
Gli attacchi al livello applicativo, che rappresentano gli indirizzi IP non contraffatti, sono stati meno diffusi rispetto al passato. Nel 2015 hanno rappresentato solo meno del 10% di tutti gli attacchi DDoS registrati.

f. Analisi degli attacchi DDoS per settore di mercato

Il settore del Gaming online è stato particolarmente colpito nel 2015, rappresentando l'obiettivo di oltre il 35% di tutti gli attacchi. Al settore del Gaming online segue quello del Software e delle Tecnologie, che ha subito una grande percentuale di tutti gli attacchi, come mostrato nella Figura 3. Il settore Internet e Telecom è al terzo posto, seguito da Servizi Finanziari, Media e Intrattenimento, Istruzione, Beni al Consumo e Settore Pubblico.
Poiché i settori Software e Tecnologie, Internet e Telecom e Media e Entertainment hanno tutti un'interconnessione nei prodotti e nei servizi del settore del Gaming online, abbiamo considerato questi stessi come obiettivi di attacchi indiretti al settore del Gaming online.

Gaming Online

Il Gaming Online è rimasto il settore più colpito sin dal secondo trimestre del 2014. Nel 2015 gli attacchi sono stati alimentati da attori malintenzionati che hanno cercato di guadagnare l'attenzione dei media o notorietà da gruppi di pari malintenzionati, di danneggiare

la reputazione e causare disagi alle aziende di Gaming online. Alcune delle più grandi reti di console di gioco sono state apertamente e ampiamente attaccate nel dicembre del 2014, a causa dei nuovi giochi in rete lanciati per le festività natalizie. Il settore del Gaming online ha seguito l'andamento generale del 2015 di un maggior numero di attacchi DDoS reflection e un minor numero di attacchi DDoS basati sull'utilizzo di botnet. Questa tendenza è stata alimentata dalla disponibilità di siti di "Booter Stresser" che utilizzano attacchi di tipo reflection e dalla popolazione di giocatori online frustrati, che aumenta il rischio DDoS per questo settore.

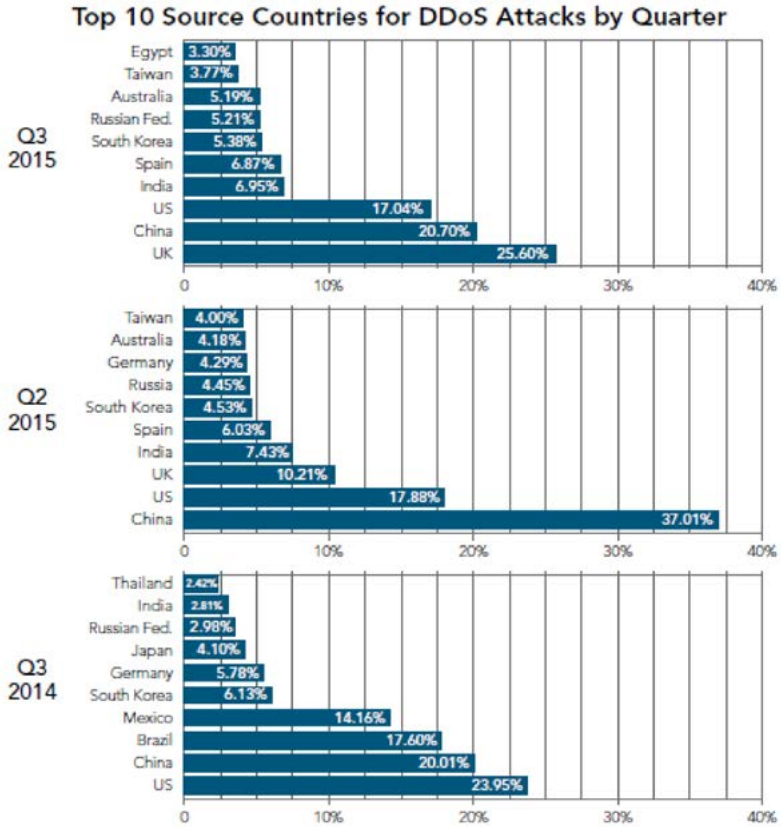


Figura 2: USA e Cina sono in evidenza tra le principali 3 nazioni fonti di attacchi provenienti da indirizzi IP non-spoofed. Fonte: Akamai

Software e Technology

Il settore del Software e Technology comprende le aziende che forniscono soluzioni come Software-as - a-Service (SaaS) e tecnologie cloud based. Sebbene questo settore abbia registrato un leggero calo (dal 28% al 25%) rispetto ad altri settori, in realtà ha subito un leggero aumento del numero di attacchi. I sub sectors verticali più comunemente mirati sono stati i fornitori di servizi di chat e gli sviluppatori di applicazioni non-gaming.

Internet e Telecom

Il settore Internet e Telecomunicazioni comprende le aziende che offrono servizi legati a Internet, come ISP e fornitori di servizi DNS. Gli aggressori di solito non bersagliano direttamente un ISP, ma mirano ai siti ospitati da un provider. Maggiore è il numero dei siti ospitati da un provider, maggiore è la probabilità che uno o più dei siti diventino l'obiettivo per un attacco DDoS. I siti possono variare da blog personali a siti di e-commerce e le motivazioni degli aggressori possono variare dalla politica all'estorsione.

Servizi Finanziari

Il settore dei Servizi Finanziari comprende banche, compagnie di assicurazioni, fornitori di strumenti di pagamento e le piattaforme di trading. Il settore finanziario ha sperimentato circa la stessa percentuale di tutti gli attacchi questo anno, come nel 2014. Recentemente, questo settore è stato al centro di vari tentativi di estorsione e il gruppo DD4BC ha aperto la strada con più attacchi di estorsione e DDoS contro i servizi finanziari. Come è il caso del settore del Software e Technology, questa industria ha visto un leggero aumento del numero di attacchi rispetto allo scorso anno 2014.

Media e Intrattenimento

Il settore dei media e dell'intrattenimento ha registrato un leggero calo nella percentuale di attacchi. Tuttavia una società in questo settore è stato il bersaglio del più grande attacco DDoS in Mpps registrato fino ad oggi che ha raggiunto i 222 Mpps. Attacchi DDoS ai Media sono di solito politicamente motivati, e gli attacchi possono essere lanciati da potenti avversari, come abbiamo visto nel corso del 2015.

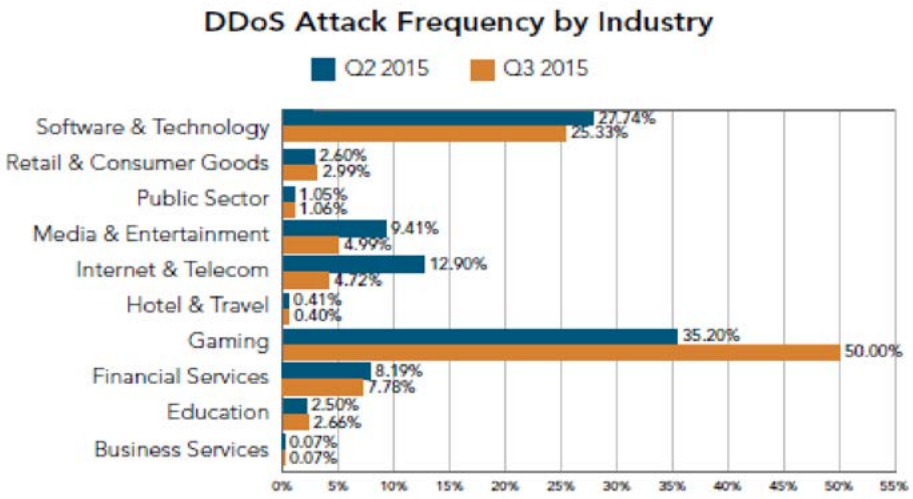


Figura 3: Insieme i settori del Gaming online e del Software e Technology sono stati obiettivo del 75% degli attacchi DDoS nel periodo Q2-Q3 2015. Fonte: Akamai

Case Study

a. Attacchi DDoS per estorcere pagamenti in Bitcoin: i gruppri DD4BC e Armada Collective

Panorama su DD4BC (DDoS-for-Bitcoin).
DD4BC, un gruppo dannoso responsabile di diverse campagne di estorsione Bitcoin dello scorso anno, sta espandendo le sue campagne di estorsione e Distributed Denial of Service (DDoS) per indirizzare una gamma più ampia di settori di mercato. DD4BC sembra utilizzare tecniche di attacco DDoS di tipo reflection basati su UDP, così come SYN Flood che imitano gli indirizzi IP crawler di Google, per mascherare il traffico dannoso.
In una lettera di minaccia, DD4BC sosteneva di avere la potenza di fuoco per lanciare attacchi DDoS oltre 400 Gbps, anche se non vi è alcuna prova concreta che potrebbe avuto effettuare un attacco di quelle dimensioni. Alla fine dell'anno scorso, il gruppo ha ripetutamente cercato di ricattare siti di Giochi online, minacciando le vittime con attacchi DDoS, al fine di estorcere bitcoin. La campagna tipicamente consisteva in una e-mail che informava la vittima che un basso livello di attacco DDoS era in corso contro il sito della vittima. Le email spiegavano che l'attività DDoS poteva essere osservata nei log del server

a livelli bassi, al fine di non interrompere il funzionamento del sitoweb della vittima. A seguito di questa spiegazione, DD4BC chiedeva un riscatto da pagare in bitcoin in cambio di proteggere il sito da un più grande attacco DDoS in grado di rendere irraggiungibile il sito web dell'azienda.
Gli obiettivi sembravano essere stati scelti per la loro riluttanza a coinvolgere le forze dell'ordine, come entità associate con attività di gioco illegale o fornitori di monete digitali non regolamentati, comunemente indicate come bitcoin. Data la natura illegale o non regolamentata delle loro attività, i proprietari dei siti di solito non hanno voluto il controllo delle forze dell'ordine.
Ma, viste le nuove minacce contro clienti che operano in operazioni di business legale e legittimo, DD4BC sembra essere più disposto a colpire obiettivi più grandi, anche se questo porta l'attenzione delle forze dell'ordine. Nella sua ultima ondata di attività di DD4BC, gli aggressori sembrano utilizzare tecniche di reflection distribuite sulla piattaforma AppEngine di Google. Gli aggressori potrebbero sfruttare i servizi di prova di Google, conseguentemente utilizzando questi servizi per attacchi di reflection. Questa teoria si basa sull'osservazione dei servizi potenzialmente sfruttabili scomparsi dopo che gli attacchi hanno fatto il loro corso.
Abbiamo identificato circa quattro campagne contro sette aziende target dove legittimi indirizzi IP di Google crowler sono stati falsificati in SYN flood contribuendo a mascherare il traffico dannoso, ma che potrebbero avere anche un impatto a lungo termine sul ranking nei motori di ricerca se fosse applicato il blocco degli IP a lungo termine. Tattiche di "Booter Stresser" sembrano anche essere state utilizzate come armi nelle ultimi attacchi.
Il gruppo è consapevole del fatto che le possibili vittime degli attacchi possano cambiare i loro indirizzi IP per difendersi e lo stesso gruppo ha minacciato vendette.

Panorama su Armada Collective

Nel 2015 abbiamo censito numerose campagne di riscatto tramite attacchi DDoS rivolte a clienti appartenenti a diversi settori di mercato. Un nuovo gruppo responsabile di questi attacchi si autodefinisce "Armada Collective". Le sue tattiche sono simili a quelle utilizzati dal Gruppo DD4BC, dove minacciano la vittima con e-mail di avviso di un imminente DDoS contro il loro sito web a meno che un riscatto non sia pagato in Bitcoin. Nei messaggi di posta elettronica, il gruppo di attori maligni si sono presentati e hanno informato la vittima che i loro server sarebbero stati vittima di un attacco DDoS a meno che non avessero pagato un riscatto specifico in Bitcoin. Armada Collective afferma che ha il potere di scatenare un attacco DDoS di più di 1 Tbps al secondo. Fino ad oggi, però, il più grande attacco di Armada Collective osservato ha raggiunto il picco di soli 772 Mbps.
Si è ha inizialmente sospettato che questo sia stato un attacco del gruppo DD4BC ripreso sotto un nuovo nome. In questa fase delle indagini siamo però più propensi a credere Armada Collective sia un gruppo di emulazione (CopyCat). Nel quadro generale le attività di attacco correnti non ci danno l'idea di una minaccia elevata. Comunque come DD4BC, vediamo Armada Collective come una fonte credibile di attacchi in futuro. Le organizzazioni

devono prendere sul serio questa minaccia.
La natura delle operazioni di Armada Collective e i successi che ha ottenuto ci porta a pensare che questo e altri gruppi continuino ad aumentare la propria gamma di obiettivi per altri mercati verticali. Le aziende a rischio di perdita di business dovuta a tempi di inattività dei loro siti Web sono a maggior rischio.
Storicamente, gli obiettivi di richieste di riscatto sono state selezionate in base alla loro reticenza di coinvolgere le forze di polizia, lasciandoli alla scelta di pagare il riscatto o di pagare per la protezione DDoS. Alcune vittime offrono premi per incoraggiare gli altri a rivelare le identità dei ricattatori ma questo può non riuscire a portare la giustizia agli esecutori del ricatto stesso.
Quando DD4BC è diventato un problema, abbiamo avvertito delle operazioni possibili di emulazione, copycat. Armada Collective è probabilmente solo il primo esempio di questo trend.

b. L'operazione DD4BC in sintesi

DD4BC, un gruppo dannoso responsabile di diverse campagne di estorsione di Bitcoin, ha ampliato la sua campagna di attacco di Distributed Denial of Service (DDoS) nel corso degli ultimi mesi. Alcuni attacchi di DD4BC identificati sono stati misurati fino a 50 gigabit al secondo (Gbps), con un volume superiore al massimo di 15-20 Gbps osservato all'inizio del mese di Maggio 2015, ma significativamente inferiore affermazioni del gruppo DD4BC di generare attacchi di 400-500 Gbps.
Gli ultimi attacchi coinvolgono nuove tattiche e metodologie, come descritto in questo Case Study. DD4BC ora minaccia di esporre un'organizzazione mirata attraverso i social media, oltre ai danni causati dalla attacco DDoS stesso. L'obiettivo è quello di mettere in imbarazzo pubblicamente il bersaglio, danneggiando in tal modo la reputazione dell'azienda e ottenendo una maggiore attenzione e credibilità per la sua capacità di creare interruzioni del servizio.
La nuova metodologia del gruppo include l'uso di campagne DDoS multi-vettore e rivisitando vecchi obiettivi. DD4BC sta' anche incorporando attacchi DDoS a livello Applicazione (layer 7) nella strategia dei suoi attacchi multi-vettore, in particolare concentrandosi sulla vulnerabilità di WordPress pingback per inviare richieste GET al bersaglio. I ricercatori hanno visto anche questo metodo di attacco incorporato nel quadro interno degli strumenti di DDoS "Booter Stresser".

Attack Timeline: Settembre 2014 – Luglio 2015. La linea temporale illustrata nella figura 4 mostra la misurazione della larghezza di banda di attacco (Gbps) e di milioni di pacchetti al secondo (Mpps) delle campagne di attacco DD4BC.
Il primo attacco DD4BC da noi osservato è stato verificato il 30 Settembre 2014. Il numero di attacchi DDoS è stato abbastanza costante durante i primi tentativi di estorsione del gruppo. Dal mese di Maggio a Luglio 2015, invece, gli attacchi dei DD4BC sono aumentati drammaticamente. Alla fine di Luglio abbiamo notato una diminuzione negli attacchi.

L'analisi temporale include gli eventi confermati fino al 24 luglio 2015. Più attacchi potrebbero essere avvenuti anche dopo tale data. Resta da vedere se la diminuzione degli attacchi della fine di Luglio sia un'indicazione che DD4BC stia perdendo capacità o semplicemente stia prendendo una pausa per rivedere le sue tattiche.

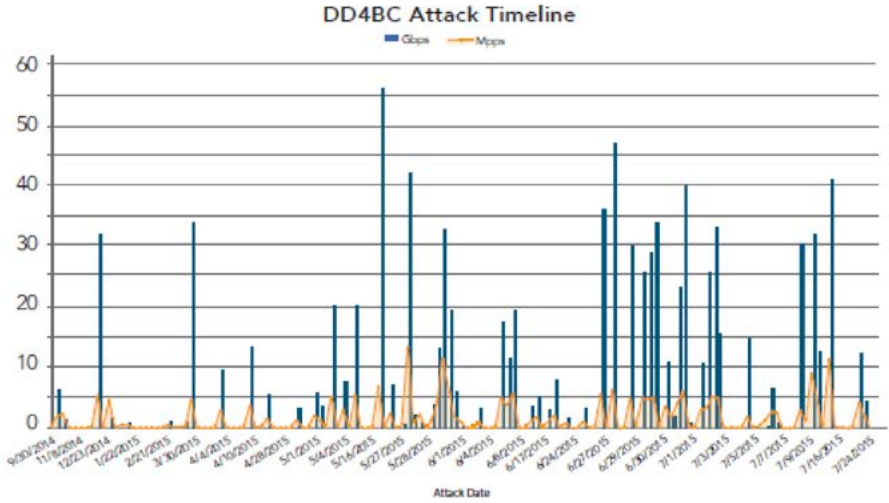


Figura 4: Periodo di attacco e misurazione della banda e del numero pacchetti per secondo relative ad attacchi DD4BC. Fonte: Akamai

I 75 attacchi identificati hanno avuto una media di 13.34 Gbps e 3.13 Mpps nel corso di un arco di 10 mesi. Nel Giugno 2015 otto attacchi hanno misurato più di 23 Gbps. La maggior parte di questi attacchi includeva vettori DDoS multipli, con durate più lunghe della media. DD4BC è stato particolarmente attivo in data 30 giugno 2015, con sei attacchi, seguiti da altri cinque il 1 luglio. L'evidenza dell'incremento nella crescita degli di attacchi è mostrata in Figura 5.

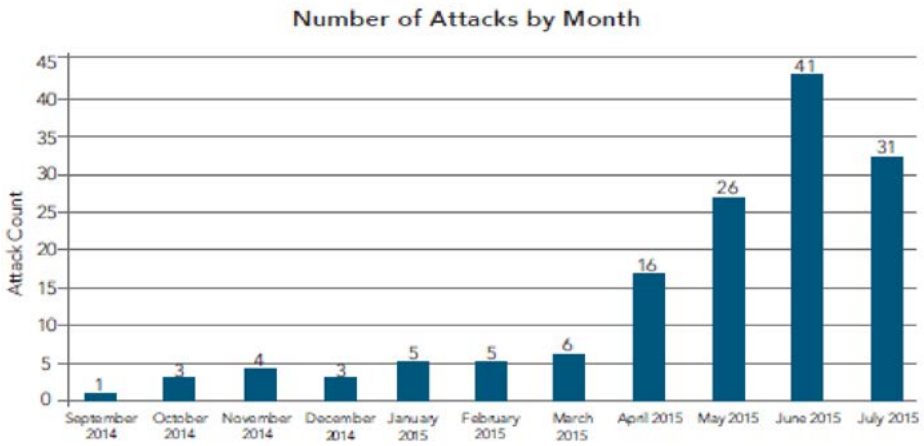


Figura 5: L'attività DDoS di DD4BC è cresciuta in modo importante in Aprile 2015, ma è diminuita a partire dal Luglio 2015. Fonte: Akamai

Mercati di riferimento – Fino al 24 Luglio 2015 DD4BC ha minacciato 124 organizzazioni, e i ricercatori hanno osservato che il gruppo ha ampliato i suoi obiettivi a diversi settori di mercato. La figura 6 mostra i mercati verticali obiettivi di attacchi DD4BC confermati. Il settore dei servizi finanziari è stato preso di mira nel 58% degli attacchi. Le banche e cooperative di credito hanno rappresentato il 35% degli attacchi a società di servizi finanziari, il 13% ai cambi di valuta, e il resto sono state società di elaborazione dei pagamenti.
I primi tentativi di estorsione sono stati fatti contro aziende di cambi di valuta e siti di gioco online nel 2014. Alla fine di Aprile 2015 il gruppo ha fatto un cambiamento di strategia ed ha iniziato a colpire il settore bancario. La maggior parte degli attacchi contro le banche e cooperative di credito si è verificato nel mese di Giugno. Quel momento è quando DD4BC è diventato più di una minaccia reale, perché i loro attacchi stavano ormai interessando aziende con una maggiore visibilità. Il settore Media e Intrattenimento ha subito il 12% degli attacchi di DD4BC, rispetto al 9% delle aziende di gioco online e del 6% per le aziende di beni al dettaglio al consumo.

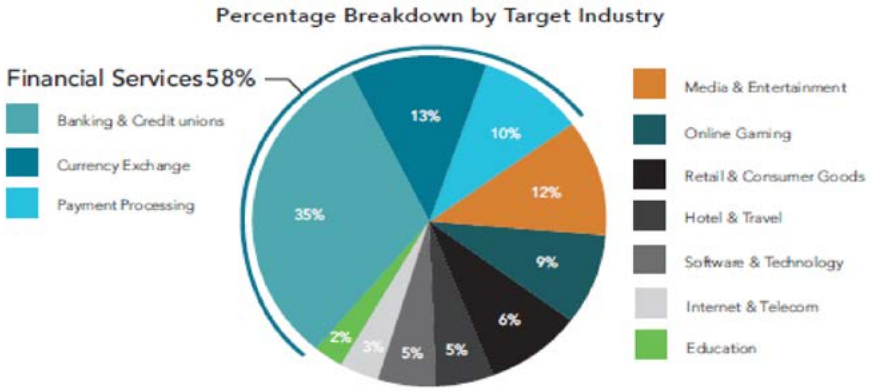


Figura 6: Distribuzione degli attacchi DD4BC per settore di mercato. Fonte: Akamai

Guardando al futuro

Ci aspettiamo di vedere un continuo trend di crescita di attacchi DDoS di lunga durata. Anche se questo 2015 ha visto un attacco che misurava più di 240 Mpps e durato più di 13 ore, prevediamo di vedere i futuri attacchi superare quei livelli.
Attori dannosi come DD4BC, Armada Collective e il Team OurMine continuano ad essere persistenti e creativi. Il loro numero e varietà di strumenti di attacco probabilmente aumenterà in futuro, rendendo gli attacchi più grandi inevitabili.
Prevediamo inoltre che i vettori SYN e SSDP rimarranno popolari. La proliferazione di dispositivi connessi a Internet non sicuri (IoT) con il protocollo Universal Plug and Play (UPnP) farà in modo che essi rimangano allettanti per l'uso come riflettori SSDP di attacchi DDoS.
Inoltre il pesante numero di attacchi nel settore dei giochi online continuerà in futuro, i giocatori continuano a ricercare un vantaggio rispetto ai concorrenti così come le vulnerabilità di sicurezza nelle piattaforme di gioco continuano ad attirare gli attaccanti in cerca di facili successi.
Il settore dei Servizi finanziari rimarrà inoltre un obiettivo di rilievo date le miriade di opportunità dei cyber criminali di estrarre e monetizzare i dati sensibili trafugati.
La collaborazione continua ad essere un imperativo per lo sviluppo dell'industria del software e dell'hardware, fornitori di servizi applicativi e cloud, e l'industria della sicurezza al fine di interrompere il ciclo di sfruttamento di massa, di costruzione di reti Botnet e per la monetizzazione.

Ci aspettiamo che gli Stati Uniti rimangano la futura fonte principale di traffico dannoso a causa del gran numero di dispositivi, vulnerabilità ed utenti connessi ad Internet negli Stati Uniti, ed è probabile che i fornitori di servizi cloud rimarranno l'obiettivo piu' importante fino a che non miglioreranno le loro procedure di sicurezza interne.

Bibliografia

- Q1 2015 State of the Internet – Security Report: https://www.stateoftheinternet.com/resources-web-security-2015-q1-internet-security-report.html

- Q2 2015 State of the Internet – Security Report: https://www.stateoftheinternet.com/resources-cloud-security-2015-q2-web-security-report.html

- Q3 2015 State of the Internet – Security Report: https://www.stateoftheinternet.com/resources-cloud-security-2015-q3-web-security-report.html

- White Paper- Making DDoS mitigation part of your incident response plan: critical steps and best practices: https://www.stateoftheinternet.com/resources-web-security-white-paper-2015-making-ddos-mitigation-part-of-your-incident-response-plan.html

- Akamai Blog-Operation Profile Armada Collective: https://www.stateoftheinternet.com/trends-blogs-operation-profile-armada-collectiver-ddos-bitcoin-extortion.html

- State of the Internet contributors (CSIRT): https://www.stateoftheinternet.com/about-contributors-experts.html

L'ecosistema criminale nel Dark Web

A cura di Pierluigi Paganini

Negli ultimi anni si sente sempre più spesso parlare di Deep Web e Dark Web, termini spesso abusati e confusi e di consueto associati ad attività criminali, cerchiamo quindi di comprendere quale è il loro significato.

Con il termine **Deep Web** si indica l'insieme dei contenuti presenti sul web e non indicizzati dai comuni motori di ricerca (ad es. Google, Bing), mentre con il termine **Dark Web** si indica l'insieme di contenuti accessibili pubblicamente che sono ospitati in siti web il cui indirizzo IP è nascosto, ma ai quali chiunque può accedere purché ne conosca l'indirizzo. Elementi appartenenti al Dark Web sono anche i contenuti privati scambiati tra utenti all'interno di un network chiuso di computer, strutture definite come darknet. Tra le darknet più popolari annoveriamo la rete TOR (The Onion Router), The Invisible Internet Project (I2P), Freenet ed anoNet. Senza dubbio la rete Tor è la più popolare tra esse, tale infrastruttura consente di anonimizzare l'accesso a internet dei suoi utenti e proprio le condizioni di pseudo-anonimato che essa offre la rendono un elemento di attrattiva per organizzazioni dedite al crimine informatico.

Altri elementi che rendono la rete TOR popolare nell'ecosistema criminale sono la difficoltà delle forze dell'ordine a svolgere operazioni di monitoraggio su larga scala e la funzione di aggregatore che si riconosce ai principali black market che la rete ospita.

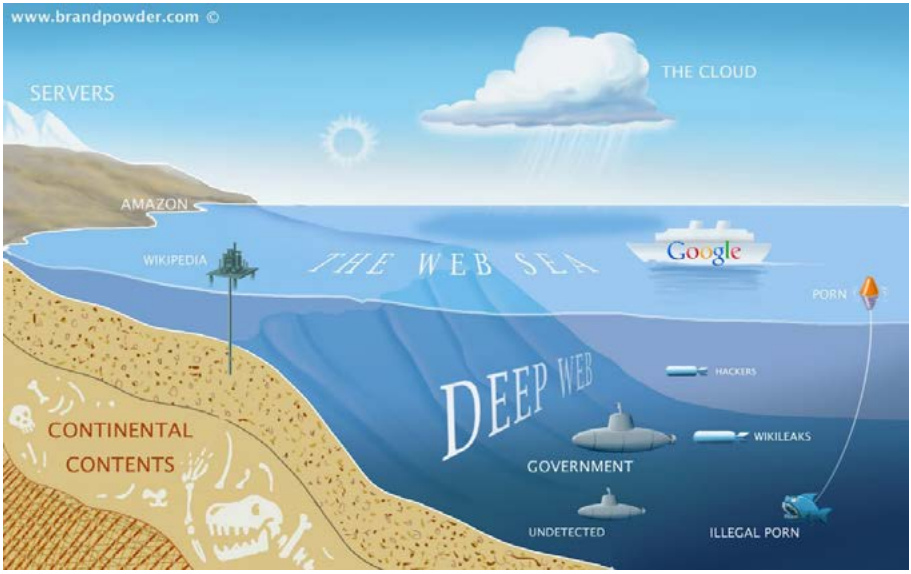


Figura 1 - Rappresentazione Deep Web

Esistono molte tipologie di Darknet, la più popolare delle quali è senza dubbio la rete TOR ed è per questo motivo che analizzeremo i principali fenomeni che l'hanno caratterizzata nell'ultimo anno.
Innanzitutto cerchiamo di comprendere quali siano gli utenti della rete TOR: è facile verificare che non esiste una vera e propria tipologia di utente in quanto la popolare rete è frequentata da attori diversi e per motivazioni distinte. Una analisi dei contenuti consente la facile verifica della presenza di gruppi di criminali, hacktivist, script kiddies, giornalisti, dissidenti, terroristi e molto probabilmente agenzie di intelligence.
Dopo una rapida perlustrazione di questa parte del web è facile rendersi conto che la maggior parte delle transazioni che sono effettuate nei principali black market sono relative alla vendita di sostanze stupefacenti e a servizi/prodotti per la realizzazione di frodi finanziarie.
In questa trattazione ci focalizzeremo sui reati perpetrati attraverso lo strumento informatico, attività illegali che di recente l'Interpol ha raggruppato nelle seguenti categorie:

- Attacchi informativi contro sistemi hardware e software
- Crimini finanziari
- Pedo pornografia

Bene, le darknet offrono ogni genere di servizio e prodotto per agevolare le pratiche illegali citate.
Il dark web è un luogo particolarmente interessante per le comunità di sviluppatori di malware e per i loro clienti. Nel molti black market che vi risiedono è molto semplice reperire codici malevoli e servizi utili alla personalizzazione e distribuzione di malware.
Le Darknet sono utilizzate dagli sviluppatori di malware per celare le strutture di comando e controllo delle botnet e renderle resistenti alle operazioni delle forze dell'ordine.
I Command & Control server occultati in reti come Tor ed I2P risultano di difficile individuazione, garantendo maggiori possibilità di successo ai gestori delle botnet.
Nella **Figura 2** sono riportati i malware che dal 2012 sono stati distribuiti utilizzando infrastrutture di controllo nascoste nelle reti Tor ed I2P. Appare evidente che il numero di malware che utilizzano le suddette reti sia aumentato negli anni a conferma dell'attitudine dei gruppi di criminali informatici a servirsene.

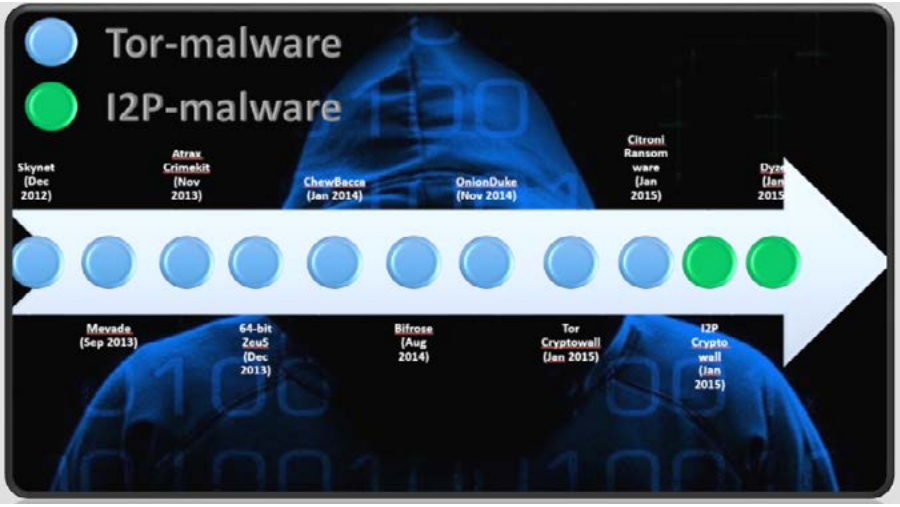


Figura 2 - Malware e Darknet

Critroni, Cryptowall, Vawtrak e Dyre sono solo alcuni esempi di malware che hanno occultato i C&C server nelle reti Tor ed I2P. Nell'underground criminale è facile trovare kit per lo sviluppo di malware, nel Maggio 2015 gli esperti dell'azienda di sicurezza McAfee hanno scoperto una piattaforma per la creazione di ransomware denominata Tox.
Per darvi un'idea dei servizi e dei relativi prezzi si pensi che per acquistare un malware è possibile spendere da poche decine fino a qualche migliaio di dollari per un servizio di personalizzazione completa di un codice malevolo.

Le Darknet offrono molto altro. È infatti possibile fruire di numerosi servizi accessori, quali servizi di crypting e servizi di distribuzione del malware.
I servizi di cripting (Crypting services) sono essenziali per nascondere le principali componenti di un codice malevolo ai principali sistemi di sicurezza, per fruire di tali servizi è sufficiente inviare il codice del malware a un servizio che provvede ad offuscarne le parti di interesse rendendone difficile l'analisi.
Nella **Figura 3** è riportata la pubblicità relativa a servizi di Crypting scoperti dagli esperti di Trend Micro nel corso di una analisi dell'underground criminale del North America.

Figura 3 - North American Underground Report (Trend Micro)

Nella tabella di **Figura 4** invece sono riportati i costi dei servizi per la diffusione del malware per area geografica, dai dati forniti da Trend Micro emerge che nell'ecosistema criminale russo è possibile spendere dagli 80 ai 130 dollari per mille istallazioni di malware su macchine europee.

PPI (Cost per 1,000 installations)	2011	2012	2013	2014	2015
Australia	US$300–500	No data	No data	US$160–190	US$100–180
UK	US$220–$300	No data	US$150–400	US$150–350	US$90–130
US	US$100–150	US$100–250	US$120–200	US$90–150	US$40–100
Europe	US$90–250	US$75–90	US$50–110	US$90–240	US$80–130
Russia	US$100–500	No data	US$140–400	US$100–300	US$100–200
Asia	No data	No data	No data	No data	US$140
Global	US$12–15	US$10–20	US$10–12	US$8–15	US$10–12

Figura 4 - Russian Underground 2.0 Report (Trend Micro)

A preoccupare maggiormente è la diffusione di servizi di malware-as-a-service in cui gli utenti pagano per avere una propria versione di un codice malevolo. A farla da padrone nel 2015 sono stati i ransomware, software in grado di bloccare l'accesso alle risorse di un computer (ad es. file utente) fino al pagamento di una somma di denaro da parte delle vittime. Un esempio? In settembre gli esperti dell'azienda Sensecy hanno scoperto la piattaforma ORX-Locker che consentiva ai propri utenti di creare il proprio ransomware in soli tre passi.

Come anticipato, tra i maggior elementi di attrattiva dell'underground criminale vi sono senza dubbio i black market, luoghi in cui gli utenti possono acquistare prodotti e servizi, è opportuno quindi analizzare quali sono gli operatori dietro queste attività e quali competenze hanno.
Rappresentando tali ambienti con una struttura piramidale, avremo al vertice figure con elevate competenze informatiche: questi operatori amministrano il sistema e ne gestiscono i proventi. Nella parte intermedia troviamo i broker e i venditori, ovvero coloro che utilizzano le piattaforme per proporre servizi di varia natura, dal noleggio di botnet a servizi di spamming. Non sempre questi operatori hanno skill elevati, tuttavia è facile imbattersi in professionisti che accanto a spiccate capacità informatiche hanno competenze di mercato che usano per proporre al meglio i propri prodotti o agendo da broker per terze parti.
Alla base della piramide, ma non per questo meno importante, troviamo i "mules", ovvero quelle figure che consentono di "convertire" le attività illegali in denaro (cash out), ad esempio attraverso attività di riciclaggio. Queste figure spesso non sono dotate di capacità tecniche, a loro sono assegnati compiti per convertire i proventi dell'attività illegale in danaro, ad esempio fisicamente acquistare merce con carte clonate oppure effettuare bonifici verso conti gestiti dai criminali trattenendo per sè una piccola quota delle somme loro versate.
Tra gli studi italiani di maggiore interesse nell'analisi dei black market pubblicati nel 2015 vi è senza dubbio l'analisi presente nell'annuale Rapporto statistico sulle frodi con le carte di pagamento No. 5/2015 prodotto dall'Ufficio Centrale Antifrode dei Mezzi di Pagamento (UCAMP). Il rapporto include un'approfondita analisi sulle attività fraudolente attraverso il Dark Web.
Per tutto l'anno 2014 gli esperti hanno osservato i principali black market, monitorando i cambiamenti nelle offerte di prodotti e servizi per un'ampia gamma di attività illegali relative alle frodi con carte di pagamento. Si è potuto constatare che il prezzo dei dati delle carte di credito è andato riducendosi nel tempo. Tale flessione è imputabile alla grande disponibilità di dati relativi a carte di pagamento sottratti nel corso dei numerosi attacchi osservati nei mesi precedenti. Alla stesura del presente rapporto i principali black marker attivi in rete TOR erano i seguenti (vedi **Figura 5**).

Black Market	Indirizzo Onion rete Tor	N° prodotti	N° prodotti per frodi con carte di pagamento	%
Abraxas	abraxasdegupusel.onion	7590	60	0,79%
Agora	agorahooawayyfoe.onion	24110	80	0,33%
AlphaBay	pwoah7foa6au2pul.onion	16150	735	4,55%
Nucleus	nucleuspf3izq7o6.onion	17361	80	0,46%
Outlaw	outfor6jwcztwbpd.onion	NA	NA	NA
Italian DarkNet Community	2qrdpvonwwqnic7j.onion	104	28	26,92%
Dream Market	ltxocqh4nvwkofil.onion	2068	30	1,45%
Haven	havenpghmfghivfn.onion	720	10	1,39%
Middle Earth	mango7u3rivtwxy7.onion	5256	22	0,42%

Figura 5 - Black Market – Rapporto Ufficio Centrale Antifrode dei Mezzi di Pagamento (UCAMP).

Gli esperti del gruppo di lavoro hanno constatato la possibilità di acquistare prodotti relativi alle frodi con carte di pagamento ai prezzi riportati nella tabella seguente. I prezzi sono riferiti a pezzi singoli e sono indicativi essendo le quotazioni variabili e funzione del volume di dati che si intende acquistare, dalla provenienza geografia, dall'importo minimo garantito e dalla data di scadenza delle carte di pagamento.

Prodotto	Prezzo
CVVs	
Visa and MasterCard CVV (US)	$3-$20
American Express CVV (US)	$5-$20
Visa and MasterCard CVV (EU)	$15-$30
Visa and MasterCard CVV (Australia)	$8-$10
Visa and MasterCard CVV (Canada)	$6-$15

continua >

Prodotto	Prezzo
DUMPs	
Visa and MasterCard Dump (US)	$20-$45
American Express DUMP (US)	$25-$50
Visa and MasterCard DUMP (EU)	$35-$60
Visa and MasterCard DUMP (Australia)	$45-$50
Visa and MasterCard DUMP (Canada)	$35-$50
FULLz	
US FULLz	$25-$100
EU FULLz	$30-$125

Il dark web è probabilmente uno dei luoghi preferiti dalle numerose comunità di hacker che affollano il web, molteplici sono i forum ed i black market che sono frequentati da questa tipologia di professionisti.
Nel corso del 2015 abbiamo assistito ad una rapida crescita delle comunità di hackers nelle principali darknet, molte delle quali si specializzano nella vendita di prodotti e servizi per hacking a per le frodi di vario genere.
Ciascun gruppo di hacker ha le sue caratteristiche, un proprio modus operandi ed una sua offerta. Ad esempio, nell'underground cinese è possibile reperire qualunque prodotto o servizio per la realizzazione di frodi attraverso dispositivi mobile, mentre nelle comunità russe ed americane è possibile reperire servizi di hacking e tutto quanto concerne lo sviluppo e la distribuzione di malware.

Di seguito alcuni esempi relativi all'offerta delle principali comunità di hacker nelle darknet:
- Un record contenente informazioni personali di un utente (PII record) è venduto a $1. (Fonte: Trend Micro).
- Account PayPal ed eBay sono acquistabili a partire da $300 (Fonte: Trend Micro).
- Account per online banking sono venduti a prezzi compresi tra $200 e $500 in funzione del saldo contabile e della relativa storia.
- Le scansioni di documenti di identità e patenti sono acquistabili per una cifra compresa tra i $10 ed i $35 (Fonte: Trend Micro).
- Documenti contraffatti costano dai $200 ai $1000, mentre una falsa patente americana può essere acquistata ad una cifra di $100-$150.
- Hackerare un account Facebook, Twitter o di altre piattaforme di social networking può costare dai $50 ai $200 dollari.
- Un Remote Access Trojan costa dai $150 ai $400.
- Il codice sorgente di un malware bancario con annessa personalizzazione è offerto per una cifra dai $900 ai $1500.

- Noleggio di una botnet per un attacco di un DDoS di circa 24 ore può arrivare a costare fino a $1500.

È lecito chiedersi a questo punto quale sia il volume di affari dell'ecosistema criminale che stiamo analizzando, un gruppo di esperti ha studiato i 35 principali black market verificando che essi riescono a gestire transazioni per un ammontare che oscilla dai $300,000 ai $500,000 al giorno.
Circa il 70% di tutti i venditori si limita alla vendita di prodotti per un ammontare complessivo inferiore ai 1.000 dollari, un altro 18% dei venditori realizza vendite tra i $ 1.000 e $ 10.000, solo il 2% dei produttori è riuscito a vendere più di $ 100.000.
Ci troviamo dinanzi ad una economia in espansione, considerando che il popolare black market Silk Road nel 2012 aveva un giro di affari annuo di circa 22 milioni di dollari (Studio Carnegie Mellon 2012).

Altra piaga del Dark Web è la pedo pornografia, purtroppo nelle principali darknet è facile imbattersi in siti web frequentati da utenti che condividono o vendono immagini di minori. L'anonimato di queste reti offre un ambiente ideale per questa tipologia di criminali, una ricerca condotta da Trend Micro lo scorso anno ha dimostrato che proprio il materiale pedo pornografico presente nelle darknet rappresenta una porzione significativa del contenuto complessivo di queste reti.
Gli esperti hanno condotto un singolare esperimento, una volta identificate 8,707 pagine "sospette" in rete hanno analizzato i link contenuti in queste pagine e che referenziavano contenuti nelle darknet. I contenuti dei siti web presenti nel dark web sono risultati i seguenti:

- Siti utilizzati per la distribuzione di malware (drive-by download) (33.7%).
- Siti per anonimizzare la navigazione in rete (31.7%).
- Siti contenenti materiale Pedopornografico (26%).

I risultati, seppur condotti su un campione non rappresentativo, lasciano poco spazio ai dubbi, le darknet sono un ambiente familiare per criminali e pedofili.
Chiudiamo questo rapido giro nel dark web con un doveroso riferimento alla tematica terrorismo. Ancora una volta le darknet possono rappresentare un'opportunità per attività illegali, in questo caso offrendo uno spazio sicuro ad organizzazioni terroristiche.
Molti siti sono utilizzati da membri di organizzazioni come l'ISIS e Al Qaeda per attività di propaganda, tali siti vengono utilizzati per condividere video e immagini relative alle attività dei gruppi radicali.
Il Dark Web è un ambiente difficile da monitorare per ammissione stessa degli esponenti delle agenzie di intelligence e delle forze dell'ordine, è naturale quindi che cellule terroristiche lo utilizzano per le proprie attività. Alcuni hidden service presenti nella rete TOR sono stati utilizzati come repositori degli eseguibili di mobile app utilizzate da gruppi jihadisti per comunicazioni sicure. Abbiamo notizia di alcuni siti utilizzati per condividere indirizzi Bitcoin per la raccolta di fondi per finanziare attività delle cellule operative in occidente.

In rete è reperibile il testo "Bitcoin wa Sadaqat al Jihad" che spiega come acquistare armi nel dark web per azioni terroristiche. Le darknet sono state anche utilizzate per diffondere un manuale, intitolato "*How to Tweet Safely Without Giving out Your Location to NSA*." che istruisce i militanti dell'ISIS a eludere le attività di sorveglianza operate dalle agenzie di intelligence occidentali.

Cosa aspettarsi nei prossimi 12 mesi?

Le Dark web continueranno a offrire un ecosistema privilegiato per gruppi di criminali, hacker e terroristi, gli autori di malware sfrutteranno con maggiore frequenza le reti TOR ed I2P per nascondere le infrastrutture di controllo delle loro botnet e renderle quindi resistenti a vari tipi di attacchi operati dalle forze dell'ordine.

Altro fenomeno che caratterizzerà il prossimo futuro dell'ecosistema criminale all'interno del Dark Web è l'affermarsi del modello di vendita noto come criminal-as-a-service (CaaS), in cui gruppi di hacker offriranno i propri servizi al crimine ordinario con conseguenze pericolose per la collettività.

Le segnalazioni del CERT Nazionale

Il CERT Nazionale si rivolge a due gruppi distinti di "utenti". Un primo gruppo, aperto, che comprende PMI e cittadini, fornendo informazioni utili per la prevenzione e soluzione di problemi informatici, nonché informazioni volte alla sensibilizzazione sui temi più generali legati alla sicurezza informatica, attraverso il sito web. Un secondo gruppo, chiuso e ristretto, costituito da diversi Operatori privati, gestori di rilevanti infrastrutture informatizzate, con i quali esiste un rapporto diretto per lo scambio di informazioni.
I riferimenti normativi che definiscono il CERT possono essere ritrovati nel Decreto Legislativo 1 agosto 2003 n. 259 ("Codice delle comunicazioni elettroniche"), modificato dal Decreto Legislativo 28 maggio 2012 n. 70 (attuazione delle direttive 2009/140/CE) che all'art. 16-bis comma 4 prevede l'individuazione del CERT Nazionale presso il Ministero dello Sviluppo Economico, con compiti di prevenzione e di supporto a cittadini ed imprese nel fronteggiare incidenti informatici; nel DPCM 24 gennaio 2013, che delineando l'architettura istituzionale per la protezione cibernetica e la sicurezza informatica nazionale, ha affidato al CERT Nazionale la funzione di supporto al Tavolo NISP – Nucleo Interministeriale Situazione e Pianificazione, che agisce come "Tavolo interministeriale di Crisi Cibernetica"; e infine nel DPCM 158 del 2013, che affida all'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione le attività di pertinenza del CERT Nazionale (art. 14).

Le attività

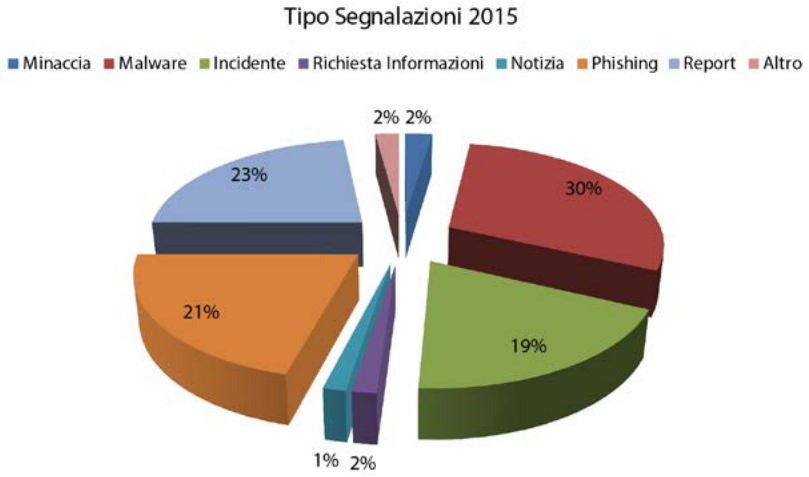
Le attività del CERT Nazionale si svolgono, conseguentemente, secondo diverse direttrici.
A livello internazionale il CERT si interfaccia con gli omologhi CERT Nazionali/Governativi, diventando il punto di contatto a livello Paese.
L'accreditamento presso organismi internazionali riconosciuti è uno dei fattori che ha determinato un significativo incremento delle attività del CERT Nazionale sia nel contesto dello scambio delle informazioni che in quello di gestione della risposta agli incidenti.
A livello europeo il CERT-EU (il CERT delle Istituzioni dell'Unione Europea) svolge un ruolo importante per lo scambio di informazioni con tutti gli altri CERT dell'Unione. Anche i rapporti con il CERT-US sono a livello avanzato e, nell'attività quotidiana, sono già moltissimi i CERT di altre nazioni che sono entrati in contatto con il CERT Nazionale, tipicamente per la richiesta di supporto per la soluzione di incidenti.
A livello nazionale, le interfacce istituzionali sono rappresentate dal CERT-PA (il CERT della Pubblica Amministrazione), il CNAIPIC ed il CERT-Difesa. Il meccanismo di *infosharing* predisposto con questi Enti garantisce che le informazioni fluiscano in maniera efficace ed efficiente per il raggiungimento nei tempi più brevi della soluzione di qualsiasi problema di sicurezza informatica.
I principali interlocutori a livello nazionale, in ambito privato, sono invece le grandi Aziende appartenenti ai principali settori industriali e della finanza, dalle telecomunicazioni, alle

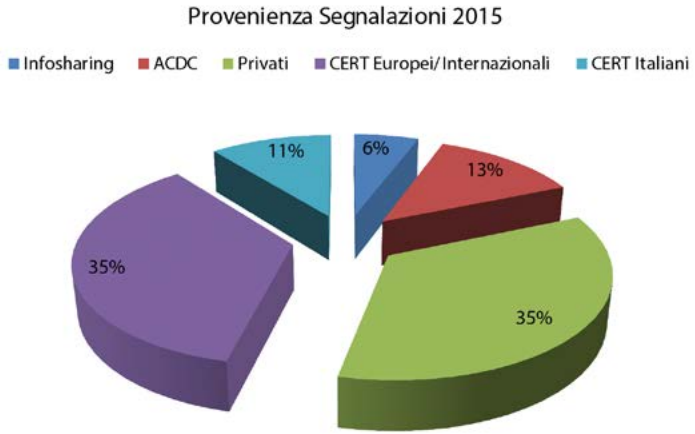
società di servizi, al comparto energetico e dei trasporti fino a quello bancario. Alcune di queste sono entrate a fare parte di un Tavolo Tecnico Permanente per la condivisione diretta delle problematiche riscontrate nelle reti, ma il CERT Nazionale resta aperto per ogni segnalazione da e verso altre entità, dalle piccole e medie imprese, fino ad arrivare al singolo cittadino.

Particolare rilevanza, per la natura dei problemi trattati, sono gli Operatori di telecomunicazioni e gli Internet Service Provider, con i quali si sono instaurati contatti a livello operativo e con i quali c'è uno scambio giornaliero di informazioni.
Allo stato attuale è stato raggiunto dalle segnalazioni del CERT Nazionale un numero considerevole di Operatori ed ISP nazionali, di varia dimensione, corrispondente ad una copertura di più di 490 AS (Sistemi Autonomi) e più di 50 Milioni di indirizzi IP a copertura di circa il 98% del totale di indirizzi afferenti ad AS italiani.

Le segnalazioni

Le attività operative di prevenzione e reazione del CERT Nazionale hanno registrato un incremento esponenziale nel corso dello scorso anno.
Il trend di crescita delle segnalazioni è dovuto, da un lato, all'estensione della rete dei contatti, a livello sia nazionale che internazionale, e dall'altro all'incremento del numero delle fonti di informazione che si traduce in nuovi servizi per gli operatori nazionali.
Nel dettaglio, i dati ricevuti direttamente da omologhi CERT nazionali ed internazionali e quelli desunti dalle nuove fonti di informazioni, tipicamente di tipo semi-aperte, con viste particolari riservate ai CERT nazionali, hanno portato complessivamente all'invio di 3.500 report corrispondenti ad oltre 750.000 eventi segnalati ai circa 375 Operatori/ISP entrati a far parte dei contatti del CERT Nazionale.
Alcuni report sono stati relativi a compromissioni specifiche rilevate e segnalate al CERT Nazionale, in altri casi sono stati relativi a campagne informative principalmente volte a segnalare vulnerabilità di apparati in rete o compromissioni di macchine. Numerosi report fanno riferimento a dati rilevati nell'ambito del progetto europeo ACDC – Advanced Cyber Defence Center.
Tra gli altri servizi offerti dal CERT Nazionale c'è la diffusione di indicatori di compromissione provenienti da omologhi CERT internazionali. Nel corso del 2015 sono stati ricevuti e forniti in modalità *infosharing* oltre 30.000 indicatori di compromissione.
Le due figure seguenti riportano, rispettivamente, la distribuzione percentuale delle diverse tipologie di segnalazioni e della loro provenienza.





Progetti

Un notevole contributo al potenziamento delle attività giornaliere del CERT Nazionale è pervenuto dai dati forniti dalla Rete *Anti-botnet* (www.antibot.it) dell'ex progetto europeo ACDC (*Avanced Cyber Defence Center*).

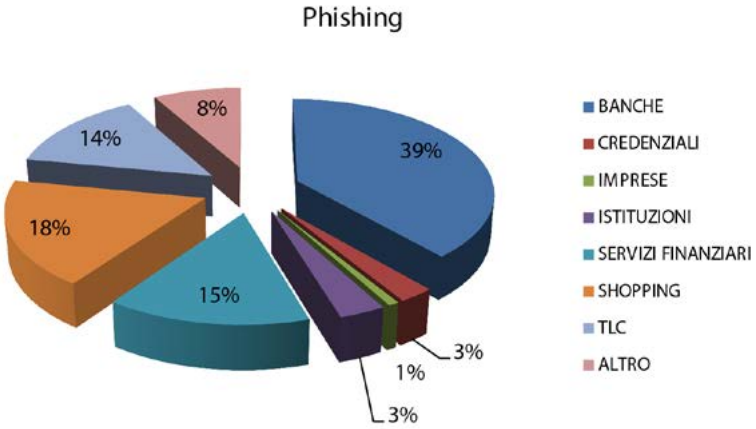
Il CERT Nazionale ha automatizzato la ricezione e l'archiviazione dei dati provenienti da tale piattaforma e provvede, sempre in maniera automatica, ad indirizzare giornalmente gli eventi segnalati agli Operatori ed ISP coinvolti.

L'informatizzazione della procedura d'invio si è resa indispensabile per l'elevato numero di dati resi disponibili dalla piattaforma. Nel corso della seconda parte dell'anno sono stati

inviati, in modalità automatica, oltre 4.000 report a circa 140 Operatori ed ISP differenti. Tra l'altro la rete di *honeypot* predisposta nell'ambito del progetto, continua a raccogliere un notevole numero di eventi (tra tentativi di connessioni malevole e tentativi di scaricamento di *malware*), nell'ordine del milione e mezzo ogni giorno, consentendo anche di avere una ricca base di dati sulla provenienza, a livello mondiale, di determinati tipi di attacco.

Phishing

Uno dei principali vettori di diffusione di *malware* e causa di compromissione di sistemi, sia a livello residenziale che a livello aziendale resta il *phishing*.
Il CERT Nazionale riceve segnalazioni di pagine di *phishing* ospitate su server italiani da diversi interlocutori, principalmente omologhi CERT internazionali o *security vendors*.
Generalmente le segnalazioni arrivano al CERT Nazionale solo dopo tentativi preventivi di contattare gli amministratori o di risolvere in altra maniera l'incidente ed il numero di segnalazioni ricevute rappresentano pertanto una quota estremamente ridotta del fenomeno.
Il grafico seguente riporta la ripartizione dei settori coinvolti, vittime di attacchi di *phishing*, con riferimento alle segnalazioni ricevute nel corso dell'anno. Il settore bancario, unito a quello dei servizi finanziari, è risultato quello per il quale è stato fatto ricorso maggiormente al CERT Nazionale per un rapido intervento.



In generale le segnalazioni ricevute dal CERT Nazionale mostrano come e-mail di *phishing* affiancate, talvolta, a tecniche di *social engineering* sempre più raffinate, rappresentino una delle principali minacce alla sicurezza delle reti. Nel corso dell'anno le segnalazioni ricevute hanno riguardato principalmente la diffusione di *ransomware* nelle sue svariate versioni, in particolare il famigerato *Cryptolocker* e le sue evoluzioni, al quale il CERT Nazionale ha dedicato molto spazio anche all'interno delle *news* pubblicate sul sito istituzionale.

In realtà va considerato il fatto che, mentre il *ransomware*, per sua natura, deve palesarsi una volta colpita la vittima, altre categorie di *malware*, come per esempio gli *stealer* di credenziali e, in particolare, i *banking malware*, hanno invece l'obiettivo opposto di mantenersi il più possibile "nascosti" all'occhio dell'utente, anche esperto. Essendo quindi estremamente più complessa la loro individuazione, il rischio che si corre è quello di sottostimarne la diffusione qualora la valutazione venga basata solo sulle infezioni acclamate.
Da questo punto di vista, il CERT Nazionale cerca di diffondere ed informare gli amministratori delle reti coinvolte, ogniqualvolta venga a conoscenza di macchine verosimilmente infette da qualsiasi tipologia di *malware*, lanciando campagne informative ad-hoc, con l'obiettivo di spingere alla verifica dei sistemi, alla loro eventuale pulizia e protezione.

Le campagne

Una delle attività avviate dal CERT Nazionale è quella di predisporre campagne informative relative a vulnerabilità o compromissioni rilevate in rete.
Le campagne, che si sono tradotte in circa 200.000 segnalazioni nel corso del 2015, hanno lo scopo di supportare le Imprese nella prevenzione degli effetti dello sfruttamento di vulnerabilità rilevate in rete e nella risoluzione di attacchi informatici.
In generale, delle campagne realizzate 7 hanno riguardato la compromissione di siti web, 24 la presenza di vulnerabilità sfruttabili per attività malevole e 10 hanno segnalato l'appartenenza di macchine a botnet di varia natura.
La tabella seguente fornisce un quadro sintetico delle altre campagne di tipo reattivo effettuate **riguardanti diverse tipologie di *botnet*.**

Botnet	Macchine compromesse
Zeroaccess	30.500
Kelihos	11.000
Gozi	8.000
Ponmocup	5.000
Palevo	4.500
Tinba	4.000
Asprox	2.500
Stealrat	2.000
Dyre	2.000
Cutwail	1.500
Slenfbot	~ 900
Lethic	~ 150
Expiro	~ 100

Diverse sono state anche le campagne di tipo "preventivo" effettuate nel corso del 2015.
In particolare alcune campagne hanno riguardato vulnerabilità riscontrate in rete: macchine con servizi "aperti" e potenzialmente utilizzabili per attacchi DDoS o per accessi non autorizzati alle macchine stesse.
Sono state circa 60.000 le segnalazioni inviate nel corso dell'anno, relative a diversi tipi di vulnerabilità. La tabella seguente ne fornisce un quadro sintetico.

Campagna	Numero Macchine Segnalate
Chargen	4090
Elasticsearch	35
IPMI	1.181
Memcached	862
NAT-PMP	15.624
NTP (Monitor)	1500
Portmapper	35.155
QOTD	446
Redis	120

Il sito

Il sito web del CERT Nazionale (https://www.certnazionale.it) si rivolge a cittadini e imprese con notizie di interesse generale legate alla sicurezza informatica, bollettini tecnici e linee guida di comportamento.
L'obiettivo è quello di trattare argomenti tecnici con la necessaria precisione, ma cercando di renderne i contenuti utili e comprensibili anche a chi non necessariamente ha profonde conoscenze tecniche.
Le news, pubblicate con cadenza giornaliera, rappresentano da questo punto di vista un ragionevole compromesso tra una trattazione tecnica specialistica ed una informativa generale relativa alle problematiche di sicurezza del momento. Molte pubblicazioni sono state dedicate al problema del *phishing*, con particolare riferimento alle campagne di *ransomware* di cui si aveva precisa evidenza in determinati periodi.
Oltra a dare elementi tecnici utili, tra i quali precisi indicatori di compromissione o indicazioni di massima sulla prevenzione e soluzione del problema, i testi pubblicati si propongono di descrivere con un linguaggio semplice le azioni opportune, spesso legate al buon senso e non a conoscenze particolarmente approfondite sul tecnicismo della minaccia, per evitare di diventare vittime dei criminali informatici.
Altro spazio è stato dedicato alla diffusione di notizie relative a nuovi tipi di *malware* o tecniche di attacco con particolare riferimento al mondo mobile, che rappresenta sempre più un obiettivo primario degli attacchi.

La visione del CERT-PA

Il CERT-PA, che opera all'interno dell'Agenzia per l'Italia Digitale - Presidenza del Consiglio dei Ministri, è il CERT governativo responsabile della sicurezza della Pubblica Amministrazione. La sua istituzione è relativamente recente (2013), anche se esso deriva dalla lunga esperienza svolta in passato dal CERT-GOV prima e CERT-SPC poi.
Il ruolo e le responsabilità del CERT-PA sono stabilite dal Quadro Strategico Nazionale, documento che esprime e definisce in modo unitario e coordinato le strategie dell'Italia in materia di protezione dello spazio cibernetico nazionale. Il Quadro definisce innanzitutto il CERT-PA come: *"Evoluzione del CERT-SPC con competenza estesa ai sistemi informativi della Pubblica Amministrazione ed ai servizi erogati per il loro tramite, oltre che alla rete di interconnessione. Esso ha il compito di supportare e coordinare la PA nella prevenzione, risposta e rientro dagli incidenti."*. Il quinto degli undici Indirizzi Operativi previsti dal Quadro Strategico prevede: *"Sviluppo e piena operatività del CERT-PA, quale evoluzione del CERT-SPC previsto dal DPCM recante regole tecniche e di sicurezza SPC dell'1 aprile 2008. Il CERT-PA è il punto di riferimento delle pubbliche amministrazioni attivando l'escalation verso il CERT Nazionale secondo modelli e procedure unitarie. Esso collabora con i CERT della pubblica amministrazione a livello europeo ed internazionale, attraverso scambi informativi e procedure concordate."*

Lo stesso Quadro Strategico definisce inoltre i rapporti tra AgID e CERT-PA, stabilendo che l'Agenzia: *"opera il CERT-SPC, CERT del Sistema Pubblico di Connettività, attuandone la trasformazione in CERT-PA, CERT della Pubblica Amministrazione, che garantisce la sicurezza cibernetica dei sistemi informativi della P.A., oltre che della loro rete di interconnessione, provvedendo al coordinamento delle strutture di gestione della sicurezza ICT - ULS, SOC e CERT, operanti negli ambiti di competenza. Il CERT-PA coopera con il CERT Nazionale e con il CERT Difesa per il raggiungimento degli obiettivi di sicurezza nazionale;"*.
Queste linee di indirizzo vengono meglio declinate nel Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica, documento che sviluppa le linee attuative di dettaglio dei principi espressi nel Quadro Strategico. Il quinto indirizzo operativo (*"Operatività del CERT Nazionale, del CERT-PA e dei CERT dicasteriali"*) prevede quindi che lo sviluppo del CERT-PA e dei CERT dicasteriali debba svolgersi secondo le seguenti direttrici:

a) Integrare la struttura del CERT-SPC trasformandola nel CERT-PA, individuando le risorse umane necessarie ed attivando opportune procedure di reperimento del personale, nonché adeguando le infrastrutture tecniche, strumentali e logistiche, per garantire la sua piena operatività.
b) Stabilire il sistema di cooperazione delle strutture di gestione della sicurezza ICT della PA, in particolare Unità Locali di Sicurezza (ULS) e Security Operations Center (SOC), promuovendone, ove possibile, la trasformazione in CERT dicasteriali.
c) Favorire la creazione di CERT Regionali con il compito di supportare le Pubbliche

Amministrazioni Locali (PAL) del territorio e di implementare regole e modelli organizzativi nazionali.

d) Adottare le procedure definite dall'Agenzia per l'Italia Digitale (AgID).
e) Perseguire uniformi livelli di sicurezza dei Data Center e degli ambienti di lavoro delle Amministrazioni e dei gestori delle infrastrutture critiche nazionali.

Le PP.AA. che istituzionalmente il CERT-PA è chiamato a gestire direttamente sono le PAC, le regioni e le città metropolitane. Le PAL vengono raggiunte per il tramite i CERT locali, operanti in un'area circoscritta (e.g. un insieme di regioni), o settoriali, che gestiscono un insieme di strutture di tipo omogeneo (e.g. presidi sanitari).

La storia

Il progetto di trasformazione del CERT-SPC nel CERT-PA è stato avviato all'inizio del 2013 ed ha individuato essenzialmente tre fasi: Pilota, Costituzione ed Operazione. La prima, che avrebbe dovuto protrarsi fino alla fine del 2015, aveva lo scopo di mettere a punto, operando con un insieme ristretto di amministrazioni con particolari competenze nel settore della sicurezza cibernetica, il modello definito nel progetto, verificando e consolidando gli strumenti e le procedure operative.

L'avvio della fase Pilota è avvenuto a dicembre del 2013 con una *constituency* formata da MAECI, MEF, MISE, Min Giustizia, Consip e, ovviamente, AgID. Nel febbraio successivo è stato attivato il presidio, con i canali di allertamento costituiti da mail, telefono e fax. A giugno la costituzione del CERT è divenuta ufficiale anche a livello europeo con la registrazione da parte di ENISA.

Nel corso della fase Pilota sono state messe a punto le procedure operative ed attivati i rapporti ed i canali di comunicazione con i CERT Nazionale, Difesa e GARR. Contemporaneamente la *constituency* si è allargata per comprendere i CERT di INAIL e Regione Friuli Venezia Giulia, nonché il CSI Piemonte.

Attivati i servizi essenziali di predisposizione alla risposta (*Early-Warning*) e di gestione degli eventi ed avendo realizzato, almeno al livello minimo, l'infrastruttura necessaria, prima dell'estate 2015, con più di sei mesi di anticipo sulla previsione iniziale, la fase pilota si è conclusa e tutte le pubbliche amministrazioni centrali, le 20 regioni e le 8 città metropolitane che formano la *constituency* istituzionale sono state invitate a procedere all'accreditamento. È così iniziata la fase di Costituzione che a novembre ha visto l'ingresso ufficiale del CERT-PA nella lista ufficiale di Trusted Introducer.

Completato il consolidamento della *constituency* e l'avviamento dei servizi con quelli avanzati si entrerà nella terza fase nella quale si attiveranno le forme di accreditamento avanzate e verrà completata la copertura territoriale con la rete di strutture locali.

I servizi

Il CERT-PA eroga verso la propria *constituency* servizi che, dove applicabili, sono resi disponibili, in modalità *best-effort*, a tutta la Pubblica Amministrazione. Ciò avviene attraverso un'infrastruttura dedicata che, oltre al sistema informativo di supporto alle attività interne,

attualmente vede tre componenti principali visibili dall'esterno:

- **Piattaforma di info-sharing**
  un portale dedicato che costituisce uno strumento di collaborazione non solo per la *constituency*, ma anche per le strutture di sicurezza con le quali il CERT-PA coopera (e.g. NSC, CERT Nazionale, CERT-GARR, SOC di provider della PA). Attraverso di essa vengono diffusi i Bollettini e gli Avvisi, nonché resa disponibile la Rubrica, che contiene i riferimenti costantemente aggiornati delle strutture di sicurezza accreditate. Tale infrastruttura ha reso possibile lo scambio rapido e protetto di informazioni e materiale durante la gestione dei principali incidenti occorsi nel 2015.
- **Sistema di posta elettronica**
  accoglie la casella di posta di allertamento, nonché quelle del personale operante nella struttura, in modo da garantire, anche sotto il profilo della riservatezza, le comunicazioni interne.
- **Sito web istituzionale**
  contrariamente alla piattaforma di info-sharing è pubblico e rende disponibili a chiunque le informazioni non riservate prodotte dal CERT-PA.

L'insieme dei servizi erogati costituisce complessivamente il Processo di Incident Response della Pubblica Amministrazione (IRPA), il quale, spaziando dalla prevenzione al ripristino, copre virtualmente tutte le attività del CERT e può essere visualmente rappresentato come nella Figura 1.

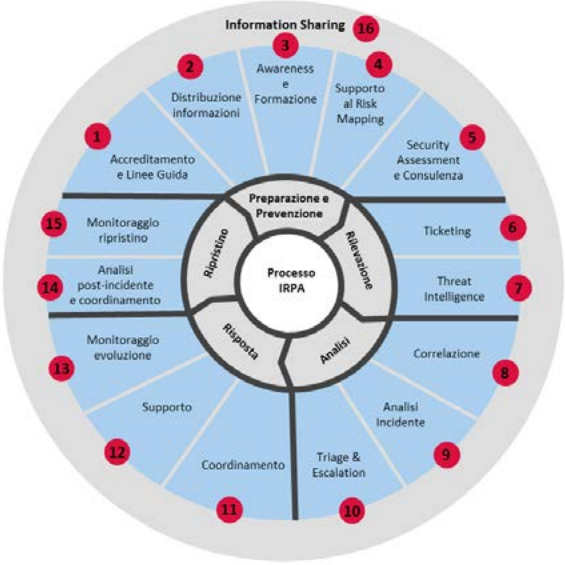


Figura 1 – Il Processo Incident Response della PA

Ad oggi i servizi su cui è focalizzata l'attenzione sono quelli essenziali di *Early-Warning* e la risposta agli incidenti. Di conseguenza quelli la cui implementazione è più avanzata sono, oltre all'**Accreditamento [1]** ed all'**Info-sharing [16]**, che costituiscono un prerequisito:

- **Ticketing [6]**
- **Distribuzione informazioni [2]**
- **Threat intelligence [7]**
- **Analisi incidente [9]**
- **Triage & Escalation [10]**
- **Correlazione [8]**
- **Supporto (alla risposta) [12]**
- **Coordinamento (della risposta) [11]**
- **Security Assessment e Consulenza [5]**

I rimanenti sono attualmente in fase di implementazione, ma anche quelli già operativi debbono essere ulteriormente sviluppati. A titolo di esempio citiamo l'Accreditamento, che oggi vede realizzato solo il primo dei tre livelli in cui è previsto articolarsi.

L'attività

L'operazione del CERT-PA può essere descritta, per la sua parte essenziale, come nella Figura 2. Il processo è avviato dall'apertura di un ticket, evento che viene causato dall'arrivo di una segnalazione su uno dei canali di allertamento, essenzialmente mail, telefono e fax, ovvero dalla rilevazione di un evento significativo nel corso dell'attività di monitoraggio delle fonti chiuse ed aperte che viene condotta costantemente.

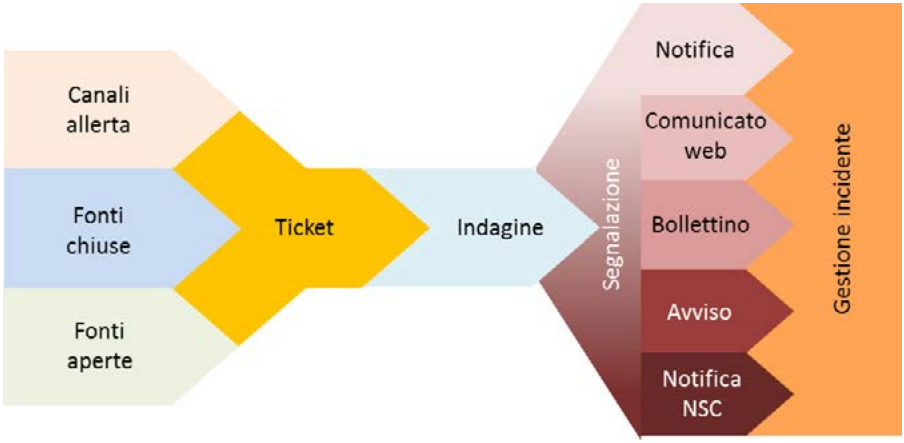


Figura 2 – Operazione del CERT-PA

All'apertura del ticket segue l'avvio di una fase di analisi, detta Indagine, durante la quale viene verificata la consistenza dell'evento e raccolta la maggiore quantità possibile di informazioni al suo riguardo al fine di determinare il tipo di azioni che debbono essere intraprese. Questa fase comprende anche l'analisi del codice e del comportamento del malware, quando questo è disponibile.
Nel caso più elementare, quando l'evento riguarda un soggetto specifico, viene prodotta una notifica, generalmente un messaggio di posta elettronica, che lo segnala all'interessato, fornendo, se del caso, indicazioni riguardo la sua gestione e offrendo supporto tecnico.
Se viceversa si tratta di eventi la cui portata è più ampia o travalica i confini di competenza (e.g. coinvolge privati) vengono emesse uno o più segnalazioni delle seguenti tipologie:

- Notifiche verso altre strutture di cybersec, quali altri CERT, ed in particolare verso il CERT Nazionale.
- Comunicati sul sito web per rendere noto l'evento al pubblico se l'impatto può essere generalizzato.
- Bollettini di contenuto tecnico, destinati principalmente alle strutture di sicurezza della *constituency*; tuttavia, trattandosi di documenti che non presentano profili di riservatezza, questi sono resi disponibili anche sul sito web a tutti gli utenti che hanno provveduto a registrarsi.
- Avvisi inviati in modo riservato ai responsabili della sicurezza delle strutture potenzialmente interessate, quando le informazioni contenute presentano profili di criticità.
- Notifiche verso NSC, quando l'ambito di interesse per l'evento comprende anche le strutture di sicurezza cibernetica nazionale.

È evidente che l'attività appena descritta è ben diversa dalla raccolta e diramazione di segnalazioni provenienti da altre fonti e richiede un notevole attività che in larga misura non può essere automatizzata. Ciò è particolarmente vero quando all'emissione della segnalazione segue la fase di gestione dell'incidente, durante la quale ne vengono verificati estensione ed impatto, supportando l'adozione delle più idonee misure di risposta e contenimento.
La tabella seguente offre un consuntivo quantitativo trimestrale delle attività appena descritte.

Trimestre	Ticket	Indagini	Bollettini	Avvisi	NSC	VA
2014 - 3	27	25	10	3		
2014 - 4	41	18	6	5		1
2015 - 1	76	33	11	6	3	1
2015 - 2	82	34	8	4	6	3
2015 - 3	83	14	11	2	1	1
2015 - 4	100	16	1	5	3	

L'ultima colonna della tabella fa riferimento all'attività di Vulnerability Assessment, che costituisce la porzione già attivata del servizio 5 - Security Assessment e Consulenza.

La minaccia per la PA

Il ruolo del CERT-PA è ovviamente di importanza strategica per garantire che il percorso di evoluzione tecnologica delle Pubbliche Amministrazioni e di digitalizzazione dei servizi da esse erogati si svolga sia prevenendo e minimizzando i rischi di sicurezza, che intervenendo tempestivamente in caso di incidenti. Si tratta tuttavia di un compito non facile, dato che la situazione generale della Pubblica Amministrazione italiana dal punto di vista della sicurezza informatica è purtroppo lungi dall'essere soddisfacente.

Lo studio svolto nel 2014 dal CIS - Sapienza su "Consapevolezza della minaccia e capacità difensiva della Pubblica Amministrazione Italiana" evidenzia ad esempio l'esistenza di lacune importanti sia in termini di cultura della sicurezza che di organizzazione, con conseguente mancata adozione da parte di moltissime Amministrazioni anche dei principi più basilari di protezione e prevenzione. Ciò si deve in larga parte alla generalizzata ignoranza o sottostima da parte delle Amministrazioni del valore strategico ed economico delle informazioni da esse trattate, che, unita alla strutturale attenzione nella spesa, porta a lesinare gli investimenti in sicurezza dirottandoli invece verso aree ritenute maggiormente produttive. La sicurezza inoltre è ancora percepita da molte Amministrazioni come una questione essenzialmente tecnologica, mentre sfugge quasi sempre la sua dimensione organizzativa e di processo, che è invece quella realmente critica, legata al concetto di *gestione del rischio* e di *governance*.

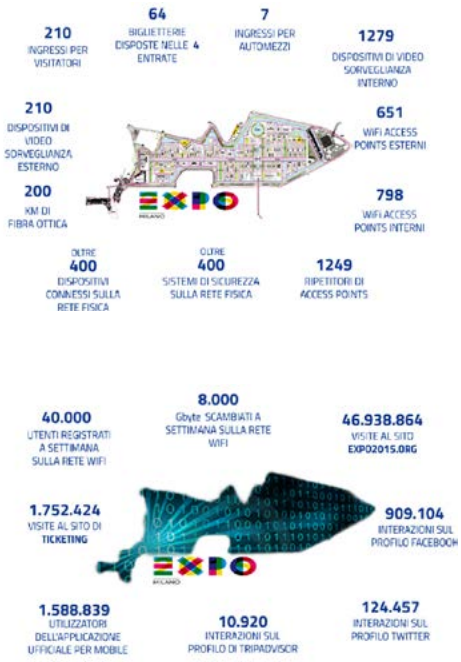
Naturalmente nel panorama evidenziato dallo studio si è riscontrata una grande variabilità di situazioni, dato che le realtà analizzate andavano dalle grandi Amministrazioni centrali alle piccole Amministrazioni locali. In generale, come prevedibile, le strutture più grandi e complesse si sono rivelate anche quelle più consapevoli dei rischi e maggiormente attente alla prevenzione, mentre le strutture più piccole e decentrate hanno confermato di essere quelle meno preparate anche e soprattutto in termini di percezione del rischio. Globalmente, comunque, la capacità difensiva del sistema si è rivelata strettamente legata alla tecnologia e quindi difficilmente in grado di fronteggiare gli attacchi che fanno leva principalmente sul fattore umano (e.g. *phishing*), che oggi rappresentano una parte sempre più consistente e pericolosa.

Di contro la tendenza globale è caratterizzata da un incremento sempre più importante del livello di minaccia, sia in termini quantitativi che qualitativi. Occorre dunque moltiplicare gli sforzi in difesa e prevenzione per limitare al più possibile i rischi di incidenti che potrebbero avere conseguenze anche rilevanti non solo per le Amministrazioni in sé ma anche e soprattutto per i cittadini e per l'intero Paese. La crescente diffusione degli APT costituisce naturalmente un pericolo specifico per la Pubblica Amministrazione, ma oramai anche minacce aspecifiche quali i *ransomware* non sono più trascurabili nel panorama dei rischi da ritenersi all'ordine del giorno.

Per contribuire a migliorare la situazione il CERT-PA sta portando avanti anche un'attività di informazione e sensibilizzazione, che si rivolge da un lato alla propria *constituency* mediante i servizi di *info-sharing* erogati tramite il portale riservato, ma dall'altro indirizza tutti i potenziali interessati, anche non appartenenti alla Pubblica Amministrazione, mediante i bollettini informativi diffusi sul proprio Web pubblico. A tal proposito, per raggiungere rapidamente un bacino sempre più ampio di utenti finali, è in fase di attivazione anche un profilo Twitter che verrà utilizzato per veicolare sia brevi notizie informative che segnalazioni urgenti.

Speciale Expo Milano 2015

L'Esposizione Universale Expo Milano 2015 ha rappresentato un momento di scambio ed aggregazione per eccellenza tra culture differenti ed il più grande evento mai realizzato su tematiche connesse alla nutrizione e all'alimentazione sostenibile.



Durante il semestre Maggio – Ottobre 2015, in un'area progettata e allestita ad hoc di **1,1 milioni di metri quadri**, **148 paesi** e organizzazioni internazionali hanno condiviso il meglio delle proprie tecnologie per fornire una risposta concreta a un'esigenza vitale: riuscire a garantire cibo sano, sicuro e sufficiente per tutti i popoli, nel rispetto del pianeta e dei suoi equilibri.
L'evento passerà alla storia anche per essere stato pensato come un modello di Digital Smart City: circa **21 milioni** di visitatori in **6 mesi**, con picchi di **100mila visitatori connessi al giorno**, hanno vissuto l'esperienza di vivere in una città intelligente in cui la tecnologia, pervasiva ma allo stesso tempo invisibile, ha costituito l'anima di tutta la manifestazione e la piattaforma in grado di abilitare ogni tipo di infrastruttura e di servizio.

A questi si sono affiancati i milioni di visitatori online che hanno acceduto ogni giorno ai più disparati servizi digitali dell'esposizione universale - quale ad esempio la vendita di biglietti - attraverso le più eterogenee tecnologie, come portali web, applicazioni mobili, beacon, piattaforme di merchandising e ticketing.
Le complessità a cui dover far fronte erano molteplici. L'accoglienza e la gestione di **250mila visitatori presenti simultaneamente** sul sito espositivo, il transito notturno di 500 mezzi per l'approvvigionamento e il trasporto dei rifiuti e le particolari esigenze di gestione e di intrattenimento presentate dai paesi partecipanti per i progetti dei propri padiglioni, in un contesto di livello di attenzione internazionale elevato. Il tutto con la finalità principale di garantire la migliore esperienza possibile ai visitatori e la completa sicurezza di persone e

cose. I grandi eventi sono infatti, per definizione, anche grandi contenitori di rischi: quante più sono le persone coinvolte nell'evento e quanto maggiore è la durata, tanto più la gestione della sicurezza - in tutte le sue accezioni - assume un ruolo centrale nell'organizzazione. Un evento di tale portata ha rappresentato uno stimolo molto forte per i cyber criminali che, attraverso azioni illecite, hanno agito non solo per perseguire vantaggi economici ma anche per ledere l'immagine e la reputazione dell'evento e del paese ospitante - l'Italia.

In tale scenario, gli aspetti di sicurezza delle informazioni sono stati oggetto di accurata progettazione e gestione da parte dell'organizzazione di Expo2015. Per questo motivo, in questo Rapporto CLUSIT abbiamo ritenuto utile e interessante condividere l'esperienza di tre attori che hanno svolto un ruolo fondamentale per garantire il successo della manifestazione, nonostante essa sia stata bersaglio dell'attenzione dei cybercriminali:

- **Cisco Systems**, selezionata come *IP Network and Solutions Partner*, che ha avuto il compito di fornire una rete pervasiva, affidabile ed efficace dal punto di vista energetico, ma con un'attenzione assoluta al tema della sicurezza. Il successo della protezione dell'evento da tentativi di intrusione e blocco di servizio, rendono l'esperienza sulle architetture e sui processi progettati e realizzati un riferimento da cui trarre molteplici spunti in termini di approccio e tecnologia.
- **Poste Italiane**, in qualità di *Official Information Security Intelligence Partner*, che tramite il proprio CERT ha erogato servizi di sicurezza di intelligence e prevenzione proattiva di minacce cibernetiche**,** facendo leva su 25 specialisti in ambito cyber security, su tecnologie di sicurezza avanzate e sulla rete di collaborazioni nazionali ed internazionali per lo scambio d'informazioni (c.d. Information Sharing). Tali attività sono state condotte presso l'unità C3, denominata **Centro di Coordinamento e Controllo** di EXPO.
- Il **C.N.A.I.P.I.C.** (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche, nucleo speciale in seno alla **Polizia Postale**), incaricato della prevenzione e della repressione dei crimini informatici che hanno per obiettivo le infrastrutture informatizzate di natura critica e di rilevanza nazionale.

Leggerete in questo "speciale" del Rapporto come è stata disegnata e realizzata l'infrastruttura tecnologica e di protezione di Expo, quali straordinari numeri è stata in grado di gestire, come questa è stata governata dall'ente organizzatore e quali eventi di sicurezza ha registrato. Scoprirete come sia fondamentale proteggere ma anche prevenire, mediante differenti approcci di intelligence, gli eventi di sicurezza, sia a carico dell'infrastruttura interna, che dei servizi ai visitatori e per la protezione dei visitatori stessi prima, durante e dopo la visita. Perché Expo è stata prima di tutto l'offerta di un'esperienza, che solo un notevole sforzo di prevenzione, contrasto e gestione ha impedito che si trasformasse in un palcoscenico mediatico per i numerosi attacchi che sono stati indirizzati contro l'evento e l'immagine del nostro Paese.

(*P. Giudice, segretario generale Clusit*)

La sicurezza dell'infrastruttura [a cura di Cisco Systems]

I numeri dell'evento e i servizi da proteggere

La rete di EXPO 2015 si è sviluppata su **360Km di fibra** installata sul sito, **45 nodi** di distribuzione e **1100 switch** di accesso - per un totale di circa **30mila porte IP**, rendendo l'evento la prima manifestazione mondiale completamente full IP a disposizione dei visitatori, dello staff dell'organizzazione, dei paesi partecipanti e di tutti i partner che hanno abilitato i propri servizi.
Per garantire la connettività mobile su tutta l'area espositiva di circa un chilometro quadrato è stata realizzata un'infrastruttura WiFi con **2700 Access Point**. La rete wireless ha permesso l'**accesso a internet gratuito a chiunque** e in ogni punto di Expo, sia outdoor che all'interno di padiglioni e aree servizio, gestendo picchi di circa **103mila connessioni**, con un traffico totale giornaliero di circa **3 TeraByte**. Allo stesso tempo, tale infrastruttura ha dovuto permettere la connessione efficace e sicura di dispositivi mobili dello staff (dispositivi di comunicazione video, di programmazione attività e segnalazione problemi, …), di sensori e sistemi di intrattenimento applicativo e multimediale, fornendo informazioni preziose di analisi di comportamento, dati di presenza e localizzazione.
La tecnologia digitale è stata ovviamente sfruttata soprattutto per informare, intrattenere e coinvolgere i visitatori e ha costituito l'elemento portante del progetto di Digital Expo. Oltre alle applicazioni ufficiali dell'organizzatore e dei singoli padiglioni, i **100 totem** e i **25 e-wall** distribuiti lungo il sito espositivo e le applicazioni multimediali e di realtà aumentata dei padiglioni hanno consentito ai visitatori un'esperienza unica con un alto livello di coinvolgimento e di informazione su servizi, contenuti ed eventi.
Non solo: tra i vari servizi, è importante sottolinearlo, vanno citati anche tutti gli strumenti per garantire la protezione fisica di persone e cose come le migliaia di telecamere di videosorveglianza, i sistemi di controllo degli accessi dei visitatori con lettore QR code, i dispositivi di rilevamento di eventuali incendi o intrusioni non autorizzate, oltre che i sensori per i parametri di consumo energetico e di ambiente, solo per fare degli esempi.

Considerando il ruolo della rete e delle soluzioni applicative e di sistema da essa abilitate, per Cisco il tema della sicurezza ha necessariamente assunto un grado di attenzione prioritario nella progettazione dei servizi per il sito espositivo e durante la manifestazione. Il successo della protezione dell'evento da tentativi di intrusione e blocco di servizio fa delle architetture e dei processi progettati per l'evento un modello di riferimento da seguire, in termini di approccio e tecnologia.
I servizi applicativi legati all'operatività interna dell'area di Expo sono stati erogati in modalità *private cloud* da una coppia di Data Center operanti in una logica di alta affidabilità; essi hanno ospitato, oltre alle componenti di elaborazione e virtualizzazione, i principali nodi core e di sicurezza dell'infrastruttura di sito e di accesso verso le connessioni esterne. Il governo totale della Smart City di Expo, della sua sicurezza fisica ed informatica, dei Data

Center e dei processi afferenti ai servizi di rete e tecnologici, è stato in capo alla **Centrale di Comando e Controllo (EC3)** che ha avuto il compito di monitorare, controllare e gestire la totalità di sistemi ed eventi in assoluta continuità e disponibilità.

L'approccio alla Sicurezza IT [1]

Expo Milano 2015 non si è svolta in uno dei momenti più sereni della storia recente. Lungo tutti i sei mesi della sua durata, l'evento ha costituito, per la sua importanza e per la grande partecipazione internazionale, un obiettivo particolarmente sensibile, a rischio di atti dimostrativi o di boicottaggio. Il successo di un potenziale attacco avrebbe potuto mettere in discussione la vita stessa dell'esposizione universale, per esempio impedendo l'apertura dei tornelli, alterando il funzionamento dei sistemi di sicurezza fisica, bloccando le attrazioni multimediali e gli strumenti di governo dei padiglioni, rendendo inefficace il controllo dalla centrale operativa, con un danno pesantissimo per l'evento e per la reputazione dell'organizzatore e dei paesi partecipanti. Permettere lo svolgimento e il successo stesso di una manifestazione universale di tale portata e visibilità implicava adottare misure di sicurezza di livello adeguato.

È stato dunque necessario progettare e attivare un'architettura di sicurezza pervasiva e multilivello e una task force dedicata al monitoraggio dell'intera infrastruttura per garantire agli organizzatori di dedicarsi agli aspetti operativi e di contare sull'incolumità dell'esposizione.

Il progetto di sicurezza IT per Expo2015 ha definito degli imperativi strategici su cui basare lo sviluppo dell'architettura di protezione.

Prima di tutto la **visibilità,** ovvero la possibilità di esercitare il controllo totale e in tempo reale dell'accesso alla rete e di garantire un'elevata capacità di riconoscimento di traffici sospetti, potenzialmente associati a dinamiche di attacco o furto di informazione. Con la garanzia totale del rispetto della privacy degli utenti e della riservatezza del traffico generato dalle centinaia di migliaia di dispositivi collegati quotidianamente alla rete, era assolutamente necessario poter riconoscere qualsiasi comportamento anomalo e risalire immediatamente al client sorgente o bersaglio di un attacco. In tal senso, la rete e tutte le sue componenti, non solo i sistemi di sicurezza ma gli stessi router, switch e dispositivi di accesso wireless, hanno costituito un'architettura integrata di "**rete come sensore**", capace di centralizzare tutte le informazioni di monitoraggio e analitica presso le applicazioni di gestione e correlazione.

In secondo luogo la **focalizzazione sulla continua evoluzione delle minacce,** per un aggiornamento continuo delle innumerevoli e mutevoli tipologie di intrusione e attacco che sarebbero state create ogni giorno nel mondo e che la rete in Expo doveva rilevare e bloccare. In ultimo un **approccio basato sull'utilizzo di piattaforme Firewall di nuova generazione flessibili e modulari** da poter distribuire sull'intero sito con pari ricchezza di funzionalità (IPS, Application Control, Anti-Malware), ma ampia scelta di scalabilità e performance. In tal senso bisogna pensare che il sito espositivo ha rappresentato una vera

[1] Per ogni dettaglio maggiore sul progetto è possibile consultare i contenuti al seguente link http://www.abcisco.it/expo2015

e propria città di servizi intelligenti cui i singoli padiglioni si sono integrati connettendo le proprie reti locali; era dunque necessario prevedere piattaforme complete (in termini di funzionalità di sicurezza) che allo stesso tempo si potessero adattare alle performance e alle capacità di investimento dei singoli paesi: per fare un'analogia, ciò è quanto può succedere in qualsiasi realtà aziendale con molteplici sedi distribuite collegate fra di loro per l'accesso ai servizi centralizzati. Ogni punto di integrazione è un punto che richiede un'attenzione di controllo particolare, a maggior ragione quando la singola sede sfrutta un collegamento alla rete pubblica internet dedicato, come succedeva per i padiglioni nel sito espositivo, in cui era opportuno poter prevedere componenti di prestazione e costo adeguati alle singole esigenze, avendo a che fare con padiglioni da 10 a centinaia di persone di staff.

Sulla base di questi tre imperativi strategici, il progetto di sicurezza per Expo2015 si è tradotto nella costruzione di un'architettura integrata di componenti distribuite e sistemi di gestione centralizzati che possiamo raggruppare secondo tre funzioni principali: la **prevenzione**, il **rilevamento dell'attacco** e **l'azione di rimedio** in caso di attacco.

Nell'ambito della **prevenzione** era necessario poter avere l'assoluto controllo e la piena conoscenza della rete, dei suoi utenti, delle sue applicazioni e della storia del suo comportamento. Per permettere esclusivamente le dinamiche di traffico autorizzate e per avere visibilità delle applicazioni utilizzate, sono stati distribuiti in posizioni chiave sul sito espositivo più di cento dispositivi firewall con capacità di Anti-Malware Protection avanzato, IPS e Application Control. Tali nodi di sicurezza, oltre a proteggere le direttrici principali da e per i Data Center di sito (con prestazioni fino a 40Gbps di analisi in tempo reale) hanno protetto i singoli padiglioni, che potevano beneficiare di connettività pubbliche dirette con tutta la tranquillità di una protezione dedicata, anche nei confronti di altri padiglioni (considerati in ogni caso realtà esterne e in alcuni casi addirittura di antagonismo politico).
Considerando poi i 100mila visitatori connessi in wireless e le centinaia di migliaia di dispositivi della Smart City, con un'elevata molteplicità di requisiti diversi in termini di diritti di accesso ai servizi, era necessario predisporre un sistema affidabile per prevenire qualsiasi connessione non permessa. L'inserimento all'interno dell'architettura integrata di un sistema di Network Admission Control (NAC) in colloquio diretto con le componenti di networking, ha reso disponibile:

- il controllo accessi alla rete (con user e password o certificati) in ogni momento ed in ogni luogo sul sito espositivo, impedendo i tentativi di accesso non permessi;
- un policy manager centralizzato, con il governo delle configurazioni automatiche della rete basate su autenticazione e caratteristiche dei dispositivi (tipologia, sistema operativo, stato di protezione applicativa);
- un livello di accesso all'infrastruttura wired e wireless totalmente slegato da configurazioni specifiche dei singoli apparati (Switch e Access Point) e al tempo stesso slegato da comportamenti diversi da parte degli utenti a seconda del luogo e della tipologia di connessione in fase di autenticazione;

- attività di installazione iniziale, di gestione e change/management di tutti gli apparati in modo rapido ed efficace.

Anche per l'esposizione universale, così come consigliabile a qualsiasi realtà, **un approccio esclusivamente preventivo sarebbe stato totalmente inefficace** a proteggere client, sistemi applicativi e di rete dalla nuova frontiera di minacce che caratterizzano lo scenario globale odierno delle problematiche di cyber security. Pertanto sono state attivate le funzionalità di analisi del traffico per rilevare traffico malevolo noto sui firewall distribuiti, integrando le stesse sonde del sito espositivo in un *Cloud Security Intelligence* mondiale. Il Cloud Security Intelligence integra informazioni di attacco, di file malware, di sorgenti di attacco e molto altro ancora con le informazioni condivise da milioni di sonde e dispositivi, oltre che da centri specializzati nell'analisi del traffico Internet. La potenza della condivisione di queste informazioni globali ha consentito ai sistemi installati presso Expo di riconoscere nuovi file o dinamiche di traffico classificati quotidianamente dall'intelligence come una nuova minaccia da bloccare nell'ambito degli APT (Advanced Persistent Threats). Per avere idea del trend di comparsa nella rete globale di nuovi malware durante l'evento si prendano in considerazione i dati di Figura 1:

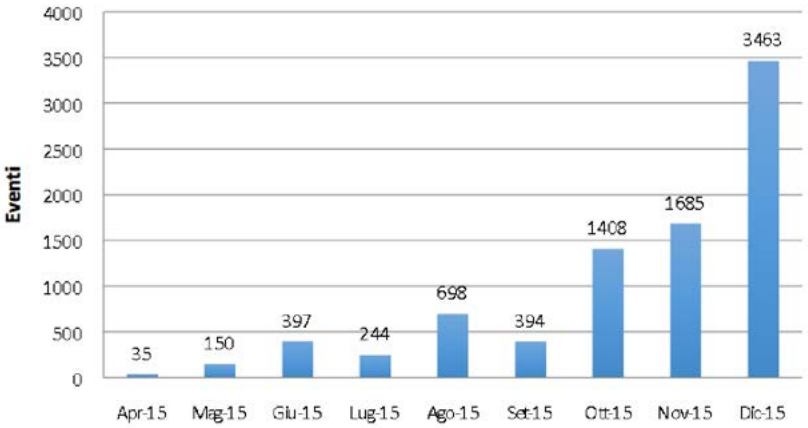


Figura 1 - Eventi Malware individuati prima dei servizi di reputazione di riferimento (Dati Cisco)

Il grafico riporta da marzo a dicembre 2015 i dati di rilevamento di nuove tipologie di malware "advanced" da parte del Cloud intelligence di Cisco a supporto di Expo, non noti ai principali servizi di reputazione di riferimento.

Senza un servizio di un Cloud Intelligence sarebbe stato impossibile impedire l'ingresso nella rete di Expo di malware nuovi che giornalmente nascevano in Internet, in particolare

considerando l'impossibilità da parte di Expo di limitare applicazioni e comportamenti di accesso alla rete pubblica da parte dei paesi partecipanti. Tutto questo con un grave rischio per la rete e per tutti i servizi essenziali ad essa appoggiati.

Se prevenzione ed efficacia nel rilevamento sono state le funzioni chiave dell'architettura di sicurezza per Expo, per consentire azioni efficaci e repentine al verificarsi di eventi malevoli era altrettanto importante assicurare il controllo, la correlazione e la visibilità degli eventi in rete, compito affidato alla Centrale di Comando e Controllo della manifestazione. Qui è stato costituito un Security Operation Center, necessario per l'importanza, le dimensioni e la durata della manifestazione, le cui decisioni sono state indirizzate dalla correlazione degli eventi provenienti dai differenti sistemi di gestione dei servizi.

Figura 2 - Expo EC3 (Expo2015 Centrale di Comando e Controllo)

A tal proposito si son dimostrati indispensabili gli strumenti di gestione centralizzata di tutte le componenti firewall, IPS e Anti-Malware protection, che hanno garantito una vista costante e in tempo reale degli eventi in rete; tramite suggerimenti automatici del sistema, con presentazione dei dati secondo diversi ordini di gravità, tali strumenti hanno reso possibile concentrarsi sugli eventi rilevanti, pianificare azioni correttive puntuali su client o dispositivi di sicurezza ove prioritario, sfruttando in maniera efficace il tempo operativo. La classificazione degli eventi veniva infatti aggiornata evidenziando il **livello di impatto** delle problematiche rispetto a quanto altamente rilevante in quel momento per l'evento, sulla base di una configurazione iniziale effettuata dagli esperti del sistema.

I risultati e gli strumenti a disposizione del SOC

L'architettura progettata e realizzata per Expo2015 ha permesso di **rilevare e bloccare**

durante i sei mesi dell'evento più di mezzo milione di tentativi di intrusione provenienti da tutto il mondo, senza contare gli oltre **10mila tentativi di presa di controllo di applicazioni e apparati**. È curioso considerare che quanto più aumentava il successo della manifestazione e il numero di visitatori, tanto più incrementava il livello di attenzione verso l'esposizione e quindi la diffusione di tentativi di intrusione, come riportato in Figura 3.

Come dimostrano i grafici statistici e informativi, condivisi a titolo di esempio in questo documento, gli strumenti di correlazione, gestione e presentazione di informazione centrali hanno rappresentato un elemento chiave dell'architettura. I risultati che questi strumenti sono stati in grado di produrre hanno oggi un valore di riferimento importante, riportando uno specchio delle minacce tipiche di questi tempi. È sicuramente interessante consultarli perché da questi si evince ad esempio che gran parte dell'attività malevole ha riguardato l'utilizzo del servizio DNS (Domain Name Server), utilizzato da tutti noi inconsciamente ogni volta che digitiamo un indirizzo internet per permettere al browser di raggiungere il server internet interessato, ma spesso sfruttato per farci cadere su pagine internet che non desideriamo, per carpire dati e informazioni o ancora per ridirigere determinate tipologie di traffico. Queste informazioni hanno aiutato Expo a capire quanto fosse essenziale imporre l'utilizzo di DNS sicuri da parte dell'utenza.

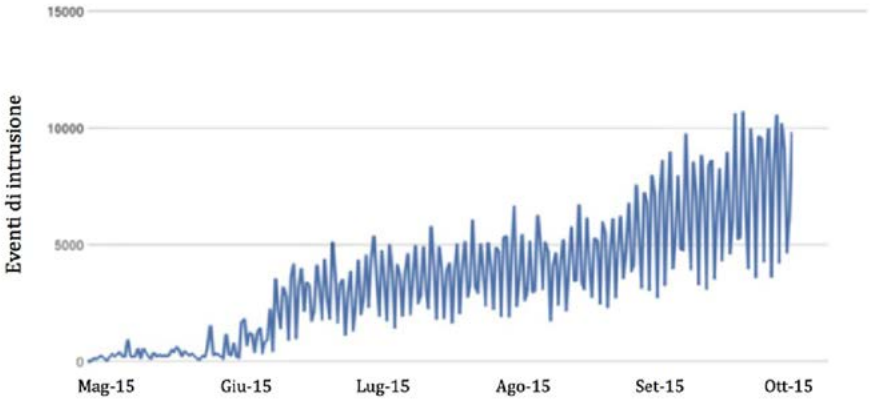
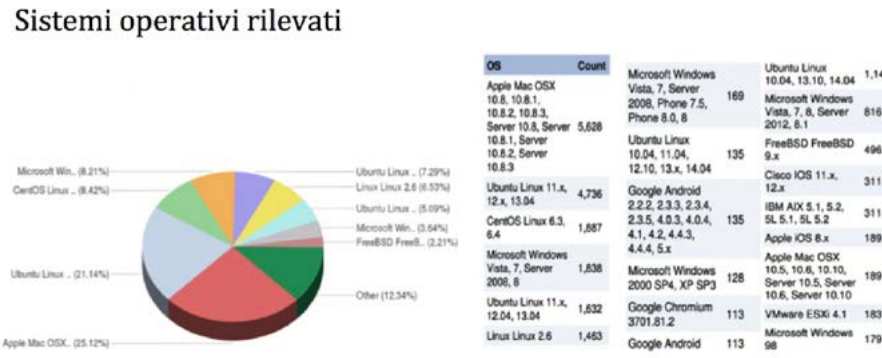


Figura 3 - Totale degli eventi di intrusione (Dati Cisco)

Altra cosa importante da notare è come la maggior parte degli eventi bloccati in maniera automatica sia stato legato ad eventi di tipo Trojan, ovvero a file scaricati da Internet, ritenuti erroneamente affidabili dagli utenti, la cui apertura avrebbe comportato l'esecuzione su personal computer di processi malevoli. Questo prevalentemente a causa dell'eterogeneità dei sistemi e dell'utenza che ha avuto accesso alla rete Expo.

Attraverso la correlazione di questi dati in tempo reale e la visibilità totale degli eventi in rete, gli operatori del SOC hanno potuto quotidianamente organizzare e rivedere il piano di azioni da intraprendere per adeguare e migliorare continuamente il grado di protezione del sito espositivo. Consultando ad esempio la distribuzione dei sistemi operativi di tutti gli oggetti connessi in rete come in Figura 4, il SOC ha potuto rilevare in ogni istante la presenza di client con vulnerabilità note, correlando tutte le informazioni a disposizione e definendo azioni correttive in modo tempestivo. Da notare la numerosità dei sistemi non aggiornati in termini di patch di sicurezza che hanno avuto accesso alla rete: questi potevano rappresentare una vulnerabilità importante, pertanto con queste informazioni i responsabili della sicurezza hanno potuto intervenire bloccando l'accesso alla rete per isolare il client.



OS	Count
Apple Mac OSX 10.8, 10.8.1, 10.8.2, 10.8.3, Server 10.8, Server 10.8.1, Server 10.8.2, Server 10.8.3	5,628
Ubuntu Linux 11.x, 12.x, 13.04	4,736
CentOS Linux 6.3, 6.4	1,887
Microsoft Windows Vista, 7, Server 2008, 8	1,838
Ubuntu Linux 11.x, 12.04, 13.04	1,632
Linux Linux 2.6	1,463
Microsoft Windows Vista, 7, Server 2008, Phone 7.5, Phone 8.0, 8	169
Ubuntu Linux 10.04, 11.04, 12.10, 13.x, 14.04	135
Google Android 2.2.2, 2.3.3, 2.3.4, 2.3.5, 4.0.3, 4.0.4, 4.1, 4.2, 4.4.3, 4.4.4, 5.x	135
Microsoft Windows 2000 SP4, XP SP3	128
Google Chromium 3701.81.2	113
Google Android	113
Ubuntu Linux 10.04, 13.10, 14.04	1,140
Microsoft Windows Vista, 7, 8, Server 2012, 8.1	816
FreeBSD FreeBSD 9.x	496
Cisco IOS 11.x, 12.x	311
IBM AIX 5.1, 5.2, 5L 5.1, 5L 5.2	311
Apple iOS 8.x	189
Apple Mac OSX 10.5, 10.6, 10.10, Server 10.5, Server 10.6, Server 10.10	189
VMware ESXi 4.1	183
Microsoft Windows 98	179

Figura 4 - Sistemi operativi rilevati (Dati Cisco)

Allo stesso tempo, dashboard con dati relativi ai principali utenti e client bersagli o oggetto di attacco, consapevole e non, hanno permesso l'attuazione di azioni di verifica e rimedio puntuali per limitare o annullare l'effetto di software malevoli che avrebbero potuto diffondersi pericolosamente. In caso di comportamenti anomali per continuo attacco subito o generazione persistente di attacco riferiti a client ed utenti specifici, i responsabili della sicurezza hanno potuto procedere ad analisi approfondite, individuando puntualmente il client e chiedendo agli utenti azioni correttive pena il blocco di accesso alla rete.

Anche conoscere la distribuzione della tipologia dei tentativi di attacco, come riportato in Figura 5 , ha permesso un adattamento continuo delle policy di protezione.

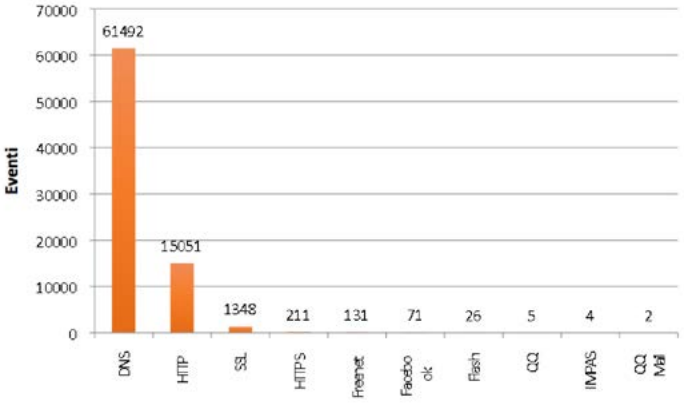


Figura 5 - Totale degli eventi di attacco per differenza di protocollo (Dati Cisco)

In particolare, le informazioni associate al grado di impatto degli eventi rilevati, personalizzate considerando la specifica realtà applicativa e di servizio dell'evento, hanno permesso di filtrare le segnalazioni di attacco in maniera efficace, portando in evidenza gli eventi veramente rilevanti per il contesto. Secondo le personalizzazioni degli strumenti di gestione nel caso di Expo, erano classificati come impatto prioritario gli eventi indirizzati verso un computer o dispositivo tecnicamente vulnerabile all'attacco correlato. Questo tipo di eventi richiedevano un'attenzione immediata, perché il rischio di un possibile incidente informatico era rilevante.

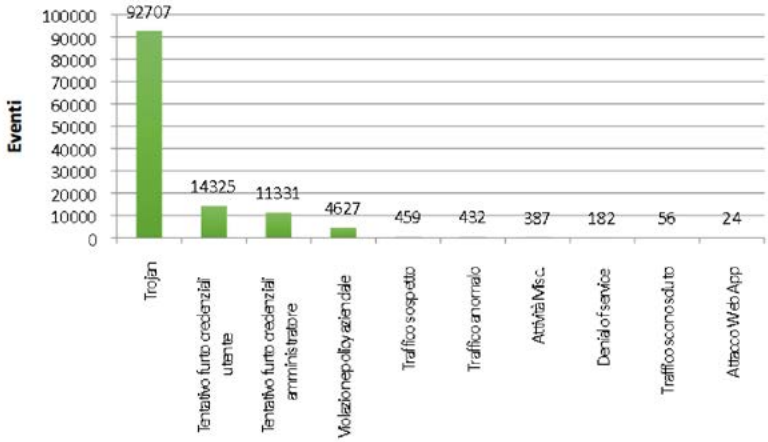


Figura 6 - Totale degli eventi bloccati (Dati Cisco)

Lo scenario di attacco e blocco riportato dai grafici (si veda in particolare la Figura 6) dimostra quanto l'approccio basato su una strategia architetturale, una forte componente di controllo e correlazione e un sistema di cloud intelligence solido ed efficace, abbiano permesso l'assenza totale di disservizi sul sito espositivo legati a problematiche di sicurezza, dimostrandosi un importante modello di riferimento per le realizzazioni future. Per Cisco, Expo ha rappresentato un caso di successo che ha dimostrato quanto la sicurezza costituisca un elemento prioritario nella progettazione e realizzazione di una Smart City. Nel consultare i dati reportistici e nel ripensare all'esperienza fatta durante i sei mesi dell'evento, è indubbio che senza un sistema di protezione efficace molti degli attacchi avrebbero potuto creare un danno serio all'evento, all'immagine dell'organizzatore ed ai suoi partner, quindi rimarrà per sempre un progetto di riferimento per sensibilizzare aziende ed enti all'importanza della Sicurezza IT.

Intelligence e Rilevazione degli incidenti
[a cura del Cert di Poste Italiane]

Il CERT di Poste Italiane [2], con lo scopo di garantire la tutela dei servizi digitali fruiti dagli utenti finali di EXPO 2015, ha erogato nel semestre Maggio-Ottobre 2015 servizi di sicurezza basati su attività di intelligence e prevenzione proattiva di minacce cibernetiche.
Durante il semestre sono stati identificati dal CERT di Poste Italiane 355 eventi di sicurezza - di cui si fornisce una ripartizione dei volumi sulle diverse aree operative quali Information Security Intelligence, Phishing, Brand Protection and Intellectual Property Right, Incident Handling e Mobile Security):

Figura 7 – Distribuzione delle segnalazioni prodotte durante il semestre

Nell'ambito dell'**Information Security Intelligence**, sono state raccolte e scambiate informazioni utili a prevenire in modo efficace attacchi informatici aventi come scopo l'interruzione della continuità dei servizi forniti attraverso i portali istituzionali di EXPO Milano 2015, o modificarne in modo illecito i contenuti.

[2] www.picert.it

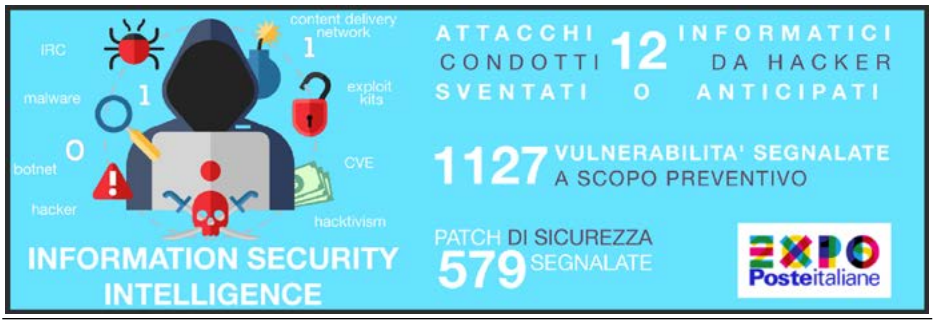


Figura 8 - Principali risultati operativi di Information Security Intelligence

Nello specifico, tramite attività di **Early Warning** e **Cyber Threat Intelligence** è stato possibile:

- notificare in maniera tempestiva e puntuale le informazioni di dettaglio in merito alle vulnerabilità che avrebbero potuto impattare la "catena tecnologica" di EXPO Milano 2015, ovvero l'hardware ed il software utilizzati dalle infrastrutture informatiche dell'esposizione universale;
- porre la giusta attenzione su informazioni e "rumors" inerenti l'evento e diffusi sui diversi canali digitali utilizzati da potenziali attaccanti (es. IRC Internet Relay Chat o sistemi di scambio di dati come *pastebin* e similari) durante le azioni propedeutiche o il coordinamento di attacchi informatici.

Nel semestre sono state quindi prodotte **265 segnalazioni di sicurezza** relative a:

- **12 attacchi** informatici identificati preventivamente;
- **1127 vulnerabilità** con un potenziale impatto sull'infrastruttura tecnologica;
- **579 patch** consigliate per sanare alcune delle vulnerabilità identificate.

In aggiunta, nei giorni precedenti l'inizio dell'evento, il monitoraggio di specifici canali IRC ha permesso di individuare:

- Due tentativi di attacco *DDoS*, uno al portale *MyExpo* dedicato alla gestione delle anagrafiche dei clienti Expo e l'altro ai server DNS del dominio **.expo2015.org*.
- Un tentativo di *defacement* del portale afferente al Padiglione Italia.
- Una copia integrale non autorizzata del database afferente a due distinti portali collegati alla manifestazione EXPO 2015.
- Alcuni server appartenenti alle *botnet* utilizzate per la conduzione di attacchi informatici, tra cui quelli DDoS.
- Alcuni server che, appartenenti al dominio EXPO, erano vulnerabili ad attacchi di tipo *Poodle* e\o *SSL Freak*, ovvero in grado di compromettere la riservatezza delle informazioni trattate dai portali istituzionali.
- Un archivio documentale che, gestito da terzi, consentiva l'accesso pubblico alle planimetrie e agli schemi dell'impianto elettrico e di condizionamento di alcuni padiglioni espositivi.

In aggiunta, le attività d'Information Security Intelligence hanno consentito di realizzare campagne di awareness e di identificare vulnerabilità relativamente alle principali tecnologie utilizzate dai sistemi della manifestazione, supportando quindi l'aggiornamento di sicurezza delle principali applicazioni e portali istituzionali utilizzati da EXPO, riducendo l'esposizione ad alcuni dei più recenti malware (es. *VisitorTracker*, *Zegost Backdoor Trojan*, etc.).

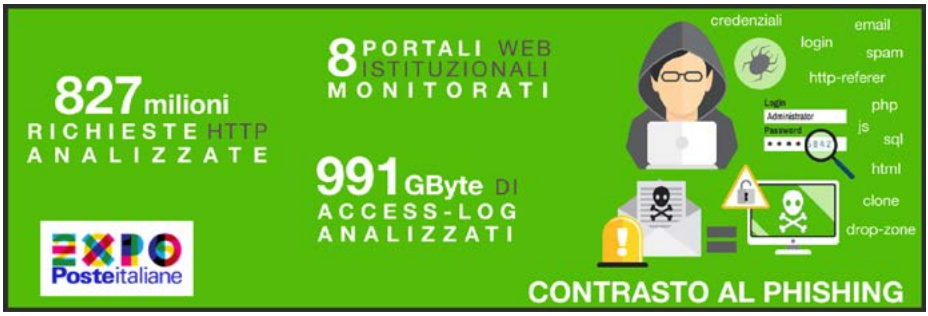


Figura 9 - Principali risultati operativi di contrasto al phishing

Le attività di contrasto al **phishing** sono state condotte dal team di sicurezza per identificare, analizzare e rimuovere/bonificare eventuali siti clone di EXPO Milano 2015 che potevano essere utilizzati per sottrarre dati anagrafici, credenziali di accesso e carte di credito, con lo scopo di eseguire successive transazioni illecite o alterare gli estremi dei ticket venduti cambiandone l'intestatario e rivendendoli in modo non autorizzato su mercati paralleli.
Nello specifico, il contrasto al phishing è stato svolto attraverso:

- il monitoraggio di caselle di posta elettronica create ad hoc per la ricezione di email fraudolente;
- il rilevamento di siti fraudolenti attraverso l'uso di strumenti dedicati all'analisi del web (*crawler*);
- attività di Open Source Intelligence (c.d. OSINT);
- segnalazioni ricevute dai circuiti internazionali di information sharing (es. il "Trust Introducer" ed il "Forum for Incident Response and Security Teams");
- l'analisi del campo *http-referer* delle richieste HTTP indirizzate ai portali istituzionali di EXPO;
- l'analisi degli access-log afferenti ai web server dei portali istituzionali dell'evento.

Figura 10 - Principali risultati operativi relativi alla tutela del marchio e della proprietà intellettuale

Particolare attenzione è stata posta alla **tutela del marchio e alla proprietà intellettuale di EXPO Milano 2015** sui canali digitali. Nello specifico, l'attività è stata volta al contrasto della compravendita di ticket contraffatti, della loro vendita da parte di soggetti non autorizzati, di forme di associazione ingannevoli e non autorizzate che utilizzavano marchi/segni distintivi dell'esposizione universale e, infine, del furto di identità. Grazie a queste azioni sono stati individuati:

- 8 rivenditori di ticket non autorizzati (alcuni a prezzi ridotti ed usufruendo illegittimamente di sconti riservati solo ed esclusivamente ai dipendenti delle aziende "Poste Italiane" ed "Agos");
- 2 domini web malevoli impropriamente riconducibili all'esposizione universale e dediti rispettivamente alla diffusione di virus informatici ed alla pubblicazione di annunci di lavoro illegittimi in nome e per conto di EXPO Milano 2015;
- **338 domini** internet indirettamente e/o erroneamente riconducibili all'evento ed oggetto di *typosquatting* (forma di *cybersquatting*[3] che si basa su errori di battitura/digitazione delle URL nel browser, finalizzata a dirottare l'utente verso un sito fraudolento), su un totale di **873.681** domini internet analizzati e costantemente monitorati.

Rilevante è stata la gestione di un furto d'identità a danni di Expo Milano 2015, manifestatosi nella diffusione di proposte di lavoro sottomesse su siti web di annunci per nome e per conto della manifestazione: gli annunci riportavano tra i contatti una serie di indirizzi email @jobs-expo2015.org e gli indirizzi internet jobs-expo2015.org e www.jobs-expo2015.org eseguivano una redirezione della navigazione degli ignari utenti verso il sito ufficiale dell'evento www.expo2015.org, al fine di non destare sospetti e far apparire la loro natura innocua. Quanto appreso è stato trasmesso al C.N.A.I.P.I.C. per le opportune azioni di contrasto e repressione dei crimini informatici.

[3] https://it.wikipedia.org/wiki/Cybersquatting

Figura 11 - Principali risultati nell'ambito della gestione degli incidenti

Le attività di **gestione degli incidenti informatici** sono state volte a supportare Expo nella gestione e prevenzione degli attacchi. Tra i principali risultati conseguiti, si evidenza la tempestiva segnalazione di **15 stati di mancata disponibilità** dei portali web istituzionali, consentendo così il rapido intervento di ripristino, e nell'identificazione di **23 server,** utilizzati per erogare servizi in ambito EXPO, verso i quali sono stati innalzati i livelli di sicurezza (i.e. cifratura) di tutti i protocolli volti alla tutela della segretezza delle comunicazioni. A complemento sono state svolte attività di monitoraggio verso specifici canali digitali che hanno permesso di identificare e analizzare preventivamente materiale atto alla realizzazione di attacchi DoS attraverso il sovraccarico dei server, sfruttando tipiche vulnerabilità del protocollo SSL/TLS.

Figura 12 - Contrasto alle minacce in ambito mobile

Tra i canali digitali utilizzati da Expo per la fruizione dei propri servizi, non poteva mancare quello "**mobile**" che, attraverso smartphone, tablet e App, ha permesso agli utenti di essere costantemente aggiornati sull'esposizione, sugli eventi in programma (concerti, degustazioni, festival, spettacoli, convegni, laboratori ecc.), esplorare i progetti architettonici, le gallerie fotografiche, i video, nonchè acquistare biglietti d'ingresso. Se, da una parte, la fruizione di questi servizi in regime di completa mobilità ha comportato notevoli vantaggi

per i visitatori, dall'altra li ha esposti a nuove forme di attacchi informatici. Con l'obiettivo di tutelare l'utente finale dalla possibilità d'installare app EXPO pubblicate su siti terzi non ufficiali (es. *1Mobile*, *Aptoide*, *Mobogenie* e *vShare*), potenzialmente alterate e pericolose, è stato attivato un programma di monitoraggio per la verifica della loro autenticità rispetto a quelle pubblicate sui sui siti ufficiali *Google Play Store* (per S.O. Android) e *Apple Store* (per S.O. iOS). In questo modo, attraverso la pubblicazione di 13 report bisettimanali, è stato possibile governare la presenza delle app sulla rete Internet, favorendo così la richiesta di rimozione di quelle contraffatte. Attraverso attività di analisi tecnica statica e dinamica dell'app "EXPO MILANO 2015", sia in versione Android che iOS, è stato inoltre possibile innalzare il livello di sicurezza dell'app stessa migliorando la gestione della sessione, la gestione dei dati trattati sul dispositivo mobile, la confidenzialità del canale di comunicazione e alcune funzionalità particolarmente delicate come quella per l'acquisto dei ticket d'ingresso all'evento. È stata infine individuata un'app che, sul market alternativo *Aptoide*, utilizzava loghi e segni distintivi simili a quelli utilizzati dall'app ufficiale "EXPO MILANO 2015", che richiedeva l'accesso a funzionalità e dati critici per l'utente (es. utilizzo connessione internet, lettura della posizione geografica, salvataggio di file sul dispositivo di archiviazione esterno).

Tutela dell'infrastruttura informatica
[a cura del CNAIPIC]

L'attività del CNAIPIC per la tutela dell'infrastruttura tecnologica di Expo 2015 costituisce una peculiare esperienza organizzativa ed operativa nel panorama delle diverse forze di polizia dedicate al contrasto del cyber crime, in quanto è la prima volta in Italia che per un grande evento è stata prevista la creazione di un dispositivo ad hoc per la gestione della sicurezza informatica. Le tecnologie IT sono infatti divenute imprescindibili per la gestione dei grandi eventi, in quanto essenziali per l'erogazione dei servizi, e perché sempre più iniziative analoghe sono caratterizzate dalla c.d. virtual experience.

Il CNAIPIC è stato istituito dal c.d. Decreto Pisanu, normativa emergenziale emanata all'indomani degli attentati di Londra del 2005. Con l'articolo 7 bis, denotando una particolare sensibilità verso la problematica riguardante la tutela delle Infrastrutture Critiche (IC), prevede la costituzione presso il Ministero dell'Interno, ovvero presso l'Organo per la Sicurezza delle Comunicazioni, di un centro dedicato alla protezione delle Infrastrutture Critiche Informatizzate.
Gli operatori del Centro, analogamente a quanto avviene per esempio in materia di contrasto alla criminalità organizzata, o in materia di contrasto al traffico di stupefacenti, vengono dotati di particolari strumenti investigativi (undercover, intercettazioni preventive).
Vantaggi della soluzione: concentrare in un'unica struttura le attività di prevenzione e contrasto a fenomeni di cyber crime (compito primario dell'istituzione Polizia di Stato), creazione di un sistema integrato pubblico-privato per la condivisione di informazioni ed ottimizzazione delle risorse.

Figura 13 - Convenzioni con le Infrastrutture Critiche

Nel corso degli anni sono state sottoscritte numerose convenzioni tra il CNAIPIC e le diverse infrastrutture critiche del Paese, con lo scopo di ampliare lo scambio di informazioni, formare gli operatori dedicati alla sicurezza IT, avviare le più corrette e meno invasive attività di indagine in caso di attacco, limitando al massimo gli eventuali disagi che in tali casi ricadono necessariamente verso le infrastrutture critiche ed i relativi gestori.

In tale quadro, il 18 dicembre 2012 è stata sottoscritta la Convenzione con EXPO: l'eccezionalità dell'evento, la centralità della componente IT nella gestione dei servizi erogati e soprattutto il breve lasso di tempo previsto tra l'allestimento dell'infrastruttura critica ed il successivo esaurimento del proprio "ciclo vitale", senza la possibilità di maturare adeguati sistemi di sicurezza che prevedono complessi cicli di VA e PT, hanno determinato eccezionalmente l'impegno del CNAIPIC nella governance e nei processi di analisi e valutazione dei rischi dell'intera piattaforma tecnologica, a partire dalla fase di progettazione.

L'avvio dell'evento ha significato invece l'attivazione del dispositivo operativo vero e proprio: due Centrali Operative, quella di via Drago e la Sala Operativa Internazionale SOI, quest'ultima popolata dagli ufficiali di collegamento e dai rappresentanti diplomatici degli stati esteri, di pronto impiego per l'espletamento delle attività di cooperazione internazionale.

Figura 14 – Centrali Operative Area Expo

Presso la centrale di via Drago sono stati creati tre centri interconnessi per la gestione degli eventi di sicurezza o di eventi critici riguardanti EXPO:

Figura 15 - Sede Operativa di Via Drago

- La sala "CNAIPIC per EXPO", dedicata esclusivamente alla sicurezza cyber dell'evento, supportata dal SOC di Telecom (general provider della manifestazione) e dal CERT di Poste Italiane, direttamente collegata alla Sala Operativa Centrale del CNAIPIC, sita in Roma ed interconnessa alle altre due sale.
- La sala COM gestita dalla Prefettura di Milano, che vedeva la presenza di tutte le Forze dell'Ordine e delle strutture di Protezione Civile, punto unico di contatto per lo scambio di informazioni, per la gestione degli interventi di sicurezza.
- La sala EC3, gestita direttamente da EXPO e dedicata agli eventi relativi ai servizi IT e non (manutenzione, pulizie etc.) erogati per il funzionamento della piattaforma, con la presenza di tutti i fornitori della manifestazione.

Le ultime due sale rispettivamente costituivano il terminale delle strutture di videosorveglianza dislocate sul territorio cittadino (COM) e lungo il perimetro e nel sito di EXPO (EC3).

Ovviamente il dispositivo messo in atto dal CNAIPIC prevedeva un'attività dedicata non solo alla piattaforma tecnologica di EXPO, ma a tutte le infrastrutture comunque connesse all'evento per determinare, in caso di attacco informatico, il livello di criticità rispetto alla manifestazione. Si pensi al sistema dei trasporti, alla distribuzione dell'energia elettrica, ai sistemi di comunicazione in generale.

Il protocollo operativo ha previsto la creazione di un team dedicato di 6 specialisti presso la Sala CNAIPIC di Via Drago, specificamente formati per le attività di monitoraggio ed analisi delle informazioni ricavate dalle attività di ricerca, anche mediante l'utilizzo di particolari software sviluppati ad hoc. Tale team è stato supportato da una complessa constituency formata da tutte le infrastrutture comunque coinvolte nella gestione dell'evento o ad esso interconnesse, che hanno fornito le informazioni riguardanti vulnerabilità, minacce ed attacchi informatici diretti verso le strutture di EXPO e degli altri enti coinvolti. Tale attività, oltre ad essere a carattere proattivo, prevedeva l'approfondimento ed il riscontro delle notizie provenienti dal SOC di Telecom (general provider della manifestazione) e dal CERT di Poste Italiane. Inoltre, il protocollo operativo ha previsto un collegamento diretto con le Sale COM ed EC3 presenti nel medesimo stabile: si pensi all'utilità delle informazioni provenienti dai social network in caso di manifestazioni *No EXPO*.
In caso di attacchi tentati ovvero consumati, il dispositivo ha previsto l'interessamento diretto del Compartimento di Milano e quindi dell'Autorità Giudiziaria competente (nella maggior parte dei casi quella Milanese).

L'importanza del dispositivo di sicurezza IT posto in essere in occasione dell'EXPO può essere valutato e meglio compreso partendo dalle dimensioni dell'infrastruttura che, come già evidenziato in precedenza, è stata attivata e sottoposta ad un alto stress in un periodo di tempo relativamente concentrato (6 mesi).
Una particolare menzione merita l'infrastruttura di rete in fibra e la completa, ridondante, copertura del servizio WI-Fi data agli utenti, senza dimenticare l'imponente macchina organizzativa posta in essere per la gestione degli ingressi al sito, totalmente automatizzata ed in grado di assorbire senza particolari problemi un'enorme mole di visitatori, anche grazie a flessibili strategie di direzionamento della folla, secondo modelli implementati con particolari software e grazie ad un complesso sistema di rilevatori.

Tale sistema tecnologico integrato, di fatto il cuore dell'intera piattaforma tecnologica, ha di riflesso generato un flusso di traffico (o meglio di attività virtuali) tale da potersi effettivamente parlare di una Virtual EXPO, realizzata in occasione dell'evento. Si pensi ai dati relativi alle visite del portale ufficiale ovvero a quelli relativi al ticketing (più di un milione e settecentomila visite), così come quelli riguardanti gli utenti dell'APP Ufficiale (più di un milione e mezzo di utilizzatori).
Un discorso a parte merita invece l'area social dedicata ad EXPO, enormemente rilevante nei numeri, già solo considerando i profili ufficiali dell'evento.

Quale l'impegno del CNAIPIC in merito?

Lo sforzo operativo direttamente connesso alla tutela dell'infrastruttura informatica di EXPO ha visto come sopra enunciato, due fasi, una preventiva ed una ad evento in corso.

Figura 16 - Attività di monitoraggio

Nel corso della prima, oltre alle attività di supporto direttamente connesse alle funzioni di analisi del rischio, si è avviata una attività dedicata di monitoraggio della rete in generale che ha visto l'impiego di 4 analisti esclusivamente dedicati ad EXPO per complessive 7.800 ore di monitoraggio. Tale attività ha permesso di fatto l'avvio e la corretta impostazione del dispositivo di sicurezza, permettendo di evidenziare il perimetro e gli obiettivi dell'azione.

A seguito dell'avvio della manifestazione, si è quindi passati ad una dedicata attività informativa finalizzata alla prevenzione di attacchi informatici, con l'impiego di 6 specialisti on site che, 24 ore su 24, 7 giorni su 7, sono stati esclusivamente dedicati alla cyber sicurezza dell'evento.
Ciò ha significato un impegno rilevante che ha visto il monitoraggio di più di **700 fonti web**, di qualsiasi natura, per un totale di **19.000 ore di monitoraggio**, finalizzato all'individuazione di vulnerabilità, minacce ed attacchi informatici.

Conclusioni

L'intera attività nel suo complesso, che ha visto coinvolti in un unico organizzato dispositivo trilatero il SOC di Telecom, il CERT di Poste Italiane ed il CNAIPIC secondo un modello di piena infosharing ed integrazione di diverse expertise, ha generato l'emanazione di ben 376 alert complessivi indirizzati ad EXPO ed alle infrastrutture critiche connesse all'evento (settore trasporti, energia, telco etc), e l'avvio di 12 attività investigative.

Figura 17 - Risultati conseguiti

A tal riguardo una menzione particolare merita la conclusione dell'operazione "Unmask" condotta dalla sezione di PG del CNAIPIC il 20 maggio 2015 che, ad EXPO avviata, ha permesso di dare un duro colpo al vertice del movimento ANONYMOUS italiano mediante l'arresto dei principali esponenti per associazione per delinquere i quali, affiancando il movimento di natura antagonista NO EXPO, si erano resi protagonisti di diversi attacchi informatici (DDoS del portale di ticketing, *sql injection* e *dump* del database di ticketing, *defacement* dei siti di riferimento).

Il mercato italiano della Sicurezza IT: analisi, prospettive e tendenze secondo IDC

La proliferazione di nuovi dispositivi, la progressiva diffusione di servizi e architetture basati su virtualizzazione e Cloud stanno cambiando radicalmente non solo il dipartimento IT, ma il modello di business di molte imprese italiane. Le infrastrutture sono innegabilmente messe sotto pressione dalla erogazione di contenuti, servizi e applicazioni attraverso architetture sempre più distribuite e dalla mobilità della forza lavoro che continua a crescere di anno in anno, con la conseguente apertura dei sistemi informativi aziendali oltre i tradizionali ambiti entro i quali erano stati concepiti e l'inevitabile esposizione di qualsiasi vulnerabilità agli exploit di potenziali aggressori, sia all'esterno che all'interno del perimetro aziendale. Inoltre, nel momento in cui una parte sempre maggiore delle transazioni economiche sono influenzate dai modelli e dalle tecnologie della Terza Piattaforma (Cloud, Big Data, Mobile, Social), la Sicurezza IT evolve da priorità meramente tecnica a priorità prevalentemente di business.

Le tensioni politiche internazionali tra NATO e Federazione Russa, le ripercussioni diplomatiche del caso Snowden e di PRISM, una rinnovata consapevolezza dell'opinione pubblica in merito allo spionaggio industriale e alle prassi di intercettazione di massa delle comunicazioni condotto da diversi governi, le nuove forme di associazione criminale attraverso l'impiego del Web come strumento di propaganda e reclutamento da parte del terrorismo internazionale, hanno ulteriormente accresciuto l'attenzione rispetto al tema della modernizzazione delle infrastrutture e dell'investimento nella Cyber-Security. L'ingresso nell'arena di nuove agenzie sponsorizzate da governi e dal terrorismo si aggiungono alle organizzazioni criminali e alle associazioni di hacktivist, dando ulteriore impulso all'industrializzazione del malware e all'ingegnerizzazione di nuove strategie di attacco, mostrando sempre più spesso l'inadeguatezza dei tradizionali sistemi di Sicurezza IT.

Nonostante alcuni progressi condotti dalle autorità nel combattere contro tali fenomeni, come le operazioni di polizia che hanno condotto alla cessazione delle attività organizzate dietro il Blackhole Exploit Kit e dietro la Gameover Zeus Botnet, tuttavia si moltiplicano esponenzialmente le varianti di malware da cui le imprese, i cittadini e le istituzione devono difendersi ogni giorno, oltrepassando le capacità dei tradizionali sistemi di individuarle e tracciarle adeguatamente. Da un lato i database per il riconoscimento dei malware assumono dimensioni sempre maggiori, determinando un impatto importante sulle performance dei server di sistema, mentre dall'altro tende ad aumentare il divario tra Time-to-Compromise e Time-to-Discovery, e quindi a incrementarsi la finestra di esposizione delle infrastrutture a potenziali minacce.
Secondo IDC, i fattori essenziali che decideranno in buona parte l'evoluzione delle tecnologie della Sicurezza IT nel 2016 sono riconducibili ad alcune tendenze di lungo termine:

- la crescita esponenziale di nuovi dispositivi e sensori intelligenti che troveranno spazio negli ambienti della vita domestica, professionale e pubblica, con problematiche di vulnerabilità del tutto sconosciute;
- l'attenuazione del confine tra vita privata e vita pubblica, in parte determinato dalla mobilità del lavoro, in parte dalla pervasività dell'informazione in ambienti sempre più intelligenti, in parte dalla digitalizzazione dell'identità civile individuale (il concetto stesso di cittadinanza può sempre più spesso essere riassunto dalla totalità delle credenziali di accesso ai sistemi della pubblica amministrazione);
- l'erosione graduale della Privacy sul Web, in un processo di dibattito pubblico caratterizzato comunque da una certa dualità e ambivalenza: da una lato la necessità di affermare vincoli normativi sempre più stringenti per la tutela dei dati personali (ad esempio, le normative emergenti relative al nuovo GDPR europeo), dall'altro l'introduzione di tecnologie sempre più sofisticate di sorveglianza da parte dei governi per tracciare il Digital Footprint di qualsiasi individuo (si pensi agli investimenti promossi da diversi governi europei per combattere contro il terrorismo digitale);
- la carenza di competenze e professionalità di alto livello, non soltanto a livello di mercato, presso le organizzazioni degli utenti finali, le imprese e le istituzioni, ma anche a livello di settore, con una competizione sempre più accesa tra i principali operatori internazionali nell'acquisizione di competenze, tecnologie ed expertise che spuntano in modo imprevedibile agli angoli del mondo.

Nel Future Scape 2016 IDC ha focalizzato la propria attenzione su alcune tendenze tecnologiche che potrebbero rivelarsi centrali rispetto agli sviluppi della Sicurezza IT nell'anno corrente. In particolare, alcuni dei punti essenziali che è possibile richiamare anche per il mercato italiano sono quelli relativi all'identificazione biometrica, alla *Security-as-a-Service*, alle *Self-defending applications*.

Nonostante la tecnologia fosse ampiamente matura già da tempo, soltanto con i primi significativi investimenti di alcuni grandi operatori (Apple Pay risale al 2014), il mercato ha cominciato a muoversi con forza in questa direzione, e sebbene l'applicazione abbia già raggiunto i principali operatori del mondo finanziario è ancora ben lontana dalla saturazione del mercato. Si tratta di una funzionalità su cui molti operatori, anche del comparto commerciale, andranno a rafforzare la propria proposizione, cercando di garantire allo stesso tempo la sicurezza delle transazioni e una *customer experience* capace di ridurre i costi legati al *churn-rate*. Secondo IDC, il canale dei pagamenti attraverso strumenti di prossimità crescerà di oltre 20 volte entro il 2020.

Sebbene il tema della Sicurezza IT sul Cloud rimanga in diversi contesti un ambito di discussione ancora aperto, tuttavia il Cloud rappresenta l'opportunità per erogare servizi di intelligence sempre più sofisticati, rispondendo alle esigenze di quella parte del mercato più sensibile ai rischi della competizione internazionale. La transizione da gateway on-premise a gateway on-Cloud per rafforzare la Web Security rimane un tema centrale nello sviluppo dell'offering del principali operatori del settore. Secondo IDC oltre la metà della Web Se-

curity sarà basata su una architettura di delivery as-a-Service entro il 2020.
La virtualizzazione sempre più profonda dei Data Center sta portando e porterà sempre più spesso nuove forme di automazione anche nel merito dei processi di Sicurezza IT. Nuovi paradigmi come i *Software-defined Environments* richiederanno un adeguamento delle logiche di sicurezza. In misura ancora maggiore, l'introduzione di Container applicativi consentirà ulteriormente di astrarre dalle specifiche condizioni hardware della macchina ma richiederà un disegno più evoluto delle soluzioni per la sicurezza applicativa. Evocativamente, e provocativamente, IDC immagina un scenario prossimo venturo fatto di applicazioni dotate nativamente degli strumenti indispensabili per garantire la sicurezza in modo autonomo e indipendente dall'ambiente operativo.

La Sicurezza IT in Italia: market spending & forecast

Nei paragrafi che seguono viene proposta una sintetica rappresentazione quantitativa dei principali segmenti della Sicurezza IT con riferimento al mercato italiano, in base alle tassonomie standard impiegate da IDC a livello internazionale. Le informazioni derivano dalla stima dei risultati dei principali operatori con riferimento ai ricavi di licenze, rinnovi, manutenzioni e sottoscrizioni a consumo di servizi rispetto al territorio nazionale. Le stime derivano sia dalla *knowledge base* accumulata da IDC a livello internazionale sia dalle attività di ricerca primaria condotte periodicamente a livello locale, e quindi dal contatti diretti con gli operatori e dall'analisi delle comunicazioni finanziarie. Per facilitare i processi di conciliazione dei dati, IDC impiega tassonomie standard rispetto alle quali vengono ricondotte e categorizzare le informazioni raccolte a livello internazionale. La Sicurezza IT rappresenta un'area tecnologica che attraversa trasversalmente almeno tre distinte tassonomie: la Software Taxonomy, la Security Product Taxonomy e la Service Taxonomy.
Comprendendo le principali declinazioni commerciali, dal software alle hardware appliances fino ai servizi, la Sicurezza IT è un mercato che in Italia vale circa 850 milioni di euro ed ha un tasso medio di crescita atteso al 2018 attorno al 2%. Nell'ultimo quinquennio si è osservato un andamento altalenante, influenzato in modo determinante sia da una cultura della sicurezza piuttosto episodica, che si risveglia soltanto quanto le cronache internazionali rendono evidente la vulnerabilità dei sistemi informativi, sia da una particolare condizione di fragilità dell'economia del paese, che più di altri in Europa ha sofferto, e ancora patisce, gli effetti dirompenti di una crisi storica (con una perdita della produzione manifatturiera stimata in decine di punti percentuali negli ultimi dieci anni).

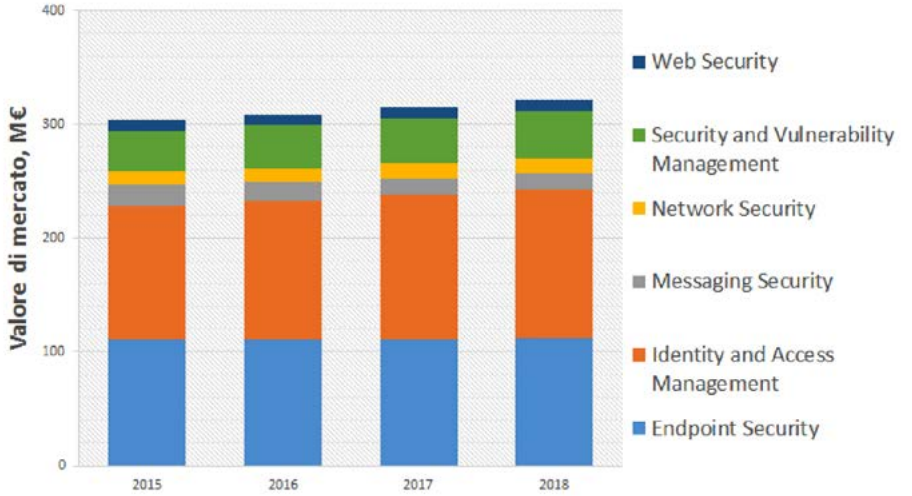


Figura 1– Software per la Sicurezza IT, i principali segmenti del mercato italiano.
Fonte: IDC Italy, 2015

Nella tassonomia software la Sicurezza IT viene segmentata in almeno sei aree principali (Web Security, Security & Vulnerability Management, Network Security, Messaging Security, Identity & Access Management, Endpoint Security) che in Italia hanno rappresentato un valore complessivo di oltre 300 milioni di euro nel 2015 (**Fig. 1**). Con un tasso di crescita medio al 2018 di circa 2%, a trainare la crescita del software sono essenzialmente le applicazioni legate a Identity & Access Management e Security & Vulnerability Management, mentre le altre aree stanno attraversando una fase di sostanziale stabilità, e in taluni casi, come per l'area Messaging, di revisione. Sebbene le trasformazioni radicali dello scenario di rischi e di minacce degli ultimi anni abbiano trovato un ampio riflesso nel rinnovamento delle proposte dei principali operatori, il mercato italiano ancora stenta a esprimere livelli di spesa più significativi, in parte per una questione prettamente culturale (come si vedrà nei paragrafi successivi), in parte per una questione strutturale (prevalenza del segmento SME su quello Enterprise).

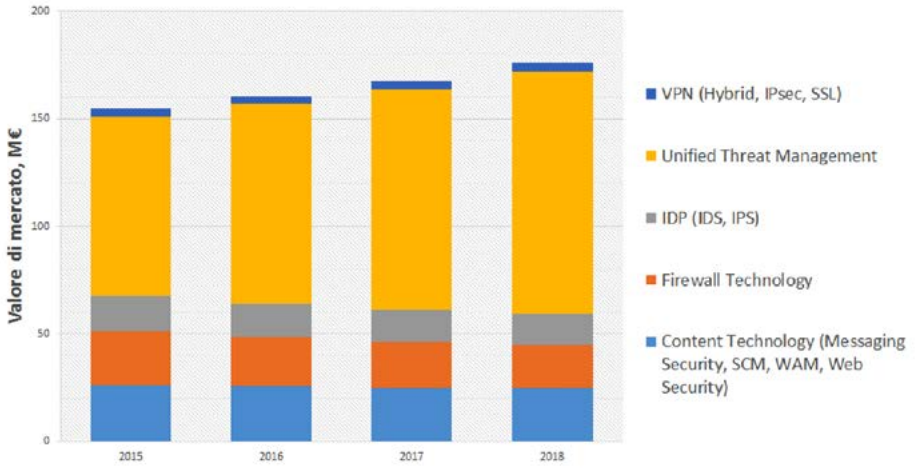


Figura 2– Appliances per la Sicurezza IT, i principali segmenti del mercato italiano. Fonte: IDC Italy, 2015

Nella tassonomia delle appliances la Sicurezza IT viene segmentata in almeno cinque aree principali (VPN, Firewall, IDP, Unified Threat Management, Content) che in Italia hanno rappresentato un valore complessivo di oltre 150 milioni di euro nel 2015 (**Fig. 2**). Con un tasso di crescita al 2018 previsto attorno al 4%, a trainare la crescita delle appliances sono essenzialmente le soluzioni di Unified Threat Management, mentre le altre aree rimangono in attesa di nuovo impulso di sviluppo, in parte per le prospettive di un quadro macroeconomico nazionale di sostanziale stagnazione a medio termine, in parte per processi di rinnovamento tecnico e organizzativo più generali che stanno trasformando i modelli di riferimento dell'IT da logiche tradizionali verso nuovi modelli di servizio.

Sebbene sia noto che negli ultimi anni il segmento abbia trovato ampia articolazione in servizi altamente differenziati sul mercato, i servizi per la Sicurezza IT vengono esaminati rispetto alla ripartizione tradizionale tra aree IT Consulting e System Integration/ Implementation (**Fig. 3**). Con un tasso di crescita al 2018 stimato attorno a 1,5%, i servizi rappresentano una parte essenziale del settore con quasi 400 milioni di euro nel 2015. A guidare la crescita sono soprattutto i progetti di consulenza, mentre le implementazioni effettive crescono più lentamente, ma su dimensioni di valore maggiori. A livello aggregato il mercato italiano cerca di comprendere le nuove traiettorie su cui si muovono le minacce alla Sicurezza IT, affrontando con maggiore cautela scelte di investimento più significative e durature.

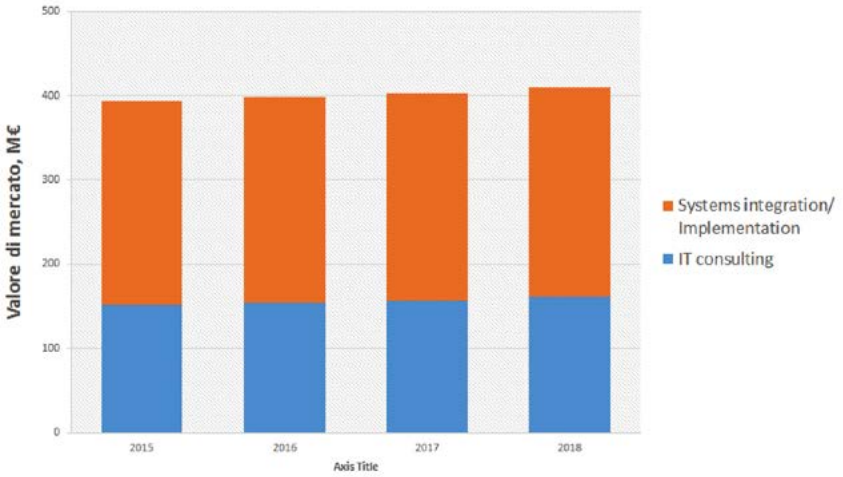


Figura 3– Servizi per la Sicurezza IT, i principali segmenti del mercato italiano.
Fonte: IDC, 2015

La Sicurezza IT in Italia: sfide e opportunità

Nella sezione seguente verranno evidenziati i principali risultati di alcune indagini condotte da IDC sul tema della Sicurezza IT nel corso del 2015 che hanno coinvolto alcune centinaia di imprese italiane. Per ciascuna indagine, il dato campionario è stato estrapolato all'universo delle imprese italiane nei segmenti di riferimento in modo tale da dare una compiuta rappresentazione del fenomeno della Sicurezza IT presso le Medie e Grandi Imprese.

Gli strumenti di indagine, composti da circa una decina di quesiti di approfondimento con domande a risposta chiusa e a risposta multipla, indagavano le priorità principali del dipartimento IT, le sfide culturali e organizzative per sviluppare una strategia di Sicurezza IT, la natura delle proprietà aziendali da tutelare, le aree tecnologiche di esplorazione e investimento nel breve termine, le esigenze percepite con riferimento ai principali profili professionali.

I questionari sono stati somministrati a campioni che comprendono sia le figure apicali dell'IT aziendale (CIO/ Directors/ etc.), sia figure più specializzate che danno una centralità di rappresentanza al tema della Sicurezza IT (Chief Information Security Officer/ IT Security Manager/ etc.), sia figure di middle management più generaliste per cui la Sicurezza IT rappresenta un compito comunque imprescindibile (IT Manager/ Responsabili IT/ etc.).

Nella sezione seguente si cercherà di tracciare quantomeno uno scorcio del ruolo essenziale della Sicurezza IT nei processi di trasformazione digitale, della sensibilità organizzativa che va emergendo in merito alle nuove tipologie di attacchi, alcune indicazioni in merito allo scenario delle competenze e delle professionalità strategiche sul mercato del lavoro.

Il ruolo della Sicurezza IT nei processi di trasformazione

La Sicurezza IT gioca sempre più spesso il ruolo di tecnologia abilitante in processi di cambiamento tecnologico e organizzativo di più ampia portata, sia a livello macro che a livello micro. Rispetto ai processi di transizione industriale alle tecnologie della Terza Piattaforma, la Sicurezza IT concorre a consolidare la struttura del nuovo spazio di prodotti e servizi che sta nascendo all'intersezione tra Cloud, Big Data/ Advanced Analytics, Social Platform e Mobile Devices. Rispetto ai processi di trasformazione delle singole organizzazioni, la Sicurezza IT risulta un fattore centrale nei processi di trasformazione digitale che stanno intraprendendo moltissime imprese per sopravvivere a una competizione sempre più sofisticata a livello internazionale.

La Terza Piattaforma determina un circolo virtuoso di trasformazioni che comportano aspettative sempre più onerose per la Sicurezza IT. Da un lato, l'accumulazione degli investimenti industriali del settore ha ormai oltrepassato una soglia critica, per cui la proliferazione delle infrastrutture di data centers sta portando a una drastica riduzione dei prezzi dei servizi Cloud e una competizione sempre più accesa tra i principali operatori (ogni settimana si rincorrono sempre più spesso le press release con annunci di riduzioni sempre più importanti). L'affermazione del Cloud come paradigma di delivery di una parte sempre più importante di servizi IT apre una sua volta una spazio maggiore a nuovi dispositivi e smart devices del tutto inediti, caratterizzati da una sempre maggiore integrazione di sensori diversi, determinando un flusso tumultuoso e continuo di dati e informazioni che saranno prodotti sia da oggetti del mondo esterno sia da individui organizzati nelle Social Platform: nel momento in cui il confine tra spazi della vita personale e spazi della vita pubblica e professionale diventano sempre più vicendevolmente permeabili, il tema della Sicurezza IT diventa così essenziale da diventare oggetto di un dibattito sempre più acceso a livello di dibattito politico e normativo, non soltanto a livello di sviluppo tecnologico e competizione di mercato.

Analogamente a quanto si osserva a livello internazionale, dall'analisi del mercato italiano si desume una connessione importante tra l'andamento della spesa in Sicurezza IT e l'orientamento strategico delle imprese rispetto ai progetti sulla Terza Piattaforma **(Fig. 4)**. Circa il 41% delle imprese con oltre 50 addetti ha previsto una incremento della spesa negli ultimi 12 mesi, nella maggior parte dei casi contenuto sotto il 10%, ma in un numero ristretto, circa il 2%, anche superiore. In posizione minoritaria, circa 12%, quanti hanno segnalato una riduzione della spesa. La gran parte delle imprese italiane, oltre il 47%, ha deciso di mantenere inalterato il livello della spesa. Tale quadro generale consente una duplice lettura, sia positiva, che negativa: da un lato, seppure molto lentamente, le imprese italiane stanno superando, e molte hanno già superato, la fase più critica di razionalizzazione della spesa IT e stanno riprendendo a investire in una funzione strategica; dall'altro, conoscendo quanto siano limitati gli investimenti IT, e soprattutto quelli relativi alla Sicurezza, appare evidente che il mantenimento di un livello di spesa inadeguato lascia le imprese italiane esposte a un rischio IT sempre più prominente a livello internazionale.

Osservando più nel dettaglio la composizione dei dati precedenti, è possibile cogliere quanto l'espansione della spesa sia riconducibile ad imprese che stanno portando avanti progetti legati alla Terza Piattaforma. Oltre la metà delle imprese che espandono la spesa in Sicurezza IT indica come particolarmente importanti (molto importanti o estremamente importanti) le iniziative previste in merito ai Mobile Devices, ai Big Data, al Cloud e ai Social Media, mentre la stessa proporzione scende a meno di un quarto tra le imprese che stanno ancora riducendo la spesa. Una parte sempre più importante della Sicurezza IT di fatto è già legata a nuovi paradigmi tecnologici, portando quella che fino a ieri era una componente minoritaria del budget IT al centro dei nuovi sviluppi progettuali a cui molte imprese si affidano per rinnovare non soltanto l'IT, ma l'intero assetto aziendale.

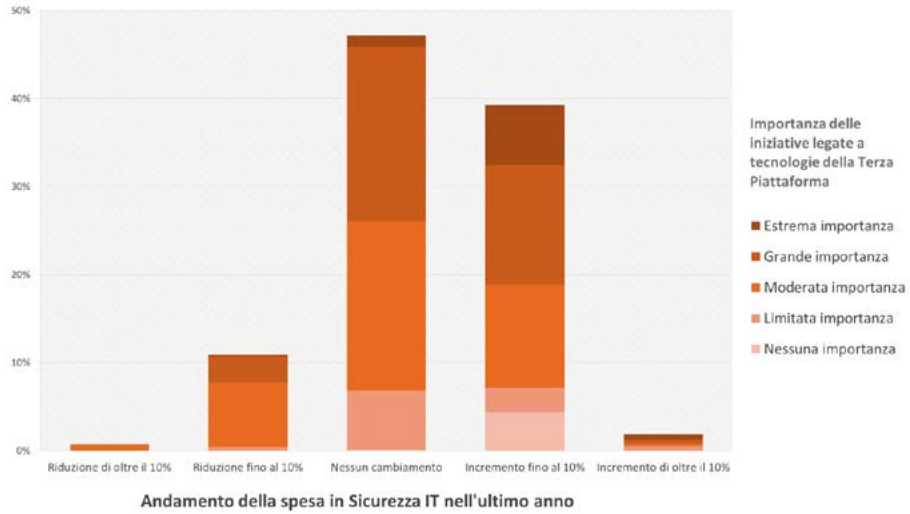


Figura 4– Rapporto tra andamento della spesa in Sicurezza IT e iniziative relative alle Third Platform Technologies. Fonte: IDC, 2015 (campione n=223, imprese con oltre 50 addetti; percentuali del campione estrapolate all'universo di riferimento)

Le tecnologie legate alla Terza Piattaforma stanno concorrendo in misura determinante a un processo di trasformazione che procede ben al di là dei confini tradizionali di un singolo settore/ mercato, per coinvolgere sezioni sempre più estese dell'economia: dal giornalismo, dove si moltiplicano casi esemplari come quello del Washington Post, all'ambito assicurativo, dove un numero crescente di operatori formano alleanze e joint-venture per sviluppare nuovi modelli organizzativi, come Allianz, Baidu e Hillhouse; dal retail, dove operatori come American Apparel stanno rapidamente adeguando il proprio front-end per rispondere alle aspettative del consumatore digitale, all'automotive, dove operatori come Google e Ford stanno accelerando lo sviluppo delle piattaforme di infotainment per creare vere e proprie

connected cars. La Terza Piattaforma ha aperto le porte alla Digital Transformation, a un processo ancora da comprendere a livello analitico nelle sue molteplici sfaccettature, che cionondimeno sta sempre più al centro dell'attenzione di manager, imprenditori e policy maker.

Non è possibile dare che una definizione molto generale e onnicomprensiva di quanto sta accadendo nei settori più disparati: la Digital Transformation è un processo di rinnovamento che attraversa le infrastrutture aziendali per arrivare a una trasformazione in taluni casi anche radicale del modello di business delle imprese. La funzione di produzione delle aziende sta cominciando a cambiare, adeguandosi a una realtà fatta di mercati virtuali dove non esistono più le frizioni e le inerzie consuete dei mercati tradizionali, dove i costi di transazione e coordinamento risultano pressoché annullati, dove la trasparenza dei prezzi consente operazioni di scambio e arbitraggio sempre più efficienti, dove le funzioni produttive delle imprese si frammentano e si delocalizzano in cerca di fattori produttivi alle migliori condizioni, dove accanto a fattori quali il capitale e il lavoro si aggiunge il dato come nuovo strumento di produzione. Questo è il contesto in cui la Digital Transformation si manifesta e si sviluppa, dando il segno della nascita di una nuova funzione produttiva che accanto alla trasformazione dei fattori tradizionali procede alla trasformazione di dati in informazione, dell'informazione in conoscenza, della conoscenza in valore.

La Digital Transformation viene indicata come un cambiamento prioritario da oltre una impresa su due (segmento con oltre 50 addetti), evidenziando come questo tema sia ampiamente entrato nell'agenda strategica delle imprese italiane, sebbene con sensibilità diverse a seconda del settore industriale e della classe dimensionale: una particolare attenzione è prestata da alcuni comparti, come il Commercio, i Servizi (soprattutto in ambito business), la Pubblica Amministrazione estesa (comprendendo anche la Sanità e l'Istruzione), e soprattutto da imprese di grandi dimensioni, sopra i 250 addetti. Si tratta di un tema ampiamente irrisolto in molti contesti, esiste ancora uno scetticismo piuttosto ampio sulla possibilità di replicare modelli esterni quando a livello infrastrutturale il mercato italiano deve ancora percorrere molta strada per essere al passo dei mercati europei e internazionali, tuttavia è lecito attendersi un ragionevole progresso della sensibilità nei prossimi anni, quando il mercato avrà fatto maggiore chiarezza e con indiscutibile evidenza saranno emersi casi di successo anche a livello italiano.

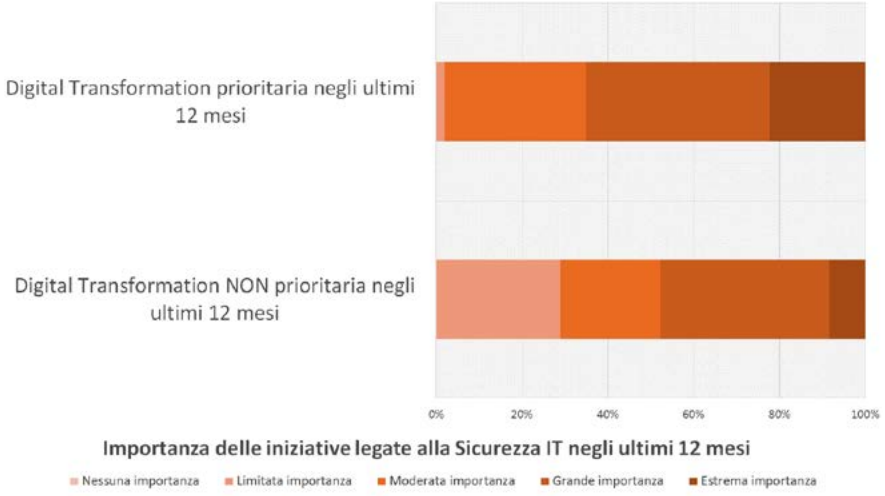


Figura 5– Rapporto tra Digital Transformation e iniziative relative alla Sicurezza IT. Fonte: IDC, 2015 (campione n=223, imprese con oltre 50 addetti; percentuali del campione estrapolate all'universo di riferimento)

Di nuovo, come evidenziato rispetto alla Terza Piattaforma, la Sicurezza IT si rivela un fattore rilevante anche rispetto alle valutazioni che le imprese italiane stanno facendo in termini di Digital Transformation. In particolare **(Fig. 5)**, è possibile trarre alcune considerazioni interessanti incrociando il dato relativa all'importanza delle iniziative legate alla Sicurezza IT con il dato relativo alla priorità che le imprese attribuiscono ai processi di trasformazione. Dal confronto fra le imprese che considerano la trasformazione digitale una priorità e quelle che invece non se ne curano, emergono alcune differenze da non sottovalutare: le imprese che non contemplano alcun processo di trasformazione riconoscono l'importanza dei progetti di Sicurezza IT il 48% dei casi (percentuale dei casi indicati come molto/estremamente importanti); invece, le imprese che stanno intraprendendo le incognite della trasformazione digitale guardano alla Sicurezza IT da una prospettiva completamente diversa, e riconoscono la centralità di tali progetti fino al 65% delle volte. Una simile differenza porta necessariamente a interrogarsi se la Digital Transformation non sia una opportunità importante per la Sicurezza IT, attribuendo una responsabilità rinnovata a una funzione che sembrava limitata esclusivamente a un ruolo di supporto.

Le principali minacce alla Sicurezza IT percepite dal mercato italiano

La Sicurezza IT assume connotazioni anche notevolmente diverse a seconda della prospettiva industriale dalla quale viene osservata. Nel momento in cui si intenda approfondire il tema è indispensabile portare una distinzione fondamentale tra i settori industriali in

base allo specifico carattere dei processi produttivi: da una parte, i settori caratterizzati da processi di produzione prevalentemente centrati, seppure in senso generale, sulla trasformazione materiale di beni e servizi (come Industria e Commercio); dall'altra, i settori caratterizzati da processi di produzione ampiamente focalizzati sulla trasformazione di dati, informazioni e fattori prevalentemente immateriali (riconducibili a settori quali i Servizi, la Finanza/ Assicurazioni, la Pubblica Amministrazione). Se si parte dal presupposto che la Sicurezza IT presenta sfumature talvolta assai differenti a seconda che venga esaminata dalla prospettiva delle *data-intensive industries* oppure delle *material-intensive industries* allora diventa possibile scorgere la complessità delle dinamiche espresse dal mercato.

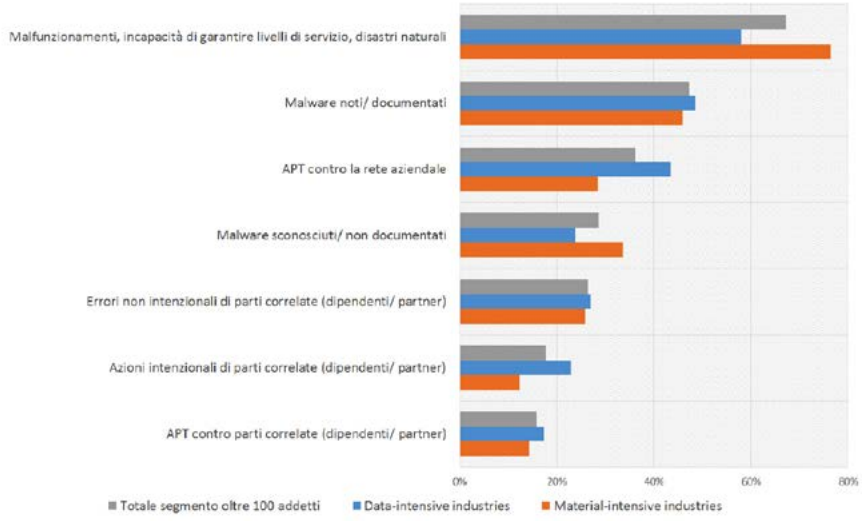


Figura 6 - Livello di allarme rispetto a diverse tipologie di incidente. Fonte: IDC Italia, 2015 (campione n=100, imprese con oltre 100 addetti, base variabile nei sottogruppi; percentuali del campione estrapolate all'universo di riferimento)

Come in altre indagini condotte sul mercato italiano, esiste una consapevolezza piuttosto limitata delle nuove tipologie di rischio, che si traduce in un livello di allarme inferiore a quanto tendenzialmente si osserva a livello internazionale **(Fig. 6)**: nonostante le cronache di attacchi sempre più sofisticati, circa il 47,3% delle imprese sopra i 100 addetti mette ancora in evidenza il malware noto/ documentato/ signature-based come il principale fattore di una preoccupazione crescente/ molta preoccupazione rispetto ad altri elementi di rischio più temibili dal punto di vista tecnico, come gli Advanced Persistent Threat (APT) condotti contro la rete aziendale (evidenziato soltanto nel 36,2% dei casi) e i malware non-noti/ non-documentati/ signatureless (28,6%). Prevalgono ancora nettamente i timori legati alle fondamenta di base dei sistemi, con un allarme che raggiunge oltre due aziende su tre in

merito a malfunzionamenti generici e disastri naturali. In molti contesti, prima ancora di porsi il problema di affrontare minacce più sofisticate, la parola chiave è ancora *back-to-basics*. Una chiara differenza di percezione emerge nel confronto tra *material-intensive* e *data-intensive industries*, dove nel primo caso si denota una maggiore attenzione agli zero-days e al malware non-documentato (evidenziato dal 33,6% delle imprese, ben oltre il dato medio totale del mercato), mentre nel secondo caso esiste una cultura potenzialmente più sviluppata rispetto al tema delle strategie di attacco eterogeneo, specifico e persistente (allarmante secondo il 43,5% delle imprese, contro un dato medio a totale considerevolmente inferiore). Nell'ordine generale di pericolosità complessiva seguono le azioni, intenzionali o meno, condotte da partner e/o dipendenti (rispettivamente, 26,4% e 17,8%), gli APT condotti contro la filiera dei partner e/o contro specifiche personalità aziendali (15,8%), di nuovo con alcune ambivalenze di valutazione che mettono in risalto la relativa maggiore sensibilità dei settori che lavorano con *assets* e *properties* intangibili. Soprattutto quest'ultimo dato mette in evidenza come una parte del mercato non abbia ancora pienamente compreso il carattere di lateralità degli APT, per cui la Sicurezza IT sta rivelandosi una variabile di sistema che va salvaguardata a livello di filiera industriale, e non soltanto rispetto a una singola impresa. Nel segmento esaminato traspare la tendenza del mercato italiano ad attestarsi su una visione piuttosto tradizionale delle minacce che possono coinvolgere i sistemi informativi aziendali, e una inclinazione piuttosto netta a sottovalutare i rischi derivanti dagli *insiders* e dai partner nella filiera produttiva, nonostante il continuo allarme alimentato dalle cronache degli ultimi anni: è come se prevalesse lo scetticismo in merito alla possibilità di essere attori principali di vicende che sembrano sempre lontanissime quando vengono presentate dai media e dalla stampa.

Analogamente a quanto si verifica in merito alle tipologie di incidente che producono maggiore allarme, il rischio percepito dalle imprese dipende in misura sostanziale dall'asset/property aziendale di maggior valore, e dunque attraversa l'intero complesso industriale con grandissima variabilità a seconda delle specifiche condizioni di ciascuna azienda. Cionondimeno, è possibile trarre qualche considerazione generale proseguendo attraverso la chiave di lettura relativa al grado di orientamento del processo di produzione al trattamento e alla trasformazione dei dati.

Come si osserva nella **Fig. 7**, l'interruzione dell'operatività aziendale e la perdita di dati personali regolati dalla legge rappresentano i timori principali delle imprese italiane (dato generale, rispettivamente, 54,7% e 50,2%), con una attenzione spiccatamente diversa nel confronto fra il gruppo data-intensive (61,7% e 57,8%) e quello material-intensive (47,2% e 42,1%): si osserva come il grado di digitalizzazione dei processi produttivi concorra a determinare una differenza di percezione piuttosto significativa, che può arrivare fino a quindici punti percentuali. Le posizioni si invertono in merito ad altre dimensioni di rischio, quali la diffusione di informazioni commerciali e finanziarie (dato generale, rispettivamente, di 42,3% e 31,8%), dove i settori prevalentemente orientati a processi di trasformazione fisica sulle stesse variabili esprimono una attenzione certamente superiore (58,3% e 41,7%) rispetto ai settori che lavorano su dati e informazioni (27,2% e 22,5%). I timori relativi a

penali contrattuali e multe delle pubbliche autorità appaiono nel complesso residuali.
Esistono altre dimensioni di rischio rispetto le quali si osserva una sostanziale convergenza di valutazioni tra *data-intensive* e *material-intensive industries*: in particolare, il tema dei danni all'immagine e al brand aziendale insieme al tema del costo di recupero e ripristino dei sistemi dopo un incidente appaiono equamente percepiti dal 36,2% e dal 30,5% dal segmento di riferimento. Occorre ricordare che un ulteriore fattore che influenza la percezione dei rischi è rappresentato dalla dimensione diacronica, ovvero, dalla specifica collocazione temporale della valutazione rispetto al momento in cui si è determinato l'incidente. La valutazione ex-post dei rischi può cambiare in modo importante rispetto a una valutazione ex-ante: alcune dimensioni di impatto, soprattutto gli impatti su valori intangibili come l'immagine, la reputazione e il brand aziendale, vengono in taluni casi sovrastimate, mentre altre legate a valori tangibili, soprattutto il costo degli interventi di ripristino, sono tendenzialmente sottostimati; dunque, una volta che si sono effettivamente determinati *data-breach* e altri incidenti similari, si osserva molto spesso una sostanziale inversione nel peso attribuito alle diversi rischi.

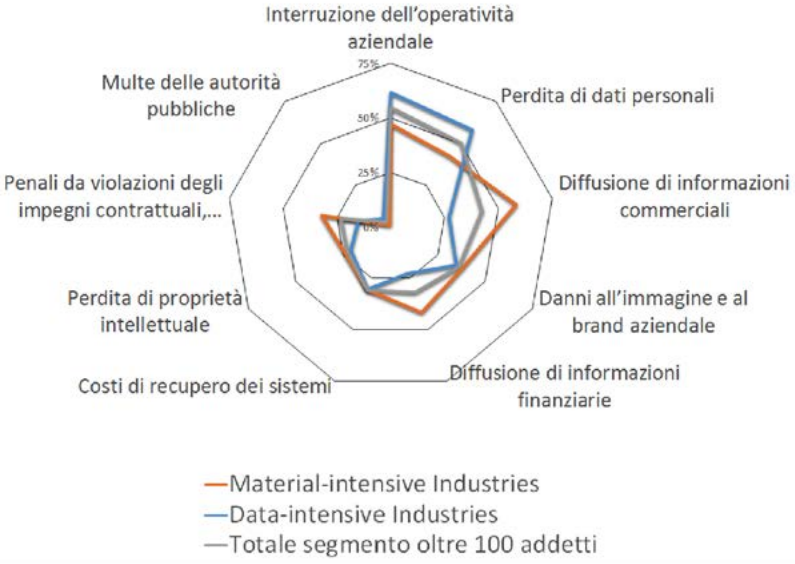


Figura 7 – Rischio atteso in caso di attacchi informatici. Fonte: IDC Italia, 2015 (campione n=100, imprese con oltre 100 addetti, base variabile nei sottogruppi; percentuali del campione estrapolate all'universo di riferimento)

La Sicurezza IT tra questioni organizzative e mercato del lavoro

A differenza di altre funzioni del dipartimento IT, la Sicurezza si trova in una posizione assai poco invidiabile, perché non è chiamata soltanto a gestire le performance tecnico-economi-

che di un sistema di soluzioni e tecnologie sempre più complesse, ma a diventare garante di un risultato che dipende da variabili organizzative che in gran parte trascendono qualsiasi soluzione tecnica. Tra le varie metriche rispetto alle quali misurare i risultati dell'IT, la Sicurezza è senza dubbio la dimensioni più difficile da valutare, perché consiste tanto di fattori tecnici quanto di fattori umani, e in modo particolare discende da una sintesi equilibrata di percezioni che derivano da *stakeholders* diversi, sia all'interno della stessa organizzazione (la Line-of-Business è il primo interlocutore, ma non l'ultimo), sia all'esterno (corpi di standard e certificazione, istituzioni di vigilanza e controllo, partner commerciali e fornitori di servizi, etc.).

Se la Sicurezza IT non sta soltanto dentro la testa del Security Manager, ma dipende da una negoziazione e dall'accordo fra diversi attori, le cui valutazioni convergono nel riconoscere di avere raggiunto un risultato apprezzabile, diventa fondamentale la posizione che tale funzione occupa all'interno dell'IT e il grado di visibilità che riceve rispetto al C-Level. Ed è proprio sul piano organizzativo, ancor prima che su quello delle competenze tecnologiche, che la Sicurezza IT va a vincere oppure perdere la possibilità di giocare un ruolo più importante nel processi di trasformazione digitale e di rinnovamento della funzione. Quando si affronta il tema del posizionamento organizzativo della Sicurezza IT, il mercato italiano presenta alcune ambivalenze che è opportuno ricordare (**Fig. 8**), soprattutto se le informazioni vengono interpretate nella distinzione tra *material-intensive industries* e *data-intensive industries*.

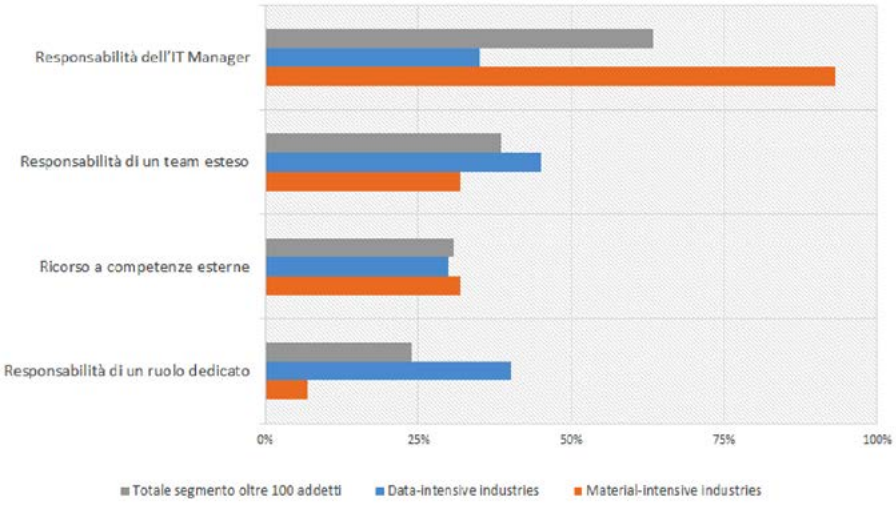


Figura 8 – Collocamento organizzativo delle responsabilità relative alla Sicurezza IT. Fonte: IDC Italia, 2015 (imprese con oltre 100 addetti, base variabile nei sottogruppi; percentuali del campione estrapolate all'universo di riferimento)

Ancora gran parte delle imprese italiane (63,3%) ritiene che la Sicurezza IT sia una responsabilità che afferisca alle competenze generali dell'IT Manager, senza alcuna considerazione in merito al grado di specializzazione richiesto o alle risorse e agli investimenti necessari per rendere operativa tale funzione. Una netta distinzione si osserva nel confronto tra *material-intensive industries* e *data-intensive industries*, dove emerge con grande chiarezza una differente sensibilità rispetto alla strutturazione organizzativa della Sicurezza IT: laddove, come nei settori di trasformazione tradizionale, non è compresa la necessità di mitigare il rischio IT come un qualsiasi altro rischio aziendale è difficile immaginare che si apra uno spazio per una funzione specifica e ruoli specializzati. Viceversa, dove il core-business è da sempre strettamente legato al trattamento dell'informazione, come nei settori *data-intensive*, esiste un livello di consapevolezza completamente diverso: la Sicurezza è concepita come un processo organizzativo più complesso che richiede il coinvolgimento di un team esteso di competenze (45%) e in molti casi di un ruolo dedicato (40%).
Questo diverso livello di consapevolezza organizzativa che distingue *material-intensive industries* e *data-intensive industries* ha un riflesso nella valutazione di quali siano i ruoli professionali di maggiore impatto per il successo dell'impresa e di maggiore difficoltà di reperimento sul mercato del lavoro. Oltre il 35% delle imprese sopra i 100 addetti (**Fig. 9**) indica i ruoli C-Level (CSO, CISO, Security Director), con una differenza trascurabile sia dal punto di vista della classe dimensionale delle imprese che dal punto di vista del settore di riferimento. Seguono i ruoli legati al middle management (34%), i ruoli di ingresso 16%) e i ruoli esterni (15%). Nei ruoli non-apicali si riscontrano differenze più marcate: le *data-intensive industries* esprimono esigenze molto più articolate in termini di professionalità, mettendo in particolare risalto i ruoli di middle management (61,6%) e mantenendo anche grande considerazione rispetto alle figure esterne (26,6%), ben al di sopra dei dati medi complessivi del segmento.

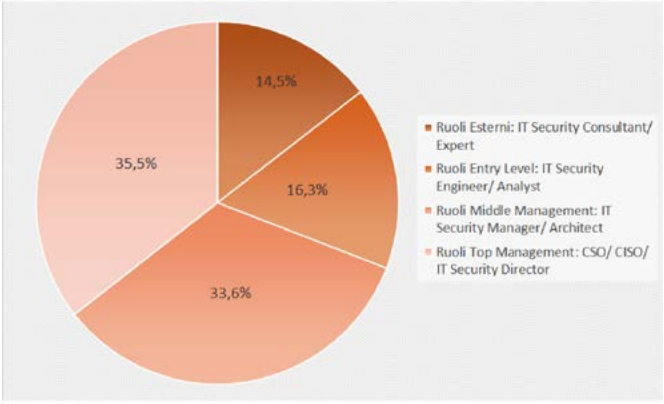


Figura 9 – Ruoli di maggiore impatto e difficoltà di reperimento sul mercato. Fonte: IDC Italia, 2015 (imprese con oltre 100 addetti; estrapolazione all'universo di riferimento)

Anche analizzando il corpus delle competenze della Sicurezza IT, sempre più ampio ed eterogeneo, emerge uno scenario di competenze in continua evoluzione. Dopo una rapida rassegna per macroaree tematiche (**Fig. 10**), è possibile ravvisare come in molte imprese sia ancora in corso una contesa, non soltanto per un riconoscimento organizzativo della Sicurezza, ma per la creazione di una cultura aziendale capace di riconoscere le nuove forme che sta assumendo il rischio IT a livello internazionale. Infatti, le imprese italiane sono ancora in cerca di competenze legate ad aree tematiche fondamentali (spesso la parola d'ordine è "*back to basics*"), come Data Privacy (55,7%), Compliance (42,3%), Business Continuity (33,4%), mentre trascurano ampiamente altri ambiti dove stanno maturando nuove minacce e sfide tecnologiche, si pensi all'area del Forensic (10,3%), oppure a quella della CyberSecurity (8,8%). Come sempre accade, qualunque scotoma nella visione manageriale ha inevitabilmente delle conseguenze rispetto alle priorità di recruiting sul mercato del lavoro.

Analogamente a quanto osservato per i profili professionali, soprattutto quando si impiega una chiave di lettura che interpreta la Sicurezza rispetto alla specifica diversità dei comparti industriali e dei segmenti dimensionali, allo stesso modo, e, se possibile, in misura ancora maggiore, si osserva una notevole variabilità nella rilevanza attribuibile alle aree di competenza: le *data-intensive industries* prestano sì una grande attenzione a tematiche basilari come la Data Privacy (78,3%), ma allo stesso modo appaiono molto attente alle aree tematiche emergenti, come Forensic (20%) e CyberSecurity (15%), mentre le *material-intensive industries* sono più sollecitate dalla necessità di garantire l'agilità dei processi di produzione, e quindi esprimono una maggiore attenzione per la Sicurezza Applicativa (31,8%) e la Sicurezza Fisica (29,5%).

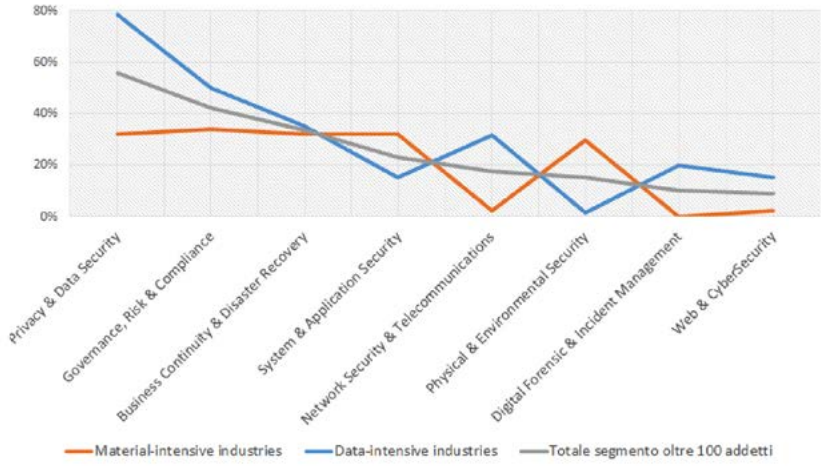


Figura 10 – Competenze di maggiore impatto e difficoltà di reperimento sul mercato.
Fonte: IDC Italia, 2015 (imprese con oltre 100 addetti; estrapolazione all'universo di riferimento)

Conclusioni

A differenza di altri comparti dell'IT, la Sicurezza è vittima di una ambivalenza piuttosto difficile da spiegare: da un lato, risalta in modo sistematico come una priorità essenziale nell'agenda dei CIO, che indicano la Sicurezza come una leve essenziale per edificare qualsiasi altra progettualità del Dipartimento IT; dall'altro lato, non trova riscontro nelle previsioni di spesa IT, ridotte al lumicino da una crisi economica che ha costretto molte imprese italiane a rivedere i modelli organizzativi su cui avevano fatto affidamento negli ultimi anni. Nel momento in cui il budget della Sicurezza si riduce a "una percentuale di una percentuale" diventa lecito interrogarsi in che senso i CIO delle imprese italiane intendano portare avanti le proprie priorità.

Da diverse indagini di IDC risultano evidenze che una parte importante dei processi di trasformazione digitale che molte imprese stanno intraprendendo fanno necessario affidamento su una risoluzione decisa del tema della Sicurezza IT. Nel momento in cui una parte del core business viene articolata attraverso canali digitali, il management prende immediatamente coscienza dell'esistenza di uno specifico rischio IT che può incidere in misura devastante sui risultati aziendali come qualsiasi altro rischio ambientale. Fino a quando l'IT era considerato soltanto una funzione di supporto, il rischio non era affatto contemplato, ma nel momento in cui l'IT diventa un fattore competitivo, comincia a farsi strada la consapevolezza di essere pericolosamente esposti, e talvolta drammaticamente impreparati.

La Sicurezza è soprattutto il combinato disposto di fattori eterogenei, di cui la tecnologia rappresenta, per quanto importante, soltanto una parte. La Sicurezza sta dentro la testa del Security Manager, laddove esiste una figura specializzata, oppure dentro la testa dell'IT Manager, come retropensiero tra le altre incombenze. Eppure, nel momento in cui la Sicurezza diventa soltanto la responsabilità di un ruolo aziendale occorre interrogarsi quanto l'azienda nel suo complesso sia effettivamente al sicuro. Perché ovviamente la Sicurezza non può essere la responsabilità di un singolo individuo ma dipende necessariamente dai comportamenti quotidiani di coloro che ruotano dentro e fuori il perimetro aziendale, i dipendenti, i partner commerciali, i clienti, etc. Da questo punto di vista, la Sicurezza IT è tanto un sistema di soluzioni e tecnologie quanto una consapevolezza organizzata e organizzativa. Per fare crescere il "sistema" della Sicurezza occorre lavorare anche sotto il profilo della cultura, in modo tale da formare un senso critico più oggettivo per valutare comportamenti, tecnologie e situazioni nella prospettiva di un mondo che cambia sempre più velocemente e diventa sempre più complesso.

Anche gli operatori del settore possono assumere un ruolo più importante nello sviluppo di una cultura del rischio IT. In modo particolare, oltre a rispondere alle peculiari esigenze dei singoli clienti, devono sviluppare proposizioni commerciali ancora più articolate per recepire le differenze sostanziali tra *material-intensive industries* e *data-intensive industries*, devono andare oltre le tradizionali formule di prodotto e servizio per diventare facilitatori di un processo di cambiamento organizzativo che non può che discendere da una nuova cultura aziendale e una rinnovata consapevolezza del rischio IT che sta emergendo sui mercati internazionali.

Rapporto Clusit 2016 – FOCUS ON

Questa sezione del Rapporto 2016 è dedicata a delle aree di particolare rilevanza per la sicurezza ICT in Italia.
Abbiamo chiesto ad alcuni dei maggiori esperti italiani, nelle singole materie, di approfondire i seguenti temi:

- **Assicurare il rischio informatico.** La pervasività delle tecnologie ICT e di Internet, rende necessaria un'attenta rilettura delle polizze tradizionali e la loro integrazione ragionata con le Polizze Cyber. Infatti, una polizza adeguata ai tempi, deve prevedere coperture in ambito materiale e immateriale, ovvero tener conto di rischi che si riferiscono al livello fisico come a quello logico e ai loro effetti. [Con il contribuito di CHUBB e Margas]

- **E-Commerce.** Per stimolare lo sviluppo del commercio elettronico nel nostro Paese è indispensabile innalzare il livello di sicurezza dell'intero sistema. Questo Focus On ne evidenzia le criticità ed indica la strada da seguire perché il consumatore possa ottenere maggiori garanzie e fiducia nello svolgimento degli acquisti on-line.
  [A cura di @Mediaservice.net e Netcomm]

- **Il furto di credenziali: fattori di rischio e linee guida per la sicurezza delle aziende italiane.**
  Il furto di credenziali rappresenta una categoria di attacchi estremamente rilevante e pericolosa. In questo capitolo si danno delle indicazioni utili per la prevenzione e mitigazione del furto di credenziali e per evitare che la compromissione di un sistema aziendale di valore limitato si traduca in una compromissione completa dell'infrastruttura aziendale.
  [A cura di Microsoft]

- **Dalla Sicurezza Informatica alla Protezione aziendale: nuovi modelli di prevenzione e di gestione degli incidenti.** L'asset da proteggere (dai device ai dati) è sempre più liquido e spesso esterno al perimetro strettamente aziendale. La comprensione e l'intercettazione delle minacce, delle vulnerabilità o degli attacchi richiede quindi nuove capacità cognitive, legate a insiemi complessi di eventi (comportamenti) più che a specifiche e riconoscibili impronte (eventi, pattern) preventivamente censite. [A cura di Hewlett Packard Enterprise]

- **Le nuove sfide nel campo della Robotica: la sicurezza informatica.** Questo focus affronta il tema della sicurezza informatica, prendendo in considerazione le potenziali vulnerabilità presenti nella robotica rispetto alla criminalità informatica, all'hacking ed agli abusi in generale per quanto riguarda la tecnologia.

Si propone inoltre di stimolare la discussione sulla dimensione legale e sulla regolamentazione generale nel campo della robotica. [A cura di Tech and Law Center]

- **Sicurezza del Database a che punto siamo?** In questo focus on si riportano i risultati delle valutazioni della sicurezza del database in 41 grandi e grandissime aziende dei settori bancari, assicurativi, energia, ingegneria e costruzione, multiutilities, sanità centrale e ospedali, pubblica amministrazione centrale e locale, internet provider e difesa. Si segnalano inoltre i principali errori di gestione del database, comuni a molte aziende. [A cura di Oracle]

- **L'insicurezza è la nuova normalità: prospettive per la Mobile Security (nel 2016).**
  Il panorama delle minacce cresce senza sosta e lascia poche speranze per il 2016. Gli smartphone saranno utilizzati per avvalersi di funzioni ben superiori a quelle offerte dal PC, tra cui i pagamenti tramite NFC. In un'ottica "Smart Working" lo smartphone, a differenza del tablet, è già oggi il gateway per lo scambio di informazioni riservate aziendali e private di ogni singolo utente, il che lo rende un obiettivo più che succulento per i criminali. [A cura di G DATA]

Assicurare il Rischio Informatico

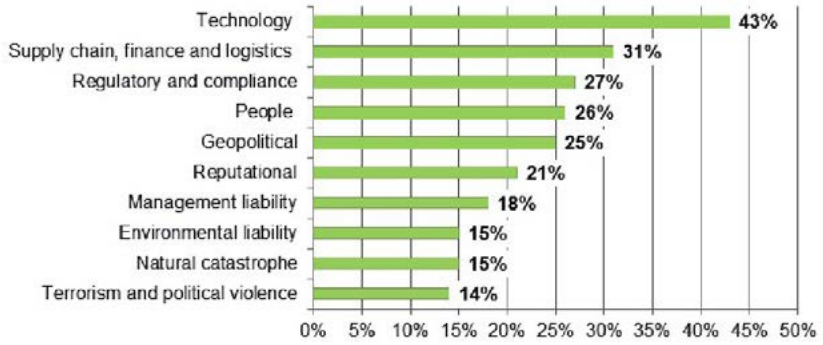
A cura di Alessio Pennasilico, Cesare Burei e Riccardo Scalici

Trasferire il rischio: questa, tra le diverse possibili azioni previste nella gestione di un rischio, è quella che tradizionalmente crea più incertezze quando si parla di sicurezza delle informazioni. Altre funzioni aziendali hanno a disposizione informazioni, know how e strumenti che hanno una lunga storia alle spalle. Assicurare i beni del magazzino o l'edificio da rischi quali furto o incendio è una delle azioni che le aziende compiono da ben prima dell'apparizione degli strumenti informatici. Stimare l'impatto che questi avvenimenti possono comportare per la gestione delle informazioni e di conseguenza per il business aziendale, è invece molto diverso.

I rischi, infatti, non possono e non devono essere catalogati per *banali colori* come troppo speso si riscontra nei file excel che si trovano compilati nelle aziende. Non esiste un rischio "alto-3-rosso": esiste un rischio da € 3.000.000, € 30.000.000 o € 300.000.000. Ed esistono le relative contromisure.

Calcolare i rischi su base economica è indispensabile per poterli raccontare in modo comprensibile alla Direzione, permettendo di prendere le decisioni strategiche corrette. Diventa poi indispensabile quantificare il rischio per poter discutere con il proprio assicuratore, ad esempio, il massimale della polizza, nel caso in cui si decida di trasferire il rischio.

In questo ultimo caso è bene fare molta attenzione a cosa si assicura e per quali evenienze. Per questo, conoscere le ratio, i contratti e gli algoritmi utilizzati dalle assicurazioni diventa fondamentale. Quasi tutte le aziende posseggono una polizza incendio. Se a bruciare, però, è la sala server, vedersi rifondere il mero valore dell'hardware sarebbe ottenere un indennizzo sul danno subito più lieve. E come assicurare un furto di dati? Come stimare la differenza tra dati finiti in mano ad un concorrente e dati pubblicati su Internet, come sempre più spesso accade? E un attacco DDoS al proprio sito come si assicura?



I rischi per il Business che attualmente preoccupano di più in Europa, Middle East ed Africa. Fonte: ACE Group

Dalla polizza "tradizionale" alla Polizza Cyber

La pervasività delle tecnologie ICT e di Internet, di fatto cervello, sistema cardio-vascolare e linfatico delle aziende, rende necessaria un'attenta rilettura delle polizze tradizionali (All Risk, Incendi, Trasporti…) e la loro integrazione ragionata con le Polizze Cyber. Infatti, una polizza adeguata ai tempi, deve prevedere coperture in ambito materiale e immateriale, ovvero tener conto di rischi che si riferiscono al livello fisico come a quello logico e ai loro effetti. Da non dimenticare il fatto che causa ed effetto (o effetto dell'effetto) possono essere alternativamente di natura "analogica" o "digitale".
Le polizze Cyber presenti oggi sul mercato italiano sono poche e sono piuttosto diverse tra loro: per linguaggio, strutturazione ed ambito d'azione.

Tipicamente ci troveremo davanti ad una serie di sezioni, attivabili o meno, che prenderanno in considerazione:

- **danni** occorsi ai **beni** ICT (macchine) e ai **dati** propri o di Terzi;
- danni legati alla **violazione della Privacy** (dati personali e/o commerciali) propria o di Terzi;
- danni causati dal **crimine informatico** e quelli **da guasto ed errore umano** (di dipendente o Terzi);
- danni che impattano **sull'attività aziendale** (Interruzione di esercizio, richieste di risarcimento da parte di terzi).

Risarcire una serie di **costi** connessi a questi danni, non è sempre previsto dalle polizze tradizionali.
Compreso cos'è il rischio *cyber* e che esso può essere analizzato, mitigato e infine trasferito, e definita la possibilità di coprire i danni e costi propri (*First Party*) o quelli di terzi (*Third Party*), può essere utile comprendere un po' meglio le **tipologie di danni e costi** per decidere se possiamo aver bisogno di una polizza *cyber* e quali caratteristiche questa deve avere per tutelare il mio *business*.

I cyber-danni

Avvalendoci della terminologia e delle definizioni tratte dalle polizze tradizionali, per calarci nel mondo dei danni *cyber*, possiamo distinguere tre grandi famiglie di danni:

1) Danni materiali diretti

Riguardano i danni (distruzione parziale o totale, furto) subiti da beni materiali (un server, la fibra ottica, i PC, un cellulare o altro *device* elettronico) e direttamente causati dall'evento che sarà normalmente di natura "analogica" o tradizionale (incendio, terremoto, fulmine, furto, atto maldestro o doloso, etc.); per la loro natura essi rientrano già nella polizza Incendio, nella polizza Trasporti, nella polizza *All Risks* (che proprio "tutti i rischi" non copre)… e naturalmente nella Polizza storicamente definita "Elettronica". **I danni materiali e diretti possono anche non essere previsti nella Polizza Cyber,** se ho provveduto alla corretta strutturazione delle coperture assicurative tradizionali.

2) Danni materiali indiretti (o consequenziali)

Si tratta ugualmente di danni a beni materiali, ma conseguenza di danni diretti: per esempio, un fenomeno elettrico che abbia danneggiato una scheda, il cui malfunzionamento danneggi a sua volta la macchina di produzione da essa controllata**. I danni materiali indiretti possono rientrare sia nelle polizze tradizionali che nella Cyber, ma vanno esplicitamente inclusi.**

3) Danni immateriali diretti e indiretti

Sono tutti quelli che non riguardano la materialità delle cose assicurate e che sono **conseguenza** di un evento garantito in polizza, anche di tipo *Cyber*.

L'evento dannoso distrugge, compromette l'integrità di un software e/o l'insieme logico di informazioni – ovvero rende indisponibili i miei dati aziendali. Esempi di questa categoria possono essere l'incendio che brucia il server con il suo contenuto informativo, l'involontaria cancellazione di un *database* clienti o ordini, l'azione erronea - anche colposa - da parte di un dipendente addetto alla gestione informatica, l'azione di un *virus* o *malware*.

Le Polizze Cyber risarciscono certamente i costi sostenuti per la sostituzione del software e le operazioni di ripristino o ricostruzione dei dati. Ma se questo non fosse possibile? Chi mi risarcisce il valore del dato perduto?

Quantificare il valore di un database è un'operazione di una certa complessità. In questo senso una **preventiva analisi degli *asset* immaterial**i, l'adozione documentata di tecnologie/procedure per circoscrivere, valorizzare e proteggere quel bene immateriale ed una accurata analisi patrimoniale renderebbe possibile una valorizzazione dell'eventuale danno alla parte logica e dunque la **adeguata personalizzazione della polizza cyber** in ottica di una mitigazione il più efficace possibile del danno subito.

Va ricordato che l'insieme dei danni materiali e immateriali si traduce tipicamente nell'impossibilità di proseguire la normale attività produttiva (informatica e non) per tutto il periodo necessario alla ricostruzione/ripristino dell'infrastruttura ICT, dei software o dei dati. Per questo si annoverano nella categoria dei Danni Immateriali Indiretti anche i **danni da interruzione di esercizio** o *Business Interruption* e cioè la perdita di quote di mercato nel periodo di indennizzo stabilito in polizza, le mancate vendite, la riduzione dell'utile. Su questi danni, non marginali, si innestano **anche maggiori costi per la ripresa dell'attività** o **la persistenza di costi insopprimibili come leasing e stipendi**. Il tutto, se preventivamente analizzato, è assicurativamente trasferibile. Da notare che in Italia le Polizze Danni da Interruzione di Esercizio vengono sottoscritte da appena il 15 % dei titolari di polizze All Risks ed incendio che ad oggi non comprendono gli eventi *cyber*. C'è da augurarsi che l'omonima sezione delle Polizze *Cyber* goda di maggior attenzione.

Dai danni ai costi

Alle classi di danni precedentemente nominate sono intrinsecamente connessi costi e spese di vario genere volte ad indagare le cause, le eventuali responsabilità e a ripristinare lo stato dell'arte; costi che ci aspettiamo siano rimborsati dalla nostra polizza assicurativa, perché è ad essa che appunto abbiamo cercato di trasferire i nostri rischi.

È opportuno ricordare qui, che:

a) la normativa italiana vieta espressamente il rimborso di multe, ammende e sanzioni amministrative. Così può non essere in altri paesi soggetti a differenti legislazioni.

b) certi assicuratori indicano esplicitamente la **conformità alle norme vigenti** (per esempio alla Legge sulla Privacy) e il raggiungimento di **livelli minimi di sicurezza** (tecnologica, procedurale o di in-formazione del personale) anche documentati da piani di *disaster recovery e business continuity*, quali pre-requisiti per la assicurabilità e la liquidabilità. Altri assicuratori intervengono direttamente con propri tecnici per offrire una polizza il più adeguata possibile alle esigenze aziendali.

Vediamo alcuni **esempi di costi o spese** tratte da diverse polizze *cyber* e quelli afferenti in particolare alla sezione/estensione di polizza **Danni Indiretti o *Business Interruption* (BI)**:

Costi tipicamente compresi e rimborsati	Costi tipicamente connessi a *Business Interruption*
Costi per Consulenza	Canoni di affitto
Consulenza di crisi	Canoni leasing
Consulenza per Pubbliche Relazioni	Stipendi dei dipendenti
Consulente di Reazione	Costi per straordinari dei dipendenti
Costi di Difesa	Spese di manodopera legate al ricorso a personale aggiuntivo
Costi di risposta	Impiego di metodi di lavorazione o di produzione alternativi
Spese per Pubbliche Relazioni	Extracosti per lavorazioni/elaborazioni presso Terzi
Costi (spese) per ripristino (dei dati)	
Servizi di pronto intervento informatico	
Spese di Gestione della Crisi	

continua >

Costi tipicamente compresi e rimborsati	Costi tipicamente connessi a *Business Interruption*
Costi di disinstallazione e reinstallazione dei beni assicurati	
Spese per il ricorso a società di servizio esterne	
Spese per il reperimento rapido di materiali	
Spese di guardiania e conservazione dei beni assicurati	
Spese di Ripristino del Sistema Informatico della Società allo stesso livello di funzionalità che esisteva prima di tale Evento di Interruzione dell'Attività; e/o per Ripristinare tecnicamente, recuperare o reinstallare dati o programmi informatici, compreso il costo di acquisto di una licenza software necessaria per riprodurre tali Dati o Programmi Informatici.	

Nel caso specifico della sezione *Business Interruption* ci si occupa di **indennizzare la Perdita di Profitto Lordo** dovuta alla **Riduzione del Volume di Affari** rispetto a quello di riferimento, e a ristorare l'assicurato delle **spese supplementari sostenute al solo scopo di evitare o contenere la riduzione del Volume di Affari** che si sarebbe verificata a causa del Sinistro.

Cyber-Sinistro, quanto mi costi? Esempi tratti dal mondo reale

Nei casi presi in considerazione e forniti dalle Assicurazioni, vengono esplicitati alcuni parametri considerati significativi: la Causa (Informatica, Errore Umano, Dolosa, …), il Tempo di ripristino (parziale o totale dell'operatività di SW, Sistemi, Macchine o dipendenti), i Costi (di ripristino), le Perdite di Profitto e ove possibile la Stima della Perdita di Quote di Mercato relative al periodo d'indennizzo. Ove è indicato: "non risarcibile" si intende che la garanzia non è stata acquistata o perché elemento indicato nelle esclusioni. Altrove è indicato "non risarcibile per sottoassicurazione" ovvero che l'importo assicurato è inferiore al danno subito. Riguardo alla Quota Perdita di mercato (p.es: da danno reputazionale), ove stimabile, si intende che non è risarcibile. Si osserva che frequentemente, per inesperienza, gli assicurati sottostimano ampiamente i Tempi di Ripristino e l'entità del danno.

- **Infezione da Virus nel settore: GDO**; Tempo di ripristino: 10 giorni; costi straordinari (solo rete UE): 0,5Milioni €; perdite di profitto risarcite: 0,6 Milioni e; perdita di mercato stimata massimo 7%
- **Errori dello staff IT Settore: TLC**; Tempo di ripristino: 85 giorni (migliaia di server della Rete); costi straordinari: 1 Milione €; perdite di profitto: non risarcibili perché escluse (stimate 55 milioni €).
- **Errori del personale su macchinario industriale nel settore: Industria**; Tempo di ripristino: 70 giorni; riparazione robot: 20% valore della macchina; costi straordinari: 0,3 Milioni €); perdite di profitto (stimate 2 milioni €), ma non liquidate perché non assicurate.

- **Cyber attack su impianti ancillari datacenter nel settore: Gambling**; Tempo di ripristino: 87 giorni (80 per tempi di ricerca); riparazione SW 85.000 €; perdite di profitto su rete 5.000 negozi (25.000 macchine): 14 Milioni €, risarciti 5 M€ per sottoassicurazione.
- **Logic Bomb nel sistema principale nel settore: Finanziario/Assicurativo**; Tempo di ripristino: 88 giorni parziale; riparazione SW 54.000€; perdita da frode informatica (distrazione fondi): 10 milioni€, non risarciti perché la frode non era assicurata, recupero impossibile.
- **Frode informatica nel settore TLC**; Tempo di ripristino 5 giorni; perdita monetaria da frode 1,5 milioni € (distrazione traffico telefonico), risarcimento 50.000 € per sottoassicurazione, recupero impossibile.
- **Data Breach con frode settore: Event Management**; Tempo di ripristino 3 giorni; perdita da concorrenza sleale: 40% del fatturato gare; nessun risarcimento *Data Base* e BI perché assicurati solo su hardware e ricostruzione archivi (polizza elettronica classica).

Conclusioni

Lo spazio di un focus-on permette solo di introdurre l'argomento stima dei danni e gestione del trasferimento del rischio. Il tema è di grande attualità e la gestione di molti aspetti è ancora oggetto di discussioni strategiche sia nel mondo assicurativo che nel mondo delle aziende.

Come al solito, un certo livello di rischio andrà accettato, o perché davvero accettabile o perché non si può fare diversamente. L'importante è conoscere il problema ed essere consci del come è stato gestito. Per non farsi sorprendere proprio nel momento peggiore, quello dell'emergenza.

E-COMMERCE

A cura di Angelo Chiarot e Marco Ivaldi

Introduzione

"*La sicurezza delle transazioni online e la protezione dei dati personali sono tra le principali preoccupazioni dei consumatori italiani che ancora esitano ad acquistare servizi e prodotti in rete. Per stimolare lo sviluppo del commercio elettronico nel nostro Paese è indispensabile innalzare il livello di sicurezza dell'intero sistema. E questo deve passare non solo da una maggior sicurezza dei siti web e dei sistemi di pagamento, ma anche da una maggior consapevolezza da parte degli utenti sui rischi e sulla necessità di utilizzare in modo responsabile le nuove tecnologie. Questo Focus On, realizzato in collaborazione con il Consorzio Netcomm, rientra tra le iniziative che Netcomm e Clusit hanno deciso di portare avanti a favore degli operatori del settore, delle aziende e dei consumatori (vedi http://clusit.it/docs/comunicato_stampa_netcomm-clusit.pdf).*" (P. Giudice, segretario generale Clusit)

Il commercio elettronico in Italia

Il termine "commercio elettronico" (e-commerce, o il più attuale *net retail*) è utilizzato fin dagli anni '70 per identificare le transazioni commerciali, principalmente costituite dall'invio di ordini d'acquisto, fatture ed altra documentazione in formato elettronico. Per giungere però alla forma che oggi tutti conosciamo si è dovuto attendere l'arrivo del World Wide Web, il quale ha creato le condizioni per l'utilizzo di piattaforme elettroniche via via sempre più evolute che hanno reso semplice, veloce e affidabile l'acquisto a distanza di beni e servizi della più disparata natura. Nella fase pionieristica degli anni '90 il *net retail* sembrava adatto solo alla commercializzazione di taluni prodotti e servizi (in primis, beni immateriali quali software e servizi) e soffriva i conflitti con gli altri canali di vendita e con le problematiche legate alla territorialità, costituendo una percentuale marginale nella totalità delle vendite dell'impresa tradizionale.

Oggi questo canale di commercio veicola una vasta tipologia di prodotti e servizi, anche di pubblica utilità, e costituisce una quota del fatturato complessivo cui le aziende non possono più rinunciare.

Rispetto al resto d'Europa, dove per motivi culturali e per un maggiore impegno dei Governi nel promuovere lo sviluppo del "sistema paese" l'e-commerce ha avuto una penetrazione più veloce e con volumi molto consistenti, in Italia il suo sviluppo è stato più lento e rappresenta un fenomeno dell'ultimo decennio.

Figura 1 – Dati del commercio elettronico in Italia

I dati presentati dall'Osservatorio e-Commerce della School of Management del Politecnico di Milano[1] in collaborazione con Netcomm[2], il Consorzio italiano del commercio elettronico, mostrano una crescita significativa e costante di questo canale.
Dal rapporto stilato con i dati dell'esercizio 2014, oltre alle stime per il 2015, dati relativi alle vendite dei siti italiani verso clienti italiani e stranieri, emergono infatti le seguenti interessanti tendenze[3]:

- Circa 11 milioni di acquirenti abituali che effettuano almeno un acquisto al mese, con una spesa media di circa 1.000 Euro l'anno.
- Un volume di transazioni che nel 2014 si è attestato sui 14.6 miliardi di Euro, con una crescita di circa il 13% rispetto all'anno precedente.
- Una crescita a due cifre anche per il 2015, con un volume di affari stimato che si aggira intorno ai 16.6 miliardi di Euro, cioè circa il 4% del totale delle vendite retail.
- Gli acquisti effettuati con gli smartphone (m-commerce) sono aumentati rispetto al 2014 del 64%, rappresentando circa il 9% dell'e-commerce complessivo. Se integrata con i dati degli acquisti effettuati mediante tablet la percentuale totale raggiunge il 20%.
- Una ripartizione dei beni acquistati costituita per il 70% dalla vendita di prodotti e per il 30% di servizi.
- Tra i prodotti maggiormente acquistati figurano: l'informatica e l'elettronica di consumo (circa il 13%), l'abbigliamento (9%), l'editoria (4%) e il food & wine (3%), che rappresenta

[1] http://www.osservatori.net/ecommerce_b2c

[2] Il Consorzio Netcomm (www.consorzionetcomm.it), costituito nel 2005, nasce con l'obiettivo di favorire la crescita e la diffusione del commercio elettronico in Italia, supportando le imprese nella loro evoluzione digitale a vantaggio dei consumatori e di tutto il sistema paese.

[3] I dati presi in analisi non comprendono al momento l'area dei micro-pagamenti (app store, e-book store, gaming, entertainment on-demand, ecc.) seppur questi stiano gradualmente acquisendo quote di mercato sempre più interessanti.

ad oggi uno dei settori più dinamici del *net retail* italiano.
- Per quanto riguarda i servizi maggiormente richiesti troviamo invece il turismo (circa il 47%, settore con il maggior numero di transazioni), le assicurazioni (7,5%) e altri servizi come ad esempio le ricariche telefoniche, il ticketing on-line, ecc. (5,5%).

Inoltre, con l'evolversi ed il consolidarsi del *net retail,* oltre alle forme di pagamento più tradizionali, gli Istituti bancari, gli Istituti di pagamento, oltre a canali meno ufficiali, hanno reso disponibili servizi e tecnologie per fornire al *consumatore finale* metodologie di pagamento diversificate, sempre più innovative e semplici da utilizzare. In particolare, in ordine crescente di innovazione, sono oggi disponibili o in via di disponibilità le seguenti metodologie di pagamento:

- **Carte di debito e di credito**
  Costituiscono la forma di pagamento più consolidata e utilizzata a livello internazionale. Con la recente introduzione dei Primary Account Number[4] (PAN) anche sulle carte di debito (bancomat) si è aperta la possibilità di utilizzarle anche per le transazioni del *net retail*. In Italia si registra tuttavia ancora una certa riluttanza nell'utilizzare le carte di debito e credito per il pagamento on-line, a favore invece di alcune "nuove" metodologie (ad esempio l'm-commerce), peraltro ancora tecnologicamente immature e che presentano un maggior fattore di rischio. Per completare il quadro, da un documento della Banca d'Italia di recente pubblicazione[5], si evince un cospicuo e costante aumento delle carte di debito (11 milioni in più a partire dal 2008), contro un decremento delle carte di credito, passate dai 16 milioni del 2008 ai 12.2 milioni del 2014. Nonostante la contrazione del numero totale delle carte di credito attive in Italia, l'incremento delle singole operazioni si attesta sui 130 milioni nel medesimo periodo di osservazione (2008-2014).
- **Moneta virtuale e cryptocurrency**
  Nonostante siano spesso associate al "mercato underground" e/o a mercati non propriamente legali, la loro diffusione è relativamente alta. Oltre al più noto Bitcoin, si registrano anche altre principali forme e declinazioni, quali il Litecoin, il Darkcoin, il Peercoin, il Dogecoin ed il Primecoin. Queste "monete"[6] potrebbero anche evolversi ed ottenere consensi più ampi dal mercato in futuro, ma al momento non rappresentano un effettivo riferimento per il *consumatore finale*.

---

[4] Il Primary Account Number (PAN) si compone di una serie di numeri (da 14 a 16) stampigliati sul fronte delle carte di pagamento (debito e credito).

[5] Testo pubblicato nell'ottobre 2015 e consultabile all'indirizzo www.bancaditalia.it/pubblicazioni/sistema-pagamenti/2015-sistema-pagamenti/suppl_56_15.pdf

[6] Per fornire qualche informazione aggiuntiva circa la diffusione di queste "monete", Investopedia.com stima la loro capitalizzazione nel mercato con i seguenti valori: Bitcoin ($ 4,754,296,898), Litecoin ($ 121,860,749), Dogecoin ($ 20,112,825), Peercoin ($ 14,882,010), Darkcoin ($ 11,066,538) e Primecoin ($ 961,543).

- **Dispositivi mobili**
  Seppur le prime forme di m-commerce abbiano visto la luce con l'avvento dei cellulari (era circa la metà degli anni '90), oggi soprattutto tra i più giovani (18-34 anni) questa forma di *net retail* pare destinata a ricavarsi una buona fetta di mercato, tanto che alcune stime prevedono una crescita globale del 42% nel solo 2016. In particolare i pagamenti effettuati tramite dispositivi mobili (m-payment), sia di prossimità (es. NFC) sia remoti, si stanno rapidamente diffondendo anche in Italia.
- **Instant payment**
  Si tratta di una metodologia emergente che consente l'esecuzione dei pagamenti da conto corrente a conto corrente, secondo una logica basata sull'IBAN[7]. Caratteristica principale di questi pagamenti è di rendere immediatamente disponibili i fondi al venditore. Sono numerosi gli Istituti bancari che stanno compiendo investimenti infrastrutturali per consentire all'utenza privata ed aziendale di usufruirne il prima possibile[8].

Lo stato della sicurezza nel settore del Net Retail

Con circa centomila operatori attivi nella vendita via Internet in Italia (*merchant*), la situazione della sicurezza, registrata anche in base alle esperienze maturate in modo trasversale nell'area dei pagamenti elettronici, è molto diversificata.

Se le grandi imprese (quali ad esempio Amazon, E-Bay, Google, ecc.) hanno già integrato da tempo nei processi di vendita i controlli di sicurezza e per la soddisfazione della legislazione vigente, per quelli di dimensione inferiore, fino ad arrivare ai *micro-merchant*, la sicurezza è un aspetto spesso demandato alla cultura del personale interno ed occupa una posizione di secondo piano rispetto al business. Questa condizione è determinata anche dalla difficoltà di integrazione dei controlli di sicurezza (e della compliance, aspetti che per la loro interrelazione appaiono inscindibili) nei processi di vendita e nella percezione comune che questi controlli possano rallentare e ostacolare le attività di business.

Altro elemento che tende a dissuadere l'integrazione di questi controlli è la disponibilità delle imprese a sostenere costi aggiuntivi, quali ad esempio quelli relativi al mantenimento di personale qualificato in materia di sicurezza (interno o esterno che sia) e all'acquisizione delle tecnologie indispensabili per garantire un adeguato livello di controllo.

[7] L'International Bank Account Number (IBAN) è uno standard internazionale utilizzato per identificare univocamente un'utenza bancaria.

[8] Ulteriori informazioni sullo stato degli "instant payment" in Europa sono disponibili sul sito della Banca Centrale Europea, https://www.ecb.europa.eu/paym/retpaym/instant/html/index.en.html

Figura 2 – Andamento della sicurezza in un tipico processo di vendita

Come schematizzato nella **Figura 2**, che vuole rappresentare gli attori tipicamente coinvolti in un processo di vendita on-line, esiste inoltre un ulteriore fenomeno che viene a crearsi in corrispondenza della maggiore distanza, di processo o relazione, dai soggetti regolati. Nello specifico, il livello generale della sicurezza tende a decrescere a mano a mano che ci si allontana dai soggetti, appunto, che per obbligo (regole di settore o del Legislatore) o per volontà (cultura interna o obiettivi di continuità del business) adottano adeguati modelli di regolazione.

Per comprendere meglio questo fenomeno è importante approfondire i ruoli dei soggetti coinvolti:

- **Gli Enti di regolazione e certificazione (1):** sono gli Enti pubblici e privati che impongono le regole di settore (citandone solo alcuni, il Legislatore italiano, la Bank of International Settlement – BIS e la Banca D'Italia per il settore bancario, il Payment Card Industry Security Standard Council – PCI SSC per i pagamenti con carte di debito e credito, ecc.) e gli Enti che attestano e certificano la conformità agli standard di sicurezza e continuità (es. ISO/IEC 27001, PCI DSS, ISO 22301, ma anche il D.Lgs. 231/01). Questi soggetti esercitano un controllo forte sul settore bancario e su quello dei pagamenti (*payment processor*), ma la loro capacità di pressione e controllo tende ad indebolirsi nei confronti dei fornitori di servizi (*service provider*) fino a risultare pressoché inapplicabile al *consumatore finale*.
- **Le banche (2):** sono soggetti vincolati a stringenti regole di settore e del Legislatore in materia di sicurezza, continuità e trasparenza; per rendere ancora più evidente ed oggettiva la loro conformità spesso adottano anche volontariamente standard internazionali per la sicurezza operativa e dei pagamenti. Possiedono generalmente un team interno dedicato alla sicurezza, ma spesso si avvalgono di terze parti per condurre attività specia-

listiche (es. Penetration Test). Questi soggetti tendono a richiedere alla clientela ed alla filiera di complemento al loro business (*payment processor*, *service provider* e *merchant*) le misure da loro stessi intraprese. Se verso i soggetti maggiormente vicini al loro business le pressioni e l'esercizio del controllo sono molto forti (*payment processor*), tendono ad attenuarsi verso gli altri soggetti, quali i *service provider*, fino a diventare talvolta molto deboli nei confronti dei *merchant*.

- **I payment processor (3):** semplificando i flussi che intercorrono tra questi e gli altri attori, sono le parti che si occupano della regolazione dei pagamenti tra i soggetti debitori e creditori nell'ambito del processo di vendita. In generale, presentano una postura matura in materia di sicurezza e continuità, ricevendo l'esercizio del controllo da parte dei soggetti soprastanti (tipicamente *banche* e Legislatore). Come le banche, possiedono generalmente un team interno dedicato alla sicurezza, ma spesso si avvalgono di terze parti per condurre attività specialistiche (es. Penetration Test). Esercitano un dominio piuttosto forte nei confronti dei più rilevanti *service provider* e con difficoltà anche verso i *merchant*.
- **I service provider (4):** sono soggetti che collaborano e/o si interpongono tra i *merchant*, i *payment processor* e spesso anche le *banche,* ricevendo in parte le pressioni generate dal fenomeno di "propagazione di filiera". Tuttavia, visto il loro numero e la loro diversità (in termini di dimensione, tipologia e collocazione), la postura assunta in materia di sicurezza è alquanto eterogenea, spesso demandata alla cultura ed alla tradizione di gestione dei singoli. Escludendo le entità di maggior rilievo, la sicurezza è difficilmente gestita con sistematicità e molte delle attività ad essa relative sono affidate a terze parti specializzate.
- **I merchant (5):** intendendo principalmente con questo termine i venditori di prodotti e servizi on-line, ma includendovi anche tutti i restanti attori che completano il processo di vendita (es. operatori dello stoccaggio e del trasporto delle merci), accettano con difficoltà e riserva le misure di sicurezza dalle quali sono raggiunti per effetto della "propagazione di filiera" e raramente possiedono un team interno dedicato a questa tematica. Inoltre, poiché per molti il *net retail* costituisce ancora un canale "innovativo" (molti vi si sono affacciati solo recentemente), spesso i *merchant* tendono ad assumere un approccio tradizionale nei confronti del *consumatore finale*, cioè quello del punto vendita fisico: lo seguono e lo aiutano nelle fasi decisionali e si prendono cura di tutelare i suoi dati (come ad esempio i dati personali o quelli delle carte di pagamento) per il tempo necessario al completamento dell'acquisto, mediamente tra i dieci e i venticinque minuti per il punto vendita fisico. Questo approccio non può tuttavia essere considerato corretto nel caso specifico del *net retail,* poiché il rapporto con il consumatore non termina una volta perfezionato l'acquisto, ma si estende per tutta la durata di conservazione dei dati che il *consumatore finale* ha fornito al *merchant*. Pertanto, la sicurezza di questi dati, sottoposti peraltro a diversi Provvedimenti del Garante della Privacy, dovrebbe essere prevista per tutto il loro ciclo di vita: dal momento dell'acquisizione al momento della loro distruzione, un lasso di tempo intercorrente tra queste due fasi che può a volte durare anni.

- **Gli utenti/consumatori finali (6):** è tutta la popolazione che effettua sporadicamente o sistematicamente acquisti in rete. In generale, nel momento in cui l'utente ha deciso di acquistare un prodotto, lo stesso non si cura particolarmente dello strumento utilizzato (PC, cellulare, game console, tablet, ecc.) o di verificare che il *merchant* abbia particolari caratteristiche o che adotti le misure di sicurezza necessarie a garantire la sicurezza dei suoi dati. Piuttosto si limita a considerare sicuro un grande brand, sfavorendo (spesso a torto) un brand meno conosciuto e/o a ricercare metodi di pagamento che a parer suo sono più sicuri di una carta di debito o di credito (es. l'acquisto mediante smartphone). Il problema a questo punto è di tipo informativo e culturale, probabilmente legato all'annosa questione della tardiva penetrazione delle tecnologie nella popolazione italiana adulta, quella che ad oggi detiene ancora il vero potere di acquisto.

Ora, traendo le conclusioni sul livello complessivo della sicurezza del *net retail* bisogna fare un ultimo distinguo: la sicurezza del *merchant*, cioè del suo business, e la sicurezza del *consumatore finale*, cioè del suo patrimonio e dei suoi dati.
Per quanto riguarda la sicurezza del business del *merchant,* questa si compone del risultato del livello di sicurezza di tutta la filiera di vendita, ivi incluso il *merchant* stesso. Seppur sostenere una frode, sia essa di grande o piccola entità, possa essere, nel tempo, un fatto fisiologico e superabile, quando il brand ed il prodotto o il servizio trovano affermazione nel mercato, fiducia e affezione nella clientela, il danno reputazionale provocato da tali eventi, se non debitamente contrastato, potrebbe compromettere seriamente la continuità del business. Poiché il raggiungimento di un adeguato livello di sicurezza e continuità del business è il risultato di una responsabilità condivisa tra tutti gli attori in gioco, vi è la convinzione che gli sforzi da compiere per raggiungere questo obiettivo siano ad oggi ancora importanti. In particolare, la sicurezza del *consumatore finale,* ancora abituato a condividere con terzi le proprie credenziali di autenticazione, i dati delle carte di pagamento, spesso indotto a cliccare link pericolosi, a diffondere i propri dati personali (e quelli della propria azienda) all'interno dei social network o di altre piattaforme pubbliche, a trasmettere i dati bancari in chiaro sulla rete, ecc. costituisce una vera e propria sfida culturale che necessita in prima istanza di perseguire un adeguato livello di consapevolezza.

Migliorare la sicurezza dei servizi di Net Retail

L'informazione e la consapevolezza sono alcuni dei temi centrali che il Consorzio Netcomm sta promuovendo tra gli operatori del settore e i consumatori. Il Consorzio, attivo dal 2005, con le numerose iniziative patrocinate costituisce ad oggi l'iniziativa italiana di maggior rilievo nell'ambito del *net retail,* dimostrandosi capace di coinvolgere gli interlocutori istituzionali e l'opinione pubblica.
Inoltre, con l'iniziativa del Sigillo di Netcomm[9], il marchio che attesta l'impegno ad offrire

[9] Il Sigillo, nelle sue declinazioni Business Partner, Netcomm e Netcomm Gold, può essere richiesto dai Merchant e posto sul portale di vendita dopo un processo di verifica, valutazione ed attestazione.

un servizio di qualità, trasparenza e affidabilità, il Consorzio sta premiando i *merchant* virtuosi che dimostrano la stretta osservanza delle regole disposte dal Legislatore e la serietà nella gestione dei rapporti con il consumatore, all'interno di tutto il ciclo di vendita.

Come abbiamo appreso dall'analisi svolta nelle pagine precedenti, il coinvolgimento, l'informazione e la sensibilizzazione di tutte le parti interessate sono elementi determinanti ma non sufficienti per il raggiungimento di un livello adeguato di sicurezza che consenta al consumatore di ottenere maggiori garanzie e fiducia nello svolgimento degli acquisti on-line.
La sicurezza, infatti, si compone di diversi attori, di competenze, esperienze ed azioni che interagiscono con gli aspetti dell'organizzazione aziendale e con tutte le tecnologie utilizzate per l'erogazione dei processi di business. Essa deve essere intesa come un processo continuo, poiché non può prescindere dal considerare l'evoluzione del business, delle tecnologie e delle abitudini di consumo della popolazione.

La sicurezza organizzativa

Migliorare la sicurezza, e quindi ridurre i rischi che incombono sull'impresa, è un obiettivo che per gli aspetti organizzativi si traduce in alcune principali azioni:

- *Conoscere l'Impresa*: lo stile di gestione, il contesto di business, le risorse umane, le informazioni interne e quelle della clientela, gli asset, il perimetro fisico e logico dove si svolgono le attività produttive e di supporto, le difese impiegate e la tipologia di rischi cui si è esposti, dovrebbero essere noti nel dettaglio e gestiti con continuità.
- *Conoscere tutte le parti che si riferiscono all'Impresa:* la corretta identificazione e valutazione delle parti, interne ed esterne, che concorrono al raggiungimento del risultato d'Impresa consentono di evidenziare gli eventuali anelli deboli e la possibile propagazione dei rischi.
- *Conoscere le vulnerabilità e le minacce:* sulla base di dati oggettivi e ciclicamente verificati, si effettuano azioni volte alla determinazione, eliminazione e/o riduzione delle vulnerabilità ed al contrasto delle minacce presenti.
- *Adottare misure pratiche per la sicurezza e la continuità*: selezionando dalle *best practice*[10] e dagli standard di settore[11] i controlli che meglio si adattano alla tipologia di rischi presenti, questi possono essere efficacemente mitigati. I risultati raggiunti, quali riconoscimenti e certificazioni, possono essere inoltre utilizzati quali elementi a valore aggiunto per incrementare la fiducia del consumatore.

[10] In particolare, si fa esplicito riferimento al Cybersecurity Framework (http://www.nist.gov/cyberframework/) e alla Special Publication 800-53 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf) del National Institute of Standards and Technology (NIST) statunitense.

[11] Ad esempio, il già citato Payment Card Industry Data Security Standard (PCI DSS), https://www.pcisecuritystandards.org/

La sicurezza delle tecnologie

L'applicazione delle azioni suggerite relative agli aspetti organizzativi permette di focalizzare e prioritizzare gli sforzi e pone le basi per una corretta gestione dei rischi all'interno dell'impresa. Al fine di incrementare il livello di sicurezza legato alle tecnologie che rendono possibile il *net retail*, limitando l'impatto delle potenziali minacce e rilevando tempestivamente il verificarsi di eventi dannosi o anomali, come già specificato sarà inoltre necessario adottare opportuni controlli derivati dalle *best practice* e dagli standard di settore. Tali controlli sono riconducibili alle seguenti categorie principali di riferimento:

- *Protezioni perimetrali*: controlli legati all'architettura di rete, alla segmentazione, alla protezione delle interconnessioni con terze parti, alla configurazione di firewall, concentratori VPN, router, switch, ecc.
- *Gestione delle configurazioni*: meccanismi di sicurezza relativi all'*hardening* dei sistemi e delle loro componenti, all'applicazione delle patch di sicurezza, alla protezione dal *malware* e al mantenimento dell'integrità.
- *Memorizzazione sicura dei dati*: controlli atti a garantire la protezione dei dati memorizzati, in conformità alla classificazione delle informazioni e alle politiche di *data retention* adottate dall'impresa.
- *Trasmissione sicura dei dati*: controlli atti a garantire la protezione, in termini di riservatezza e integrità, dei dati trasmessi attraverso reti pubbliche o private, *wired* o *wireless*.
- *Sviluppo sicuro del software*: integrazione di pratiche di sicurezza all'interno del Software Development Life Cycle (SDLC) adottato dall'impresa, al fine di garantire la robustezza del software sviluppato internamente o esternamente.
- *Controllo degli accessi*: controlli atti a regolamentare gli accessi, tramite processi di identificazione, autenticazione e autorizzazione degli individui che richiedono l'accesso a risorse protette.
- *Tracciamento delle operazioni*: meccanismi di monitoraggio, tracciamento e allarme, correlazione degli eventi di sicurezza, non ripudio, piattaforme Security Information and Event Management (SIEM) e Security Operations Center (SOC), sistemi di rilevamento delle intrusioni (IDS/IPS) e *honeypot*.
- *Continuità operativa*: meccanismi che implementano l'alta disponibilità per garantire l'erogazione di servizi critici ai fini del business e il rapido ripristino dell'operatività in caso di incidenti, sistemi di backup e Disaster Recovery.
- *Gestione degli incidenti*: Data Forensics & Incident Response (DFIR), stipula di polizze assicurative specifiche per tutelarsi da intrusioni informatiche e *cybercrime* (settore al momento carente, ma in rapida espansione).
- *Verifiche di sicurezza*: pianificazione di audit periodici e di attività di Vulnerability Assessment e Penetration Test, finalizzate al monitoraggio continuo della postura di sicurezza dell'impresa.

Oltre alle misure organizzative e tecnologiche discusse, sarà infine necessario predisporre adeguati controlli per garantire la sicurezza fisica (controllo degli accessi, sorveglianza, ecc.) e del personale (consapevolezza e formazione, verifica dei precedenti penali e controllo delle referenze, ecc.).

Conclusioni

Come si è visto, la situazione della sicurezza nel settore del *net retail* è attualmente molto diversificata. Gli attori coinvolti in un tipico processo di vendita on-line, ognuno dei quali riveste un ruolo determinante ai fini della protezione del patrimonio e dei dati personali dei consumatori finali, spesso adottano approcci differenti che determinano posture di sicurezza non omogenee. In particolare nel caso dei *merchant* di piccole dimensioni, gli sforzi da compiere per raggiungere un adeguato livello di controllo sono ad oggi considerati ancora importanti ed in buona parte incompiuti.

In questo scenario, la sicurezza va intesa come un processo continuo che si compone di diversi attori, di competenze, esperienze ed azioni che interagiscono con gli aspetti dell'organizzazione aziendale e con tutte le tecnologie utilizzate per l'erogazione dei processi di business. Il coinvolgimento, l'informazione e la sensibilizzazione di tutte le parti interessate e l'applicazione delle azioni suggerite derivanti dalle *best practice* e dagli standard di settore rappresentano elementi fondamentali per il raggiungimento di un livello adeguato di sicurezza che consenta al consumatore di ottenere maggiori garanzie e fiducia nello svolgimento degli acquisti on-line.

Il furto di credenziali: fattori di rischio e linee guida per la sicurezza delle aziende italiane

A cura di Andrea Piazza

In un contesto in cui le minacce informatiche vanno crescendo col passare del tempo in frequenza, impatto e sofisticazione, il furto di credenziali rappresenta una categoria di attacchi estremamente rilevante e pericolosa, nella situazione sempre più frequente in cui le stesse credenziali vengono utilizzate per accedere a sistemi differenti per ruolo e importanza nella rete aziendale facendo leva su meccanismi di single sign-on.

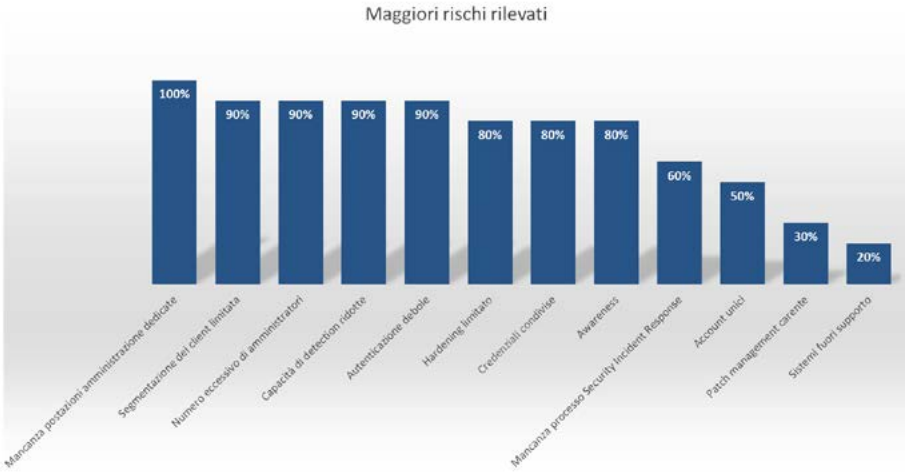
L'estrema pericolosità risiede nel fatto che, a partire dalla compromissione di un singolo sistema (anche di poco valore come la postazione di un utente finale) tramite tecniche classiche di social engineering o di sfruttamento di vulnerabilità note, l'attaccante cattura le credenziali presenti sul sistema compromesso e le riutilizza per accedere a tutti i sistemi dove quelle credenziali sono valide (Lateral Movement), andando a rubare credenziali **sempre più privilegiate** fino ad ottenere per passi successivi il controllo totale dell'infrastruttura (Privilege Escalation).[1]-[2] Queste attività risultano nella maggior parte dei casi inosservate per lungo tempo a causa delle difficoltà di individuazione e rilevamento di questa classe di attacchi, che tipicamente danno luogo sulla rete ad attività del tutto analoghe al normale traffico di autenticazione.

In una situazione in cui il personale IT è numericamente limitato e sotto pressione rispetto alla mole di attività richiesta dal business, nel corso di centinaia di attività di security assessment svolti su aziende italiane negli ultimi 18 mesi abbiamo osservato pratiche di amministrazione che vanno esattamente nella direzione opposta rispetto a quanto sarebbe necessario realizzare, portando a uno scenario in cui tutte le aziende analizzate si sono dimostrate esposte significativamente al rischio di furto di credenziali.

Il grafico seguente mostra in modo qualitativo la percentuale di aziende esposte ai vari fattori di rischio.

[1] Mitigating Pass-the-Hash and Other Credential Theft v1 http://download.microsoft.com/download/7/7/a/77abc5bd-8320-41af-863c-6ecfb10cb4b9/mitigating%20pass-the-hash%20(pth)%20attacks%20and%20other%20credential%20theft%20techniques_english.pdf

[2] Mitigating Pass-the-Hash and Other Credential Theft v2 http://download.microsoft.com/download/7/7/a/77abc5bd-8320-41af-863c-6ecfb10cb4b9/mitigating-pass-the-hash-attacks-and-other-credential-theft-version-2.pdf



Esposizione al rischio di furto di credenziali delle aziende italiane – Fonte: Microsoft Security Assessments 2014-2015

- **Mancanza di postazioni di amministrazione dedicate**: l'uso di Privileged Admin Workstations è pressoché nullo, il modello prevalente è quello che fa uso di sistemi ponte, che non comporta una riduzione del rischio di furto di credenziali.
- **Segmentazione dei client limitata**: raramente vengono limitate le possibilità di movimento laterale tramite la segmentazione di rete dei client.
- **Numero eccessivo di amministratori**: il numero di utenze amministrative è spesso sovradimensionato (decine e in taluni casi centinaia) rispetto alle reali esigenze, aumentando così drasticamente la superficie di attacco esposta al rischio di furto di credenziali privilegiate.
- **Capacità di detection ridotte**: gran parte delle aziende utilizza strumenti di audit e log collection per obiettivi di sola compliance alla normativa del Garante. È raro imbattersi in aziende che effettuano un'analisi proattiva e di correlazione degli eventi volta ad identificare tentativi di compromissione.
- **Autenticazione debole**: un notevole punto di debolezza è rappresentato dall'uso di protocolli di autenticazione deboli, unito all'uso molto limitato dell'autenticazione a due fattori, a volte anche per gli accessi da remoto.
- **Hardening limitato**: il numero di vulnerabilità derivanti da un'errata configurazione dei sistemi è molto elevato, nonostante la presenza di baseline di configurazione sicura pubbliche e validate da fonti autoritative (NIST, CIS).
- **Credenziali condivise**: I sistemi client presentano delle credenziali di amministrazione, definite in fase di installazione iniziale dei sistemi, identiche per tutti i client: la compromissione di un singolo client espone alla compromissione di tutti quelli dove quella

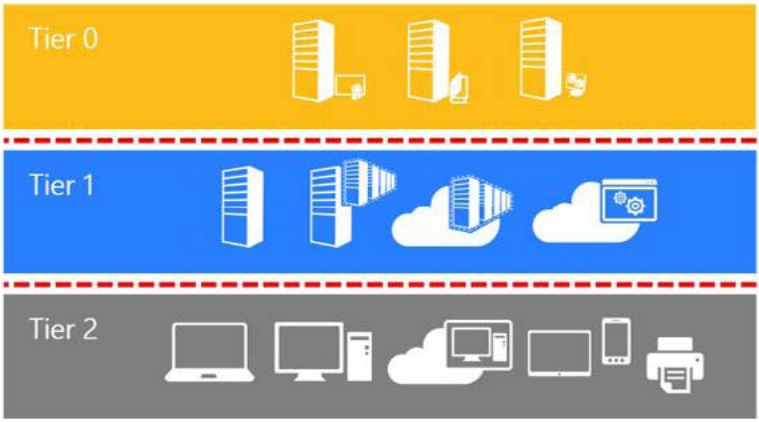
credenziale è definita.

- **Awareness**: il livello di conoscenza e sensibilità rispetto a questa classe di attacchi è in crescita, ma manca la consapevolezza delle misure più efficaci alla prevenzione e alla detection, anche perché prevale una visione della sicurezza molto focalizzata sulle difese perimetrali e di rete quando, nella realtà che osserviamo quotidianamente, il concetto stesso di perimetro è diventato labile: l'identità è divenuta il nuovo "perimetro".
- **Mancanza di un processo di Security Incident Response**: il processo di gestione degli incidenti di sicurezza è spesso completamente assente o limitato al solo ripristino del servizio, mentre manca la definizione dei processi di comunicazione, di un team dedicato, così come l'analisi dei potenziali impatti dell'incidente.
- **Account unici**: Non è raro imbattersi in amministratori che, con la stessa utenza amministrano i sistemi, accedono a Internet, leggono la posta, svolgono cioè anche le attività che sono comuni agli utenti standard e che espongono le loro credenziali al rischio di compromissione. In uno scenario di questo tipo è sufficiente accedere ad un sito internet compromesso o aprire l'allegato di posta sbagliato per mettere a rischio l'intera infrastruttura aziendale.
- **Patch management carente**: gli aggiornamenti delle componenti applicative, spesso resi impossibili da vincoli di compatibilità con applicazioni Line of Business, così come l'aggiornamento dei sistemi server, risultano poco frequenti.
- **Sistemi fuori supporto**: in diverse realtà è ancora numerosa la presenza di sistemi obsoleti, non più aggiornabili, e le cui caratteristiche hardware bloccano la possibilità di passaggio a un sistema operativo più moderno e sicuro.

Quali sono le attività più efficaci per ridurre il rischio di furto di credenziali? Com'è possibile limitare l'impatto di questo tipo di incidenti?

Esiste un principio che, se rispettato nell'ambito dei processi di amministrazione, aiuta a minimizzare questa tipologia di rischio: "**evitare di esporre credenziali privilegiate su sistemi meno privilegiati e potenzialmente compromessi"**.

In linea generale, sarebbe utile pensare ad una infrastruttura suddivisa in vari livelli (Tier) di privilegio, dove al livello più alto risiedono le utenze e i sistemi maggiormente critici o che contengono le informazioni business critical e al livello più basso le utenze e i sistemi meno privilegiati. In questo modello, un'utenza più privilegiata (livello 0) non deve mai essere usata per collegarsi a sistemi di un livello inferiore (1 o 2). Qualora la stessa persona fisica abbia la necessità di amministrare sistemi di livello differente, è necessario che sia dotata di più utenze, ognuna specifica per il livello da amministrare.



Una conseguenza del principio precedente è che **un utente privilegiato dovrebbe evitare di compiere attività rischiose (come accedere a Internet o leggere la posta elettronica) dalla stessa postazione che usa per fare attività di amministrazione**, in quanto così facendo espone il sistema di amministrazione al rischio di compromissione e al potenziale furto di credenziali privilegiate.

Pertanto **l'amministrazione viene svolta a partire da una macchina sicura, e possibilmente dedicata (Privileged Admin Workstation – PAW)**, ed eventuali attività rischiose sono svolte su un sistema secondario dove vengono esposte solamente credenziali non privilegiate.[3]

Un secondo principio importante è quello di **evitare che sistemi meno privilegiati abbiamo la possibilità di effettuare modifiche su sistemi più privilegiati**. Se ad esempio sono in presenza di un server di livello 0 (privilegio massimo), su cui sono in esecuzione

[3] http://aka.ms/cyberpaw

dei servizi relativi a un sistema di monitoraggio di livello 1, che può eseguire delle attività di amministrazione sul server, sto a tutti gli effetti abbassando il livello di sicurezza del server da 0 a 1. Se sono in presenza di client su cui risultano in esecuzione dei servizi che utilizzano credenziali di livello 0, il livello di sicurezza della mia intera infrastruttura viene ridotto alla sicurezza del sistema più insicuro su cui sono esposte le credenziali di livello 0. È quindi fondamentale individuare i punti in cui le credenziali privilegiate vengono esposte e segmentare logicamente i sistemi tra loro sulla base del livello di privilegio delle credenziali su essi utilizzate.

Nell'implementazione di un'architettura più robusta come sopra descritto, devono essere considerati anche i seguenti strumenti e buone pratiche:

- Strumenti che permettono di definire password casuali per le utenze built-in e di servizio (PIM)[4].
- Di **Just-In-Time-Administration** per limitare nel tempo la validità delle credenziali di amministrazione[5].
- Strumenti e protocolli di amministrazione remota che non espongano le credenziali sul sistema amministrato.
- Segmentare la rete e limitare gli accessi tra sistemi a diversa criticità, limitando così le possibilità di lateral movement.
- L'aggiornamento regolare delle componenti di sistema operativo e delle applicazioni, soprattutto di quelle maggiormente esposte ad attacchi.
- La riduzione al minimo del numero di amministratori di sistema e l'assegnazione dei privilegi minimi per effettuare attività di amministrazione.
- La profilazione corretta delle applicazioni "legacy" al fine di definire una roadmap evolutiva che elimini i vincoli sui sistemi hardware e software.
- L'utilizzo delle funzionalità presenti nelle versioni più recenti del sistema operativo (come l'isolamento delle credenziali in un ambiente virtuale sottostante il sistema operativo, la verifica dell'integrità del codice, la protezione delle macchine virtuali dal loro Host) per ridurre il rischio di furto di credenziali e di esecuzione di codice ostile.
- L'utilizzo di strumenti di detection mirati al riconoscimento del furto di credenziali[6].
- L'uso dell'autenticazione multifattore[7]: è bene notare però come questa misura presenti un'efficacia limitata rispetto alla protezione dal furto di credenziali se non è accompagnata dalle misure precedenti e non deve essere vista come l'unica soluzione da adottare.

Come è possibile individuare se sono in corso attacchi di furto di credenziali di utenze privilegiate?

Il furto di credenziali è una tipologia di attacco di difficile individuazione poiché, in diverse

[4] https://aka.ms/laps

[5] http://aka.ms/PAM; http://aka.ms/azurepim; http://aka.ms/jea

[6] http://aka.ms/ata

[7] http://aka.ms/Passport

fasi dell'attacco, vengono usati strumenti leciti e modalità di accesso del tutto equivalenti al normale processo di autenticazione, cosa che rende estremamente complessa la fase di Detection dell'attacco stesso.
In linea di principio si può affermare che l'individuazione di questi attacchi richiede l'analisi dei comportamenti seguiti durante le attività di autenticazione e di eventuali comportamenti anomali, come ad esempio, se una credenziale privilegiata viene utilizzata a partire da un sistema di un utente finale per fare amministrazione remota di un server sensibile.
Pertanto, oltre all'analisi tradizionale degli eventi di sicurezza, è necessario affiancare la definizione di una baseline di comportamento normale, e la rilevazione degli eventuali scostamenti tramite l'individuazione di particolari "punti di controllo", che possono essere identificati mediante la seguente strategia:

- Identificare e dare priorità agli asset di maggior valore.
- Ragionare come l'avversario:
  - A quali sistemi voglio arrivare?
  - Chi ha accesso amministrativo a quei sistemi?
  - Attraverso la compromissione di quali sistemi posso catturare quelle credenziali?
- Identificare il comportamento normale su questi asset.
- Approfondire gli scostamenti dal comportamento normale:
  - Dove è stata usata una credenziale
  - Quando è stata usata
  - Creazione di una nuova utenza
  - Esecuzione di software non atteso
  - Uso di diverse utenze privilegiate dalla stessa postazione, in un breve lasso di tempo, a partire dalla stessa sessione.

Maggiore è il dettaglio della strategia definita, minore è la complessità del rilevamento: gli eventi di audit tracciati del sistema operativo[8] possono pertanto essere impiegati in modo efficace per individuare la presenza di un attore malevolo che effettua attività di furto di credenziali, monitorando nello specifico gli eventi sopra descritti, anche riutilizzando strumenti già presenti in azienda, come SIEM (security incident & event management platform) e Log Collector.
È chiaro che, aumentando la complessità dell'ambiente, un'analisi di questo tipo richiede strumenti di automazione opportuni e di semplice utilizzo, che siano suscettibili il meno possibile a falsi positivi, e che siano in grado di evidenziare i comportamenti anomali attraverso l'aggregazione di dati relativi al comportamento normale e, tramite attività di machine learning e analytics, l'individuazione degli scostamenti dalla normalità.
Sono nate in quest'ambito soluzioni, classificate come **User and Entity Behavior Analytics (UEBA)9**, che si prefiggono di:

- Minimizzare i tempi di analisi degli eventi di sicurezza.

[8] http://www.nsa.gov/ia/_files/app/Spotting_the_Adversary_with_Windows_Event_Log_Monitoring.pdf

[9] http://www.gartner.com/technology/reprints.do?id=1-2NVC37H&ct=150928&st=sb

- Ridurre il volume di alert e assegnare la corretta priorità agli alert rimanenti.
- Identificare gli attori malevoli.

Questi obiettivi vengono raggiunti attraverso:
- Il monitoraggio delle utenze e di altre entità avvalendosi di varie sorgenti di dati.
- La profilazione e l'individuazione di anomalie con tecniche di machine learning.
- La valutazione delle attività delle utenze e di altre entità per individuare attacchi avanzati.

È intuibile come l'introduzione di strumenti di questo tipo aumenti le capacità di detection delle aziende, andando a ridurre in modo significativo il tempo che intercorre tra la compromissione del primo sistema e la rilevazione dell'attacco da parte dell'azienda; tempo che, allo stato attuale, secondo quanto riportato in diversi studi indipendenti, si aggira nell'ordine dei 250 giorni e, in diversi casi, è nell'ordine degli anni.

Il Cloud come strumento di mitigazione del rischio

Premessa la necessità di mantenere on-premise diverse applicazioni, per tutti quei servizi che oggi rappresentano una "commodity" (SaaS), è possibile sfruttare il Cloud come fattore mitigante demandando a una terza parte (Service Provider) la responsabilità della gestione del servizio e, di conseguenza, la sicurezza.
Sulla base dei risultati degli assessment svolti sul panorama italiano, è evidente come le misure di sicurezza adottate nel cloud siano in grado di migliorare il livello medio di sicurezza di gran parte delle realtà italiane. Rispetto al Credential Theft, possono risultare utili le funzionalità di Multifactor Authentication, gli strumenti di detection degli attacchi e di correlazione di eventi tramite tecniche di Machine Learning, così come, nel caso di SaaS, la possibilità di demandare al provider l'esecuzione delle attività di aggiornamento dei sistemi.
In generale, la necessità per i service provider di assicurare standard di sicurezza elevati che siano in compliance con una varietà di standard e normative fa sì che il livello minimo di sicurezza fornito dai servizi Cloud sia molto più elevato di quello mediamente rilevabile in diverse infrastrutture IT del nostro Paese. Il Cloud può quindi rappresentare un'arma in più nell'arsenale del Security Officer per mitigare certe minacce che non vengono o non possono essere affrontate on-premise, anche per ragioni di costo.

Conclusioni

La prevenzione e mitigazione del furto di credenziali privilegiate deve rientrare tra le priorità del Security Officer e del CIO. È necessario agire per evitare che la compromissione di un sistema aziendale di valore limitato si traduca nel rischio di una compromissione completa dell'infrastruttura aziendale.
La pubblicazione di studi approfonditi sulle modalità di attacco e di linee guida sulle misure più efficaci di prevenzione, la revisione dell'architettura e l'introduzione di nuove tecnologie atte a mitigare il rischio e la disponibilità di soluzioni volte e migliorare il rilevamento degli attacchi, sono fattori che rendono immediatamente possibile l'attuazione di una strategia di mitigazione del rischio efficace.

Dalla Sicurezza Informatica alla Protezione aziendale: nuovi modelli di prevenzione e di gestione degli incidenti

A cura di Federico Santi e Danilo Benedetti

Introduzione

Nell'eterogeneo e fluttuante mondo dell'Information Technology, il mercato della Sicurezza appare in continuo e profondo cambiamento e aumenta la velocità con cui evolvono trend crescenti e decrescenti, tra i quali non mancano fenomeni effimeri e slogan commerciali. Tuttavia, mettendo a fattor comune i diversi scenari che emergono dal settore IT & Security con quanto sta emergendo dai tavoli istituzionali (governativi ed europei) e dalle principali Comunità strategiche di settore, è possibile tracciare un quadro francamente incoraggiante nel quale, finalmente, la Sicurezza, almeno nelle grandi aziende e nelle PMI più illuminate, esce dalla sua confort zone informatica per partecipare alle strategie del top management.

Questa evoluzione si esprime in termini di:

- Governance, come strategia di indirizzo delle politiche di Sicurezza in termini di tutela degli asset-chiave delle organizzazioni, via via sempre più immateriali (processi, organizzazione, utenti interni ed esterni, dati, cittadinanza, ambiente).
- Controllo, come monitoring del corretto disegno e della efficacia ed efficienza del sistema di controllo IT.
- Trasformazione, ovvero delle capacità di continuo aggiustamento correttivo ed evolutivo del sistema di controllo.
- Prevenzione degli attacchi e degli incidenti, intesa come capacità di monitorare trend e comportamenti interni ed esterni alle organizzazioni allo scopo di prevenire la costituzione degli attacchi e soprattutto la realizzazione degli exploit.
- Gestione degli incidenti, come capacità tecnologiche di rilevare tempestivamente l'evento-incidente, filtrarlo rispetto a logiche di analisi in grado di scartare gli eventuali falsi positivi, innescare i processi di comunicazione, escalation e reazione, predisporre i relativi piani di rientro.

Figura 1 – Costo del cybercrime in Italia (fonte: elaborazione HPE su dati Ponemon)

Nell'Industria come nella Pubblica Amministrazione si fa largo una cultura aziendale evoluta nella quale la Sicurezza è percepita nel suo significato più ampio di protezione dell'azienda, in termini di patrimonio infrastrutturale, di asset immateriali, di processi, di dati e di risorse umane.

Questa evoluzione spiega bene l'attuale crescita di attenzione e di investimenti nell'area della Security Intelligence (SOC, CERT) rispetto al tradizionale approccio alla sicurezza perimetrale.

L'asset da proteggere infatti (dai device ai dati) è sempre più liquido e spesso esterno al perimetro strettamente aziendale. La comprensione e l'intercettazione delle minacce, delle vulnerabilità o degli attacchi richiede quindi nuove capacità cognitive, legate a insiemi complessi di eventi (comportamenti) più che a specifiche e riconoscibili impronte (eventi, pattern) preventivamente censite.

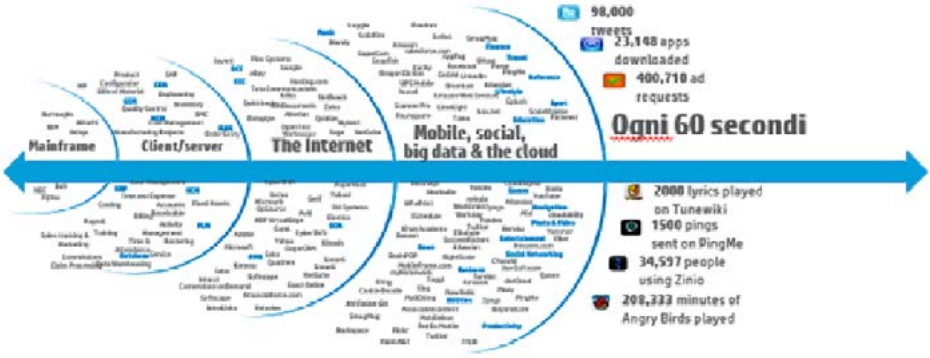


Figura 2 – Evoluzione dei volumi di dati

Tutto questo sposta il focus della protezione non solo in termini spaziali ma anche temporali, estendendo il monitoraggio dalla reazione ad eventi, soprattutto noti, alla prevenzione. Poiché tutto ha un costo è evidente che questo tipo di estensioni comporta la necessità di aumentare la capacità e la velocità di analizzare grossi volumi di dati, spesso destrutturati e provenienti da fonti molto eterogenee, nonché la necessità di sviluppare regole di intelligenza che siano allo stesso tempo non tradizionali, dinamiche e dotate di capacità di autoapprendimento. Da qui, volendo sintetizzare, l'urgenza di investire non solo in neuroni ma anche in sinapsi.

In questo sfidante scenario va quindi ridefinito cosa sia veramente un incidente degno di essere monitorato, gestito ed utilizzato per successivi scopi preventivi. Innanzitutto bisognerebbe trasformare i SOC e i CERT in organizzazioni capaci di espandere le proprie capacità dalla reazione alla prevenzione fino alla resilienza, dedicando un'attenzione nuova ai fattori a monte (fonti, eventi e comportamenti da monitorare) e a valle (catene di comunicazione, CERT esterni).

Tra il monte e la valle, nel bel mezzo dei processi aziendali, appare quindi necessario avviare delle attività di trasformazione che tengano conto delle evoluzioni a cui stiamo assistendo in termini di strategie di attacco e difesa.

I trend di attacco

Gli anni recenti sono stati caratterizzati, in termini di cybersecurity, dall'emergenza di tre macrotrend principali in termini di attacco:

1 L'emergenza degli Stati come sviluppatori e perpetratori di sofisticate strategie di attacco, mirate sia allo spionaggio – industriale o politico – sia a vere e proprie azioni di sabotaggio contro i sistemi critici di stati avversari
2 La "commoditization" di sistemi e meccanismi di attacco, con la possibilità per chiunque di acquisire o noleggiare, attraverso il dark web, "cyber weapon" o infrastrutture tecno-

logiche (botnet) attraverso le quali lanciare attacchi verso le infrastrutture del bersaglio scelto.

3 Il consolidarsi degli attacchi di tipo Advanced Persistent Threat (APT) il cui obiettivo – spionaggio e furto di dati – è supportato da una sofisticata strategia di attacco e mascheramento, il cui scopo è mantenere il più a lungo possibile la propria presenza all'interno dei sistemi attaccati.

A queste tre caratteristiche si affiancherà ben presto una quarta, legata alla diffusione dell'Internet of Things (IOT), ovvero l'aumento esponenziale di oggetti fisici connessi attraverso Internet. Seppur per ora limitate a casi d studio o semplici curiosità, stanno già emergendo dei casi pratici che dovrebbero allarmare sulle possibilità (malevole) future. Per citare solo due casi recenti, i ricercatori di sicurezza hanno evidenziato la possibilità di violare i sistemi di innumerevoli oggetti, dalle bambole Barbie con Wi-Fi ai SUV da due tonnellate. Per il momento non si registrano ancora attacchi malevoli nel mondo reale, ma è opportuno ricordare che una nota marca di auto ha disposto il richiamo di 1,4 milioni di autovetture per eliminare la falla nella sicurezza che, se sfruttata, avrebbe permesso ad un hacker di controllare alcune funzioni chiave della vettura, fra cui i freni e l'accensione – o spegnimento – del motore.

I trend di difesa

Se ci è concesso un parallelo storico, la cybersecurity è sottoposta allo stesso tipo di pressione evolutiva che ha trasformato le vicende militari nel corso del secolo passato. Il concetto di "sicurezza perimetrale" che tanto successo ha riscosso e riscuote tutt'ora in ambito cyber, ricorda da vicino la dottrina dei "fronti" della prima guerra mondiale: linee continue che delimitano quello che è dentro e protetto, da ciò che è fuori ed è insicuro. L'epigono di questa strategia (seppur non l'ultimo esempio) è la tristemente nota linea Maginot. Oggi la cybersecurity si trova in una situazione analoga: i sistemi di protezione perimetrale, sempre più sofisticati ed efficienti, sono comunque esposti all'aggiramento da parte di avversari sufficientemente evoluti, finanziati e determinati.

Con questo non si vuole sostenere che la sicurezza perimetrale sia inutile o superata tout-court, anzi. Però il nostro avviso è che il contrasto a questo tipo di minacce dovrebbe basarsi su tre elementi chiave:

- Il contrasto a più livelli della minaccia attraverso la comprensione delle sue modalità operative.
- La prevenzione attiva, grazie all'acquisizione d informazioni sui trend di attacco più probabili.
- L'adozione di una mentalità – e conseguentemente di un'organizzazione – che consideri sempre presente l'eventualità della violazione.

Il contrasto va nella direzione per così dire "tradizionale" della cybersecurity normalmente intesa, ovvero l'adozione di processi e tecnologie che riducano la vulnerabilità e rendano quindi difficile (e costoso) per un attaccante la violazione dei dati aziendali. Questa visione tradizionale deve però evolvere da una strategia del fronte continuo a quella della difesa in

profondità, per rimanere nell'ambito dei riferimenti alla strategia militare.
In particolare, la difesa in profondità dovrebbe avere come obiettivo quello di contrastare individualmente ciascuna della cinque fasi principali di un moderno attacco cyber, e non limitarsi solo al contrasto dell'attività di infiltrazione come molto spesso ancora accade.

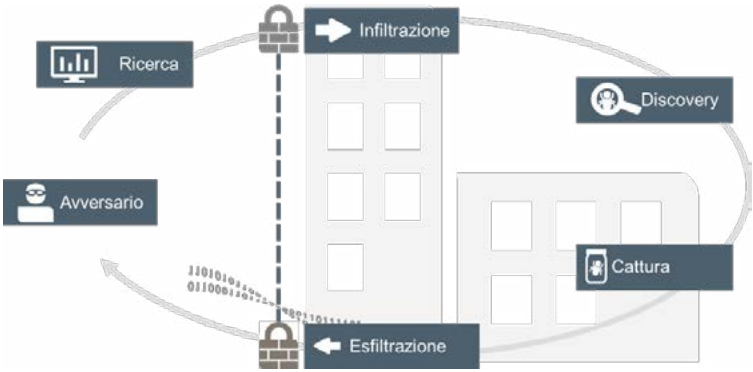


Figura 3 – Le fasi di un attacco tipo Advanced Persistent Threat

Coprendo una ad una le fasi di attacco, abbiamo idealmente le seguenti attività di difesa:
Ricerca - Formazione e intelligence: il modo più efficace per limitare la capacità dell'attaccante è quella di limitare la sua capacità di acquisire informazioni o di sfruttare "il fattore umano" come veicolo inconsapevole di software malevolo. Un'efficace e continua strategia di (in)formazione sui rischi derivanti dall'uso scorretto del web e dei social media e sulle principali strategie di attacco (phishing e spear phishing) può aiutare sia a prevenire il verificarsi di eventi avversi, sia a sviluppare una sensibilità che comporti la veloce segnalazione di ogni fenomeno sospetto. In parallelo, le aziende più esposte possono dotarsi di adeguate capacità di intelligence per anticipare possibili trend e vettori di attacco, ricorrendo sia a fonti pubblicamente disponibili (OSINT – Open Source Intelligence) sia a "sensori" operanti nel dark web, capaci di intercettare l'addensarsi di minacce specifiche o di settore.
Infiltrazione - Protezione perimetrale: Come già detto, la protezione perimetrale, se pure insufficiente da sola a garantire la sicurezza di un'organizzazione, costituisce pur sempre un tassello fondamentale della strategia di cybersecurity. Le scelte tecnologiche ed organizzative devono però essere guidate dall'analisi del rischio e mirare a proteggere principalmente gli obiettivi del business aziendale, non limitarsi all'acquisizione della tecnologia più cool del momento. Inoltre nel costruire le proprie difese vanno considerate attentamente la possibile obsolescenza dei sistemi – che devono dunque essere "agganciati" ad idonei sistemi di aggiornamento per garantire che la propria efficacia non vada riducendosi nel tempo – e la necessità di mantenere attivo un monitoraggio continuo di tali sistemi, per garantire una sollecita indagine di eventi sospetti.

Discovery - Monitoraggio interno: A differenza del fronte continuo, la difesa in profondità prevede che il nemico possa superare la frontiera, e quindi predispone ulteriori sistemi di difesa all'interno del proprio perimetro (firewall interni, segmentazione delle reti, hardening di tutti i sistemi, non solo quelli esposti su internet, controllo accessi, honeypot oltre agli ormai ubiqui Antivirus) e un adeguato sistema di monitoraggio interno che possa identificare comportamenti anomali. In questa fase – e nelle due successive - le aziende dovrebbero anche riflettere sull'opportunità di eseguire scansioni periodiche ed approfondite dei propri sistemi alla ricerca di eventuali "intrusi" che abbiano superato o eluso le difese. Tali analisi superano il tradizionale Penetration test che mira, in una logica tradizionale, a saggiare la difesa dell'organizzazione, perché partono invece dall'ipotesi che la rete sia stata violata e ricercano non vulnerabilità, ma indicatori di compromissione (IOC, indicator of compromise), ovvero evidenze di attività malevole.
Cattura – Protezione del dato: l'accesso al dato deve essere adeguatamente protetto e monitorato, utilizzando ad esempio sistemi crittografici, data masking, sistemi di Data Loss Prevention, e controllo degli accessi al dato. I sistemi per la gestione delle identità e degli accessi devono essere adeguatamente configurati, ed inoltre è necessario prestare particolare attenzione alla efficacia e tempestività del processo di gestione del ciclo di vita delle utenze.
Esfiltrazione – Monitoraggio delle connessioni: la difesa va attualizzata abbandonando l'illusione che l'unico traffico sospetto sia quello proveniente dall'esterno. Sistemi quali i Web Secure Gateway, opportunamente alimentati ed aggiornati con le liste dei server e URL sospetti, possono costituire sia una barriera all'esfiltrazione, sia una fonte informativa circa il verificarsi di comportamenti sospetti (ad esempio l'improvvisa generazione di traffico verso direzioni o indirizzi IP precedentemente non noti).
Tutti questi sistemi devono ovviamente essere costantemente monitorati, per garantire che i comportamenti o eventi anomali siano prontamente individuati ed indagati, al fine di aumentare sia le capacità di prevenzione, sia quelle di rilevamento delle intrusioni. Lo scopo in questo caso è di avere informazioni sufficienti per identificare i comportamenti anomali ed indagarli. Solo in questo modo, infatti, è possibile ridurre il tempo necessario per individuare una violazione di sicurezza, limitando così il danno potenziale.

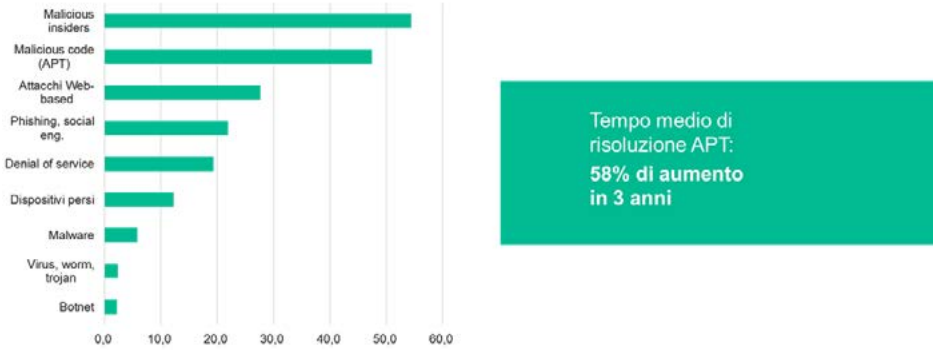


Figura 4 – Tempo medio di risoluzione APT – (Fonte: HPE)

Va inoltre notato che, come chiarito nel capitolo dedicato alla normativa UE sulla privacy, un'adeguata organizzazione ed infrastruttura di monitoraggio diverrà presto necessaria per poter ottemperare all'obbligo di notifica entro 72 ore previsto dalla succitata normativa.

I trend normativi

La Direttiva EU Cyber Security

Dal tavolo delle Infrastrutture Critiche, nato nel 2007/2008, alla futura Direttiva sulla Cybersecurity (2016) il percorso è stato spesso lento e tortuoso.
Tante le difficoltà nel tentativo di mettere a fattor comune diversi schemi nazionali sul tema, diverse esigenze specifiche per le industry e diversi schemi normativi preesistenti.
Questo lavoro di ingegneria normativa è stato avviato nel 2014 dalla Commissione Europea, aprendo un confronto pubblico-privato sul tema, attraverso la piattaforma Network and Information Security nella quale Hewlett Packard Enterprise ha giocato un ruolo molto attivo.
I lavori della piattaforma si sono articolati in 3 gruppi:

- Workgroup 1 - Risk Management
- Workgroup 2 - Information Sharing
- Workgroup 3 - Research and Innovation

A Dicembre 2015 è stato finalmente approvato dal Consiglio d'Europa il testo definitivo della direttiva che ora andrà all'approvazione formale degli organi europei.
Tra gli ostacoli principali lungo il percorso di questa Direttiva ci sentiamo di segnalarne in particolare i seguenti tre:

- La persistenza di una cultura della Sicurezza raggiunta attraverso un isolamento e una scarsa condivisione delle informazioni con analoghi attori. Questa cultura della Security by Obscurity, che impedisce di fruire degli evidenti vantaggi di una condivisione preventiva e reattiva delle informazioni (Information Sharing), rappresenta la principale

dimostrazione del diffuso mediocre livello culturale con cui vengono affrontate le sfide di Sicurezza a livello globale. Questo livello di risposta è in evidente contrasto con la capacità da parte del mondo del Cyber crime di fare associazione (a delinquere), e costituisce uno dei nodi principali che abbiamo cercato di sciogliere con il Gruppo di Lavoro della Commissione Europea dedicato proprio all'Information Sharing.

- La crisi di lungo periodo che ha tagliato gli investimenti su ricerca e innovazione.
- La cronica debolezza del vincolo comunitario che auspichiamo tutti possa trovare un'inversione di rotta di fronte alle sfide sulla Sicurezza, non solo informatica, che questa fase storica ci sta ponendo davanti.

Le misure proposte nel testo approvato comprendono l'obbligo per gli Stati membri dell'UE di adottare una strategia di Network and Information Security (NIS) e designare un'autorità nazionale competente, con risorse adeguate per prevenire, gestire e rispondere ai rischi e incidenti informatici; la creazione di un meccanismo di cooperazione tra gli Stati membri e la Commissione per la condivisione di early warning su rischi e incidenti e per lo scambio di informazioni, ed infine l'obbligo per alcune società e servizi digitali ad adottare pratiche di gestione del rischio e di segnalare prontamente i principali incidenti di sicurezza IT all'autorità nazionale competente.

L'obbligo di segnalare gli incidenti di sicurezza IT si pone come obiettivo quello di contribuire allo sviluppo di una cultura di gestione del rischio e quello di agevolare la condivisione delle informazioni tra settore pubblico e settore privato. Fra gli enti obbligati a dare pronta comunicazione degli incidenti di sicurezza, oltre agli operatori di telecomunicazioni, già normati in tal senso, citiamo:

- Gestori di infrastrutture critiche in settori come i servizi finanziari, i trasporti, l'energia e la salute.
- Società di servizi IT, tra cui ad esempio application store, piattaforme di e-commerce, piattaforme di pagamento internet, piattaforme di cloud computing, motori di ricerca e social network.
- Amministrazioni pubbliche.

La traiettoria sviluppata, seppure con alcuni compromessi di natura volontaristica (piuttosto che obbligatoria) traccia un cammino che mira a cambiare il paradigma della gestione della Sicurezza in Europa.

Il Regolamento EU Privacy

Nel testo recentemente approvato del nuovo Regolamento Europeo sulla Data Privacy spicca innanzitutto il concetto che la Privacy, intesa come protezione dei dati personali, deve essere un parametro di sicurezza opportunamente configurato già in fase di disegno delle soluzioni tecnologiche come dei processi (*Privacy by design*, art. 23).

I controlli quindi devono essere il più possibile:

- Di natura preventiva.
- Dove possibile impostati di default.
- Disegnati nativamente in fase di progettazione.

- Compatibili contemporaneamente con il presidio dei rischi di Sicurezza e con le esigenze di Business.
- Gestiti nell'intero ciclo di vita.
- Trasparenti.
- Concepiti per un uso agevole da parte dell'utente.

Un altro aspetto centrale del Regolamento è la previsione di un obbligo di correlazione tra le misure di Sicurezza ed il *Data Privacy Impact Assessment* (DPIA, art. 30), che prevede in particolare:

- L'implementazione di contromisure di sicurezza con una portata ed una priorità correlata ai risultati del DPIA.
- Una revisione almeno biennale del DPIA.
- Una consultazione preventiva con il Garante per ogni aspetto rilevante.

Altro aspetto dominante della normativa sarà l'obbligo di notificazione tempestiva delle violazioni di confidenzialità sui dati personali (*data breach, art. 31-32*).
Il regolamento prevedrà l'obbligo di notifica al garante ed all'interessato non oltre le 72 ore, prevedendo però un'esenzione da quest'obbligo qualora i dati trafugati non siano decifrabili.
Ulteriori aspetti che rinforzano la struttura della norma saranno:

- La necessità di prevedere un nuovo ruolo nell'Organizzazione, il Data Protection Officer (art. 35), obbligatorio per Pubbliche Amministrazioni e aziende con 5.000+ interessati (data subjects) all'anno e comunque necessario quando si attuano trattamenti di Profilazione e/o ci sono particolari categorie di dati ed interessati.
- Lo stabilimento di un quadro di certificazione dei livelli di Privacy attraverso l'European Data Protection Seal (art. 39), che prevede il rilascio della certificazione da parte del Garante Europeo, con validità di 5 anni, oppure mediante L'utilizzo di terze parti accreditate. La certificazione consentirà una maggiore facilità di trasferimento dei dati all'estero ed un'esenzione da eventuali sanzioni (salvo casi di dolo o grave negligenza).
- La creazione di un European Data Protection Board (art. 64), organismo che assemblerà il Garante Europeo, le Autorità degli stati membri e la Commissione Europea.

L'intero quadro normativo appare infine profondamente rafforzato da una previsione di importanti controlli e sanzioni tra cui il richiamo scritto per la prima non conformità purché non sia intenzionale, l'esecuzione di Audit periodici e regolari ed infine la possibilità di comminare multe proporzionate e dissuasive, fino a 100 milioni di euro o al 5% del fatturato mondiale annuo.

SOC - CERT Intelligence

Nel quadro di trasformazione dell'approccio alla sicurezza, un tassello fondamentale è rappresentato dalla capacità di identificare, reagire e segnalare il verificarsi di attività sospette, attività svolta dai Security Operation Center (SOC) e dai Computer Emergency response Team (CERT).
È dunque evidente la necessità di adeguare, vorremmo dire in via prioritaria, le competenze

e le capacità assegnate a queste organizzazioni, che andranno trasformate per acquisire competenze evolute. Per il SOC si tratta di un'evoluzione verso il cosidetto Next Generation SOC, che dovrà essere aperto a fonti non tradizionali, regole di analysis business oriented e integrato con strumenti di monitoring in grado di analizzare Big Data.
Per il CERT, invece sarà opportuna un'evoluzione che preveda l'integrazione dell'Incident Response Team (IRT) con processi di Information Sharing, coerentemente con le linee guida della Piattaforma Europea NIS – Network and Information Security e con i dettami del Regolamento Europeo della Privacy di prossima attuazione.
In questo quadro evolutivo, un ruolo chiave è rappresentato dalla Cyber Security Intelligence, con gli obiettivi di migliorare l'infrastruttura, aumentare la capacità di prevenire e reagire, incrementare le capacità di resilienza nel tempo.
In questo ambito ci sentiamo di evidenziare la necessità per il mercato di poter accedere a soluzioni di Security Intelligence di eccellenza che inglobino servizi e tecnologia in termini sia di capacità di investigazione/analisi forense/risoluzione di incidenti (Global Incident Response) che di valutazione del livello di maturità della postura di Cyber Security (Advanced Compromise Assessment), eventualmente anche in modalità Managed Security Services.
Le sfide sono molte e complesse ma il tessuto manageriale delle nostre aziende **è** decisamente all'altezza di esse.

I Big Data e l'Artificial Intelligence

Nella sfida rappresentata dai nuovi profili di minaccia di tipo cyber, un elemento che emerge chiaramente è la necessità di raccogliere, correlare ed interpretare moli sempre crescenti di dati, per intercettare quegli eventi che possono indicare un tentativo di compromissione o un attacco già in atto.
Nella progettazione o evoluzione del SOC, dovrebbe quindi essere considerata, fra gli elementi chiave per la valutazione dei prodotto utilizzati, la capacità dei sistemi di raccolta e correlazione dati di integrare prodotti per la gestione e l'analisi di grandi moli di essi (big data).
Tale integrazione va distinta in due macrocategorie: l'integrazione con prodotti capaci di accelerare l'accesso ai database, come nel caso, ad esempio, di database colonnari capaci di aumentare la velocità di accesso ai dati da 50 a 1.000 volte, e che permette di operare con database dell'ordine dei Petabyte, e l'integrazione con dei sistemi capaci di analizzare il contenuto delle informazioni (content analytical engine) che permettono di ricercare specifiche informazioni in fonti di dato non strutturate (chat, conversazioni, video, email).
L'integrazione di queste capacità nel SOC permette di ampliare le possibilità di identificare eventi pericolosi per la sicurezza dei dati aziendali, sia in termini quantitativi – rendendo possibili ricerche su quantità di dati, e dunque numero di sorgenti e intervalli temporali, più elevate – che in termini qualitativi, permettendo di riscontrare violazioni anche in sorgenti non strutturate, che normalmente sfuggono alle competenze di un SOC.
Un passo ulteriore nello sviluppo delle capacità di un SOC è quello di predisporre sistemi in grado di analizzare i dati provenienti dai vari sistemi di sicurezza e raccolti dal SOC, per

identificare eventuali pattern operativi che differiscono in maniera significativa dall'operatività "standard".
Questo è un compito adatto alle nuove generazioni dei sistemi di intelligenza artificiale, come ad esempio le reti neurali "deep learning" già oggi usate per la catalogazione delle immagini o il riconoscimento vocale. Tali sistemi possono imparare a riconoscere, attraverso meccanismi di apprendimento con o senza supervisione, dei parametri operativi "standard" (ad esempio, orario dei login, frequenza di accesso ai dati, sotto-reti relazionali fra utenti e dati e così via). Una volta acquisita questa conoscenza, tali sistemi sono in grado di "osservare" i dati raccolti dal SOC e portare alla luce quelle catene di eventi che potenzialmente indicano un attacco in corso.
L'obiettivo dovrebbe essere quello di disegnare SOC con un elevato livello di automazione, che liberi gli operatori umani, sempre indispensabili, dai task più onerosi affinché possano dedicare più tempo alla indagine di eventi sospetti e alle attività di analisi forense.
Per illustrare meglio le potenzialità offerte dall'analisi di tipo big data e da sistemi di intelligenza artificiale, la tabella seguente mostra le fasi di un tipico attacco APT e i possibili meccanismi di rilevazione.

Fase dell'attacco	Scopo della fase	Metodo di detection potenziale	Fonte di dati necessaria
Fase 1: L'attaccante esegue un attacco spearphishing verso un utente	Compromettere una macchina nella rete bersaglio	Analisi del traffico e-mail per segni di spearphishing	Flusso di e-mail in entrata
Fase 2: L'attaccante ha accesso alla macchina del dipendente	Utilizzare tool per l'analisi di rete e per la raccolta di password	Analisi dei payload in ingress e uscita per identificare download sospetti	Traffico in ingresso/uscita, DNS call
Fase 3: Stabilire un contatto con server CC assegnati dinamicamente	Stabilire una connessione per ricevere istruzioni	Analisi DNS alla ricerca di richieste di risoluzione DNS automatiche	Log DNS
Fase 4: Download di comandi della shell, codificati, per mezzo di HTTP POST	Ricezione delle istruzioni	Analisi dei payload in ingresso ed uscita, per identificare comandi shell nei campi http	Traffico in ingresso/ uscita
Fase 5: Login nel domain controller	Accedere ai nomi utente e agli hash delle password	Analisi del comportamento d'utente all'interno dell'AD, per identificare deviazioni dalla norma.	Log dell'AD
Fase 6: RDP (remote desktop protocol) alle workstation di altri utenti	Spostamenti laterali per poter accedere ad ulteriori informazioni	Analisi del comportamento d'utente delle connessioni MtoM per identificare deviazoni dalla norma	NetFlow

Fase 7: fuoriuscita dei dati	Fuoriuscita dei dati raccolti nella Fase 6 tramite FTP	Analisi del traffic per segni di prelevamento di dati	Traffico in ingresso/ uscita

In questo contesto, va segnalata la disponibilità di numerosi tool di alto livello, quali ad esempio il framework di intelligenza artificiale TensorFlow, rilasciato da Google per libero uso nel 2015, o il potente motore di deep learing sviluppato da Microsoft, CNTK, rilasciato a gennaio 2016. Tali tool possono costituire una efficace "scorciatoia" perché le aziende possano iniziare a sviluppare applicazioni specifiche, in grado di utilizzare i dati pregressi – ad esempio, i log prodotti da sistemi SIEM - per affiancare gli operatori nell'identificazione di quegli eventi che si discostano dai comportamenti di normale operatività.
Si tratta quindi di un potenziale ulteriore passo per evolvere la postura di sicurezza dalla semplice verifica di "signature" di oggetti/eventi malevoli noti verso una sicurezza sempre più preventiva, che è in grado di monitorare ed intercettare comportamenti (Security behavioural analytics).

Conclusioni

L'insieme dei trend di attacco, delle evoluzioni nelle strategie di difesa e la spinta regolatoria che si profila per il 2016, appaiono convergere in maniera coerente verso un diverso utilizzo degli strumenti e delle metodologie di Sicurezza.
Non si tratta per una volta di incoronare una tecnologia miracolosa o un framework particolarmente accattivante, ma di dare uno spessore concreto alle strategie di tutela delle organizzazioni.
Le tecnologie esistono già da tempo e dei framework di Sicurezza bisogna imparare a farne un uso più efficace invece che stravolgerli periodicamente con operazioni di marketing.
Le condizioni ambientali sono quindi favorevoli a investimenti sull'Intelligenza aziendale puntando alla protezione dei beni di maggior valore (materiale e immateriale), più diffusi e più centrali per lo svolgimento delle attività, ovvero i processi, i dati e gli utenti.
Un corretto bilanciamento di competenze, di soluzioni e di tecnologie sono l'obiettivo comune sia delle aziende pubbliche e private sia dei tanti loro fornitori.

Le nuove sfide nel campo della robotica: la sicurezza informatica

A cura di Giuseppe Vaciago e Francesca Bosco

Negli ultimi anni, la proliferazione dell'uso della robotica, sia per scopi civili che militari, ha sollevato una pletora di domande riguardanti la risposta agli incidenti in caso di malfunzionamento del robot intenzionale o accidentale, con conseguenti questioni di responsabilità e di regolamentazione. Questo focus tenta di affrontare il tema della sicurezza informatica, prendendo in considerazione le potenziali vulnerabilità presenti nella robotica rispetto alla criminalità informatica, all'hacking ed gli abusi in generale per quanto riguarda la tecnologia. Si propone inoltre di stimolare la discussione sulla dimensione legale e sulla regolamentazione generale nel campo della robotica.

Introduzione

A meno che l'umanità non riprogetti se stessa cambiando il proprio DNA attraverso l'alterazione del nostro patrimonio genetico, i robot generati dai computer conquisteranno il nostro mondo (Stephen Hawking).

I prossimi anni sono certamente cruciali per l'industria della robotica, per come questi implementeranno, in maniera massiccia, la capacità di produrre robot. Quando questo cambiamento avverrà, i robot saranno sempre più integrati nella nostra vita quotidiana. L'uso di veicoli aerei senza equipaggio (UAV) noti anche come droni, è in aumento sia nel settore militare che in quello civile. Anche se siamo abituati al concetto di droni militari, l'uso commerciale e civile di questa tecnologia è in continua evoluzione. Anche nel settore dei servizi avanza l'automazione, con l'uso non solo di software, ma anche di robot umanoidi, ambito in cui il Giappone sta facendo una sperimentazione concreta e massiccia. Intanto in fabbrica sta prendendo piede una seconda generazione di robot, più intelligenti, più agili, più collaborativi e più adattabili[1]. Nel settore dei trasporti, lo sviluppo di Google Driveless Car e di Apple Carplay, consentono di comprendere il futuro del trasporto privato.

[1] Bloomberg, How to Build Industrial Robots That Don't Kill Humans, disponile all'URL: http://www.bloomberg.com/news/articles/2015-08-25/how-to-build-industrial-robots-that-don-t-kill-humans

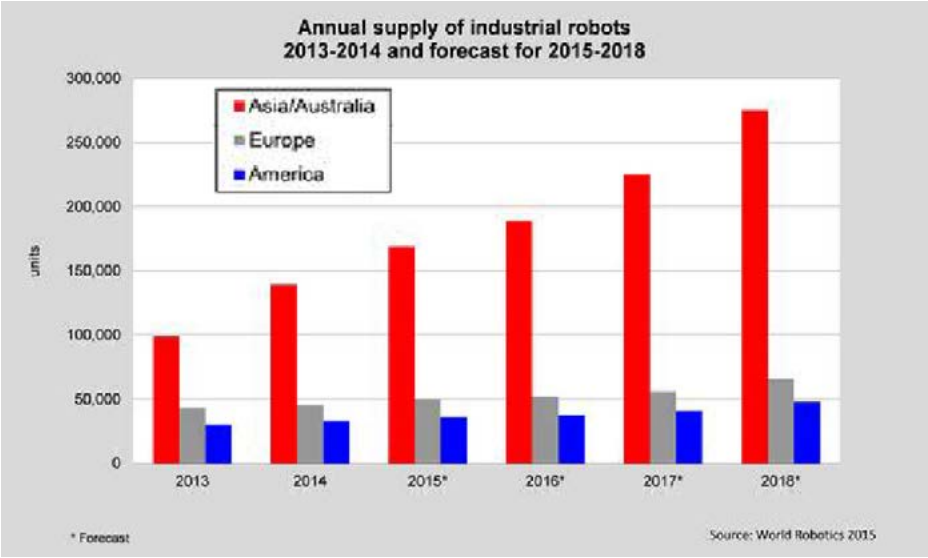


Tavola: I robot installati nel mondo-previsioni fino al 2018. Fonte: IFR-International Federation of Robotics2

Se non vi è alcun dubbio circa l'utilità della robotica in termini di sviluppo dell'innovazione e di crescita economica per i governi o le aziende che stanno progressivamente facendo un ampio uso di essa, meno noti sono i possibili rischi che queste invenzioni possono generare per la comunità. Certamente, l'obiettivo di questo focus non ha a che fare con il tema accattivante e ben esplorato del conflitto tra umani e robot, ma ha quello di evidenziare la mancanza della letteratura scientifica che si occupa specificamente di valutare il modo migliore per prevenire un attacco informatico ad un robot (sicurezza informatica).
I robot hanno tre caratteristiche essenziali: l'interattività, l'autonomia e la capacità di adattamento. Una possibile conseguenza è che le loro azioni possono essere imprevedibili, sia nei confronti dei programmatori e dei costruttori sia nei confronti dei loro proprietari. Il comportamento del robot, anche se attribuibile al software impostato dal programmatore o dal produttore, potrebbe non essere del tutto pianificato nei dettagli specifici in ragione dell'aumento di esperienza fatta dallo stesso robot. Cosa potrebbe accadere se il danno non dovesse derivare da un difetto del robot, ma dal suo comportamento?
A prescindere dalla misura in cui i requisiti di sicurezza previsti dalla legislazione della Comunità Europea (nota come "Machinery Directive")[3] siano soddisfatti dal robot e dal drone, sarebbe opportuno non sottovalutare la sicurezza del sistema operativo o delle applicazioni

2 IFR statistics- World Robotics 2015 Industrial Robots: http://www.ifr.org/industrial-robots/statistics/

3 Direttiva 2006/42/EC relativa alle macchine recepita con il D.Lgs n° 17/2010.

di controllo del robot o del drone e come un potenziale attacco IT contro il loro software potrebbe avere effetti devastanti sul modo in cui operano.
Nei prossimi anni, la sicurezza informatica diventerà sempre più importante nel settore della robotica, dando luogo a ripercussioni legali che saranno certamente interessanti per i "giuristi IT". Vale la pena citare Eugene Spafford, che nel 1989 affermò che: "L'unico sistema veramente sicuro è quello che è stato spento, rinchiuso in un blocco di cemento, sigillato in una stanza le cui pareti sono state schermate con piombo e protette da guardie armate. Ma, anche in questo caso, è altamente improbabile che il sistema sia sicuro[4].
Per questo motivo, non possiamo certo sottovalutare il rischio connesso all'inevitabile e crescente uso di Internet quando si parla di robot e droni, al fine di condividere le informazioni e le istruzioni in tempo reale.
Infatti, nel settore industriale un attacco informatico può significare la completa distruzione di un'intera linea di prodotti o l'interruzione di una linea di montaggio, avendo come risultato enormi danni alla capacità economica e di fabbricazione. Nel settore della robotica, un attacco informatico potrebbe mettere in pericolo la vita delle persone o fornire informazioni strategiche, dando la possibilità ai cyber criminali di commettere atti illeciti.

Sicurezza informatica

L'estrema rapidità con la quale il campo della robotica si è sviluppato nel corso degli ultimi anni, non ha reso difficile ipotizzare gli attacchi informatici che potrebbero sfruttare le vulnerabilità dei sistemi operativi dei robot per scopi illeciti.
Per fornire un esempio concreto di vulnerabilità di sicurezza informatica in questo campo, basta guardare al diffuso utilizzo di droni negli ultimi anni. Un attacco informatico di successo contro un veicolo aereo senza equipaggio potrebbe avere conseguenze mortali.
Come primo esempio, il Parrot AR Drone, progettato per uso civile, è già stato infettato da un malware, chiamato Maldrone, che ha il potere di scollegare i droni dai loro operatori e consente agli hacker di assumere il comando dei sistemi di controllo. Inoltre, attualmente, vi è una grande preoccupazione per la sicurezza dei sistemi GPS dei droni militari e del fatto che possano essere controllati da terze parti. Proprio per questa ragione, alcuni ricercatori della Georgia Institute of Technology e della University of Virginia, hanno sviluppato dispositivi in grado di essere installati sui droni con l'intento di rilevare attività insolita, avviare dei meccanismi di recupero e riferire ai controllori umani se vi è il sospetto di una violazione della sicurezza.
Come altro esempio, sempre relativo ai droni, Todd Humphrey, ricercatore presso l'Università del Texas, ha dimostrato che spendendo $ 1000 era in grado di effettuare lo "spoofing GPS" di un drone civile, prendendo il controllo completo del velivolo. Attraverso questa tecnica di attacco è possibile generare un falso segnale GPS che riesce ad ingannare i sistemi di navigazione più sofisticati usando il segnale malevolo per la triangolazione e quindi il reindirizzamento verso la destinazione desiderata dall'utente malintenzionato. Missy

[4] E. Spafford, citato in Computer Recreations: Of Worms, Viruses and Core War, by A. K. Dewdney in Scientific American, March 1989.

Cummings, professoressa di Aeronautica e Astronautica al MIT, è arrivata alle stesse conclusioni[5].

Nel 2015 ha scatenato un grande dibattito l'esperimento di Charlie Miller e Chris Valášek, che in un ambiente protetto, realizzato ad hoc da Wired US, sono riusciti a prendere il controllo di una Jeep Cherokee lanciata in autostrada a 110 km/h. Attraverso tale attacco, i due ricercatori hanno potuto manovrarne non solo il climatizzatore, l'impianto stereo e il pannello touch, ma anche: tergicristalli, trasmissione, freni e (in retromarcia) sterzo[6]. Per poter avere accesso, hanno sfruttato una falla nel sistema di collegamento a Internet Uconnect rimasta ancora senza rimedio sulla maggior parte dei modelli interessati.

Ci sono più dispositivi per proteggerci contro tali attacchi, ma, ove non dovessero essere efficaci, il potenziale danno può essere assolutamente rilevante: l'hacking dei dati di localizzazione su una macchina rappresenta solo una violazione della privacy, mentre l'hacking del sistema di controllo di una macchina costituisce una minaccia per la vita.

La robotica gioca inoltre un ruolo fondamentale nei sistemi di controllo delle infrastrutture critiche, rendendo un attacco su sistemi di controllo di supervisione e acquisizione dati di un impianto (SCADA) un problema serio per gli analisti di sicurezza informatica, per i policy makers e per le aziende. Come veniva già ampiamente descritto nel report di SANDIA 2005, si era già verificato un numero notevole di incidenti aventi ad oggetto sistemi SCADA:

"Mentre veniva eseguito un ping sweep su una rete SCADA attiva, che controllava un braccio robotico di 3 metri, è stato rilevato che il braccio si attivava autonomamente, ed effettuava una rotazione di circa 180 gradi. Prima dell'avvio del ping sweep, il controller del braccio era in modalità standby. Fortunatamente, la persona nella stanza era al di fuori della portata del braccio"[7].

Gli esempi riportati possono rappresentare casi rari, ma va tenuto presente che diversi studi mostrano che, entro il 2030, ogni famiglia sarà in possesso di un robot e si stima che gli investimenti nel settore della robotica raggiungeranno i 100 miliardi di dollari entro il 2020[8].

Un ultimo esempio molto significativo è il caso Raven II. Nel mese di aprile 2015, un gruppo di ricercatori dell'Università di Washington hanno dimostrato come un malintenzionato può interrompere il comportamento di un Telerobot (chiamato Raven II e sviluppato dallo stesso gruppo di ricercatori) durante un intervento chirurgico e anche prendere il controllo. I ricercatori hanno testato tre diversi tipi di attacchi per determinare la sicurezza del sistema. Il primo attacco cambiava i comandi inviati dall'operatore eliminando, ritardando, o

5 BBC News, Why everyone may have a personal air vehicle, articolo pubblicato il 31 ottobre 2013 e disponibile al seguenteURL:http://www.bbc.com/future/story/20131031-a-flying-car-for-everyone.

6 Wired,

7 SANDIA report (2005), Penetration Testing of Industrial Control Systems, 2005, disponibile al seguente URL: http://energy.sandia.gov/wp/wp-content/gallery/uploads/sand_2005_2846p.pdf

8 New York Times, German Maker of Robots Gains as Chinese Wages Rise, articolo pubblicato il 14 aprile 2014, disponibile al seguente URL:http://www.nytimes.com/2012/04/14/business/global/kuka-german-maker-of-robots-will-expand-in-china.html?_r=0

riordinando gli stessi. Il secondo tipo di attacco modificava l'obiettivo dei segnali da parte dell'operatore, e il terzo attacco consisteva in un dirottamento che prendeva completamente il controllo del robot.[9]

Gli sforzi legislativi dell'Unione Europea

La sicurezza "fisica" è certamente importante, e si ottiene attraverso il rispetto della legislazione nazionale e di quella dell'Unione Europea in materia (nota come "Direttiva Macchine"), ma la sicurezza informatica dei sistemi operativi che controllano i robot e i droni riveste un ruolo altrettanto importante su cui si deve cominciare a riflettere in modo più concreto.

Con riferimento alla decisione quadro 2005/222/GAI e alla direttiva 2013/40/UE in materia di attacchi contro i sistemi informatici, il Parlamento Europeo e il Consiglio d'Europa, nel corso degli ultimi anni, hanno iniziato a delineare una regolamentazione quadro a cui tutti gli Stati membri dovranno conformarsi.

Gli obiettivi della presente direttiva sono quelli di ravvicinare il diritto penale degli Stati membri nel settore degli attacchi contro i sistemi d'informazione, stabilendo norme minime relative alla definizione dei reati e delle sanzioni rilevanti, migliorare la cooperazione fra le autorità competenti, compresi la polizia e gli altri servizi specializzati degli Stati membri incaricati dell'applicazione della legge, nonché le competenti agenzie e gli organismi specializzati dell'Unione, come Eurojust, Europol e il suo Centro europeo per la criminalità informatica, e l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA).

Inoltre, la direttiva 2013/40/UE introduce specifici reati riguardanti l'accesso illecito ai sistemi di informazione (§ 3) e l'interferenza illecita nei sistemi e nei dati (§ 4 e 5). Questi ultimi due sono relativi a qualsiasi azione intrapresa per ostacolare gravemente o interrompere un sistema di informazione mediante l'inserimento di dati informatici, trasmettendo, danneggiando, cancellando, deteriorando, alterando o sopprimendo tali dati.

L'Unione europea ha inoltre presentato il 7 febbraio 2013 una nuova strategia sulla sicurezza informatica che coinvolgerà tutti gli Stati membri, attraverso una "Proposta di Direttiva riguardante le misure volte a garantire un livello elevato e comune di sicurezza delle reti e le informazioni in tutta l'Unione" cd. "NIS Directive" (Directive on Network and Information Security)[10]. Il 7 dicembre 2015, la presidenza del Consiglio dell'UE ha raggiunto un accordo informale con il Parlamento europeo, si attende dunque il testo nella direttiva per il 2016.

---

[9] Technology Review, Security Experts Hack Teleoperated Surgical Robot, aprile 2015, disponibile al seguente URL:http://www.nytimes.com/2012/04/14/business/global/kuka-german-maker-of-robots-will-expand-in-china.html?_r=1&.

[10] Brussels, 7.2.2013 COM(2013) 48 final 2013/0027 (COD) - Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, disponibile al seguente URL: http://eur-lex.europa.eu/procedure/EN/202368

Conclusioni

Mentre alcuni anni fa, il dibattito sulle "leggi della robotica" introdotte da Asimov nel 1940 è stato ad appannaggio esclusivo di filosofi del diritto, al giorno d'oggi è diventato una delle priorità della politica legislativa Europea, la quale, anche se non intende porre freno allo sviluppo economico del settore, sta cominciando a chiedersi se sia necessario adottare una legislazione specifica per il settore della robotica.

Se è vero che una normativa altamente dettagliata del settore potrebbe essere prematura e rischierebbe di ostacolare lo sviluppo tecnologico, per lo stesso motivo, l'attuale mancanza di esecuzione potrebbe, nel medio termine, sollevare dubbi per i potenziali investitori e di conseguenza penalizzare la ricerca scientifica.

Tuttavia, normative ad hoc in determinati settori non devono avere l'effetto di bloccare lo sviluppo di altre applicazioni che potrebbero essere estremamente utili a livello sociale. In sintesi, la regolamentazione della robotica dovrebbe promuovere l'innovazione nel rispetto delle leggi, che certamente avranno un ruolo cruciale nel definire e indirizzare il mercato che si svilupperà nei prossimi anni.

Da questo punto di vista, una possibile forma di regolamentazione dovrebbe essere in grado di coniugare norme giuridiche con le necessità tecniche, in modo da essere in grado di garantire una maggiore capacità di adattamento in casi di particolare complessità tecnica.

Comprendere l'importanza di una normativa in grado di "entrare in un dialogo" con la tecnologia attraverso la creazione di *best practices* e politiche condivise, è il punto di partenza per adeguare la legislazione esistente in materia nel settore della robotica. Lo scopo non è quello di creare allarmismi o di imporre regole supplementari, oltre a quelli già esistenti in questo settore, ma di adattarle al contesto della robotica attraverso l'impiego mirato di strumenti offerti da misure non vincolanti. Ad esempio, la Commissione Europea ha recentemente proposto di fissare nuovi severi standard per regolare il funzionamento dei droni per uso civile con particolare riferimento alla sicurezza, alla privacy, alla protezione dei dati, all'assicurazione e alla responsabilità.[11]

In conclusione, il quadro normativo che disciplina la sicurezza informatica nell'ambito della robotica è di enorme importanza, ma non dovrebbe essere circoscritto alla sola tecnologia. Occorre considerare tutti gli aspetti giuridici correlati. Tra questi, i seguenti sono da considerarsi come priorità:(i) la formalizzazione di regole e procedure per l'acquisizione e l'utilizzo di prove digitali nel rispetto delle *best practices* nazionali e internazionali; (ii) la formalizzazione di regole e procedure che disciplinano la sicurezza informatica che sono in grado di proteggere robot o droni contro possibili attacchi digitali; (iii) il rispetto per la privacy degli utenti che deve essere costantemente bilanciato con le necessità, tipiche della sicurezza informatica, di conservazione e protezione dei dati.

[11] EC COM 2014 (207), "Communication from the Commission to the European Parliament and the Council: A New Era for Aviation, Opening the Aviation Market to the Civil Use of Remotely Piloted Aircraft Systems in a Safe and Sustainable Manner," disponibile al seguente URL:http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014DC0207&from=EN.

Sicurezza del Database: a che punto siamo?

A cura di Alessandro Vallega e Paolo Marchei

E' abbastanza ovvio parlare dell'innovazione tecnologica e dei cambiamenti avvenuti in questi anni in ambito Information Technology. Li abbiamo davanti agli occhi tutti i giorni tanto da non farci più caso, ma per comprendere il caso della Sicurezza del Database è necessario riepilogare alcuni punti:

1. La nostra società, il nostro mondo e le nostre aziende sono iper-connesse; ogni comunicazione passa attraverso la rete ed è soggetta a sfide inedite ed inconcepibili fino a pochi anni fa. La nozione di "Perimetro", sulla quale si basa una concezione tradizionale della sicurezza, veniva nel 2014 abbinata alla parola "quaint" (pittoresco) nel report "Risk and Responsibility in a Hyperconnected World" del World Economic Forum.[1]
2. Scomparendo il Perimetro si devono necessariamente predisporre importanti misure di sicurezza attraverso tutti i livelli (IT layer) dell'infrastruttura tecnologica che realizza i servizi informativi. Bisogna proteggere e monitorare i dati e la loro trasmissione ovunque: nei cosiddetti "endpoint" (dagli smartphone dei collaboratori ai sensori nello stabilimento), sulla rete esterna e interna, nel File System, nelle Applicazioni, nell'Application Server, nel Database Server e nello Storage Server.
3. Bisogna seguire le migliori pratiche di sicurezza, in particolare per quanto riguarda la separazione dei compiti, il principio del privilegio minimo e l'accountability. E' necessario proteggere i dati e le comunicazione tramite encryption e anonimizzazione come ormai ci raccomandano anche le leggi europee e le migliori norme settoriali ed industriali. Infine serve anche agire sul "layer" delle risorse umane. Visto che la tecnologia "fa quello che può" è necessario formare ed informare le persone che operano in modi diversi e a diversi livelli con i Sistemi Informativi. Per esempio è difficile proteggersi quando la password della VPN è stata rubata tramite un attacco di social engineering e quindi a tutti gli effetti una buona strategia include le risorse umane. Inoltre le persone, una volta che siano formate ed informate, possono farsi parte attiva per segnalare potenziali vulnerabilità dei processi e delle tecnologie o delle loro configurazioni.

A fronte di tutte queste considerazioni (iperconnessione, defense in depth, best practice, risorse umane), tre anni fa è stato istituito in Oracle un programma chiamato Security Maturity Evaluation (SME) che ha permesso di valutare la sicurezza del database dell'infrastruttura tecnica ed organizzativa di molte grandi aziende europee.
Il metodo permette di comprendere il livello di maturità aziendale tramite una lunga inter-

[1] Risk and Responsibility in a Hyperconnected World" del World Economic Forum in collaborazione con McKinsey & Company, January 2014 – "The common notion of security implies isolation, the protection of a defined perimeter or an objective defined by the prevention of an event. This notion of security seems quaint in a world where it is impossible to draw a clean ring around the network of one country or one company, and where large organizations can be the target of 10,000 cyberattacks per day." http://bit.ly/RAndRWEF

vista alle persone direttamente coinvolte, esplorando le pratiche, le tecnologie e l'organizzazione preposte alla gestione delle basi dati.

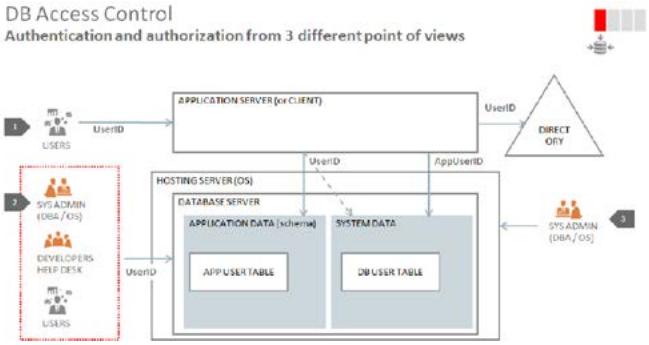
In questo "focus on" si riportano i risultati delle valutazioni di maturità della sicurezza del database e si fanno alcune considerazioni comuni a molte grandi aziende. Purtroppo sarà illustrata una situazione di partenza molto scarsa.

Il campione della nostra ricerca consiste oggi in 41 grandi e grandissime aziende e pubbliche amministrazioni dei settori bancari, assicurativi, energia, ingegneria e costruzione, multiutilities, sanità centrale e ospedali, pubblica amministrazione centrale e locale, internet provider e difesa[2].
L'intervista dura circa 4 ore e si compone di 250 domande organizzate in dominii. Viene fatta a personale selezionato nell'organizzazione aziendale; nello specifico: Responsabile della Security, Responsabile delle Basi Dati, Responsabile delle Applicazioni (ruoli obbligatori) e Rischio IT, Compliance IT e Architetture (ruoli facoltativi). In qualche caso i responsabili sono assistiti da persone più tecniche e/o dai loro outsourcer (infrastruttura o applicazioni).
I dominii dell'intervista sono 6; due sono più generali (Business Context e Technical Context) e 4 più specifici che sono: Database Access Control, Monitoring Blocking and Auditing, Data Protection e infine Secure Configuration.

[2] Il maggior numero sta nel settore delle banche e dell'energia. In un caso abbiamo trattato un centro servizi amministrativi delle forze armate di un paese comunitario (risorse umane e logistica "no weapon"). Non sono ancora completati, alla data corrente (gennaio 2016), i casi di studio relativi alle grandi aziende nel settore delle telecomunicazioni.

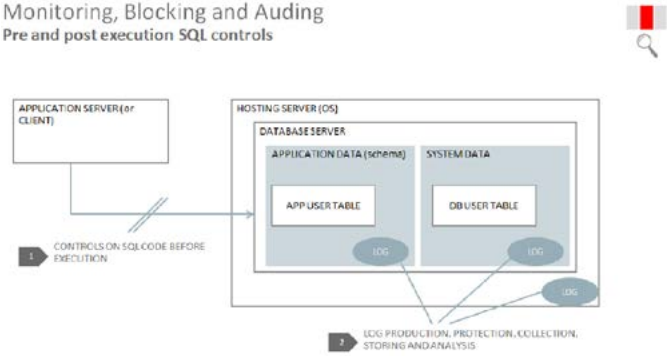
Database Access Control

Le domande relative a questo dominio sono orientate a capire come vengono autenticati ed autorizzati diversi tipi di utilizzatori: gli utenti finali che accedono al DB attraverso le applicazioni, le applicazioni stesse incluso il machine to machine, il personale tecnico come gli amministratori di sistema, i DBA, gli sviluppatori e il personale dell'help desk di secondo livello, gli utenti finali con accesso diretto al database server e infine gli amministratori di sistema dei server che ospitano lo stesso database e il suo storage.



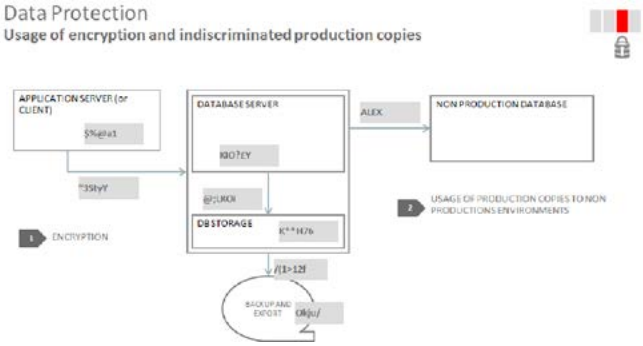
Monitoring Blocking and Auditing

Qui si esplorano i controlli preventivi sull'SQL (prima che raggiunga il database), le traccie che lascia nei log e l'uso che se ne fa (dal log al SIEM, al SOC fino al CERT). Inoltre in questo dominio si trattano anche i temi legati all'audit di compliance, ai controlli di vulnerability assessment / penetration testing e le eventuali policy di programmazione sicura.



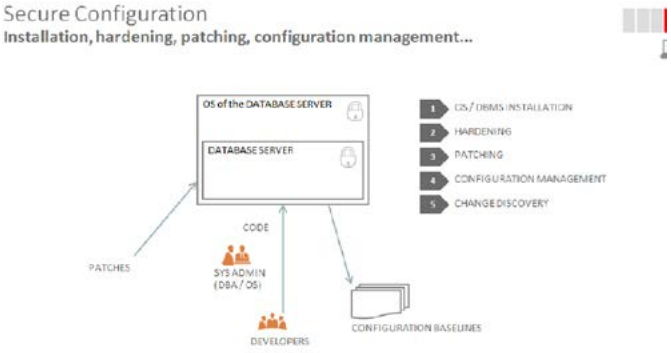
Data Protection

In questo dominio si considera la tematica della protezione del dato tramite encryption (da parte dell'applicazione, della rete tra l'applicazione o il client e il database server, dello storage, dei backup e degli export) e quella relativa all'uso di copie vere dei dati di produzione negli ambienti di sviluppo e test.



Secure Configuration

L'intervista in questa area tratta i temi dell'installazione (del database e del sistema operativo che lo ospita), dell'hardening e del patching. Inoltre policy, controlli e separazione dei compiti nell'ambito del software development life cycle (in particolare i passaggi in produzione) e infine i controlli in merito all'alterazione non autorizzata delle baseline approvate (utenti, privilegi, configurazioni e software eseguibile nel database stesso come package e procedure).



Il livello di maturità

Una parte del report prodotto fornisce una valutazione numerica del livello di maturità dell'azienda nella specifica area (livello "As Is"). Inoltre vengono raccomandate delle azioni atte a rimediare o migliorare le situazioni più gravi o che possano produrre un impatto positivo maggiore con un costo, tempo e rischio di progetto più limitato. Queste azioni, se attuate, potrebbero cambiare il livello di maturità (livello "To Be") e rappresentano in sintesi il livello di maturità che gli esperti consigliano di raggiungere e sui quali i professionisti della stessa azienda concordano.

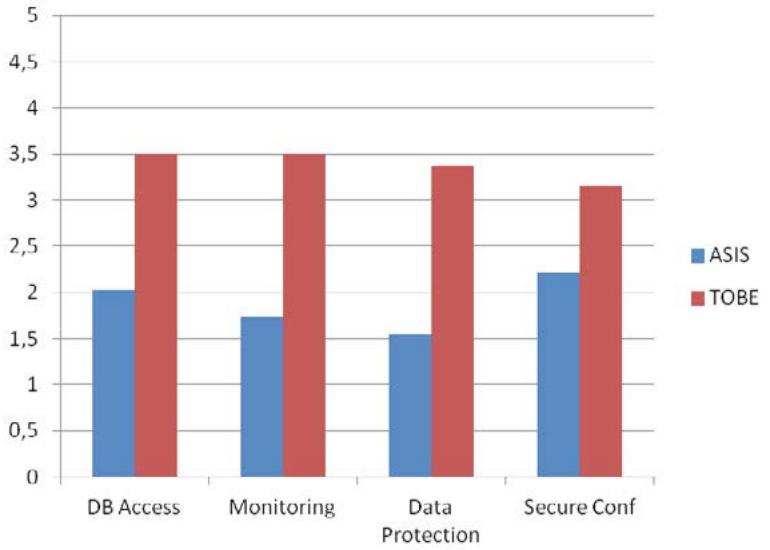


Figura 1: Database Security Maturity level per Knowledge Area; source Oracle SME Methodology

Nella Figura 1 sono riportate le valutazioni "As Is" e "To Be" nelle 4 aree del campione analizzato. Seguono alcuni commenti e precisazioni:

- La scala va da un minimo di 1 al massimo di 5. La valutazione, per motivi di praticità, essendo l'intervista progettata a domanda aperta, è data secondo il giudizio degli esperti senza che si usi un criterio matematico[3]. Le linee guida che si usano sono: il valore "1" rappresenta l'assoluta assenza di misure tecnologiche e organizzative nell'area indicata. Per esemplificare nell'ambito della Data Protection: se i dati sono trasmessi e trattati

[3] Nelle ultime esecuzioni è stato dato uno score automatico usando la tecnica dei Most Common Mistakes presentata in seguito. I dati finora raccolti tendono a fornire dei risultati molto simili.

sempre in chiaro, includendo le password gestite dalle applicazioni; se i dati riservati (ovvero quelli sensibili rispetto ad una violazione di riservatezza per motivi di business o di compliance) sono copiati da produzione a sviluppo; infine, se i sistemi di sviluppo non sono provvisti di misure di sicurezza equiparabili a quelli di produzione viene assegnato il valore "1". All'estremo opposto verrebbe assegnato il valore "5" se fossero stati presi in esame e realizzati tutti i possibili accorgimenti tecnici ed organizzativi; inoltre, se l'organizzazione avesse istituito un processo di retroazione per valutare i risultati delle misure e per migliorarle nel tempo.

- Il campione è limitato; è riferito per lo più a grandi e grandissime aziende ed è eterogeneo rispetto al settore industriale. L'analisi quindi va sempre interpretata con una certa cautela.
- La situazione di partenza, ("As Is") rappresentata tramite le barre blu, rappresenta una situazione molto scarsa, soprattutto rispetto alle aree del Monitoring e della Data Protection.
- C'è accordo tra gli esperti che è necessario migliorare le misure di sicurezza in tutte e quattro le aree. Questo accordo è rappresentato dall'ampio gap tra le barre dell' "As Is" con quelle del "To Be" e confermato da chi scrive osservando le decisioni di investimento e i progetti fatti partire, a valle dell'analisi, per ridurre i "gap".

Most Common Mistakes

Nel condurre le interviste si sono riscontrati degli errori di gestione comuni a molte aziende. Nella tabella seguente se ne riporta la lista unitamente all'informazione relativa alla frequenza di osservazione. Il valore 100% indica il fatto che tutte le aziende analizzate[4] commettono quello specifico errore. Segue una disanima degli errori più gravi nelle quattro aree sopra citate.

Segnaliamo tre errori nell'area del controllo accessi (**Database Access Control**), che si interroga su come vengono autenticati e autorizzati gli utenti (dipendenti, clienti, fornitori) e gli "account" tecnici che accedono al DB:

1. l'uso delle potenti utenze tecniche non nominative da parte degli amministratori del DB
2. privilegi eccessivi dati all'account usato dall'applicazione stessa
3. l'uso di quest'ultimo da parte degli sviluppatori per svolgere i loro compiti di ricerca dei malfunzionamenti, modifica manuale dei dati e del software.

Si violano così i princìpi di sicurezza relativi al privilegio minimo, all'accountability e alla separazione dei compiti di cui si fa un gran parlare.

Nell'area del **Monitoring, Auditing and Blocking** rientrano le pratiche relative al controllo dell'SQL prima che sia eseguito e delle tracce che esso lascia nei log una volta eseguito. Rispetto al primo tema, nonostante tutti i report internazionali documentino numerosi databreach tramite la tecnica della SQL Injection, normalmente le aziende non si dotano di tool per il controllo preventivo a "run time" dell'SQL. Anche rispetto all'auditing e log-

[4] In certi casi, alcuni MCM non sono stati valutati per via di specifiche configurazioni dell'azienda analizzata o delle conoscenze disponibili nel team intervistato.

ging la situazione è carente. Per motivi di superficialità, performance e occupazione di spazio disco, i log sono disattivati oppure, quando sono prodotti, non sono protetti, non sono conservati a lungo e non sono analizzati proattivamente in nessun modo. In pratica si conservano per un po' perchè "non si sa mai". Purtroppo, visto che gli incidenti vengono scoperti tardivamente, spesso sono già stati cancellati nel momento in cui servono ed inoltre, qualora fossero stati prodotti, sarebbero quasi inutili per via della scarsa "accountability" appena spiegata (database access control).

Nell'area della **Data Protection,** che tratta il tema della cifratura e dell'anonimizzazione, si osservano due macro problemi:

1. le aziende non applicano alcuna cifratura al DB, allo storage che lo contiene, alla rete che trasporta i dati verso gli application server e neanche quando si produce un backup o un export che viene spedito in un sito remoto;
2. la consuetudine di copiare il DB di produzione nei sistemi di sviluppo e test per facilitare le attività di programmazione e test. Così facendo si espongono dati sensibili o confidenziali (rispetto al business o alla compliance) ad un ampio pubblico di addetti che in realtà non avrebbe bisogno del dato reale, ma al quale potrebbe bastare un dato fittizio.

Infine per quanto riguarda la **Secure Configuration** si osserva che in ambito server le aziende utilizzano versioni obsolete di sistemi operativi e di DB e tardano ad applicare le patch di sicurezza perchè hanno delle oggettive difficoltà rispetto al fermo dei sistemi di produzione e al rischio di introdurre degli errori di regressione non avendo adeguati strumenti e organizzazione per i test preventivi. Inoltre a volte si lascia che siano gli sviluppatori a portare in produzione le nuove versioni del software, mancando così il criterio della separazione dei compiti. Infine non ci sono controlli per verificare che la configurazione in esercizio non sia stata illecitamente alterata rispetto alla baseline approvata.

Most Common Mistake	**Frequency**
No distinction between Application User and Schema Owner - AC1	68%
Application user credential not protected in the application server - AC2	50%
Developers use application user credential - AC3	16%
DBA do not have personal accounts and use technical accounts - AC4	64%
Technical accounts defined with a human algorithm and never changed - AC5	100%
End users have direct access to the DB bypassing the application - AC6	36%
No lifecycle management for DB users - AC7	50%
OS administrators can escalate their privileges to DBA - AC8	95%
DBA have full access to DML - AC9	95%
No preventive SQL controls - LG1	100%

No or partial and inconsistent logs - LG2	65%
Logs are not analyzed - LG3	91%
Logs are not managed - LG4	64%
No DB user accountability - LG5	64%
No end user accountability - LG6	100%
Applications do not encrypt - DP1	73%
No datafile encryption - DP2	95%
No storage encryption - DP3	91%
No network encryption - DP4	100%
No backup / export encryption - DP5	90%
Production data copied to development environments - DP6	67%
Obsolete DB / OS releases - SC1	59%
No DB / OS hardening - SC2	35%
No patching - SC3	64%
Poor SDLC production promotion and SoD - SC4	65%
No production user, privileges, db objects change control - SC5	100%

Figura 2: Most Common Mistakes; source Oracle Security Maturity Evaluation SME-MCM

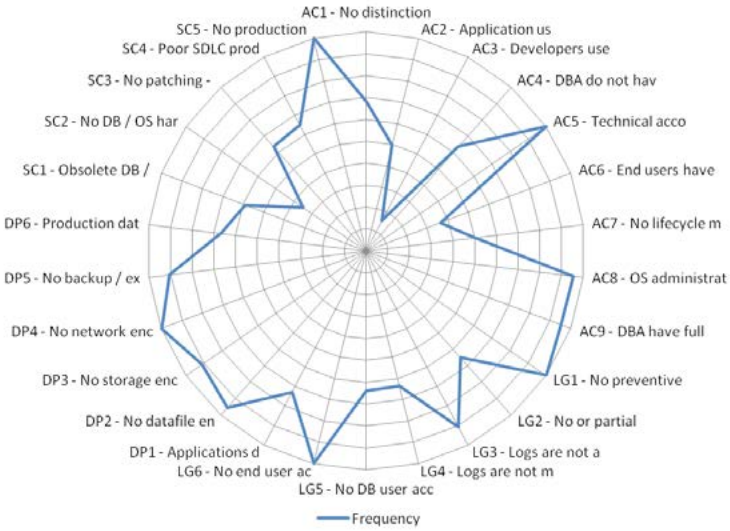


Figura 3: Benchmarking MCM; source Oracle Security Maturity Evaluation SME-MCM

Considerazioni finali

Spesso questi errori hanno radici profonde nella cultura informatica delle aziende e sono legati alla lentezza con la quale le organizzazioni prendono atto delle nuove sfide di sicurezza. **Il problema principale sta nel continuare ad affidarsi all'esistenza di un perimetro che separa in modo netto e definitivo "il dentro dal fuori e i buoni dai cattivi".** Non ci si rende pienamente conto della pervasività dell'IT e che tramite esso si possono commettere ogni genere di errori e subire attacchi molto profondi e pericolosi[5]. La complessità di intervenire sull'organizzazione, l'incapacità di mettere serenamente in dubbio la fedeltà o di discutere della possibile ingenuità o incompetenza dei nostri tecnici interni, collaboratori e outsourcer (ammistratori, sviluppatori, help desk) unitamente al reiterato discorso sul mancato ritorno dell'investimento in security[6], frena fortemente molte iniziative di modernizzazione e lascia le aziende esposte ad un rischio che purtroppo ne potrà compromettere la sopravvivenza.

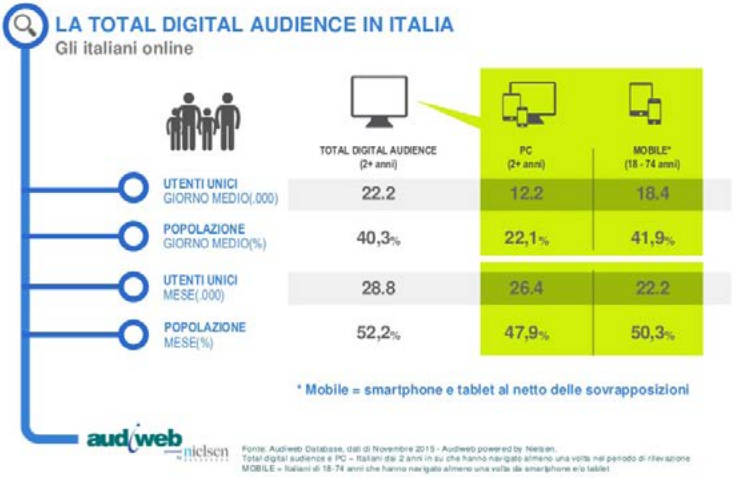
[5] Oltre i Rapporti Clusit che ogni anno alzano il livello di allarme, si segnala a questo proposito un lavoro di Oracle Community for Security sulle Frodi ICT, scaricabile a questo link http://frodi.clusit.it/#/

[6] Sul Ritorno dell'Investimento in Security si segnala una pubblicazione di Oracle Community for Security scaricabile a questo link: http://rosi.clusit.it/#/ e un Focus On presente nel rapporto Clusit precedente, riportato anche qui: http://bit.ly/1nUTE5d

L'insicurezza è la nuova normalità: prospettive per la Mobile Security (nel 2016)

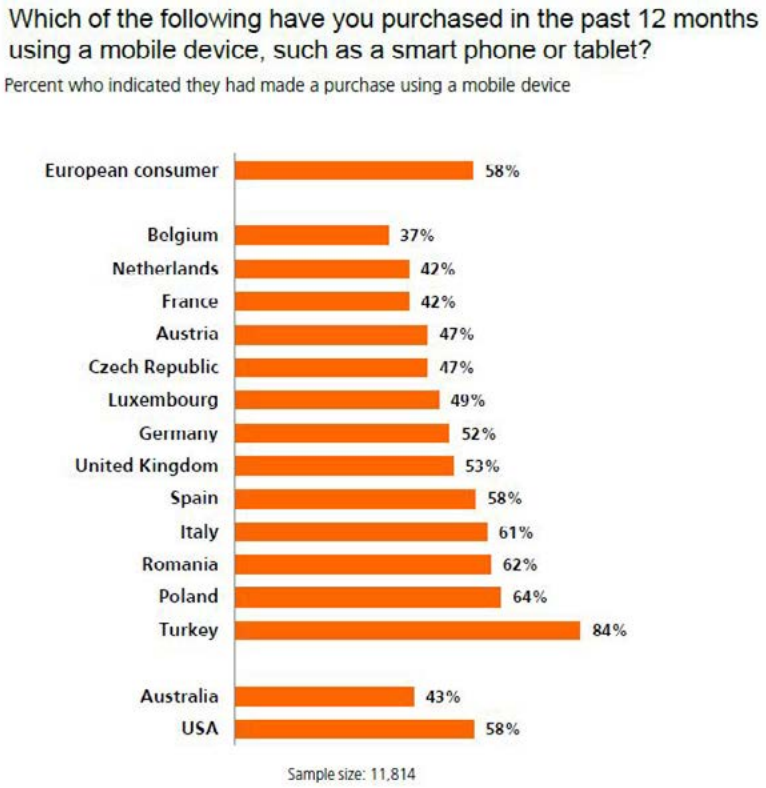
A cura di Marco Landi e Andrea Travaini

Che la mobilità stia rivoluzionando il modo di lavorare degli italiani è un dato di fatto. Strumenti di lavoro imprescindibili nella maggior parte delle aziende e tecnologie abilitanti per lo smart working, smartphone e tablet vengono impiegati da larga parte della popolazione per attività professionali come private, senza discriminare tra dispositivi forniti dall'azienda e quindi soggetti a policy di sicurezza ben precise e uso privato dei dispositivi, all'insegna del BYOD. Ma non solo: secondo audiweb (analisi del novembre 2015) quasi il 42% della popolazione italiana tra i 18 e i 74 anni ha usufruito di un device mobile per connettersi ad internet, un dato che supera di gran lunga la total digital audience del mese (che comprendende PC e utenti di fasce di età ben inferiori) e indice del fatto che le piattaforme mobili stiano scalzando sempre più rapidamente il classico PC nella fruizione di contenuti digitali e nell'espletamento di attività (transazioni, acquisti, vita "digitale") precedentemente riservate al desktop.



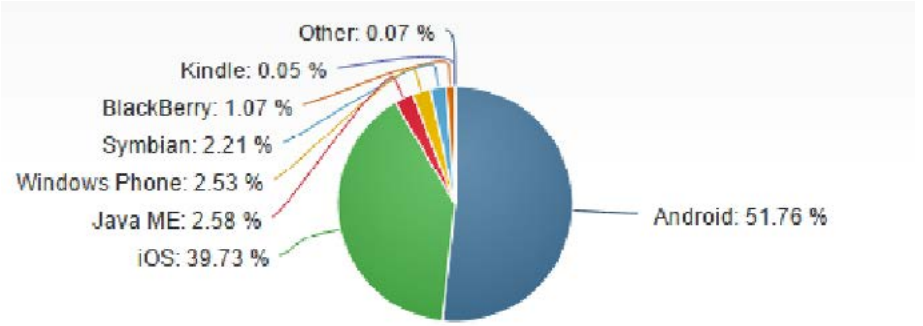
Fonte: audiweb total digital audience novembre 2015: il 41,9% della popolazione italiana tra i 18 e i 74 anni si è collegato ad internet almeno una volta tramite smartphone o tablet.

Lo studio internazionale condotto da ING Direct e pubblicato nel mese di Aprile 2015 conferma questo trend: seppur ancora indietro in termini meramente numerici rispetto ad altri Paesi europei, oltre un terzo degli italiani si avvale già del mobile banking e il 20% conta di farlo nei prossimi mesi. Una quota però irrisoria rispetto alla stragrande maggioranza (61% degli italiani dotati di smartphone o tablet) che ha confermato di aver effettuato acquisti con il proprio smartphone o tablet.



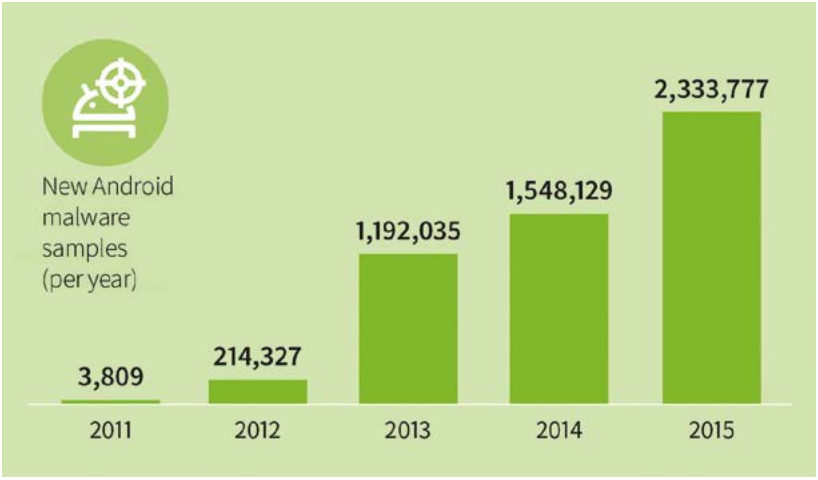
Fonte ING International Survey Aprile 2015: Il 61% degli italiani acquista tramite device mobili.

Entrando nel dettaglio del tipo di smartphone o tablet usato, si riscontra un forte apprezzamento per Android da parte degli utenti su scala globale-



(*Fonte: Netmarketshare 2015*)

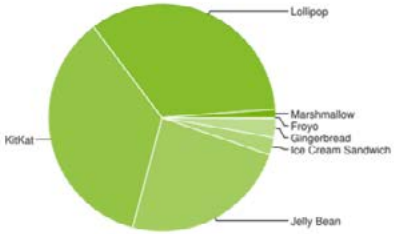
Una preferenza, quella per Android, accordata al sistema operativo anche dai cybercriminali che, in un'impennata di "creatività" senza pari che nel 2015 ci ha regalato quasi un milione di nuovi malware rispetto al biennio 2013/2014, hanno dato vita a oltre 2,3 milioni di nuovi ceppi di malware prodotti ai danni dell'utenza, frutto di una capacità evolutiva con cui le aziende non riescono a tenere il passo, e presa assolutamente sotto gamba dai produttori di device mobili.



Fonte: G DATA Security Labs: numero di nuovi ceppi di malware registrati anno su anno.

Il fattore di vulnerabilità primario di Android è infatti che ad oggi oltre l'80% dei dispositivi presenti un firmware obsoleto, alla mercè dei cybercriminali (cfr. G DATA Mobile Malware Report Q3/2015), la stragrande maggioranza monta ancora Android 4.4 e inferiori.

Version	Codename	API	Distribution
2.2	Froyo	8	0.1%
2.3.3 - 2.3.7	Gingerbread	10	2.7%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	2.5%
4.1.x	Jelly Bean	16	8.8%
4.2.x		17	11.7%
4.3		18	3.4%
4.4	KitKat	19	35.5%
5.0	Lollipop	21	17.0%
5.1		22	17.1%
6.0	Marshmallow	23	1.2%



Fonte: http://developer.android.com/

In questo frangente, è un dato di fatto, che per proprie politiche di prodotto o per difficoltà lato hardware, a quattro mesi dal lancio, Android 6.0 Marshmallow supera di poco una diffusione dell'1%, e che non sia ancora disponibile per la maggior parte dei dispositivi mobili come aggiornamento OTA. Una delle risposte fornite dal mercato libero è la diffusione di aggiornamenti "custom" non ufficiali tramite comunità Android open source. L'esempio più noto, e ritenuto da molti "la salvezza" **è il** progetto CyanogenMod, che per quanto eccellente, corrisponde ad una vera e propria manipolazione del firmware, poiché "sbrandizza" e richiede permessi root sul telefono, mettendolo ancora più a rischio, specie se il terminale in questione è nelle mani di utenti inesperti, che non prestano attenzione alle autorizzazioni richieste dalle app che installano a posteriori del mod. Interessante il fatto che sul blog della community campeggino dallo scorso aprile informazioni fuorvianti in merito alla vulnerabilità di Android, oltre al chiaro invito a non utilizzare antivirus sui device mobili: gli utenti sarebbero "sicuri" avvalendosi di app proposte dagli store ufficiali. L'evidenza quotidiana dimostra che purtroppo non è così e affermazioni simili confermano quella stessa perniciosa assenza di consapevolezza per la sicurezza dei device mobili che riscontriamo in utenti e aziende, favorita anche da grandi nomi della Cybersecurity, che a tutt'oggi si concentrano quasi esclusivamente sulla protezione delle infrastrutture IT in azienda disdegnando il mondo mobile. Una carenza su cui i cybercriminali fanno leva. E' irrisoria la percentuale di utenti italiani che ha dotato il proprio smartphone o tablet di soluzioni antimalware ade-

guate, o che ritiene necessario farlo. Un rischio estremo di esposizione al cybercrimine per le PMI, dove, sebbene sia ormai prassi impiegare lo stesso dispositivo mobile per il lavoro e per la vita personale, solo di rado sono implementate soluzioni per una gestione centralizzata dei device mobili e delle rispettive policy di sicurezza.
Certo, su mobile non abbiamo ancora casi di hack o ransomware clamorosi per diffusione o conseguenze (da non dimenticare comunque il LockerPIN, che bloccava il telefono e chiedeva un riscatto, senza certezza che il PIN venisse effettivamente sbloccato nonostante il pagamento), come quelli che hanno colorito l'annata 2015 su web e PC, ma le minacce all'universo di smartphone, tablet e phablet sono una – purtroppo solida – realtà, e non solo per device Android, di cui abbiamo parlato per l'alta penetrazione di questo sistema operativo sul mercato mobile. Anche iOS non è scevro da vulnerabilità né l'App Store al sicuro da app manipolate. Al contrario il 2015 ha dimostrato che non solo i dispositivi con iOS manipolati dagli utenti (jailbreak) sono soggetti alle più varie forme di malware, ma che anche smartphone e tablet con firmware originale ne subiscono le conseguenze. La differenza tra i dispositivi Apple e gli innumerevoli terminali mobili dotati di Android è che in questo caso abbiamo un singolo produttore che sviluppa il proprio firmware e lo aggiorna con regolarità chiudendo le falle più evidenti. Lo stesso produttore, che acquista con un notevole esborso le competenze degli hacker che producono jailbreak dei firmware o ne rivelano le vulnerabilità, si è accorto però troppo tardi della presenza sul proprio App Store ufficiale di numerose app con codice malevolo create con un Xcode contraffatto e non ha potuto proteggere milioni di utenti dai danni cagionati tramite violazione degli account iCloud. Non ci aspettiamo una diminuzione delle minacce a iOS, tutt'al più un incremento, ora che i criminali sanno come vincere la partita almeno fino alla prossima patch.
Tornando ad Android, il 2015 è stato caratterizzato da smartphone con firmware manipolati di fabbrica o tramite intermediari nella supply chain a scopo di lucro o con app spia per carpire dati riservati di utenti e aziende, da attacchi multipiattaforma (windows/android) sempre più sofisticati per dirottare transazioni bancarie e / o di acquisto su siti illegittimi, da una proliferazione di hacking tools disponibili sul mercato nero (cfr. WhatsApp sniffer – per nominarne uno tra i più innocui -) fino a app che paiono inoffensive ma in realtà richiedono autorizzazioni root sul dispositivo o per funzionalità di sistema non necessarie, tramite cui accedono e trasmettono a ignoti dati personali e – in taluni casi – dirottano la navigazione dell'utente su app e siti illegittimi o sottoscrivono abbonamenti a servizi a pagamento mai richiesti dall'utente. L'ultima frontiera sono app che assicurano di individuare vulnerabilità sul dispositivo avvisandone l'utente ma, per farlo, sfruttano proprio queste falle. Da non dimenticare infine gli innumerevoli casi di scam e phishing tradizionali di cui sono spesso vittime anche gli utenti che utilizzano lo smartphone per leggere la propria posta elettronica, e questo, ovviamente, indistintamente su tutti i dispositivi mobili, non solo gli Android.
Sebbene il panorama delle minacce per smartphone sia particolarmente ampio e cresca senza sosta, ancora pochi produttori di dispositivi e aziende di cybersecurity se ne occupano attivamente, non li biasimiamo però, perché il "business case" viene creato dalla domanda, e la domanda non c'è, o meglio, non è ancora numericamente rilevante.

Uno status quo che lascia poche speranze per il 2016, soprattutto alla luce del fatto che gli smartphone in generale saranno utilizzati per avvalersi di funzioni ben superiori a quelle offerte dal PC, tra cui ad esempio i pagamenti tramite NFC, e che, in un'ottica "Smart Working" lo smartphone, a differenza del tablet, è già oggi il gateway per lo scambio di tutte le comunicazioni, informazioni riservate aziendali e private di ogni singolo utente, il che lo rende un obiettivo più che succulento per i criminali. Infine non dobbiamo dimenticare che per flessibilità e impatto sul mercato, Android sarà la piattaforma più utilizzata per applicazioni IoT, tra cui non figurano esclusivamente app con un basso potenziale negativo sull'utente come fitness tracker e similari. Pensiamo alla domotica, o ancor più specificamente alle auto "connesse": come assicurarci che Android venga utilizzato solo per il sistema di intrattenimento in vettura e non per funzioni vitali come la gestione della centralina o il controllo sui freni? Non vogliamo neanche immaginare le conseguenze di eventuali hack "in corsa".

GLOSSARIO

Account hijacking	Compromissione di un account ottenuta ad esempio mediante ***phising*.**
Adware	Tipo di ***malware*** che visualizza pubblicità solitamente senza il consenso dell'utente. Può includere funzionalità ***spyware*.**
Apt (Advanced Persistent Treath)	Schemi di attacco articolati, mirati a specifiche entità o organizzazioni contraddistinti da: • un accurato studio del bersaglio preventivo che spesso continua anche durante l'attacco • l'impiego di tool e ***malware*** sofisticati • la lunga durata o la persistenza nel tempo cercando di rimanere inosservati per continuare a perpetrare quanto più possibile il proprio effetto.
Arbitrary File Read	***Vulnerabilità*** che consente ad un attaccante di accedere a file tramite richieste Web remote.
Backdoor	Soluzione tecnica che consente l'accesso ad un sistema superando i normali meccanismi di protezione.
Botnet	Insieme di dispositivi (compromessi da ***malware***) connessi alla rete utilizzati per effettuare, a loro insaputa, un attacco ad esempio di tipo ***DDOS***.
Business continuity	Soluzioni di natura tecnica ed organizzativa predisposte per garantire la continuità dell'erogazione di un servizio (eventualmente con uno SLA ridotto).
C&C (Command &Control)	I centri di comando e controllo (C&C) sono quegli host utilizzati per l'invio dei comandi alle macchine infette (bot) dal ***malware*** utilizzato per la costruzione della ***botnet***. Tali host fungono da ponte nelle comunicazioni tra gli host infetti e chi gestisce la ***botnet***, al fine di rendere più difficile la localizzazione di questi ultimi.

Cyber intelligence	Attività volte a raccogliere e rielaborare informazioni al fine prevedere possibili minacce (non esclusivamente di natura informatica) agli asset oggetto di tutela.
Cryptolocker	***Malware*** che ha come finalità criptare i file presenti nel dispositivo infetto al fine di richiedere un riscatto alla vittima per renderli nuovamente intellegibili.
Cyber crime	Attività criminali effettuate mediante l'uso di strumenti informatici.
Cyber espionage	Attività di spionaggio effettuata mediante l'uso di tecniche informatiche illecite.
Cyber resilience	Capacità di un organizzazione di resistere preventivamente o ad un attacco e di ripristinare la normale operatività successivamente allo stesso.
Defacement	Manipolazione del contenuto di una pagina web (tipicamente la home page) a scopi dimostrativi.
DNS (Domain Name System)	Indica sia l'insieme gerarchico di dispositivi, sia il ***protocollo***, utilizzati per associare un indirizzo IP ad un nome di dominio tramite un database distribuito.
DNS Open Resolver	Sistemi vulnerabili utilizzati come strumento per perpetrare attacchi informatici di tipo ***DDOS*** amplificati.
Dos (Denial of Service)	Attacchi volti a rendere inaccessibili alcuni tipi di servizi. Possono essere divisi in due tipologie: • applicativi, tesi a generare un numero di richieste maggiore o uguale al numero di richieste massimo a cui un server può rispondere (ad esempio numero di richieste web HTTP/HTTPS concorrenti). • volumetrici, tesi a generare un volume di traffico maggiore o uguale alla banda disponibile in modo da saturarne le risorse. Se vengono utilizzati più dispositivi per l'attacco coordinati da un centro di ***C&C*** si parla di ***DDoS*** (Destribuited Denial of Service)

DDoS (Distributed Denial of Service)	Attacchi ***DOS*** distribuiti, cioè basati sull'uso di una rete di apparati, costituenti in una botnet dai quali parte l'attacco verso l'obiettivo.
DRdos (Destribuited Reflection Denial of Service)	Sfruttando lo ***spoofing*** dell'indirizzo IP di una vittima, un utente malintenzionato può inviare piccole richieste ad un host vulnerabile inducendolo ad indirizzare le risposte alla vittima dell'attacco. Questa tipologia di ***DDoS*** permette al malintenzionato di amplificare la potenza del suo attacco anche di 600 volte, come dimostrato nel caso del ***protocollo NTP***.
Exploit	Codice con cui è possibile sfruttare una ***vulnerabilità*** di un sistema. Nel database Common Vulnerabilities and Exposures (cve.mitre.org) sono presenti sia le ***vulnerabilità*** note, sia i relativi exploit.
Exploit kit	Applicazioni utilizzabili anche da attaccanti non esperti, che consentono di sfruttare in forma automatizzata le ***vulnerabilità*** di un dispositivo (di norma browser e applicazioni richiamate da un browser).
Fast flux	Tecnica che permette di nascondere i ***DNS*** usati per la risoluzione dei domini malevoli dietro ad una rete di macchine compromesse in continua mutazione e perciò difficili da mappare e spegnere.
Fix	Codice realizzato per risolvere errori o ***vulnerabilità*** nei software.
Hacktivism	Azioni, compresi attacchi informatici, effettuate per finalità politiche o sociali.
Information warfare	Insieme di tecniche di raccolta, elaborazione, gestione, diffusione delle informazioni, per ottenere un vantaggio in campo militare, politico, economico…

Incident handling	Gestione di un incidente di sicurezza informatica. ENISA classifica le fasi di tale gestione in Incident report, Registration, Triage, Incident resolution, Incident closure, Post-analysis.
Keylogger	***Malware*** (o dispositivi hardware) in grado di registrare quello che la vittima digita sulla tastiera (o altrimenti inserisce), comunicando tali informazioni all'attaccante.
Malvertising	Tecniche che utilizzano l'ambito della pubblicità on line come veicolo di diffusione di ***malware***.
Malware	Definizione generica di applicazioni finalizzate a arrecare in qualche modo danno alla vittima (ad esempio raccogliendo o intercettando informazioni, creando malfunzionamenti nei dispositivi sui quali sono presenti, criptando i file al fine di richiedere un riscatto per renderli nuovamente intellegibili…).
Man in the browser	Tecnica che consente di intercettare le informazioni trasmesse dalla vittima, quali le credenziali di accesso al sito di un banca, al fine di poterle riutilizzare.
NTP (Network Time Protocol)	***Protocollo*** che consente la sincronizzare degli orologi dei dispositivi connessi ad una rete.
Payload	Letteralmente carico utile. Nell'ambito della sicurezza informatica è la parte di un ***malware*** che arreca danni.
Password hard-coded	Password inserite direttamente nel codice del software.
Pharming	Tecnica che consente di indirizzare la vittima verso un sito bersaglio simile all'originale (ad esempio un sito bancario) al fine di intercettare ad esempio le credenziali di accesso.
Phising	Tecnica che induce la vittima, mediante una falsa comunicazione in posta elettronica, a collegarsi verso un sito bersaglio simile all'originale (ad esempio il sito di una banca) al fine di intercettare informazioni trasmesse, quali le credenziali di accesso.

Phone hacking	Attività di hacking che ha come oggetto i sistemi telefonici; ad esempio mediante l'accesso illegittimo a caselle vocali.
Protocollo di comunicazione	Insieme di regole che disciplinano le modalità con cui i dispositivi connessi ad una rete si scambiano informazioni.
Ransomware	***Malware*** che induce limitazioni nell'uso di un dispositivo (ad esempio criptando i dati o impedendo l'accesso al dispositivo).
Rootkit	***Malware*** che consente sia il controllo occulto di un dispositivo, sia di nascondere la presenza propria e di altri malware.
Scrubbing center	Letteralmente centro di pulizia. In uno Scrubbing center il traffico di rete viene analizzato e "ripulito" delle componenti dannose.
Social engineering	Tecniche di attacco basate sulla raccolta di informazioni mediante studio/interazione con una persona.
Spoofing	Modifica di una informazione, ad esempio l'indirizzo mittente di un pacchetto IP.
Spyware	***Malware*** che raccoglie informazioni sul comportamento della vittima trasmettendole all'attaccante.
Sql injection	Tecnica di attacco basata sull'uso di query indirizzate a database SQL che consentono di ricavare informazioni ed eseguire azioni anche con privilegi amministrativi.
SSDP (Simple Service Discovery Protocol)	***Protocollo*** che consente di scoprire e rendere disponibili automaticamente i dispositive di una rete.

TCP Synflood	Tipo di attacco nel quale tramite pacchetti SYN in cui è falsificato l'IP mittente (spesso inesistente) si impedisce la corretta chiusura del three-way handshake, in quanto, nel momento in cui il server web vittima invia il SYN/ACK, non ricevendo alcun ACK di chiusura, essendo l'IP destinatario inesistente, lascerà la connessione "semi-aperta". Con un invio massivo di pacchetti SYN in concomitanza ad un alto tempo di timeout delle connessioni, il buffer del server verrebbe presto saturato, rendendo il server impossibilitato ad accettare ulteriori connessioni TCP, anche se legittime.
Tecniche di riflessione degli attacchi (DRDoS – Distributed Reflection Denial of Service)	La tecnica più diffusa sfrutta host esposti sulla Big Internet come riflettori del traffico a loro indirizzato sfruttando le ***vulnerabilità*** intrinseche ad alcuni protocolli quali ***NTP*** o ***DNS***.
Tecniche di amplificazione degli attacchi	Sfruttando lo ***spoofing*** dell'indirizzo IP di una vittima, un utente malintenzionato può inviare piccole richieste ad un host vulnerabile inducendolo ad indirizzare le risposte alla vittima dell'attacco. Ad esempio nel caso del ***protocollo NTP*** si può amplificare la potenza dell'attacco anche di 600 volte.
TOR	Rete di dispositivi che consente l'uso dei servizi internet in modalità anonima (www.torproject.org).
Trojan horse	***Malware*** che si installa in modo occulto su un dispositivo con diverse finalità, quali ad esempio raccogliere informazioni.
UPD Flood	Il ***protocollo*** UDP non prevede l'instaurazione di una connessione vera e propria e possiede tempi di trasmissione/risposta estremamente ridotti. Tali condizioni offrono maggiori probabilità di esaurire il buffer tramite il semplice invio massivo di pacchetti UDP verso l'host target dell'attacco.
UpnP (Universal Plug and Play)	***Protocollo*** di rete che consente la connessione e condivisione automatica di dispositivi ad una rete.

Vulnerabilità	Debolezza intrinseca di un asset (ad esempio un'applicazione software o un ***protocollo*** di rete) che può essere sfruttata da una minaccia per arrecare un danno.
Watering Hole	Attacco mirato nel quale viene compromesso un sito web al quale accede normalmente l'utente target dell'attacco.
Zero-day attach	Attacco compiuto sfruttando ***vulnerabilità*** non ancora note/risolte.

Bibliografia

Oltre alle fonti già citate nei singoli capitoli, segnaliamo altre fonti e Report che sono stati utili per la realizzazione del presente rapporto.

1. **Worldwide Infrastructure Report di Arbor Networks**
   http://www.arbornetworks.com/resources/annual-security-report
2. **Report semestrale sulla sicurezza Cisco 2015**
   http://www.cisco.com/web/IT/offers/lp/2015-midyear-security-report/index.html
3. **Cisco Annual Security Report 2016**
   http://www.cisco.com/web/IT/press/cs16/20160126.html
4. **Il Futuro della Cyber Security in Italia – Consorzio Cini**
   https://www.consorzio-cini.it/index.php/it/labcs-home/libro-bianco
5. **ENISA Threat Landscape 2015**
   https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/etl2015/etl2015/at_download/fullReport
6. **Global Information Security Survey 2015 – Ernst & Young**
   http://www.ey.com/GL/en/Services/Advisory/ey-global-information-security-survey-2015-1
7. **The 2016 Forcepoint Cybersecurity Predictions Report**
   https://blogs.forcepoint.com/it/security-labs/raytheonwebsense-previsioni-sulle-principali-minacce-alla-cybersecurity-il-2016
8. **GDATA White Papers**
   https://www.gdatasoftware.com/securitylabs/information/whitepaper
9. **http://hackmageddon.com/**
10. **2016 State of Security Operations Report - Hewlett Packard Enterprise**
    http://www8.hp.com/uk/en/software-solutions/enterprise-security-products-services
11. **Le previsioni sulle minacce nel 2016 - McAfee Labs - INTEL Security**
    http://www.mcafee.com/it/resources/reports/rp-threats-predictions-2016.pdf
12. **Cyber security: a failure of imagination by CEOs - KPMG**
    https://assets.kpmg.com/content/dam/kpmg/pdf/2015/12/cyber-ceo-report.pdf
13. **Security and the IoT ecosystem - KPMG**
    https://assets.kpmg.com/content/dam/kpmg/pdf/2015/12/security-and-the-iot-ecosystem.pdf

14. **2015 Global Audit Committee Survey - KPMG**
http://www.kpmg.ie/aci/documents/through-a-cyber-security-lens-june-2015.pdf
15. **Rapporti semestrali - MELANI**
https://www.melani.admin.ch/melani/it/home/dokumentation/rapporti.html
16. **Microsoft Security Intelligence Report**
https://www.microsoft.com/security/sir/default.aspx
17. **Microsoft Cybersecurity vision**
https://www.microsoft.com/security/cybersecurity
18. **Rapporto statistico sulle frodi con le carte di pagamento - Ministero dell'Economia e delle Finanze, Dipartimento del Tesoro**
http://www.dt.tesoro.it/export/sites/sitodt/modules/documenti_it/antifrode_mezzi_pagamento/antifrode_mezzi_pagamento/Ultimo_Rapporto_Statistico_Carte_di_Pagamento_.pdf
19. **An Inside-Out Approach to Enterprise Security - Oracle**
http://www.oracle.com/us/dm/oraclemarketplace-adv-may-cso-1937065.pdf
20. **Report sulla sicurezza Trend Micro del 3° trimestre 2015**
http://www.trendmicro.it/it/informazioni-sulla-sicurezza/ricerca/trendlabs-q3-2015-security-roundup/
21. **Previsioni Trend Micro sulla sicurezza 2016**
http://www.trendmicro.it/informazioni-sulla-sicurezza/ricerca/previsioni-sulla-sicurezza-2016/index.html
22. **2015 Data Breach Investigations Report - Verizon**
www.verizonenterprise.com/resources/reports/rp_dbir-report-2015-executive-summary_it_xg.pdf
23. **2015 Protected Health Information Data Breach Report - Verizon**
http://www.verizonenterprise.com/resources/reports/rp_2015-protected-health-information-data-breach-report_en_xg.pdf
24. **Security Advisory: minacce ai sistemi di pagamento nel settore hospitality - Verizon**
http://www.verizonenterprise.com/resources/reports/rp_verizon-hospitality-security-advisory_en_xg.pdf

Gli autori del Rapporto Clusit 2015

Luca Bechelli è consulente indipendente nel campo della sicurezza informatica dal 2000. Con aziende partner svolge consulenza per progetti nazionali ed internazionali su tematiche di Compliance, Security Governance, Risk Management, Data Protection, Privilege Management, Incident Handling e partecipa alla progettazione ed al project management per attività di system integration. Svolge attività di ricerca e sviluppo con aziende nel campo della sicurezza e tramite collaborazioni con enti di ricerca, nell'ambito delle quali ha svolto docenze per master post-laurea. Ha collaborato alla realizzazione di numerosi studi e pubblicazioni di riferimento per il settore. Dal 2007 è membro del Consiglio Direttivo e del Comitato Tecnico Scientifico del Clusit, con delega su Tecnologie e Compliance. Ha partecipato come docente a numerosi seminari Clusit Education, anche nell'ambito dei Security Summit.

Danilo Benedetti inizia la sua carriera nel 1998 come consulente, occupandosi principalmente di telecomunicazioni a larga banda, su reti fisse e mobili. Inizia ad occuparsi di temi di sicurezza nel 2005 e nel 2010 consegue la certificazione CISM. Nel 2009 inizia a lavorare come Solution Architect IT per HP ES, e dal 2013 si occupa principalmente di sicurezza all'interno dell'organizzazione Enterprise Security Services, con il compito di disegnare soluzioni di sicurezza per i clienti HPE, sia in ambito consulenziale che tecnologico. In anni recenti ha partecipato al dibattito sulla sicurezza presentando articoli per Limes e partecipando, in qualità di speaker, al Security Summit 2015, con un intervento sulla sicurezza delle infrastrutture critiche. Danilo ha sviluppato i suoi 15+ anni di esperienza anche in contesti internazionali, con esperienze consulenziali e progettuali in Italia, Francia, Germania, Indonesia ed Africa Occidentale. Le aree di maggiore focalizzazione riguardano il monitoraggio e la risposta agli incidenti di sicurezza ed il rispetto della compliance, in particolare negli ambiti Privacy e PCI-DSS.

Mirko Berlier, laureato in Ingegneria delle Telecomunicazioni presso il Politecnico di Torino, opera da 15 anni nell'attività di progettazione di servizi di Networking, Collaboration e Security per la Pubblica Amministrazione. In CSI Piemonte dal 2001 al 2007 si è occupato di Service Creation e Project Management a supporto delle iniziative di innovazione ICT per la PA Piemontese. Come Systems Engineer in Cisco Italia dal 2007, fa parte del team tecnico Public Sector e Major Accounts a supporto dei principali enti di Pubblica Amministrazione locale, Università e Sanità per i progetti di infrastrutturazione e digitalizzazione. Dal 2013 e per tutta la durata dell'Esposizione Universale di Milano ha partecipato per Cisco alla definizione e alla predisposizione dei servizi della Smart City di Expo2015, con focus particolare per quelli di Collaboration, Edutainment e Sicurezza IT.

Gianluca Bocci ha conseguito nel 1996 la laurea in Ingegneria Elettrica presso l'Università La Sapienza di Roma. È certificato CISM, CISA, Lead Auditor ISO/IEC 27001:2013, Lead Auditor ISO/IEC 22301:2012, CSA STAR Auditor e ITIL Foundation v3. Ha maturato un'esperienza pluriennale nel settore della Sicurezza Informatica in qualità di Security Solution Architect presso multinazionali di rilevanza nel settore dell'ICT e della Sicurezza Informatica. Attualmente supporta le attività del CERT di Poste Italiane e la realizzazione del Distretto Tecnologico di Cyber Security previsto nell'ambito delle iniziative del Programma Operativo Nazionale (PON) in qualità di referente tecnico scientifico del progetto "Protezione dell'Utente Finale". Da Gennaio 2015 ricopre il ruolo di Membro del Comitato Tecnico Scientifico del CLUSIT e dal 1 Maggio al 31 Ottobre 2015 ha ricoperto il ruolo di "Mobile Application Security & Mobile Threats" Service Manager per assicurare ad EXPO Milano 2015 il governo ed il controllo della sicurezza delle sue applicazioni mobili. È autore di diversi articoli e pubblicazioni scientifiche.

Francesca Bosco si è laureata a pieni voti in giurisprudenza ed ha iniziato a lavorare nel 2006 presso l'UNICRI (United Nations Interregional Crime and Justice Research Institute). All'interno della Emerging Crimes Unit, svolge il ruolo di project officer ed ha acquisito esperienza nei programmi di contrasto alla criminalità informatica ed alla criminalità organizzata. E'attualmente responsabile dei programmi relativi alla sicurezza informatica e sta approfondendo la ricerca in merito all'uso improprio della tecnologia. È membro dell'Advisory Group on Internet Security dello European Cybercrime Center (EC3) presso l'Europol. È co-fondatrice del Tech and Law Center.

Paolo Bufarini, Head of Security Sales for Mediterranean Region Akamai Italia. Paolo, 51 anni, entra in Akamai a maggio 2014 con l'incarico di guidare le operazioni della divisione security della multinazionale in Italia, Grecia, Turchia, Israele e Medio Oriente. Con oltre 26 anni di esperienza in qualità di Sales Manager in Europa e nel Medio Oriente, Paolo Bufarini vanta numerose esperienze maturate in diversi settori dell'Information Technology tra cui Security, Networking ed Enterprise Software. Prima di entrare in Akamai, Bufarini ha lavorato presso Imperva, dove si è occupato dell'espansione del business della multinazionale in Italia e nei Balcani, oltre ad aver precedentemente ricoperto incarichi di responsabilità presso Hewlett-Packard, McAfee, Citrix Systems, Wall Data, Dataware Technology, Fulcrum, Bull SA, Itway e Sentrigo. Paolo Bufarini ha iniziato la sua carriera nell'Esercito Italiano, con il grado di Tenente nel dipartimento ICT ed Intelligence.

Cesare Burei, nato nel 1967, vive e lavora a Padova. Laureato in Scienze Economiche con una Tesi sul ruolo del Broker nelle Assicurazioni, ha conseguito il Master in Risk Engineering di Cineas (Consorzio di Ingegneria delle Assicurazioni) presso il politecnico di Milano. In seguito ha collaborato con Assicurazioni Generali per sviluppare modelli di analisi per le coperture Danni Indiretti, tutt'ora utilizzati.
È attualmente Amministratore di Margas srl - Consulenti e Broker Assicurativi. Esperto in rischi industriali e tecnologici di imprese italiane internazionalizzate, oggi segue in stretta collaborazione con partner di Information Security le aziende nell'assessment e

nell'analisi del rischio informatico da un punto di vista assicurativo. È socio CLUSIT e ha incarichi come formatore CINEAS in ambito Cyber Risk.

Giancarlo Butti ha acquisito un master di II livello in Gestione aziendale e Sviluppo Organizzativo presso il MIP Politecnico di Milano. Si occupa di ICT, organizzazione e normativa dai primi anni 80 ricoprendo diversi ruoli: security manager, project manager ed auditor presso gruppi bancari, consulente in ambito sicurezza e privacy presso aziende dei più diversi settori e dimensioni. Ha all'attivo oltre 600 articoli e collaborazioni con oltre 20 testate. Ha pubblicato 19 fra libri e white paper alcuni dei quali utilizzati come testi universitari; ha partecipato alla redazione di 5 opere collettive. Partecipa ai gruppi di lavoro di ABI LAB sulla Business Continuity e Rischio Informatico, di ISACA-AIEA su Privacy EU e 263, di Oracle Community for Security su frodi e Privacy EU. È membro della faculty di ABI Formazione e del Comitato degli esperti per l'innovazione di OMAT360. Ha inoltre acquisito le certificazioni/qualificazioni LA BS7799, LA ISO/IEC27001, CRISC, ISM e DPO.

Giantonio Chiarelli, laureato in Informatica, certificato Lead Auditor ISO/IEC 27001:2013 e CSA STAR Auditor, ha la passione per gli aspetti più nascosti e tecnici della (In)Sicurezza Applicativa Mobile e della Information Security Intelligence. Ha partecipato come relatore a congressi di sicurezza, ed è coautore di pubblicazioni scientifiche e tecnico/divulgative su metodologie di analisi e rischi connessi ai mobile malware.
La passione per la sicurezza e la programmazione lo porta sempre più spesso al rilascio di vulnerability advisory (es. 0day ed exploit per il plugin Appointment Booking Pro di Joomla), alla produzione di bugfix per tool open-source (es. Androguard), alla scrittura di nuovi tool di analisi di sicurezza (es. PhisHunter e DroidTrail) o di security awareness (es. MyBOSS - My Botnet Over SmS). Dopo essersi occupato di consulenza in ambito Risk & Compliance, di Defensive/Offensive Security presso il CERT di Poste Italiane, ed aver ricoperto l'incarico di Technical Project Manager per i servizi di Cyber Security erogati da Poste Italiane nell'ambito di EXPO Milano 2015, attualmente ricopre il ruolo di Senior Cyber Security Specialist presso Poste Italiane.

Angelo Chiarot si occupa di informatica dal 1980, anno in cui produce e commercializza la sua prima applicazione in linguaggio Assembler. Da quel momento, seppur alternativamente abbia dato spazio ad attività imprenditoriali (nel 1993 avvia una web & communication agency e nel 1998 ottiene fondi con un Venture Capital per lo sviluppo della – allora - più grande rete Wi-Fi italiana), si dedica completamente all'Information Security conseguendo certificazioni da Lead Auditor BS7799 (ora ISO/IEC 27001), Internal Auditor ISO 20000 e PCI DSS Qualified Security Assessor, maturando esperienza in diversi settori. Contestualmente svolge anche attività di verifica e implementazione di sistemi di gestione della compliance principalmente sulle tematiche Basilea II/III (Operational Risk), D.Lgs. 196/03, D.Lgs. 231/01, svolgendo anche attività di Business Process Re-engineering & Management. Dall'autunno 2011 è membro del Security Advisory Team di @ Mediaservice.net S.r.l., Gruppo di lavoro dedicato al supporto di grandi Clienti sulle tematiche della sicurezza delle informazioni, gestione degli incidenti, continuità operativa e compliance. Dal 2008 è autore di diversi articoli e pubblicazioni.

Davide Del Vecchio, conosciuto in rete con il nickname "Dante", da sempre appassionato di sicurezza informatica, ha firmato parecchie ricerche in quest'ambito. È il responsabile del Security Operation Center di FASTWEB da cui vengono erogati i servizi di sicurezza gestita per migliaia di Clienti. Scrive sporadicamente per Wired ed altre testate ed è tra i fondatori del Centro Hermes per la Trasparenza e i Diritti Umani Digitali. Ha collaborato con diverse università e ha partecipato come relatore a numerosi congressi nazionali e internazionali. Nel 2014 è entrato a far parte del comitato direttivo del Clusit.

Roberto Di Legami, Primo Dirigente della Polizia di Stato**,** è Direttore del Servizio di Polizia Postale e delle Comunicazioni. Per anni ha svolto attività investigativa presso la Squadra Mobile di Palermo. Nel 1992 è stato assegnato al gruppo investigativo incaricato di fare luce sugli attentati a Giovanni Falcone e Paolo Borsellino. Successivamente, ha diretto per nove anni l'Ufficio "Criminalità Organizzata" dell'Europol.
Nel settembre 2001 si è recato negli USA per stabilire la piattaforma di cooperazione EU-US, per lo scambio delle informazioni con le principali agenzie americane deputate alla lotta al terrorismo ed

al crimine organizzato (C.I.A, F.B.I., I.N.S., U.S. Customs, U.S. Secret Service, e successivamente U.S. Homeland Security). Nel maggio 2003, il Consiglio dell'Unione Europea gli ha conferito l'incarico di creare e dirigere il Centro di Eccellenza per il Crimine Informatico di Europol (High-Tech Crime Center), oggi ridenominato EC3 (European Cyber Crime Centre). Ha ricevuto numerosi riconoscimenti dai vertici della Polizia italiana e da varie Autorità giudiziarie nazionali e straniere.

Gabriele Faggioli, legale, è Presidente del Clusit e docente del MIP – Politecnico di Milano. È membro del Gruppo di Esperti sui contratti di cloud computing della Commissione Europea. È specializzato in contrattualistica informatica e telematica, in information & telecommunication law, nel diritto della proprietà intellettuale e industriale e negli aspetti legali della sicurezza informatica, in progetti inerenti l'applicazione delle normative inerenti la responsabilità amministrativa degli enti e nel diritto dell'editoria e del marketing. Ha pubblicato diversi libri fra cui, da ultimo, "*I contratti per l'acquisto di servizi informatici*" (Franco Angeli), "*Computer Forensics*" (Apogeo), "*Privacy per posta elettronica e internet in azienda*" (Cesi Multimedia) oltre ad innumerevoli articoli sui temi di competenza ed è stato relatore a molti seminari e convegni.

Paolo Giudice è segretario generale del CLUSIT. Negli anni 80 e 90 ha svolto attività di consulenza come esperto di gestione aziendale e rischi finanziari. L'evoluzione del settore IT, che ha messo in evidenza le carenze esistenti in materia di Security, lo ha spinto ad interessarsi alla sicurezza informatica e, nel luglio 2000, con un gruppo di amici, ha fondato il CLUSIT. Dal 2001 al 2008 ha coordinato il Comitato di Programma di Infosecurity Italia e dal 2009 coordina il Comitato Scientifico del Security Summit. Dal 2011 coordina il Comitato di Redazione del Rapporto Clusit. Paolo è Partner di C.I.S.C.A. (Critical Infrastructures Security Consultants & Analysts) a Ginevra.

Corrado Giustozzi è esperto di sicurezza cibernetica presso l'Agenzia per l'Italia Digitale per lo sviluppo del CERT della Pubblica Amministrazione, membro per i mandati 2010-2012, 2012-2015 e 2015-2017 del Permanent Stakeholders' Group dell'Agenzia dell'Unione Europea per la Sicurezza delle Reti e delle Informazioni (ENISA), membro del Comitato Direttivo di Clusit. In trent'anni di attività come consulente di sicurezza delle informazioni ha condotto importanti progetti di *audit* ed *assessment*, e progettato infrastrutture di sicurezza e *trust*, presso grandi aziende e pubbliche amministrazioni. Collabora da oltre quindici anni con il Reparto Indagini Tecniche del ROS Carabinieri nello svolgimento di attività investigative e di contrasto del *cybercrime* e del cyberterrorismo. Ha collaborato con l'Ufficio delle Nazioni Unite su progetti internazionali di contrasto alla cybercriminalità. Insegna in diversi corsi di Laurea e di Master presso varie università italiane. Giornalista pubblicista e membro dell'Unione Giornalisti Italiani Scientifici (UGIS), svolge da sempre un'intensa attività di divulgazione culturale sui problemi tecnici, sociali e legali della sicurezza delle informazioni. Ha al suo attivo oltre mille articoli e quattro libri.

Marco Ivaldi è un ricercatore e consulente con esperienza ventennale nel campo della sicurezza informatica. Lavora con la qualifica di Senior Security Advisor presso @ Mediaservice.net, per conto della quale si occupa della gestione dei progetti, dell'esecuzione di verifiche di sicurezza e audit di conformità, della ricerca di vulnerabilità e dello sviluppo di exploit. In qualità di membro dell'ISECOM Core Team, collabora attivamente allo sviluppo dell'Open Source Security Testing Methodology Manual (OSSTMM), lo standard internazionale di riferimento per l'esecuzione di verifiche di sicurezza, e al progetto Hacker Highschool (HHS), una raccolta di lezioni che mirano a formare i più giovani sul tema della sicurezza su Internet. Marco ha pubblicato articoli tecnici su numerose testate del settore e ha collaborato alla stesura di alcuni libri di fama internazionale, tra cui Hacking Exposed Linux.

Marco Landi vanta un'esperienza di più di 20 anni nel settore IT come Infrastructure Architect ed esperto di sicurezza per importanti vendor e system integrator. In G Data Software dal 2014 con il ruolo di Presales Consultant, si occupa di Security Intelligence, Big Data, Data Privacy, Business Continuity e sicurezza delle reti.

Rocco Mammoliti, nato nel 1968, ha studiato Ingegneria Elettronica presso l'Università di Pisa e ha conseguito un Master in sicurezza presso il Ministero della Difesa - Centro Alti Studi. Ha svolto per diversi anni attivita' di ricerca scientifica presso il CNR. È autore di diverse pubblicazioni scientifiche su temi legati alla modellistica, data mining, sicurezza ICT oltre che su temi di innovazione e nuove tecnologie. Ha lavorato per aziende di rilevante importanza nel campo dell'IT ed industrie TLC quali Ericsson, Bull e Telecom Italia, ricoprendo in quest'ultima il ruolo di Responsabile della Funzione di Information Security. Ha svolto attivita' di consulenza per diverse società nel settore ICT e Telecomunicazioni. È membro di associazioni professionali internazionali tra cui l'IEEE e la Computer Society. Le sue principali aree di competenza sono afferenti ai domini nel Network & Information Security, creazione e gestione di Security Operation Center e Computer Emergency Response Team, Abuse & Cybercrime Prevention, Child Online Protection, etc. Attualmente è Responsabile della funzione Sicurezza delle Informazioni di Poste Italiane S.p.A., del CERT di Poste Italiane, del Distretto di Cyber Security di Cosenza e Direttore Generale della Fondazione GCSEC (Global Cyber Security Center) di cui Poste Italiane è fondatore.

Paolo Marchei, nato nel 1971, si è laurato in Ingegneria Informatica presso il Politecnico di Milano. È in Oracle dal 1998 dove ha maturato significative esperienze nella realizzazione di soluzioni complesse sia nell'area 'Fraud Detection' per i sistemi di pagamento che nell'area dei portali web intranet e Internet. Dal 2001 opera come sales consultant con focus sulle soluzioni di sicurezza e compliance. Nel ruolo di Principal Sales Consultant in Oracle supporta dal 2005 la forza commerciale e i partner nella definizione di architetture di sicurezza sia nell'area Identity & Access Management che relative alla DataBase Security.

Pierluigi Paganini è Chief Information Security Officer presso Bit4Id e membro del gruppo Threat Landscape Stakeholder Group dell'agenzia ENISA (European Union Agency for Network and Information Security). Collaboratore SIPAF - Prevenzione dell'utilizzo del sistema finanziario per fini illegali – Ministero dell'Economia e delle Finanze. Ricopre anche il ruolo di capo editore per la nota rivista statunitense Cyber Defense Magazine e vanta una esperienza di oltre venti anni nel settore della cyber security. È membro dei gruppi di lavoro del portale "The Hacker News" e dell'ICTTF International Cyber Threat Task Force, è inoltre autore di numerosi articoli pubblicati sulle principali testare in materia di sicurezza quali Infosec Institute e The Hacker News Magazine. Ha pubblicato due libri "The Deep Dark Web" e "Digital Virtual Currency and Bitcoin" rispettivamente sulla tematiche inerenti Deep Web ed i sistemi di moneta virtuali.

Fabio Panada, Cisco Security Consultant, ha maturato piu' di un ventennio di esperienza nell'Information Technology e si occupa di sicurezza dai primi anni '90. In precedenza, Panada ha lavorato in IBM, dove ha ricoperto il ruolo di Tech Sales Leader per la Security Business Unit. Nel corso del suo percorso professionale, Panada ha collaborato con diverse aziende, tra cui Compaq Computer, ora HP e Digital Equipment Corporation. Tra le esperienze più significative segnaliamo, inoltre, il contributo allo Start-up di Internet Security Systems (ISS) Italia, all'inizio del 2000, come EMEA Tech Sales Manager e di Sourcefire Italia come Security Consultant.

Alessio L.R. Pennasilico, Security Evangelist in Obiectivo, si dedica ad aumentare l'altrui percezione delle problematiche legate a sicurezza, privacy ed utilizzo della tecnologia, oltre che a prevenire o respingere attacchi informatici conosciuti o non convenzionali. Da anni partecipa come relatore ai più blasonati eventi di security italiani ed internazionali. Collabora con diverse università ed a diversi progetti di ricerca. Fa parte del Comitato Direttivo e del Comitato Tecnico Scientifico di Clusit, è Vice Presidente dell'Associazione Informatici Professionisti (AIP), membro del Comitato per la Salvaguardia dell'imparzialità di LRQA e Membro del comitato di schema 11506 per Kiwa Cermet.

Andrea Piazza, nei 16 anni in cui ha lavorato in Microsoft, ha svolto il ruolo di Technical Account Manager e successivamente di Security Premier Field Engineer, dove ha ricoperto mansioni di crescente responsabilità da Tech Lead Italia, a Tech Lead EMEA, a Technology Manager EMEA. Dal 2014 è National Security Officer della filiale italiana di Microsoft, dove coordina le attività volte a promuovere la consapevolezza e l'adozione delle tecnologie di sicurezza da parte dei clienti, gestendo i rapporti sulle tematiche di sicurezza e cybersecurity con le government élites, i leader accademici e i decisori pubblici, nonché con i responsabili e i team di sicurezza delle aziende italiane. A livello EMEA coordina i servizi di sicurezza del supporto Microsoft, come Security Assessment, Workshop, attività di risposta agli incidenti e di remediation, si occupa in prima persona dell'attività di formazione e aggiornamento degli engineer di sicurezza, e collabora con i team di sviluppo dei servizi di sicurezza Microsoft. In Microsoft ha collaborato al whitepaper "Mitigating Pass-the-Hash Attacks and Other Credential Theft-Version 2". Collabora al Comitato di Redazione de "Il Documento Digitale", ed ha partecipato alla redazione delle linee guida UNICRI 2015 per le PMI. È certificato CISSP, ISO27001 Lead Auditor e ITIL.

Domenico Raguseo è Manager del team europeo di Technical Sales per IBM Security. Ha 16 anni di esperienza manageriale in diverse aree. Domenico collabora con alcune università nell'insegnamento di Service Management e del Cloud Computing. Dal 2010 Domenico è membro del comitato scientifico del Master in IT Governance dell'Università di Roma. Domenico è IBM Master inventor grazie a una moltitudine di brevetti e pubblicazioni in diverse discipline (Business Processes, ROI, Messages and Collaborations, Networking). Infine, è stato speaker di Sicurezza delle Informazioni, Service Management, Cloud computing, Energy Optimization e Smarter Planet in eventi nazionali e internazionali.

Pier Luigi Rotondo si occupa di Technical Enablement per IBM Security su soluzioni di Identity Governance. Con una laurea in Scienze dell'Informazione presso l'Università degli Studi di Roma "La Sapienza" ricopre incarichi di docenza su temi di Sicurezza delle Informazioni in Master e corsi di Dottorato presso l'Università degli Studi di Roma "La Sapienza" e l'Università degli studi di Perugia. Ha contribuito a molti lavori sul tema della cyber security, divulgando oltre ai risultati IBM anche regole pratiche per il contrasto delle frodi online. Per conto di IBM viene spesso chiamato ad illustrare la strategia, le soluzioni e i prodotti di sicurezza ai propri clienti, e a divulgare sul mercato italiano i risultati del team di ricerca IBM X-Force.

Federico Santi inizia la sua carriera in ambito sicurezza nel 2000, prima di assumere il ruolo di Security Principal per il Sud Europa in Hewlett Packard Enterprise, ha lavorato in Andersen e Deloitte. La sua esperienza nella Security segue una vista multidisciplinare e business-oriented centrando l'attenzione su processi (SOC/SIEM), dati (Data Protection & Privacy) e utenti (Identity Governance). Tra le responsabilità principali: Business Development nella Regione; Capability Leader dei servizi SSRM (Security Strategy and Risk Management) Trusted advisory su clienti strategici; Relazioni Istituzionali; Attività di comunicazione interna ed esterna. Federico vanta numerose partecipazioni accademiche (Instructor in un Master in IT Governance presso l'Università Nazionale di Milano) e come speaker per la sicurezza e IT Governance presso i principali tavoli nazionali (DIS, CNR, CLUSIT, AIEA, AIIC) ed europei (Membro della NIS Platform). Federico ha sviluppato i

suoi 15+ anni di esperienza anche in contesti internazionali, con esperienze in Italia, Spagna, Francia ed Africa Occidentale ed ha seguito con una particolare attenzione i contesti del Settore Pubblico e dell'Energy & Utilities.

Riccardo Scalici, Senior Underwriter - Cyber Unit - presso CHUBB. È responsabile per la sottoscrizione della linea Cyber per l'Italia. Ha una trentennale esperienza nel settore Property e Technical Lines, ventennale esperienza nell'elettronica e informatica. Creatore del prodotto a marchio Data flow®. Co-Fondatore del CLUSIT, è autore del Bollettino sui rischi informatici per account e specialist. Si è laureato presso il Politecnico di Milano.

Sofia Scozzari si occupa con passione di informatica dall'età di 16 anni. Ha lavorato come consulente di sicurezza presso primarie aziende italiane e multinazionali, curando gli aspetti tecnologici ed organizzativi di numerosi progetti. Chief Executive Officer de iDIALOGHI, negli anni si è occupata di Social Media Security, ICT Security Training e di Servizi di Sicurezza Gestita, quali Vulnerability Management, Mobile Security e Threat Intelligence. Membro di CLUSIT ed Assintel, è autrice di articoli e guide in tema di Social Media Security. È tra gli autori del paper "La Sicurezza nei Social Media" pubblicato nel 2014 dalla Oracle Community for Security. Fin dalla prima edizione contribuisce alla realizzazione del "Rapporto Clusit sulla Sicurezza ICT in Italia" curando l'analisi dei principali attacchi a livello internazionale e nazionale.

Claudio Telmon è consulente freelance nel campo della sicurezza e gestione del rischio IT da circa vent'anni. Ha gestito il laboratorio di sicurezza del Dipartimento di Informatica dell'Università di Pisa, ed in seguito ha collaborato per diversi anni con il Dipartimento per attività di didattica e di ricerca, in particolare nel campo della sicurezza e gestione del rischio. Si è occupato come professionista dei diversi aspetti tecnologici ed organizzativi della sicurezza, lavorando per aziende del settore finanziario, delle telecomunicazioni e per pubbliche amministrazioni. Membro del comitato direttivo e del comitato tecnico scientifico del CLUSIT.

Mario Terranova, specializzato in Ingegneria dei sistemi di controllo e calcolo automatico presso "La Sapienza" di Roma nel 1979 e docente presso questa università dal 1980 al 1996, è dirigente dal 1998. È stato consulente di primarie società, tra cui Alenia, Urmet e Cap Gemini, occupandosi di basi di dati, sistemi distribuiti, reti locali, sicurezza informatica, crittografia e firma digitale. Per quest'ultima è stato rappresentante italiano a Bruxelles. Oggi è responsabile dell'Area Sistemi, tecnologie e sicurezza informatica dell'Agenzia per l'Italia Digitale, nonché del CERT-PA.

Andrea Travaini lavora in G Data Software dal 2009 dove ha ricoperto vari ruoli in Germania e in Italia. Dapprima responsabile del supporto tecnico ai grandi clienti, oggi segue i temi della Mobile Security e delle soluzioni di Mobile Device Management per le piattaforme IOS e Android.

Giuseppe Vaciago è Avvocato, iscritto all'Ordine degli Avvocati di Milano dal 2002. Ha prestato la sua attività professionale per alcune importanti società nazionali e internazionali nel settore dell'information technology. Ha conseguito un PHD in Digital Forensics all'Università degli Studi di Milano Bicocca ed è docente di informatica giuridica presso l'Università degli Studi dell'Insubria dal 2007. Ha frequentato in qualità di Visiting Scholar la Stanford Law School e la Fordham Law School di New York. Ha la qualifica di lead auditor ISO 27001/2013. È co-fondatore del Tech and Law Center di Milano. È fellow presso il Nexa Center di Torino e presso il Cybercrime Institute di Colonia e membro del comitato editoriale della Rivista Digital Investigation edita da Elsevier. È membro dell'Organismo di Vigilanza di Procter & Gamble Italy S.p.A., Whirlpool S.p.A e Fondazione Albero della Vita.

Alessandro Vallega, in Oracle Italia dal 1997 come Project Manager in ambito ERP e nell'Information Technology dal 1984, è Business Development Director e si occupa a livello Europeo di Governance Risk and Compliance, Database Security ed Identity & Access Management. Ha definito ed esportato un approccio per valutare la Security Maturity dei database e per valutare i vantaggi aziendali nell'uso di soluzioni IAM. Inoltre è il fondatore e il coordinatore della Oracle Community for Security. È coautore, editor o team leader di una decina di pubblicazioni su diversi temi legati alla sicurezza (misure, rischio, frodi, ritorno dell'investimento, compliances, privacy...) liberamente scaricabili dal sito Clusit (http://c4s.clusit.it). Ha fondato insieme a Clusit e ad Aused un osservatorio permanente sulla nuova legge europea per la Protezione dei Dati Personali chiamato EuroPrivacy.info. Contribuisce fin dal 2012 ai Rapporti Clusit sulla Sicurezza ICT in Italia. È socio AIEA, CSA Italy e membro del Consiglio Direttivo di Clusit.

Giancarlo Vercellino è Research Manager, IDC Local Research, dove si occupa di ricerca per clienti nazionali e internazionali del settore IT, con particolare focus in area software applicativo. Prima di raggiungere IDC, Giancarlo ha lavorato come market analyst e business manager presso diverse fondazioni e centri ricerca e ha insegnato economia presso il Politecnico di Torino. Giancarlo si è laureato con lode presso l'Università di Torino, ha un Master in gestione strategica dell'IT presso il Politecnico di Torino, un Phd in economia industriale al Politecnico di Milano e ha frequentato i corsi di MBA della Anderson School of Management, University of California, Los Angeles.

Andrea Volponi ha conseguito nel 2003 la laurea in Ingegneria Elettronica presso l'Università degli Studi di Roma Tre. Ha ricoperto la posizione di Project e Program Manager per progetti in ambito security governance, technical security, compliance e audit. Ha lavorato per primarie aziende del settore della consulenza quali Reply ed Almaviva, maturando esperienze presso clienti appartenenti a diversi settori di business (telco, energy, pubblica amministrazione) e sviluppando competenze in ambito cyber security, risk management, security auditing e business continuity management. Attualmente ricopre il ruolo di responsabile del CERT di Poste Italiane, coordinando le attività di prevenzione, gestione incidenti informatici di sicurezza e contrasto del cyber crime. Ha conseguito un executive master presso il Politecnico di Milano ed il Consorzio ELIS, è Lead Auditor ISO/IEC 27001:2013, ha conseguito le certificazioni STAR Auditor e l'ITIL Foundation.

Andrea Zapparoli Manzoni si occupa con passione di ICT dal 1997 e di Information Security dal 2003, mettendo a frutto un background multidisciplinare in Scienze Politiche, Computer Science ed Ethical Hacking. Dal 2012 è membro dei Consiglii Direttivi di Clusit e di Assintel, e Board Advisor del Center for Strategic Cyberspace + Security Science di Londra.
È stato Presidente de iDialoghi per oltre 10 anni, società milanese dedicata alla formazione ed alla consulenza in ambito Cyber Security. Nel gennaio 2015 ha assunto il ruolo di Senior Manager della divisione Information Risk Management di KPMG Advisory.
È spesso chiamato come relatore a conferenze ed a tenere lezioni presso Università, sia in Italia che all'estero. Come docente Clusit tiene corsi di formazione su temi quali Cyber Crime, Mobile Security, Cyber Intelligence e Social Media Security, e partecipa come speaker alle varie edizioni del Security Summit, oltre che alla realizzazione di white papers (FSE, ROSI v2, Social Media) in collaborazione con la Oracle Community for Security. Fin dalla prima edizione del "Rapporto Clusit sulla Sicurezza ICT in Italia" cura la sezione relativa all'analisi dei principali attacchi a livello internazionale, ed alle tendenze per il futuro.

Ringraziamenti

Clusit e Security Summit ringraziano tutti gli autori e le persone che hanno contribuito alla realizzazione del Rapporto Clusit 2016.

Si ringraziano inoltre: @Mediaservice.net, Akamai, Arbor Networks, Chubb, Cert Nazionale, Cert-PA, Cisco Systems, Consorzio Netcomm, Ernst & Young, Ministero dell'Economia e delle Finanze – Dipartimento del Tesoro, ENISA, FASTWEB, Forcepoint, Hewlett Packard Enterprise, G DATA, IBM, IDC, iDialoghi, Intel Security, KPMG Advisory, Lombardia Informatica, Margas, Microsoft, ORACLE, Osservatori Digital Innovation del Politecnico di Milano, Polizia Postale e delle Comunicazioni, Poste Italiane, Tech and Law Center, Trend Micro, Verizon.

Il Clusit, nato nel 2000 presso il Dipartimento di Informatica dell'Università degli Studi di Milano, è la più numerosa ed autorevole associazione italiana nel campo della sicurezza informatica. Oggi rappresenta oltre 500 organizzazioni, appartenenti a tutti i settori del Sistema-Paese.

Gli obiettivi

- Diffondere la cultura della sicurezza informatica presso le Aziende, la Pubblica Amministrazione e i cittadini.
- Partecipare alla elaborazione di leggi, norme e regolamenti che coinvolgono la sicurezza informatica, sia a livello nazionale che europeo.
- Contribuire alla definizione di percorsi di formazione per la preparazione e la certificazione delle diverse figure professionali operanti nel settore della sicurezza.
- Promuovere l'uso di metodologie e tecnologie che consentano di migliorare il livello di sicurezza delle varie realtà.

Le attività e i progetti in corso

- Formazione specialistica: i Webinar e i Seminari CLUSIT.
- Ricerca e studio: Premio "Innovare la Sicurezza delle Informazioni" per la migliore tesi universitaria arrivato alla 12a edizione.
- Le Conference specialistiche: Security Summit (Milano, Cosenza, Cagliari, Roma e Verona).
- Produzione di documenti tecnico-scientifici: i Quaderni CLUSIT e le Pillole di Sicurezza.
- I Gruppi di Lavoro: con istituzioni, altre associazioni e community.
- Il progetto "Rischio IT e piccola impresa", dedicato alle piccole e micro imprese.
- Progetto Scuole: la Formazione sul territorio.
- Rapporti Clusit: Rapporto annuale sugli eventi dannosi Cyber crime e incidenti informatici) in Italia; analisi del mercato italiano dell'ICT Security; analisi sul mercato del lavoro.
- Il Mese Europeo della Sicurezza Informatica, iniziativa di sensibilizzazione promossa e coordinata ogni anno nel mese di ottobre in Italia da Clusit, in accordo con l'ENISA e con l'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione del Ministero dello Sviluppo Economico (ISCOM).

Il ruolo istituzionale

In ambito nazionale, Clusit opera in collaborazione con: Presidenza del Consiglio, numerosi ministeri, Banca d'Italia, Polizia Postale e delle Comunicazioni, Arma dei Carabinieri e Guardia di Finanza, Agenzia per l'Italia Digitale, Autorità Garante per la tutela dei dati personali, Autorità per le Garanzie nelle Comunicazioni, CERT Nazionale e CERT P.A., Università e Centri di Ricerca, Associazioni Professionali e Associazioni dei Consumatori, Confindustria, Confcommercio e CNA.

I rapporti internazionali

In ambito internazionale, Clusit partecipa a svariate iniziative in collaborazione con: i CERT, i CLUSI, Università e Centri di Ricerca in oltre 20 paesi, Commissione Europea, ENISA (European Union Agency for Network and Information Security), ITU (International Telecommunication Union), OCSE, UNICRI (Agenzia delle Nazioni Unite che si occupa di criminalità e giustizia penale), le principali Associazioni Professionali del settore (ASIS, CSA, ISACA, ISC², ISSA, SANS) e le associazioni dei consumatori.

Security Summit è il più importante appuntamento italiano per tutti coloro che sono interessati alla sicurezza dei sistemi informatici e della rete e, più in generale, alla sicurezza delle informazioni.

Progettato e costruito per rispondere alle esigenze dei professionals di oggi, Security Summit è un convegno strutturato in momenti di divulgazione, di approfondimento, di formazione e di confronto. Aperto alle esperienze internazionali e agli stimoli che provengono sia dal mondo imprenditoriale che da quello universitario e della ricerca, il Summit si rivolge ai professionisti della sicurezza e a chi in azienda gestisce i problemi organizzativi o legali e contrattuali dell'Ict Security.

La partecipazione è libera e gratuita, con il solo obbligo dell'iscrizione online.

Il Security Summit è organizzato dal Clusit e da Astrea, agenzia di comunicazione e organizzatore di eventi di alto profilo contenutistico nel mondo finanziario e dell'Ict.

Certificata dalla folta schiera di relatori (più di 350 sono intervenuti nelle scorse edizioni), provenienti dal mondo della ricerca, dell'Università, delle Associazioni, della consulenza, delle Istituzioni e delle imprese, la manifestazione è stata frequentata da oltre 12.000 partecipanti, e sono stati rilasciati circa 7.000 attestati validi per l'attribuzione di oltre 12.000 crediti formativi (CPE).
Tutte le sessioni prevedono il rilascio di Attestati di Presenza e danno diritto a crediti/ore CPE(Continuing Professional Education) validi per il mantenimento delle certificazioni CISSP, CSSP,CISA, CISM o analoghe richiedenti la formazione continua.

L'edizione 2016

L'ottava edizione del Security Summit si tiene a Milano dal 15 al 17 marzo, a Roma il 7 e 8 giugno e a Verona il 5 ottobre. Sono allo studio le tappe di Cosenza, Cagliari e Treviso.

Informazioni

- Agenda e contenuti: info@clusit.it, +39 349 7768 882
- Altre informazioni: info@astrea.pro
- Informazioni per la stampa: press@securitysummit.it
- Sito web: http://www.securitysummit.it/
- Foto reportage: https://www.facebook.com/groups/64807913680/photos/?filter=albums
- Video riprese e interviste: http://www.youtube.com/user/SecuritySummit

In collaborazione con

F-Secure

intel Security

Microsoft

TREND MICRO

Research Partner

IDC
Analyze the Future

Il presente Rapporto
è stato prodotto in occasione del

EUROPEAN
CYBER
SECURITY
MONTH

SECURITY SUMMIT
Technologies
Management
Compliance

www.securitysummit.it