NUOVA EDIZIONE
SETTEMBRE 2018

# Rapporto

Clusit

# 2018

sulla sicurezza ICT
in Italia

SECURITY 10 ANNI
TECHNOLOGIES
MANAGEMENT COMPLIANCE
SUMMIT

# Indice

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

# Prefazione

Il rapporto CLUSIT che leggerete è il frutto del lavoro di un pool di esperti che ha analizzato e confrontato una serie di fonti e che non può che farci giungere a una sola conclusione: nel 2017 il cybercrime è andato del tutto fuori controllo.

La stima dei danni globali causati dal fenomeno ammontano a circa 500 miliardi di dollari. Si tratta di un vero e proprio "salto quantico".

Mentre scrivo queste righe si sta votando in Italia.
Si tratta di elezioni politiche di grande importanza cadute in un momento di attenzione mediatica spasmodica sul fenomeno cybercrime e di grandi investimenti in sicurezza perlomeno sul fronte delle aziende grandi e grandissime per via dei progetti di adeguamento al GDPR. Tuttavia, nonostante questa "tenaglia" mediatico/normativa che ben difficilmente si ripresenterà nel breve periodo, la campagna elettorale non ha tenuto in nessuna considerazione il tema della sicurezza informatica e della necessità di aumento dell'attenzione dei cittadini, della pubblica amministrazione e delle imprese su questo fenomeno.

In termini numerici, nel Report leggerete che si è assistito ad una crescita del 240% degli attacchi informatici rispetto al 2011, anno a cui risale la prima edizione del Rapporto Clusit, e del 7% rispetto al 2016. Ma non è tanto il dato numerico a spaventare quanto invece l'elemento qualitativo sottostante: oggi il fenomeno mira a interferire in maniera pesante non solo nella vita privata dei cittadini (peraltro vittime nel 2017 di crimini estorsivi su larghissima scala) quanto invece sul piano finanziario e geopolitico.
Insomma, il gioco si fa serio e un altro innalzamento del livello potrebbe non essere sopportabile.
Alcuni dati: il Rapporto Clusit 2018 sottolinea come il Cybercrime (la cui finalità ultima è sottrarre informazioni, denaro, o entrambi), è sempre la prima causa di attacchi gravi a livello mondiale (76% degli attacchi complessivi, in crescita del 14% rispetto al 2016).
Inoltre, sono in forte aumento rispetto gli attacchi compiuti con finalità di Information Warfare con un preoccupante +24% rispetto al 2016 ed ancora il Cyber Espionage (lo spionaggio con finalità geopolitiche o di tipo industriale, a cui va tra l'altro ricondotto il furto di proprietà intellettuale) cresce del 46% rispetto al precedente periodo di osservazione.
Il dato più interessante di tutti, e più preoccupante, è però quello relativo ai costi generati globalmente dalle sole attività del Cybercrime: dal Rapporto Clusit 2018 emerge infatti che sono quintuplicati per un importo complessivo, come già scritto a inizio prefazione, di 500 miliardi di dollari nel 2017. Si deve considerare, nel calcolo, che nel corso del 2017 truffe, estorsioni, furti di denaro e di dati personali hanno colpito quasi un miliardo di persone nel mondo, causando ai soli privati cittadini una perdita stimata in 180 miliardi di dollari.
E l'Italia come è messa in questo contesto?
Sulla base delle cifre in gioco a livello globale noi stimiamo che l'Italia nel 2016 abbia subito danni derivanti da attività di cyber crimine per quasi 10 miliardi di euro. Non abbiamo dati

più recenti e non interessa forse neanche sapere se la cifra sovra o sottostima i danni.
L'ordine di grandezza è sintomatico di un problema più ampio perché comunque sia i danni appaiono essere 10 volte superiori alla stima degli investimenti in sicurezza risultate dalle ricerche dell'Osservatorio Sicurezza & Privacy del Politecnico di Milano.

Come nelle precedenti edizioni, il Rapporto Clusit 2018 dedica nei cosiddetti "Focus On" approfondimenti a singoli settori e a problematiche particolarmente attuali in tema di sicurezza cyber, a firma di esperti autorevoli. Quest'anno sono in evidenza la Sicurezza Marittima, l'Industria 4.0, il Cloud, la Mail Security, il Business Risk, le attività di Profiling, la diffusione delle criptovalute e la Blockchain, il Ransomware, la Gestione dei Fornitori.

Come già accaduto nei mesi precedenti al Rapporto Clusit 2017 l'attenzione mediatica sul tema è fortissima e si contano a centinaia se non a migliaia gli eventi che vengono organizzati in Italia e che ruotano attorno, in questo momento storico, alla sicurezza informatica e al GDPR.
Per questo motivo ci aspettiamo che gli investimenti in sicurezza aumentino così come ci attendiamo che sempre più forte sarà la spinta verso la esternalizzazione con la finalità di aumentare la sicurezza delle imprese e pubbliche amministrazioni che non avranno mai la capacità economica di proteggersi adeguatamente.

Vi lascio quindi alla lettura del Rapporto Clusit 2018 che avete fra le mani, augurandomi ancora una volta che la nostra ricerca serva ad aumentare la consapevolezza della necessità di una maggiore e sempre più efficace cultura della sicurezza informatica.

Ringrazio tutti coloro che hanno dedicato tempo e sforzi alla stesura del Rapporto Clusit 2018 e mi auguro che le elezioni politiche ci consegnino un governo ancora più attento a questa tematica e che miri alla cultura della sicurezza informatica fin dai più giovani e che completi e renda attuabile un quadro di indirizzo e normativo che permetta di raggiungere gli importanti traguardi necessari per vincere una sfida difficilissima.

2.500 copie cartacee, oltre 70.000 copie in elettronico e più di 300 articoli pubblicati nel 2017, 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 inizia con una panoramica degli eventi di cyber-crime più significativi degli ultimi 12 mesi. Possiamo dire che il 2017 si è caratterizzato come "l'anno del trionfo del Malware, degli attacchi industrializzati realizzati su scala planetaria contro bersagli multipli e della definitiva discesa in campo degli Stati come attori di minaccia". Per quanto riguarda gli impatti, i numeri parlano chiaro: nel periodo considerato dalle nostre analisi (2011-2017), i costi generati globalmente dalle sole attività cybercriminali sono quintuplicati, passando da poco più di 100 miliardi di dollari nel 2011 a oltre 500 miliardi nel 2017, quando truffe, estorsioni, furti di denaro e dati personali hanno colpito quasi un miliardo di persone nel mondo, causando ai soli privati cittadini una perdita stimata in 180 miliardi di dollari. Fatte salve tutte le considerazioni di dettaglio a partire dai dati raccolti per il 2017, il problema più grave ed urgente rimane la cronica (e drammatica) insufficienza degli investimenti in cyber security nel nostro Paese, che ci pone sostanzialmente ultimi tra i paesi avanzati e rischia di condizionare seriamente lo sviluppo dell'Italia ed il benessere dei suoi cittadini nei prossimi anni.

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 35 milioni di eventi di sicurezza (circa il doppio dell'anno scorso).
L'analisi degli attacchi è poi completata da due contributi tecnici: il "Rapporto 2017 sullo stato di Internet ed analisi globale degli attacchi DDoS e applicativi Web" e "Ransomware 2017 in Italia – WannaCry, NotPetya/EternalPetya, BadRabbit… ma non solo".
Seguono le rilevazioni e segnalazioni della Polizia Postale e delle Comunicazioni, del CERT Nazionale e del CERT-PA.

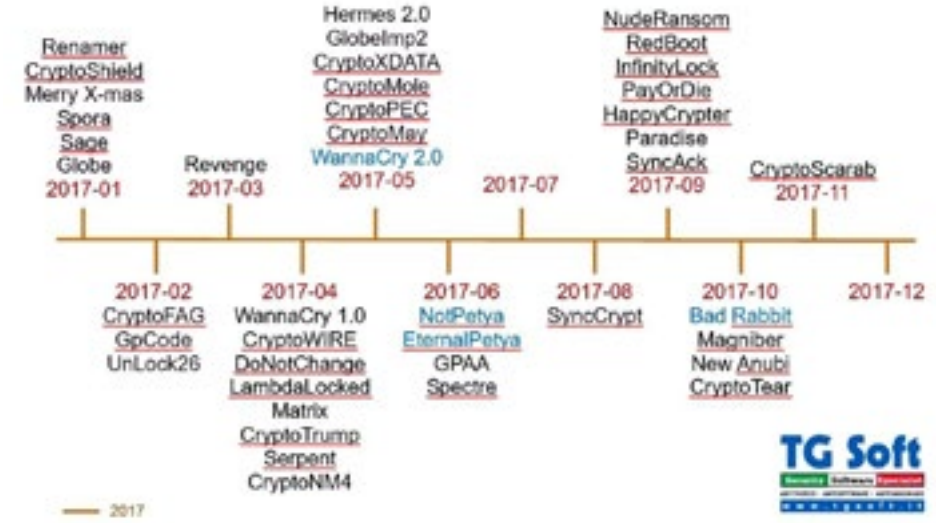
Presentiamo a questo punto l'abituale capitolo dedicato al settore FINANCE, con 3 contributi: "Elementi sul Cyber-crime nel settore finanziario in Europa"; "Analisi del Cyber-crime in Italia in ambito finanziario nel 2017"; "Carding – Tecniche di vendita: evoluzioni recenti e future".

Nel momento in cui sta andando in stampa il Rapporto Clusit, mancano solo novanta giorni alla scadenza del 25 maggio ma tutto il 2018 sarà l'anno di avvio dell'era del GDPR. Ci è parso quindi indispensabile inserire nel Rapporto 2018 uno "Speciale GDPR", che contiene 2 contributi, "GDPR ai blocchi di partenza" e "La notifica del Data breach: opportunità o adempimento burocratico?". Lo Speciale GDPR contiene anche i risultati di una survey realizzata dagli Osservatori del Politecnico di Milano sull'impatto del GDPR sulle aziende italiane.
Anche in questa edizione del rapporto, troviamo un'analisi del mercato italiano della sicurezza IT, realizzata appositamente da IDC Italia.

Questi sono infine i temi trattati nella sezione FOCUS ON: «INDUSTRY 4.0: La nuova frontiera dei cyber criminali nell'anno del GDPR"; "Maritime e Sicurezza IT"; "Email Security: I trend rilevati in Italia nel corso del 2017"; "Attacchi e difese nel Cloud Computing nel 2017"; "La Cyber Security, una priorità per il Board; "La governance dei fornitori: adottare un maturity model efficace"; "Il fattore umano nella gestione dell'innovazione e dell'information security aziendale (Social Engineering e Social Profiling)"; "La diffusione delle criptovalute: rischi ed opportunità in tema di sicurezza e regolamentazione del mercato".

## Ransomware 2017 in Italia – WannaCry, NotPetya/ EternalPetya, BadRabbit… ma non solo [A cura di TG Soft]

Anche nel 2017 i ransomware si sono presentati con tutta la loro devastante potenza distruttiva. Nei primi mesi del 2017 sono continuate in modo massivo le campagne del CryptoLocker (TorrentLocker), Cerber e Locky, ma non sono mancati i casi eclatanti di nuovi ransomware che hanno contraddistinto il 2017 tra maggio e ottobre.




Già a partire da gennaio troviamo una nutrita schiera di nuovi ransomware che hanno colpito anche l'Italia: Renamer; CryptoShield; MerryXmas; Spora; Sage e Globe.

Il Trojan.Win32.Renamer è da considerarsi un ransomware particolare, perché non cifra il contenuto del file, ma il nome del file, rendendo inaccessibile ogni esecuzione del programma colpito. Si diffonde attraverso un attacco al desktop remoto attraverso l'utente "*Guest*" o altri utenti con **password deboli**.
Quando il malfattore riesce ad entrare nel computer delle vittima esegue il payload con il **Trojan.Win32.Renamer**.
Ogni file viene rinominato aggiungendo il prefisso iniziale "**unCrypte@INDIA.COM_**" seguito dalla cifratura del nome originale con l'algoritmo **AES 256.**
Per conoscere il riscatto richiesto è necessario inviare un email a: unCrypte@INDIA.COM
Il riscatto richiesto da **Trojan.Win32.Renamer** è di 0,5 BTC.
Fortunatamente è possibile recuperare i file che sono stati cifrati riportandoli al loro nome originario senza, necessariamente, dover pagare il riscatto.

A febbraio sono stati segnalati *CryptoFAG*, *GpCode*, *UnLock26*.
Un marzo in frenata con un solo nuovo ransomware segnalato realmente circolante, si tratta del *Revenge*.

I segnali di febbraio e marzo avrebbero potuto lasciar pensare ad un forte rallentamento della diffusione di nuovi ransomware, ma ad aprile vi è una nuova recrudescenza del fenomeno: *WannaCry 1.0*; *CryptoWIRE*; *DoNotChange*; *LambdaLocked*; *Matrix*; *CryptoTrump*; *Serpent*; *CryptoNM4* sono solo alcuni dei nuovi ransomware scoperti. Molti di questi nuovi ransomware sembrano siano stati sviluppati per goliardia, come il *CryptoTrump* ispirato al presidente degli Stati Uniti d'America, ma altri, come WannaCry 1.0, danno inizio ad un nuovo filone di attacco che toccherà il suo apice il 12 maggio.

Il mese di maggio vede consolidarsi il fenomeno ransomware con: *Hermes 2.0*; *GlobeImposter 2.0*; *CryptoXData*; *CryptoMole*; *CryptoPec*; *CryptoMay* e ultimo, ma non ultimo, ***WannaCry 2.0***.

Il vettore d'infezione utilizzato da *GlobeImposter 2.0* nella campagna di maggio è stata la posta elettronica, dove il messaggio infetto conteneva in allegato un file zip con all'interno un Javascript con estensione **.js**.
Tale file **.js** ha funzione di dropper e quando viene eseguito, procede a scaricare ed eseguire il payload dal seguente sito: hxxp://pichdollard[.]top/admin[.]php?f=404

Una volta scaricato ed eseguito, il ransomware avvia un processo di cifratura dei file di dati presenti nel PC e nella rete.
Ai file cifrati da GlobeImposter 2.0 viene aggiunta l'estensione ***.crypt***, che avranno quindi la seguente struttura: *<nomefile>.<estensione>****.crypt***
Il riscatto richiesto è di 1 Bitcoin da accreditare sul seguente portafoglio (Wallet):
**1FuCGsCmmGWZnDkzg2aa7y6RvK3KP7TG7K**

Alla data di venerdì 19 maggio,il wallet dove vengono incassati i riscatti di GlobeImposter 2.0 risulta avere incassato solamente 1 bitcoin.
Dall'analisi del wallet, visti i ridotti incassi, sembrerebbe essere, per ora, un ransomware a bassa diffusione oppure un test per verificare se la metodologia di pagamento è da considerarsi agevole per gli utenti ricattati che volessero pagare il riscatto.

**CryptoPEC** alias **PEC 2017** è un ransomware che poteva avere un impatto devastante sugli enti/imprese italiani. Anche per il CryptoPEC il vettore d'infezione è stata la posta elettronica attraverso due tipologie distinte di campagne mail, entrambe scritte in un buon italiano. La prima è l'invio di un curriculum da parte di una fantomatica "Nevia Ferrara" che si proponeva come Analista Contabile, qui il target erano gli studi di commercialisti e più

in generale le aziende. Singolare è la mail del mittente: nevia.ferrara(at)agenzia-entrate.com
La seconda, sempre inviata dalla fantomatica "Nevia Ferrara", che intendeva rendere noto ad un Primo Cittadino, la propria denuncia riguardo un dissesto stradale che le ha provocato un incidente. In questo caso il target erano i comuni italiani.

La richiesta di riscatto era di 1 BTC se il pagamento avviene entro 120 ore, raddoppia se fatto successivamente ma non oltre i 30gg.
Tutti i file cifrati vengono rinominati con estensione **.PEC**
Analizzando le mail, gli autori sembrerebbero essere ragionevolmente italiani, anche se i Cyber-ricattatori si appoggiano a server olandesi per la loro infrastruttura e quindi potrebbero anche non essere italiani, ma godere di collaborazioni locali per la corretta redazione delle mail e dei testi delle pagine di richiesta di riscatto.
Le prime segnalazioni di attacchi CryptoPEC sono dei primi giorni di maggio, sebbene come impostazione potesse sembrare un ransomware particolarmente temibile e redditizio per i suoi creatori, il 12 maggio i Cyber-ricattatori danno l'annuncio della chiusura del progetto con il rilascio della Master Key, cioè della chiave di decrittazione universale.
Come già avvenuto per la chiusura del progetto "Tesla" nel maggio 2016 viene da chiedersi il perché di questa decisione… Naturalmente, ancora una volta, ai posteri l'ardua sentenza.

## 12 maggio 2017 – Attacco mondiale WannaCry 2.0

Venerdì 12 maggio 2017 si diffonde la notizia di un attacco mondiale di un nuovo potentissimo ransomware chiamato **WannaCry 2.0**.
La sua peculiarità di diffusione è che non utilizza un vettore di infezione "classico", come potrebbe essere tramite invio di email o siti infetti, ma sfrutta per la sua diffusione una vulnerabilità dei Sistemi Operativi Windows chiamata ***EternalBlue***.
Se nei precedenti vettori d'infezione giocava un ruolo fondamentale l'utente, ad esempio con l'apertura dell'allegato infetto, con EternalBlue non è necessario l'interazione da parte dell'utente per essere infettato. Ogni computer è potenzialmente attaccabile da un altro PC precedentemente infettato da WannaCry.
La vulnerabilità denominata ***EternalBlue*** è stata resa pubblica dal gruppo hacker **Shadow Brokers il 14** aprile 2017 che avevano "trafugato" questa informazione e l'arsenale di armi cibernetiche "rubandole" nell'agosto 2016 ad un altro gruppo di hacker chiamato **Equation Group,** probabilmente fornitori della **National Security Agency** (NSA) americana.
Il ransomware WannaCry procede a "scandagliare" gli indirizzi IP della rete alla ricerca di computer ove sia presente questa vulnerabilità e quindi procedere ad attaccarli.
Dall'analisi del codice di WannaCry 2.0 si rileva immediatamente la presenza di una funzionalità di Kill Switch che permette ai suoi autori, ma come vedremo anche ad altri, di bloccare l'attacco.
Gli autori di WannaCry hanno inserito un controllo per bloccare la propagazione di questa prima release verificando se è attivo il dominio hxxp://www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com, e se questo risulta essere online il

ransomware termina senza fare ulteriori operazioni.
Dall'analisi del codice questo controllo sembra essere stato inserito in modo un po' affrettato, quasi "all'ultimo momento" poco prima del suo rilascio, probabilmente per paura delle possibili conseguenze che questo ransomware potesse avere.
Fatto sta, che un ricercatore inglese che si fa chiamare MalwareTech, analizzando il codice è riuscito ad intuirne la presenza e ha ben pensato di registrare il dominio, rallentando l'infezione. Gli autori del ransomware però si sono affrettati a mettere in circolazione release di WannaCry 2.0 senza Kill Switch.
Questo ransomware ha avuto un impatto mediatico a livello mondiale. I mezzi di informazione hanno diffuso notizie quanto mai allarmistiche, dell'ordine di 150 paesi colpiti e oltre 300.000 computer bloccati da WannaCry. Portando alla ribalta un tema troppo spesso trascurato riguardo alla sicurezza informatica dei computer, che inizia dall'aggiornamento dei Sistemi Operativi, infatti per evitare l'infezione sarebbe bastato aver effettuato gli aggiornamenti del S.O. resi disponibili da Microsoft già da oltre un mese.

## I guadagni di WannaCry


Sulla base dei dati di diffusione del ransomware segnalati dai mezzi di informazione, incrociandoli con i tre wallet dove vengono indirizzati i pagamenti del riscatto in BitCoin, si evince che al 27 giugno 2017, cioè circa 45 giorni dopo l'inizio dell'attacco, l'incasso complessivo dei malfattori era costituito da 350 transazioni complessive cioè il pagamento di 350 riscatti, per un totale di poco superiore ai 50 BitCoin, che al cambio dell'epoca (2100 USD) corrispondevano a poco più di 122 mila dollari.

## L'Impatto di WannaCry 2.0 sull'Italia

La copertura mediatica che questo attacco ha avuto per oltre una settimana, passando ogni giorno la notizia ai telegiornali, come anche a varie trasmissioni di intrattenimento con interviste e opinioni di vari esperti, ha fatto percepire a tutti di poter essere in ogni momento

sotto attacco o poter essere vittime di queste temibile minaccia. Tutto questo ha portato ad aumentare la consapevolezza del pericolo imminente non solo da parte dei tecnici informatici, ma anche dell'opinione pubblica.
L'impatto sull'Italia di WannaCry è stato fortunatamente meno critico di quello che l'opinione pubblica ha percepito probabilmente perché, questo ransomware, non aveva come prioritario l'attacco agli indirizzi IP italiani.

## Chi potrebbe esserci dietro a WannaCry

Vi sono varie ipotesi su chi ci sia dietro a WannaCry, taluni dicono che si tratti della Corea del Nord e che dietro ci sia il famigerato gruppo Lazarus, quindi WannaCry 2.0 sarebbe da considerarsi un ransomware / malware di stato.
Si potrebbe anche ipotizzare che il gruppo Shadow Brokers abbia ritenuto opportuno dare una prova di efficacia delle tecnologie trafugate ad Equation Group facenti parte dell'arsenale delle armi cibernetiche di NSA, per dimostrare a potenziali interessati l'efficacia di questi codici e incrementarne il prezzo.
Viste le cifre ottenute con i riscatti pagati per attacchi da WannaCry 2.0 dell'ordine dei 120.000,00 USD al 27 giugno si ritiene di poter escludere che l'obiettivo possa essere quello di fare guadagni con i riscatti.
Anche in questo caso ai posteri l'ardua sentenza…

Non ha fatto in tempo a placarsi l'interesse mediatico su WannaCry che a giugno 2017 si scatena un attacco di NotPetya/Eternal Petya un ransomware / wiper simile alle creazioni di Janus nello specifico a Petya GoldenEye.

## 27 giugno NotPetya alias Eternal Petya

Martedì 27 giugno si scatena l'attacco di un altro ransomware che è fortemente somigliante a ***Petya***, in particolar modo alla versione Petya GoldenEye 4.0, che va a cifrare la Master File Table (MFT) dei dischi fissi. Anche in questa occasione viene sfruttata la vulnerabilità Eternal Blue che permettere la diffusione del malware/ransomware senza interazione con l'utente procedendo a "scandagliare" gli indirizzi IP della rete alla ricerca di computer ove sia presente questa vulnerabilità e quindi procede ad attaccarli infettandoli.
Questa release di Petya procede a cifrare la MFT con chiave generata dall'algoritmo SALSA20 mentre la cifratura dei file avviene con l'algoritmo AES.
Il riscatto è di 300 $ in BitCoin:

- i file cifrati possono essere recuperati pagando il riscatto;
- la MFT è cifrata con una chiave casuale non collegata al'ID della vittima che non ne permette il recupero anche pagando il riscatto.

## NotPetya/Eternal Petya è Ransomware o Wiper ?

Questo malware è molto simile a ***Petya GoldenEye*** di Janus, ma non è una sua variante sebbene i due codici differiscano di soli 43 byte. Gli autori di ***NotPetya/EternalPetya*** han-

no eseguito un "dump" dei settori infetti di **Petya GoldenEye** da un computer infetto. Il codice di Petya GoldenEye a livello di settori è stato modificato con un hexeditor e inglobato nel progetto ***NotPetya/EternalPetya***. Come detto i due codici differiscono per qualche decina di byte, 43 per l'esattezza, ad esempio in NotPetya/EternalPetya è stata eliminata la visualizzazione del teschio della morte, che invece contraddistingue tutte le versioni di Petya realizzate da Janus. L'inglobazione del "dump" di Petya in NotPetya/EternalPetya, non ha permesso di gestire in modo corretto le generazione della chiave per cifrare l'MFT con il "core" di Petya GoldenEye e il corrispondente ID per la sua decifratura. Per questo motivo vi è l'impossibilità di decifrare l'MFT anche pagando il riscatto, molti ricercatori hanno quindi ipotizzato che si tratti invece di un wiper e non di ransomware. Janus, l'autore del codice originale del ransomware Petya, si è trovato, suo malgrado, coinvolto in questo attacco mondiale.

Lo stesso Janus dai suoi account twitter ha smentito che si tratti di una sua creazione e, forse sentendosi indirettamente responsabile dei danni prodotti, con l'intento di aiutare le vittime, ha rilasciato la Master Key di tutte le versioni di Petya, nella speranza che possa essere utile per la decifratura dell'MFT.

Purtroppo la Master Key rilasciata da Janus non è utile allo scopo.

## Chi era l'obiettivo dell'attacco


*Supermercato in Ucraina bloccato da NotPetya/EternalPetya*

NotPetya si è diffuso principalmente in Ucraina e in alcune nazioni baltiche, fortunatamente l'obiettivo primario, come per WannaCry, non è stata l'Italia poiché in particolare per NotPetya non c'è la possibilità di recuperare la MFT.

Alcuni analisti ritengono che questo attacco sia opera dei famigerati hacker russi e che sia stato architettato/commissionato dalla Russia. Da cui si ritiene che l'impossibilità di decifrare l'MFT anche da parte dei Cyber-ricattori non sia un errore ma una scelta voluta e, se così fosse, non si dovrebbe più parlare di ransomware ma di wiper cioè di un malware realizzato al solo scopo di danneggiamento.

Di fatto un attacco deliberato alle infrastrutture informatiche ucraine.
Da analisi più approfondite sui vettori di infezione utilizzati, si è scoperto che la prima diffusione di ***NotPetya/EternalPetya*** è avvenuta attraverso l'aggiornamento del software gestionale M.E. Doc. Si è scoperto che il server per l'aggiornamento era stato precedentemente attaccato e che l'upgrade del software gestionale era stato modificato per contenere il dropper di NotPetya/EternalPetya. È interessante notare che nel mese precedente di maggio, lo stesso server per l'aggiornamento del gestionale M.E. Doc aveva distribuito un altro ransomware chiamato CryptoXDATA, noto anche con il nome di AES-NI. Dietro al ransomware CryptoXDATA (alias AES-NI) sembra vi sia un gruppo che si fa chiamare TELEBOTS, il quale potrebbe essere collegato anche agli attacchi di Black Energy alle centrali elettriche in Ucraina.

La risonanza mediatica a livello mondiale data dai media a **NotPetya** e all'impossibilità di poter recuperare i dati ha fortemente rallentato il rilascio di nuovi ransomware poiché i cyber-ricattatori hanno, probabilmente, preferito attendere qualche mese così che non fosse troppo fresco nell'opinione pubblica il ricordo che neanche pagando sarebbe stato possibile recuperare i dati resi inaccessibili dalla cifratura dell'MFT.

A settembre vi è stata la ripresa della produzione anche di nuovi ransomware a livello goliardico è doveroso citare ***NudeRansomware*** che per fornire la chiave di decifratura dei file richiede delle foto nude, almeno dieci, del proprietario del PC maschi o femmine indifferentemente, la *par condicio* prima di tutto!

## Bad Rabbit il coniglio cattivo!


A ottobre riceve grande interesse mediatico il ransomware ***Bad Rabbit*** molto simile a NotPetya, poiché non si limita a cifrare i file , ma cifra anche i settori del disco fisso utilizzando un programma opersource chiamato "DiskCryptor". Bad Rabbit utilizza due vettori d'infezione per propagarsi:

- il primo, attraverso la navigazione su siti compromessi, dove viene richiesto di scaricare un finto Flash player;
- il secondo attraverso un attacco brute force delle credenziali attraverso il protocollo Samba per infettare il maggior numero di PC nella rete locale.

***Bad Rabbit*** è simile a NotPetya/EternalPetya, ma oltre a cifrare i file di documento o dati, esso cifra anche i settori del disco fisso attraverso un driver modificato del programma "Disk Cryptor", rendendo inaccessibile il disco.

I Cyber-ricattatori, in questa occasione, nelle istruzioni per il pagamento del riscatto assicurano che la chiave di cifratura è realmente disponibile, naturalmente previo pagamento del riscatto. Vi è il forte sospetto che dietro a Bad Rabbit ci sia ancora il gruppo Telebots, che in questo caso hanno sostituito il problematico "dump" di Petya, con il programma di cifratura dei dischi "Disk Cryptor". In questo caso è però possibile decifrare il disco pagando il riscatto.

A novembre si diffonde anche in Italia ***CryptoScarab*** che si "innesca" tramite l'esecuzione di uno script (.VBS) contenuto in un file archivio (7z nei file analizzati dal CRAM ) allegato ad una **falsa mail**.
Le caratteristiche del messaggio che il malcapitato utente riceve, sembrano quelle che si manifestano quando si ricevono delle scansioni di documenti nella casella di posta. Scansioni possibili mediante particolari stampanti multifunzione.

## Attacchi Ransomware in Italia su computer reali verificati

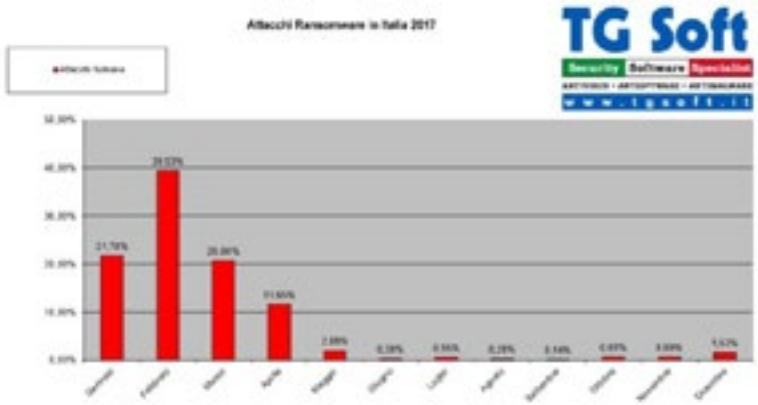
Si può notare che il primo grafico ha visto il picco degli attacchi Ransomware in Italia nel febbraio 2017 con quasi il 40% degli attacchi rispetto al totale dell'anno.


Questi per la maggior parte, sono riconducibili a ransomware persistenti come Cryptolocker. Da maggio queste campagne sembrano, almeno in Italia, essere scomparse o quasi.

Come già segnalato gli attacchi mondiali da WannaCry, NotPetya e BadRabbit, seppur temibilissimi, non trovano particolari riscontri oggettivi in Italia poiché, fortunatamente, il nostro paese non è risultato un obiettivo primario.
Singolare è l'andamento degli attacchi ransomware che tendono a concentrarsi nei primi 4/5 mesi dell'anno da gennaio a aprile/maggio, cosa già osservata nel 2016 e che si è ripetuta anche nel 2017 per poi andare scemando ma procedendo in modo più o meno stabile.
Gli attacchi Ransomware rilevati in Italia riguardano complessivamente 24 famiglie/tipologie distinte. L'ha fatta da padrone, praticamente incontrastato l'arcinoto **CryptoLocker** responsabile di oltre il 76% degli attacchi nell'anno.

## Conclusioni

Il 2017 è stato contraddistinto da tre grandi attacchi ransomware a livello mondiale. Nei primi quattro mesi dell'anno era continuato il trend della campagne di ***CryptoLocker***, ***Cerber*** e ***CrySis***, già ben noti dal 2016. Da maggio in poi, queste tipologie di campagne sono scemate, lasciando il posto ad attacchi "spot", come abbiamo visto il 12 maggio WannaCry 2.0, 27 giugno NotPetya e il 24 ottobre Bad Rabbit.
Dall'analisi dei dati delle statistiche, si è notato un calo nelle campagne rispetto al 2016, non solo di quelle note, ma anche nello sviluppo di nuove famiglie di ransomware.



## Quali aspettative per il 2018…

I ransomware, è bene ricordarlo, sono dei malware specificatamente progettati a scopo di ricatto e quindi con l'obiettivo del guadagno. Si ritiene che nel 2018 le aspettative dovrebbero far pensare ad una progressiva riduzione degli attacchi ransomware poiché non è irragionevole ipotizzare che alcuni dei Cryber-ricattatori possano valutare di concentrare i loro sforzi, ed alcuni probabilmente lo stanno già facendo, nella produzione e diffusione di malware che sfruttano i processori dei PC / Server colpiti per "minare" crypto-valute (BitCoin ma non solo…).

In questo modo non producono danni devastanti agli utenti infetti ma sfruttano "solamente" le risorse dei processori producendo dei più o meno sensibili rallentamenti dei PC / Server. Già da qualche tempo alcuni siti web sono stati opportunamente modificati sia dai loro proprietari, ma anche all'insaputa di questi, dove le pagine più visitate sono state integrate con dei codici di "mining" in grado di sfruttare le potenzialità di calcolo dei computer che consultano queste pagine per "minare" cripto-valute. Da queste pagine, può accadere che vengano anche rilasciati in modalità, più o meno nascosta, dei codici di "mining" anche sulla macchina locale di modo che l'estrazione di Cripto-Valuta possa continuare anche dopo la chiusura della/e pagina/e Web.

# Gli autori del Rapporto Clusit 2018

**Andrea Antonielli**, laureato in Giurisprudenza presso l'Università degli Studi di Milano nel 2016. È Ricercatore presso gli Osservatori Digital Innovation del Politecnico di Milano e si occupa dei temi connessi all'Information Security & Privacy, con particolare focus sulla normativa europea in materia di protezione dei dati personali.

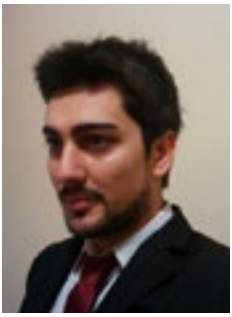
**Luca Bechelli,** Information Security & Cyber Security Advisor, svolge dal 2000 consulenza per progetti nazionali ed internazionali su tematiche di Compliance, Security Governance, Risk Management, Data Protection, Privilege Management, Incident Handling e partecipa alla progettazione ed al project management per attività di system integration. Svolge attività di ricerca e sviluppo tramite collaborazioni con enti di ricerca e associazioni, 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. Svolge attività di divulgazione su tematiche di sicurezza IT, mediante la partecipazione a convegni, la pubblicazione di articoli su testate generaliste o di settore e la partecipazione a gruppi di lavoro.

**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), dove svolge il ruolo di program officer. Ha acquisito esperienza nei programmi di contrasto alla criminalità informatica ed alla criminalità organizzata. È attualmente responsabile dei programmi relativi alla sicurezza informatica e all'uso improprio della tecnologia, tra cui l'utilizzo terroristico di internet. Sta approfondendo la ricerca in tema di sfide e opportunità delle nuove tecnologie, tra cui la robotica e l'intelligenza artificiale, la blockchain, i big data e il quantum computing. È membro dell'Advisory Group dello European Cybercrime Center (EC3) presso l'Europol. È co-fondatrice del Tech and Law Center.

**Giancarlo Butti** ha acquisito un master in Gestione aziendale e Sviluppo Organizzativo presso il MIP Politecnico di Milano. Si occupa di ICT, organizzazione e normativa dai primi anni 80. Security manager, project manager e auditor presso gruppi bancari e consulente in ambito sicurezza e privacy. Ha all'attivo oltre 700 articoli e collaborazioni con oltre 20 testate. Ha pubblicato 21 fra libri e white paper alcuni dei quali utilizzati come testi universitari; ha partecipato alla redazione di 9 opere collettive. Partecipa ai gruppi di lavoro di ABI LAB sulla Business Continuity, Rischio Informatico, GDPR, Blockchain, di ISACA/AIEA, di Oracle Community for Security, di UNINFO sui profili professionali privacy; è fra i coordinatori di europrivacy.info. È membro della faculty di ABI Formazione per il quale fra gli altri ha curato il Percorso professionalizzante Privacy Expert e DPO in banca. È docente presso ITER, ISACA/AIEA, CLUSIT, Convenia, Informa Banca, CETIF, IKN, Università Statale di Milano. Ha inoltre acquisito le certificazioni/qualificazioni LA BS7799, LA ISO/IEC27001, CRISC, ISM, DPO, CBCI, AMBCI.

**Nunzia Ciardi**, Dirigente Superiore della Polizia di Stato, è il Direttore del Servizio Polizia Postale e delle Comunicazioni. Laureata in giurisprudenza, con una pregressa pluriennale esperienza, maturata prima come Direttore della I Divisione del Servizio Polizia Postale e successivamente come Dirigente del Compartimento Polizia Postale e delle Comunicazioni del Lazio, coordina attualmente le unità specializzate della Polizia di Stato nel contrasto al cyberterrorismo, al financial cybercrime, alla pedopornografia on-line, alla tutela delle infrastrutture critiche informatiche nazionali, all'hacking e ai crimini informatici in generale.
È membro dell' European Union Cybercrime Taskforce di Europol e del Progetto europeo EU-OF2CEN per l'adozione di strategie comuni contro il crimine organizzato nel settore delle frodi on-line. È coordinatore e membro di gruppi di lavoro sulla tutela dei minori nel mondo della comunicazione, sulla disinformazione in ambito di piattaforme digitali, e sulla sicurezza digitale. È rappresentante del Ministero dell'Interno in seno al Nucleo sicurezza cibernetica ed al Tavolo Tecnico Cyber. Svolge attività di docenza presso le scuole di Polizia e numerosi Enti.

**Davide Del Vecchio**, membro del direttivo Clusit, lavora in ambito Cyber Security da circa 15 anni. Negli anni ha lavorato come ricercatore indipedente, ethical hacker, incident handler e SOC manager ed è attualmente il responsabile della Cyber Security di una grande multinazionale italiana. È co-fondatore del "Centro Hermes", associazione no-profit che si occupa di trasparenza e diritti digitali e nel 2014 ha vinto il premio Fibonacci come "miglior informatico dell'anno".



**Luca Dinardo**, laureato in Sicurezza dei sistemi e delle reti informatiche presso l'Università degli Studi di Milano nel 2008, consulente in ambito Cyber Security da 10 anni. Lavora in Lutech dal 2015, specializzato in tematiche di Cyber Security in contesti CERT e SOC, si occupa attivamente di Cyber Threat Intelligence, Malware & Threat Analysis, Incident Response e Cyber Deception. Svolge attività di ricerca e sviluppo mirate all'analisi ed al contrasto di fenomenti legati al Cyber Crime.

**Luca Dozio**, laureato in Ingegneria Gestionale al Politecnico di Milano. Lavora come Ricercatore per gli Osservatori Digital Innovation del Politecnico di Milano sulle tematiche del Cloud e dell'Information Security.

**Giorgia Dragoni** si è laureata in Ingegneria Gestionale al Politecnico di Milano, indirizzo Manufacturing & Management, con una Tesi sull'evoluzione di ruoli e competenze all'interno delle Direzioni ICT.
È Ricercatrice presso gli Osservatori Digital Innovation del Politecnico di Milano e si occupa dei temi connessi all'Information Security & Privacy e ai Big Data Analytics.

**Francesco Faenzi**, laureato in Scienze dell'Informazione, certificato CISSP, CISA, SANS GCIH e ITIL , è Head of Cyber Security Business Platform in Lutech. È stato Security Advisor e Head of IT Security Technologies Team in Securteam (oggi parte di Leonardo) fino al 2001. Ha poi continuato in Lutech, dove dirige i professional service, il business development, la ricerca e innovazione in generale in ambito Cyber Security e con particolare focus su Cyber Threat Intelligence, Breach Detection and Incident Response, Ethical Hacking, Governance Risk & Compliance, Cybersecurity by Design, Data Classification & Encryption, Telco Backbone Protection. Ha partecipato a progetti europei quali DRIVE, CANDELA, C2-SENSE e cura personalmente il Security Advisoring di grandi clienti. Speaker in numerose conferenze ed eventi (GCSEC, CLUSIT, ABILAB, ANIMP, ANIPLA, EECTF), è anche uno degli autori del libro Mondadori "La sicurezza dei sistemi informativi: teoria e pratica a confronto".

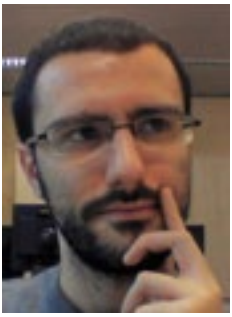
**Gabriele Faggioli**, legale, è amministratore delegato di Partners4innovation S.r.l. (a Digital360 Company di cui è socio e amministratore). È Presidente del Clusit (Associazione Italiana per la Sicurezza Informatica).
È Responsabile Scientifico dell'Osservatorio Security&Privacy del Politecnico di Milano. È Adjunct Professor 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 amminstrativa degli enti e nel diritto dell'editoria e del markerting. 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.co dell'anno".

**Sergio Fumagalli** è responsabile della Practice Data Protection di P4I, società di management consulting del Gruppo Digital360. È membro del direttivo di Clusit e del coordinamento di Europrivacy.info. Dal 2004 al 2012 è stato Vice Presidente del Cda di Webank Spa. Dal 1996 al 2001 è stato Deputato al Parlamento e Segretario della XIII Commissione Attività produttive. Co-autore delle pubblicazioni della Oracle Community for Security sui temi Fascicolo Sanitario Elettronico, Privacy nel cloud, Security e social media, Le frodi nella rete, è co-autore del testo "Privacy guida agli adempimenti", IPSOA 2004 (seconda editione 2005). È laureato in Fisica presso l'Università di Milano.

**Marco Tullio Giordano** è Avvocato dal 2008 ed esercita la professione presso il Foro di Milano, occupandosi prevalentemente di diritto penale delle nuove tecnologie, con particolare riguardo alla sicurezza informatica, alla protezione dei dati personali ed alla responsabilità di privati ed aziende in rete. Ha partecipato ad alcuni dei primi processi penali in tema di *cybercrimes* e violazione della privacy in Italia. Dal 2009 gestisce i rapporti con le Autorità Giudiziarie per alcune delle più conosciute *web companies* italiane ed internazionali e si occupa della formazione e dell'assistenza alle Forze di Polizia Giudiziaria in tema di richiesta di prestazioni obbligatorie agli Internet Service Provider e richieste di dati informatici attraverso le procedure previste dai *Mutual Legal Assistance Treaties*. È cultore della materia presso la cattedra di informatica giuridica della facoltà di Giurisprudenza dell'Università degli Studi di Milano Bicocca ed ha partecipato, in qualità di docente e relatore, a numerosi eventi formativi aventi ad oggetto il diritto delle nuove tecnologie. Ha conseguito la certificazione ISO Foundation per la gestione della sicurezza delle informazioni ed è *lead auditor* certificato UNI CEI ISO/IEC 27001:2014. Presta la propria consulenza in tema di *compliance privacy* e *cybersecurity* in favore di numerose aziende italiane. Iscritto alla Camera Penale di Milano, ha fatto parte del comitato di redazione dell'omonimo sito web. È autore di pubblicazioni specialistiche in tema di reati informatici. Scrive online di diritto e nuove tecnologie.

**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.



**Andrea Granata**, Cyber Security Specialist presso Communication Valley Reply, si occupa delle attività di prevenzione, analisi e gestione degli incidenti informatici e contrasto al Cyber Crime presso il Cyber Security Command Center (CSCC) di Communication Valley Reply. Ha una pluriennale esperienza come Security Tester, Fraud Expert e Security Data Analyst, con particolare attenzione ai temi della Malware Analysis, del Reverse Engineering e della Cyber Threat Intelligence. Collabora alla stesura del bollettino mensile ABI LAB focalizzato sui principali fenomeni di Phishing e malware rilevati a livello italiano ed è attualmente impegnato nelle attività di ingegnerizzazione ed erogazione dei servizi antifrode.

**Michele Onorato** oggi è Security Office Manager di Hitachi Systems CBT S.p.A. Vanta un'esperienza di oltre 10 anni nel settore dell'Information Technology e della Sicurezza Logica in particolare, con una carriera manageriale che gli ha permesso di assumere crescenti responsabilità sino a divenire anche punto di riferimento per le aziende partner del Systems Integrator Giapponese dall'anima italiana. Con una laurea in Matematica e una profonda esperienza tecnica, Michele vanta oltre 14 certificazioni e numerosissimi progetti in ambito security per realtà di rilievo, come SIAE o Ministero della Pubblica Istruzione, ma anche ruoli manageriali in importanti player del mercato IT europeo, quali Sistemi Informativi e Visiant Security. Come Security Department Manager di Hitachi, oggi Onorato ha la responsabilità di guidare un team altamente specializzato con la mission di aiutare quotidianamente le aziende private e pubbliche di grandi e medie dimensioni nell'implementazione di progetti di Cyber Security e Compliance, tramite l'erogazione di servizi gestiti ed utilizzando le migliori soluzioni tecnologiche presenti sul mercato.

**Stefano Orciari,** appassionato di tecnologia e matematica fin dall'età di 10 anni, intraprende il percorso di studi in Informatica presso l'Università degli Studi di Milano Bicocca specializzandosi in sicurezza e crittografia, conseguendo poi nel 2008 il Dottorato di Ricerca. Da 10 anni lavora e coordina numerosi progetti nel campo della sicurezza informatica. Da sempre interessato al cybercrime, è attualmente responsabile del Cyber Security Operation Center e dell'unità antifrode di Fastweb.

**Marco Pacchiardo** è Senior Enterprise Security Architect EMEA per Akamai Technologies. Ha iniziato la sua carriera nella sicurezza informatica nel 1995, lavorando per diverse aziende italiane tra cui Siosistemi, dove ha avuto modo di sviluppare nuove funzionalità di sicurezza e ampliare il portfolio aziendale. Successivamente è entrato a far parte di INS, in qualità di Principal Security Consultant. In questa posizione si è occupato di supporto ai clienti a livello globale e ha avuto l'opportunità di collaborare con aziende ed enti governativi su attività e progetti legati alla sicurezza informatica, alla compliance e al risk management. É poi approdato in BT Italia, dove ha lavorato con l'obiettivo di ottimizzare e consolidare il posizionamento dell'azienda relativamente alla sicurezza. Marco è autore di due libri, *Intranetworking* (1998) e *Azienda Sicura* (2003) e nel corso della sua carriera ha avuto modo di ideare e progettare innovativi servizi di sicurezza, compliance e risk management.

**Pamela Pace** è Amministratore unico della Obiectivo, advisory company specializzata nella gestione dell'information security che propone un'offerta di servizi di Cyber Security Strategy, Information Security Governance, Risk Intelligence, Risk Management. Negli anni ha rivestito molteplici incarichi di crescente responsabilità nel campo dell'information security, dell'innovazione e delle tecnologie. È componente della Commissione Tecnologie, Sicurezza e Mobile Payment dell'Associazione Italiana Istituti di Pagamento e Moneta Elettronica, Vicepresidente della Piccola Industria di Unindustria e componente del Comitato Tecnico Nazionale Ricerca ed Innovazione di Confindustria. È inoltre membro del comitato direttivo del Centro Ricerche Nuove Tecnologie e Processi di Pagamento

dell'Università degli Studi Internazionali di Roma e Docente del corso "La Gestione della Sicurezza delle Informazioni a Tutela del Patrimonio Aziendale" presso la Business School Scuola di Palo Alto.

**Alessio L.R. Pennasilico**, Information & Cyber Security Advisor, Security Evangelist, noto nell'hacker underground come -=mayhem=-, è internazionalmente riconosciuto come esperto dei temi legati alla gestione della sicurezza delle informazioni e delle nuove tecnologie. Per questa ragione partecipa da anni come relatore ai più rilevanti eventi di security italiani ed internazionali ed è stato intervistato dalle più prestigiose testate giornalistiche, radio e televisioni nazionali ed internazionali. All'interno di P4I, per importanti Clienti operanti nei più diversi settori di attività, sviluppa progetti mirati alla riduzione dell'impatto del rischio informatico/cyber sul business aziendale, tenendo conto di compliance a norme e standard, della gestione del cambiamento nell'introduzione di nuovi processi ed eventuali tecnologie correlate. Credendo che il cyber risk sia un problema organizzativo e non un mero problema tecnologico, Alessio da anni aiuta il top management, lo staff tecnico e l'organizzazione nel suo complesso a sviluppare la corretta sensibilità in merito al problema, tramite sessioni di awareness, formazione e coaching. Alessio è inoltre membro del Comitato Direttivo e del Comitato Tecnico Scientifico di Clusit, Presidente di Associazione informatici Professionisti - AIP, membro del Comitato di Schema UNI 11506 di Kiwa Cermet e Vice Presidente del Comitato di Salvaguardia per l'Imparzialità di LRQA, l'ente di certificazione dei Lloyd's.

**Andrea Piazza** ricopre il ruolo di WW Cybersecurity Architect, Chief Security Advisor in Microsoft, collaborando allo sviluppo dei servizi di cybersecurity di consulenza e supporto, alla formazione dei team di consulenza e al miglioramento della qualità dei progetti di sicurezza e delle attività di risposta agli incidenti. Nei 17 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 stato National Security Officer della filiale italiana di Microsoft, dove ha coordinato 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 ha coordinato i servizi di sicurezza del supporto Microsoft, come Security Assessment, Workshop, attività di risposta agli incidenti e di remediation, si è occupato in prima persona dell'attività di formazione e aggiornamento degli engineer di sicurezza, e collaborato 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 e ai rapporti CLUSIT 2016 e 2017. È certificato CISSP, ISO27001 Lead Auditor e ITIL.

**Alessandro Piva** si occupa da oltre dieci anni di ricerca sui temi dell'innovazione digitale. Dopo essersi laureato in Ingegneria delle Telecomunicazioni ed Ingegneria Gestionale al Politecnico di Milano, ha conseguito un Executive Master in Business Administration presso il MIP. Attualmente è Direttore di svariati Osservatori del Politecnico, quali l'Osservatorio Information Security & Privacy, l'Osservatorio Artificial Intelligence, l'Osservatorio Cloud Transformation.

**Domenico Raguseo** è Manager del team europeo di Technical Sales per IBM Security. Ha 19 anni di esperienza manageriale e 27 nel campo della cybersecurity in diverse aree. Domenico collabora con alcune università nell'insegnamento di Service Management e del Cloud Computing. 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 su Sicurezza delle Informazioni, Service Management, Cloud computing, Energy Optimization e Smarter Planet in eventi nazionali e internazionali.

**Marco Raimondi**, nato nel 1987, si laurea in Ingegneria delle Telecomunicazioni presso il Politecnico di Milano. Ha iniziato la sua carriera nell'ambito IT per poi orientare la sua attività nel mondo commerciale, con un focus particolare sul mercato Enterprise. Dal 2012 ha lavorato presso Vodafone Italia dove ha ricoperto nella Business Unit Enterprise dapprima il ruolo di Presales e successivamente il ruolo di Marketing Product Manager nel mercato delle PMI. Dal 2017 in Fastweb ricopre il ruolo di Product Manager responsabile dello sviluppo di servizi di sicurezza per il mercato Enterprise e del supporto alle attività di Go to Market.

**Pier Luigi Rotondo** si occupa di Technical Enablement per IBM Security. Con una laurea in Scienze dell'Informazione presso l'Università degli Studi di Roma "La Sapienza", ha ricoperto per oltre dieci anni incarichi di docenza presso università Italiane, tra cui il Master in Sicurezza delle Informazioni dell'Università di Roma "La Sapienza", e corsi di Dottorato per l'Università degli studi di Perugia. Organizza in per l'Italia alcuni degli eventi dell'iniziativa European Cyber Security Month, dell'Unione Europea, divulgando regole pratiche per il contrasto delle frodi online. È stato istruttore nella prima CyberChallenge nazionale, programma di addestramento alla cybersecurity per giovani di talento, e afferisce al Cyber Security National Lab.

**Rodolfo Saccani**, Security R&D Manager in Libra Esva, vive l'IT dal 1994, in qualità di sviluppatore, sistemista, consulente e project manager. Ha vissuto e lavorato negli USA e in Danimarca. Da sempre interessato al mondo della *security*, ha un'esperienza tecnica eterogenea: sistemi linux embedded, avionica sperimentale, telecomunicazioni sicure in ambienti ostili, TV connessa, controllo di processo e automazione industriale, ricerca clinica, piattaforme web SaaS. Per passione si occupa anche di sicurezza nel volo libero: consigliere alla sicurezza in FIVL (Federazione Italiana Volo Libero) dal 2007, è expert presso il CEN (Comitato Europeo di Normazione) e partecipa alla stesura delle norme europee di certificazione delle attrezzature da volo libero.
In Libraesva coordina la ricerca e sviluppo per l'e-mail security.

**Luca Sangalli** si è laureato in Sicurezza dei sistemi e delle reti informatiche presso l'Università degli Studi di Milano nel 2015 e da allora lavora presso Lutech occupandosi di tematiche di Cyber Security come Cyber Threat Intelligence Analyst, Researcher & Developer ed Ethical Hacking, specializzandosi in particolare nell'ambito Finance. Si occupa anche di attività di ricerca e sviluppo in contesto antifrode.

**Federico Santi**, Security Principal – South EMEA in DXC.technology, 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 fino ad assumere il ruolo di Director dei Security Services.La sua esperienza nella Security segue una vista risk & business-oriented centrando l'attenzione su processi (Security Monitoring & Incident Management), dati (Data Protection & Privacy) e utenti (Identity Governance). Tra le responsabilità principali Strategic Advisory, Relazioni Istituzionali e Go To Market. Numerose le collaborazioni accademiche (Università Nazionale di Milano, La Sapienza, Tor Vergata). In particolare è attualmente membro del Comitato Strategico del Centro di Ricerca e Sviluppo sull'E-Content dell'Università di Tor Vergata di Roma. Attiva partecipazione ai principali tavoli europei (collaborazione con la Commissione Europea per la NIS Platform e l'Organizzazione Europea per la Cyber Security - ECSO) e nazionali (DIS, CNR, CLUSIT, AIEA, AIIC). Ha sviluppato i suoi 20 anni di esperienza in contesti internazionali, in particolare Italia, Spagna, Francia ed Africa ed ha seguito con una particolare attenzione i contesti del Settore Pubblico e dell'Energy & Utilities.

**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. Già 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 del Comitato Tecnico Scientifico di CLUSIT, 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**, Adviser e consulente da più di vent'anni nel campo della sicurezza e della gestione del rischio IT, è membro del Comitato Direttivo e del Comitato Tecnico di 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.

**Girolamo Tesoriere** si è laureato in Ingegneria delle Telecomunicazioni presso il Politecnico di Bari. 10+ anni di esperienza nel settore delle TLC con una specializzazione nella consulenza sui servizi di Network Security e Cyber Security. Dopo aver lavorato per diversi anni come Technical Consultant in ambito networking e reporting operativo, nel 2013 partecipa allo start-up del Security Operations Center Enterprise di Fastweb. Ha lavorato per Eni come Cyber Security Engineer e al momento occupa la posizione di Enterprise Security Architect in Fastweb. Contribuisce allo sviluppo delle nuove soluzioni di sicurezza da erogare ai clienti TOP, grandi aziende e pubblica amministrazione.

**Enrico Tonello**, laureato in ingegneria a Padova, è socio co-fondatore di TG Soft S.a.s. Da sempre attento agli aspetti di sicurezza informatica ed in particolare agli attacchi da virus&malware, è autore di numerosi articoli su virus&malware informatici pubblicati su alcune delle principali riviste italiane del settore e relatore in conferenze e seminari sui virus&malware informatici realmente circolanti come Security Evangelist. È co-autore della suite AntiVirus-AntiSpyware-AntiMalware Vir.IT eXplorer PRO per Windows® Microsoft.

**Gianfranco Tonello**, laureato in ingegneria informatica a Padova, è Malware Analyst e CEO di TG Soft. È riconosciuto a livello internazionale quale analista di virus&malware di nuova generazione e sviluppatore di tecnologie AntiMalware. Dal 1990 è analista di Virus/Malware con pubblicazione di analisi tecniche presso il VTC (Virus Test Center) dell'Università di Amburgo e su numerose riviste italiane. È Autore/Sviluppatore di software, specializzato nella produzione di tecnologie AntiVirus-AntiSpyware-AntiMalware. È docente CLUSIT. È analista/reporter della WildList, che individua i virus/malware on the wild cioè realmente circolanti a livello mondiale. È membro di AMTSO (Anti-Malware Testing Standards Organization), di VIA (Virus Information Alliance di Microsoft) e di MVI (Microsoft Virus Initiative).

**Giuseppe Vaciago** è Avvocato, iscritto all'Ordine degli Avvocati di Milano dal 2002. Le aree di specializzazione sono il diritto penale delle nuove tecnologie e il diritto penale societario. 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 partecipato a numerosi convegni presso le più prestigiose Università italiane ed estere. È fellow presso il Nexa Center di Torino e presso il Cybercrime Institute di Colonia. È membro del comitato editoriale della Rivista Digital Investigation edita da Elsevier. È autore di numerose pubblicazioni di carattere universitario tra cui "Computer Crimes", "Digital Forensics" e "Modelli di organizzazione gestione e controllo ai sensi del D.lgs. 231/01". È membro dell'Organismo di Vigilanza di Procter & Gamble Italy S.p.A., Whirlpool S.p.A, Duracell, Labocos S.r.l., Team System S.r.l., Gruppo Ospedaliero San Donato.

**Andrea Vallavanti** è ICT Manager del Rigassificatore di Livorno OLT, una delle realtà industriali Italiane OFFSHORE (FSRU – floating storage regassification Unit) dedicate alla trasformazione del gas naturale (LNG) In questo ruolo ha acquisito significative esperienze in ambito ICT Maritime. Prima del mondo Oil&Gas ha ricoperto posizioni di senior Project Manager IT nel mondo Energy in EON Italia dove si è occupato della reingegnerizzazione delle rete SCADA ed IT manager in Endesa Italia nella gestione di progetti TLC volti alla completa autonomia societaria. Ha inoltre ricoperto ruoli di responsabilità in Elettrogen nel distacco tecnologico dai sistemi di telecomunicazioni su power over line ed in ENEL, come specialista di Elettroregolazioni. Viene aggiunto alla sua esperienza lavorativa, un periodo di insegnamento nella Scuola Pubblica Superiore ed una collaborazione con l'Università Cattolica del S. Cuore di Piacenza.

**Alessandro Vallega** lavora in Oracle con il ruolo di Business Development Director e si occupa a livello EMEA (Europe, Middle East and Africa) di Security e di GDPR (regolamento EU 679/2016 sulla protezione dei dati personali) . È il responsabile della Oracle GDPR War Room (EMEA - Tech). 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). Nel 2015 ha fondato insieme a Clusit e ad Aused un osservatorio permanente sul GDPR 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 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. È stato membro dell'Osservatorio per la Sicurezza Nazionale (OSN) nel 2011-12 e del Consiglio Direttivo di Assintel dal 2012 al 2016, coordinandone il GdL Cyber Security. Dal 2012 è membro del Consiglio Direttivo di Clusit, e Board Advisor del Center for Strategic Cyberspace + Security Science (CSCSS) di Londra. Per oltre 10 anni è stato Presidente de iDialoghi, società milanese dedicata alla formazione ed alla consulenza in ambito ICT Security. Nel gennaio 2015 ha assunto il ruolo di Head of Cyber Security Services della divisione Information Risk Management di KPMG Advisory. Dal giugno 2017 è Managing Director di un centro di ricerca internazionale in materia di Cyber Defense. 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 (2011) del "Rapporto Clusit sulla Sicurezza ICT in Italia", si è occupato della sezione relativa all'analisi dei principali attacchi a livello internazionale, ed alle tendenze per il futuro.

Il Clusit, nato nel 2000 presso il Dipartimento di Informatica dell'Università degli Studi di Milano, è la più numerosa e 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 13ª edizione.
- Le Conference specialistiche: Security Summit (Milano, Treviso, 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 (Interna-

tional 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.
Certificata dalla folta schiera di relatori (più di 500 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 15.000 partecipanti, e sono stati rilasciati circa 10.000 attestati validi per l'attribuzione di oltre 16.000 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.

**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.

## L'edizione 2018

La decima edizione del Security Summit si tiene a Milano dal 13 al 15 marzo, a Treviso il 16 maggio, a Roma il 6 e 7 giugno e a Verona il 4 ottobre.

## 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

panda

TREND MICRO

### Research Partner

IDC

Il presente Rapporto è stato prodotto in occasione del

EUROPEAN CYBER SECURITY MONTH

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT 10 ANNI

**www.securitysummit.it**