

## SPECIALE FINANCE SECURITY

finance security



Nell'anno 2016 sia l'ambito globale sia quello italiano sono stati caratterizzati da un forte incremento delle attività legate al cyber-crime in ambito finanziario e il 2017 presenta trend peggiorativi. Il Rapporto Clusit 2017 delinea caratteristiche trend ed evoluzione delle minacce che interessano gli utenti, le aziende e le organizzazioni correlati ai dati di natura finanziaria.

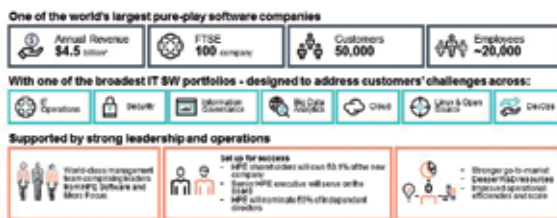
pag. 2

## LA SICUREZZA HPE ANCORA PIÙ FORTE

In procinto di integrarsi con Microfocus, Hewlett Packard Enterprise sviluppa e accresce l'offerta software. La futura azienda sarà tra le prime sei software company al mondo, con oltre 50mila clienti e 4,5 miliardi di dollari di fatturato annuo, di cui il 60% costituito da sottoscrizioni ricorrenti. Avrà come Ceo Christopher Hsu, attualmente Executive Vice President, General Manager HPE Software e Chief Operating Officer di Hewlett Packard Enterprise, e come Chief Financial Officer l'attuale CFO di Microfocus, Mike Phillips.

pag. 14

### Micro Focus + HPE Software



... and we're just beginning... the new company will have a strong platform for M&A.

\*Using 2016 revenue as of April 30, 2017 for HPE & Software segment and the Micro Focus revenue based on data for the full year

## IN QUESTO NUMERO:

### SPECIALE

pag. 02-06

- Gli attacchi al mercato finanziario in Italia

pag. 07

- Le regole per proteggersi dalle minacce

pag. 08-09

- I principali malware per le frodi bancarie

pag. 10-11

- Il mercato illegale della compravendita di carte di credito

### SOLUZIONI

pag. 12-13

- La security intelligence di FireEye a portata del mid-market

pag. 14-15

- La sicurezza HPE ancora più forte

## GLI ATTACCHI AL MERCATO FINANZIARIO IN ITALIA

*L'analisi a cura di Gianluigi Sisto di Reply Communication Valley riportata all'interno del Rapporto Clusit 2017, delinea lo scenario per l'anno passato del cyber crime indirizzato alle istituzioni finanziarie del nostro Paese*

finance sec

**N**ell'anno 2016 sia l'ambito globale sia quello Italiano sono stati caratterizzati da un forte incremento delle attività legate al cyber-crime in ambito finanziario.

Reply Communication Valley, tramite il suo Cyber Security Command Center (CSCC), da anni effettua

The background image shows a hand holding a credit card over a laptop keyboard. A large red shield with a white padlock icon is overlaid on the right side of the image. The word 'Security' is written in large blue letters on the left side, partially overlapping the keyboard and the shield.

# Security

attività di monitoraggio a supporto di alcune delle principali realtà bancarie Italiane.

Questo punto di vista privilegiato ha consentito di analizzare le caratteristiche e l'evoluzione dei principali attacchi in Italia indirizzati all'ambito bancario nel 2016, in uno studio curato da Gianluigi Sisto e

riportato all'interno del Rapporto Clusit 2017.

L'analisi di Reply ha organizzato gli attacchi osservati in tre macro categorie:

- Attacchi di ingegneria sociale (phishing).
- Attacchi tramite malware infostealer.
- Attacchi tramite malware ransomware.

### Massima efficacia sfruttando i brand più noti

Nel nostro Paese la tendenza vede ancora i malware classici ingegnerizzati per pc come responsabili per la grandissima maggioranza degli attacchi, ma gli attacchi su dispositivi mobile, in particolar modo in ambiente Android, hanno un trend in continua crescita che li ha portati al 5% degli attacchi globali osservati. Il principale vettore di attacco utilizzato per la diffusione degli attacchi sopracitati è stato, in larghissima maggioranza, lo spam veicolato attraverso posta elettronica.

Le campagne di spam sono a tutti gli effetti attacchi di ingegneria sociale, che diventano sempre più complessi e difficili da contrastare con i normali mezzi a disposizione degli utenti.

Tra le varie campagne di spam osservate in Italia sono da ricordare nel mese di febbraio quella relativa una falsa fattura ENEL da pagare con breve scadenza che portava a scaricare da un sito esterno il file Bolletta ENEL.zip, che conteneva un malware che scaricava il ransomware Cryptolocker. Altra campagna massiva di spam, sempre con l'obiettivo di diffondere malware di tipo ransomware, si è avuta tra i mesi di giugno e luglio avvalendosi del brand Vodafone per spingere gli utenti ad aprire un link contenente un exploit per Microsoft Explorer che abilitava il download e l'esecuzione di Cryptolocker. I altri casi analoghi, i cyber criminali hanno sfruttato altri marchi con messaggi quali: cartella esattoriale Equitalia, pacco DHL in consegna, fattura Telecom.

Degna di particolare attenzione è stata l'imponente

campagna di spam avvenuta su caselle certificate PEC del provider Aruba.

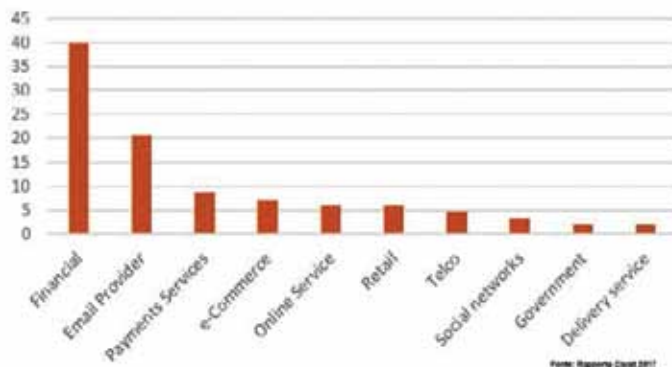
### Attacchi di ingegneria sociale (phishing)

Nell'ultimo anno in Italia il CSCC ha identificato attacchi di ingegneria sociale particolarmente complessi effettuati verso alcuni istituti bancari. Questi attacchi, che ricadono nella categoria del phishing, sono particolarmente efficaci in quanto l'attacco non viene effettuato sul perimetro tecnologico della banca ma sul singolo utente.

Tra le tecniche di attacco utilizzate si segnala lo spear phishing, una forma mirata di truffa via email che prende di mira un gruppo specifico o un'organizzazione a seguito di una lunga fase di studio del target attaccato, basata sullo studio delle comunicazioni aziendali. Gli attacchi di spear phishing hanno uno schema consolidato che prevede sempre l'utilizzo di tre fattori chiave: l'email appare inviata da una persona conosciuta e di fiducia; il layout e il contenuto sono molto accurati; le istruzioni richieste sono logiche e credibili per il destinatario.

Un'altra tecnica, molto utilizzata in Italia e che si è evoluta per attaccare i sistemi bancari dotati di "strong authentication" è l'instant phishing. Il concetto di questo modello di attacco si basa sul fatto che, nell'istante in cui l'utente inserisce le credenziali o più in generale le informazioni all'interno del sito clone, il cyber criminale apre una sessione verso il vero sito della banca e utilizza, quasi contemporaneamente, queste informazioni per effettuare azioni dispositive.

### Settori più colpiti dal phishing (dato percentuale)



A partire dal 2016 ha cominciato a diffondersi in Italia anche la tecnica detta del CEO Fraud che prevede attacchi di phishing mirati verso figure aziendali di altissimo profilo, tramite una email il cui testo è solitamente una richiesta di un bonifico urgente verso un determinato IBAN per un determinato motivo. L'email viene scritta come se fosse stata inviata dal CEO, dal CFO o altra figura aziendale con analoghi poteri decisionali, solitamente è molto curata in modo da non contenere elementi sospetti e contiene una motivazione apparentemente valida dell'urgenza del bonifico. È evidente che questo tipo di attacco richiede una lunghissima fase di preparazione e, per avere successo deve contare su una persona con la facoltà di gestire la richiesta, ma che sia poco esperta sui temi della sicurezza, evitando

di porsi il problema di comunicazioni fraudolente simili a quella appena ricevuta.

### Attacchi tramite infostealer

L'analisi effettuata dal CSCC ha evidenziato un numero complessivo di attacchi tramite infostealer nel 2016 in linea con il dato dell'anno precedente, mentre si osserva una diminuzione del numero complessivo di attacchi effettuati tramite malware infostealer Zeus.

I principali malware infostealer operanti in Italia sono Dridex e Dyre: due malware di ultima



generazione molto più complessi rispetto alle prime versioni del capostipite Zeus.

In Italia sono state anche individuate diverse campagne di spam con l'obiettivo di diffondere il malware infostealer Gozi che predilige come target i servizi di corporate banking e sono stati identificati diversi malware "informativi" con l'obiettivo di registrare, tramite video ad-hoc, l'intera navigazione effettuata dall'utente.

Nella classifica degli attacchi in base ai target bancari è emerso che il 70% degli attacchi è diretto verso i sistemi di Retail Banking, il 25% verso i siti di gestori carte di credito, il 3% verso i sistemi di Corporate Banking e il 2% nei confronti dei principali fornitori di servizi di social media (Facebook e LinkedIn in particolare) e di servizi freemail (Gmail e Hotmail).

L'analisi dei server Command & Control relativi alle botnet responsabili degli attacchi sulle banche Italiane ha confermato gli Stati Uniti come primo Paese al mondo per hosting di questo tipo di server. Un altro dato interessante relativamente agli infostealer analizzati è che, scelto un campione di 10 dei principali antivirus commerciali, un nuovo sample di malware infostealer viene rilevato mediamente dopo 12 giorni dall'inizio della diffusione e solo due giorni dopo il picco massimo di infezioni.

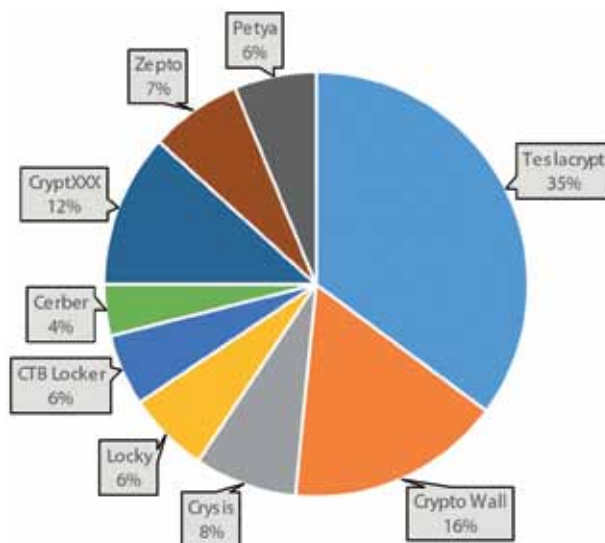
L'arco di tempo nei quali i computer sono mediamente non protetti da malware di ultimissima generazione è quindi di quasi due settimane: un periodo di tempo che risulta più che sufficiente per portare a termine una campagna di attacco da parte dei cyber criminali.

## Attacchi tramite ransomware

L'Italia è una triste protagonista dello scenario relativo gli attacchi tramite ransomware, con quasi il 7% degli attacchi globali di questo tipo effettuati, indirizzati verso il nostro Paese.

Analizzando i vari ransomware che hanno attaccato il bacino di utenti Italiani si evidenzia come TeslaCrypt sia stata la minaccia principale, responsabile del 35% degli attacchi; seguono a ruota in seconda e terza posizione i ransomware Crypto Wall (16%) e CryptXXX (12%).

Nel complesso, analizzando l'insieme degli attacchi osservati è emerso che le campagne di spam per la diffusione di ransomware riescono ad aggirare i sistemi antispam con un'efficacia di circa il 20% e che il numero di utenti che effettivamente cade vittima del ransomware è di circa il 3% del totale; in ambito bancario la percentuale scende però a meno dell'1%.



*I ransomware in Italia nel 2016  
(Fonte: Rapporto Clusit 2017)*

## LE REGOLE PER PROTEGGERSI DALLE MINACCE



### *Pochi controlli di base per minimizzare il rischio*

Con poche regole pratiche è possibile limitare la probabilità di successo di un eventuale malware che dovesse approdare sui nostri sistemi, riducendo se non eliminando l'impatto di potenziali azioni fraudolente. Questa è l'indicazione che proviene da IBM e riportata all'interno del Rapporto Clusit 2017.

L'insieme delle pratiche minime suggerito è di prestare la massima attenzione almeno sui seguenti comportamenti:

- 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);
- 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;
- configurare le applicazioni di office automation per aprire sempre in modalità protetta i documenti provenienti da Internet, memorizzati in percorsi potenzialmente non sicuri, o allegati a e-mail;
- avere un antivirus attivo e funzionante su ciascun dispositivo connesso ad Internet;
- 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;
- 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;

- attendere sempre che l'antivirus completi la scansione di allegati a email prima di aprirli.

Le realtà enterprise dovrebbero inoltre adottare strategie più articolate per evitare o limitare attacchi aziendali, come:

- sensibilizzare i collaboratori sull'esistenza di attacchi mirati;
- utilizzare servizi di IP address reputation;
- introdurre soluzioni per il calcolo in tempo reale del fattore di rischio di ciascuna transazione;
- bloccare il traffico verso le reti di anonimizzazione;
- adottare soluzioni per la protezione dell'endpoint, con verifica dell'integrità del browser e del sistema;

Le istituzioni finanziarie dovrebbero applicare livelli di protezione ancora più avanzati come, per 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 (per esempio SMS), utilizzo della geo localizzazione del dispositivo mobile come ulteriore fattore di autenticazione;
- fornire ai propri clienti meccanismi di notifica in tempo reale di transazioni elettroniche.

# I PRINCIPALI MALWARE PER LE FRODI BANCARIE

*Crescono in numero e sofisticazione. La scomparsa di Dyre ha lasciato spazio a Neverquest e Dridex/Bugat*

I malware specializzati per frodi bancarie e finanziarie sono certamente tra quelli più critici per pericolosità e sofisticazione. Si tratta per la maggior parte di malware che mirano a impossessarsi delle credenziali di autenticazione usate per accedere ai servizi di Web banking o, in generale ai sistemi di pagamento, per poi riutilizzarle in maniera automatica per effettuare transazioni illegittime a danno della vittima. Le frodi finanziarie hanno un risultato sempre misurabile con attendibilità: il danno è pari alle somme trasferite verso l'esterno con transazioni elettroniche fraudolente e difficilmente recuperabili.

Il 2016 ha visto l'uscita di scena del famigerato malware Dyre a seguito dell'operazione del Novembre 2015, apparentemente a opera delle autorità russe, a cui era attribuibile il 16% di tutte le infezioni individuate nel 2015.

Nel corso del 2014 e 2015 a Dyre erano state imputate frodi per decine di milioni di dollari a carico di utenti di numerose banche del Regno Unito, Stati Uniti, Australia, Spagna e in forma minore anche altre nazioni Europee, oltre a campagne di attacco mirate verso grosse organizzazioni tra cui colossale frode di 4,6 milioni di euro ai danni della compagnia

aerea Irlandese Ryanair del Maggio 2015.

Dati di IBM X-Force e IBM Security Trusteer mostrano che, per l'anno 2016, il fenomeno del malware bancario e malware specializzato in frodi finanziarie, limitatamente al panorama europeo, si è polarizzato attorno a quattro principali famiglie di malware: Neverquest, Dridex/Bugat, Gozi e Gootkit.

Numerosi altri malware sono stati usati nel corso dell'anno (per esempio Goznym, Kronos, tinba, zeus/Zeus\_Citadel, corebot, urlzone, kronos, ramnit) ma, cumulativamente, la loro presenza è stata esigua e limitata a campagne di attacco mirate verso organizzazioni e soggetti specifici.

Da un punto di vista generale continua lo spostamento dall'utente individuale verso utenti aziendali e corporate, con il chiaro obiettivo di massimizzare gli importi frodati per ciascuna azione criminale.

## **Neverquest**

Neverquest (conosciuto anche come Vawtrak) ha continuato a dominare la scena, almeno nel primo semestre. Si tratta di un banking trojan individuato per la prima volta nel 2013 e che appare come un'evoluzione della precedente famiglia di malware Gozi/ISFB Trojan, di cui condivide parti di codice e



### Dridex

Dridex (evoluzione del malware Bugat) è stato nel 2016 il malware osservato nel maggior numero di varianti, con una conseguente difficoltà di individuazione da parte dei prodotti antimalware. 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 che inducono la vittima ad aprire documenti Office allegati all'email, oppure raggiunti tramite un link. Questi documenti contengono macro o script oppure, 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 localmente il malware. Il furto delle credenziali avviene attraverso web injects, ovvero contenuti da far comparire nel browser, e keylogger che al momento opportuno tracciano quanto digitato sulla tastiera e lo inviano verso l'esterno.

l'infrastruttura dei server di Command-and-Control (C&C).

Dopo la scomparsa di Dyre, Neverquest si è affermato come il malware per frodi finanziarie più usato in Europa, e così è rimasto durante tutto il 2016. Neverquest è in vendita nei forum dell'undeground sin dalla sua creazione. L'aggiornamento del codice sorgente, l'infrastruttura di botnet che lo veicola e le diverse campagne che si sono susseguite nel corso dell'anno sono a cura di diverse bande di cyber criminali.

Neverquest è un toolkit completo che mette a disposizione strumenti per costruire frodi basate sul furto di credenziali. Tra le funzionalità di base ci sono strumenti di form grabbing con cattura di schermate statiche e di video, file transfer, inserimento di contenuti durante la visualizzazione di una pagina (web injection), controllo remoto della macchina via VNC, furto ed esfiltrazione di certificati.

Neverquest compromette i browser e si interpone tra l'utente e il sito web della banca durante le operazioni di web banking. Basandosi su file di configurazione scaricati dalla rete di Command & Control e costantemente aggiornati, Neverquest è in grado di mostrare contenuti addizionali sullo schermo (web injects) e catturare quanto digitato sulla tastiera per poi inviarlo all'esterno in forma cifrata. Finora le configurazioni di Neverquest hanno avuto come obiettivo principale siti di web banking e altre istituzioni finanziarie di lingua inglese.

# IL MERCATO ILLEGALE DELLA COMPRAVENDITA DI CARTE DI CREDITO

*Aumenta la diffusione degli attacchi indirizzati a sottrarre i dati personali di carattere finanziario, segno del successo del loro commercio su molteplici black-market*

La necessità di scambio di articoli illegali ha determinato negli anni l'affermazione di siti dedicati alla loro compravendita, i black-market, in cui chiunque può comprarli o venderli in maniera anonima. Si tratta di un fenomeno in crescita a cui il Team di Cyber Threat Intelligence di Lutech (Francesco Faenzi, Roberto Romano e Luca Sangalli) ha recentemente dedicato uno studio pubblicato all'interno del Rapporto Clusit 2017 focalizzato sulla compravendita illegale di dati di carte di credito (fenomeno detto del carding). Lo studio ha identificato oltre 900 indirizzi relativi alla compravendita illegale di tali dati, presenti sia nel Deep Web che nel Dark Web all'interno di 85 black-market attivi.

## Le caratteristiche dei black-market

Per via della tipologia di articoli trattati, la maggior parte dei black-market garantisce l'anonimato sia per i venditori sia per gli utenti. Le transazioni avvengono in forma anonima tramite cripto monete e implementano un meccanismo di fiducia per i venditori in modo che i più affidabili abbiano più visibilità e si costruiscano una "reputazione".

Spesso tali siti sono ospitati all'interno del Dark Web, principalmente nelle reti Tor e I2P, ma altrettanto spesso sono raggiungibili attraverso la normale rete Internet all'interno del Deep Web, in quanto il contenuto di tali "store" non è indicizzato dai classici motori di ricerca ed è quindi necessario sia

*Sito Web di Central-Shop, uno dei principali black-market per la compravendita di dati legati alle carte di credito*

ID	Name	Price	Status	Date	Type	Card	CVV	Exp.	Issuer	Bank	Card No.	CVV	Exp.	Issuer	Bank
1	MasterCard	12.000	OK	2017	WELLS FARGO			12/17	USA				12/17	USA	
2	MasterCard	12.000	OK	2017	WELLS FARGO			12/17	USA				12/17	USA	
3	MasterCard	12.000	OK	2017	CHASE			12/17	USA				12/17	USA	
4	MasterCard	12.000	OK	2017	CHASE			12/17	USA				12/17	USA	
5	MasterCard	12.000	OK	2017	CHASE			12/17	USA				12/17	USA	
6	MasterCard	12.000	OK	2017	CHASE			12/17	USA				12/17	USA	
7	MasterCard	12.000	OK	2017	CHASE			12/17	USA				12/17	USA	
8	MasterCard	12.000	OK	2017	CHASE			12/17	USA				12/17	USA	
9	MasterCard	12.000	OK	2017	CHASE			12/17	USA				12/17	USA	
10	MasterCard	12.000	OK	2017	CHASE			12/17	USA				12/17	USA	
11	MasterCard	12.000	OK	2017	CHASE			12/17	USA				12/17	USA	
12	MasterCard	12.000	OK	2017	CHASE			12/17	USA				12/17	USA	
13	MasterCard	12.000	OK	2017	CHASE			12/17	USA				12/17	USA	
14	MasterCard	12.000	OK	2017	CHASE			12/17	USA				12/17	USA	
15	MasterCard	12.000	OK	2017	CHASE			12/17	USA				12/17	USA	
16	MasterCard	12.000	OK	2017	CHASE			12/17	USA				12/17	USA	
17	MasterCard	12.000	OK	2017	CHASE			12/17	USA				12/17	USA	
18	MasterCard	12.000	OK	2017	CHASE			12/17	USA				12/17	USA	
19	MasterCard	12.000	OK	2017	CHASE			12/17	USA				12/17	USA	
20	MasterCard	12.000	OK	2017	CHASE			12/17	USA				12/17	USA	

conoscere l'indirizzo esatto del market che si vuole raggiungere sia avere un accesso privato a esso. Molti black-market specializzati in carding mettono a disposizione dei propri utenti dei servizi di "checker" che eseguono una micro transazione tipicamente verso organizzazioni no-profit, per testare la validità delle carte acquistate sul market. Inserendo i dati delle carte (numero, scadenza, cvv), il checker restituisce il risultato del test effettuato sulla carta, generalmente nella forma "valida" o "non valida". Un black-market tipico può supportare molteplici funzionalità, quali: accesso protetto da password, filtri avanzati di ricerca (Paese, banca, tipo carta, livello, indirizzo, cap e così via), comunicazioni multilingua, per arrivare a fornire anche servizi di customer care (tramite ticketing).

*Il supporto tramite FAQ disponibile sul sito*



## Meno di venti dollari per comprare la vostra carta di credito

I dati delle carte di pagamento sono venduti sui black-market a prezzi variabili in base a diversi fattori che possono essere specifici della carta in vendita come il circuito (per esempio, Visa, MasterCard, JCB, American Express) o la classe di livello (per esempio, Visa Electron, Visa Classic, Visa Gold) oppure relativi alle informazioni disponibili e messe in vendita, come: i dati della carta (numero, scadenza e CVV), il nome dell'intestatario, il suo indirizzo e numero di telefono, il PIN e altri dati aggiuntivi. La completezza dei dati e il plafond disponibile sulla carta (dipendente da circuito e livello) sono i fattori principali che determinano le variazioni dei prezzi delle carte di pagamento vendute. Nella maggior parte dei black-market, una carta viene venduta a un prezzo variabile fra gli 8 e i 15 dollari.

La maggior parte dei black-market presenti in rete ha a disposizione dati prevalentemente statunitensi, poiché negli USA le carte di pagamento non integrano i chip elettronici ma sono dotati solo di banda magnetica. Tuttavia sono presenti numeri significativi anche per quanto riguarda le carte emesse da istituti di paesi europei, fra cui l'Italia.

## LA SECURITY INTELLIGENCE DI FIREEYE A PORTATA DEL MID-MARKET

*L'azienda specializzata in cyber security rilascia il report M-Trends 2017 che delinea gli scenari a livello globale delle minacce. Nel contempo amplia la propria proposizione commerciale indirizzandosi verso le aziende di dimensione media lanciando la piattaforma integrata Helix*

*di Riccardo Florio*

**A**cinque anni di distanza dal suo arrivo in Italia, FireEye si conferma un'azienda in crescita e tra le realtà più interessanti all'interno del competitivo mercato della sicurezza ICT.

Focalizzata sul tema della cyber security con un'attenzione agli aspetti di security intelligence e un approccio orientato ai servizi, FireEye si avvale delle tecnologie di intelligence iSight e delle competenze e servizi nell'ambito dell'Incidente response ottenuti con l'acquisizione tre anni fa di Mandiant (azienda presente in quasi tutte le aziende top 500 americane e meno nota in Europa).

La focalizzazione sugli aspetti di resilienza della sicurezza resta la direttrice strategica dell'azienda, che sta ampliando il proprio target, finora concentrato sul "government" e sulle realtà di livello enterprise che dispongono di un Security Operation Center (SOC), anche verso il mid-market. Questo passaggio è legato al recente lancio di Helix, una piattaforma integrata e modulare di sicurezza per la

rilevazione, l'analisi e la risposta alle minacce che, di fatto, mette a disposizione un "SOC in a box" erogato in forma di servizio, appannaggio anche delle realtà più piccole, che non dispongono delle risorse e del know how per realizzare un SOC in casa.

Una svolta che, Marco Riboli, vice president Southern Europe di FireEye, ritiene che contribuirà ad ampliare notevolmente la penetrazione dell'azienda sul mercato italiano.

«Attualmente FireEye vanta in Italia un centinaio di clienti - precisa Riboli - che ricadono tra le società di primaria importanza, che devono confrontarsi con

minacce crescenti in numero e sofisticazione. Trentasei dei nostri clienti li abbiamo acquisiti lo scorso anno, segno che la sensibilità verso il tema della sicurezza sta cambiando. Il mid-market richiede fortemente queste soluzioni e sono convinto che troveremo ampio riscontro. FireEye rappresenta l'eccellenza per quanto riguarda l'Incident response grazie soprattutto alle tecnologie e competenze di Mandiant,



*Marco Riboli, Vice  
Presidente per il Sud  
Europa di FireEye*

*Il Report M-Trends 2017*

che è l'azienda che ha dato una svolta metodologica innovativa alla gestione degli incidenti».

FireEye eroga alcuni servizi specifici direttamente ma, prevalentemente, opera attraverso una serie di partner "managed" con cui l'azienda di sicurezza lavora costantemente: Security Reply, Puntotit, R1, Sorint, Innovery, Leonardo, CY4GATE, 7Layers, Lutech, Business E, Var Group. In Italia le soluzioni FireEye sono distribuite da Arrows ed Esclusive Networks che gestiscono un centinaio di partner attivi.

### **Il report M-Trends 2017 e la situazione italiana**

Da diversi anni Mandiant pubblica M-Trends, un report che analizza a livello globale e per aree geografiche lo scenario degli incidenti, per fornire indicazioni su tendenze ed evoluzione dell'attività criminale.

L'Italia in EMEA si colloca al quinto posto come target per gli attacchi e solo il 6% delle aziende interpellate da Mandiant ritiene di non essere a rischio; nonostante ciò un terzo delle aziende soprattutto del settore small e medium investe poco o nulla in sicurezza.

La nuova edizione del report evidenzia che l'attività di cyber crime in Italia è incrementata del 33% rispetto all'anno precedente. Questo anche grazie alla grande facilità con cui le infiltrazioni riescono a

essere efficaci: segno di una carenza culturale in ambiti quali il contrasto al phishing. Gli attacchi hanno generato quasi 9 miliardi di perdite e il target tende ad ampliarsi al di fuori dei settori più tradizionali come quello finanziario.

Tra i "numeri" di rilievo vi è il tempo di permanenza medio di un attaccante all'interno di un ambiente compromesso, che è di 106 giorni nelle organizzazioni EMEA e di 99 giorni su scala globale. Un dato in rapida diminuzione, soprattutto in Europa, anche se si mantiene ancora troppo elevato: a livello globale era di 243 giorni nel 2012 e di 146 nel 2015 mentre in EMEA nel 2015 era di 469 giorni.

Un altro dato interessante è che gli attaccanti con motivazioni finanziarie hanno raggiunto nuovi elevati livelli di sofisticazione spostandosi verso l'uso di backdoor personalizzate con una configurazione unica per ogni sistema compromesso, incrementando il livello di resilienza della loro infrastruttura e migliorando le tecniche anti-forensi utilizzate.

Mandiant segnala anche che nel 2016 gruppi di cyber criminali russi hanno avuto un'ingerenza nelle elezioni presidenziali statunitensi e che ci sono segnali che questi gruppi rivolgeranno le loro prossime attenzioni anche alle elezioni europee.

Tra le indicazioni fornite dal report vi è anche l'invito rivolto alle organizzazioni che risiedono in EMEA a dedicare particolare attenzione ai rischi per il settore energetico e i sistemi di controllo industriali, verso i quali sembra si sta concentrando l'attenzione del cyber crime.

Il report completo M-Trends 2017 è disponibile a questo link: [https://www2.fireeye.com/RPT\\_IT\\_M-Trends\\_2017.html](https://www2.fireeye.com/RPT_IT_M-Trends_2017.html)

## LA SICUREZZA HPE ANCORA PIÙ FORTE

*In procinto di integrarsi con Micro Focus,  
Hewlett Packard Enterprise sviluppa e accresce  
l'offerta software*

di Gaetano Di Blasio

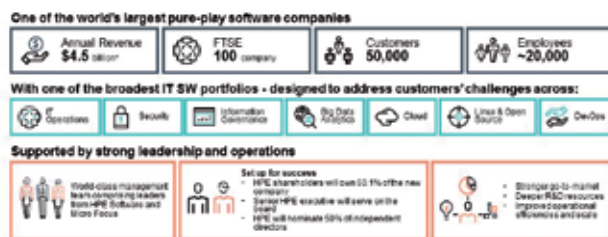
Le risorse  
combinata  
di HPE e  
Micro Focus

Dimitri Crea, channel manager di HPE, intervenuto al Partner Summit di Coretech, ha illustrato l'offerta software che Hewlett Packard Enterprise "porta in dote" nella nuova società che prenderà corpo dopo la fusione tra HPE e Micro Focus: «Noi forniamo un portfolio di livello enterprise completo di soluzioni "best in class" con capacità di analytics integrate. L'operazione prevede lo spin off della divisione software di HPE e la successiva fusione, per un valore complessivo di 8,8 miliardi di dollari, di cui 6,3 miliardi saranno distribuiti come quote della nuova azienda (per un totale di 50,1%, con un valore previsto di 6,3 miliardi di dollari), mentre altri 2,5 miliardi saranno riconosciuti in cash.

La futura azienda avrà come Ceo Christopher Hsu, attualmente Executive Vice President, General Manager HPE Software e Chief Operating Officer di Hewlett Packard Enterprise, e come Chief Financial Officer l'attuale CFO di Micro Focus, Mike Phillips.

Secondo Crea, la futura società sarà tra le prime sei software company al mondo, con oltre 50mila clienti e 4,5 miliardi di dollari di fatturato annuo, di cui il 60% costituito da sottoscrizioni ricorrenti.

Aldilà delle cifre, sono da considerare i software che HPE andrà ad aggiungere al portafoglio di Micro Focus, in ambiti quali i Big data (con Idol, Vertica e HPE



Haven on Demand), le soluzioni di cloud orchestration e data center operation, l'application delivery e management (con ALM e AppPulse), le soluzioni per l'enterprise security (con Fortify, ArchSight, Atalla e Voltage Security, e, per ultime ma non ultime quelle dell'Information management e governance (con VM Explorer, Data Protector e Storage Optimizer).

Proprio queste ultime sono tra quelle che Crea ha evidenziato, ricordando che una delle più importanti soluzioni per fronteggiare i ransomware è un solido sistema di backup e recovery.

HPE VM Explorer, ha spiegato il manager italiano, è la migliore soluzione per il backup di ambienti VmWare e Hyper V, proteggendo e replicando ambienti virtuali per le piccole e medie imprese.

Tra le funzionalità principali: backup completi o incrementali, storage snapshot, disaster recovery basato su replica degli ambienti e test automatici dei backup e recovery delle virtual machine, replica server to server veloce. Cinque i livelli di restore, mentre i backup sono indirizzabili verso supporti quali: NAS, dischi, nastri o cloud.

Altre caratteristiche comprendono un task Scheduler, gestione tramite Command Line Interface, rapporti inviati via mail. Per gli ambienti più esigenti di taglio enterprise, VM Explorer aggiunge: Instant virtual machine recovery (IVMR) per ESX/ESX; cinque livelli di restore dal cloud e test automatici dei backup su cloud; interfaccia Web multiutente; supporto per vMotion su IVMR; supporto VMware vSAN; encryption (256 bit AES) support per snapshot storage EMC ScaleIO.

Massima flessibilità nella destinazione dei backup è garantita sia on premise sia in cloud, dove le imprese possono scegliere tra Amazon S3, OpenStack, Helion & Rackspace, Azure e possono costruire la propria infrastruttura di backup Object Storage, basata su OpenStack.

Tra i clienti, figurano Ricoh, Greenpeace, Hitachi, Swiss Aviation Software, Nokia, Asus, Avaloq, WWF, Swisscom, SAP, Veolia, Siemens, Sungard, Mizou, T System, ThyssenKrupp, Caritas, Infinigate.

### **Quattro famiglie di soluzioni per una protezione a 360 gradi**

La nuova società riceverà in dote il ricco portafoglio di soluzioni software che definiscono l'approccio di Predictive Security sviluppato da HPE.

Quattro attualmente le famiglie di prodotti, per abilitare una protezione a 360 gradi.

La gamma ArcSight raggruppa i componenti della soluzione di Security Information and Event Management (SIEM) di HPE che, da 13 anni di seguito, è inserita da Gartner tra i leader all'interno del suo Magic Quadrant per questo tipo di soluzioni. ArcSight rappresenta una piattaforma integrata per l'individuazione delle minacce e la gestione della compliance che abbina un motore avanzato per la raccolta, l'analisi e la correlazione delle informazioni e dei log di sicurezza, con una piattaforma (ArcSight Data Platform) che sfrutta le più avanzate tecnologie di Machine Learning e la capacità di correlazione in tempo reale di dati provenienti da qualsiasi fonte, per fornire visibilità immediata sulle attività che interessano l'intera infrastruttura enterprise.

Fortify è l'insieme di soluzioni per la sicurezza delle applicazioni che rappresentano, attualmente, il principale vettore di attacco. La gamma di soluzioni Fortify si avvale di tecnologie di autoprotezione RASP (Runtime Application Self Protection) e permette di realizzare un approccio allo sviluppo del codice applicativo di tipo "secure by design", eliminando alla fonte le possibili vulnerabilità e predisponendo ambienti di test di tipo statico, dinamico e in tempo reale adatti a verificare le caratteristiche di sicurezza del codice. Questo livello di protezione viene fornito anche come servizio on-demand per sottoporre a verifica il livello di sicurezza di ogni tipo di applicazione, incluse quelle commerciali.

Voltage è l'insieme di soluzioni per la crittografia dei dati e l'accesso sicuro basato su token adatte per ambienti enterprise, cloud, mobile e Big Data. Realizza un approccio che consente di applicare la sicurezza nel punto di creazione del dato e di seguirlo in ogni condizione: sia a riposo sia in movimento.

La gamma di soluzioni Atalla abilita un approccio alla protezione delle informazioni che sfrutta tecniche innovative di cifratura, proteggendo i dati on-premise e nel cloud e rendendo sicure le transazioni elettroniche.

# SICUREZZA COSTANTE, INTELLIGENTE

**E PUOI AVERLA SUBITO.**

Le tue aree di vulnerabilità aumentano. I contenuti si moltiplicano.

I cybercriminali sono sempre più scaltri.

Fortinet offre una singola infrastruttura di sicurezza intelligente che protegge la tua rete dalle minacce attuali e future.

**Visita [www.fortinet.it](http://www.fortinet.it) per maggiori informazioni.**

**FORTINET®**

**Sicurezza senza compromessi**