proofpoint

REPORT

REPORT TRIMESTRALE SULLE MINACCE

3° TRIM. 2017

proofpoint.com

Il *Report trimestrale sulle minacce Proofpoint* espone minacce, tendenze e i dati principali osservati all'interno della nostra ampia base di clienti e nel più ampio panorama delle minacce.

Al fine di proteggere le aziende di tutto il mondo dalle minacce avanzate, ogni giorno analizziamo oltre 1 miliardo di messaggi email, centinaia di milioni di post sui social media e oltre 150 milioni di campioni di malware. Continuiamo a osservare minacce sofisticate nei tre vettori primari: posta elettronica, social media e dispositivi mobili. Il nostro lavoro costituisce un punto di osservazione privilegiato, dal quale rivelare e analizzare tattiche, strumenti e bersagli degli attacchi informatici di oggi.

Questo report è concepito per fornire informazioni di pratico utilizzo per combattere meglio gli attacchi di oggi, prevedere le minacce emergenti e gestire la propria sicurezza. Insieme alle nostre analisi, il report suggerisce le misure da adottare per proteggere persone, dati e marchi.

SOMMARIO

DATI PRINCIPALI: RITORNO AL FUTURO

Negli ultimi anni il terzo trimestre è diventato un periodo intensissimo per i ricercatori delle minacce, con picchi nei volumi dei messaggi e un'anteprima degli strumenti e delle tecniche che gli autori degli attacchi useranno nei mesi a venire. Il terzo trimestre ha seguito un andamento simile anche quest'anno.

In più di due anni il volume di attacchi email che usano URL nocivi (anziché gli allegati) è esploso, andando a costituire la maggior parte di questo tipo di attacchi. Il ransomware e i trojan dei servizi bancari rimangono i payload preferiti.

Nel frattempo, il social engineering e le tecniche mirate si sono evolute ulteriormente in frodi tramite email e attacchi sui social media.

Secondo il nostro primo report pubblico sui domini fasulli ma verosimili, utilizzati per attacchi e frodi, i malintenzionati sembrano vincere la corsa alla registrazione dei domini. Per ogni registrazione "difensiva" effettuata da aziende proattive, abbiamo riscontrato 20 registrazioni simili sospette, effettuate da qualcun altro.

Di seguito i dati principali di questo trimestre.

EMAIL

Il volume di email nocive è cresciuto dell'85% dal trimestre precedente, alimentati da un'esplosione di attacchi provenienti da URL dannosi.
Il volume di email contenenti URL dannosi che collegano al malware è esploso di quasi il 600% rispetto al trimestre precedente e di oltre il 2.200% dallo stesso periodo dell'anno scorso. L'aumento ha amplificato una tendenza già osservata nella prima metà dell'anno, quando le email con URL hanno raggiunto la massima proporzione in termini di volume (rispetto a quelle con allegati) dal 2014 ad oggi. Comunque anche vaste campagne che utilizzano allegati dannosi hanno contribuito all'aumento degli attacchi via email: in questo caso si tratta di malware occultato nei file compressi allegati.

Il ransomware è ancora la prima categoria di malware.
Fra la nostra clientela il ransomware ha costituito quasi il 64% di tutto il malware via email. Nuovi ceppidi ransomware sono comparse ogni giorno, ma Locky è rimasto il payload principale, costituendo quasi il 55% del volume totale dei messaggi e oltre l'86% di tutto il volume del ransomware. Allo stesso tempo, grazie a poche campagne ad alto volume sferrate da un solo aggressore, alcune piccole varianti regionali come Philadelphia e GlobeImposter si sono trasformate in minacce globali.

TROJAN DEI SERVIZI BANCARI
Questo tipo di malware ruba le credenziali di accesso bancario delle vittime, solitamente reindirizzandone il browser verso una versione fasulla del sito web della banca oppure iniettando moduli di accesso falsi nel sito reale.

I TROJAN DEI SERVIZI BANCARI hanno rappresentato il 24% di tutto il volume di email nocive, con il ceppo The Trick responsabile del 70% di quel totale.
Spinto da campagne massicce di un solo autore, The Trick ha spodestato Dridex come principale trojan bancario (Dridex, dopo una stasi per gran parte del primo trimestre, è riemerso in vaste campagne nel secondo trimestre). Dridex – insieme ai Ursnif, Bancos e Zloader – ha continuato l'attività in campagne di livello regionale. È inoltre comparsa una nuova versione di Retefe. Per diffondersi sulle reti interne, ha utilizzato un exploit trapelato dall'Agenzia per la Sicurezza Nazionale degli Stati Uniti (NSA) e noto come **ETERNALBLUE**.

ETERNALBLUE
EternalBlue è un potente strumento di hacking che sfrutta una falla di un componente di condivisione file di Windows. È stato sottratto all'Agenzia per la Sicurezza Nazionale degli Stati Uniti ed è diventato di dominio pubblico all'inizio del 2017.

Le frodi via email sono cresciute del 29% rispetto al trimestre precedente.
Anche la frequenza degli attacchi è aumentata: i tentativi di frode via email per ciascuna azienda presa di mira sono cresciuti del 12% rispetto al trimestre precedente e del 32% rispetto allo stesso periodo dell'anno scorso. Anche se le frodi via email non distinguono le dimensioni delle delle aziende, quelle con le catene di fornitura più complesse sono i bersagli più frequenti.

KIT DI EXPLOIT E ATTACCHI BASATI SUL WEB

KIT DI EXPLOIT
I kit di exploit sono attivi sul web, rilevando e sfruttando le vulnerabilità dei computer che si connettono a essi. I dei kit di exploit, spesso venduti come servizio agli autori degli attacchi, facilitano l'infezione dei PC durante i download guidati del malware.

Il traffico proveniente dai KIT DI EXPLOIT si è mantenuto stabile, ma a un livello di solo il 10% del picco riscontrato nel 2016.
Il kit RIG è stato responsabile del 76% di tutta l'attività dei kit di exploit. Nelle campagne dei kit di exploit vengono ora inseriti schemi di social engineering e tale tendenza indica che gli autori stanno guardando oltre i soli exploit, che sono più difficili da trovare e ottenere.

REGISTRAZIONI DIFENSIVE
Pratica raccomandata che consiste nell'acquistare i domini Internet confondibili con il proprio, prima che lo facciano i pirati informatici. I domini simili possono essere usati per ingannare clienti e partner con siti web fasulli e email fraudolente, in apparenza provenienti dalla tua azienda.

ANGLER PHISHING
Nell'angler phishing gli aggressori creano falsi account di assistenza clienti sui social media per indurre coloro che stanno cercando aiuto a visitare un sito di phishing o a fornire le credenziali del proprio account.

DOMINI

Le registrazioni sospette di domini hanno superato quelle DIFENSIVE DI 20 a 1.
Alcune aziende stanno registrando attivamente i domini per combattere il typosquatting e lo spoofing dei domini, ma sono una minoranza. La registrazione difensiva dei domini posseduti da un marchio è scesa del 20% rispetto allo stesso periodo dell'anno scorso. Le registrazioni sospette dei domini sono a loro volta cresciute della stessa percentuale.

SOCIAL MEDIA

Gli account di assistenza fraudolenti, usati per il cosiddetto ANGLER PHISHING, sono raddoppiati rispetto al trimestre dell'anno precedente.
Il numero di account falsi di assistenza clienti è cresciuto del 5% rispetto al trimestre precedente, mentre il volume dei link di phishing sui canali social delle aziende è aumentato del 10%.

TENDENZE DELLE MINACCE BASATE SULL'EMAIL

Statistiche: le campagne malware basate sugli URL sono cresciute di quasi il 600% sul trimestre precedente e di oltre il 2.200% sullo stesso periodo dell'anno scorso.

TA505
Spinto da un movente economico, questo autore delle minacce è all'origine delle più grandi campagne di attacchi via email mai registrate, comprese quelle che diffondono i trojan bancari Dridex e The Trick, i ransomware Locky e Jaff e molti altri.

Il volume delle email fraudolente che inviano il malware tramite gli URL dannosi è cresciuto notevolmente. Uno dei principali responsabili è **TA505**, un aggressore molto prolifico, noto soprattutto per le massicce campagne di Locky, inviato prima tramite allegati e poi tramite gli URL. TA505 ha diffuso anche i ransomware Philadelphia e GlobeImposter, oltre al trojan bancario The Trick, con volumi sufficientemente alti da essere riconoscibile.

Questo picco ha fatto aumentare dell'85% il volume complessivo di email dannose rispetto al trimestre precedente, nonostante un calo del 74% di quelle con allegati nocivi.

LOCKY
Locky è il principale ceppo di ransomware osservarvato all'interno di email nocive, che cifra e tiene "in ostaggio" i dati delle vittime finché queste non pagano per decrittografare i dati. Per la maggior parte del 2016 e diversi mesi del 2017, Locky è stato responsabile di un'impennata nel traffico di email nocive.

Questi ultimi rimangono ancora un mezzo vitale per la diffusione. Gli autori degli attacchi hanno sferrato un minor numero di campagne con allegati, ma alcune di esse erano eccezionalmente grandi e nascondevano il codice nocivo in file compressi. I formati di archivio usati erano RAR e 7-Zip, di solito contenenti un JavaScript o VBScript nocivo. Durante l'esecuzione, gli script scaricavano e installavano il ransomware **LOCKY**.

Come mostrano le Figure 1 e 2, i messaggi URL nocivi come percentuale del volume totale dei messaggi globali hanno raggiunto il 64%. Si tratta di una proporzione mai vista dal 2014, l'ultimo anno in cui le email contenenti URL nocivi costituirono la maggioranza delle campagne di attacco. Comunque entrambi gli approcci hanno obiettivi simili: che fosse inviato tramite URL o come allegato, Locky era il payload della maggior parte di tali campagne ad alto volume.

Volume dei messaggi nocivi quotidiani indicizzati, per tipo di attacco, dall'inizio del 2017

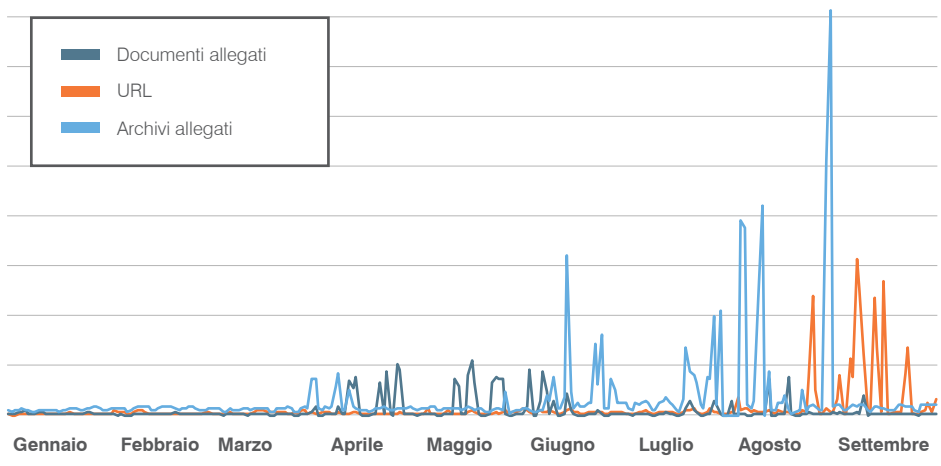

Figura 1: tendenza dei tipi di attacco indicizzati, da gennaio a settembre 2017 (273 giorni)

Confronto del volume dei messaggi nocivi quotidiani indicizzati per tipo di attacco, terzo trimestre 2017

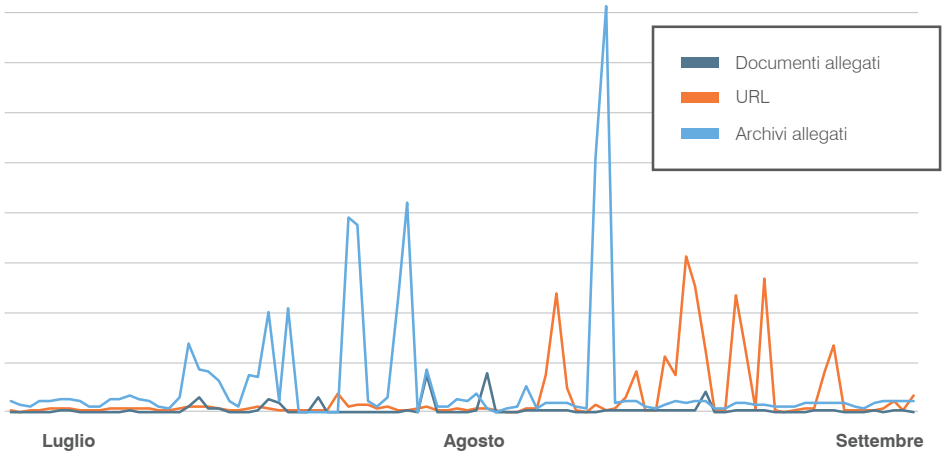

Figura 2: tendenza dei tipi di attacco indicizzati, da luglio a settembre 2017 (92 giorni)

La Figura 3 mostra il continuo predominio del ransomware, in particolare di Locky. I picchi verificatisi verso la fine del trimestre sono stati creati da poche grandi campagne che hanno distribuito il trojan bancario **THE TRICK**.

THE TRICK
The Trick, noto anche come Trickbot, è un trojan bancario strettamente correlato a Dyre. Gli operatori di Dyre sono stati arrestati nel 2015 dalle autorità russe, ma il malware è riemerso nel 2017.

Ransomware rispetto ai trojan bancari e ad altri malware

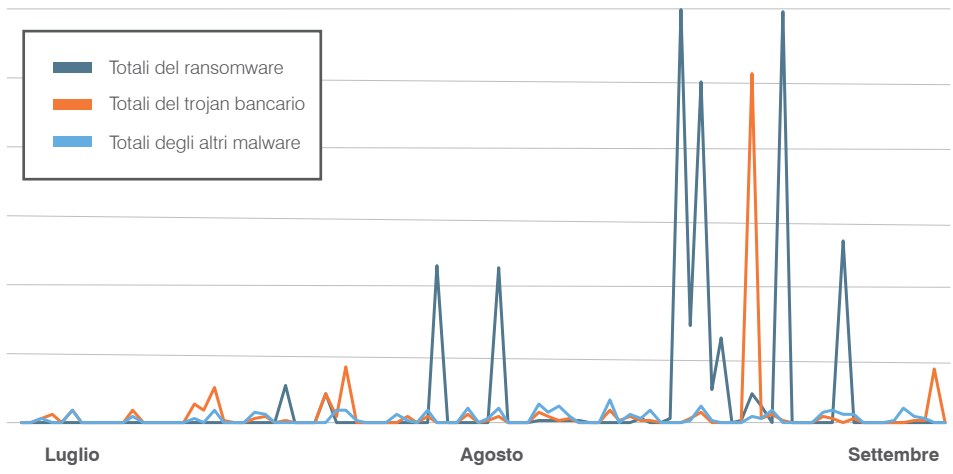

Figura 3: da luglio a settembre 2017 (92 giorni)

TROJAN DEI SERVIZI BANCARI: NUOVE TENDENZE PER VECCHI PROTAGONISTI

Statistiche: The Trick ha costituito il 70% di tutte le email contenenti i trojan bancari. La maggior parte di questo malware proveniva da TA505, il pirata informatico autore delle massicce campagne di email utilizzanti il ransomware Locky e il trojan bancario Dridex.

Con il passaggio di TA505 a The Trick il traffico di **DRIDEX** è sceso notevolmente. Contemporaneamente l'attività di **ZLOADER** si è mantenuta stabile per gran parte del trimestre, benché a livelli più bassi rispetto al secondo trimestre. Nel frattempo, in campagne di livello regionale di grandi dimensioni sono comparsi Zeus Panda, Emotet e URLZone.

In uno sviluppo potenzialmente più grande, i trojan bancari come **RETEFE** e The Trick si sono associati all'exploit EternalBlue. Ciò ha consentito ai trojan di diffondersi senza aiuto nelle reti interne dopo l'iniziale infezione via email. Retefe, che ha colpito principalmente le banche svizzere con esche in lingua tedesca, non ha mai raggiunto il volume o la portata di Dridex o Zeus. Ma queste "correnti" di inizio estate dell'epidemia **WANNACRY** – utilizzante anch'essa EternalBlue – indicano una potenziale tendenza per il 2018. Un maggior numero di aggressori potrebbe approfittare dei punti deboli nella protezione rivelati da WannaCry e NotPetya.

La Figura 4 mostra il mix quotidiano dei trojan bancari. I picchi di traffico di The Trick hanno caratterizzato il trimestre, superando di gran lunga correnti minori principalmente di Zloader e Panda Banker.

DRIDEX
Dridex è un diffuso trojan bancario, che si propaga attraverso una varietà di vettori, soprattutto via email, infettando le vittime e rubando le credenziali bancarie.

ZLOADER
Zloader, noto anche come Terdot, è un downloader spesso usato con il trojan bancario Zbot e altre varianti del malware.

RETEFE
Questo trojan bancario ha preso di mira soprattutto alcune aree dell'Europa. Invece di iniettare moduli di accesso fasulli in siti web bancari legittimi per rubare le credenziali (come fanno molti trojan bancari), reindirizza l'utente a una versione falsa del sito web della banca tramite una serie di server proxy.

WANNACRY
A maggio questo ransomware ha infettato decine di migliaia di sistemi in oltre 150 paesi, uno degli attacchi informatici più grandi di sempre. Si diffonde tramite una falla in un componente per la condivisione file di Microsoft Windows.

Tendenza del volume dei messaggi quotidiani indicizzati, principali trojan bancari, terzo trimestre 2017

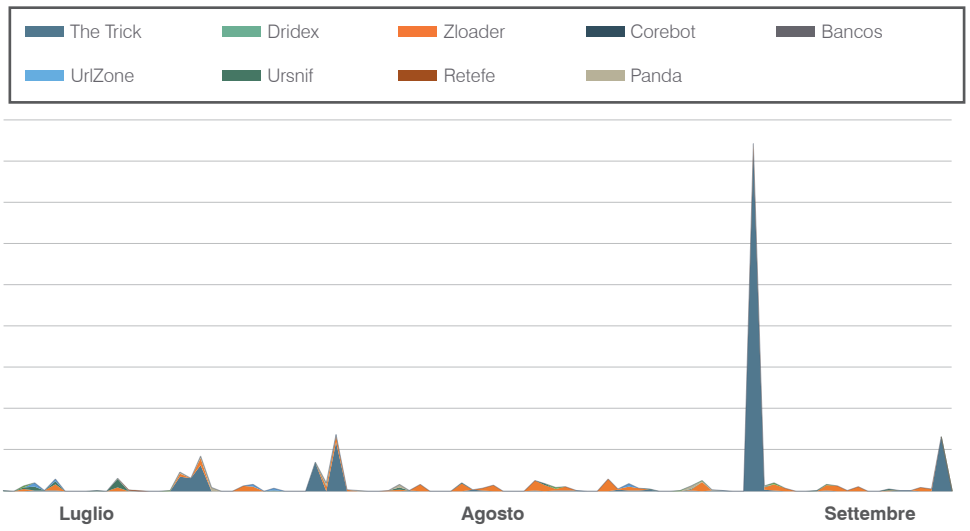

Figura 4: volumi dei messaggi quotidiani indicizzati, principali ceppi dei trojan bancari, luglio-settembre 2017

RANSOMWARE: LOCKY RADDOPPIA, MENTRE AUMENTA IL RANSOMWARE DISTRUTTIVO

Statistiche: i tentativi di ransomware hanno costituito il 64% del volume totale dei messaggi nocivi fra la nostra clientela.

Il ransomware ha continuato a dominare il panorama delle minacce. Nuove varianti sono emerse ogni giorno, lo sviluppo di ransomware distruttivo è proseguito e gli attacchi mirati sono aumentati.

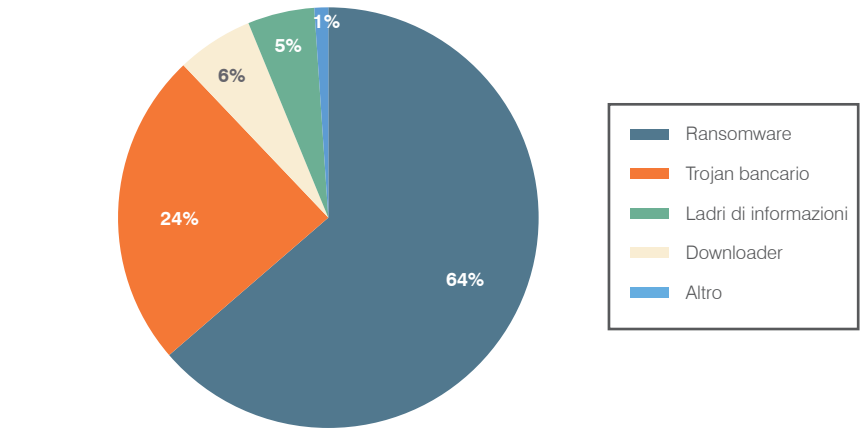

Figura 5: confronto dei volumi complessivi trimestrali dei messaggi

La maggior parte del ransomware è comparsa nelle enormi campagne di Locky lanciate da TA505, che ha diffuso anche le varianti GlobeImposter e Philadelphia. Da notare che una di tali forme includeva una versione "offline" di Locky che, per cifrare i file delle vittime, non richiedeva un'infrastruttura di controllo e comando (C&C).

Altri pirati informatici si sono mossi ulteriormente, passando da campagne indiscriminate ad alto volume ad attacchi più mirati. Uno di questi attacchi su scala ridotta ha introdotto ad agosto il ceppo di ransomware Defray, che ha colpito obiettivi dei settori istruzione e sanità. Altri pirati informatici ne hanno seguito l'esempio, nuovi **ID AFFILIATI** a Locky sono infatti apparsi in campagne volte a colpire il mondo delle università e della sanità. Almeno uno di questi (Affid=36) ha distribuito la versione offline di Locky.

Alla fine del secondo trimestre sono poi emersi nuovi ceppi, sulla scia degli attacchi ucraini WannaCry e simili a Petya. Hell (scoperto a luglio) e IsraByte (scoperto ad agosto) non sono riusciti a guadagnare terreno o pubblicità. Ma come **NOTPETYA** e WannaCry, erano apparentemente concepiti più a scopo di distruzione che di lucro.

Come mostra la Figura 6, nel terzo trimestre gli attacchi ad alto volume si sono aggregati in un piccolo numero di forme di ransomware, nonostante nuovi ceppi e utilizzi. Sotto la spinta di TA505, Locky, GlobeImposter e Philadelphia hanno dominato, mentre al totale si sono aggiunti i nuovi distributori di Locky. Ceppi come SAGE e TorrentLocker sono praticamente scomparsi.

ID AFFILIATI
Spesso gli autori del malware pagano degli affiliati per diffondere le loro creazioni. L'ID affiliato viene codificato nelle versioni del malware per assicurare che il merito dell'infezione venga riconosciuto alle persone giuste.

NOTPETYA
Questo ceppo di malware è camuffato da ransomware Petya ma sembra essere uno strumento sponsorizzato da uno Stato per creare disordine, piuttosto che per estorcere un riscatto.

Tendenza dei volumi di messaggi quotidiani indicizzati, principali ceppi di ransomware, terzo trimestre 2017

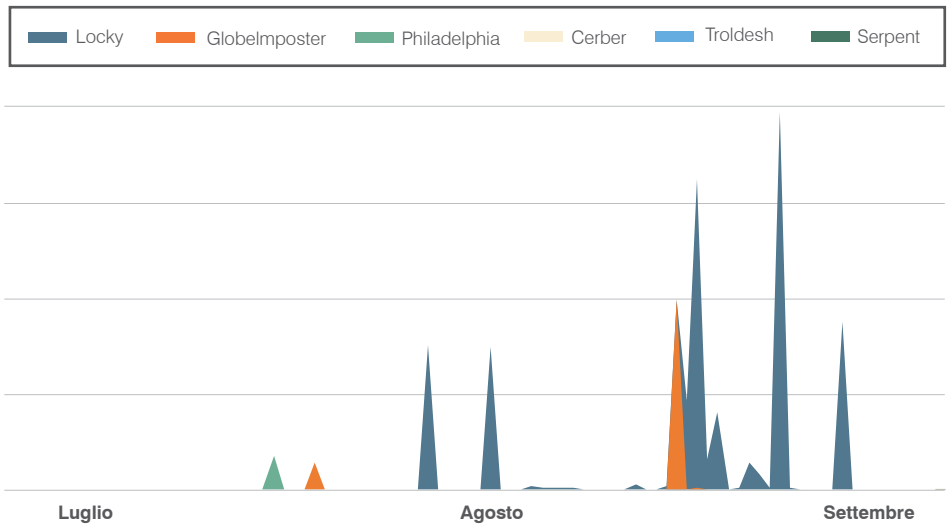

Figura 6: volume dei messaggi quotidiani indicizzati, principali ceppi di ransomware, luglio-settembre 2017

RANSOMWARE
Questo tipo di malware blocca i dati delle vittime cifrandoli, poi chiede un "riscatto" per sbloccarli con una chiave di decrittografia.

La crescita pressoché esponenziale delle nuove forme di **RANSOMWARE** nell'ultimo anno sembra finalmente in lieve rallentamento, ma non a causa della riduzione di una minaccia.

In media, ogni giorno sono comparse 1,4 nuovi ceppi di ransomware, in calo dagli 1,8 al giorno del trimestre precedente. La diminuzione è probabilmente dovuta a un grosso calo dei ceppi di ransomware "progetti minori", proof-of-concept, sperimentali e creati dagli smanettoni degli script, che avevano gonfiato in precedenza i totali.

In altre parole, il rallentamento non indica un livello di minaccia più basso da parte del ransomware. Al contrario, suggerisce il fatto che gli autori degli attacchi si stiano focalizzando su pochi ceppi più efficaci, usando il ransomware in nuovi e più sofisticati modi (Figura 7).

Nuovi ceppi segnalati

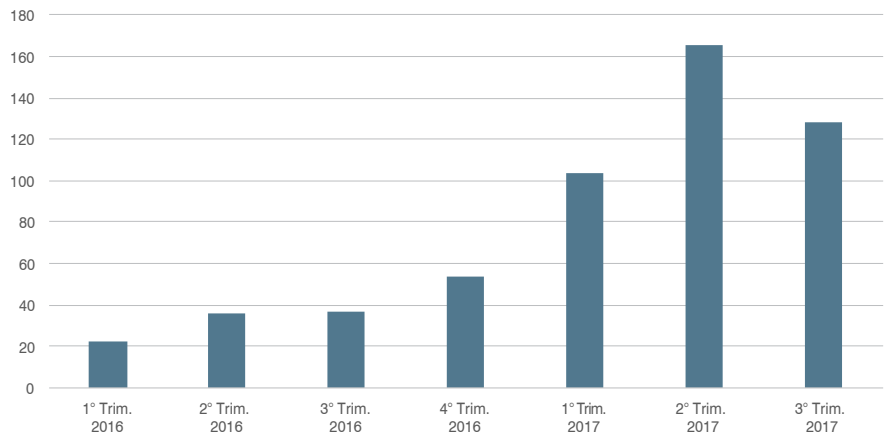

Figura 7: nuovi ceppi di ransomware segnalati per trimestre, 2016 e dall'inizio del 2017

L'OSSESSIONE COINMINER

Gli estrattori delle **CRIPTOVALUTE**, o "coinminer", sono ceppi di malware che usano le risorse di sistema dei computer infetti per generare contanti elettronici da mettere a disposizione degli attori delle minacce. Le criptovalute come Bitcoin e Litecoin incorporano dei meccanismi per creare penuria e così assicurare il valore della valuta. Ciò rende sempre più difficile il completamento dei calcoli necessari per "estrarre" le nuove unità della valuta. Bitcoin, la più popolare criptovaluta, per essere estratta richiede ora una potenza computazionale pari quasi a quella dei supercomputer. Ma altre criptovalute come Litecoin e Monero possono ancora essere estratte da un normale computer desktop oppure rubando i cicli delle CPU di un gran numero di sistemi client.

Il risultato è che il malware per l'estrazione di queste valute (coinminer) è in crescita e si diffonde tramite i kit di exploit, le strategie di social engineering, e perfino attraverso gli exploit della NSA come EternalBlue. Di recente The Pirate Bay ha fatto notizia perché usava i cicli delle CPU dei visitatori per estrarre la valuta Monero.

Si tratta di una minaccia ramificata. Alcuni attacchi puntano alle vulnerabilità web lato server per incorporare gli script che invitano i coinminer a usare le risorse CPU dei browser visitatori. Un'altra tendenza ampia e in rapida crescita è invece quella degli attacchi che usano il phishing per rubare le credenziali del portafogli di criptovaluta degli utenti. Altri attacchi usano infine il malware per trasformare gli stessi PC degli utenti in coinminer.

A prescindere dei metodi utilizzati, gli attori delle minacce esploreranno probabilmente nuovi metodi per sfruttare i PC delle vittime ai fini dell'estrazione. Finché le valute minori non raggiungeranno i livelli di saturazione di Bitcoin, le prospettive di lucro sono ottime. I malintenzionati hanno mostrato più e più volte la loro volontà di "seguire il denaro".

CRIPTOVALUTA
Una forma di denaro digitale concepita per essere sicura e anonima. La valuta – che può essere sia usata per comprare e vendere beni sia scambiata con le valute nazionali – viene creata tramite un processo di "estrazione" che usa la potenza dei computer per risolvere complessi problemi matematici.

DOMAIN SPOOFING
Il domain spoofing impersona colleghi o contatti affidabili facendo apparire le email di un aggressore come provenienti da un indirizzo legittimo e noto. Alcuni domain spoofing usano dei nomi di dominio ingannevolmente simili a quelli reali.

LE TECNICHE SI AFFINANO E LE FRODI VIA EMAIL AUMENTANO

Statistiche: fra la nostra clientela i tentativi di frode via email sono aumentati del 29% rispetto al trimestre precedente.

Se il numero totale delle frodi via email aumenta, lo stesso si può dire della frequenza degli attacchi a determinate aziende: +12% rispetto al trimestre precedente e +32% rispetto allo stesso periodo dell'anno scorso.

È aumentato anche il DOMAIN SPOOFING, una comune tecnica di frode via email. È possibile prevenire completamente questo tipo di attacco con l'autenticazione della posta elettronica. Ciononostante l'89% delle aziende ha subìto almeno un attacco di domain spoofing nel trimestre.

Settori colpiti

Le frodi via email continuano a colpire tutti i settori ma, come nei trimestri precedenti, sembrano preferire le aziende con catene di fornitura più complesse. Il settore manifatturiero, per esempio, continua a essere colpito più spesso di altri. La Figura 8 mostra la relativa frequenza degli attacchi per settore verticale. Confrontando il terzo trimestre 2017, il secondo trimestre 2017 e il terzo trimestre 2016 si notano andamenti simili.

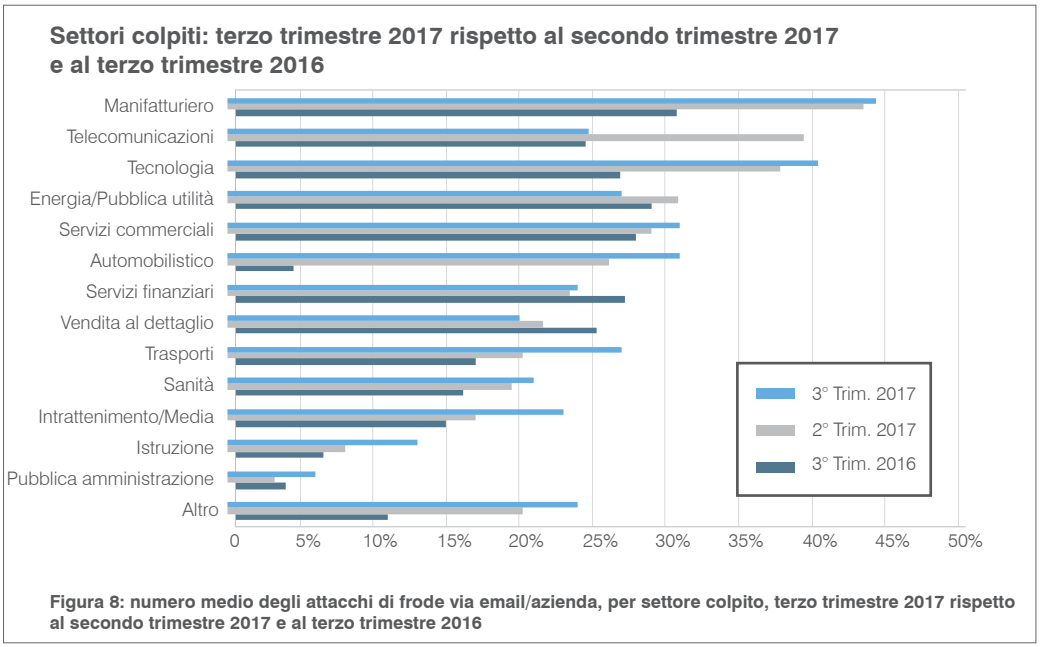

Figura 8: numero medio degli attacchi di frode via email/azienda, per settore colpito, terzo trimestre 2017 rispetto al secondo trimestre 2017 e al terzo trimestre 2016

FRODE VIA EMAIL
Negli attacchi delle frodi via email, un messaggio di posta elettronica apparentemente proveniente da un dirigente di alto livello chiede al destinatario di fare un bonifico bancario o di inviargli dei dati sensibili. Dato che non usa allegati o URL può essere difficile da rilevare e fermare.

La nostra analisi delle **FRODI VIA EMAIL** non ha riscontrato alcuna correlazione fra le dimensioni di un'azienda e la frequenza dei tentativi subiti. Nel secondo trimestre abbiamo osservato indizi della priorità data alle grandi aziende da parte dei criminali informatici, ma non a un livello statisticamente significativo. In questo trimestre qualsiasi apparente relazione è scomparsa del tutto: sono state colpite indifferentemente aziende di tutte le dimensioni.

Gli attacchi agli individui mostrano un affinamento.

Per sua natura, la frode via email è altamente mirata. Ciò è risultato più chiaro che mai, dato che è stato falsificato un maggior numero di identità e sono stati presi di mira più dipendenti per azienda. Quasi tre quarti delle aziende colpite aveva più di un'identità falsificata e più di un dipendente colpito. È ancora comune il cosiddetto "whaling", cioè l'attacco in cui l'email falsificata di un dirigente di alto livello viene usata per colpire un altro dirigente di pari livello (questo tipo di attacchi è rappresentato nella Figura 9 come attacco "da uno a uno"). Ma i criminali informatici stanno espandendo la loro portata puntando a un maggior numero di persone in ciascuna azienda.

Identità falsificate per numero di dipendenti colpiti, terzo trimestre 2017 rispetto al secondo trimestre 2017 e al terzo trimestre 2016

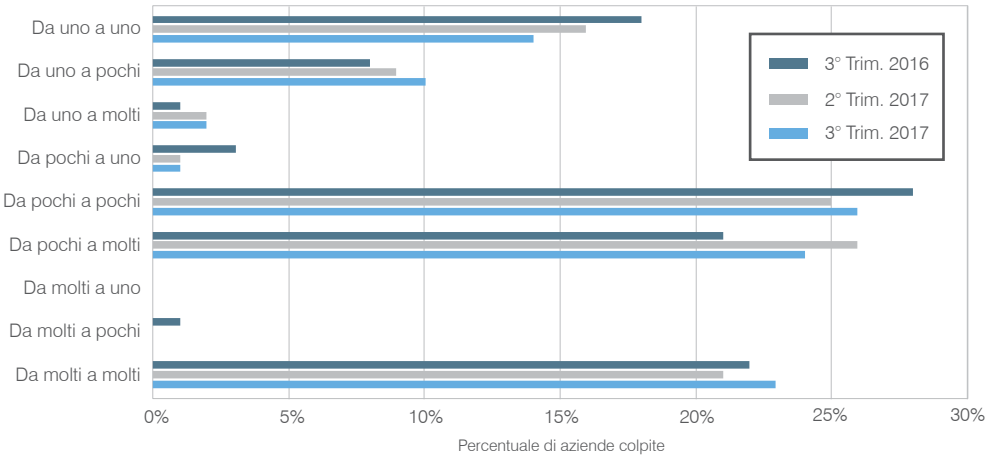

Figura 9: tipi di attacco per numero di identità di dirigenti falsificate rispetto al numero di persone colpite. Per esempio, l'attacco di frode via email subito da un'azienda con quattro identità di dirigenti falsificate e dieci dipendenti dell'ufficio finanziario colpiti, viene classificato come "Da pochi a molti".

Continuano inoltre a usare catene di email fasulle per rendere più convincente il proprio messaggio. Nel terzo trimestre questa tattica è stata utilizzata da circa il 10% di tutte le frodi via email.

KIT DI EXPLOIT: IN CALO MA NON FUORI GIOCO

RIG
RIG è diventato il kit di exploit più popolare dopo la scomparsa di Angler, i cui operatori sono stati arrestati nel giugno 2016.

Statistiche: il 73% di tutte le attività di exploit del terzo trimestre coinvolgeva il kit di exploit RIG.
Dopo un picco a inizio 2016 i kit di exploit hanno subito un drastico e ben pubblicizzato declino. Anche se l'attività è ristagnata a solo il 10% dei livelli del 2016, i kit di exploit restano una parte importante del panorama delle minacce. Ciò è particolarmente vero nelle regioni in cui alti livelli di pirateria software impediscono un'applicazione regolare delle patch.

Con i kit di exploit vengono inoltre utilizzati anche nuovi schemi di social engineering, il che significa che gli autori non devono affidarsi ai kit più recenti per raggiungere i propri scopi. Vediamo però una maggiore attività dei "traffer": reti progettate per indirizzare il traffico alle pagine di destinazione dei kit di exploit. Questo cambio indica una possibile ripresa dell'attività dei kit di exploit nei mesi a venire.

Per ora il kit di exploit RIG resta quello dominante, essendo responsabile del 73% di tutto il traffico dei kit di exploit di questo trimestre. Alla fine del trimestre, il già fiacco traffico associato al kit di exploit Angler era pressoché scomparso. Anche Neutrino, che si era conteso la prima posizione con RIG in alcuni periodi del trimestre, alla fine ha lasciato il campo a RIG. La Figura 10 mostra il traffico dei primi kit di exploit.

Attività dei kit di exploit: percentuali di campioni raccolte nel terzo trimestre 2017

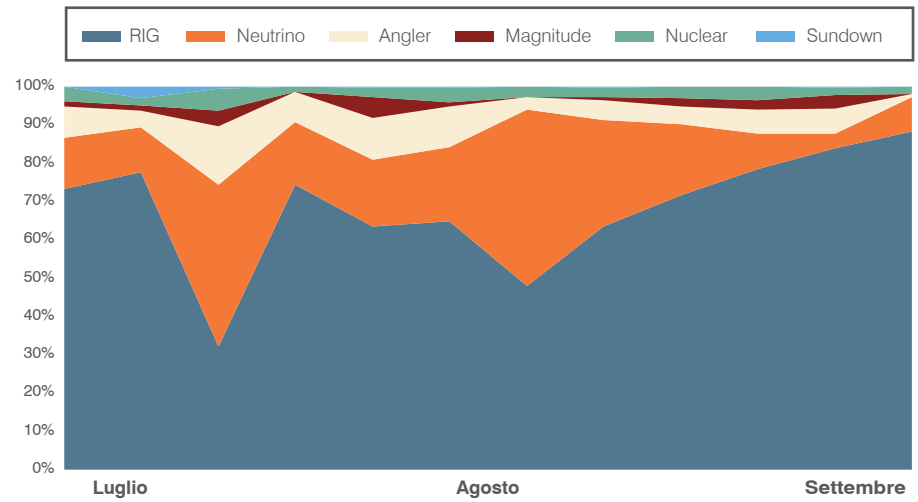

Figura 10: traffico dei principali kit di exploit in percentuale del totale, aprile-maggio 2017

TENDENZE NEI DOMINI

Statistiche: le registrazioni sospette dei domini hanno superato quelle difensive di 20 a 1, ampliando il divario fra le aziende che cercano di proteggere il proprio marchio e i malintenzionati che tentano di sfruttarlo.

Nel terzo trimestre abbiamo esteso la nostra ricerca per esaminare le registrazioni dei "domini sospetti" tra le aziende Fortune 50. I domini sospetti sono quelli che probabilmente vengono utilizzati per il **TYPOSQUATTING** e lo spoofing.

TYPOSQUATTING
I truffatori registrano dei domini che sono versioni con errori ortografici o comunque storpiate di domini legittimi, al fine di ingannare gli utenti che digitano male gli URL o che non prestano attenzione alle intestazioni delle email.

Dall'inizio del 2015 fino alla fine di agosto 2017, il numero di domini difensivi di proprietà dei rispettivi marchi è crollato, mentre il numero di quelli sospetti registrati da estranei è aumentato (Figura 11). Da gennaio ad agosto 2017, le registrazioni dei domini sospetti sono aumentate del 20% rispetto allo stesso periodo dell'anno prima, mentre le registrazioni difensive sono calate della stessa percentuale.

Anche con le registrazioni difensive, i domini sospetti hanno storicamente superato di gran lunga i domini di proprietà dei marchi. Nel 2016 per ogni registrazione difensiva abbiamo riscontrato dieci registrazioni simili sospette, eseguite da estranei. Quest'anno il rapporto è stato di 20 a 1.

Inoltre, i picchi delle registrazioni difensive sono solitamente legati a un evento importante relativo al marchio, come il lancio di un nuovo prodotto, piuttosto che a una forma di difesa continua.

Confronto delle registrazioni di domini sospetti e delle registrazioni difensive di proprietà dei marchi, dall'inizio del 2017

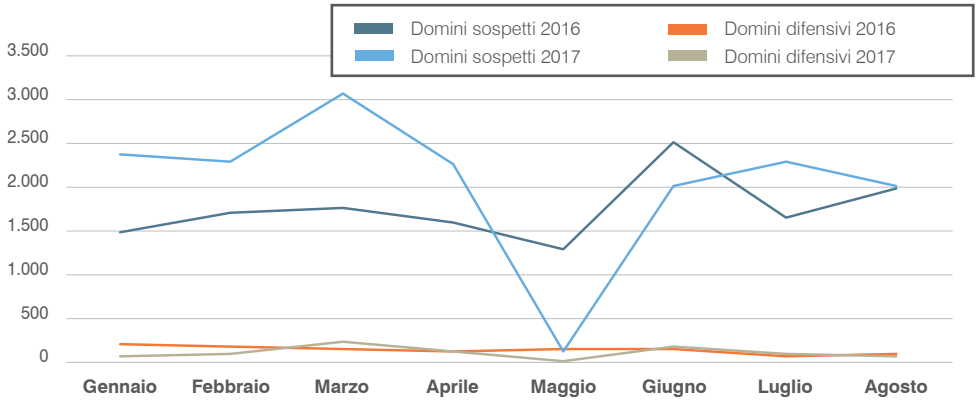

Figura 11: confronto su base annua (Primo - Terzo trimestre 2016 e 2017, rispettivamente) delle registrazioni di domini sospetti e delle registrazioni difensive di proprietà dei marchi Fortune 50

TENDENZE NEI SOCIAL MEDIA

Statistiche: gli account di assistenza clienti fraudolenti sono raddoppiati rispetto al trimestre dell'anno precedente.

Le minacce nei social media sono varie e numerose, dalla distribuzione del malware alla frode. Ne individuiamo due categorie principali:

- account di assistenza fraudolenti utilizzati per il cosiddetto "angler phishing";
- link di phishing più tradizionali che conducono le persone su pagine che sottraggono loro credenziali e dati personali.

Il numero di falsi account di assistenza clienti è cresciuto del 5% rispetto al trimestre precedente e sono raddoppiati rispetto allo stesso periodo di un anno prima. I link di phishing nei social media delle aziende è cresciuto del 10% rispetto al trimestre precedente (Figura 12), pressoché invariato rispetto all'anno scorso.

Nel complesso questi dati suggeriscono un'ampia mutazione negli attacchi ai social media. Anche se gli autori degli attacchi reagiscono a eventi o tendenze stagionali con il phishing convenzionale, stanno volgendo la loro attenzione al più remunerativo angler phishing.

Il phishing tradizionale delle credenziali tramite i social media può essere più semplice, ma l'angler phishing mirato ha maggiori probabilità di successo perché dà un'impressione di legittimità alla vittima. Sembra molto più umano dei link casuali inseriti nei commenti ai social media delle aziende.

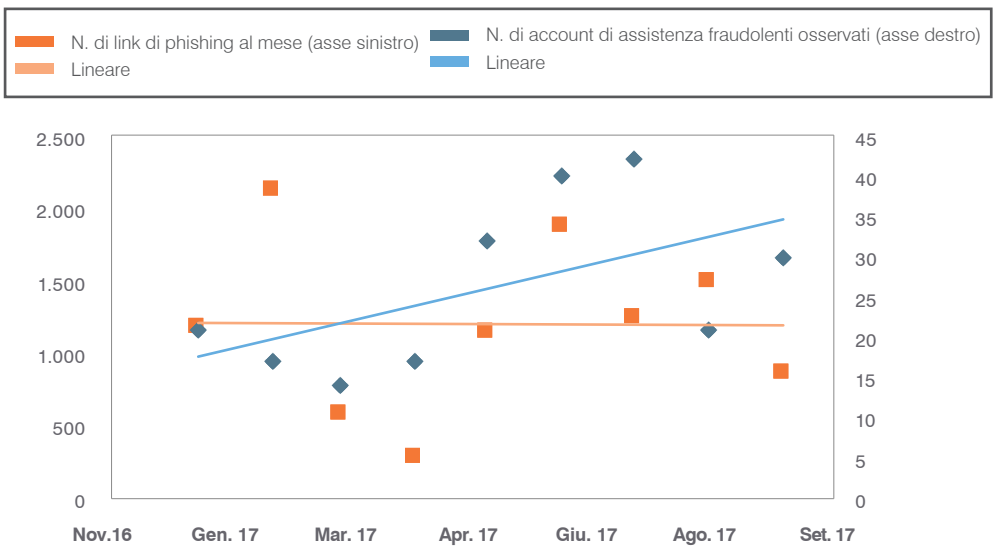

Figura 12: attività mensile relativa nella distribuzione dei link di phishing tramite i social media rispetto agli account di assistenza fraudolenti

SUGGERIMENTI

Questo report esamina i cambiamenti nel panorama delle minacce per fornire informazioni da utilizzare per la strategia di sicurezza informatica dell'azienda. Ecco le nostre migliori raccomandazioni su come proteggere dati, persone e marchi nei mesi a venire.

Combatti il typosquatting sul web.
La registrazione difensiva dei domini è una tattica semplice e conveniente per impedire ai pirati informatici di creare domini simili allo scopo di perpetrare le frodi via email e il phishing delle credenziali. Lavora con i tuoi responsabili per definire un elenco di possibili domini da registrare. Includi i siti web delle conferenze e delle campagne di marketing, che sono dei bersagli frequenti.

Implementa l'autenticazione della posta elettronica per bloccare le tecniche di domain spoofing usate nelle frodi via email.
Con i protocolli come DMARC (Domain-based Message Authentication, Reporting & Conformance), puoi impedire ai truffatori di usare il dominio della tua posta elettronica. Per gli attacchi tramite messaggi email che usano dei domini simili a quelli veri, la tua soluzione deve essere in grado di trovare quei domini che potrebbero essere confusi con i tuoi e poi deve collaborare con i servizi di terze parti per farli chiudere.

Proteggi i tuoi utenti dagli attacchi via email di tutti i tipi.
Che si tratti di allegati di malware, URL dannosi o frodi tramite social engineering, la difesa della tua posta elettronica deve coprire la più ampia gamma di minacce. Una protezione efficace include solide capacità di analisi per identificare e mettere preventivamente nella sandbox gli URL e allegati sospetti. L'analisi nella sandbox deve essere a più fasi per identificare gli URL e gli allegati nocivi, sia al punto di consegna sia quando i dipendenti vi fanno clic. Deve inoltre identificare e bloccare le minacce che non sono malware, come quelle email che potrebbero indurre i dipendenti a inviare soldi e dati sensibili agli impostori.

Associati a un fornitore di intelligence sulle minacce.
Attacchi più piccoli e mirati richiedono informazioni sofisticate sulle minacce. Adotta una soluzione che abbini i dati delle analisi con le informazioni sulle minacce, combini le tecniche statiche e dinamiche per rilevare i nuovi strumenti, tattiche e bersagli degli attacchi, per poi apprendere da essi. Correlando i risultati delle analisi con i feed di informazioni sulle minacce, si possono catturare le email difficili da rilevare prima che un utente abbia la possibilità di farvi clic.

Proteggi il tuo marchio dagli impostori annidati nei social media.
Cerca una soluzione di sicurezza che ti allerti degli account simili al tuo nei social media, specialmente di quelli che offrono servizi fraudolenti di "assistenza clienti". La soluzione non deve solo rilevare tali account illeciti ma anche lavorare con i servizi di rimozione per far cessare l'attività ingannevole nei confronti dei tuoi clienti e partner.

Per le informazioni e le analisisulle minacce più recenti,
visita il blog Threat Insight di Proofpoint
all'indirizzo **proofpoint.com/us/threat-insight**

INFORMAZIONI SU PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT), società specializzata nella sicurezza informatica di nuova generazione, consente alle aziende di proteggere il lavoro dei dipendenti dalle minacce avanzate e dai rischi di conformità. Proofpoint aiuta i professionisti della sicurezza informatica a proteggere i propri utenti dagli attacchi avanzati che li colpiscono (tramite email, app mobili e social media), a tutelare le informazioni critiche create dalle persone e a dotare il personale delle informazioni e degli strumenti giusti per reagire rapidamente quando si verifica un problema. Le principali aziende di ogni dimensione, compreso oltre il 50% delle Fortune 100, si affidano alle soluzioni Proofpoint. Concepite per gli ambienti informatici di oggi, mobili e social, le nostre soluzioni sfruttano sia la potenza del cloud sia una piattaforma analitica basata su big data per combattere le moderne minacce avanzate.

proofpoint.

www.proofpoint.com