REPORT

proofpoint.

REPORT TRIMESTRALE SULLE MINACCE

QUARTO TRIMESTRE

proofpoint.com/it

Il *Report trimestrale sulle minacce Proofpoint* espone le tendenze e i dati principali degli attacchi 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 app cloud. Il nostro lavoro costituisce un punto di osservazione privilegiato, dal quale individuare 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: ESTRATTORI DI VALUTA E RANSOMWARE SONO IN PRIMA LINEA

Di seguito i dati principali relativi al quarto trimestre 2017.

EMAIL

Il volume dei messaggi con allegati documenti dannosi è salito del 300%.
Gran parte di questo traffico è derivato da imponenti campagne di attacco che hanno abusato del protocollo **DYNAMIC DATA EXCHANGE** di Microsoft e utilizzato tecniche di social engineering.

IL RANSOMWARE è rimasto il principale payload distribuito tramite messaggi dannosi.
Questo tipo di attacco ha rappresentato il 57% del volume complessivo dei messaggi dannosi.

Il numero di richieste di pagamento ransomware denominate in Bitcoin è sceso del 73% tra ampie oscillazioni del valore della CRIPTOVALUTA.
Gli aggressori stanno sempre più imponendo importi in termini di dollari americani o di valuta locale (sebbene il pagamento di per sé di solito sia ancora in criptovaluta).

THE TRICK è stato il trojan bancario più utilizzato.
Ha rappresentato l'84% di tutto lo spam dannoso che conteneva un trojan bancario.

Domini fotocopia e CON URL DIROTTATO TRAMITE TYPOSQUATTING sono stati utilizzati in una vasta gamma di attacchi
Lo scambio di caratteri si è dimostrata la tecnica migliore utilizzata per creare domini che potrebbero essere confusi con un marchio o un'azienda consolidata.

KIT DI EXPLOIT E ATTACCHI BASATI SUL WEB

Le tecniche di social engineering si sono sviluppate man mano che gli exploit del browser ricadevano tra le campagne di attacco di alto profilo basate sul web.
IL TRAFFICO PROVENIENTE DAI KIT DI EXPLOIT (KE) è sceso del 31% rispetto al trimestre precedente. Il KE RIG è stato il più utilizzato.

SOCIAL MEDIA

Il numero di account di assistenza clienti fraudolenti sui social media è aumentato del 30%.
Allo stesso tempo, i collegamenti di phishing nei social media sono aumentati del 70% rispetto al trimestre precedente.

DYNAMIC DATA EXCHANGE
Dynamic Data Exchange (DDE) è un protocollo di comunicazione esistente da 20 anni in Microsoft Windows che consente ai documenti di estrarre informazioni da altri documenti. La tecnica è stata ampiamente sostituita dai nuovi protocolli ma è ancora supportata in Windows.

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

CRIPTOVALUTA
Una forma di denaro digitale progettata per essere sicura ed anonima, il che la rende adatta per i pagamenti di ransomware, poiché non permette di rintracciare l'aggressore.

THE TRICK
The Trick, noto anche come TrickBot, è un trojan dei servizi bancari strettamente correlato a Dyre. Sebbene i suoi operatori siano stati arrestati nel 2015 dalle autorità russe, ha vissuto una rinascita nel 2017.

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

KIT DI EXPLOIT
I kit di exploit (KE) sono attivi sul web, rilevando e sfruttando le vulnerabilità dei computer che si connettono a siti compromessi, pubblicità dannose e pagine di destinazione controllate dagli aggressori. I KE, spesso venduti agli aggressori come un servizio, permettono di infettare in modo semplice i PC con download di malware "drive-by" e vengono sempre più utilizzati per distribuire attacchi di social engineering che non si affidano a exploit attivi.

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

LOCKY
Locky è il ceppo più comune di ransomware osservato all'interno di email dannose, che crittografa i dati delle vittime e li tiene in "ostaggio" finché la vittima paga per la decodifica. Per la maggior parte del 2016 e diversi mesi nel 2017, Locky ha rappresentato la maggior parte del traffico email dannoso.

GLOBEIMPOSTER
Questa variante di malware, nota anche come Fake Globe, imita e prende il nome da una precedente varietà ransomware denominata Globe. Inizialmente utilizzato in campagne regionali limitate, GlobeImposter è diventato una minaccia globale quando il prolifico malintenzionato TA505 ha iniziato a impiegarlo in campagne più ampie.

EMAIL: I DOCUMENTI DANNOSI SUPERANO GLI URL

Statistiche: il volume dei messaggi con allegati documenti dannosi è salito del 300% rispetto al terzo trimestre.

Il volume complessi di messaggi con allegati dannosi ha preso il volo, aumentando di oltre il 300% rispetto al trimestre precedente. Spinti da campagne ad alto volume sferrate dal malintenzionato **TA505**, questi messaggi spesso distribuivano il trojan bancario Trick o un assortimento di ceppi ransomware, tra cui **LOCKY** e **GLOBEIMPOSTER**.

Diversi aggressori hanno approfittato della divulgazione di una tecnica per abusare del protocollo Dynamic Data Exchange (DDE) di Microsoft per distribuire malware in campagne di grandi e piccoli volumi.

Alla fine di ottobre, gli aggressori avevano già in gran parte abbandonato tale tecnica mentre si rivolgevano ai loro soliti metodi di sfruttamento di macro dannose e altre forme di codice incorporato. Ma le campagne sporadiche che utilizzavano la tecnica DDE sono proseguite nei mesi di novembre e dicembre, dal momento che la tecnica si è conquistata il suo posto all'interno del toolkit a rotazione utilizzato dai malintenzionati.

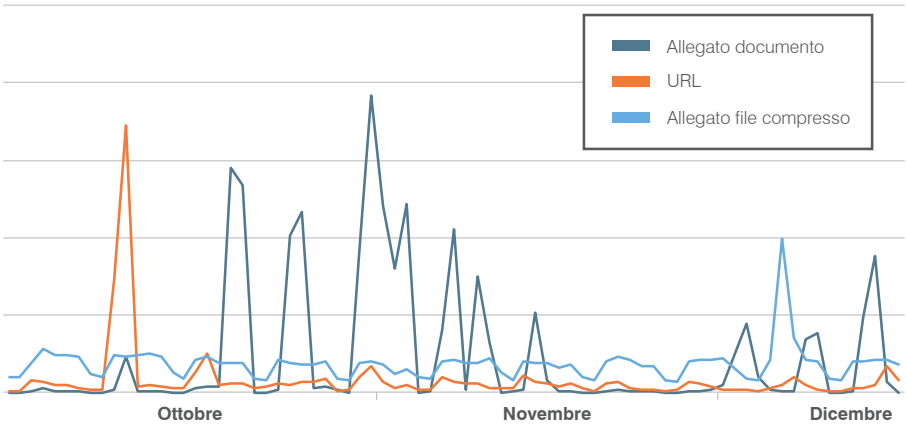


Figura 1: tendenza dei tipi di attacco indicizzati, ottobre-dicembre 2017 (77 giorni)

Viceversa, l'utilizzo di URL dannosi è crollato: i volumi eccezionalmente elevati del terzo trimestre si sono rivelati un'anomalia. Comunque, tutti i tipi di attacco rimangono popolari con un ricco assortimento di malintenzionati.

La figura 1 mostra notevoli oscillazioni nel volume di messaggi nocivi che utilizzano URL dannosi, allegati di documenti e allegati di file di archivio (come ZIP o 7-Zip). Questi cambiamenti costanti evidenziano la flessibilità degli aggressori, che variano continuamente tipi di attacco, payload e tecniche di infezione per diventare più efficaci e ottenere i maggiori guadagni possibili.

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.

ZEUS PANDA
Noto anche come Panda Banker, questo trojan dei servizi bancari è correlato a Zeus, uno dei primi trojan in questo campo.

ESTRATTORI DI VALUTA
La criptovaluta viene creata attraverso un processo di "estrazione" che utilizza la potenza di un computer per risolvere complessi problemi matematici. Gli estrattori di valuta sono ceppi di malware che si impadroniscono dei sistemi infetti a questo scopo, generando criptovaluta per il malintenzionato che distribuisce il malware.

WEBINJECT
Una tecnica che altera le pagine web così come vengono visualizzate agli utenti. Gli aggressori utilizzano i webinject per allegare moduli pericolosi a siti Web apparentemente sicuri. Quando gli utenti compilano i moduli (per esempio, con le loro credenziali bancarie), tali informazioni vengono inviate all'aggressore invece che alla banca.

TROJAN DEI SERVIZI BANCARI: NON SOLO PER IL SETTORE BANCARIO

Statistiche: i messaggi che hanno distribuito The Trick hanno rappresentato l'84% del volume di messaggi di TROJAN DEI SERVIZI BANCARI.

The Trick ha proseguito la sua corsa come il principale trojan bancario per volume di messaggi globale. È apparso in sei volte più messaggi di tutti gli altri trojan dei servizi bancari osservati messi insieme. Situazione ben lontana da quella del 2016, quando Dridex e Vawtrak erano i migliori trojan in ambito bancario e The Trick si limitava a campagne per lo più piccole e mirate geograficamente.

Insieme a The Trick, anche **ZEUS PANDA** (noto anche come Panda Banker) ed Emotet sono apparsi frequentemente nelle campagne del quarto trimestre. E diversi aggressori abituali hanno rapidamente adottato un nuovo Trojan denominato IcedID.

Alcuni trojan dei servizi bancari - soprattuttoThe Trick - hanno aggiunto moduli per l'estrazione di criptovaluta o bot. Altre campagne nell'ambito dei servizi bancari hanno aggiunto gli **ESTRATTORI DI VALUTA** come payload successivi, espandendo una tendenza che abbiamo segnalato nel terzo trimestre.

Negli anni passati, durante i mesi autunnali abbiamo osservato maggiori variazioni nell'individuazione degli obiettivi da parte dei trojan dei servizi bancari. Nel quarto trimestre è stato lo stesso. Campagne di Zeus Panda che hanno integrato e ampliato il consueto banking online del bot **WEBINJECT** con infezioni "inject" contro i siti di shopping online di diversi negozi fisici di grandi catene.

Questi cambiamenti servono a ricordare che i Trojan dei servizi bancari non si limitano affatto a prendere di mira i clienti delle società di servizi finanziari. I clienti online di *qualsiasi* azienda o servizio sono potenziali obiettivi.

RANSOMWARE: LA VOLATILITÀ DEI BITCOIN STRAVOLGE IL BUSINESS

Statistiche: l'utilizzo di Bitcoin per denominare le richieste di ransomware è sceso del 73%.

Nonostante l'aumento del volume di messaggi Trojan dei servizi bancari - in gran parte spinto da estese campagne da parte di un singolo utente aggressore che utilizza The Trick - il ransomware è rimasto il payload dannoso principale nelle campagne email. Ha rappresentato oltre il 57% di tutti i messaggi dannosi, come mostrato nella figura 2.

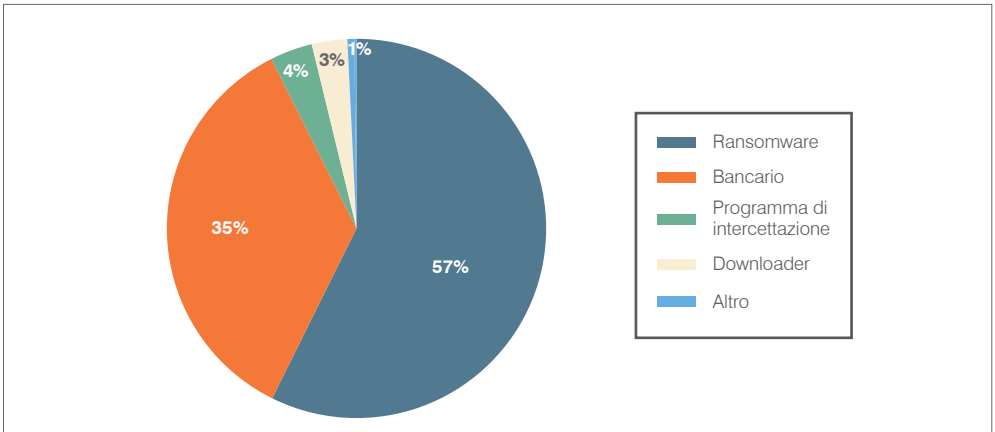


Figura 2: quota del volume di messaggi nocivi globale per famiglia di malware, quarto trimestre 2017

Per gran parte degli ultimi due anni, i riscatti degli aggressori sono stati denominati in valori Bitcoin. La quantità richiesta è espressa come un certo ammontare di bitcoin, sia interi che frazioni come "0,5" o "0,15".

L'impennata dei valori di criptovaluta sono un vantaggio per i possessori di Bitcoin. Ma rappresentano una sfida per chiunque tenti di valutare il proprio prodotto o servizio in Bitcoin - aggressori inclusi.

Nel quarto trimestre, i nuovi ceppi di ransomware sembravano tenerne conto. Il ransomware Sigma è apparso per la prima volta a metà novembre richiedendo un pagamento denominato in dollari statunitensi.

La denominazione di riscatti in una valuta emessa dal governo, anche se il pagamento effettivo è effettuato sotto forma di Bitcoin, offre due grandi vantaggi a un aggressore. Consente ai malintenzionati di mantenere prezzi stabili e continuare ad accettare i pagamenti in modo anonimo e in una valuta che, per il momento, continua a crescere di valore rapidamente.

Analizzando le richieste di ransomware su un periodo di 90 giorni a metà dicembre, è facile capire che il cambio di valuta era parte di una diffusa tendenza in diversi attacchi (figura 3).

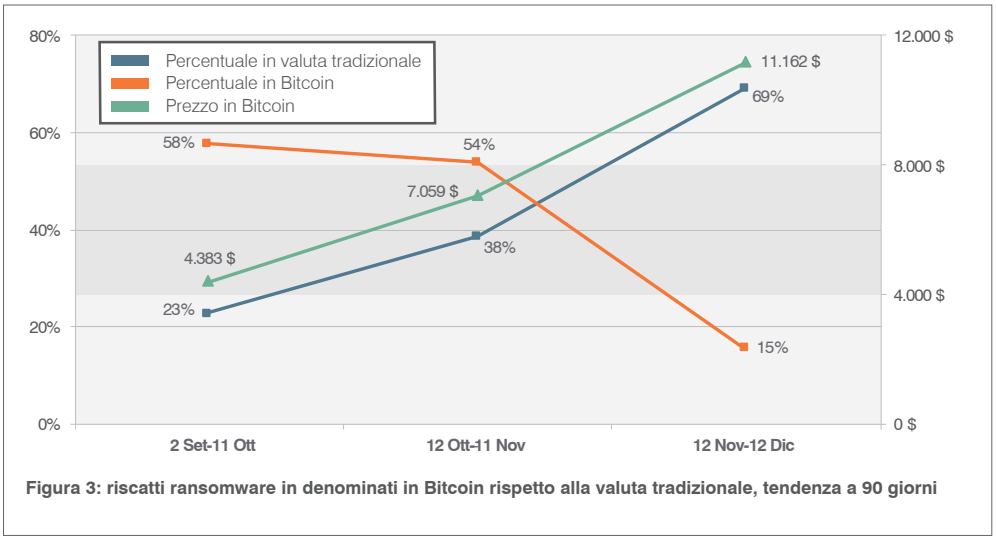


Figura 3: riscatti ransomware in denominati in Bitcoin rispetto alla valuta tradizionale, tendenza a 90 giorni

La denominazione delle richieste di ransomware in valuta tradizionale invece che in Bitcoin o in aggiunta ai Bitcoin è chiaramente correlata all'aumento delle valutazioni dei Bitcoin. L'economia suggerirebbe che quest'ultimo elemento sia effettivamente causa del primo.

Questa tendenza potrebbe invertirsi se i prezzi del Bitcoin tornassero a livelli realistici. Qualunque cosa accada, la correlazione è la prova più evidente del profitto come motivazione dei criminali informatici moderni. Scelgono gli strumenti e le tecniche che meglio consentono loro di "seguire il denaro".

MALINTENZIONATI MIRATI APRONO LA SUPERFICIE

Molte delle campagne monitorate dai nostri ricercatori nel quarto trimestre sono rappresentate da payload malware distribuiti in modo diffuso. Ma abbiamo anche analizzato e segnalato le attività di numerosi malintenzionati estremamente mirati, tra cui Lazarus Group, APT28 e un nuovo attore di minacce che abbiamo soprannominato Leviathan.

Le email e i documenti utilizzati in questi attacchi erano spesso personalizzati e adattati agli interessi e alle attività del destinatario preso di mira. Spesso, è stato utilizzato materiale di branding rubato e documenti pubblici. Inoltre, sono stati sfruttati domini simili o colpiti da attacchi di typosquatting per ingannare i destinatari portandoli a fare clic sui collegamenti o scaricare file.

LA MINACCIA DELLE FRODI VIA EMAIL: DARE UN SENSO ALLE PRATICHE FRAUDOLENTE DI DENOMINAZIONE DEI DOMINI

Statistiche: il numero medio di REGISTRAZIONI DIFENSIVE DI DOMINI ammonta a 300 domini. Per le grandi imprese, i domini registrati in modo sospetto possono superare i domini registrati dall'azienda nell'ordine di 20 a 1.

REGISTRAZIONI DI DOMINI DIFENSIVE
Pratica raccomandata che consiste nell'acquistare i domini Internet confondibili con quelli di marchi legittimi, prima che lo facciano i pirati informatici. I domini simili possono essere utilizzati per ingannare clienti e partner con siti web fasulli ed email fraudolente, in apparenza provenienti dalla propria 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.

La nostra ricerca suggerisce che i malintenzionati superano notevolmente i brand nella registrazione di domini sospetti rispetto alle registrazioni difensive. Questa ampia lacuna lascia i marchi vulnerabili a frodi, phishing, spoofing e altro ancora.

Per difendersi, le aziende non devono registrare ogni possibile permutazione del proprio dominio o domini. Invece, possono analizzare le modifiche e le sostituzioni più comuni per assegnare la priorità alle loro registrazioni difensive e gestire un sottoinsieme più ragionevole di potenziali domini colpiti da attacchi di typosquatting.

I domini "fotocopia" rappresentano poco più del 3% dei tentativi complessivi di frode via email. Ma costituiscono un numero sproporzionato di domini utilizzati nelle frodi via e-mail, phishing, ANGLER PHISHING e altri attacchi.

Mentre alcuni osservatori prestano maggiore attenzione alle nuove o insolite registrazioni fraudolente di domini di primo livello (TLD), le registrazioni sospette per l'estensione ".com" standard rimangono di gran lunga le più comuni.

Quasi l'82% di tali registrazioni utilizza ".com". Inoltre, quasi il 90% delle registrazioni sospette ha utilizzato lo stesso TLD del marchio per cui si spacciavano. I truffatori tramite email spesso utilizzano semplici variazioni sui nomi di dominio legittimi all'interno del TLD del marchio che stanno cercando di impersonare.

La figura 4 evidenzia i modelli di ortografia comuni nelle registrazioni di domini sospetti.

Tipo di dominio similare (cousin)	TLD diverso	Stesso TLD	Totale
Scambio di un singolo carattere	3,49%	37,60%	41,09%
Inserimento di un carattere aggiuntivo	0,97%	31,15%	32,12%
Aggiunta o rimozione di caratteri iniziali/finali	0,73%	12,51%	13,25%
Rimozione di un carattere	0,41%	5,10%	5,51%
Corrispondenza esatta con l'aggiunta di un trattino	1,23%	3,40%	4,63%
Corrispondenza esatta	3,40%	0,00%	3,40%
Totale	**10,23%**	**89,77%**	**100,00%**

Figura 4: tecniche di typosquatting

Lo scambio di singoli caratteri del nome di un marchio all'interno dello stesso TLD è la tecnica di typosquatting più comune. La figura 5 mostra i cambi di lettere nello specifico.

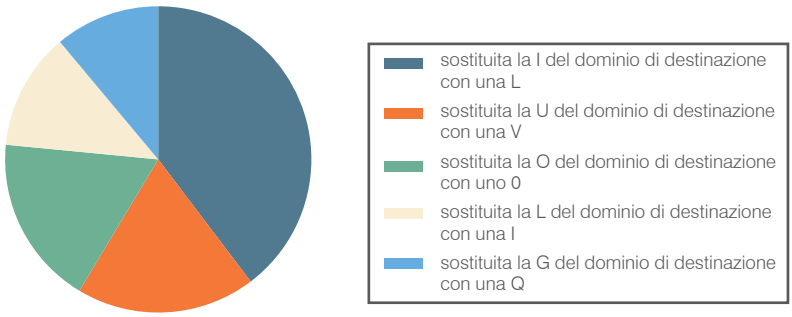


Figura 5: schemi di sostituzione di caratteri in presunti attacchi di typosquatting di domini

MINACCE BASATE SUL WEB: CONSOLIDAMENTO E SOCIAL ENGINEERING

Statistiche: il traffico di kit di exploit osservato è sceso del 31% rispetto al terzo trimestre.

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

Il già ridotto traffico di kit di exploit, che era rimasto stabile per diversi trimestri a circa il 10% del picco del 2016, è ulteriormente diminuito nel quarto trimestre. Il **KE RIG** ha rappresentato quasi il 98% del traffico di kit di exploit osservato nel quarto trimestre 2017. Ma la sua quota di traffico complessivo è diminuita alla fine del trimestre a fronte di una recente ondata del KE Magnitude (figura 6).

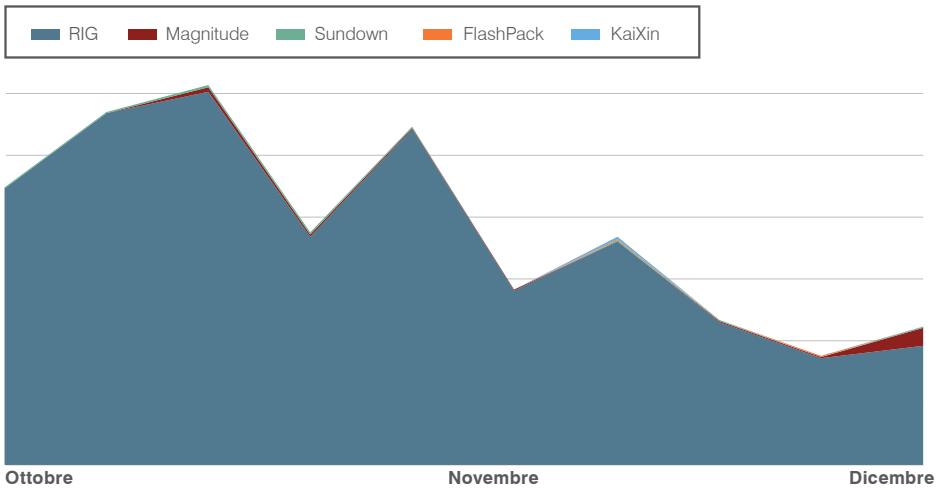


Figura 6: traffico principali kit di exploit come percentuale del totale, ottobre-dicembre 2017

BAD RABBIT
Il ceppo ransomware ha fatto la sua prima apparizione in ottobre, prendendo di mira la popolazione in Russia e Ucraina. È simile al ceppo ransomware NotPetya. Si presenta come un aggiornamento Adobe Flash e infetta i sistemi attraverso download "drive-by" ma richiede alla vittima di avviare l'aggiornamento fasullo.

Ma la grande novità è stata la scoperta di una sofisticata campagna di malvertising di grandi proporzioni rivolta agli utenti di un famoso sito di video per adulti. Invece di sfruttare difetti tecnici nel browser web degli utenti, gli attacchi hanno indotto le persone a installare il malware loro stessi. Gli aggressori hanno utilizzato filtri sofisticati per colpire in base a posizione e provider di servizi internet. Agli utenti designati veniva presentata una pagina Web che chiedeva loro di scaricare un aggiornamento per il loro browser o Adobe Flash. Invece, ricevevano il malware per frodi pubblicitarie Kovter, una tecnica osservata nell'epidemia di ransomware **BAD RABBIT** in ottobre.

Gli aggressori affrontano la mancanza di exploit di browser Web e le limitazioni generali degli exploit come tecnica di infezione. Come previsto con i primi esempi alla fine del 2016, si sono rivolti ad approcci basati sulle tecniche di social engineering simili a quelli usati negli attacchi via email, spesso con grande effetto.

IL MALWARE CHE ATTACCA IL PUNTO VENDITA HA I SUOI ALTI E BASSI

Nel 2016, abbiamo osservato quadruplicarsi il traffico associato a specifici ceppi di malware per i punti vendita (POS) specifici durante il fine settimana del Black Friday. Nel 2017, i picchi sono stati meno elevati. Un insieme dei più importanti ceppi di malware POS è risultato attivo in vari momenti nel corso nell'anno, non soltanto durante il Black Friday (vedere la figura 7).

Per esempio, FindPOS era attivo a marzo, si è placato durante l'estate, ed ha ripreso l'attività verso la fine di ottobre. È successo praticamente nello stesso periodo in cui MagikPOS ha rallentato l'attività, suggerendo che un singolo attore aveva adottato strumenti diversi. D'altro canto, il traffico di NewPosThings, a parte un picco nel mese di giugno, è rimasto basso e costante per gran parte dell'anno.

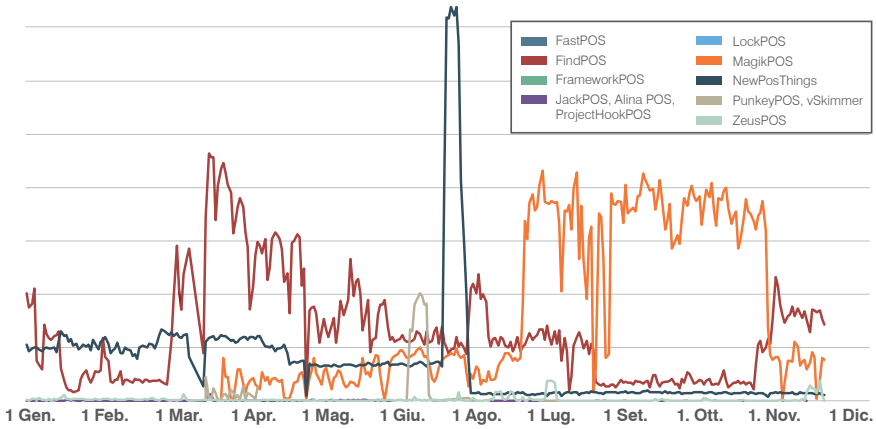


Figura 7: traffico malware POS (Point of Sale), gennaio-novembre 2017

I punti salienti? Possiamo ipotizzare che implementazioni complesse della tecnologia chip e PIN stiano indebolendo il malware che prende di mira i POS, riducendo il potenziale successo di campagne stagionali che portano a picchi nel traffico. Ma è necessario studiare ulteriormente le tendenze cicliche del malware POS per stabilire come, o se, i protagonisti del panorama delle minacce adotteranno tutti varianti nuove ed esistenti.

LE MINACCE NEI SOCIAL MEDIA AUMENTANO NEL 2018

Statistiche: gli account di assistenza clienti fraudolenti nei social media sono aumentati del 30% rispetto al trimestre precedente e all'anno nel suo complesso.

Nello scorso trimestre le minacce nei social media sono aumentate. Il numero di account di assistenza clienti fasulli è aumentato del 30% rispetto all'anno precedente e allo stesso periodo nel 2016.

Dopo essere rimasti invariati per la maggior parte del 2017, anche i link di phishing nei social media hanno mostrato una forte crescita nel quarto trimestre, aumentando di quasi il 70% rispetto al terzo trimestre (figura 8).

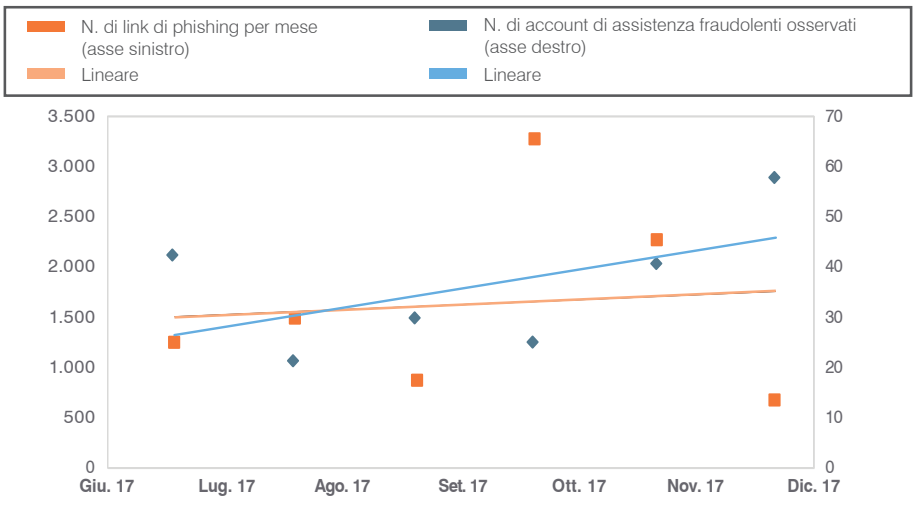


Figura 8: attività mensile relativa nella distribuzione di link di phishing tramite social media rispetto ad account di assistenza fraudolenti

RACCOMANDAZIONI

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 l'azienda e il brand nei mesi a venire.

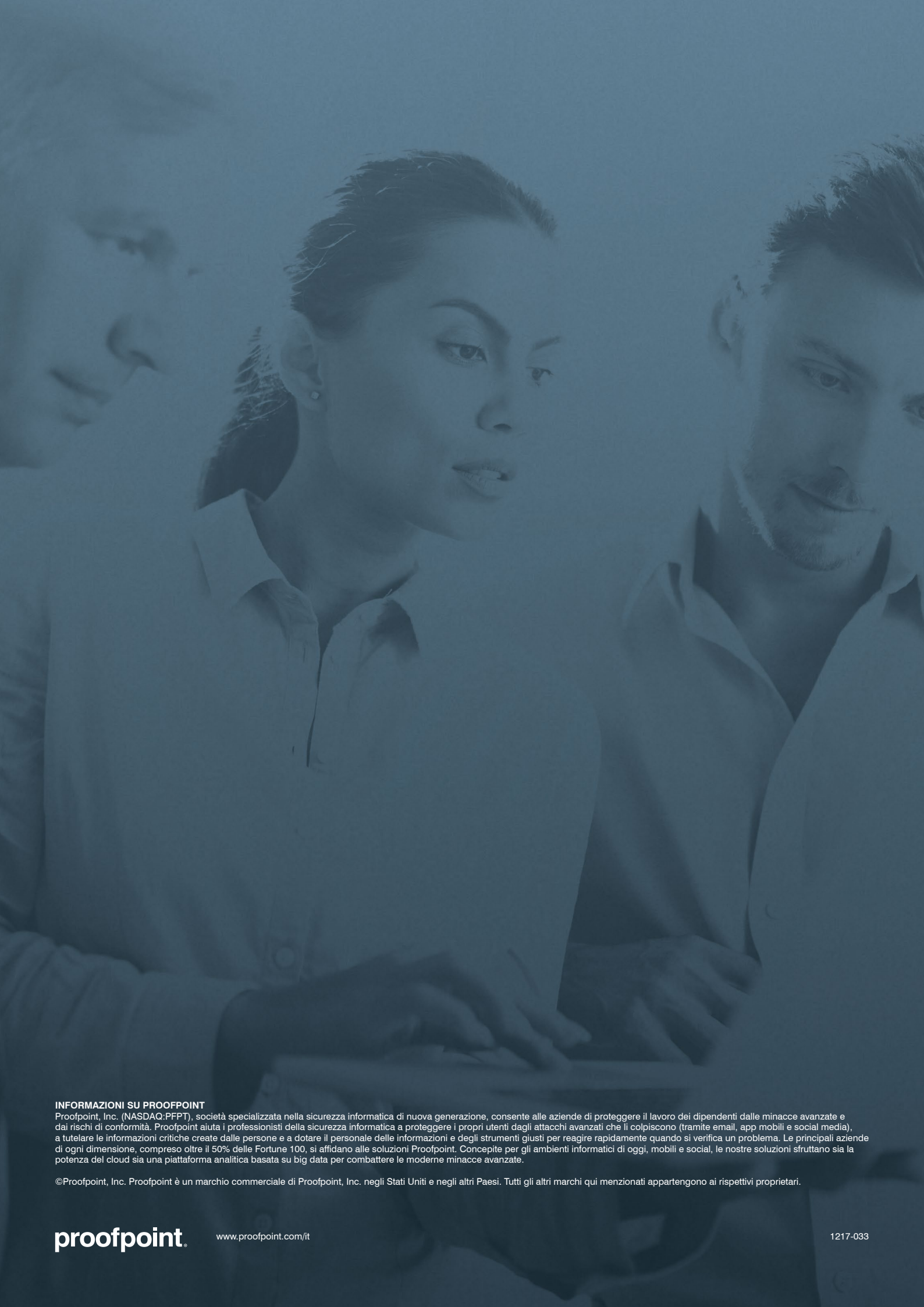
Presupporre che gli utenti facciano clic. Il social engineering è sempre più il modo più popolare per lanciare attacchi email e i criminali continuano a trovare nuovi modi per sfruttare la componente umana. Sfruttare una soluzione che identifica e mette in quarantena le minacce email in entrata che prendono di mira i dipendenti e le minacce in uscita verso i clienti prima che raggiungano la casella di posta in arrivo.

Costruire robuste difese per proteggersi dalle frodi via email. Truffe tramite email fraudolente estremamente mirate ma di basso volume, spesso non hanno alcun payload e sono perciò difficili da rilevare. Investire in una soluzione con funzionalità di classificazione dinamiche che possono essere utilizzate per creare policy di quarantena e di blocco.

Proteggere reputazione e clienti. Combattere gli attacchi rivolti che prendono di mira i clienti su social media, email e dispositivi mobili, in particolare gli account fraudolenti che si agganciano al marchio. Cercare una soluzione completa per la sicurezza dei social media che analizzi tutti i social network e segnali attività fraudolente.

Associarsi a un fornitore di intelligence sulle minacce. Attacchi più contenuti e mirati richiedono informazioni sofisticate sulle minacce. Sfruttare una soluzione che combini tecniche statiche e dinamiche per rilevare nuovi strumenti, tattiche e obiettivi di attacco, oltre a un panorama in continua evoluzione, e quindi apprendere da essi.

Per le più recenti ricerche e indicazioni sulle minacce avanzate odierne e sui rischi digitali, visitare **proofpoint.com/it/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/it

1217-033