proofpoint®

PROTEGGERE LE PERSONE

ESTATE 2018

ANALISI TRIMESTRALE SUGLI ATTACCHI ALTAMENTE MIRATI

proofpoint.com/it

LA MAGGIOR PARTE DEI REPORT SULLA SICUREZZA INFORMATICA DEDICA AMPIO SPAZIO ALLE MINACCE E AI MECCANISMI CHE QUESTE METTONO IN ATTO. QUESTO STUDIO SI OCCUPA DELLE PERSONE E DI COME VENGONO COLPITE.

Il vero obiettivo degli attacchi infatti oggi sono le persone e non la tecnologia. Raggirano i tuoi collaboratori inducendoli ad aprire un allegato non sicuro o ad aprire un link sospetto sul web. Si spacciano per il tuo amministratore delegato e ordinano all'ufficio contabilità di effettuare un bonifico. E poi convincono i tuoi clienti a condividere le loro credenziali di accesso con un sito web o un loro account di un social media pensando che sia il tuo.

Per quanto la gestione della tua infrastruttura IT possa essere efficace, non c'è modo di evitare questi attacchi rivolti alla persona. Ad essere vulnerabile è la natura umana stessa.

Per difendersi dalle minacce attuali occorre capire chi sono le loro potenziali vittime. In questa analisi unica nel suo genere abbiamo studiato quali sono i dipendenti e i reparti aziendali più esposti alle minacce via email altamente mirate. Successivamente abbiamo esaminato le modalità con cui avviene l'attacco, analizzando le tecniche e gli strumenti adottati dai criminali informatici.

Nel report sono raccolti i dati relativi al periodo aprile-giugno 2018, insieme a dati raccolti in precedenza per consentire un confronto storico. In base ai risultati ottenuti, suggeriamo alle aziende le misure concrete che possono adottare per creare una difesa incentrata sulle persone.

Nota: i dati sono stati raccolti da una serie di clienti in un determinato trimestre. In alcuni casi, i confronti storici possono avvenire tra dati di gruppi di clienti sovrapposti, ma non identici.

CHI SONO LE VITTIME DEGLI ATTACCHI

Singoli collaboratori e dirigenti di grado inferiore costituiscono circa il

60%

DEI SOGGETTI COLPITI DA ATTACCHI ALTAMENTE MIRATI.*

Ma direttori e dirigenti di grado superiore, che rappresentano una minoranza rispetto alla forza lavoro complessiva, sono stati vittime di una quota sproporzionatamente elevata di attacchi

**malware e phishing delle credenziali*

Coloro che ricoprono incarichi in ambito operation e produzione sono i più esposti e

RAPPRESENTANO IL

23% DEI SOGGETTI COLPITI DA ATTACCHI ALTAMENTE MIRATI.*

**malware e phishing delle credenziali*

Complessivamente, il numero di attacchi fraudolenti via email per azienda vittima della frode

È CRESCIUTO DEL **25%**

rispetto al trimestre precedente (con una media del 35%) e

DELL'85% RISPETTO ALLO STESSO TRIMESTRE DELL'ANNO PRECEDENTE.

LA MAGGIOR PARTE DELLE AZIENDE È STATA COLPITA ALMENO UNA VOLTA.

TECNICHE DI ATTACCO UTILIZZATE

Il volume delle email dannose

È AUMENTATO DEL **36%**

rispetto al trimestre precedente

È STATA REGISTRATA UNA GAMMA PIÙ AMPIA DI PAYLOAD DI POSTA ELETTRONICA E DI CRIMINALI INFORMATICI RISPETTO ALLO STESSO TRIMESTRE DELL'ANNO PRECEDENTE.

Si è registrata una ripresa del ransomware, che ha raggiunto

QUASI L' **11%**

DEL VOLUME TOTALE DELLE EMAIL DANNOSE.

I collegamenti di phishing inviati tramite i social media

SONO BALZATI AL **30%**

La tendenza ha segnato un'inversione dopo mesi di declino dovuta al fatto che i criminali informatici hanno trovato o il modo di aggirare gli strumenti automatici di difesa.

La truffa dei falsi centri di supporto clienti

HA AVUTO UN'IMPENNATA DEL **39%**

rispetto al trimestre precedente e

HA RAGGIUNTO IL PICCO DEL **400%** RISPETTO ALLO STESSO TRIMESTRE DELL'ANNO PRECEDENTE.

SEZIONE 1: CHI SONO LE VITTIME DEGLI ATTACCHI

Per proteggere le persone occorre innanzitutto sapere chi sono le vittime degli attacchi all'interno di un'azienda e perché possono finire nel mirino dei malintenzionati. È necessario sapere che ruolo rivestono, a quali dati hanno accesso e la loro potenziale esposizione.

I DESTINATARI DI MALWARE E PHISHING ALTAMENTE MIRATI

METODOLOGIA

Per capire meglio le minacce rivolte a persone specifiche, abbiamo preso in esame gli attacchi più mirati contro i clienti Fortune Global 500. Abbiamo raccolto gli indirizzi email più colpiti (assegnando un punteggio basato sulla quantità, la gravità e la complessità delle minacce ricevute) di ogni azienda. Abbiamo quindi confrontato titolo e funzione dei destinatari. Per confrontare le email con le mansioni lavorative abbiamo utilizzato i profili dei social media, i database Internet, notizie e altre fonti.

Le vittime degli attacchi appartengono a qualsiasi livello di carriera. L'analisi per gruppi evidenzia che i singoli collaboratori e i dirigenti di grado inferiore costituiscono circa il 60% delle vittime di attacchi di malware e phishing delle credenziali altamente mirati. Ma se si considera che i dirigenti di alto livello rappresentano una percentuale inferiore della forza lavoro totale, i dati mostrano che i membri del consiglio di amministrazione, gli amministratori delegati, i direttori e i capi di dipartimento vengono colpiti con una frequenza sproporzionatamente più elevata.

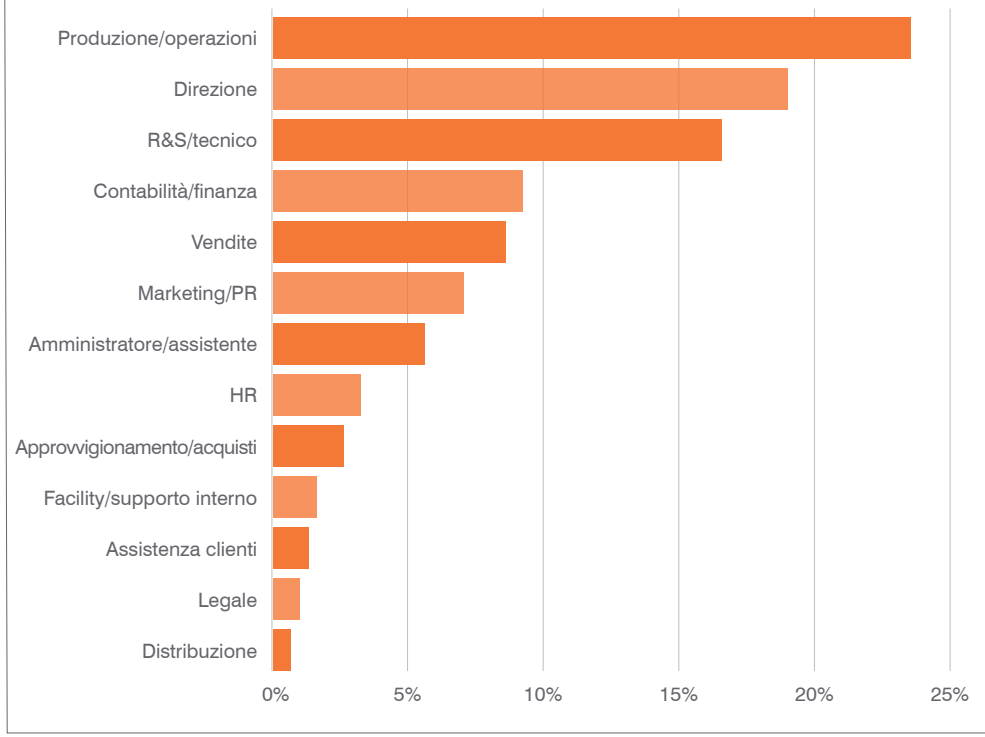
Chi ricopre incarichi in ambito operation e produzione, lo zoccolo duro della forza lavoro di un'azienda tipica, è più esposto, con il 23% degli attacchi altamente mirati. I dirigenti costituiscono la seconda mansione più esposta, seguita a breve distanza dai reparti R&S e tecnico.

I dipendenti più colpiti

A livello di gruppi, i dipendenti di livello inferiore costituiscono circa il 60% delle vittime di attacchi altamente mirati. Ma gli amministratori delegati, i direttori e i capi di dipartimento possono essere colpiti con una frequenza sproporzionatamente più elevata

I dipartimenti più colpiti

I dipendenti coinvolti nelle operazioni principali delle società sono i più colpiti, seguiti a breve distanza dai dipendenti dei reparti amministrativo e tecnico.



SETTORI COLPITI DALLE FRODI VIA EMAIL

Complessivamente, il numero di attacchi fraudolenti via email è salito del 25% dal trimestre precedente (fino a una media di 35) e dell'85% rispetto allo stesso trimestre dell'anno precedente. La maggior parte delle aziende è stata colpita almeno una volta.

Per sua natura, la frode via email colpisce aziende e destinatari specifici. Funziona fingendosi qualcuno che il destinatario conosce e di cui si fida. L'autore dell'attacco può chiedere di eseguire un bonifico o di fornire informazioni sensibili. In ogni caso, l'ordine sembra una normale richiesta di natura aziendale.

In alcuni settori, l'aumento rispetto all'anno precedente è stato a tre cifre. Il numero medio di attacchi fraudolenti via email nei confronti delle aziende del settore automotive è aumentato più del 400%. Gli attacchi in ambito istruzione sono saliti del 250%.

Non abbiamo individuato alcuna correlazione tra le dimensioni di un'azienda e la probabilità di subire un attacco fraudolento via email: i truffatori offrono a tutti pari opportunità.

ATTACCHI PER SETTORE

Gli attacchi via email colpiscono aziende di tutti i settori, con una prevalenza di attacchi nel secondo trimestre rispetto agli altri tre.

Per il secondo trimestre consecutivo, le società immobiliari sono state le più colpite, con una media di 67 email fraudolente inviate (questa tendenza può riflettere il tentativo dei criminali informatici di inserirsi in transazioni di alto valore per le quali il fattore tempo è determinante).

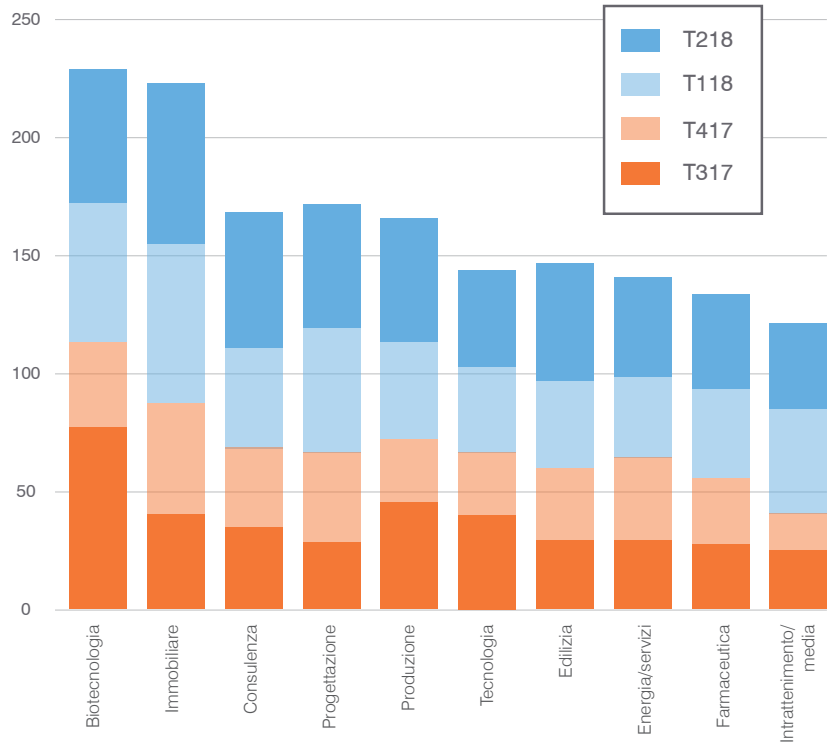
Se si sommano gli attacchi degli ultimi quattro trimestri, le aziende dell'industria biotecnologica e dei dispositivi medicali risultano più colpite come gruppo con una media di 228 attacchi.

METODOLOGIA

Abbiamo riunito i tentativi di frode via email rilevati dal nostro motore di classificazione delle email che protegge clienti in tutto il mondo. Abbiamo messo in relazione questi attacchi con le dimensioni delle aziende e la categoria di settore per stabilire quali tipi di aziende sono più colpiti. Abbiamo anche esaminato le email per analizzare le tecniche utilizzate dagli autori degli attacchi.

Attacchi per settore

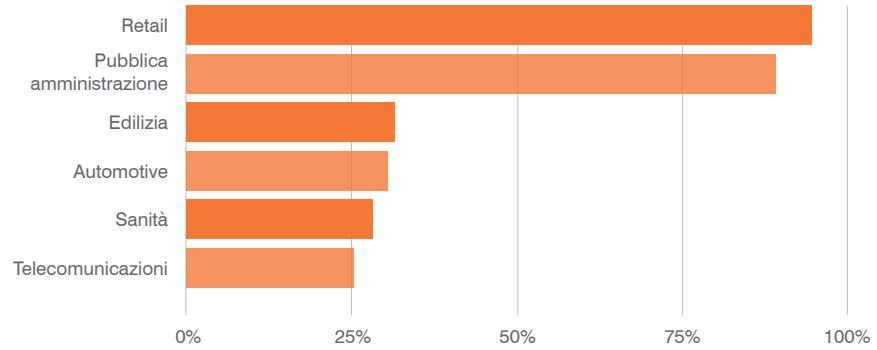
Le aziende dell'industria biotecnologica, dei dispositivi medicali e del settore immobiliare sono vittime di frodi via email più di altri settori.



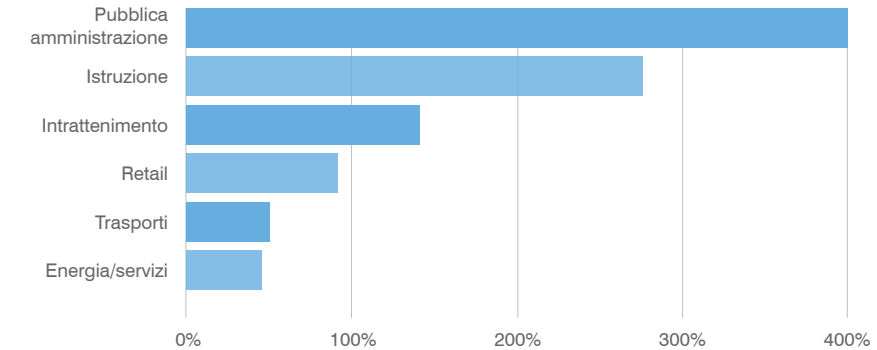
I TRUFFATORI INTENSIFICANO GLI ATTACCHI CONTRO I SETTORI RETAIL, PUBBLICO E DEI MEDIA

Il settore retail e gli enti governativi hanno visto un'enorme crescita, trimestre dopo trimestre, dei tentativi di frode via email, con un aumento degli attacchi per azienda rispettivamente del 91% e dell'84%. Considerati su base annua, gli incrementi sono ancora più impressionanti. Gli attacchi nei confronti di agenzie governative sono più che quintuplicati; le aziende del settore istruzione, intrattenimento e dei media hanno subito aumenti a tre cifre.

Aumento rispetto al trimestre precedente



Aumento rispetto allo stesso trimestre dell'anno precedente

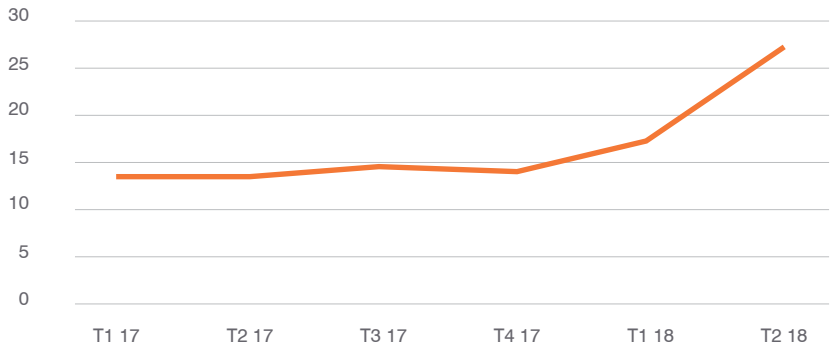


LE PERSONE COLPITE

Oltre il 65% delle aziende colpite da frodi via email ha subito il furto dell'identità di più di cinque dipendenti. Si tratta di oltre il triplo rispetto allo stesso trimestre dell'anno precedente, a dimostrazione che i truffatori stanno diventando più creativi nello scoprire nuovi modi per colpire. Una volta in possesso dei dati dei dipendenti, possono trovare molti modi per insinuarsi nell'ambiente aziendale.

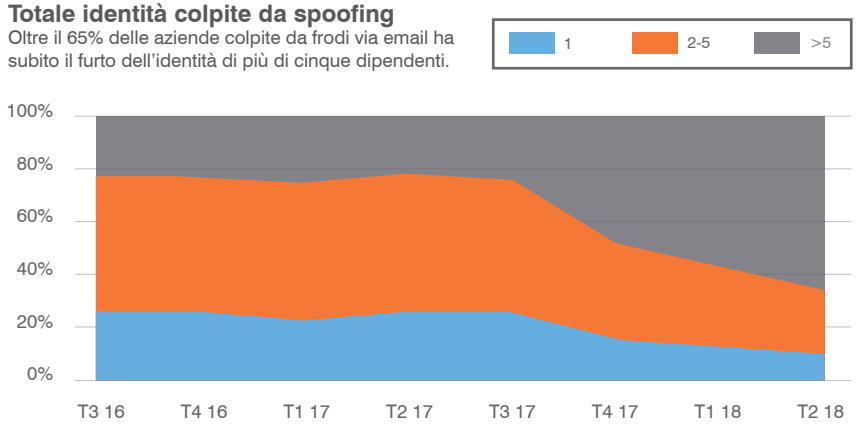
Numero medio di persone colpite (media)

L'azienda media ha registrato 28 persone colpite, 17 in più rispetto al trimestre precedente



Totale identità colpite da spoofing

Oltre il 65% delle aziende colpite da frodi via email ha subito il furto dell'identità di più di cinque dipendenti.



LE AZIENDE STATUNITENSI SONO I PRINCIPALI OBIETTIVI DELLE FRODI DEI DOMINI

La frode di un dominio comporta la registrazione di un dominio Internet che assomiglia vagamente a quello di aziende o brand di solida reputazione. Gli autori degli attacchi utilizzano questi domini fotocopia per effettuare frodi via email, il phishing delle credenziali, contraffazioni e altro. Un dominio email fotocopia, ad esempio, può indurre i destinatari a fidarsi di un truffatore che cerca di rubare denaro o dati sensibili. Un dominio web fotocopia inoltre può sembrare uguale all'originale inducendo gli utenti a inserire le proprie credenziali di accesso.

Quasi un terzo (23%) dei domini sospetti che imitano i principali brand statunitensi presentano record MX attivi che consentono l'invio di email fraudolenti a clienti e dipendenti ignari.

I consumatori e le imprese di lingua inglese sono gli obiettivi principali degli attacchi che utilizzano domini Web e di posta elettronica fotocopia.

METODOLOGIA

Per capire meglio le modalità con cui i criminali informatici si agganciano a brand digitali fidati, abbiamo utilizzato il nostro strumento di monitoraggio e protezione dei domini per analizzare oltre 350 milioni di registrazioni effettuate all'interno del database globale WHOIS. Abbiamo cercato tutti i nuovi domini sospetti simili a quelli dei primi 10 brand globali. Abbiamo inoltre verificato quanti di questi domini avevano record MX (di scambio di posta) attivi.

SEZIONE 2: TECNICHE DI ATTACCO UTILIZZATE

Per proteggere le persone è necessario sapere come vengono attaccate, il volume degli attacchi, chi sono gli autori degli attacchi e quali tecniche e strumenti utilizzano.

METODOLOGIA

I nostri dati in tempo reale coprono email, social media e applicazioni cloud mettendo in correlazione informazioni globali sulle minacce provenienti da oltre 5 miliardi di email al giorno, 200 milioni di account sui social media e 250.000 campioni di malware al giorno. Tutto questo ci permette di capire come vengono attaccate le persone per offrire loro un livello di protezione più elevato.

GLI ATTACCHI EMAIL SONO IN AUMENTO

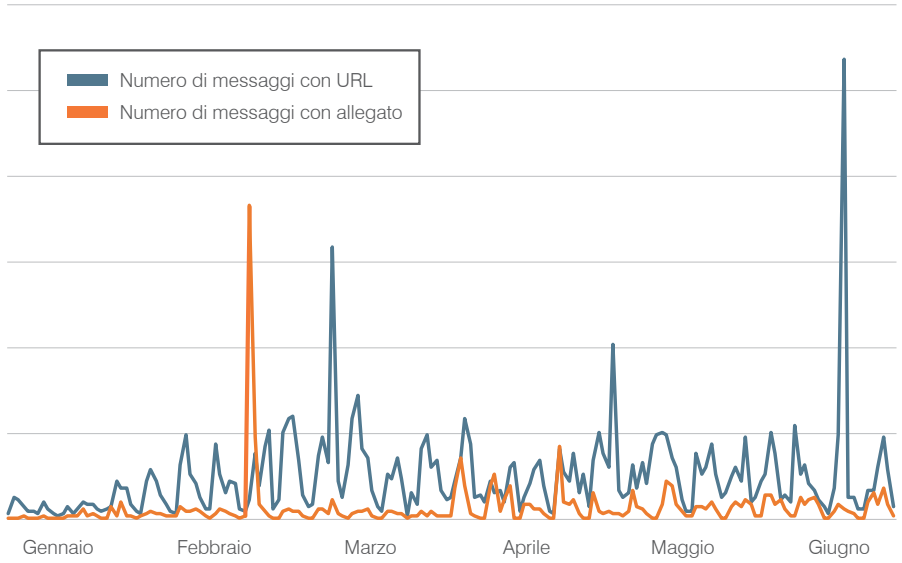
Il volume delle email malevole è cresciuto del 36% rispetto al trimestre precedente, sostenuto da una nutrita serie di payload di posta elettronica e di criminali informatici. Questa diversa combinazione di minacce rappresenta una svolta rispetto al trimestre dello scorso anno, caratterizzato da un numero minore di campagne, sebbene di maggiore portata.

Fatta eccezione per un picco molto elevato di attacchi che facevano uso di allegati malevoli registrato in febbraio, la maggior parte degli attacchi ha utilizzato URL dannosi.

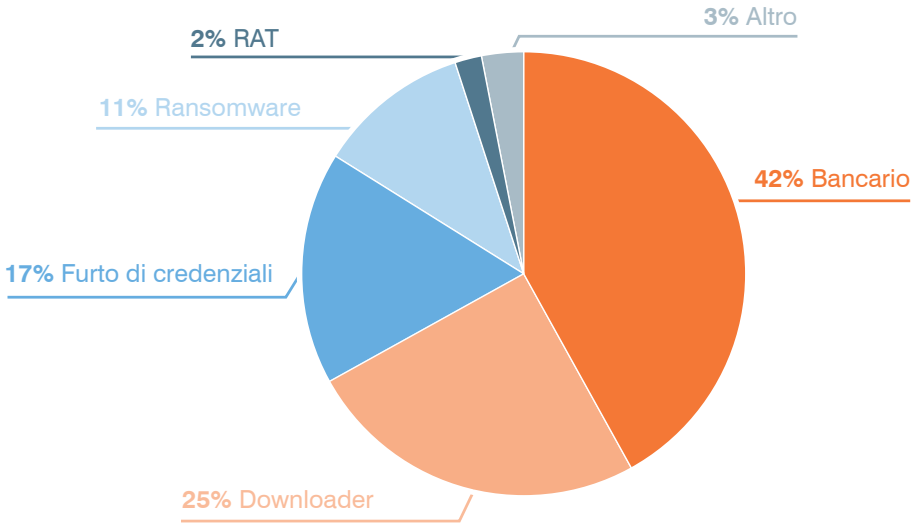
IL RITORNO DEL RANSOMWARE

Si è registrata una ripresa del ransomware, che ha raggiunto quasi l'11% del volume totale delle email dannose. Questo tipo di malware, che blocca i dati critici della vittima, costretta a pagare un riscatto per sbloccarli, aveva subito un forte declino nei trimestri precedenti, dopo aver dominato per gran parte del 2017.

Volume dei messaggi quotidiani indicizzato per tipo di attacco
Tendenza indicizzata dei tipi di attacchi quotidiani



Malware per categoria
Mix relativo di payload malware nelle email per categoria



TECNICHE DELLE FRODI VIA EMAIL

Chi utilizza la posta elettronica per compiere una frode utilizza varie tecniche per indurre i destinatari ad aprire l'email e compiere l'azione richiesta. Ad esempio tramite la riga dell'oggetto, eseguendo lo spoofing di mittenti fidati e scegliendo con cura le vittime.

LA RIGA DELL'OGGETTO

Abbiamo assistito a un'ondata di attacchi in cui il criminale informatico citava a un file o a un documento. Se questa ondata sia un fenomeno temporaneo o l'inizio di un trend non è ancora chiaro.

A parte questo variazione, la riga dell'oggetto ha mantenuto all'incirca la stessa posizione dei trimestri precedenti. Le truffe con la parola "pagamento" o "richiesta" nella riga dell'oggetto rimangono le più comuni.

SPOOFING DEL DOMINIO E DEL NOME VISUALIZZATO

Quasi due terzi delle aziende vittime di attacchi hanno subito abusi riguardanti i loro domini. In alcuni casi i truffatori hanno perpetrato attacchi che utilizzavano l'identità falsificata del datore di lavoro stesso del destinatario.

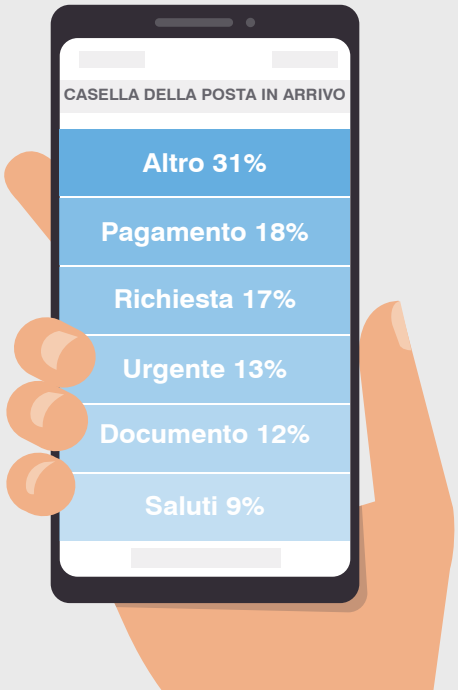
Indipendentemente dalle altre tattiche utilizzate, la maggior parte degli hacker effettua lo spoofing del nome visualizzato del mittente in email fraudolente.

Il nome visualizzato è quello che appare nel campo "Da:" quando si legge il messaggio. Non è legato all'indirizzo email reale del mittente o all'indirizzo a cui viene inviata l'eventuale risposta. Può essere qualsiasi cosa. Nello spoofing del nome visualizzato, il criminale informatico si serve di un nome e di un indirizzo email familiare per ottenere la fiducia del destinatario.

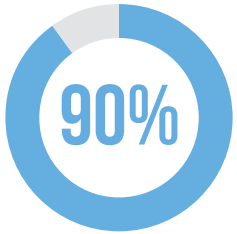
Allo stesso tempo, sembra calare lo spoofing dei domini grazie all'adozione, da parte di un numero sempre maggiore di aziende, di tecnologie di autenticazione dei messaggi di posta elettronica, quali DMARC (Domain-based Message Authentication, Reporting and Conformance).

Il nome visualizzato è l'identificativo di un messaggio di posta elettronica più facile da falsificare e il più visibile per i destinatari. Si comprende così perché la maggior parte dei tentativi di frode via email ricorra allo spoofing del nome visualizzato, anche se non viene effettuato lo spoofing del dominio di posta elettronica.

Oggetto nelle frodi via email
Le truffe con la parola "pagamento" o "richiesta" nella riga dell'oggetto rimangono le più comuni



Spoofing del nome visualizzato



La maggior parte degli attacchi utilizza una forma di spoofing del nome visualizzato

Lo spoofing del dominio di posta elettronica

È SCESO AL **18%**

DI TUTTI GLI ATTACCHI FRAUDOLENTI VIA EMAIL A SEGUITO DELL'ADOZIONE DI DMARC DA PARTE DI MOLTE ORGANIZZAZIONI

ATTACCHI TRAMITE I SOCIAL MEDIA

Sui social media si è registrata un'impennata delle frodi dei falsi account di assistenza clienti, anche note come "angler phishing". Nell'angler phishing, l'hacker crea un un account su un social media che imita gli account dell'assistenza clienti di noti brand. Quando un cliente chiede aiuto su un social media, il criminale informatico si inserisce prontamente utilizzando il falso account del centro di assistenza clienti, spesso prima che quello vero abbia persino il tempo di rispondere. Con la scusa di offrire aiuto, l'autore dell'attacco invia il cliente su un falso sito di login per rubare le sue credenziali oppure gli chiede direttamente di fornire le credenziali.

METODOLOGIA

Utilizzando la nostra soluzione di protezione dalle frodi social, abbiamo esaminato gli account che hanno utilizzato il nome della nostra base clienti globale, o un nome simile, e gli URL di phishing che hanno diffuso nella prima metà del 2018.

Il numero di falsi account di assistenza che minacciano la nostra base clienti globale è aumentato del 37% rispetto al trimestre precedente. Contemporaneamente è aumentato del 30% il numero di URL di phishing inviato tramite questi account.

Account di angler phishing

T1 2018	T2 2018
363	499

La frode dei falsi account di assistenza, anche nota come angler phishing ha registrato un forte incremento.

URL malevoli

T1 2018	T2 2018
364	472

SEZIONE 3: COME GARANTIRE PROTEZIONE

Le minacce incentrate sulle persone richiedono un approccio incentrato sulle persone per poter essere debellate. Il nostro suggerimento è di partire dalle seguenti considerazioni:

ASSUMERE UN ATTEGGIAMENTO INCENTRATO SULLE PERSONE NEI CONFRONTI DELLA SICUREZZA.

I criminali informatici non hanno una visione del mondo come se fosse un diagramma a rete. Adottare una soluzione che dia visibilità sulle vittime degli attacchi, su come vengono attaccate e che registri se l'attacco è andato a segno. Considerare il rischio individuale rappresentato da ogni utente, includendo il modo in cui sono stati scelti, i dati a cui hanno accesso e se tendono ad essere facili bersagli degli attacchi.

INSEGNARE AGLI UTENTI A INDIVIDUARE E SEGNALARE LE EMAIL MALEVOLE.

Una formazione stabile e attacchi simulati possono costituire una barriera contro molti attacchi e aiutare a identificare i soggetti che sono particolarmente vulnerabili. Le simulazioni migliori sono quelle che imitano le tecniche di attacco del mondo reale. Cercare soluzioni che siano saldamente collegate e abbiano accesso ai trend correnti e all'intelligence sulle minacce più aggiornata.

CONTEMPORANEAMENTE, CONSIDERARE CHE QUALCHE UTENTE FINIRÀ PER FARE CLIC SU UNA MINACCIA.

I criminali troveranno sempre nuovi modi per sfruttare i punti deboli della natura umana. Cercare una soluzione che individui e blocchi le minacce email in entrata che prendono di mira i dipendenti prima che raggiungano la casella della posta in arrivo e fermare le minacce esterne che fanno uso del vostro dominio per colpire i clienti.

CREARE UNA SOLIDA DIFESA DALLE FRODI VIA EMAIL

Le frodi via email possono essere difficili da rilevare con gli strumenti di sicurezza convenzionali. Investire in una soluzione in grado di gestire le email in base a policy di quarantena e di blocco personalizzate.

PROTEGGERE LA REPUTAZIONE E I CLIENTI DEL BRAND NEI CANALI DI CUI NON SI È PROPRIETARI.

Combattere gli attacchi che prendono di mira i vostri clienti sui social media, tramite email e sul web, soprattutto i falsi account che si agganciano al vostro brand. Cercare una soluzione per i social media completa, in grado di scansionare tutti i social network e segnalare le attività fraudolente.

COLLABORARE CON UN FORNITORE ESPERTO IN INTELLIGENCE SULLE MINACCE.

Gli attacchi più circoscritti e mirati necessitano di un'intelligence sulle minacce avanzata. Affidarsi a una soluzione che combini tecniche statiche e dinamiche per rilevare nuovi strumenti, tattiche e obiettivi di attacco e fate tesoro di tali informazioni.

ULTERIORI INFORMAZIONI

Per ricevere ulteriori informazioni su come si traduce nella pratica un approccio incentrato sulle persone, partecipa al nostro webinar.

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.