2020 Report sulle minacce nel settore assicurativo e dei servizi finanziari

INTRODUZIONE

La pandemia globale ha costretto molte compagnie assicurative e società di servizi finanziari ad accelerare la loro trasformazione digitale. Questo sforzo ha avuto molti risultati positivi: contatti quotidiani semplificati con i clienti a distanza, un'infrastruttura scalabile per agevolare l'espansione del perimetro e disposizioni per soddisfare le esigenze di comunicazione e conformità in rapida evoluzione. Benché tali cambiamenti abbiano aiutato banchieri, consulenti patrimoniali, operatori di borsa e agenti a capire i mercati e a gestire i flussi finanziari, offrono anche maggiori opportunità ai criminali informatici.

I criminali informatici sfruttano qualsiasi crisi sociale e il COVID-19 non fa eccezione. Dato che il settore assicurativo e dei servizi finanziari si espande oltre il perimetro della rete, i criminali informatici fanno altrettanto. Inoltre, le minacce non si limitano a spostarsi, ma assumono nuove forme e colpiscono nuovi obiettivi. Ogni tuo dipendente rappresenta un differente livello di sicurezza o rischio per la conformità a causa dei dati a cui ha accesso e al modo in cui utilizza la tecnologia per svolgere il suo lavoro.

Per aiutare i responsabili del settore assicurativo e dei servizi finanziari a comprendere meglio il mutevole panorama delle minacce informatiche, abbiamo analizzato i dati di un anno, concentrandoci sulla prima metà del 2020. Il team Proofpoint di ricerca sulle minacce informatiche ha studiato migliaia di minacce analizzando milioni di messaggi. Questo report presenta le nostre conclusioni, supportate da dati ed esempi reali per mettere in luce le minacce che colpiscono il settore assicurativo e dei servizi finanziari.

Pubblico e scopo

Il presente report è destinato ai dirigenti e ai responsabili della sicurezza delle compagnie assicurative e delle società di servizi finanziari. Si pone come obiettivo quello di aiutarle a ridurre i rischi per i dati personali, i dati finanziari, la proprietà intellettuale, le informazioni non di dominio pubblico, gli ecosistemi di terzi del settore assicurativo e dei servizi finanziari e i rischi di frode. Inoltre, è volto a sensibilizzare i dipendenti delle compagnie assicurative e delle società di servizi finanziari al fine di migliorare la sicurezza e la protezione dei dati.

Metodologia di ricerca

La ricerca ha preso in esame una combinazione di dati Proofpoint relativi a diversi criminali informatici, campagne di attacco, violazioni dell'email aziendale (Business Email Compromise, BEC) e VAP (Very Attacked People™ ovvero le persone più attaccate in azienda), nel quarto trimestre del 2019 e nella prima metà del 2020. In alcuni casi, abbiamo utilizzato informazioni di pubblico dominio per affrontare tematiche di sicurezza di nostro interesse ma che non sono rappresentate nei dati raccolti da Proofpoint.

Sommario

Sintesi

Il settore assicurativo e dei servizi finanziari è costantemente bersagliato da criminali informatici con i moventi più svariati: fiduciari, legati all'attivismo informatico o terroristici. Di seguito alcune delle principali conclusioni presenti nel report:

Le persone, non le tecnologie, sono il principale vettore d'attacco.

Secondo di dati di threat intelligence di Proofpoint, oltre il 96% di tutti gli attacchi inizia con il social engineering, il pretexting, il phishing e le minacce interne, mentre molte aziende spendono la maggior parte dei loro budget in soluzioni tecnologiche.

In base all'analisi degli indicatori di violazione e delle tattiche, tecniche e procedure svolta da Proofpoint, è possibile stilare l'elenco dei VAP al fine di personalizzare l'affidabilità della sicurezza in funzione di tali minacce mirate.

I criminali informatici si adattano rapidamente alle circostanze che cambiano.

Il Report 2020 sulle violazioni dei dati di Verizon evidenzia che l'anno scorso gli attacchi basati sul cloud sono raddoppiati, in linea con l'aumento dei telelavoratori.

I criminali informatici che prendono di mira il settore dei servizi finanziari adottano strategie sofisticate, sono estremamente metodici nell'uso delle tattiche e conoscono bene le loro vittime.

Oltre il secondo livello, le aziende hanno un controllo limitato sui rischi legati alla supply chain.

La supply chain dei servizi finanziari è economicamente più volatile che in qualsiasi altro settore, in quanto include borse, regolanti, stanze di compensazione e banche centrali con un raggio d'azione internazionale.

Bisogna essere consapevoli delle sfumature dei requisiti di sicurezza della supply chain. La riduzione dei requisiti interni della tua azienda per forzare la conformità alle misure di sicurezza specifiche per i fornitori di primo e secondo livello, può creare delle lacune di sicurezza per il fornitore coinvolto o impedire loro di servire adeguatamente la tua azienda.

Ciascun segmento del settore ha sfumature specifiche nel proprio panorama delle minacce.

I dati di threat intelligence di Proofpoint e di report indipendenti illustrano le variazioni negli indicatori di violazione e le tattiche, tecniche e procedure in ogni segmento del settore, in modo che le difese vengano adattate di conseguenza.

Le criptovalute sono in piena crescita.

L'Office of the Comptroller of the Currency (OCC) ha di recente rilasciato una dichiarazione che consente agli istituti bancari di conservare le chiavi digitali dei portafogli di criptovaluta.

Se le banche sono autorizzate a conservare a fini legali le risorse digitali per conto dei loro clienti, le responsabilità legali e i rischi per la sicurezza informatica legati alle criptovalute vengono trasferiti alle banche stesse.

Indicatori di sicurezza e minacce specifici del settore assicurativo e dei servizi finanziari

Il settore dei servizi finanziari presenta delle caratteristiche semi-uniche, che attirano i malintenzionati come api sul miele:

POSTA IN GIOCO ELEVATA

Il ritorno economico in caso di violazione di una società dei servizi finanziari è più alto che negli altri settori, proprio perché è qui che si concentra il denaro.

IMPATTO ELEVATO

Qualsiasi violazione, non importa se grande o piccola, può fare notizia e provocare la reazione dei mercati. I suoi effetti possono diffondersi ampiamente, dalle singole aziende fino alle economie globali.

REGOLAMENTAZIONI SPECIFICHE

Il rispetto di processi e procedure ben definiti dai regolamenti, semplifica le missioni di ricognizione sui bersagli specifici per i criminali informatici.

TECNOLOGIE DI VECCHIA GENERAZIONE

Intrinsecamente legati all'età dei sistemi informatici, i rischi per la sicurezza sono creati dalla cessazione del supporto da parte del produttore, dall'accumulo di sistemi proprietari con il susseguirsi di fusioni e acquisizioni, da sistemi ritenuti "troppo critici per essere aggiornati" o dalla perdita i competenze in merito.

INFRASTRUTTURA COMPLESSA

Il settore è stato sempre attivo per quanto riguarda le fusioni e acquisizioni, che introducono complessità e opacità. Integrazioni approssimative fra i sistemi più disparati creano infrastrutture frammentate che moltiplicano le vulnerabilità e aumentano la pressione sulle risorse di difesa e di monitoraggio della sicurezza.

LE TECNOLOGIE CLOUD/CONTENITORE

La migrazione delle applicazioni di vecchia generazione in cloud (o nei contenitori) può comportare l'esposizione di vulnerabilità precedentemente sconosciute o l'introduzione di nuove vulnerabilità, a causa del modello di implementazione. Il coinvolgimento di nuovi fornitori SaaS ai quali affidare i sistemi non critici può creare una nuova superficie d'attacco nella quale la capacità di gestire gli incidenti è fortemente limitata.

AUTOMAZIONE PERVASIVA

Le compagnie assicurative e le società di servizi finanziari ricorrono sempre di più all'automazione per ridurre i costi e modernizzare i sistemi di vecchia generazione. Tuttavia, la banalizzazione dell'automazione le lascia vulnerabili quando dipendono da sistemi obsoleti, introducono nuova logica aziendale oppure utilizzano metodi non documentati.

Il settore assicurativo e dei servizi finanziari presenta alcune statistiche peculiari in termini di prevenzione, minacce emergenti e attacchi persistenti:

Security awareness training

I dipendenti delle compagnie assicurative e delle società di servizi finanziari sono leggermente più consapevoli delle minacce interne e dei rischi di autenticazione degli account rispetto a quelli di altri settori.

- Nei servizi finanziari il tasso di insuccesso è del 20%, rispetto al 22% della media generale.
- Hanno ottenuto risultati migliori nelle categorie "Identificazione e prevenzione delle minacce interne" e "Autenticazione degli account".
- Hanno fatto registrati risultati peggiori solo nelle categorie "Protezione contro i rischi fisici" e "Prevenzione degli attacchi ransomware".

Minacce trasmesse via email

Le aziende hanno ricevuto URL pericolosi che allegati dannosi.

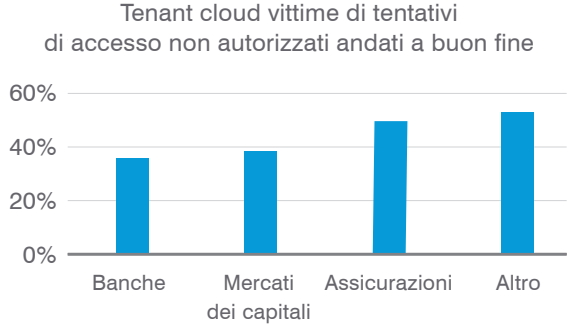
- Nel settore dei servizi finanziari l'82% dei messaggi dannosi ricevuti conteneva degli URL.
- Il 72% degli attacchi erano basati su malware.

Accesso al cloud

Le tattiche di social engineering volte a ottenere l'accesso al cloud hanno registrato un *tasso di successo* impressionante pari al 75%, mentre gli attacchi di forza bruta hanno avuto successo solo in circa il 9,7% dei casi. È chiaro che, per un criminale informatico, gli attacchi incentrati sulle persone offrono il ritorno sull'investimento più promettente.

Le compagnie assicurative subiscono più accessi non autorizzati rispetto a banche e mercati di capitali.

- Il 72% è stato colpito da attacchi di forza bruta, ma solo il 7% è stato compromesso tramite tale metodo.
- Il 28% è stato preso di mira da tecniche di social engineering. Il 21% è stato compromesso con il phishing.



Prevenzione della perdita di dati (DLP) e minacce interne

Ogni segmento del settore assicurativo e dei servizi finanziari ha il proprio rischio di minacce interne. Uno studio interno sugli incidenti condotto tra il 1996 e il 2018 ha indicato le banche come le più colpite[1].

Segmento	Gruppo/i	Rischio/i di minacce interne	Numero di incidenti interni[2]
Banche	Risparmio, credito, finanza	Dati personali, ladri di account	190
Mercati dei capitali	Banche di investimento, gestione patrimoniale	Proprietà intellettuale, fusioni e acquisizioni, insider trading	nessun dato disponibile
Assicurazioni	Intermediazione, beni immobiliari e infortuni	Dati personali, frodi assicurative	14
Ecosistema	Borse, regolanti, dati del mercato, cloud/SaaS, supply chain	Antiriciclaggio, controparti, SWIFT, stanze di compensazione automatizzate, manipolazione del mercato	33

Tattiche, tecniche e procedure usate negli attacchi di origine interna contro il settore dei servizi finanziari

Tra il 2005 e il 2012, il CERT, in collaborazione con il dipartimento americano per la Sicurezza interna e lo United State Secrect Service (USSS), ha studiato gli incidenti di origine interna verificatisi per rispondere alla seguente domanda: "Quali precursori tecnici e comportamentali delle frodi interne possono essere osservati nel settore finanziario e quali strategie di prevenzione dovrebbero essere di conseguenza prese in considerazione per affrontale?"[3] Fra i principali risultati di questa ricerca spiccano i seguenti:

Gli attacchi lenti e di basso profilo sono quelli che causano più danni e sfuggono al rilevamento più a lungo.

Le soluzioni tecnologiche basate sul rilevamento delle anomali non sono solo inefficaci, ma controproducenti, poiché le attività dannose a lungo termine entrano a far parte dell'attività quotidiana degli utenti.

I mezzi impiegati dai criminali informatici non erano tecnicamente sofisticati.

Questa mancanza di sofisticazione significa che i dati dei sensori esistenti possono essere inseriti in un programma di gestione delle minacce interne. Il segreto, ovviamente, risiede nell'analisi del comportamento.

Le frodi perpetrate dai dirigenti sono sostanzialmente diverse da quelle degli impiegati di livello inferiore, in termini di danno e durata.

I dirigenti hanno la capacità di cambiare i processi aziendali, a volte manipolando i dipendenti subordinati, a scopo di lucro. Tra i dipendenti di livello inferiore sono spesso rappresentanti del servizio clienti che alterano gli account oppure sottraggono le informazioni di identificazione personale dei clienti a loro vantaggio.

La maggior parte degli incidenti viene rilevata durante una verifica oppure in seguito al reclamo di un cliente o alla segnalazione di un collega.

Questo è un dato importante: mentre le violazioni esterne lasciano anomalie nel loro percorso, le minacce interne sono alimentate da sentimenti, motivazioni e stati d'animo degli utenti, fattori non facilmente rilevabili dalla tecnologia.

La volpe a guardia del pollaio

A volte è l'azienda in carico di rilevare e analizzare le minacce interne a caderne vittima. Nel 2019 un ex esaminatore della conformità dei titoli della SEC è stato denunciato per aver utilizzato delle informazioni, relative a un'indagine svolta nei confronti di una società di capitali privati, al fine di ottenere la posizione di Chief Compliance Officer nella stessa società[4]. Il fatto che la persona in questione occupasse - e gli fosse stato assegnato - un incarico relativo alla conformità non è solo ironico, ma dimostra che per le minacce interne non c'è alcuno scrupolo di moralità.

[1] Miller & Trotman (2018), *"Insider Threats in Finance and Insurance (Part 4 of 9: Insider Threats Across Industry Sectors)" (Le minacce interne nel settore finanziario e assicurativo - Parte 4 di 9 dell'analisi delle minacce interne per settore d'attività),* SEI dell'università Carnegie Mellon

[2] Ibid.

[3] Cummings, Lewellen, McIntire, Moore e Trzeciak (2012), "*Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector*" (Studio sulle minacce interne: attività informatica illecita che coinvolge la frode nel settore dei servizi finanziari degli Statti Uniti), SEI dell'università Carnegie Mellon, Direzione delle scienze e tecnologie del dipartimento americano della Sicurezza interna, USSS e Insider Threat Center del CERT

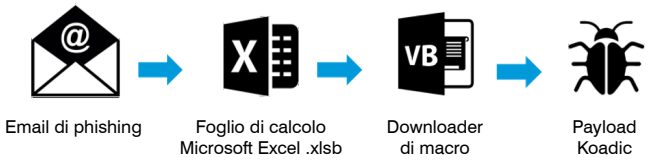
[4] Godoy e Lorenzo (2019), "Ex-SEC Compliance Expert Denies Pilfering Info For PE Firm" (Un ex della SEC esperto di conformità nega il furto di informazioni per un fondo di private equity), Law360

Tattiche comunemente utilizzate negli attacchi contro il settore assicurativo e dei servizi finanziari

I dati di threat intelligente di Proofpoint mostrano una crescita di alcune tattiche specificamente usate dai criminali informatici:

Manipolazione del codice VBA (VBA stomping)

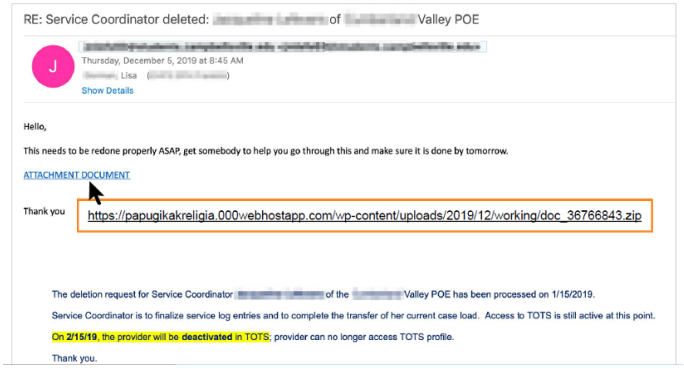
Questa tecnica basata su allegati dannosi presenta ai motori delle analisi di sicurezza un codice VBA (eseguibile) diverso da quello effettivamente eseguito, aggirando così molti strumenti di rilevamento basati sulle firme dei codici e sul rilevamento euristico.



Hijacking del thread di discussione

Questo tipo di attacco BEC fa molte vittime iniettando il contenuto di email false (come degli URL pericolosi) in un thread di discussione già esistente. Gli utenti generalmente si fidano di un thread esistente, per cui sono più propensi ad aprirlo e a fare clic sui link.

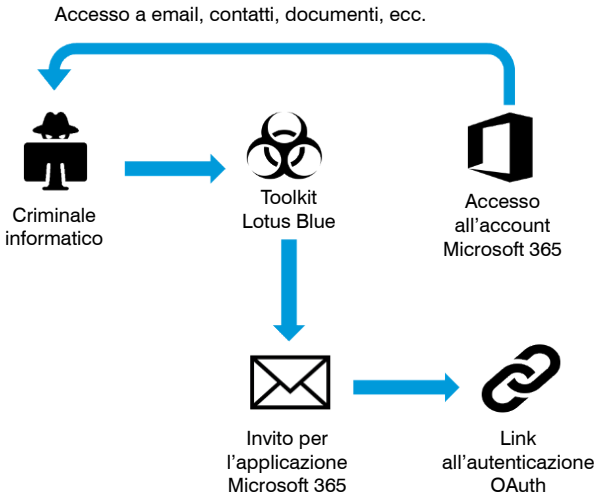
Un'altra tattica consiste nell'incorporare degli URL pericolosi nella sezione dell'email originale del messaggio, che di solito è esclusa dall'analisi di molti strumenti per la sicurezza dell'email. Anche in questo modo è possibile aggirare molti strumenti di rilevamento basati sull'euristica.



Nel caso di Emotet, il malware più prolifico degli ultimi due anni, i criminali informatici hanno effettivamente automatizzato il processo di creazione di modelli al fine di usare questa tecnica su larga scala. Tipicamente ciò implicherebbe un'analisi e una personalizzazione da parte dei criminali informatici stessi.

Autenticazione delle terze parti (3PA) usata con intento dannoso

Questa tecnica di assunzione del controllo di un account usa la tipica alterazione del DNS per indurre gli utenti a fornire i token di autorizzazione basati sul linguaggio SAML alle applicazioni cloud di un dipendente (per esempio, Microsoft 365, Google Workspace, etc.). Tipicamente tutto inizia con un attacco BEC, per poi trasformarsi rapidamente in una violazione degli account email (EAC, Email Account Compromise). Grazie all'accesso all'account email di un utente, diventa possibile effettuare il reset delle password per altre applicazioni, permettendo di assumere il controllo di tali account.



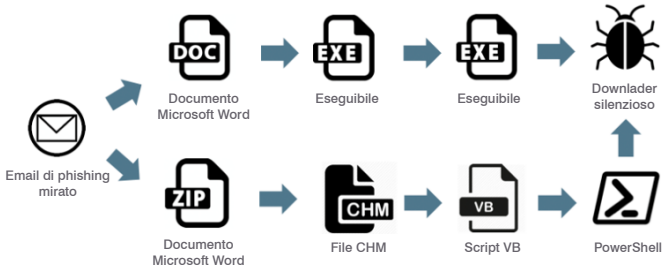
Il motivo per cui questo tipo di attacco è più pericoloso di altri è che una volta che un account è stato autorizzato, cambiare la password o applicare l'autenticazione a più fattori è inutile. L'unico modo per revocare l'accesso a un criminale informatico è quello di rimuovere esplicitamente i token di autorizzazione, una procedura di cui la maggior parte degli utenti è ignara.

Attacco multi-livello alle condivisioni dei file

Questa tecnica utilizza un documento ospitato che a sua volta contiene più livelli di URL che puntano a documenti ospitati su numerosi siti di condivisione di file diversi, che infine fanno capo a un payload infettato dal malware.

La crescente diffusione di condivisioni di file in cloud (e dell'autenticazione di terzi), nell'ambito dei servizi finanziari, ha fatto aumentare il ricorso a questa tecnica.

Per esempio, un payload (uno script VB che carica Ursnif, un trojan dei servizi bancari incorporato) è protetto da una password (cifrata) inclusa nel corpo di un'email.



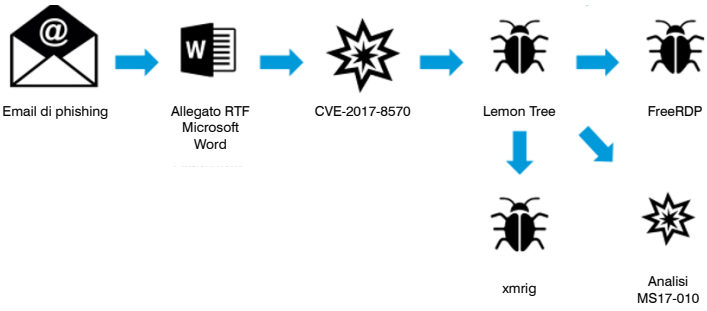
Da un lato, l'aggiunta di passaggi, come il costringere la vittima designata a immettere una password, sembra controintuitiva, perché più passaggi ci sono da seguire, più è alta la probabilità che qualcuno commetta un errore o rinunci prima di aver completato tutti i passaggi.

D'altro canto, ciò impedisce la semplice analisi dell'allegato. Le soluzioni hanno quindi dovuto utilizzare delle tecniche che comportano l'uso di un dizionario delle password usate più comunemente regolarmente aggiornato (gli autori desiderano mantenerle semplici per la ragione di cui sopra, senza cambiarle a ogni campagna) oppure l'analisi del corpo dei messaggi (che è difficile da compiere su vasta scala).

Abbiamo osservato dei casi in cui la password era in realtà un'immagine anziché un testo. In questo caso, quest'ultimo metodo di analisi delle password di testo risulta inefficace.

Attacchi che sfruttano le risorse locali (senza file/server)

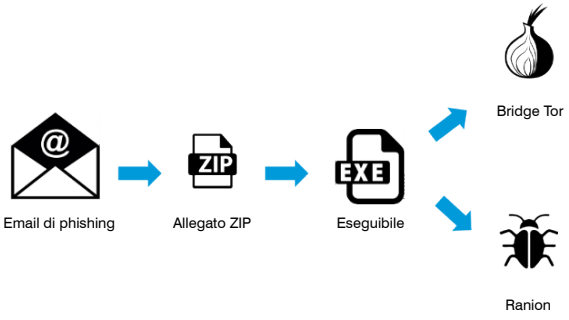
Questa tecnica di attacco usa le funzionalità esistenti nel sistema operativo del sistema operativo dell'obiettivo, come ad esempio PowerShell, per eseguire il proprio payload. Il payload stesso non è di tipo binario, pertanto può eludere i metodi di rilevamento basati sulle firme e sulle analisi euristiche.



Ransomware-as-a-Service (RaaS)

Le piattaforme di ransomware sono ormai disponibili diffusamente, analogamente a molte altre piattaforme di attacco.

I fornitori di piattaforme RaaS che prima prendevano una commissione sul riscatto, sono passati a un servizio su abbonamento. Ciò non solo rende il RaaS più attraente di altre piattaforme di attacco, ma i fornitori si assolvono anche dalla responsabilità diretta nei reati (immaginiamo i procedimenti che verrebbero intentati contro i fabbricanti di armi se questi esigessero una commissione per ogni proiettile sparato).



Le recenti iterazioni di questo servizio includono l'installazione automatica dei client di TOR sui computer delle vittime, rendendo più facile il pagamento del riscatto.

Approfondimenti sul settore dei servizi finanziari

Banche

Negli ultimi anni il settore bancario è stato quello più interessato da innovazioni e progressi: dall'avvento delle transazioni mobili ai servizi guidati dalle interfacce API (Application Programming Interface), fino all'uso dell'elaborazione basata sull'intelligenza artificiale. Con ogni nuova tecnologia arrivano nuovi metodi di attacco. Tuttavia, le motivazioni e gli obiettivi dei criminali informatici restano gli stessi, Accenture stima in 347 milioni di dollari il rischio per il settore bancario[5].

FOCUS SUL SETTORE BANCARIO	
VAP:	**Phishing su larga scala**: • Team tecnologico • Dirigenti **Attacchi BEC mirati:** • Responsabili delle relazioni • Relazioni con gli investitori/Consulenti finanziari • Sviluppo commerciale
Obiettivi:	• Clienti (diretti) • Dipendenti (diretti) • Clienti (indiretti): forza lavoro con accesso a dati e sistemi dei clienti • Dipendenti (indiretti): forza lavoro con accesso a dati e sistemi delle Risorse Umane
Obiettivi:	• Perdite finanziarie per i clienti

Banche attacchi mirati

I dati di threat intelligence di Proofpoint hanno identificato degli attacchi che prendono di mira una specifica funzione o azienda nel settore bancario. I criminali informatici all'origine di questi attacchi hanno quindi obiettivi precisi, scelti tramite ricognizioni specifiche per ogni azienda presa di mira.

Grande istituto bancario

Commenti degli analisti: una banca Fortune 100 ha ricevuto 12 messaggi (100%) che utilizzavano la nuova tecnica WhiteShadow[6] per distribuire un set sconosciuto di malware. Si tratta di un fatto interessante per vari motivi.

Il fatto che il malware non sia stato identificato potrebbe indicare che questa istituzione è semplicemente una cavia per un attacco sistemico più ampio.

WhiteShadow viene spesso usato per distribuire Crimson, un trojan di accesso remoto (RAT) identificato per la prima volta nel 2016 come payload usato da un gruppo di criminali informatici sponsorizzati dal governo pakistano battezzato "Transparent Tribe"[7]. Da allora, Crimson RAT è stato utilizzato da numerosi pirati informatici, ma il team di threat intelligence di Proofpoint ha ricevuto numerose domande dagli istituti bancari, che si chiedevano se la catena di attacco da WhiteShadow a Crimson potesse ancora essere un'attività sostenuta da uno Stato.

Il fatto che la tecnica WhiteShadow abbia iniettato altro malware oltre a Crimson, da un'infrastruttura non esplicitamente associata alla rete pakistana, evidenzia e corrobora l'ipotesi di un'adozione diffusa di questa tecnica e dei payload associati.

Cooperative di credito: attacco alla supply chain

Commenti degli analisti: una cooperativa di credito ha ricevuto 67 messaggi (87%) inviati anche ad altre società di contabilità regionali. Qualsiasi relazione fra la cooperativa di credito e queste società potrebbe indicare un attacco al canale laterale o contro la supply chain.

Il payload di GuLoader QuasarRAT non ha niente di particolare, ma è rappresentativo della notevole evoluzione di tattiche, tecniche e procedure osservate nel panorama delle minacce negli ultimi due anni, finalizzato a gettare le basi per la distribuzione di ulteriori payload. Inoltre, QuasarRAT, in quanto open source, permette ai sofisticati criminali informatici che lo utilizzano di coprire le loro tracce. Per esempio, se un criminale informatico riesce a entrare in un sistema grazie a un software generico o ampiamente diffuso, sarà molto più difficile capire chi ha lanciato effettivamente l'attacco. Nel caso di una violazione riuscita, questa tecnica consente comunque al criminale informatico di distribuire un ulteriore payload dopo aver condotto alcune attività di ricognizione.

[5] Accenture (2020), "The State of Cybercrime in Banking and Capital Markets" (Lo stato del crimine informatico nel settore bancario dei mercati dei capitali)

[6] https://www.proofpoint.com/us/threat-insight/post/new-whiteshadow-downloader-uses-microsoft-sql-retrieve-malware

[7] https://www.proofpoint.com/us/threat-insight/post/Operation-Transparent-Tribe

Banche: tendenze e analisi delle minacce

Nell'arco di sei mesi, dal quarto trimestre 2019 al secondo trimestre 2020, il team di threat intelligence di Proofpoint ha osservato le minacce mostrate nella Figura 1, che colpiscono costantemente il settore bancario.

Bonifico bancario

Commenti degli analisti: le banche commerciali ricevono quasi il doppio dei messaggi rispetto al secondo settore verticale più vicino, anche se le società di investimenti finanziari, di servizi di transazioni finanziarie e i protagonisti dell'ecosistema finanziario li ricevono tutti. L'invio di tali messaggi è un fenomeno diffuso in maniera abbastanza equa fra i vari istituti e aree geografiche, piuttosto che concentrarsi su un singolo cliente con una manciata di messaggi a clienti simili. L'esca simula un invio di denaro tramite Western Union, finalizzato all'iniezione di un RAT. Per farlo, utilizza un messaggio con un oggetto che fa riferimento alla conformità.

Altre campagne degne di nota

Bot TeamViewer (MINEBRIDGE) | Word Documents | "Indeed Application: Cassiere a tempo pieno"
Questa campagna colpisce principalmente il settore dei servizi finanziari con un'esca che simula domande di lavoro per "Cassiere a tempo pieno" da parte di una società di collocamento fasulla.

GuLoader / Parallax "warii" | Allegati | "MAJ Code Banques"
Questi messaggi includevano allegati di Microsoft Office contenenti delle macro che, se attivate, scaricano ed eseguono GuLoader il quale, a sua volta, scarica e installa Parallax. Gli obiettivi principali erano banche e società di servizi.

jSocket "88.150.189[.]98" | URL | "Dichiarazione dei redditi"
Questi messaggi contengono degli URL che puntano a un file Java compresso. Quasi tutti i messaggi sono stati inviati a un istituto bancario.

Get2 / SDBbot | Documenti Excel
Queste email includono allegati di Microsoft Excel contenenti delle macro che, se attivate, eseguono una DLL incorporata (malware loader "Get2"). Get2 scarica SDBbot e un malware sconosciuto. Obiettivo primario: le banche. Il 76% dei messaggi di questa campagna era diretta a società di servizi finanziari. La campagna ha colpito le banche nel dicembre 2018 e nel gennaio 2019. Le banche hanno continuato a essere obiettivi frequenti.

URL | Documenti Word | PDF
Gli Stati Uniti sono colpiti da email contenenti URL, documenti Word o PDF. Questi ultimi sfruttano i marchi di molte banche Fortune 100. Questa campagna prevede l'invio alle società di servizi finanziari di un falso avviso di pagamento che finge di provenire da una società di vendita al dettaglio.

CobInt | Gruppo Cobalt | URL
I messaggi contengono link a un file PDF ospitato su Microsoft OneDrive. Il PDF include dei link per scaricare il file "Documents.rtf". A sua volta il file include degli exploit che, se hanno successo, scaricano CobInt. Negli Stati Uniti diversi dipendenti sono stati colpiti dal malware CobInt, che appartiene alle famiglie dei backdoor e downloader. L'attacco è stato lanciato da un gruppo di criminali informatici sotto sorveglianza che attacca principalmente le banche e gli istituti di credito, oltre a quelle nell'industria multimediale e dell'intrattenimento. In questo caso, oltre il 50% delle email è stato inviato ai dipendenti di società di servizi finanziari, rendendole il settore più esposto.

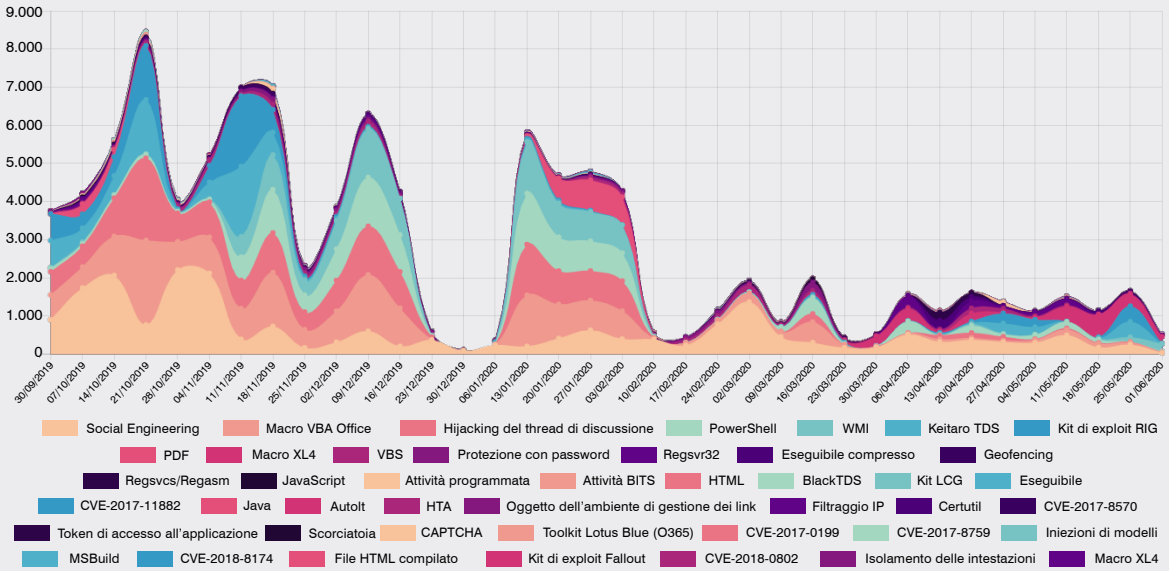


Figura 1: Casse di risparmio - Exploit mirati (Fonte: Proofpoint).

Mercati dei capitali

Accenture stima in 47 miliardi di dollari il rischio di perdite causate da attacchi informatici ai mercati di capitali[8].

FOCUS SUL SETTORE MERCATI DI CAPITALI	
VAP:	**Phishing ampio**: • Team tecnologico • Dirigenti/Partner gestionali **Attacchi BEC mirati:** • Consulenti e analisti finanziari • Gestori di fondi/Gestori di portafogli • Direttori della ricerca
Obiettivi:	• Denaro/Risorse (diretti): forza lavoro con accesso alle risorse • Clienti (indiretti): forza lavoro con accesso a dati e sistemi dei clienti
Obiettivi:	• Perturbazione del settore • Perturbazione dei mercati/attività economiche

Mercati dei capitali: attacchi mirati

I dati di threat intelligence di Proofpoint hanno identificato degli attacchi che prendono di mira una specifica funzione o azienda nel settore dei mercati capitali. I criminali informatici all'origine di questi attacchi hanno quindi obiettivi precisi, scelti tramite ricognizioni specifiche per ogni azienda presa di mira.

I payload nascosti potrebbero in realtà essere in vantaggio

Benché questi particolari attacchi usino delle esche di basso profilo, come fatture di spedizione, link di tracciamento di pacchi e tasse, il payload si basa sull'esecuzione di NodeJS. NodeJS è una piattaforma di esecuzione molto diffusa fra server e host web, perciò sarebbe logico concludere che il payload non dovrebbe essere eseguito quando viene scaricato su un endpoint locale.

È interessante notare che diversi framework per lo sviluppo delle applicazioni distribuiscono NodeJS in locale [9]. Benché la maggior parte delle applicazioni finanziarie costruite su queste piattaforme sia focalizzata sulle criptovalute, esistono diverse applicazioni open source e freeware per il monitoraggio dei mercati azionari, l'analisi dei dati finanziari e le piattaforme per il libero scambio (usate con maggiore probabilità dalle società di intermediazione prese di mira)[10].

Mercati dei capitali: tendenze e analisi delle minacce

Gli investimenti finanziari sono il settore più colpito, con il 31% dei messaggi e il 23% dei clienti. Da notare una certa sovrapposizione con le banche commerciali.

Nell'arco di sei mesi, dal quarto trimestre 2019 al secondo trimestre 2020, il team di threat intelligence di Proofpoint ha osservato le minacce mostrate nella Figura 2, che colpiscono costantemente il settore dei mercati di capitale.

[8] Accenture (2020), "The State of Cybercrime in Banking and Capital Markets" (Lo stato del crimine informatico nel settore bancario dei mercati dei capitali)

[9] https://brainhub.eu/blog/javascript-frameworks-for-desktop-apps/

[10] https://www.electronjs.org/apps?category=finance

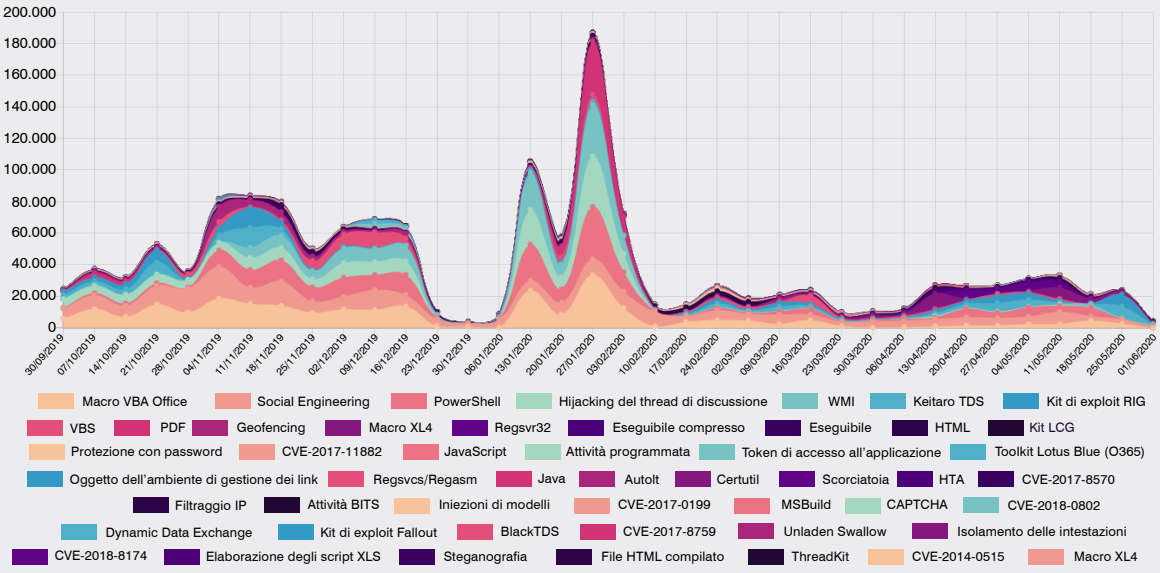


Figura 2: intermediazione di titoli - Exploit mirati (Fonte: Proofpoint).

Tendenze di attacco specifiche per regione

Commenti degli analisti: prendendo in esame le prime 20 banche d'investimento globali è risultato che, benché abbiano la sede centrale negli Stati Uniti e avrebbe senso che la maggior parte dei dipendenti fosse basata a Londra o New York, quasi tutti i loro primi 50 VAP si trovano a Singapore, in Cina o in Giappone.

Ciò potrebbe essere dovuto all'aumento delle nuove assunzioni in Asia-Pacifico, in risposta al rinnovato interesse negli investimenti in tali paesi. "Le banche stanno scoprendo che le aziende statali cinesi hanno giocato un ruolo importante nei negoziati nel 2020 e stanno svolgendo campagne di reclutamento massicce per stimolare l'attività dei mercati di capitali[11]."

Altre campagne degne di nota

QuasarRAT | HTML | "Avvisi di corrispondenza fiscale"

Le email con oggetto "Avvisi di corrispondenza fiscale" contengono un allegato HTML compresso che, se aperto, inietta un documento Word incorporato. Quest'ultimo usa delle macro per scaricare uno script VB che a sua volta scarica QuasarRAT. I mercati di capitali (investimenti e titoli) sono stati l'unico obiettivo di questa campagna.

Assicurazioni

Le assicurazioni sono considerate un segmento del settore dei servizi finanziari, in quanto si basano sulla gestione fiduciaria di fondi che devono essere a disposizione in caso di sinistro. Tuttavia questo segmento è piuttosto differente dagli altri perché i principali rischi a cui è esposto derivano da eventi esterni.

Dato l'elevato numero di potenziali obiettivi delle attività criminose, è importante prestare attenzione non solo a chi viene preso di mira in azienda ma anche al perché.

FOCUS SUL SETTORE ASSICURATIVO

VAP:

Phishing su larga scala:
- Team tecnologico
- Dirigenti
- Risorse umane/Addetti al reclutamento

Attacchi BEC mirati:
- Agenti assicurativi/Account manager
- Responsabili di programmi/piani (piani pensionistici, indennità di gruppo e molto altro)

Inoltre, i dati di threat intelligence di Proofpoint indicano che il segmento assicurativo ha subito un maggior numero di accessi non autorizzati ai tenant cloud rispetto al settore bancario e dei mercati di capitali.

Ciò può essere il risultato dell'utilizzo da parte delle compagnie di assicurazioni di big data e delle tecnologie di intelligenza artificiale[12], che sono convenienti economicamente solo se implementati in cloud[13]. Oppure, potrebbe anche essere dovuto alla continua ottimizzazione dei costi delle operazioni tramite l'automazione dei processi robotici, l'esternalizzazione di operazioni di routine o la migrazione di dati e operazioni nel cloud[14].

[11] Chatterjee, Murdoch (2020), "Exclusive: Bank of America to hire 50 bankers for Asia dealmaking team in 2020—sources" (Esclusivo: Bank of America assumerà 50 banchieri per il suo team di trading in Asia nel 2020 - Sources), Reuters

[12] Oliver (2019), "Insurance sector prepares for disruption" (Il settore assicurativo si prepara a delle perturbazioni), Financial Times

[13] Thomson (2020), "Are Insurers' Confidence in their Cyber Defense Exposing Them to Revenue Losses?" (La fiducia degli assicuratori nelle loro difese informatiche li espone a perdite di fatturato?), Accenture

[14] Deloitte (2020), "Deloitte Insights—2020 Insurance Outlook" (Deloitte Insights - Stato del settore assicurativo nel 2020)

Assicurazioni: attacchi mirati

I dati di threat intelligence di Proofpoint hanno identificato degli attacchi che prendono di mira una specifica funzione o azienda nel settore assicurativo. I criminali informatici all'origine di questi attacchi hanno quindi obiettivi precisi, scelti tramite ricognizioni specifiche per ogni azienda presa di mira.

L'affiliazione a TrickBot

Commenti degli analisti: in generale, più grande è la portata di una campagna dal punto di vista del volume complessivo dei messaggi e del numero di destinatari, minore è la probabilità che si tratti di una campagna mirata. Nel settore assicurativo, osserviamo concentrazioni molto elevate di categorie di vittime all'interno di una singola campagna.

In questo caso, 21 aziende destinatarie su 26 (81%) sono affiliate a un'assicurazione, mentre il 96% di tutti i messaggi è stato inviato a una compagnia assicurativa. La maggioranza dei messaggi va a una particolare compagnia di assicurazioni. Ma non è una coincidenza che altre 25 aziende che ricevono meno messaggi appartengano tutti allo stesso settore. Tipicamente, la distribuzione dei settori destinatari è più diversificata, ma le assicurazioni rappresentano solitamente circa il 10% - 13% dei casi, mentre il segmento verticale più colpito riceve solo il 16% - 18% dei messaggi.

Il payload del malware è uno dei trojan dei servizi bancari di più alto profilo: gli operatori eseguono la loro botnet sulla base di un modello di affiliazione. Per capire queste tattiche, tecniche e procedure sono diventate comuni, guardiamo a come opera questa minaccia. Un criminale informatico diventa cliente degli operatori di TrickBot. Gli viene quindi attribuito un parametro "group tag", in questo caso "yas24", in cui il codice di tre lettere denota la campagna/sottogruppo/affiliato responsabile dell'infezione. Il numero tende a essere iterativo in quanto il gruppo continua a distribuire il malware.

Assicurazioni: tendenze e analisi delle minacce

Nell'arco di sei mesi, dal quarto trimestre 2019 al secondo trimestre 2020, il team di threat intelligence di Proofpoint ha osservato le minacce mostrate nella Figura 3, che colpiscono costantemente il settore assicurativo.

AZORult | "daffy"

Le email con oggetto "Report postale da support@WellsFargo.com" contengono un allegato Microsoft Word denominato "ordine d'acquisto nl5753637.doc" e sfruttano la vulnerabilità CVE-2017-8570. Se aperto, l'allegato scarica ed esegue AZORult ("daffy.exe"). Il settore assicurativo riceve l'85% dei messaggi e rappresenta il 18% delle vittime.

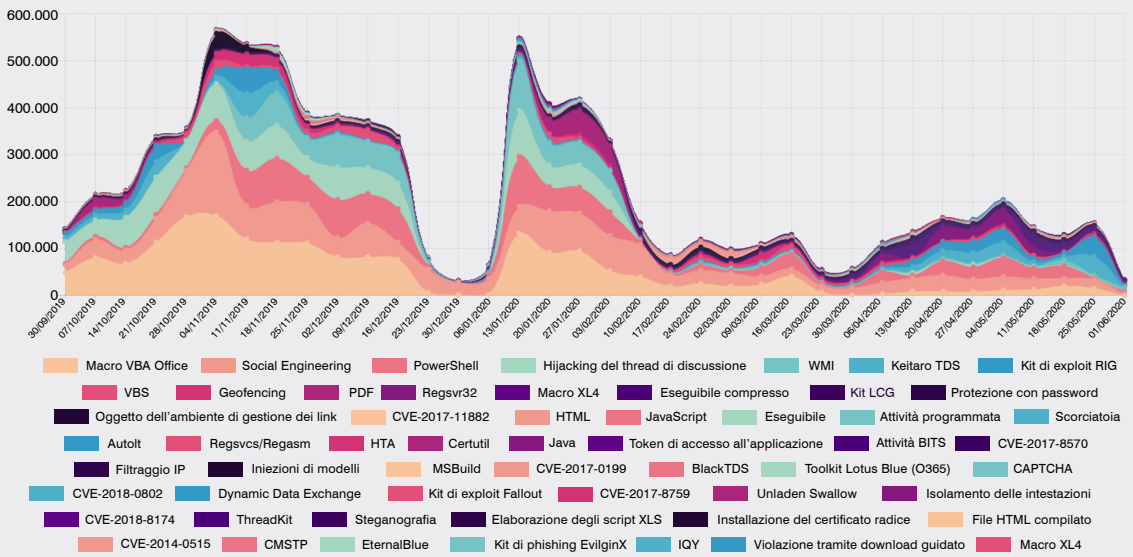


Figura 3: Assicurazioni - Exploit mirati (Fonte: Proofpoint).

Conclusioni e raccomandazioni

Nel settore delle assicurazioni e dei servizi finanziari la sicurezza informatica deve tenere conto non solo delle superfici di attacco esterne, ma anche delle lacune nella protezione create dalle attività interne di ottimizzazione di processi e tecnologie. Gli attacchi di oggi prendono di mira le persone, non soltanto la tecnologia. Sfruttano il "fattore umano" del settore delle assicurazioni e dei servizi finanziari come lo conosciamo oggi: il desiderio di aiutare i clienti a raggiungere i loro obiettivi e diventare un motore di opportunità. La pandemia globale ha costretto molte compagnie assicurative e società di servizi finanziari ad accelerare la loro trasformazione digitale per gestire meglio le relazioni multicanale con i clienti, oltre a facilitare la vendita e la fornitura delle soluzioni. Proteggere le informazioni e garantirne la conformità, cercando nel frattempo di proteggere e aumentare l'a produttività dei dipendenti in telelavoro, non è mai stato più complesso e importante per le aziende. Le minacce e i rischi per la conformità che le compagnie assicurative e le aziende di servizi finanziari devono affrontare attualmente richiedono un nuovo approccio incentrato sulle persone.

Queste sono le nostre raccomandazioni per i responsabili delle compagnie di assicurazioni e delle società di servizi finanziari:

- **Adotta un approccio alla sicurezza incentrato sulle persone.** I criminali informatici non hanno una visione del mondo in termini di topologia di rete. Prendono di mira le persone. Devi pertanto adottare una soluzione che ti permetta di identificare le vittime degli attacchi in azienda, i metodi utilizzati e ti permetta di stabilire se hanno fatto clic su un link dannoso. Valuta il singolo rischio rappresentato da ciascun utente. Una soluzione incentrata sulle persone ti indicherà i metodi utilizzati per colpire le tue persone, a quali dati hanno accesso e se sono inclini cadere nelle trappole tese dagli hacker.
- **Utilizza i dati del tuo programma incentrato sulle persone per pianificare e ricevere finanziamenti per i tuoi programmi di sicurezza.** Questi dati ti aiuteranno a spiegare ai dirigenti e al consiglio di amministrazione le tue priorità e i tuoi programmi per ridurre il profilo di rischio dell'azienda. Ti permetteranno inoltre di spiegare ai colleghi le motivazioni alla base del tuo programma e consentire loro di proteggere se stessi e l'azienda.
- **Insegna agli utenti a individuare e segnalare le email pericolose.** Una formazione regolare e simulazioni degli attacchi possono contribuire a ridurre il rischio in due modi. In primis, insegnano agli utenti a prevenire molti attacchi. In secondo luogo, permettono di identificare gli utenti particolarmente vulnerabili. Le simulazioni più efficaci sono quelle che imitano le tecniche di attacco del mondo reale. Prendi in considerazione soluzioni che tengano conto delle attuali tendenze degli attacchi contro il settore assicurativo e dei servizi finanziari e che includono le informazioni più recenti sulle minacce. Nel momento in cui gli utenti segnalano email sospette, l'automazione permette di verificare e neutralizzare le minacce reali.
- **Contemporaneamente, parti dal principio che qualche utente finirà inevitabilmente per fare clic su un link.** I criminali troveranno sempre nuovi modi per sfruttare le debolezze della natura umana. Trova una soluzione che rilevi e blocchi le minacce email in entrata destinate agli utenti prima che raggiungano la casella della posta in arrivo. Neutralizza le minacce esterne che fanno uso del tuo dominio aziendale per colpire i tuoi clienti. Una soluzione efficace per la prevenzione della perdita di dati (DLP) dall'email aiuta a mantenere i dati protetti e accessibili. Opta per una soluzione che classifichi in modo preciso le informazioni critiche e sensibili e garantisca che l'accesso a questi dati sia accordato alle persone autorizzate.
- **Crea una solida difesa contro gli attacchi BEC.** Gli strumenti di sicurezza tradizionali a volte faticano a rilevare le email fraudolente. Investi in una soluzione in grado di gestire le email in base a policy di quarantena e di blocco personalizzate. Poiché gli hacker a volte utilizzano account compromessi per ingannare gli utenti all'interno della stessa azienda, la tua soluzione deve analizzare sia le email esterne che quelle interne. Implementa l'autenticazione DMARC (Domain-base Message Authentication, Reporting and Conformance) per bloccare le email falsificate, prima che i dipendenti e i collaboratori esterni siano vittime di una frode.
- **Adotta un approccio Zero Trust per l'accesso remoto.** Le compagnie assicurative e le società di servizi finanziarie non hanno mai memorizzato ed elaborato così tanti dati come oggi. La loro presenza digitale è più estesa. Il loro personale è più disperso. Tutto ciò è manna dal cielo per i criminali informatici. Inoltre, le tradizionali tecnologie VPN non sono più all'altezza. Investi in una soluzione Zero Trust in grado di connettere i tuoi dipendenti, collaboratori e clienti al tuo data center e al cloud in modo rapido e sicuro.
- **Isola siti web e URL pericolosi.** Proteggi il tuo ambiente da contenuti web pericolosi. La tecnologia di isolamento del web è in grado di valutare le pagine web sospette e gli URL non verificati in un contenitore protetto all'interno del browser web abituale dell'utente. Questo approccio può fornire una protezione critica per gli account email condivisi, che sono difficili da proteggere tramite l'autenticazione a più fattori. La stessa tecnologia può isolare la navigazione personale e i servizi webmail degli utenti, garantendo loro libertà e riservatezza senza mettere in pericolo l'azienda.

- **Proteggi Microsoft 365 e le altre piattaforme cloud.** A fronte della migrazione di una crescente quantità di dati e applicazioni del settore assicurativo e dei servizi finanziari verso il cloud, hai bisogno di visibilità in tempo reale sulle attività nel cloud. Una soluzione CASB (Cloud Access Security Broker) ti aiuta ad analizzare e neutralizzare rapidamente le potenziali violazioni delle policy email nel cloud per garantire la continuità dei servizi.
- **Identifica e neutralizza le minacce interne.** Proteggiti dalle fughe di dati, dal sabotaggio e dai danni al marchio causati da utenti interni malintenzionati, negligenti o compromessi. Adotta una soluzione di gestione interna delle minacce che correli l'attività e il movimento dei dati per aiutarti a collegare il comportamento e l'intento dell'utente. Aiuta i team della sicurezza a identificare i rischi legati agli utenti, rilevare e contrastare le violazioni dei dati di origine interna e accelerare la risposta agli incidenti.
- **Riduci i rischi di conformità.** Le normative di conformità per il settore assicurativo e dei servizi finanziari sono in costante evoluzione. Le aziende sono soggette a maggiori controlli e a sanzioni più elevate e devono garantire il rispetto delle normative dei loro partner. Scegli una soluzione per l'archiviazione e la conformità in grado di rilevare e arrestare rapidamente le fughe di dati interne, sia intenzionali che accidentali. Identifica e poni fine a pratiche commerciali fraudolente, come le fatture fraudolente e le tangenti.
- **Collabora con un fornitore esperto di threat intelligence.** Per gestire gli attacchi altamente mirati, è necessario disporre di threat intelligence avanzata. Affidati quindi a una soluzione che combina tecniche statiche e dinamiche per rilevare nuove caratteristiche di attacco (ovvero strumenti, tattiche e obiettivi) e fare tesoro di tali informazioni.

PER SAPERNE DI PIÙ

Per maggiori informazioni visita **proofpoint.com/it**.

INFORMAZIONI SU PROOFPOINT

Proofpoint (NASDAQ: PFPT) è un'azienda leader nella cybersecurity e nella conformità, che protegge dai rischi il patrimonio più importante di un'azienda: le persone. Con una suite integrata di soluzioni basate su cloud, Proofpoint aiuta le aziende di tutto il mondo a bloccare le minacce mirate, a salvaguardare i propri dati e a proteggere gli utenti dagli attacchi IT. Aziende di ogni dimensione, tra cui più della metà delle Fortune 1000, si affidano alle soluzioni di sicurezza e di conformità incentrate sulle persone di Proofpoint per mitigare i rischi di sicurezza veicolati via email, cloud, social media e web. Per ulteriori informazioni: **www.proofpoint.com/it**.

proofpoint.

0400-003-01-01 1/21