Microsoft

The Confidence Game

Compromissione della posta elettronica aziendale (BEC)

Microsoft Threat Intelligence

Cyber Signals

Maggio 2023

La Digital Crimes Unit di Microsoft ha osservato, tra il 2019 ed il 2022, un **aumento del 38 percento** per quanto riguarda il Cybercrime-as-a-Service (CaaS), che conta, tra i vari target, la posta elettronica aziendale.

Introduzione

I tentativi di frode alle e-mail aziendali continuano ad aumentare, con il Federal Bureau of Investigation (FBI), che segnala più di 21.000 reclami con perdite rettificate superiori ai 2,7 miliardi di dollari. Microsoft ha infatti osservato un aumento della sofisticazione e delle tattiche messe in pratica dagli autori di tali minacce, specializzati nella compromissione della posta elettronica aziendale (BEC), incluso l'utilizzo di indirizzi di protocollo internet (IP) residenziali, per dare l'idea che le campagne di attacco avvengano a livello locale.

Questa nuova tattica sta aiutando i criminali a monetizzare ulteriormente il Cybercrime-as-a-Service (CaaS), e ha attirato l'attenzione delle forze dell'ordine federali perchè consente ai criminali informatici di eludere gli avvisi del sistema di sicurezza del tipo "impossible travel"- utilizzato per identificare e bloccare i tentativi di accesso anomali ed altre attività sospette.

We are all cybersecurity defenders.

Security Snapshot

Questi dati riportano la media annuale e giornaliera dei **Tentativi BEC rilevati e su cui ha indagato** la Microsoft Threat Intelligence Digital Crimes Unit (DCU) da Aprile 2022 ad Aprile 2023. Le rimozioni degli URL a scopo di phishing qui riportate dalla Microsoft Digital Crimes Unit fanno riferimento al periodo Maggio 2022 -Aprile 2023.[1]

35 Milioni
All'anno

156,000
Al giorno

417,678
Rimozioni degli URL a scopo di phishing

L’ascesa di BulletProftLink nell’ambito della BEC

Gli attacchi di Cyber-Crime legati alla posta elettronica aziendale continuano ad aumentare. Microsoft ha osservato, ad esempio, una tendenza significativa per quanto riguarda l’utilizzo di BulletProftLink, una piattaforma nota per la creazione, su larga scala, di campagne email minacciose. BulletProftlink fornisce un servizio end-to-end che include modelli automatizzati per la BEC. Chi utlizza questo CaaS riceve le credenziali e l’indirizzo IP della vittima. Gli autori delle minacce BEC quindi, acquistano gli indirizzi IP dai servizi IP residenziali che corrispondono alla location della vittima, creando delle proxies IP residenziali che consentono ai criminali informatici di mascherare la propria origine.

Gli autori delle minacce BEC, oltre ad essere dotati di uno spazio-indirizzo localizzato, di nomi utenti e password, oscurano i movimenti, raggirano le bandiere di “impossible travel”, aprono un gateway per condurre ulteriori attacchi. Microsoft ha osservato che gli autori di tali minacce si trovano più frequentemente in Asia o in alcune zone dell'Europa orientale. “Impossible travel” è un sistema di rilevamento e notifica delle minacce in caso di compromissione degli account. Alert di questo tipo segnalano che un’attività viene eseguita in due località differenti, senza che vi sia stato il tempo necessario per spostarsi effettivamente da un luogo all’altro.

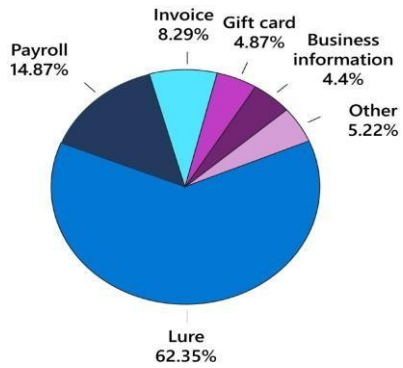
Gli attacchi informatici potrebbero quindi intensificare l'utilizzo di indirizzi IP residenziali per eludere qualsiasi rilevamento. Gli indirizzi IP residenziali mappati rispetto alla location delle vittime danno la possibilità di raccogliere grandi volumi di credenziali compromesse e account di accesso. Gli autori di tali minacce utilizzano servizi IP/proxy che i marketer e altri soggetti potrebbero utilizzare per misurare questi attacchi.

Threat briefing

Un fornitore di servizi IP, ad esempio, detiene 100 millioni di indirizzi IP che possono essere modificati ogni secondo. Mentre gli autori delle minacce utilizzano phishing-as-a-service come Evil Proxy, Naked Pages e Caffeine per implementare campagne di phishing e ottenere credenziali in maniera compromessa, BulletProftLink offre un design di gateway decentralizzato, che include nodi Blockchain pubblici per ospitare siti di phishing e BEC, creando un’offerta web ancora più sofisticata, decentralizzata, e sempre più difficile da interrompere. Distribuire l'infrastruttura di questi siti attraverso la complessità e la crescita in evoluzione delle blockchain pubbliche rende più complessa la loro identificazione e l'allineamento delle azioni di rimozione. Sebbene sia possibile rimuovere un collegamento di phishing, il contenuto rimane online ed i criminali informatici tornano a creare un nuovo collegamento al contenuto CaaS esistente. Gli attacchi BEC riusciti costano alle organizzazioni centinaia di milioni di dollari all'anno. Nel 2022, il Recovery Asset Team dell'FBI ha avviato la Financial Fraud Kill Chain su 2.838 denunce BEC riguardanti transazioni nazionali con perdite potenziali di oltre 590 milioni di dollari.

Compromissione della posta elettronica aziendale: attacchi di Phishing per tipologia

I dati rappresentano le tipologie di phishing BEC, da Gennaio 2023 ad Aprile 2023



Sebbene le implicazioni finanziarie siano significative, nel più ampio raggio dei danni a lungo termine includiamo il furto delle identità (se le informazioni di identificazione personale -PII, sono compromesse) o la perdita di dati riservati (se le informazioni sensibili o la proprietà intellettuale sono esposte al traffico di e-mail e messaggi dannosi).

I target principali della BEC sono: dirigenti, finance managers ed il personale delle risorse umane. Quest'ultimo, infatti, detiene l'accesso ai registri personali dei dipendenti, ai numeri di previdenza sociale, dichiarazione dei redditi e altre PII. Rientrano nel mirino degli autori di tali minacce anche i dipendenti recentemente assunti, forse meno propensi a verificare l'autenticità delle richieste di posta elettronica sconosciute. La maggior parte delle forme di attacchi BEC è in aumento. Attacchi BEC specifici prendono di mira buste paga, gift card e business information. Tali attacchi, tuttavia, si distinguono nel settore del Cyber-crime per la loro enfasi sull'ingegneria sociale e sull'arte dell'inganno. Invece di sfruttare le vulnerabilità dei dispositivi privi di patch, gli operatori BEC sfruttano il traffico e-mail e altre forme di messaggistica, inducendo le vittime a fornire informazioni finanziarie o a intraprendere azioni dirette, come l'invio di fondi ad account "money mule".

Rispetto ad un attacco ransomware, che tende a presentarsi con messaggi di estorsione più evidenti, gli operatori della BEC mettono in atto un tranquillo "confidence game", servendosi di scadenze artificiose ed urgenze al fine di sollecitare i destinatari. Rispetto ai nuovi malware, gli avversari BEC allineano le proprie tattiche per concentrarsi su strumenti che migliorino gamma, plausibilità, e probabilità di riuscita di ricezione di messaggi dannosi. Sebbene ci siano stati diversi attacchi di alto profilo che si sono serviti dell'indirizzo IP, Microsoft e le agenzie federali di polizia condividono la preoccupazione che questa tendenza non possa essere rapidamente ridimensionata -rendendo difficile, in più casi, rilevare attività con allarmi o notifiche tradizionali.

Variazioni in location di login non sono di per sè dannose. Per esempio, uno user potrebbe accedere alle business applications tramite laptop utilizzando il Wi-Fi locale, e simultaneamente, aver effettuato l'accesso alle stesse app sul proprio smartphone tramite rete cellulare. Per questo motivo le organizzazioni possono personalizzare le soglie di "impossible travel flag" sulla base della propria tolleranza al rischio. Tuttavia, la scala industriale legata allo spazio-indirizzo IP, localizzato per attacchi BEC, crea nuovi rischi per le aziende, in quanto la BEC sceglie sempre più spesso di generare posta elettronica dannosa tramite lo spazio-indirizzo più vicino ai propri target.

Raccomandazioni:

Sfrutta al massimo le impostazioni sulla sicurezza della tua posta in entrata: Le aziende possono configurare i propri sistemi di posta elettronica per contrassegnare i messaggi inviati da parti esterne. Abilita le notifiche nel caso di mittenti e-mail non verificati.
Blocca i mittenti con identità non verificate e segnala le loro e-mail come phishing o spam, grazie alle app di posta elettronica.

Configura l'autenticazione avanzata: Rendi più difficile la compromissione delle e-mail attivando l'autenticazione a più fattori, che richiede, per effettuare l'accesso, un codice, un PIN o un'impronta digitale. Gli account abilitati all'autenticazione a più fattori sono meno esposti al rischio di compromissione delle credenziali e a tentativi di accesso, indipendentemente dallo spazio-indirizzo utilizzato dagli utenti malintenzionati. La tecnologia "no password" garantisce maggiore sicurezza, facendo una verifica delle identità direttamente sul dispositivo, piuttosto che far passare le credenziali dell'utente utilizzando una connessione online poco sicura.

Aiuta i dipendenti ad individuare i segnali di pericolo: Dai la possibilità ai tuoi dipendenti di individuare le email fraudolente, come una mancata corrispondenza nel dominio o negli indirizzi email.

Proteggiti dagli attacchi

La lotta alla BEC richiede vigilanza e consapevolezza

Sebbene gli autori di tali minacce abbiano ideato strumenti specializzati per facilitare la BEC (tra cui kit di phishing e liste di indirizzi mail verificati che hanno come target dirigenti C-suite e altri ruoli specifici), le imprese possono comunque ricorrere a mezzi di difesa per mitigarne i rischi.

Per esempio, un'autenticazione "domain-based message, reporting and conformance" (DMARC), offre la protezione più efficace contro le email contraffatte, e si accerta che i messaggi non autenticati vengano rifiutati dal mail server, ancora prima di essere inviati. In più, i rapporti DMARC, consentono a un'organizzazione di essere informata in caso di tentativi di falsificazione.

Nonostante le organizzazioni abbiano già iniziato a gestire la propria forza lavoro completamente o parzialmente da remoto, è tutt'ora necessario, nell'era del lavoro ibrido, ripensare le policy sulla Sicurezza. Poichè i dipendenti sono sempre più a contatto con fornitori e appaltatori, ricevono più email, ed è quindi un dovere essere consapevoli dei rischi e dei cambiamenti cui gli ambienti di lavoro sono oggi soggetti.

Gli attacchi del tipo BEC possono essere di diversi tipi—incluse chiamate, messaggi di testo, e-mail, o messaggi social. Un buon primo passo per la difesa è il consolidamento delle policy di contabilità, maggiori controlli interni, e consapevolezza su come rispondere in caso di richieste di modifiche per quanto riguarda strumenti di pagamento o ricezione di bonifici bancari.

Esitare, in caso di richieste che in modo sospetto non rispettino le policy interne, può salvare le organizzazioni da perdite inimmaginabili.

Gli attacchi BEC sono un chiaro esempio del perchè i rischi cyber debbano essere affrontati in maniera trasversale, con i dirigenti, dipendenti finanziari, responsabili delle risorse umane e altri che più in generale hanno solitamente accesso a: numeri di previdenza sociale, dichiarazione dei redditi, informazioni di contatto e orari. Il DCU di Microsoft lavora per combattere le reti cyber-criminali e le infrastrutture che si servono di azioni civili, mandati penali e partnership pubbliche e private.

Raccomandazioni:

Utilizza una soluzione di posta elettronica fidata: Oggi le piattaforme cloud di posta elettronica sfruttano l'IA per migliorare le difese, garantendo una protezione avanzata dal phishing e minacce sospette. Le app cloud per la posta elettronica offrono anche vantaggi di aggiornamenti software continui ed automatici di gestione centralizzata delle politiche di sicurezza.

Proteggi le identità per proibire il lateral movement: La protezione delle identità è un pilastro fondamentale per combattere la BEC. Grazie a Zero Trust,controlli l'accesso alle app, ai dati e la governance automatizzata delle identità.

Adotta una piattaforma di pagamento sicura: Prendi in considerazione la possibilità di passare dalle fatture inviate via e-mail a un sistema progettato per autenticare i pagamenti.

Fai una telefonata per verificare le transazioni effettuate: Ti consigliamo di effettuare una rapida conversazione telefonica per verificare la legittimità delle informazioni di cui disponi, anzichè affidarti a una risposta rapida o un click. Ricorda ai tuoi dipendenti che è importante contattare direttamente le organizzazioni o gli individui—senza utilizzare le informazioni fornite tramite messaggi sospetti—per controllare richieste finanziarie o di altro tipo.

Expert Profile

> "La compromissione della posta elettronica si serve di: ingegneria sociale, violazione delle credenziali e pura grinta".

Simeon Kakpovi

Senior Threat Intelligence Analyst, Microsoft Threat Intelligence

Simeon Kakpovi voleva inizialmente diventare un medico, ma presto si rese conto che quella non era la sua vocazione. "Ho cambiato specializzazione un paio di volte, e alla fine mi sono ritrovato ad avere a che fare con i sistemi informatici. Ho deciso di passare alla sicurezza informatica perchè i miei mentori erano già del settore."

Da studente del secondo anno alla Howard University, ha frequentato lezioni di Cybersecurity presso un college locale, che alla fine, gli ha permesso di approdare alla Lockheed Martin Cyber Analyst Challenge. "Ci hanno spedito una chiavetta USB con 80 gigabyte di dati. Quello che è venuto fuori dopo è stata una delle cose più divertenti che mi sia mai successa. La sfida richiedeva ai partecipanti di analizzare il caso di un'intrusione Informatica, utilizzando il processo di cattura dei pacchetti ed i file di memoria. "Arrivato a quel punto, pensai, è questo quello che mi piacerebbe fare nella vita.'"

Questo lo ha poi portato a fare uno stage presso il Lockheed Martin e a lanciare il cyberskilling game KC7.

"Molti corsi sulla cybersecurity utilizzano acronimi e concetti vaghi perchè non si ha l'accesso a dati reali. Si genera quindi un problema circolare, perchè non puoi avere le competenze finchè non hai un lavoro, ma non puoi avere un lavoro se non dimostri di avere le competenze." Oggi Simeon guida il team di analisti Microsoft che conta più di 30 gruppi Iraniani e nota come questi condividano un tratto comune: la tenacia.

"Abbiamo più volte riscontrato che l'Iran è persistente e paziente, disposto a spendere tempo e risorse per perseguire i propri obiettivi. Gli autori di tali minacce, in Iran, ci ricordano che non è necessario utilizzare nuove tecniche offensive per avere successo. Per compromettere la posta elettronica, tutto ciò che serve sono: email di phishing, ingegneria sociale e, per concludere, pura grinta.

"L'ingegneria sociale non è roba così semplice come apparentemente potrebbe sembrare. Abbiamo visto gli autori delle minacce sfruttare le informazioni personali rivelate sui social media per attirare le vittime durante le campagne di ingegneria sociale." Per esempio, Crimson Sandstorm utilizza profili Social fake e prende di mira individui sulla base delle offerte di lavoro che compaiono sui loro profili LinkedIn. Poi, per alcuni mesi, tenta di stabilire delle relazioni di fiducia con queste persone. Infine, l'invio delle BEC si serve di file dannosi sotto forma di video o sondaggi. Tuttavia, poichè si tratta di relazioni sviluppatesi in lunghi periodi di tempo, è più probabile che le vittime abbiano ignorato gli avvisi di sicurezza ricevuti. Simeon osserva come gli autori di tali minacce, in Iran, siano motivati da diverse ragioni.

"A volte, durante il monitoraggio di Mint Sandstorm e degli attacchi ad agenzie che lavorano con enti governativi, la politica nucleare è il driver principale. La pubblicazione di informazioni critiche nei confronti del governo Iraniano ad opera di think tanks o Istituzioni accademiche, può suscitare l'ira di tali gruppi. Questi infatti potrebbero venire facilmente a conoscenza delle politiche degli Stati Uniti o di altri paesi Occidentali, e prenderebbero di mira tali soggetti servendosi di informazioni utili al loro governo".

[1] Methodology: For snapshot data, Microsoft platforms including Microsoft Defender for Office, Microsoft Threat Intelligence, and Microsoft Digital Crimes Unit (DCU) provided anonymized data on device vulnerabilities and data on threat actor activity and trends. In addition, researchers used data from public sources, such as the Federal Bureau of Investigation (FBI) 2022 Internet Crime Report and Cybersecurity & Infrastructure Security Agency (CISA). The cover stat is based on Microsoft DCU business email Cybercrime-as-a-Service engagements 2019 through 2022. Snapshot data represents adjusted annual and average daily BEC attempts detected and investigated.