EBOOK

Il cloud nel mirino

Come i criminali informatici sfruttano le vulnerabilità legate alla condivisione di file, alle identità e alla supply chain in Microsoft 365

proofpoint.

Introduzione

Nell'era digitale attuale, Microsoft 365 è uno strumento di produttività fondamentale. Sfortunatamente, la sua popolarità lo ha reso un obiettivo primario per i criminali informatici. Sebbene Microsoft 365 includa una serie di funzionalità native per bloccare gli attacchi informatici, questi strumenti non sono all'altezza degli attuali attacchi sofisticati.

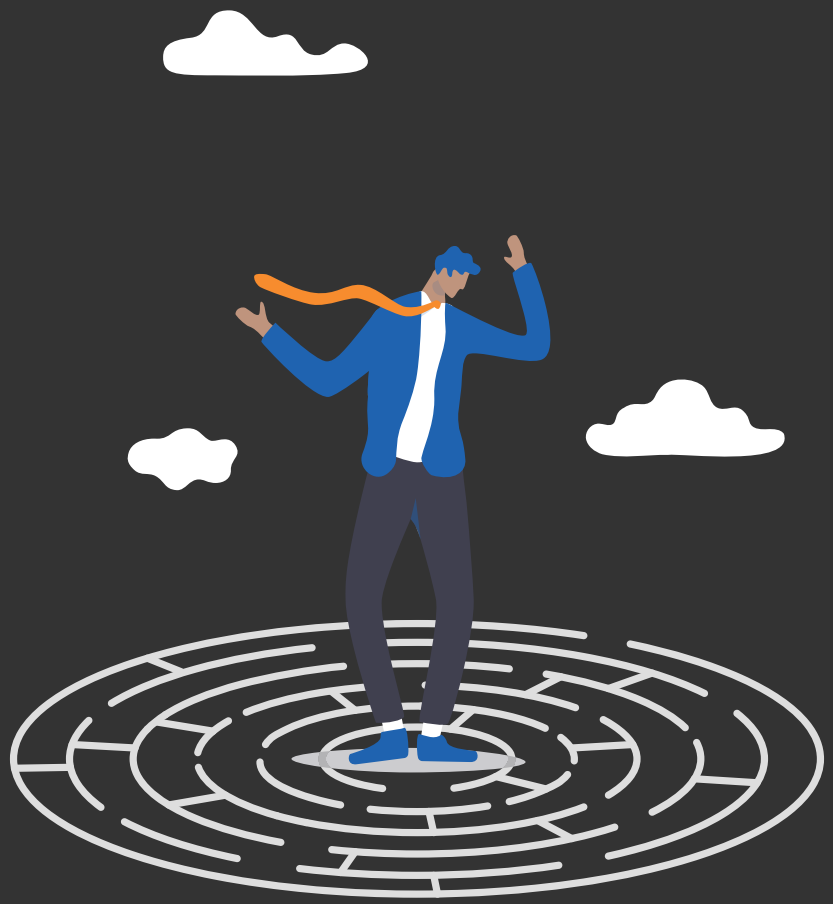
Gli attacchi incentrati sulle persone contro Microsoft 365 costano ogni anno milioni di dollari alle aziende e causano frustrazione sia ai team della sicurezza che agli utenti. Si è arrivati al punto che gli esperti del settore, come Gartner, concordano sul fatto che gli strumenti integrati per il cloud dovrebbero essere rafforzati da soluzioni di terze parti[1].

Il motivo per cui gli strumenti integrati non sono più sufficienti è semplice: i criminali informatici sono diventati esperti nel colpire le persone. E questo li rende sempre più difficili da contrastare.

La violazione degli utenti è di solito il primo passo di una serie molto più ampia di eventi che si verificano quando un'azienda viene violata. Denominati "catena di attacchi informatici", questi eventi iniziano con la violazione dell'utente e proseguono con l'abuso di privilegi, il furto di dati e altro ancora.

Passaggi nella catena di attacchi informatici.

1 Gartner, "Market Guide for Email Security" (Guida al mercato della sicurezza dell'email), febbraio 2023.



Questo eBook prende in esame cinque tipi di attacchi incentrati sulle persone che offrono ai criminali informatici un punto d'accesso e, allo stesso tempo, espongono le aziende a rischi di violazione più gravi. Sono molto difficili da rilevare solo con le funzionalità di Microsoft 365.

1. Violazione dell'email aziendale (BEC, Business Email Compromise)
2. Attacchi tramite telefonate (TOAD, Telephone-Oriented Attack Delivery)
3. Condivisione di file dannosi
4. Takeover degli account
5. Violazione degli account dei fornitori

Ogni sezione include diversi esempi che illustrano quanto vari e creativi possono essere questi attacchi. Tali esempi mostrano anche come quasi tutti gli utenti di Microsoft 365 possano essere vittime di un criminale informatico esperto se non adottano misure di sicurezza aggiuntive.

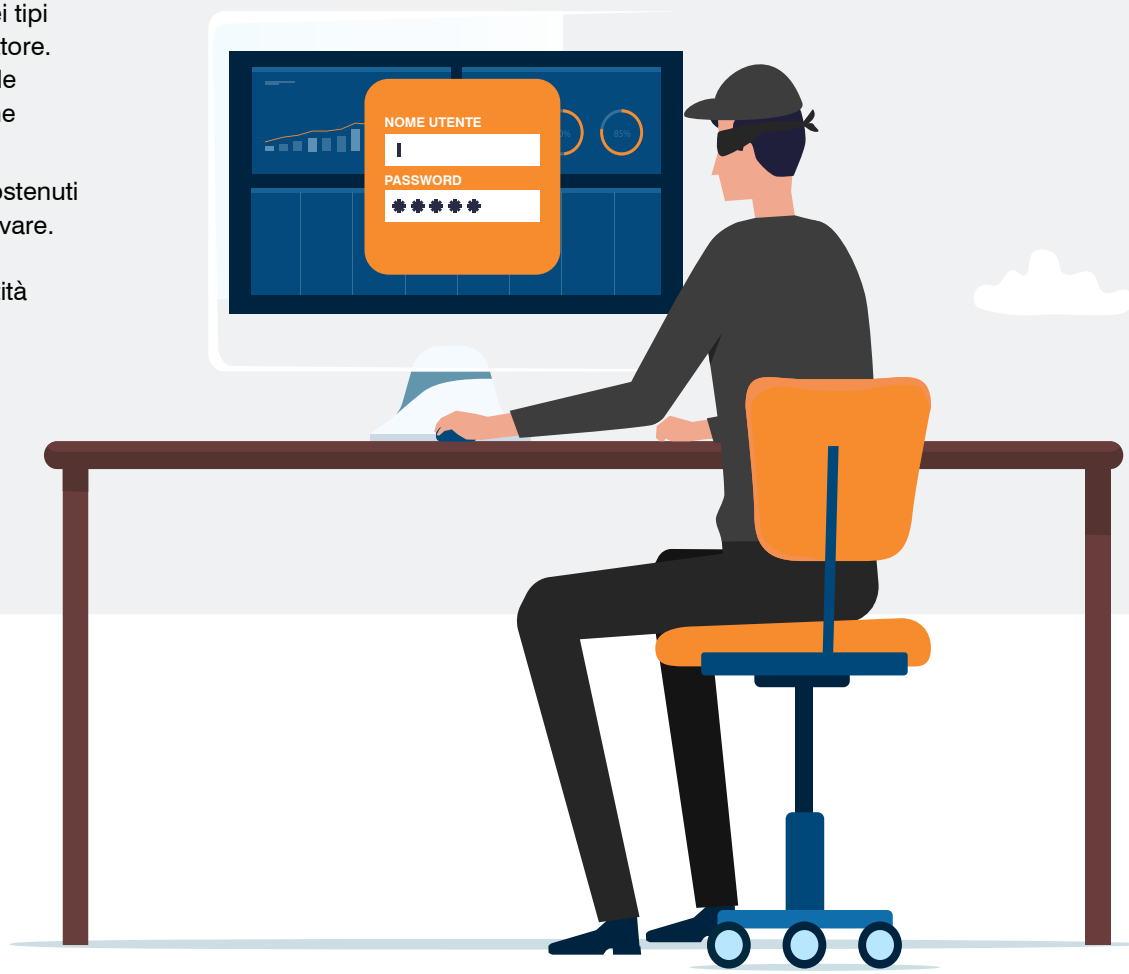
Tutti questi esempi sono minacce reali osservate da Proofpoint nelle valutazioni dei rischi realizzate per conto delle aziende.

SEZIONE 1

VIOLAZIONE DELL'EMAIL AZIENDALE (BEC)

La violazione dell'email aziendale (BEC, Business Email Compromise) è uno dei tipi di attacco più costosi che prendono di mira le aziende di ogni dimensione e settore. Ogni anno, le perdite continuano ad aumentare. Nel 2022, l'FBI ha rilevato che le aziende hanno perso 2,7 miliardi di dollari a causa di attacchi BEC. Una cifra che equivale a 300 milioni di dollari in più rispetto al 2021.

Molti degli schemi BEC attuali sono estremamente sofisticati, ben finanziati e sostenuti da un'attenta attività di ricerca e pianificazione. Sono anche molto difficili da rilevare. In effetti, i criminali informatici non inviano i payload classici che siamo abituati ad analizzare - ovvero URL o file allegati dannosi - ma si affidano al furto d'identità e altre tecniche di social engineering.



2 FBI. "2022 Internet Crime Report" (Report 2022 sui reati di Internet), 2023.

Ambiente:
Microsoft 365

Categoria della minaccia:
social engineering

Tipo di attacco:
reindirizzamento degli stipendi

Obiettivo:
responsabile delle indennità

Attacco di reindirizzamento degli stipendi

Gli attacchi di reindirizzamento degli stipendi sono attacchi di frode via email che solitamente prendono di mira i collaboratori che lavorano in ambito finanziario, fiscale, paghe e contributi e risorse umane. In questi attacchi, i criminali informatici mirano a conquistare la fiducia dei collaboratori al fine di modificare le coordinate bancarie e rubare lo stipendio del personale. Poiché si basano sulle tattiche di social engineering, a volte possono essere molto difficili da individuare. Gli attacchi di reindirizzamento degli stipendi sono considerati un rischio di medio livello per le aziende.

Esempio di attacco di reindirizzamento degli stipendi.

In questo attacco, un truffatore ha inviato un'email al responsabile delle indennità da un account Gmail fingendo di essere un collaboratore che chiedeva il pagamento del proprio stipendio su un nuovo conto bancario. In questo esempio, sia il truffatore che la vittima sono stati autorizzati a scambiarsi più messaggi. Nelle valutazioni e nei Proof of Concepts (PoC) condotti da Proofpoint, i controlli nativi di sicurezza dell'email di Microsoft non sono stati in grado di bloccare questo tipo di attacchi.

Ambiente:
Microsoft 365

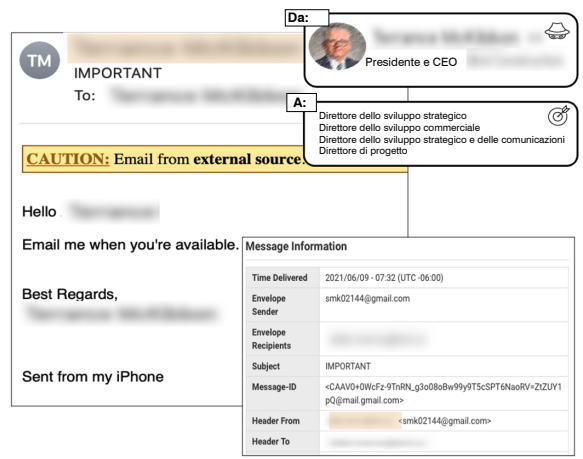
Categoria della minaccia:
social engineering

Tipo di attacco:
furto d'identità

Obiettivo:
responsabili della strategia e dello sviluppo commerciale

Attacco di furto di identità di un dirigente

Quando un criminale informatico riesce a farsi passare per un collaboratore, la frode può essere molto costosa per l'azienda. Ma quando i criminali informatici rubano l'identità di un dirigente di alto livello, le perdite possono essere molto più gravi. Negli ultimi anni, tali attacchi sono aumentati drasticamente. Da marzo 2020, Proofpoint ha osservato lo spoofing delle email di oltre 7.000 CEO. Più della metà dei clienti Proofpoint ha avuto almeno uno degli account email dei propri dirigenti di alto livello utilizzato in un tentativo di truffa.



Esempio di un attacco di furto d'identità di un dirigente.

In questo caso, un criminale informatico ha inviato un'email a dei collaboratori da un account Gmail, spacciandosi per un CEO che aveva bisogno che eseguissero un'azione. Se i collaboratori avessero risposto all'email, il truffatore avrebbe potuto facilmente esfiltrare dati o sottrarre denaro. Nelle valutazioni e nei PoC (Proof of Concept) condotti da Proofpoint, i controlli nativi di sicurezza dell'email di Microsoft non sono stati in grado di bloccare questo tipo di attacchi.

Ambiente:
Microsoft 365

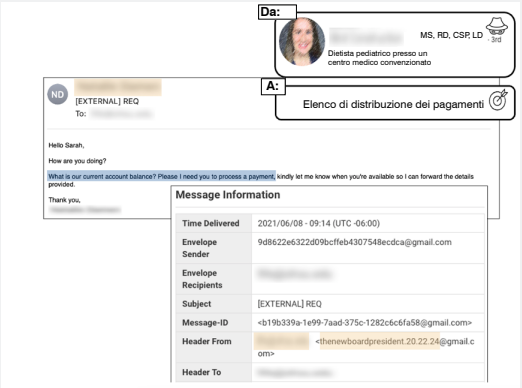
Categoria della minaccia:
social engineering

Tipo di attacco:
frode delle fatture

Obiettivo:
dipartimento finanziario

Frode delle fatture dei fornitori

La maggior parte degli attacchi BEC prende di mira le persone, come ad esempio la frode delle carte regalo. Tuttavia, le truffe BEC B2B che prendono di mira i fornitori sono estremamente mirate. Anche se il loro volume è inferiore, le perdite finanziarie derivanti possono essere molto consistenti. Proofpoint ha bloccato diversi tentativi di frode delle fatture dei fornitori, che sarebbero potuti costare milioni di dollari alle aziende. In questi attacchi, i criminali informatici inviano fatture fasulle o nuove coordinate bancarie in modo che i pagamenti vengano effettuati su un conto bancario da loro controllato.



Esempio di frode delle fatture dei fornitori.

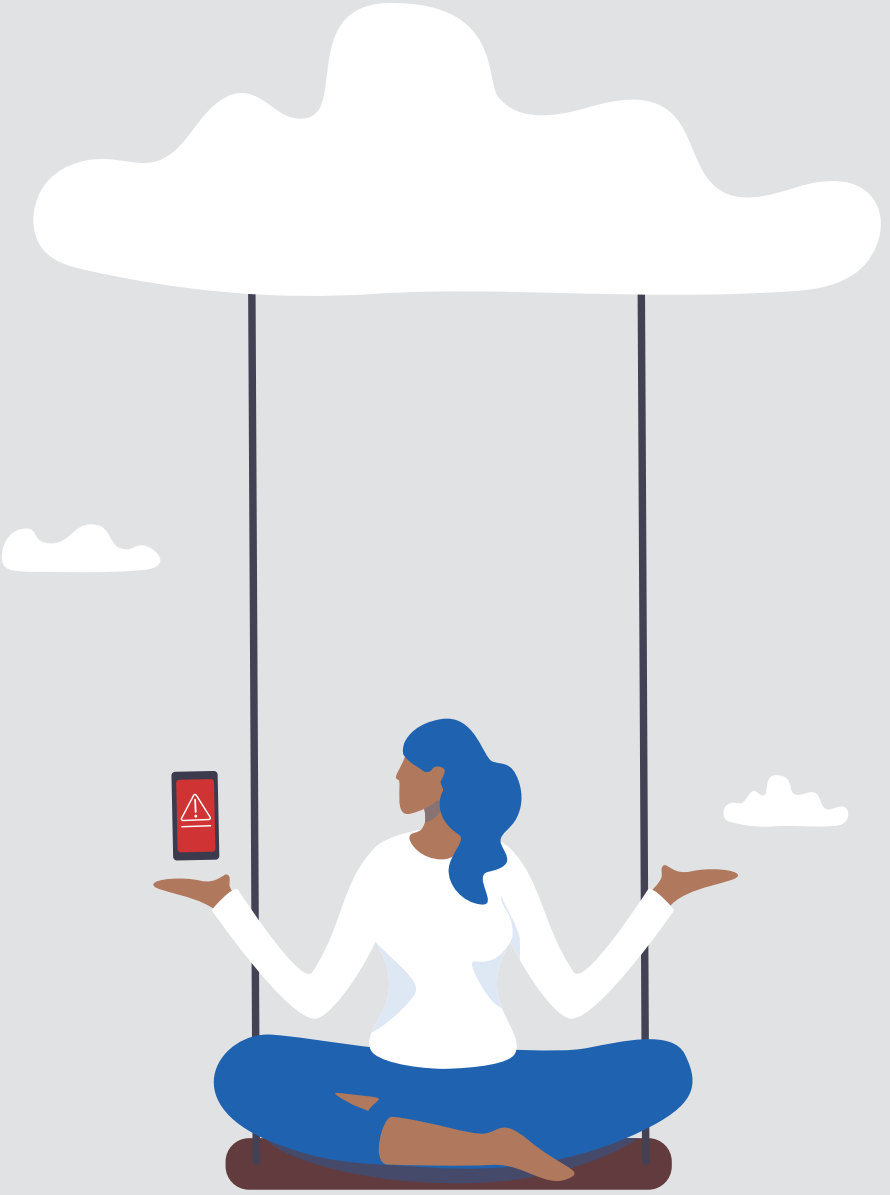
In questo esempio, il criminale informatico ha finto di essere un ex collaboratore che ora lavora presso un'azienda partner che aveva bisogno di elaborare un pagamento. Questo messaggio, inviato al dipartimento finanziario con un account Gmail, ha superato i controlli nativi di sicurezza dell'email di Microsoft.

Spesso i criminali informatici utilizzano Gmail o altri servizi di email gratuiti quando tentano questo tipo di frode, perché in questo modo riescono ad aggirare i controlli di autenticazione delle email come SPF (Sender Policy Framework) e DKIM (DomainKeys Identified Mail). I criminali informatici possono anche inviare URL o allegati dannosi per accedere a informazioni finanziarie o ad altri dati preziosi.

SEZIONE 2

ATTACCHI TRAMITE TELEFONATE

Negli attacchi tramite telefonate (TOAD, Telephone-Oriented Attack Delivery), l'obiettivo riceve un messaggio che solitamente include una fattura o un avviso fasullo. Il messaggio contiene anche il numero di un servizio clienti da contattare in caso di domande o per correggere un errore. Se l'obiettivo chiama il numero, si trova a parlare con un criminale informatico. Al picco delle attività, Proofpoint ha registrato l'invio di oltre 13 milioni di messaggi TOAD al mese nel 2022. Questo numero è in costante aumento da quando la tecnica è apparsa nel 2021[3].



3 Proofpoint, report "Il fattore umano", 2023.

Ambiente:
Microsoft 365

Categoria della minaccia:
social engineering

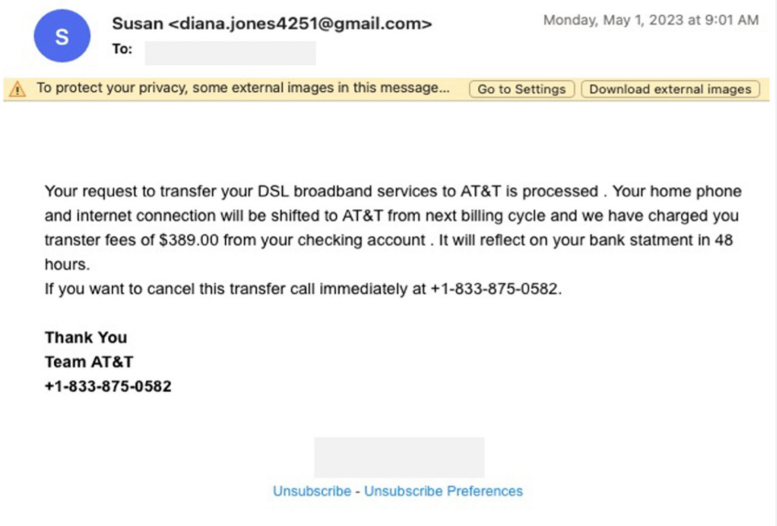
Tipo di attacco:
TOAD

Obiettivo:
utente di Microsoft 365

Minaccia TOAD

Le frodi via email basate su falsi operatori del servizio clienti dei call center sono prolifiche e redditizie. In molti casi, le vittime perdono decine di migliaia di dollari sottratti direttamente dai loro conti bancari. 68,4 milioni di americani hanno perso 39,5 miliardi di dollari a causa di attacchi di frode tramite telefonate tra il 2021 e il 2022[4].

Proofpoint osserva regolarmente due tipi di minacce provenienti dai call center. La prima utilizza dei software di assistenza remota gratuiti e legittimi per sottrarre denaro. La seconda utilizza dei malware camuffati da documenti per compromettere un computer e può portare alla distribuzione di altro malware.



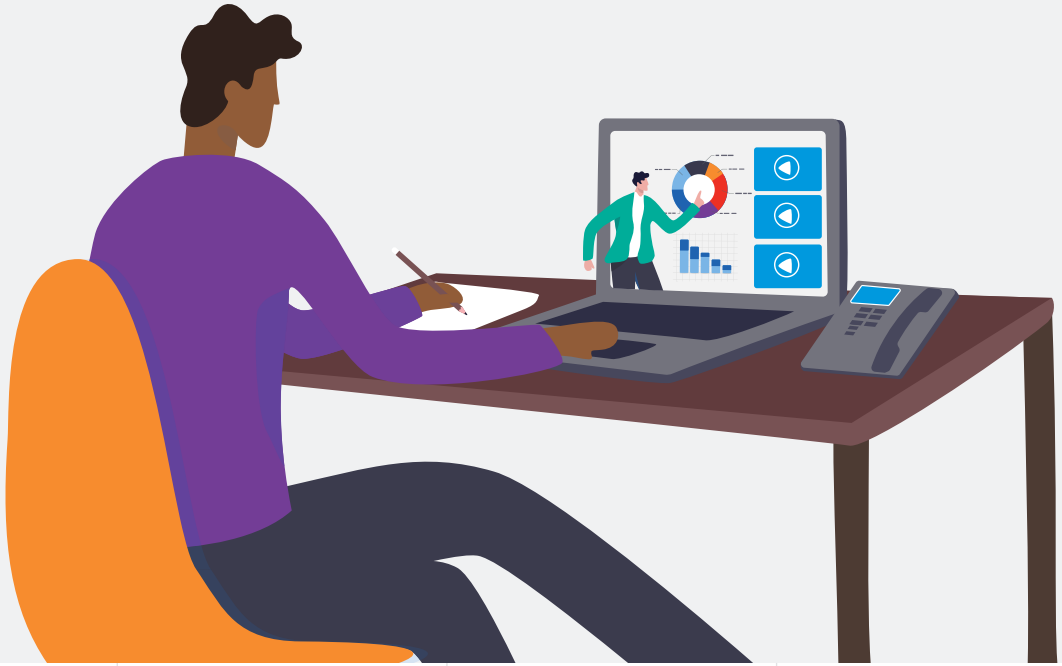
Esempio di attacco TOAD.

4 Truecaller. U.S. Spam & Scam Report, (Report su spam e truffe negli Stati Uniti), 2022.

In un tipico attacco proveniente da un call center, un utente riceve un messaggio presumibilmente urgente, come l'email di cui sopra. Spesso il messaggio include una ricevuta per un acquisto importante e sembra essere inviato da un'azienda legittima. Il destinatario viene invitato a chiamare un numero di telefono indicato nell'email per annullare la transazione o contestare l'acquisto.

Se l'utente chiama il numero di telefono indicato nell'email, un falso rappresentante del servizio clienti lo guiderà a un sito web o un negozio di applicazioni mobili. I passaggi successivi osservati dai ricercatori di Proofpoint sono diversi: download di malware, trasferimento di denaro o attivazione di un accesso remoto per le vittime.

Microsoft non nota questi messaggi perché non includono payload o URL dannosi.



SEZIONE 3

CONDIVISIONE DI FILE DANNOSI

Gli attacchi di condivisione di file dannosi sono uno dei tipi di attacchi basati su URL più comuni. I dati interni sulle minacce di Proofpoint mostrano che gli URL sono utilizzati nei tre quarti delle minacce informatiche. Gli URL di condivisione di file vengono utilizzati in oltre il 50% di questi attacchi.

Poiché gli utenti ritengono affidabili servizi come Microsoft OneDrive e Microsoft SharePoint, i criminali informatici utilizzano frequentemente i link a tali servizi. Microsoft si trova in una posizione unica quando si tratta di questi attacchi. Non solo ospita inavvertitamente questi file dannosi, ma permette anche che passino attraverso le sue soluzioni di sicurezza dell'email.

Nel 2021, abbiamo scoperto che oltre 45 milioni di minacce basate su URL inviate ai nostri clienti includevano contenuti dannosi ospitati da Microsoft.

Ambiente:
Microsoft 365

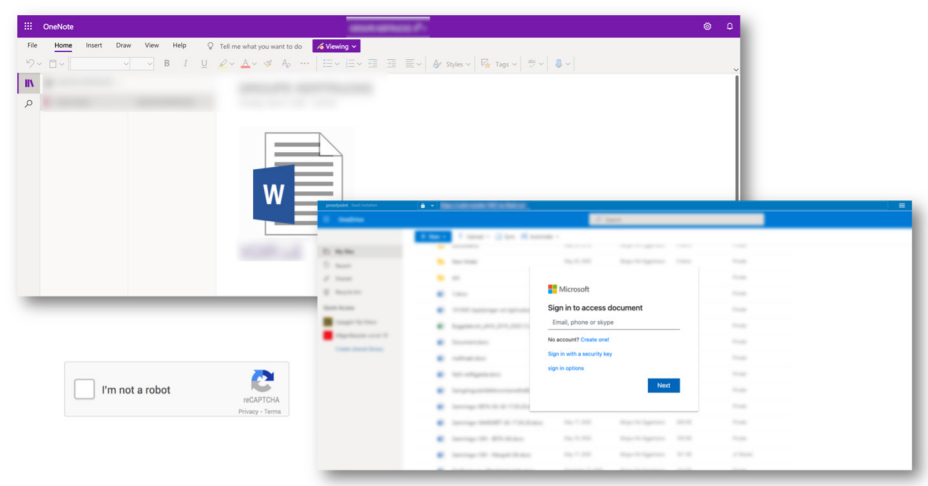
Categoria della minaccia:
condivisione di file basata su URL

Tipo di attacco:
phishing delle credenziali d'accesso

Obiettivo:
utenti di caselle email condivise

Phishing delle credenziali di accesso di OneNote

In base ai dati di Proofpoint[5], l'utilizzo di CAPTCHA da parte dei criminali informatici è aumentato di 50 volte in un anno. In questi attacchi, i criminali informatici cercano di rubare le credenziali d'accesso degli utenti inviando loro link a documenti fasulli. Quando gli utenti fanno clic su questi link, viene visualizzato un CAPTCHA. Dopo aver selezionato la casella, l'utente viene indirizzato su una pagina Microsoft fasulla in cui viene invitato a inserire le proprie credenziali d'accesso.



Esempio di pagina Microsoft OneNote che include un link a un falso documento Word.

5 Proofpoint, report "Il fattore umano", 2022.

In questo esempio, un criminale informatico ha finto di essere un fornitore di terze parti che stava inviando una richiesta alla casella email condivisa di un'azienda di telecomunicazioni. Inviando un link a un falso documento Word contenente un CAPTCHA, il criminale informatico mirava a convincere gli utenti della casella email a rivelare le proprie credenziali d'accesso. Trasmesso tramite OneDrive, il link alla pagina dannosa aggirava i controlli di sicurezza nativi di Microsoft.

È sorprendente che, anche dopo la segnalazione di Proofpoint, la pagina OneDrive fosse ancora attiva un mese dopo. Questa è solo una dei milioni di pagine di condivisione di file fraudolente che impersonano il marchio di Microsoft ogni mese.

Ambiente:
Microsoft 365

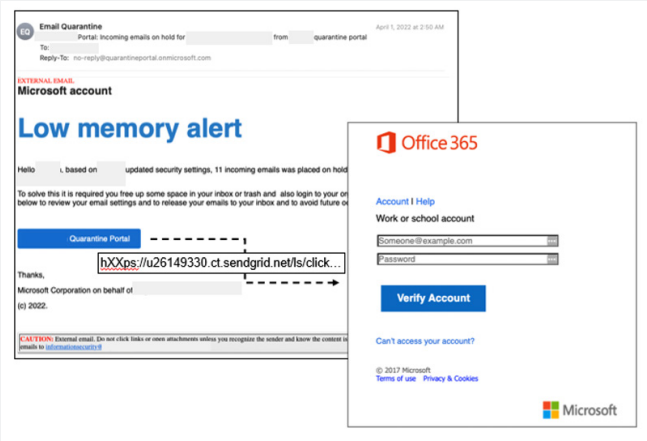
Categoria della minaccia:
abuso di servizi cloud legittimi

Tipo di attacco:
phishing delle credenziali d'accesso

Obiettivo:
utenti di Microsoft 365

Phishing delle credenziali d'accesso tramite l'utilizzo abusivo di servizi cloud legittimi

Il furto delle credenziali di accesso a Microsoft 365 è una tattica comunemente utilizzata dai criminali informatici per violare gli account degli utenti. Una volta preso il controllo dell'account della loro vittima, i criminali informatici sono in grado di ottenere informazioni che permettono loro di inviare messaggi molto convincenti. Di conseguenza, sono in grado di rubare dati preziosi e appropriarsi di fondi.



Esempio di furto delle credenziali di accesso che imita il marchio Microsoft tramite un servizio cloud legittimo.

In questo esempio, il criminale informatico ha utilizzato SendGrid come host e inviato un messaggio da un dominio Microsoft contraffatto (onmicrosoft.com) per farlo sembrare legittimo. In fondo al messaggio, ha persino incluso Microsoft Corporation nella firma.

Vale la pena notare che quando i criminali informatici utilizzano servizi cloud legittimi, i loro attacchi spesso non vengono rilevati da Microsoft. Ciò è dovuto al modo in cui Microsoft gestisce i link. La funzione Collegamenti sicuri di Microsoft non effettua il sandboxing predittivo nel momento in cui gli utenti fanno clic. Si basa unicamente sulla reputazione, il che significa che non è in grado di rilevare le nuove minacce che provengono da servizi cloud e di condivisione dei file legittimi.

SEZIONE 4

TAKEOVER DEGLI ACCOUNT

Gli attacchi di takeover degli account sono una tattica comunemente utilizzata dai criminali informatici. In questi attacchi, un criminale informatico ruba le credenziali d'accesso dell'account di un utente in modo da poter assumere la sua identità aziendale. Un singolo set di credenziali d'accesso è estremamente prezioso per i criminali informatici perché può essere utilizzato per accedere all'email, all'archiviazione dei documenti e ad altri servizi di Single Sign-On. Con un tale accesso, gli effetti di un attacco andato a buon fine possono essere molto gravi. Nel 2021, le aziende hanno perso in media 6,2 milioni di dollari a causa di violazioni di account cloud[6]. E questi attacchi sono in aumento. Nel 2022, Verizon ha rilevato che il 76% degli attacchi di social engineering implicava il furto delle credenziali di accesso[7].

6 Ponemon Institute, report "The Cost of Cloud Compromise and Shadow IT" (Il costo delle violazioni degli account cloud e della Shadow IT), 2021.
7 Verizon, "Data Breach Investigations Report" (Report sulle violazioni dei dati), 2023.

Ambiente:
Microsoft 365

Categoria della minaccia:
basata su URL

Tipo di attacco:
furto delle credenziali d'accesso

Obiettivo:
servizio clienti

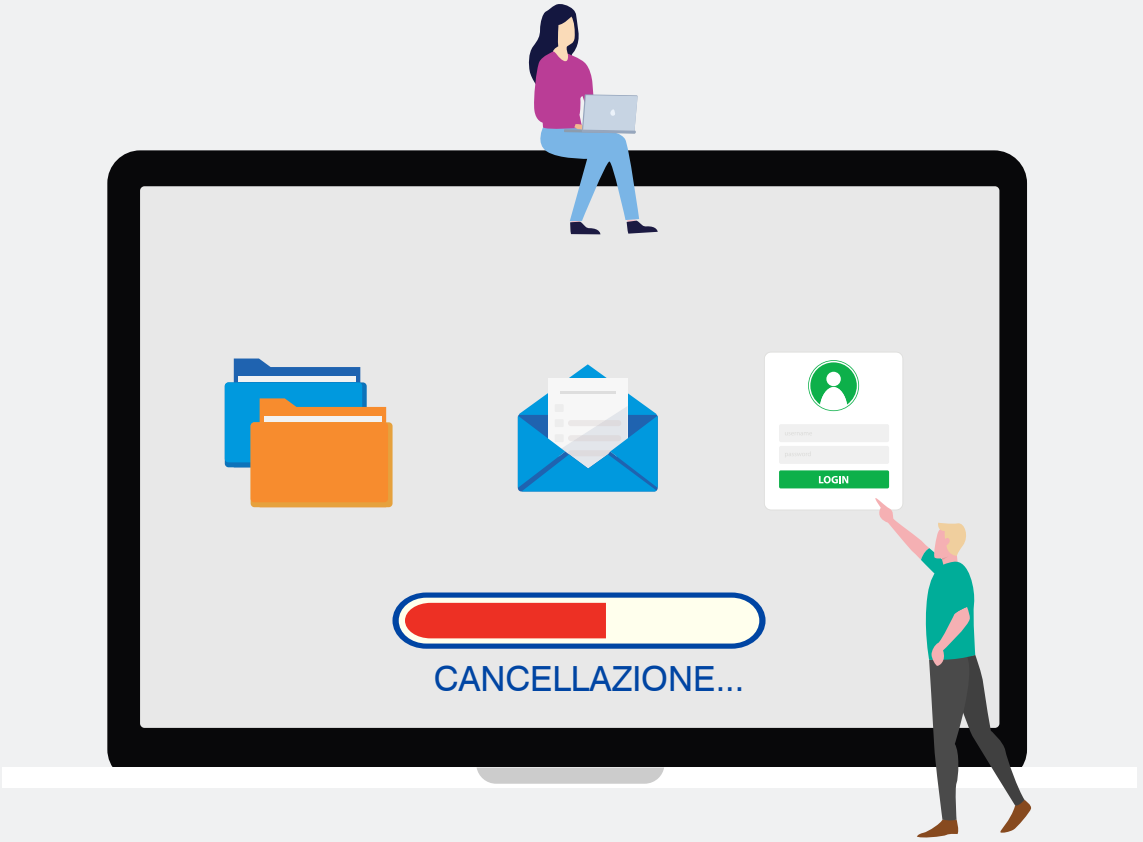
Attacco di raccolta delle credenziali di accesso di Microsoft 365

Molti tentativi di furto delle credenziali d'accesso utilizzano la stessa tattica: imitano Microsoft per aggirare le sue difese perimetrali. Lo sfruttamento della familiarità e della fiducia che riponiamo nei grandi marchi è una delle forme più semplici di social engineeering. Molti criminali informatici abusano del marchio Microsoft. Secondo alcune ricerche condotte da Proofpoint, Microsoft occupa quattro delle prime cinque posizioni per quanto riguarda i marchi più abusati nel 2022[8].

Esempio di attacco di raccolta delle credenziali di accesso.

8 Proofpoint, report "Il fattore umano", 2023.

Questo tentativo di furto di credenziali ha eluso i controlli nativi di sicurezza dell'email di Microsoft. Il criminale informatico ha inviato un messaggio a un collaboratore del servizio di assistenza clienti fingendo di essere un membro del personale dell'assistenza informatica. Per sembrare autentico, il messaggio del criminale informatico includeva un nome visualizzato riconoscibile e il marchio Microsoft. Proofpoint osserva spesso i criminali informatici utilizzare un URL legittimo (in questo caso, sendgrid.net) per aggirare le funzionalità di analisi degli URL di Microsoft.



Ambiente:
Microsoft 365

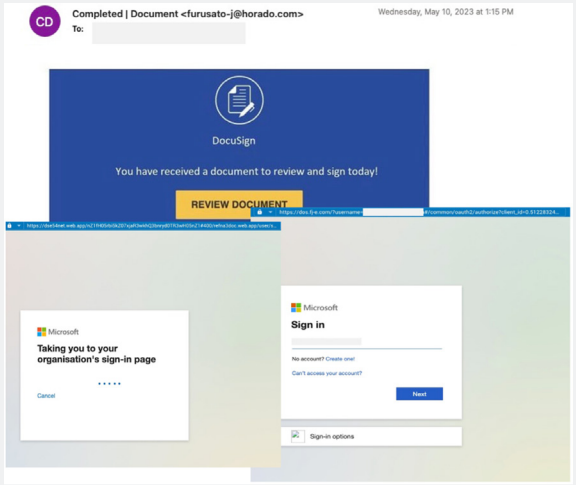
Categoria della minaccia:
phishing dell'autenticazione a più fattori (MFA)

Tipo di attacco:
phishing delle credenziali d'accesso

Obiettivo:
utenti di Microsoft 365

Phishing dell'autenticazione a più fattori (MFA)

L'autenticazione a più fattori (MFA) non è più sufficiente per impedire gli attacchi di takeover degli account. I criminali informatici sono sempre più abili nell'aggirarla. Secondo le ricerche condotte da Proofpoint, durante il picco di attività, l'elusione dell'autenticazione a più fattori ha rappresentato più di un milione di messaggi al mese nel 2022[9].



Esempio di phishing dell'MFA con un URL che reindirizza a una falsa pagina di login di Microsoft.

Questo attacco ha eluso i controlli di sicurezza nativi di Microsoft perché sembrava una pagina DocuSign con un link che consentiva all'utente di apporre la propria firma. Invece di indirizzare l'utente su DocuSign, l'URL punta a una falsa pagina di login Microsoft.

Per portare a termine questo attacco, il criminale informatico ha utilizzato EvilProxy, un framework di phishing che utilizza un reverse proxy per personalizzare le landing page per ogni destinatario e raccogliere le credenziali d'accesso e aggirare la protezione MFA. Questo kit è relativamente nuovo ed è disponibile per la vendita sui forum di exploit. Una volta raccolte le credenziali di autenticazione a più fattori, fornisce un accesso persistente a un account, anche se la password viene reimpostata.

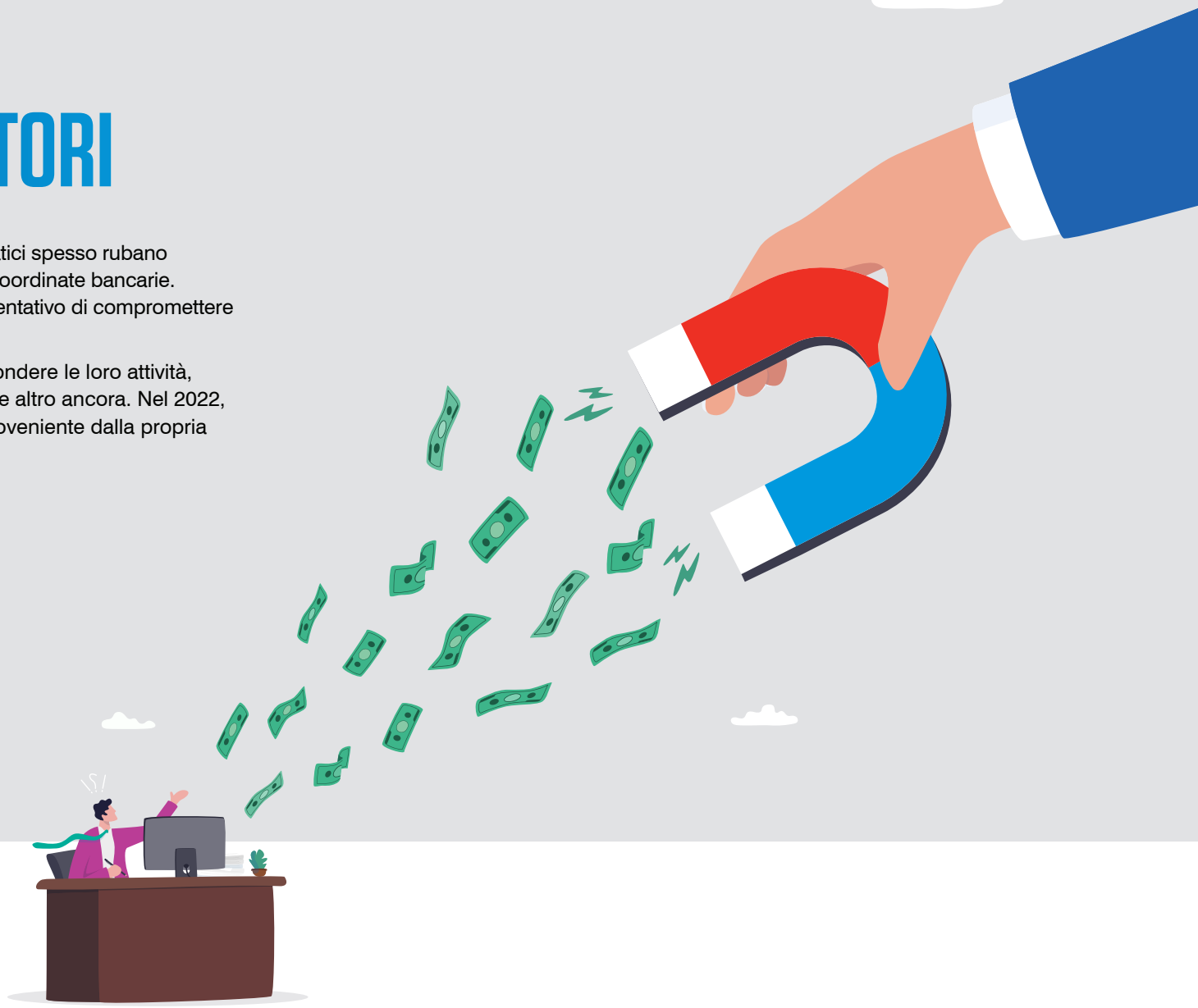
9 Proofpoint, report "Il fattore umano", 2023.

SEZIONE 5

VIOLAZIONE DEGLI ACCOUNT DEI FORNITORI

Come già discusso, in caso di attacchi BEC, i criminali informatici spesso rubano l'identità dei fornitori per inviare fatture fasulle o modificare le coordinate bancarie. Possono anche attaccare fornitori e altre terze parti fidate nel tentativo di compromettere gli account dei tuoi collaboratori o rubare denaro e dati.

Una volta entrati nella tua rete, creano regole email per nascondere le loro attività, accedere alla proprietà intellettuale, modificare i dati bancari e altro ancora. Nel 2022, il 69% delle aziende di tutto il mondo ha subito un attacco proveniente dalla propria suppy chain[10].



10 Proofpoint, "State of the Phish", 2023.

Ambiente:
Microsoft 365

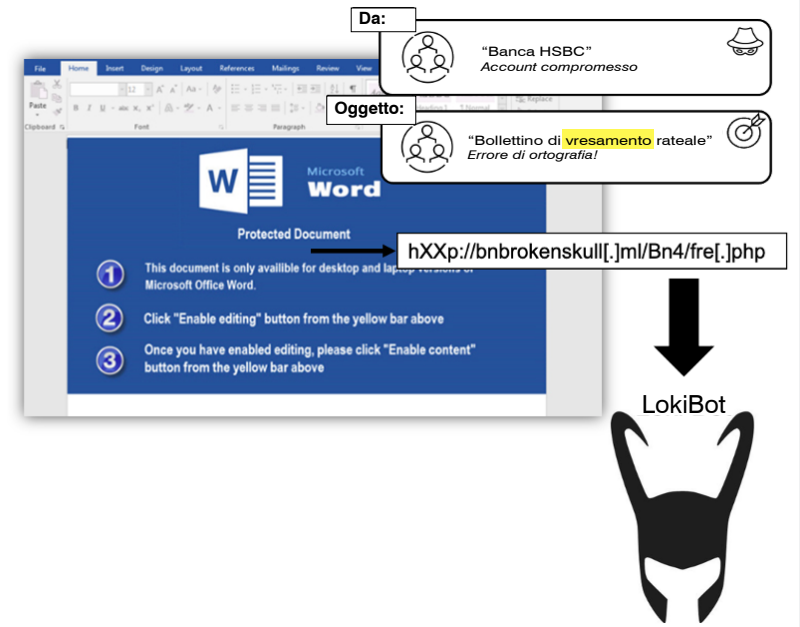
Categoria della minaccia:
basata su URL

Tipo di attacco:
downloader

Obiettivo:
dissimulato in copia nascosta (CCN) dell'email

Allegati dannosi

Il malware è una delle tecniche che permette di entrare in una rete. Recentemente, Proofpoint ha effettuato un'analisi interna dei dati di quasi 4.600 aziende. Abbiamo scoperto che l'85% di queste aziende ha subito frodi da parte di fornitori via email su un periodo di sette giorni che si è concluso il 31 gennaio 2023. Il malware è stato coinvolto in circa il 13% di questi attacchi[11].

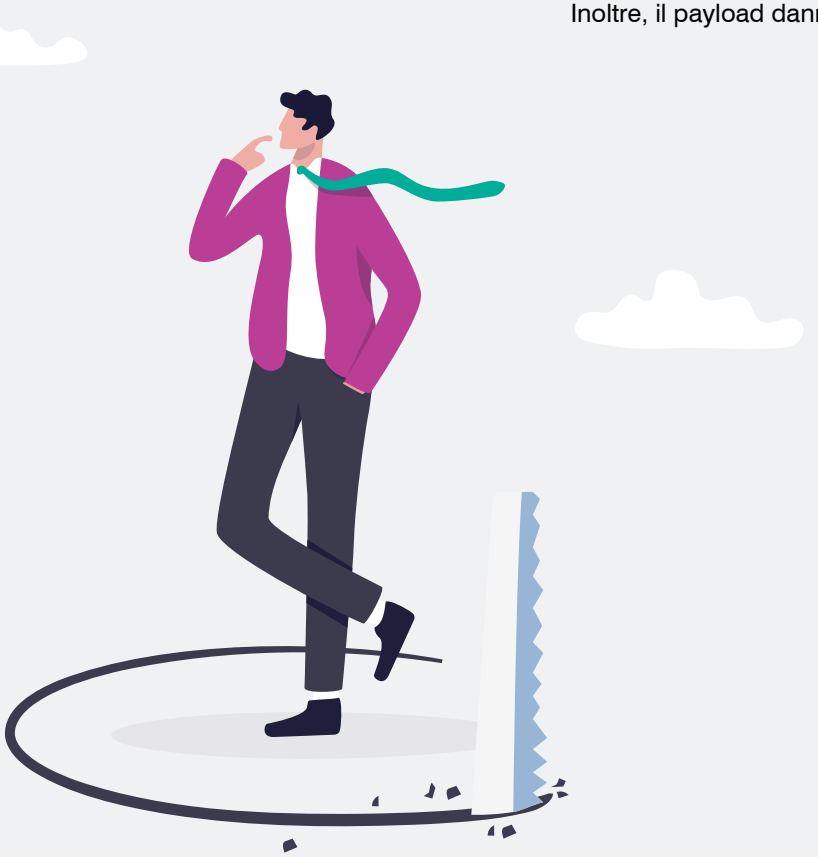


Esempio di attacco LokiBot.

11 Proofpoint, "Hidden Risk: How to Recognize and Prevent Supply Chain Attacks." (Rischio nascosto: come riconoscere e prevenire gli attacchi alla supply chain), aprile 2023.

Questo attacco è stato inviato da un account email compromesso di una banca mondiale. Il messaggio includeva un link a un documento Word che sfruttava varie vulnerabilità dell'Editor di equazioni per scaricare LokiBot, un bot in grado di rubare le password da browser, applicazioni FTP/SSH e account email.

Microsoft non ha rilevato questo attacco perché il messaggio è stato inviato da un dominio legittimo, per cui l'analisi statica della reputazione non lo ha identificato come dannoso. Il messaggio ha anche superato l'autenticazione SPF. Inoltre, il payload dannoso ha utilizzato tecniche di elusione della sandbox e di offuscamento dei file.



Ambiente:
Microsoft 365

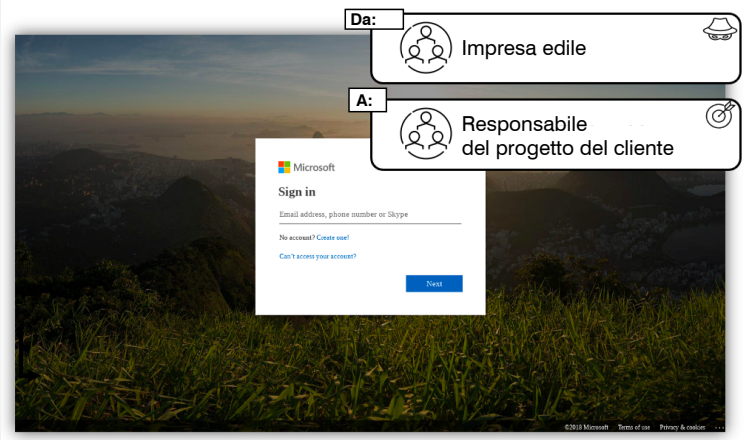
Categoria della minaccia:
basata su URL

Tipo di attacco:
phishing delle credenziali d'accesso

Obiettivo:
responsabile dei progetti dei clienti

Phishing delle credenziali d'accesso

I criminali informatici sfruttano anche gli account dei fornitori compromessi per rubare le credenziali di accesso degli utenti. In questi casi, le conseguenze possono essere ancor più dannose. Sfortunatamente, gli utenti si sentono spesso liberi di interagire con queste minacce perché — anche a un esame più attento— questi messaggi sembrano legittimi, poiché vengono inviati da un dominio che lo è.



Pagina che imitano una pagina di accesso a Microsoft 365.

Questo attacco è stato inviato da un account compromesso che appartiene a un'impresa edile legittima. Questo account invia email regolarmente a un responsabile di progetto che è uno dei suoi clienti. L'email dannosa conteneva un URL verso una pagina che imitava il marchio Microsoft per raccogliere le credenziali d'accesso di Microsoft 365.

Questa minaccia è stata distribuita nella casella email del responsabile di progetto per diversi motivi. Per cominciare, l'analisi della reputazione di Microsoft spesso non rileva i nuovi URL dannosi, anche quando usurpano il marchio Microsoft. Inoltre, questo messaggio è stato inviato dal dominio di un fornitore legittimo, per cui l'analisi statica della reputazione effettuata da Microsoft non ha identificato il mittente come dannoso. La busta non ha innescato alcun caso d'uso evidente di spoofing.

Ambiente:
Microsoft 365

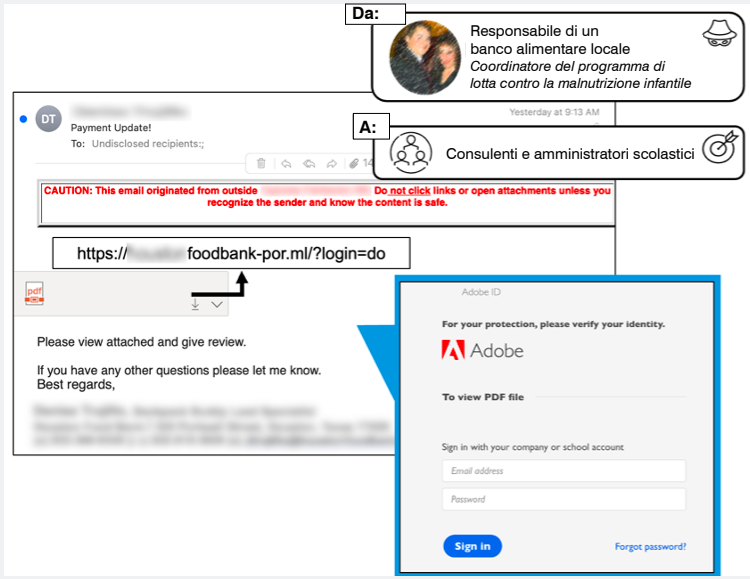
Categoria della minaccia:
basata su allegati, contenente una minaccia basata su URL

Tipo di attacco:
phishing delle credenziali d'accesso

Obiettivo:
consulenti e amministratori scolastici

Attacco tramite un URL incorporato

Non tutti i criminali informatici prendono di mira Microsoft 365. Con l'aumento delle applicazioni cloud, è spesso più facile abusare degli account cloud che sono meno protetti di Microsoft 365. Per aumentare la probabilità che la vittima attivi un attacco, il criminale informatico invia un messaggio dall'account compromesso di un partner.



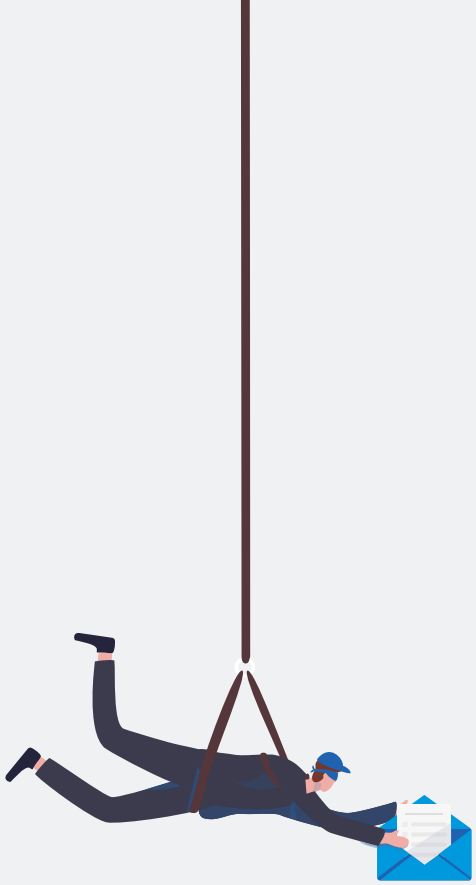
Informazioni sulla minaccia

Attacco di phishing inviato da un account del partner compromesso volto a instaurare un rapporto di fiducia e incoraggiare i destinatari a divulgare le proprie credenziali d'accesso, con conseguente perdita di dati.

Funzionamento

1. Inviato dall'account di un partner compromesso
2. Elusione delle verifiche di autenticazione SPF/DKIM
3. Nome attendibile con corrispondenza regolare
4. Porta alla violazione dell'account

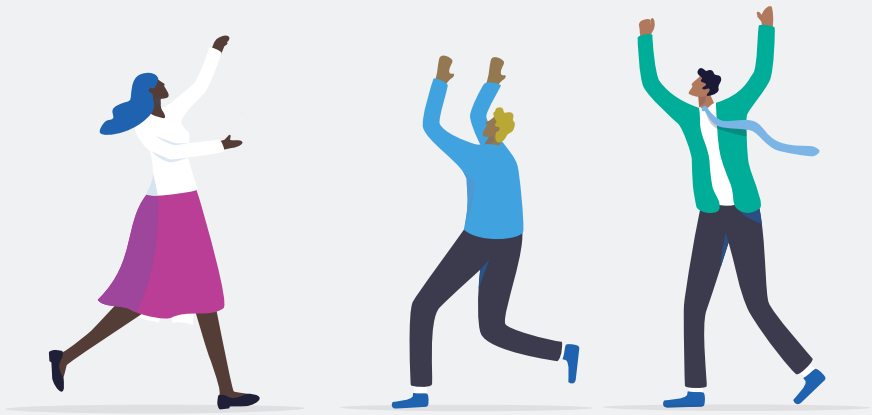
Pagina che imita una pagina di accesso Adobe.



Questo attacco di raccolta delle credenziali di accesso è stato inviato dall'account compromesso di un partner legittimo a cui l'utente inviava regolarmente email. Come illustrato sopra, un link all'interno del messaggio indirizza l'utente su una pagina che imita il marchio Adobe nel tentativo di raccogliere le credenziali d'accesso dell'utente.

Microsoft non è riuscita a bloccare l'attacco per diversi motivi. In primo luogo, è stato inviato dall'account di un partner legittimo, quindi ha superato l'autenticazione SPF/DKIM. Inoltre, poiché esisteva una corrispondenza regolare con questo account, quest'ultimo era considerato affidabile, quindi ha superato l'analisi statica della reputazione di Microsoft.

Inoltre, il criminale informatico è riuscito a eludere il sandboxing inserendo il payload dannoso (URL) nell'allegato e non nell'email stessa. L'URL non è stato rilevato dall'analisi della reputazione di Microsoft, che potrebbe non rilevare nuovi URL dannosi.



Ambiente:
Microsoft 365

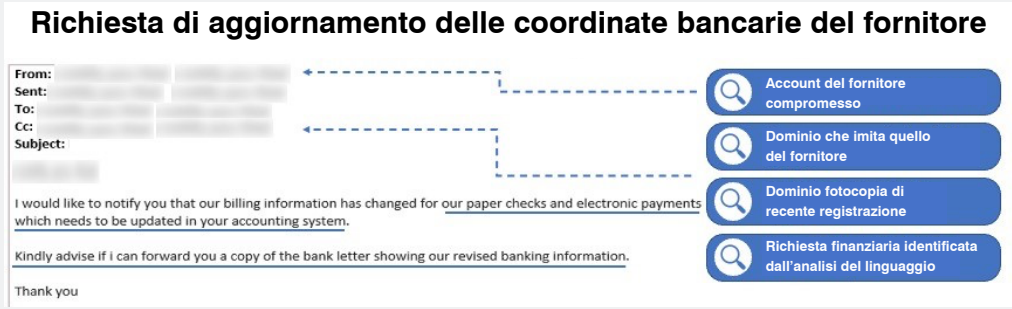
Categoria della minaccia:
social engineering, violazione di un account di un fornitore

Tipo di attacco:
frode delle fatture

Obiettivo:
titolari dell'account

Attacco di furto d'identità di un fornitore

Gli utenti sono più propensi a rispondere a un'email dannosa quando sembra provenire da qualcuno che conoscono. Quando uno di questi attacchi viene inviato da un fornitore apparentemente legittimo, diventa ancora più pericoloso.



Email iniziale del criminale informatico.

Risposta del cliente, inviata a un dominio fotocopia

Il messaggio iniziale è stato inviato a un gruppo mondiale della grande distribuzione dall'account di un fornitore legittimo. Il mittente ha richiesto un aggiornamento delle sue coordinate bancarie. Questa richiesta in apparenza inoffensiva era in realtà dannosa, poiché l'account del mittente era stato compromesso. Il criminale informatico ha cercato di reindirizzare le email di risposta verso un dominio fotocopia appena registrato con l'obiettivo di intercettare le informazioni sensibili e dirottare i pagamenti.

Microsoft non ha fermato questa minaccia perché è stata inviata da un cliente legittimo e ha anche superato i controlli di autenticazione SPF/DKIM. Inoltre, poiché esisteva una corrispondenza regolare con questo account, quest'ultimo era considerato affidabile, quindi ha superato l'analisi statica della reputazione di Microsoft.

CONCLUSIONI

Le funzionalità di sicurezza integrate di Microsoft 365 sono un buon punto di partenza per mantenere protetta la tua azienda, ma con il moltiplicarsi e l'evolversi delle minacce, potrebbero essere necessari ulteriori livelli di protezione.

I criminali informatici non dipendono più da tecniche isolate. Al contrario, combinano tattiche avanzate per sfruttare le persone. Sono anche alla ricerca di relazioni di cui approfittare, fiducia di cui abusare e accessi da sfruttare. Per bloccarli è necessario un approccio a più livelli incentrato sulle persone che copre l'intera catena d'attacco.

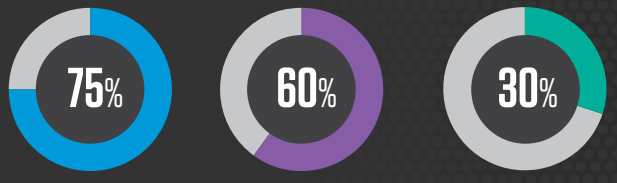
Per saperne di più su come Proofpoint può rafforzare la sicurezza nativa di Microsoft 365 e proteggere i tuoi collaboratori dagli attacchi informatici avanzati, visita il sito all'indirizzo proofpoint.com/it.

Perché scegliere Proofpoint

Ogni giorno, analizziamo oltre:

2,6 MLD DI EMAIL	**49 MLD** DI URL	**1,9 MLD** DI ALLEGATI
1,7 MLD DI MESSAGGI MOBILE	**430 MIO** DI DOMINI WEB	**143.000** ACCOUNT SOCIAL MEDIA

Le nostre soluzioni sono state adottate da oltre:



DELLE AZIENDE FORTUNE 100

DELLE AZIENDE FORTUNE 1000

DELLE AZIENDE FORTUNE GLOBAL 2000

8.000 GRANDI AZIENDE

200.000 PICCOLE IMPRESE

PER SAPERNE DI PIÙ

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