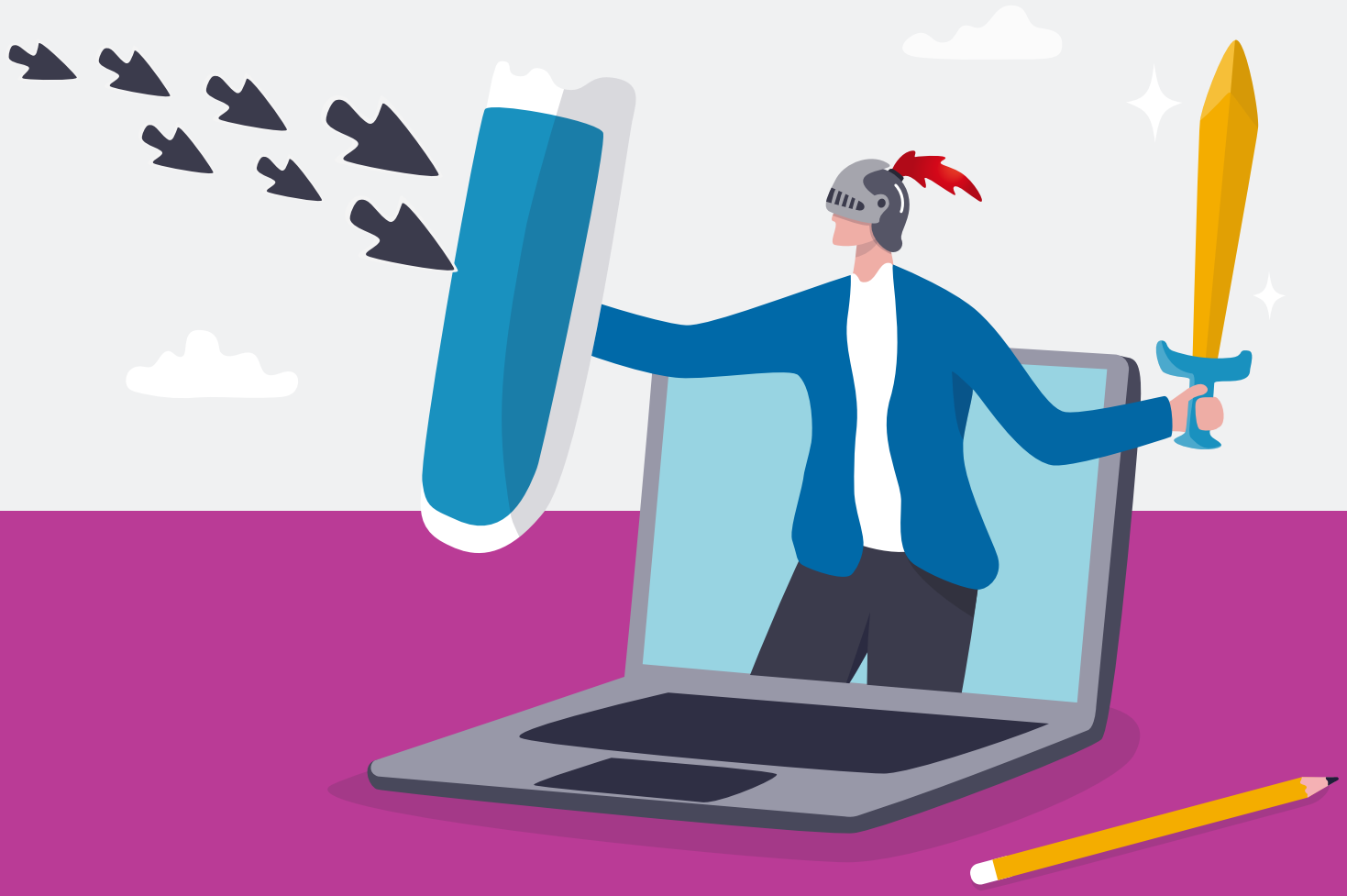
proofpoint.

EBOOK

Cinque attacchi informatici reali e come neutralizzarli

vol. 2: attacchi tecnici



proofpoint.com/it

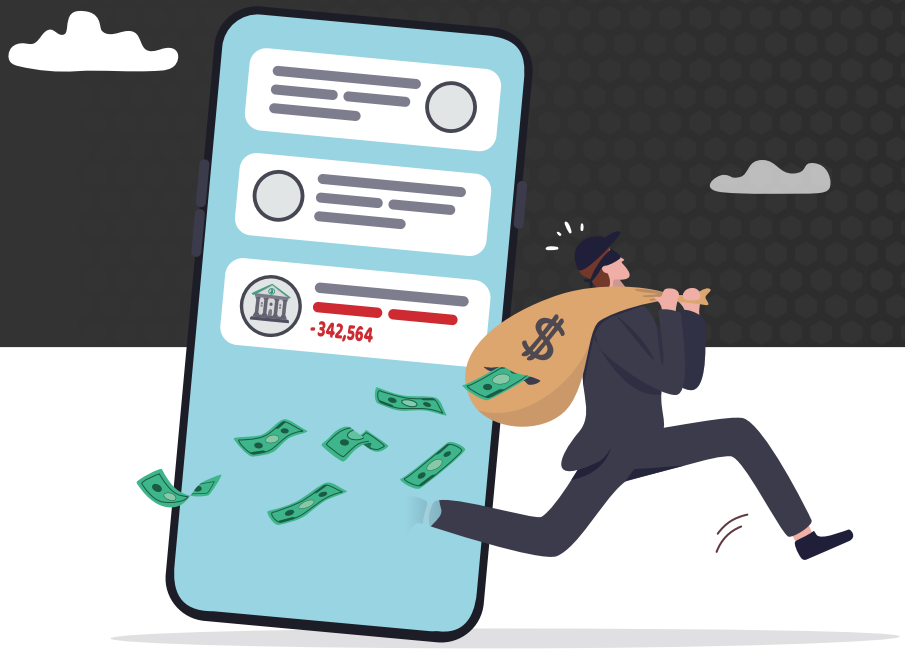
Introduzione

I criminali informatici sono astuti ed estremamente motivati. Perché non dovrebbero esserlo? Operano in un settore in forte crescita dove i rischi sono bassi e i vantaggi così elevati che, secondo le previsioni, entro il 2027 il crimine informatico costerà al mondo 23.800 miliardi di dollari all'anno[1].

Con una tale prospettiva di guadagno, la creatività dimostrata negli attacchi informatici sembra infinita. Nuove campagne di malware, attacchi di phishing e ingegnose tattiche di social engineering appaiono ogni giorno, mentre gli addetti alla sicurezza combattono una battaglia impari contro i criminali informatici. Sebbene queste nuove minacce possano sembrare infinitamente varie, hanno tutte dei punti in comune: sono veicolate tramite la posta elettronica e prendono di mira i collaboratori.

In questa serie di eBook abbiamo raccolto alcuni dei più insidiosi attacchi via email attualmente in circolazione. Molti di questi sono riusciti a eludere le difese di diversi strumenti di sicurezza prima di essere rilevati. Per aiutarti a comprenderne il motivo, ti illustriamo passo-passo ogni attacco per mostrarti il funzionamento di ciascuno e il modo in cui i criminali informatici hanno cercato di sfruttare le vulnerabilità umane. Poi ti spieghiamo come sono stati neutralizzati.

Nel precedente volume 1 abbiamo trattato gli attacchi che utilizzano il social engineering. Nel volume 2 prendiamo in considerazione gli attacchi più tecnici.



1 Forum Economico Mondiale. "2023 Was a Big Year for Cybercrime – Here's How We Can Make Our Systems Safer" (Il 2023 è stato un ottimo anno per il crimine informatico. Ecco come rafforzare la sicurezza dei nostri sistemi), gennaio 2024.

Sommario

1 Il toolkit di phishing EvilProxy 4

2 L'attacco di SocGholish 9

3 Il phishing tramite codici QR 15

4 La manipolazione della MFA 20

5 L'attacco tramite codice QR multilivello 24

6 Conclusioni 28

CAPITOLO 1

Il toolkit di phishing EvilProxy

EvilProxy è un toolkit di phishing che permette di rubare le credenziali di accesso degli utenti e i token dell'autenticazione a più fattori (MFA).

Funziona occultandosi dietro una pagina web legittima. Quando un utente si collega a una pagina di phishing, gli presenta una pagina di accesso fasulla che ha l'aspetto e il funzionamento del portale d'accesso reale. Quando l'utente accede, EvilProxy acquisisce le credenziali d'accesso e il token della sessione di autenticazione. L'autore dell'attacco può quindi utilizzare tali informazioni per aggirare le protezioni della MFA ed effettuare un accesso al posto dell'utente.

EvilProxy e le altre minacce che eludono l'autenticazione a più fattori si stanno moltiplicando poiché i criminali informatici si adattano ai controlli di sicurezza rafforzati. I metodi tradizionali, come l'analisi della reputazione degli indirizzi IP e degli URL, non sono sufficienti per bloccare queste minacce.

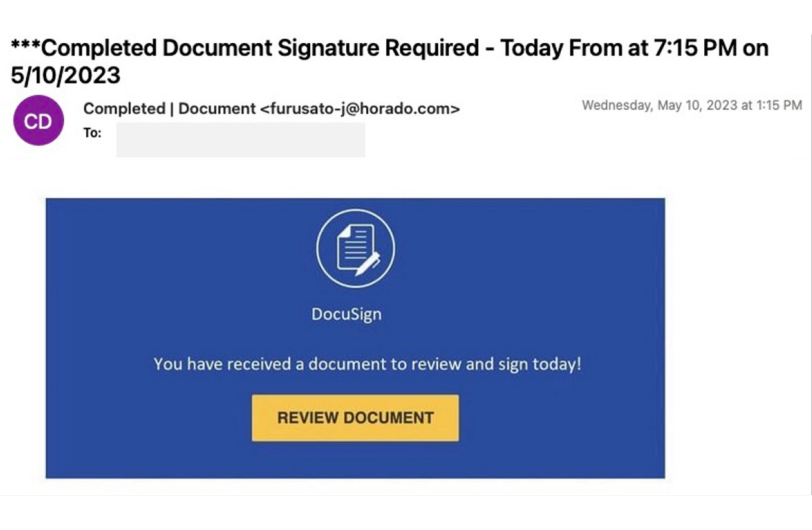
Lo scenario

Nel corso di una valutazione delle minacce via email, Proofpoint ha scoperto che un'azienda del settore tecnologico con 1500 clienti era stata esposta a EvilProxy. L'azienda possedeva già un altro strumento di sicurezza della posta elettronica, che però non era riuscito a rilevare la minaccia.

Svolgimento dell'attacco

Esaminiamo più da vicino come si è svolto l'attacco.

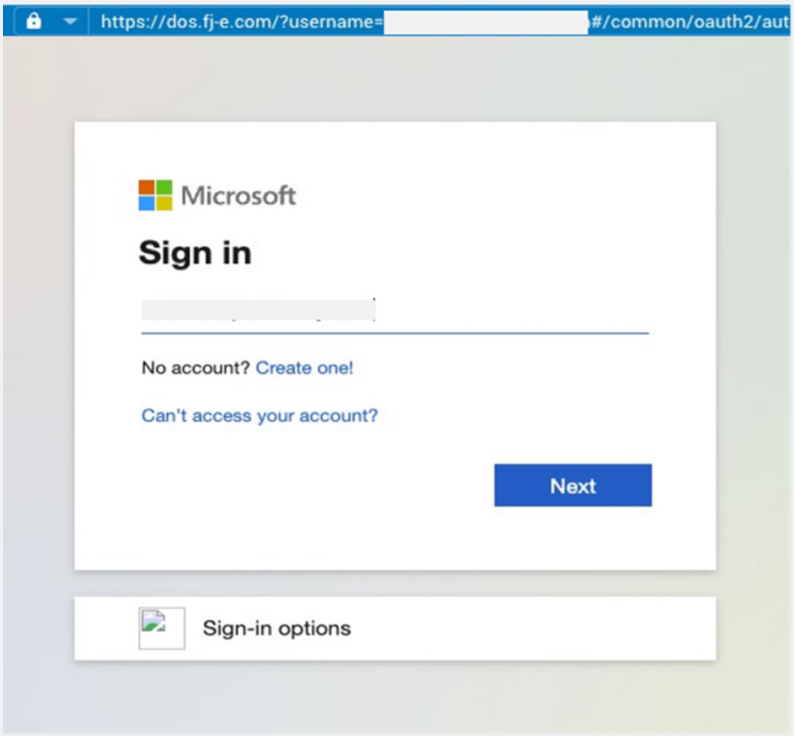
1. **Il messaggio ingannevole.** L'attacco è iniziato con un'email che sembrava un legittimo avviso di DocuSign, comunicante ai destinatari la disponibilità di un documento pronto da firmare. Questo messaggio apparentemente innocuo era in realtà la porta d'accesso a un attacco informatico di tipo avanzato.



L'email ingannevole iniziale ricevuta dal cliente.

2. **L'URL dannoso.** Quando i destinatari hanno fatto clic sull'URL incorporato, sono stati indirizzati alla propria pagina di accesso di Microsoft. Dietro questa pagina era però celato il proxy degli aggressori, che ha così indotto gli utenti a inserire le proprie credenziali.

3. **La struttura di phishing di EvilProxy.** Il motore dell'attacco è stato questo: i criminali informatici hanno utilizzato una tecnica di proxy inverso per intercettare i tentativi di accesso degli utenti attraverso la loro pagina di accesso di Microsoft. In questo modo hanno potuto estrarre segretamente i codici MFA e le credenziali di accesso degli utenti.



La pagina di accesso Microsoft dannosa.

4. **L'elusione della verifica MFA.** Grazie ai codici MFA e alle credenziali di accesso degli utenti, gli aggressori hanno ottenuto libero accesso agli account compromessi. Grazie alla capacità di eludere la verifica MFA, sono riusciti a entrare nell'ambiente aziendale.

Come Proofpoint ha rilevato l'attacco

Proofpoint utilizza il machine learning (ML) avanzato per decifrare il contesto dei messaggi in entrata e analizzarne il linguaggio al fine di individuare potenziali minacce. Stabiliamo se un'email è innocua, dannosa o sospetta analizzando il corpo del messaggio e il contesto. Esaminiamo anche i modelli di invio tipici del mittente. Se l'email contiene dei payload sospetti, Proofpoint li invia a una sandbox per l'analisi approfondita. Questo ci aiuta a individuare i contenuti dannosi, anche se non sono mai stati visti prima.

In questo scenario Proofpoint ha scoperto che il messaggio era sospetto per diversi motivi. Innanzitutto, in genere il destinatario non riceveva email da quel mittente. Inoltre, il mittente chiedeva al destinatario di eseguire un'azione (fare clic sull'URL). Poiché inizialmente non siamo riusciti a capire se l'URL fosse innocuo o dannoso, lo abbiamo preventivamente isolato per ulteriori analisi.

Seguendo l'URL, abbiamo notato che utilizzava una tattica di elusione del reindirizzamento per mascherare la propria natura dannosa. Continuando a seguirlo, il nostro motore URL ha scoperto che conduceva a una pagina web molto somigliante alla pagina di accesso di Microsoft. Sulla base del comportamento di tale pagina web, Proofpoint ha rilevato un framework URL che utilizzava un servizio proxy progettato per rubare le credenziali degli utenti e le risposte MFA in tempo reale. Queste caratteristiche erano coerenti con EvilProxy. Intercettando le credenziali e la domanda/risposta MFA in tempo reale, i malintenzionati possono accedere rapidamente all'account di un utente anche quando la protezione della MFA è abilitata.

Sunto delle osservazioni di Proofpoint sull'email di firma elettronica che hanno portato alla segnalazione dell'email stessa.

Rilevamento della struttura di phishing EvilProxy in Proofpoint.

CAPITOLO 2

L'attacco di SocGholish

Osservato in circolazione fin dal 2018, SocGholish è una variante di malware che continua a prosperare. Dato che utilizza un'ampia varietà di fasi, controlli di idoneità e routine di occultamento, è ancora una delle famiglie di malware più sfuggenti. L'assenza di dettagli sulla scelta degli obiettivi, sulla logica di elusione e sulle procedure specifiche nelle fasi intermedie contribuiscono ad avvolgerlo nel mistero.

Funziona in quattro fasi fondamentali:

Fase 1: iniezioni dannose
Un malintenzionato compromette un sito web legittimo e vi inietta un codice JavaScript dannoso che traccia il profilo degli utenti, al fine di individuare i candidati ideali per ulteriori attacchi.

Fase 2: scaricamento di SocGholish
Se un utente soddisfa determinati criteri, il codice JavaScript introduce di nascosto SocGholish, spesso come un falso aggiornamento del browser. Facendovi clic, SocGholish viene scaricato nel dispositivo dell'utente.

Fase 3: comunicazione con l'esterno
Successivamente il malware comunica con i proxy di comando e controllo per ricevere ulteriori istruzioni.

Fase 4: malware e infezioni successive
SocGholish continua a profilare il dispositivo dell'utente e ripete le comunicazioni con i server di comando e controllo per la distribuzione dei malware successivi. Spesso si tratta di trojan di accesso remoto o di ransomware.

Difendersi da SocGholish è difficile, poiché è molto diffuso ed è in grado di eludere anche gli strumenti di sicurezza della posta elettronica più avanzati. In un solo mese del 2023, Proofpoint ha riscontrato che il malware è sfuggito al rilevamento da parte di altri livelli di sicurezza in migliaia di casi in tutto il mondo.

Lo scenario

Nel corso di una valutazione delle minacce via email, abbiamo scoperto che un'azienda del settore tecnologico con 4000 utenti era stata esposta a SocGholish. Tale minaccia non era stata rilevata dallo strumento esistente per la sicurezza dell'email.

Svolgimento dell'attacco

Esaminiamo più da vicino come si è svolto l'attacco.

1. **Il messaggio iniziale.** Gli utenti hanno ricevuto un'email che li invitava a inviare un articolo per la pubblicazione su una nota rivista accademica. L'email in sé non era dannosa e non era stata falsificata da un malintenzionato. Come è tipico delle campagne di SocGholish, il codice dannoso non si è manifestato finché l'utente non è arrivato al sito web compromesso, ma legittimo.

Follow up: Paper Invitation: [Environment and Social Psychology] (Indexed in Scopus) is Open for Submission

TS

To:

Thursday, June 29, 2023 at 6:05 AM

Dear

Hope this mail finds you well.

We were wondering if you have received our paper invitation for the journal *Environment and Social Psychology*. We are writing to inquire if you are interested in submitting a paper for publication in this journal.

More information can be found on the website:
https://esp.apacsci.com/index.php/esp/index

Benefits of publishing with ESP:
1.Open access (unlimited and free access for readers).
2.Indexed by the Scopus, NLB, Portico, and other databases.
3.Fast Publication combined with thorough peer review.
4.As indicated on the website, the APC of USD 1250 in 2023 applies to submitted papers.
5.We will provide discount for early bird submission:
*Early Bird Submission before July 31, 2023: 90%
*Early Bird Submission before August 31, 2023: 60%
*Early Bird Submission before September 30, 2023: 50%

We cordially invite you to submit a paper. In addition, we would appreciate it if you could recommend this journal to your colleagues. If you are interested, please kindly let us know.

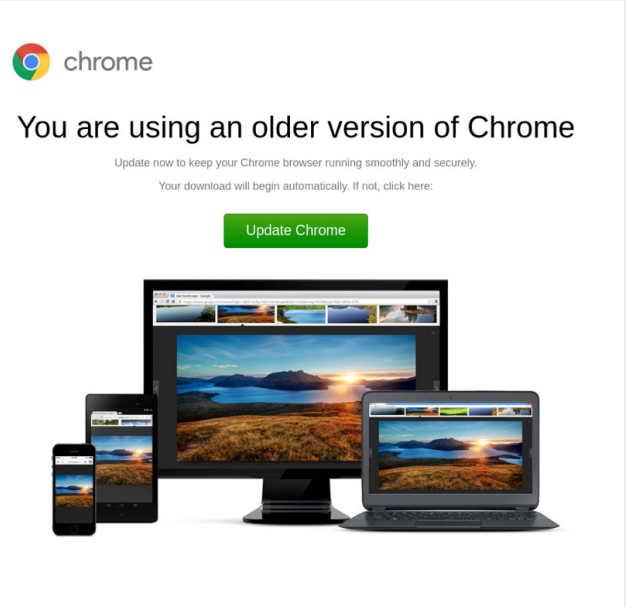
For any questions regarding technical issues or applying discount, please feel free to contact

We look forward to hearing from you.

Kind regards,

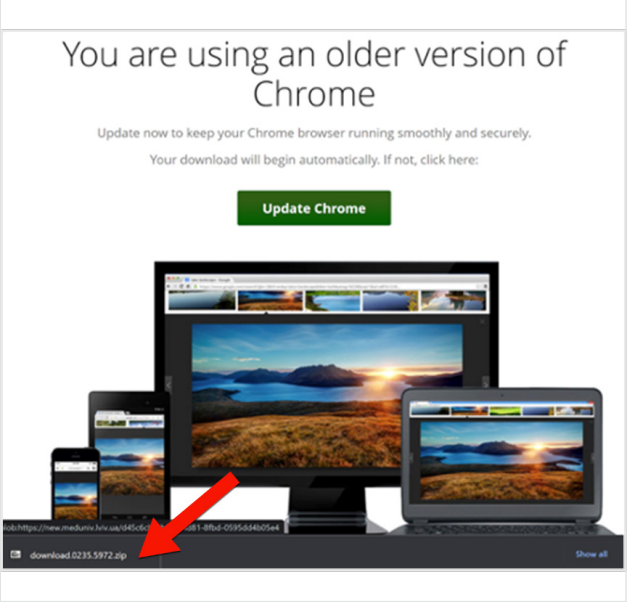
L'email iniziale ricevuta dal nostro cliente.

2. **L'URL compromesso.** Se l'utente faceva clic sull'URL presente nell'email, il codice JavaScript iniettato nella destinazione iniziava a tracciarne il profilo per scoprire se era idoneo a ulteriori attacchi. Ad alcuni utenti selezionati compariva un pop-up a pagina intera che segnalava la necessità di aggiornare il browser.



La falsa richiesta di aggiornamento del browser.

3. **Installazione di SocGholish.** Se l'utente scaricava il pacchetto di aggiornamento, SocGholish stilava un profilo del dispositivo dell'utente, della sua configurazione e degli elementi a cui aveva accesso. SocGholish chiedeva quindi ai proxy di comando e controllo ulteriori istruzioni e se fosse necessario installare un malware successivo.



Il file scaricato tramite il falso aggiornamento del browser.

Perché queste minacce sono difficili da rilevare

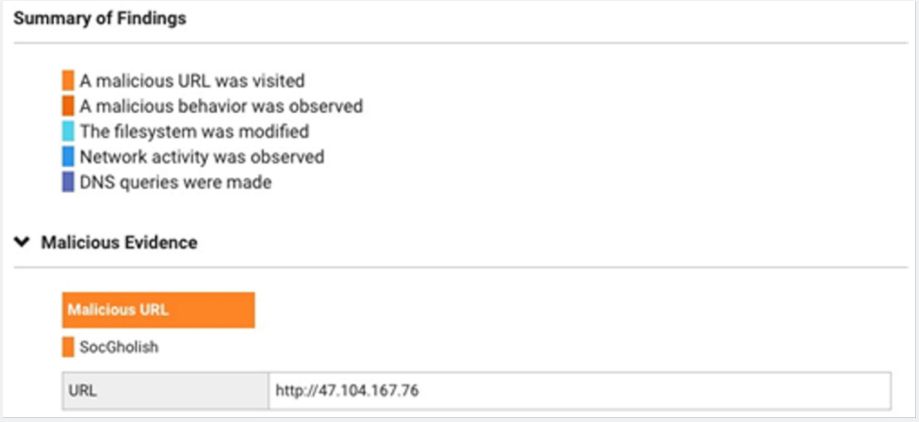
La maggior parte degli strumenti di sicurezza della posta elettronica è in grado di rilevare i JavaScript dannosi, ma SocGholish è evasivo per natura. In particolare, molti strumenti di sicurezza hanno difficoltà a rilevare le tecniche di profilazione. Tra queste rientrano l'analisi dell'indirizzo IP del dispositivo, del sistema operativo, del browser e della lingua locale. Inoltre gli strumenti che si basano esclusivamente sul rilevamento delle anomalie hanno difficoltà con gli attacchi come SocGholish, perché sia il messaggio email sia l'URL sono legittimi.

SocGholish utilizza anche delle tattiche di elusione sensibili alle sandbox. Ciò significa che non si manifesta se rileva un ambiente simulato, come la sandbox di un analista delle minacce. Inoltre gli strumenti di sicurezza della posta elettronica che dichiarano di analizzare le minacce con IA/ML hanno difficoltà a rilevare SocGholish, perché il messaggio di posta elettronica in sé non è dannoso e non verrebbe considerato anomalo neanche in base ai precedenti modelli di invio.

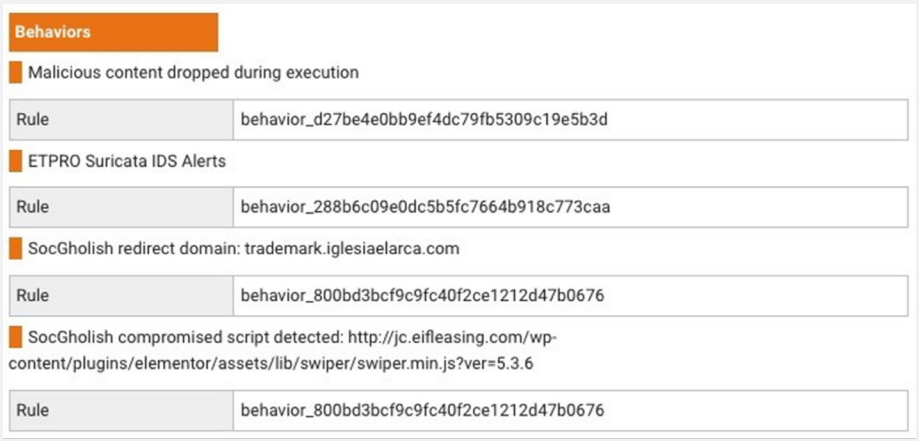
Come Proofpoint ha rilevato l'attacco

Proofpoint utilizza un'analisi approfondita del comportamento degli URL per rilevare i molteplici comportamenti sospetti associati a SocGholish, come la profilazione. Analizzando l'attività di rete possiamo vedere il malware che comunica con i proxy di comando e controllo. Individuiamo anche un'altra tattica già osservata con SocGholish: il reindirizzamento a un servizio DNS e lo sfruttamento di script compromessi.

In questo scenario Proofpoint ha rilevato i modelli di invio insoliti. Abbiamo quindi posto gli URL in una sandbox prima che gli utenti facessero clic su qualsiasi collegamento. Il sandboxing predittivo di URL selezionati è una funzione distintiva ed esclusiva di Proofpoint, nonché uno dei motivi per cui siamo in grado di rilevare le minacce URL nuove, mai viste prima.



Rapporto forense della dashboard di TAP che mostra le attività indicanti un attacco di SocGholish.



Rapporto forense della dashboard di TAP che mostra gli specifici comportamenti di un attacco di SocGholish.

Proofpoint dà inoltre priorità alla scansione frequente e approfondita degli URL. Il criminale informatico TA569, comunemente associato a SocGholish, ha dimostrato tenacia nel mantenere il controllo sui siti iniettati. Abbiamo osservato dei casi in cui pagine web pulite sono state nuovamente compromesse e un sito è stato reiniettato con attacchi simili o diversi.

Per questo motivo poniamo preventivamente gli URL in una sandbox anche dopo che sono stati ritenuti sicuri o sono stati approvati. Il monitoraggio continuo contribuisce a garantire che qualsiasi potenziale compromissione o utilizzazione di un sito come arma venga scoperta rapidamente.

CAPITOLO 3

Il phishing tramite codici QR

Il phishing tramite codici QR sposta il canale di attacco dall'ambiente protetto della posta elettronica al dispositivo mobile dell'utente, che spesso è molto meno sicuro.

I codici QR permettono di non esporre un URL nel corpo di un'email. Questo approccio rende inefficaci la maggior parte delle scansioni di sicurezza della posta elettronica. Inoltre, la decodifica di queste truffe mediante il riconoscimento delle immagini o il riconoscimento ottico dei caratteri (OCR) diventa rapidamente un'attività che richiede molte risorse ed è difficile da attuare su vasta scala.

Lo scenario

Proofpoint ha di recente rilevato uno di questi attacchi presso un'azienda agricola con oltre 16.000 collaboratori. Un malintenzionato aveva creato un inganno di phishing che sembrava contenere informazioni sullo stipendio di uno di loro. Il messaggio invitava il collaboratore in questione a scansionare un codice QR con il proprio telefono cellulare per accedere alle informazioni, anziché a fare clic su un collegamento. Dopo la scansione, una falsa schermata di accesso a SharePoint chiedeva di fornire le proprie credenziali.

Svolgimento dell'attacco

Ecco come si è svolto questo attacco:

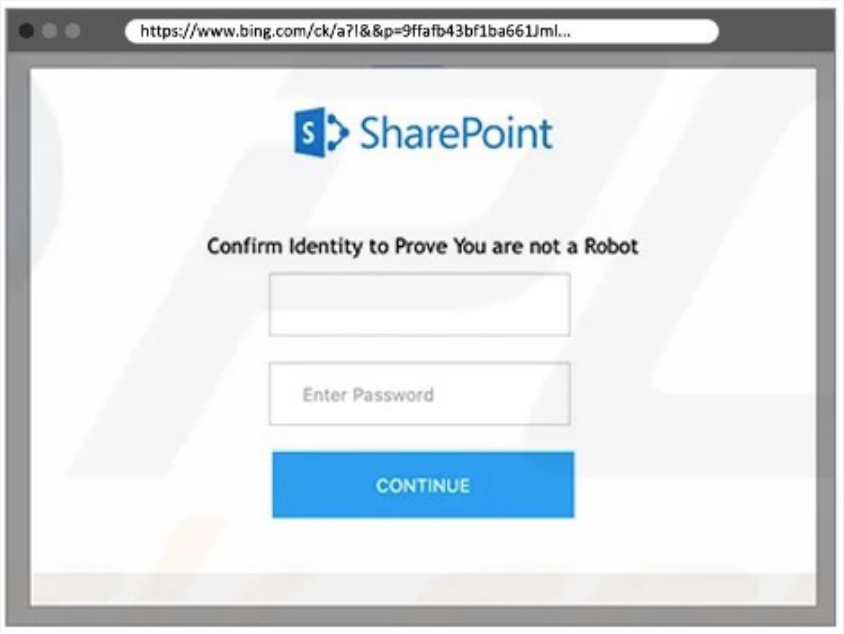
1. **Il messaggio ingannevole.** Il collaboratore ha ricevuto un'email apparentemente dell'ufficio risorse umane dell'azienda, che sosteneva di possedere informazioni sulla busta paga.

Email dannosa bloccata da Proofpoint prima del suo recapito nella casella di posta dell'utente. (Nota: per motivi di sicurezza abbiamo sostituito il codice QR dannoso con uno che rimanda a Proofpoint.com. Il resto del messaggio è una schermata dell'originale censurata.)

2. **Sequenza dell'attacco tramite codice QR.** Al collaboratore è stato chiesto di scansionare il codice QR con il proprio dispositivo mobile.

Sequenza di un tipico attacco tramite codice QR.

3. **L'esca di phishing basata su SharePoint.** Una volta che il collaboratore ha decodificato l'URL, una falsa schermata di accesso a SharePoint ha cercato di indurlo a inserire le proprie credenziali.

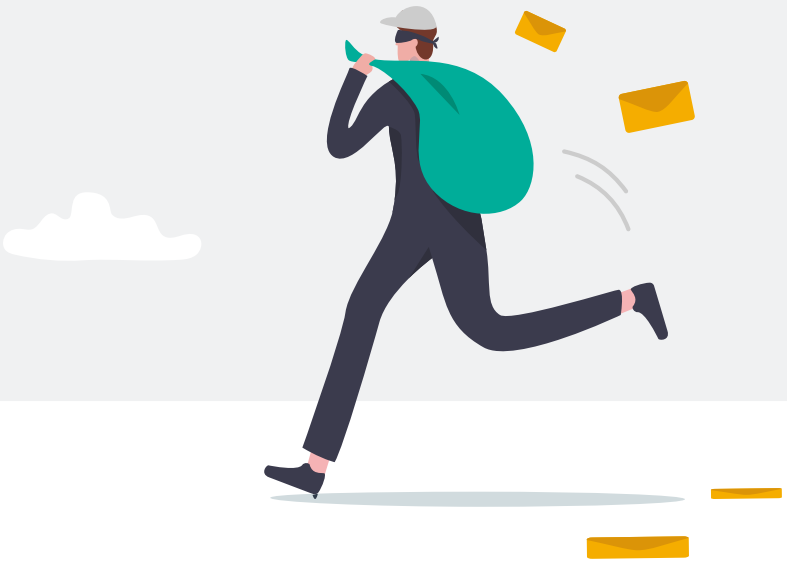


Codice QR decodificato che reindirizza l'utente a una pagina di phishing basata su SharePoint.

Perché queste minacce sono difficili da rilevare

Innanzitutto l'URL di phishing all'interno di un codice QR non è facile da estrarre e scansionare, poi c'è il problema dell'ubiquità dei codici QR. La maggior parte delle firme innocue nelle email contiene logo, collegamenti ai social media incorporati nelle immagini e persino codici QR che puntano a siti web legittimi. Quindi la presenza di un codice QR di per sé non è un segno certo di phishing.

Spesso gli strumenti di sicurezza tentano di fermare tali minacce utilizzando solo modelli di invio insoliti. Tuttavia rappresentano una base debole per condannare un messaggio e possono portare a classificare erroneamente un messaggio benigno come maligno. Questo è spesso il caso degli strumenti di sicurezza della posta elettronica che cercano di affrontare le minacce dopo la consegna.



Come Proofpoint ha rilevato l'attacco

Proofpoint utilizza una combinazione avanzata di segnali e di livelli di analisi per distinguere fra i codici QR benigni e quelli usati come arma. Analizziamo e profiliamo:

- il mittente;
- i modelli di invio del mittente;
- la relazione tra il mittente e il destinatario in base alle loro precedenti comunicazioni.

Tutti questi indizi ci aiutano a identificare i mittenti sospetti e a capire se si stanno comportando in un modo che si discosta dal profilo stabilito. In questo esempio, i nostri sistemi non avevano mai osservato tale mittente comunicare con questa azienda o questo destinatario.

Segnali utilizzati da Proofpoint per identificare il messaggio come una minaccia.

Ma non ci affidiamo solo ai modelli di invio insoliti. Per ridurre il numero di falsi positivi combiniamo molti altri segnali, al fine di estrarre la natura e il metonimo del contenuto del messaggio. Un metonimo è una parola o una frase usata per rappresentare qualcos'altro, ad esempio "la Corona" per indicare la famiglia reale britannica. Questo tipo di analisi ci aiuta a dedurre l'intento di un mittente, indipendentemente dalle parole che usa per esprimerlo.

Analizziamo la cronologia delle email del mittente insieme a un'analisi linguistica e semantica del corpo dell'email. Utilizzando questo approccio abbiamo identificato il linguaggio che rivelava, nell'email, la richiesta al destinatario di compiere un'azione, in questo caso di scansionare un codice QR con il proprio dispositivo mobile.

Oltre all'analisi comportamentale e linguistica, abbiamo rilevato tattiche di inganno anche nelle intestazioni del messaggio. Per ottenere la fiducia della vittima, spesso i malintenzionati cercano di impersonare entità attendibili o altri collaboratori. In questo caso i malintenzionati hanno modificato le intestazioni dell'email in modo che sembrasse provenire dall'ufficio risorse umane e stipendi del datore di lavoro.

Siamo andati anche oltre, e più in profondità, analizzando il codice QR. Utilizzando la tecnologia OCR e di riconoscimento delle immagini nei nostri motori di rilevamento, abbiamo scansionato e identificato come pericolosi gli URL nascosti all'interno del codice QR stesso. Estraiamo sia gli URL sia il testo per garantire che vengano recapitati tutti i messaggi legittimi, mentre quelli che non devono essere recapitati vengano bloccati o corretti.

CAPITOLO 4

La manipolazione della MFA

La manipolazione dell'autenticazione a più fattori (MFA) rappresenta una minaccia significativa per le piattaforme cloud. Si tratta di una tecnica avanzata con cui i malintenzionati introducono il proprio metodo MFA in un account cloud compromesso.

I modi a disposizione per aggirare l'MFA sono svariati. Uno di essi è quello di utilizzare un attacco di tipo Adversary-in-the-Middle (AiTM), in cui il malintenzionato frappone un server proxy tra la vittima e il sito web a cui sta tentando di accedere. In questo modo può rubare sia la password dell'utente sia il cookie di sessione.

L'utente non ha alcun sentore di essere stato attaccato: gli sembra solo di aver effettuato l'accesso al proprio account come al solito. Invece gli aggressori hanno preso tutto il necessario per stabilire la persistenza, ossia per mantenere l'accesso anche se le credenziali MFA rubate vengono revocate o considerate non valide.

Gli attacchi di manipolazione della MFA vengono utilizzati dopo un attacco di takeover di un account cloud (ATO). Purtroppo, la diffusione di questo tipo di attacco è allarmante. Nel 2023 i team di ricerca sulle minacce informatiche di Proofpoint hanno riscontrato che quasi tutte le aziende (96%) sono state prese di mira dagli attacchi basati sul cloud. La compromissione è riuscita nel 60% dei casi, con almeno un account di cui è stato preso il controllo.

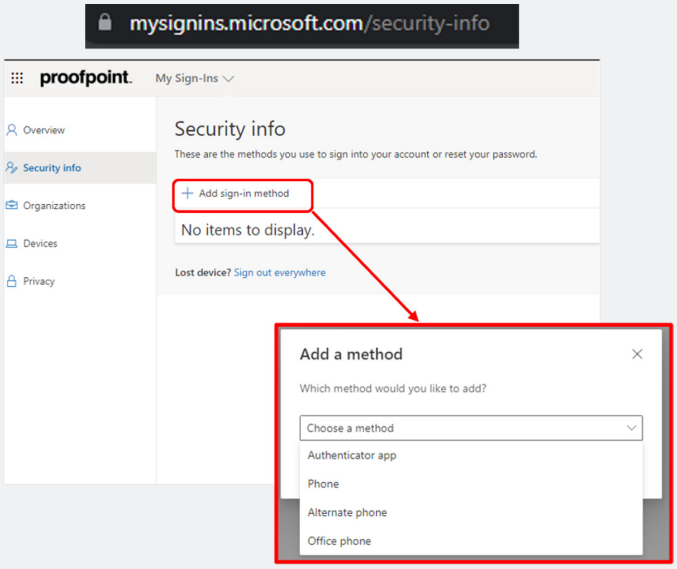
Lo scenario

Proofpoint ha intercettato una serie di attacchi di manipolazione della MFA ai danni di una grande società immobiliare. In un caso i malintenzionati hanno utilizzato un attacco AiTM per rubare le credenziali del controllore finanziario dell'azienda e il cookie di sessione. Dopodiché hanno effettuato l'accesso all'account aziendale dell'utente generando 27 attività di accesso non autorizzato.

Svolgimento dell'attacco

Esaminiamo più da vicino come si è svolto l'attacco.

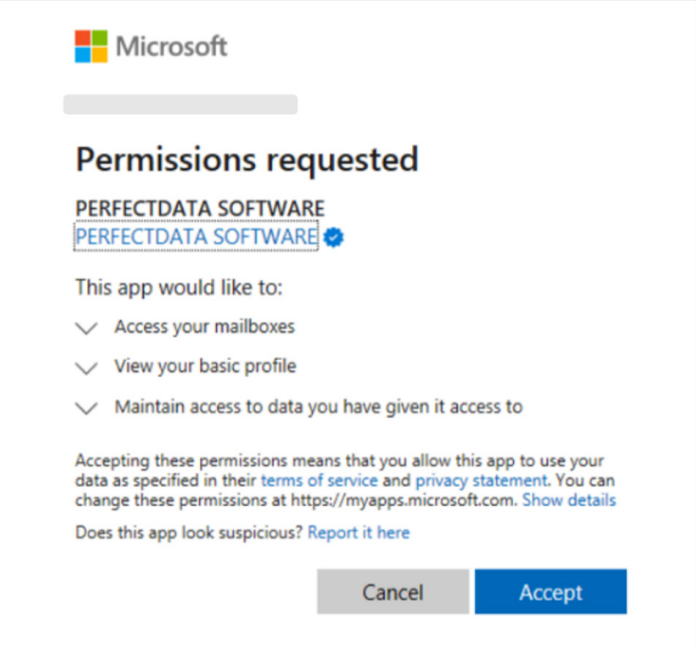
1. **Consolidamento della posizione.** Per aggiungere i propri metodi MFA e compromettere gli account di Microsoft 365 i malintenzionati hanno utilizzato l'app nativa "I miei accessi". Abbiamo osservato gli aggressori registrare la propria app di autenticazione con notifica e codice, subito dopo aver ottenuto l'accesso all'account compromesso con un'esecuzione automatizzata dell'attacco. Ciò, a sua volta, ha consentito loro di consolidare la propria posizione nell'ambiente cloud preso di mira.



Il tipico flusso di manipolazione della MFA tramite l'app "I miei accessi" di Microsoft.

2. **Combinazione delle tattiche di attacco.** Gli aggressori hanno utilizzato un approccio molto sofisticato, combinando la manipolazione della MFA con l'abuso dell'applicazione OAuth. In sostanza, l'abuso di OAuth si verifica quando un aggressore utilizza un'app di terze parti per rubare dati, diffondere malware o creare scompiglio.
3. **Ottenimento dell'accesso persistente.** Gli aggressori abusano di un'app anche per mantenere la persistenza dopo che l'accesso iniziale a un account compromesso è stato interrotto. In questo caso hanno autorizzato l'applicazione apparentemente innocua "PERFECTDATA SOFTWARE" per ottenere un accesso persistente all'account e ai sistemi dell'utente, nonché alle sue risorse e applicazioni. Ecco le autorizzazioni richieste dagli aggressori per questa app:
    - accesso permanente completo alla casella di posta dell'utente;
    - accesso offline ai dati;
    - accesso al profilo dell'utente.

Se queste autorizzazioni fossero state concesse, gli aggressori sarebbero stati liberi di rubare dati sensibili in modo continuativo. Sarebbe stato facile per loro diffondere minacce dannose agli account utente interni o esterni.



Richiesta di autorizzazioni per l'app "PERFECTDATA SOFTWARE", che mostra gli ambiti associati.

Perché queste minacce sono difficili da rilevare

Questi attacchi composti da più fasi sfruttano le legittime funzionalità del cloud e si integrano perfettamente con le normali attività, ecco perché spesso aggirano le misure di sicurezza tradizionali. Concentrandosi su eventi isolati, gli altri fornitori hanno difficoltà a metterli in relazione.

Come Proofpoint ha rilevato l'attacco

Per scoprire dove si sono introdotti gli aggressori e cosa hanno fatto dopo la compromissione Proofpoint ha utilizzato diverse strategie, tra cui l'utilizzo dei feed di intelligence interni e dell'analisi del comportamento degli utenti e delle entità (UEBA).

I nostri passi successivi sono stati l'automatizzare la correzione delle sessioni dannose e il revocare l'abusata app PERFECTDATA SOFTWARE. Ciò ha consentito agli addetti alla sicurezza della società immobiliare di adottare immediatamente le misure correttive.

Durante le indagini su questo caso, il team di ricerca sulle minacce informatiche nel cloud di Proofpoint ha consigliato l'azienda, contribuendo a garantire che tutti i metodi di MFA controllata dagli aggressori venissero rimossi definitivamente, riducendo i rischi futuri.

Dettagli dell'app di terze parti revocata.

CAPITOLO 5

L'attacco tramite codice QR multilivello

In genere, in un attacco tramite codice QR, un codice QR dannoso viene incorporato direttamente in un'email. Di recente però gli aggressori hanno ideato una variante nuova e sofisticata. In questi attacchi multilivello, il codice QR dannoso viene nascosto in quello che sembra un innocuo allegato PDF.

Per rallentare il rilevamento automatico e confondere gli strumenti tradizionali di sicurezza della posta elettronica, gli aggressori utilizzano tattiche di elusione come l'aggiunta di un CAPTCHA sulla pagina di destinazione. Ciò significa che gli strumenti che utilizzano il rilevamento tradizionale della reputazione degli URL si trovano ad affrontare una dura battaglia nel tentativo di identificarli.

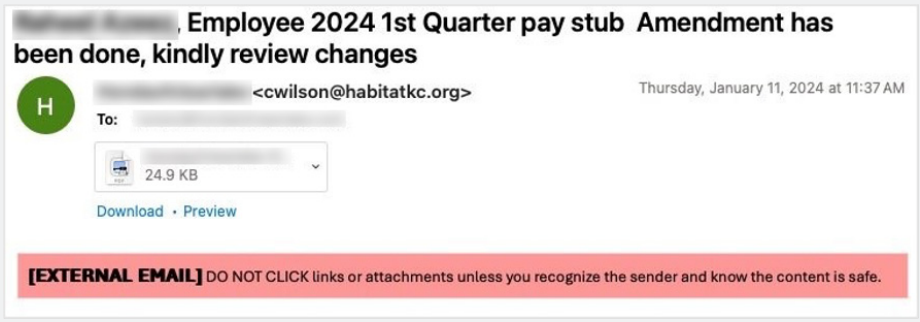
Lo scenario

Proofpoint ha di recente scoperto una di queste minacce durante una valutazione delle minacce presso una casa automobilistica statunitense con 11.000 collaboratori. Gli strumenti di sicurezza esistenti nell'azienda, ossia uno strumento di sicurezza della posta elettronica basato sulle API e la sua protezione nativa, vantavano entrambi le funzionalità di scansione dei codici QR. Tuttavia avevano classificato l'email come pulita, recapitandola all'utente finale.

La minaccia: come si è svolto l'attacco?

Esaminiamo più da vicino come si è svolto l'attacco.

1. **Un'esca ingannevole.** L'email era stata concepita per sembrare legittima e fare leva sull'urgenza legata al periodo di dichiarazione dei redditi. Ciò ha spinto il destinatario ad aprire il PDF allegato.

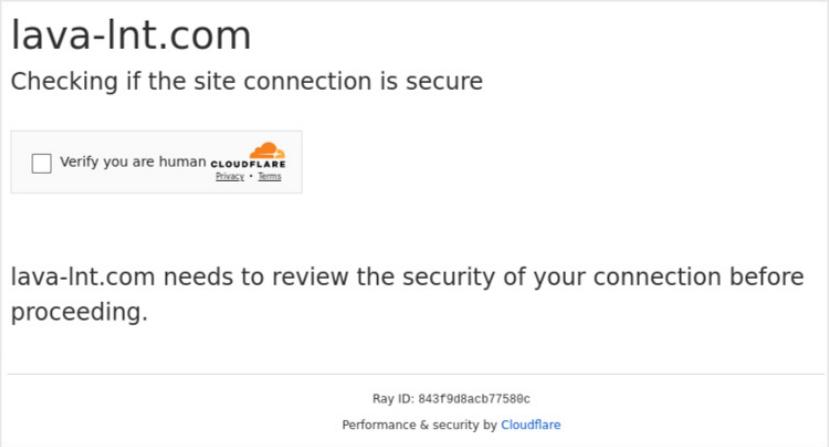


L'email iniziale inviata all'utente finale.

2. **Codice QR dannoso incorporato nel PDF.** A differenza dei precedenti attacchi tramite codice QR, in questo attacco l'URL dannoso non era direttamente visibile nell'email, perché era nascosto nel PDF allegato. Forse il destinatario non si è insospettito data l'ubiquità dei codici QR.

Il PDF allegato con il codice QR incorporato (oscurato).

3. **L'ostacolo dei CAPTCHA di Cloudflare.** L'aggressore ha aggiunto un ulteriore livello di inganno. Ha utilizzato un CAPTCHA di Cloudflare sulla pagina di destinazione partendo dall'URL del codice QR, per nascondere ulteriormente la minaccia sottostante. Questo passaggio mirava a eludere gli strumenti di rilevamento che si basano esclusivamente sull'analisi della reputazione di un URL.



CAPTCHA di Cloudflare nella pagina di destinazione dell'URL del codice QR.

4. **La mossa finale del phishing delle credenziali.** Una volta risolto il CAPTCHA, il codice QR dannoso portava a una pagina di phishing creata per rubare le credenziali dell'utente. Il furto delle credenziali di un utente consente a un malintenzionato di accedere all'account di tale utente per diffondere gli attacchi dall'interno. Può anche utilizzarle esternamente per ingannare partner o fornitori, come appunto nel caso degli attacchi di compromissione della posta elettronica dei fornitori.

Perché queste minacce sono difficili da rilevare

L'uso del riconoscimento ottico dei caratteri (OCR) o di altre tecniche di scansione dei codici QR svolge un ruolo fondamentale nella difesa dalle minacce tramite codici QR. Ma la scansione del codice QR è solo il meccanismo utilizzato per estrarre l'URL nascosto, non funge da meccanismo di rilevamento per distinguere i codici QR legittimi da quelli dannosi.

Molti strumenti, come quelli per la sicurezza della posta elettronica utilizzati dalla casa automobilistica, sostengono di analizzare i codici QR e di estrarne l'URL per l'analisi. Tuttavia non possono eseguire la scansione degli URL contenuti in un'immagine incorporata in un allegato.

Come Proofpoint ha rilevato questo attacco

Pochi strumenti hanno sviluppato la capacità di utilizzare un'analisi URL approfondita su larga scala come quelli di Proofpoint. Noi combiniamo la scansione dei codici QR con uno stack di rilevamento multilivello che sfrutta intelligenza artificiale e machine learning avanzati. Analizzando sia l'URL sia il suo comportamento, possiamo comprendere il contesto dei messaggi di posta elettronica e rilevare quelle minacce URL avanzate che altri strumenti non riescono a individuare.

Ecco cosa abbiamo utilizzato per rilevare e fermare questa minaccia:

Scansione del codice QR. Proofpoint ha utilizzato la scansione dei codici QR per convertire le immagini in un formato leggibile dai computer. Ciò ci ha consentito di estrarre l'URL nascosto per l'ulteriore analisi. La nostra scansione dei codici QR supporta PDF, corpo delle email, immagini, file di Microsoft Word e molto altro.

Indicatori comportamentali. Proofpoint ha analizzato il comportamento degli utenti, il contesto dell'email e la sua natura tematica. Gli schemi riscontrati indicavano un'alta probabilità che l'email fosse dannosa.

Sandboxing degli URL. Ponendo l'URL estratto all'interno di una sandbox, Proofpoint può analizzare elementi visivi, modelli di reindirizzamento, processi negli endpoint, attività in rete, chiamate DNS e processi di CPU e memoria. Possiamo rilevare anche le tattiche anti-evasione come i CAPTCHA. Anche se l'URL sembra pulito, nonostante mostri degli indicatori comportamentali associati ad attività dannose, continuiamo a monitorarlo e a scansionarlo per rilevare eventuali compromissioni o utilizzi impropri in futuro.

CAPITOLO 6

Conclusioni

Tutte queste truffe non fanno che sottolineare la necessità di adottare solide misure di sicurezza informatica multilivello.

Per tenere testa a simili pericoli in costante evoluzione, bisogna adottare un approccio completo alla protezione contro le minacce che prendono di mira i collaboratori:

- **Rileva le minacce prima della consegna.** Il solo mezzo di proteggere gli utenti è di bloccare i messaggi dannosi prima della loro consegna. In base alle ricerche condotte da Proofpoint, un utente su sette fa clic su un'email entro un minuto. Scegli uno strumento che combina algoritmi di machine learning e una threat intelligence avanzata per identificare e bloccare le minacce avanzate.
- **Forma i tuoi utenti.** I tuoi collaboratori, collaboratori interinali e partner sono la tua prima linea di difesa. Assicurati che ricevano il security awareness training per tutti i tipi di attacchi. Ricorda loro di segnalare rapidamente tutti i comportamenti insoliti.
- **Esegui regolarmente le verifiche di sicurezza.** Le verifiche possono aiutarti a identificare le potenziali vulnerabilità nel tuo ambiente. Come parte del lavoro, assicurati di cercare le irregolarità nelle tue configurazioni e nei log d'accesso.
- **Imposta il tuo sistema per monitorare gli errori di configurazione.** Oltre a ricercare gli errori di configurazione, non dimenticarti di attivare la correzione automatica. Potrai così rilevare le modifiche non autorizzate e correggerle prontamente, impedendo ai criminali informatici di stabilire la persistenza nella tua azienda.
- **Crea un piano di risposta agli incidenti.** Identifica diversi scenari d'attacco. Quindi, stabilisci come analizzerai e correggerai gli incidenti. Assicurati di testare la reale efficacia del tuo piano eseguendo regolarmente esercizi di simulazione.

Passi successivi

Oggi più che mai è importante proteggere la tua azienda dalle minacce email in aumento. Adotta un approccio preventivo per proteggere azienda, collaboratori e clienti dagli attacchi avanzati come ransomware, minacce BEC e phishing delle credenziali di accesso.

La valutazione rapida dei rischi legati all'email di Proofpoint ti fornisce visibilità e informazioni complete sulla tua vulnerabilità agli attacchi. Ti aiuta a identificare i collaboratori presi di mira dalle minacce via email nella tua azienda.

Non aspettare che sia troppo tardi per testare la sicurezza della tua email. Contatta Proofpoint per una **valutazione gratuita dei rischi legati all'email.**

PER SAPERNE DI PIÙ

Per maggiori informazioni visita il nostro sito all'indirizzo **proofpoint.com/it**.

INFORMAZIONI SU PROOFPOINT

Proofpoint 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 l'85 delle Fortune 100, 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, Inc. Proofpoint è un marchio commerciale di Proofpoint, Inc. negli Stati Uniti e negli altri Paesi. Tutti gli altri marchi qui menzionati appartengono ai rispettivi proprietari.

proofpoint.

0503-007-05-01 08/24