Report del 2023 di Zscaler ThreatLabz sul phishing

Contenuti

Riepilogo

Le truffe di phishing sono una minaccia in crescita. I metodi adottati dai criminali informatici stanno diventando sempre più sofisticati, e rendono questi attacchi sempre più difficili da individuare e bloccare.

Analizzando 280 miliardi di transazioni giornaliere e 8 miliardi di attacchi bloccati ogni giorno durante tutto il 2022, il team di Zscaler ThreatLabz ha rilevato un aumento del 47,2% dei tentativi di phishing rispetto al 2021; una crescita che, secondo le previsioni, proseguirà anche nel 2023.

È stato registrato un significativo incremento dell'uso dei kit di phishing provenienti dai mercati neri e dei chatbot basati sull'IA, come ChatGPT, che consentono agli aggressori di sviluppare con facilità campagne di phishing più mirate. Il miglioramento del targeting ha consentito di semplificare la manipolazione degli utenti per indurli a compiere azioni che compromettano le loro credenziali di sicurezza. Per questo motivo, gli utenti stessi e le loro organizzazioni sono molto più vulnerabili.

Con la sempre maggiore diffusione di soluzioni basate sull'IA e di tipo PaaS, per i criminali informatici è molto più semplice compromettere le istituzioni e accedere ai dati sensibili aziendali, personali e finanziari a scopo di estorsione. Sebbene oggi molte organizzazioni dispongano di solide infrastrutture di cybersecurity, queste devono essere riesaminate alla luce delle tendenze attuali prendendo in considerazione l'adozione di un approccio zero trust.

Questo report aiuterà a riconoscere le tattiche di social engineering e il sofisticato codice utilizzato negli attacchi di phishing per prevenire costose violazioni dei dati. Nelle prossime pagine, verranno presentate informazioni dettagliate riguardo alle ultime tendenze del phishing, le osservazioni che il team di ThreatLabz ha raccolto nel corso dell'ultimo anno e le best practice che consentiranno alle organizzazioni di difendersi contro tecniche di phishing in continua evoluzione.

I principali risultati del 2022

Nel 2022, gli attacchi di phishing sono aumentati del 47,2% rispetto al 2021.

I marchi di Microsoft, tra cui OneDrive e Sharepoint, l'exchange di criptovalute Binance e i servizi di streaming illegale sono stati i più colpiti.

Stati Uniti, Regno Unito, Paesi Bassi, Russia e Canada sono stati i cinque Paesi che hanno subito più attacchi.

L'istruzione è stato il settore più colpito, con un incremento degli attacchi del **576%**, mentre il settore che aveva subito più attacchi nel 2021, quello della vendita al dettaglio e all'ingrosso, ha registrato una diminuzione del **67%**.

Gli attacchi a tema COVID, che hanno rappresentato il **7,2%** delle truffe di phishing nel 2021, sono scesi ad appena il **3,7%** nel 2022.

Gli strumenti basati sull'intelligenza artificiale hanno contribuito in modo significativo all'aumento degli attacchi di phishing, in quanto hanno abbattuto le barriere tecniche e consentito ai criminali di risparmiare tempo e risorse.

Per indurre le vittime ad aprire allegati dannosi, gli aggressori stanno passando dal phishing via SMS (SMiShing) al phishing basato sulla messaggistica vocale (Vishing).

I sofisticati attacchi AiTM (Adversary-in-Middle) aiutano gli aggressori a bypassare le misure di sicurezza dell'autenticazione a più fattori (MFA).

Le offerte di lavoro false, che colpiscono chi è in cerca di un'occupazione, stanno diventando sempre più diffuse.

I principali obiettivi del phishing nel 2022

Zscaler ThreatLabz ha analizzato i dati relativi a Paesi, settori, marchi e piattaforme, per capire quali sono stati i principali obiettivi del phishing nel corso del 2022.

Tentativi di phishing per Paese nel 2022

I dieci Paesi più colpiti dalle truffe di phishing nel corso dell'ultimo anno sono stati:

1. Stati Uniti
2. Regno Unito
3. Paesi Bassi
4. Russia
5. Canada
6. Singapore
7. Germania
8. Francia
9. Giappone
10. Cina

Gli Stati Uniti, come sempre, sono ancora una volta i più colpiti dagli attacchi di phishing. La nostra ricerca indica che oltre il 65% di tutti i tentativi di phishing si è verificato qui, un dato in aumento rispetto al 60% dell'anno scorso. Nel Regno Unito questi attacchi sono aumentati del 269%.

Nel corso del 2022, diversi Paesi hanno riscontrato un aumento dei tentativi di phishing, tra cui il Canada, che ha registrato un impressionante incremento del 718%. Alcuni esperti di ThreatLabz attribuiscono questo picco al parallelo aumento degli obiettivi nel settore dell'istruzione. La Russia ha rilevato una crescita degli attacchi del 198%, mentre il Giappone del 92%. Al contrario, in Ungheria si è registrato un calo significativo degli attacchi di phishing pari al 90%, mentre a Singapore il totale degli attacchi è diminuito di quasi il 48%.

La diminuzione del numero di attacchi di phishing contro Singapore può essere dovuta all'incremento delle attività del governo in materia di cybersecurity, come le iniziative della Cyber Security Agency (CSA) del Paese. Questa agenzia fornisce linee guida e suggerimenti a privati e aziende su come proteggersi dalle minacce informatiche e, insieme alla Personal Data Protection Commission (PDPC), fa rispettare le leggi e i regolamenti in materia di protezione dati.

Figura 1: attacchi di phishing per Paese nel 2022

Tentativi di phishing per settore nel 2022

Nel corso del 2022, il settore dell'istruzione ha registrato un aumento del 576% dei tentativi di phishing, passando dall'essere l'ottavo settore più colpito al più colpito in assoluto, e superando così il settore della vendita al dettaglio/all'ingrosso che era invece al primo posto l'anno precedente. Gli autori degli attacchi di phishing hanno probabilmente sfruttato i processi di rimborso dei prestiti agli studenti e le richieste di riduzione del debito presentate durante lo scorso anno, facendo leva sulle vulnerabilità insite nell'apprendimento da remoto. Anche il settore finanziario e quello assicurativo hanno registrato un incremento del 273% degli attacchi di phishing nel 2022.

Inoltre, sono cresciuti esponenzialmente i tentativi di phishing rivolti al settore sanitario, che sono passati da poco meno di 31 milioni a oltre 114 milioni. I pazienti che avevano rimandato i propri controlli clinici di routine durante il primo anno della pandemia di COVID-19, nel 2022, hanno ripreso i loro trattamenti sanitari, accedendo ai loro account online e interagendo potenzialmente con aggressori che li hanno colpiti con attacchi di phishing fingendosi organizzazioni sanitarie. Inoltre, per riuscire a compromettere i dati delle organizzazioni sanitarie, gli aggressori che utilizzano i ransomware stanno sfruttando un numero maggiore di tattiche di phishing.

Tuttavia, nel 2022 questi attacchi sono relativamente diminuiti, con il settore del commercio al dettaglio e all'ingrosso che ha registrato un calo del 67% e il settore dei servizi che ha riscontrato una diminuzione del 38%. La riduzione del numero di attacchi contro il settore della vendita al dettaglio e all'ingrosso è probabilmente dovuta a una flessione nel comportamento dei consumatori dopo la forte crescita degli acquisti e della spesa online del 2021.

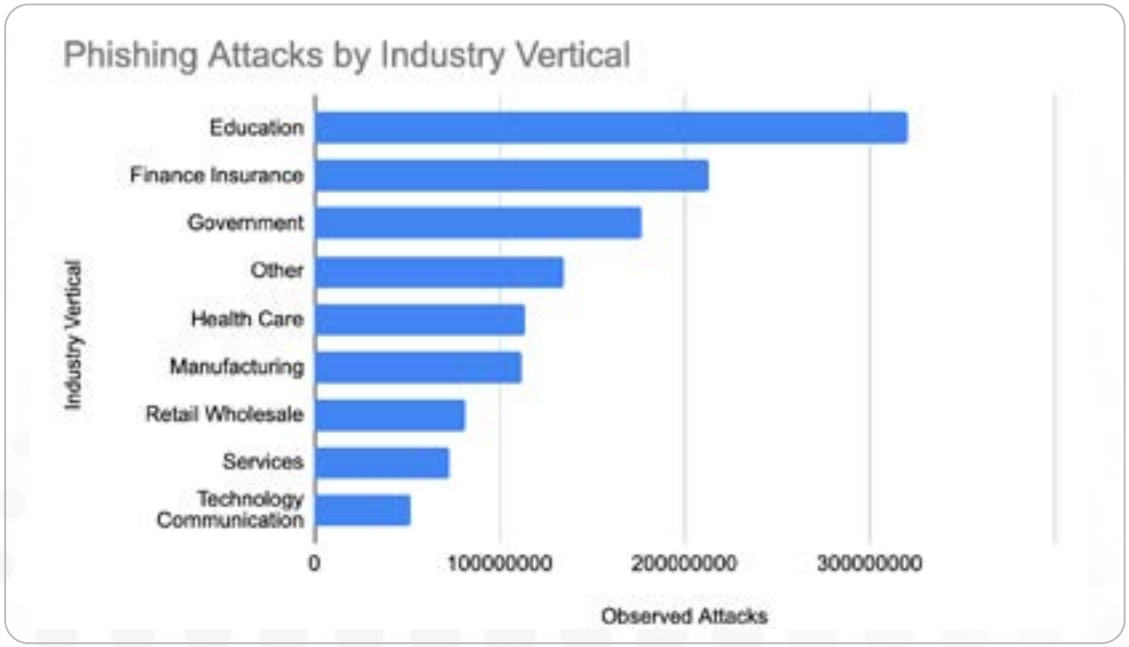
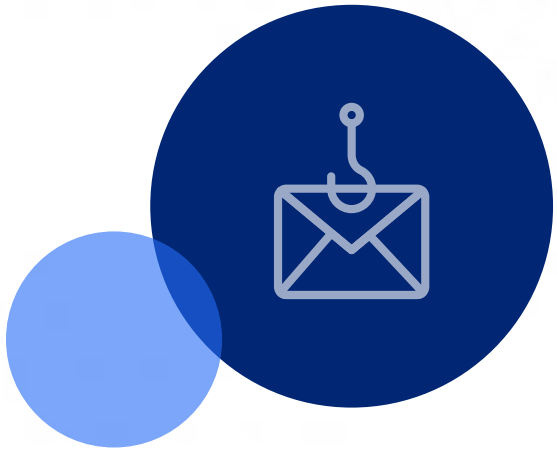


Figura 1: attacchi di phishing per settore nel 2022



I marchi più imitati negli attacchi di phishing del 2022

Spesso, gli operatori degli attacchi di phishing sfruttano le tendenze dei consumatori spacciandosi per marchi famosi, in modo da ingannare chi è più vulnerabile. Le categorie di marchi colpite più di frequente includono: strumenti di produttività, siti di criptovalute, siti di streaming illegale, piattaforme social e servizi di messaggistica, istituzioni finanziarie, siti governativi e servizi di logistica.

Microsoft è stato ancora una volta il marchio più imitato dell'anno, con una percentuale di poco al di sotto del 31% degli attacchi. Il marchio OneDrive è stato coinvolto nel 17% degli attacchi, SharePoint quasi nel 4% e Microsoft 365 in un ulteriore 1,7%. Nel 2022, Zscaler ha rilevato che gli aggressori hanno utilizzato sempre più spesso OneNote, che può essere integrato con OneDrive e altri prodotti Microsoft, per distribuire malware tramite e-mail di phishing. In passato, gli utenti venivano presi di mira impiegando documenti dannosi con macro abilitate, ma nel luglio 2022 Microsoft ha disabilitato le macro per impostazione predefinita su tutte le applicazioni di Microsoft 365 (Office), rendendo questo approccio meno affidabile per la distribuzione di malware.

L'imitazione del marchio dell'exchange di criptovalute Binance ha rappresentato il 17% degli attacchi. Per questi attacchi, gli aggressori si sono spacciati per falsi rappresentanti di clienti di banche o società P2P. I siti di streaming illegale sono stati coinvolti nel 13,6% degli attacchi, con picchi in occasione di eventi sportivi importanti, come la Coppa del Mondo FIFA a novembre e dicembre del 2022.

Sebbene in calo, gli attacchi a tema COVID sono ancora molto diffusi. Questi attacchi, che rappresentavano il 7,2% delle truffe di phishing nel 2021, sono infatti scesi ad appena il 3,7% nel 2022.

I 20 marchi più imitati negli attacchi di phishing del 2022 sono:

1. Microsoft
2. OneDrive
3. Binance
4. Siti di streaming illegale
5. SharePoint
6. Fondi per COVID-19
7. Pubblica amministrazione
8. Netflix
9. Facebook
10. Microsoft 365
11. Google
12. Telegram
13. Adobe
14. DHL
15. Amazon
16. American Express
17. WhatsApp
18. Roblox
19. PayPal
20. DocuSign

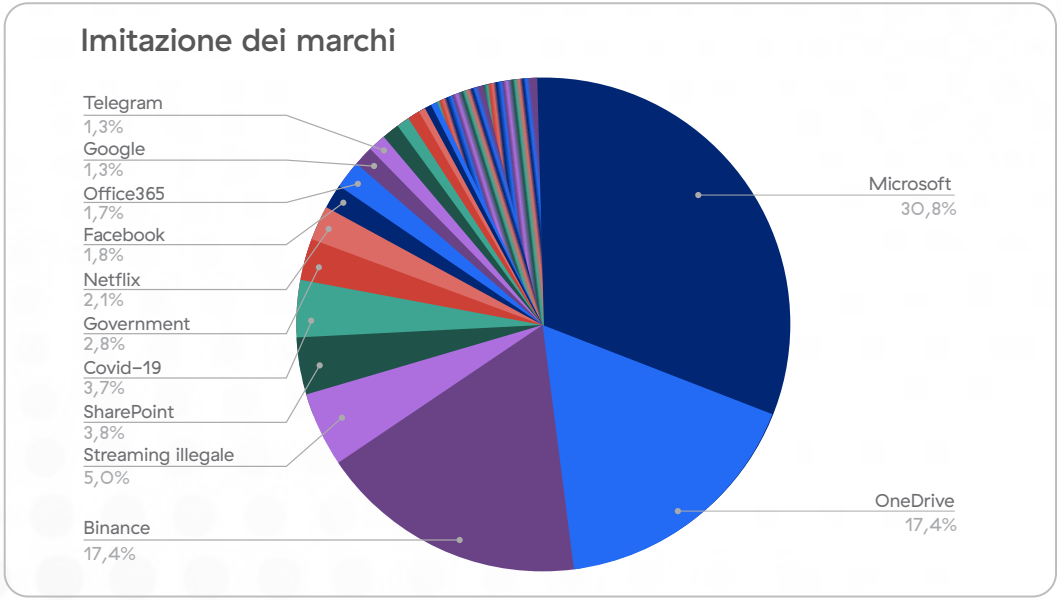


Figura 3: i marchi più imitati negli attacchi di phishing

I principali domini di reindirizzamento nel 2022

Spesso, gli aggressori utilizzano domini attendibili per manipolare le vittime e reindirizzarle verso siti web di phishing. Possono ad esempio acquistare pubblicità su siti di notizie o sulle piattaforme di ricerca, come Google e Bing, oppure possono pubblicare post o annunci su forum aziendali e marketplace, come Walmart e Amazon, o abusare di siti/servizi di condivisione, come Evernote, Dropbox e GitHub.

Abbiamo analizzato i vari domini di reindirizzamento per determinare quali sono quelli più sfruttati dagli aggressori. Nel 2022, tali domini includevano siti di streaming video, exchange di criptovalute e altri siti in ambito finanziario, builder per siti web e moduli, siti che ospitano contenuti generati dagli utenti, motori di ricerca e altro ancora.

Di seguito, sono elencati i 20 principali domini di reindirizzamento del 2022:

1. qumucloud.com
2. vimeo.com
3. bittrex-appemail.com
4. bittrex-global-emaill-i.com
5. googlesyndication.com
6. typeform.com
7. mhtestd.gov.zw
8. gutefrage.net
9. dow.com
10. framer.com
11. google.com
12. finanznachrichten.de
13. holldingsglobaloverview marketcap.com
14. hesgoal.com
15. doubleclick.net
16. elonshib.net
17. myftp.biz
18. principal.com
19. marathonbet.ru
20. baidu.comDocuSign

I 20 principali domini di reindirizzamento utilizzati negli attacchi di phishing

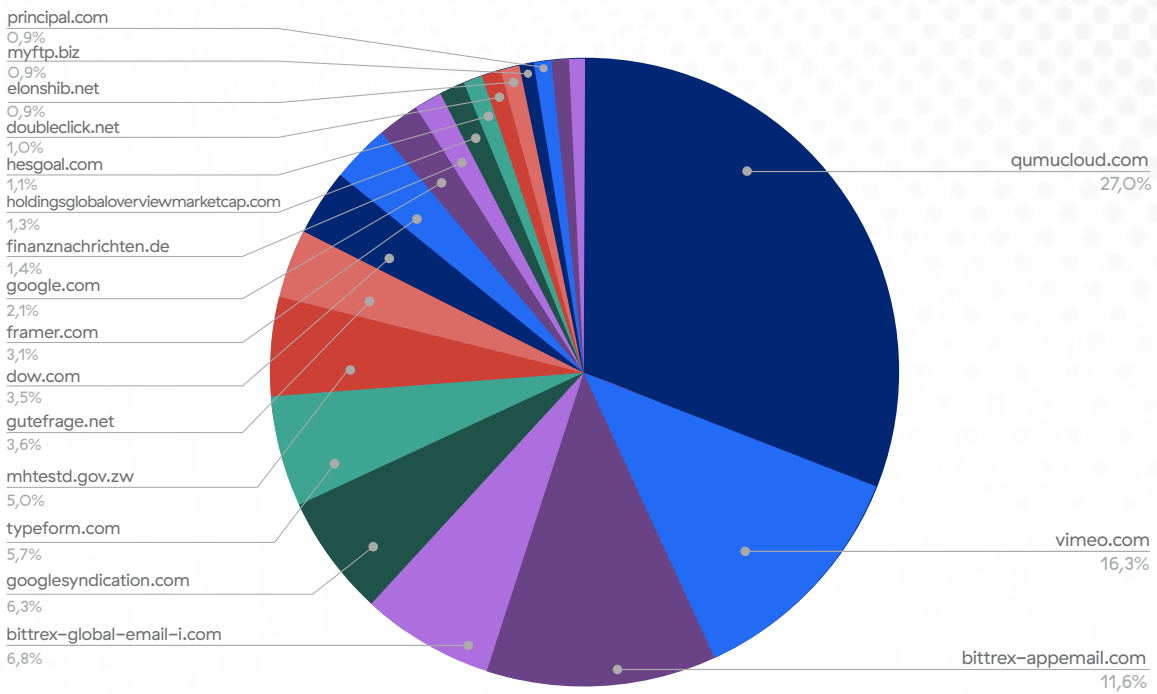


Figura 4: domini di reindirizzamento più comuni utilizzati negli attacchi di phishing nel 2022

Attacchi ai sistemi autonomi nel 2022

Un sistema autonomo (AS, Autonomous System) è una rete o un gruppo di reti con una sola policy di routing. Ogni AS ha un identificativo numerico univoco, noto come ASN. Nell'ambito di questa analisi, il team di Zscaler ThreatLabz ha esaminato gli ASN responsabili dell'hosting dell'infrastruttura di phishing.

La nostra analisi ha mostrato che, nel 2022, il 39% degli attacchi di phishing ha utilizzato siti di hosting (in calo rispetto al 50,6% del 2021), il 53% ha impiegato gli ISP (in aumento rispetto al 39,2% del 2021) e l'8% i domini aziendali.

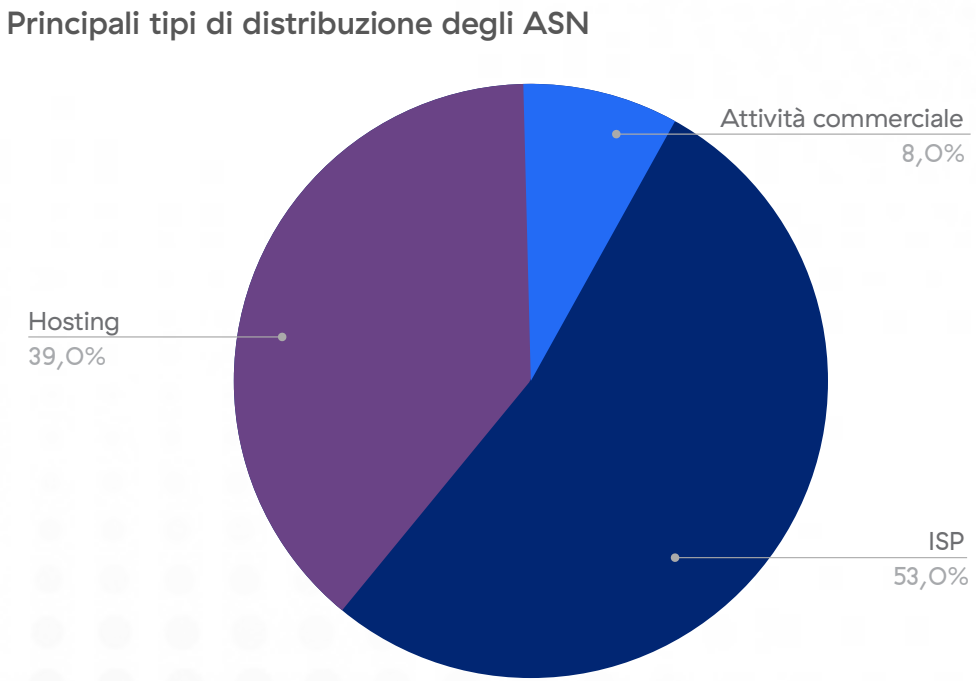


Figura 5: ASN per l'infrastruttura di phishing

L'evoluzione delle tendenze del phishing

Ogni anno, gli aggressori utilizzano tattiche sempre più sofisticate e approcci sempre più avanzati per portare a termine le loro truffe di phishing. Per assicurarsi che l'organizzazione sia preparata e che il team sia sempre all'avanguardia nel rispondere agli attacchi, è fondamentale rimanere informati sulle ultime tendenze relative alle minacce. Di seguito, sono riportati i principali dati sulle tendenze del phishing osservate nel corso del 2022.

Attacchi di vishing

Gli attacchi di vishing, ossia le campagne di phishing basate sulla messaggistica vocale, inducono le vittime ad aprire allegati dannosi. A metà del 2022, gli aggressori hanno preso di mira utenti di varie organizzazioni degli Stati Uniti con e-mail dannose basate su messaggi vocali, allo scopo di rubare le credenziali di Microsoft 365 e Outlook.

Abbiamo inoltre osservato campagne di phishing con allegati alle e-mail di messaggistica vocale, come il seguente:

Figura 6: e-mail della campagna di vishing

Il file .html contiene un JavaScript offuscato:

Figura 7: codice dell'e-mail di una campagna di vishing con JavaScript nascosto

Svelando il codice dell'e-mail, si può notare che se un utente dovesse aprire il file, verrebbe reindirizzato a un server controllato dall'aggressore:

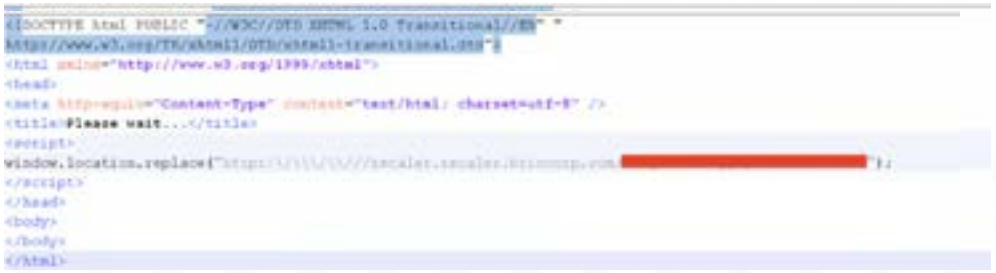


Figura 8: codice dell'e-mail di una campagna di vishing in cui il JavaScript nascosto è stato svelato

Porta a una pagina di phishing di Microsoft:

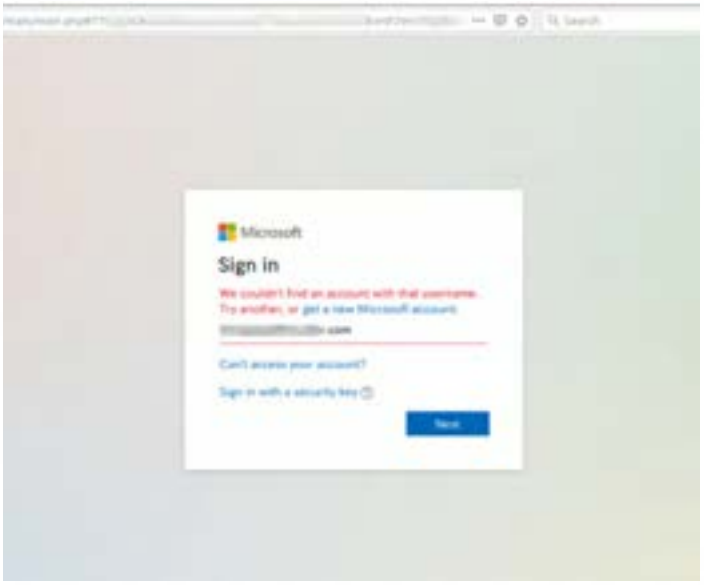


Figura 9: pagina di destinazione della campagna di vishing

ThreatLabz ha inoltre individuato un tipo di truffa con chiamata vocale, in cui un aggressore colpisce un dipendente aziendale spacciandosi per un manager. Inizialmente, la vittima riceve una telefonata fittizia con un saluto preregistrato, poi la chiamata viene conclusa. Successivamente, la vittima riceve un messaggio dal truffatore, il quale riferisce che il gestore ha problemi di connettività di rete e chiede di proseguire la comunicazione tramite messaggi. Il truffatore tenta quindi di convincere la vittima a rivelare informazioni sul conto aziendale o a trasferire fondi.

Per evitare di cadere nelle trappole degli aggressori, è fondamentale istruire i dipendenti a comunicare tra loro solo attraverso i canali ufficiali e a rimanere vigili di fronte queste truffe.

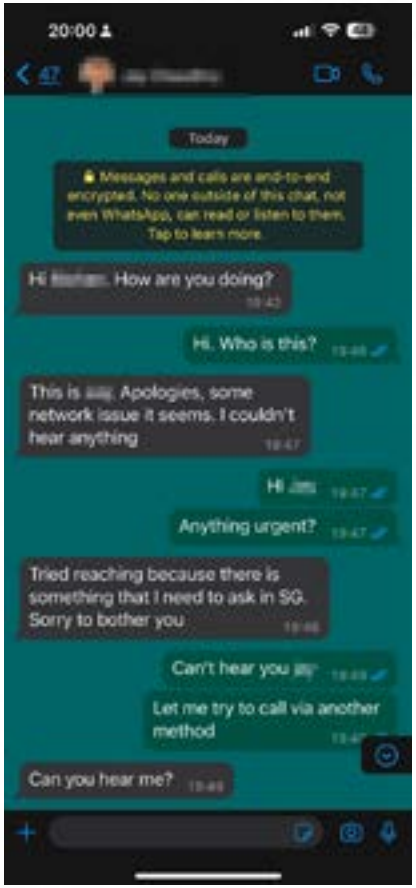


Figura 10: messaggi di vishing

Offerte di lavoro false

Nel corso del 2022, ThreatLabz ha registrato un incremento del numero di truffe rivolte alle persone in cerca di un'occupazione. Queste truffe impiegavano annunci di lavoro, siti web o portali e moduli esca per attirare chi era in cerca di lavoro.

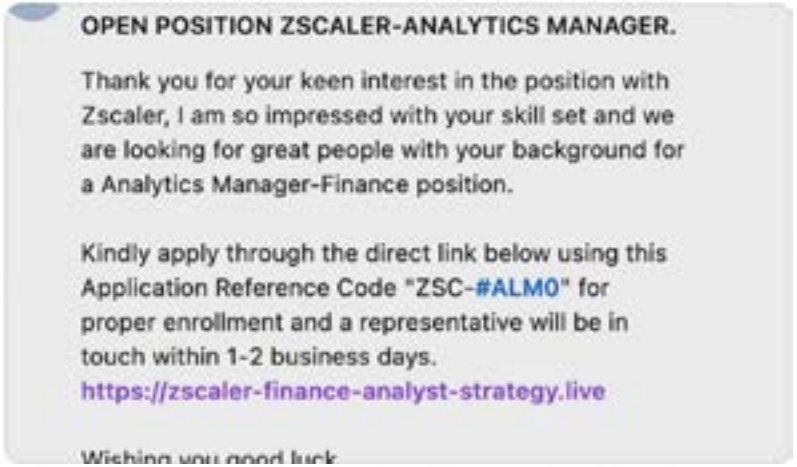


Figura 11: finto annuncio su LinkedIn con un URL di phishing

In questo caso, l'aggressore ha pubblicato un falso annuncio su LinkedIn con un URL di phishing. Visitando l'URL fittizio, le potenziali vittime potevano candidarsi per il lavoro.

Dopo la candidatura, l'aggressore comunicava con la vittima e richiedeva un colloquio via Skype, durante il quale impersonava un rappresentante delle risorse umane.

Figura 12: finta e-mail di reclutamento

Esaminando il codice sorgente, è possibile notare il codice impiegato per esfiltrare i dati delle carte di credito.

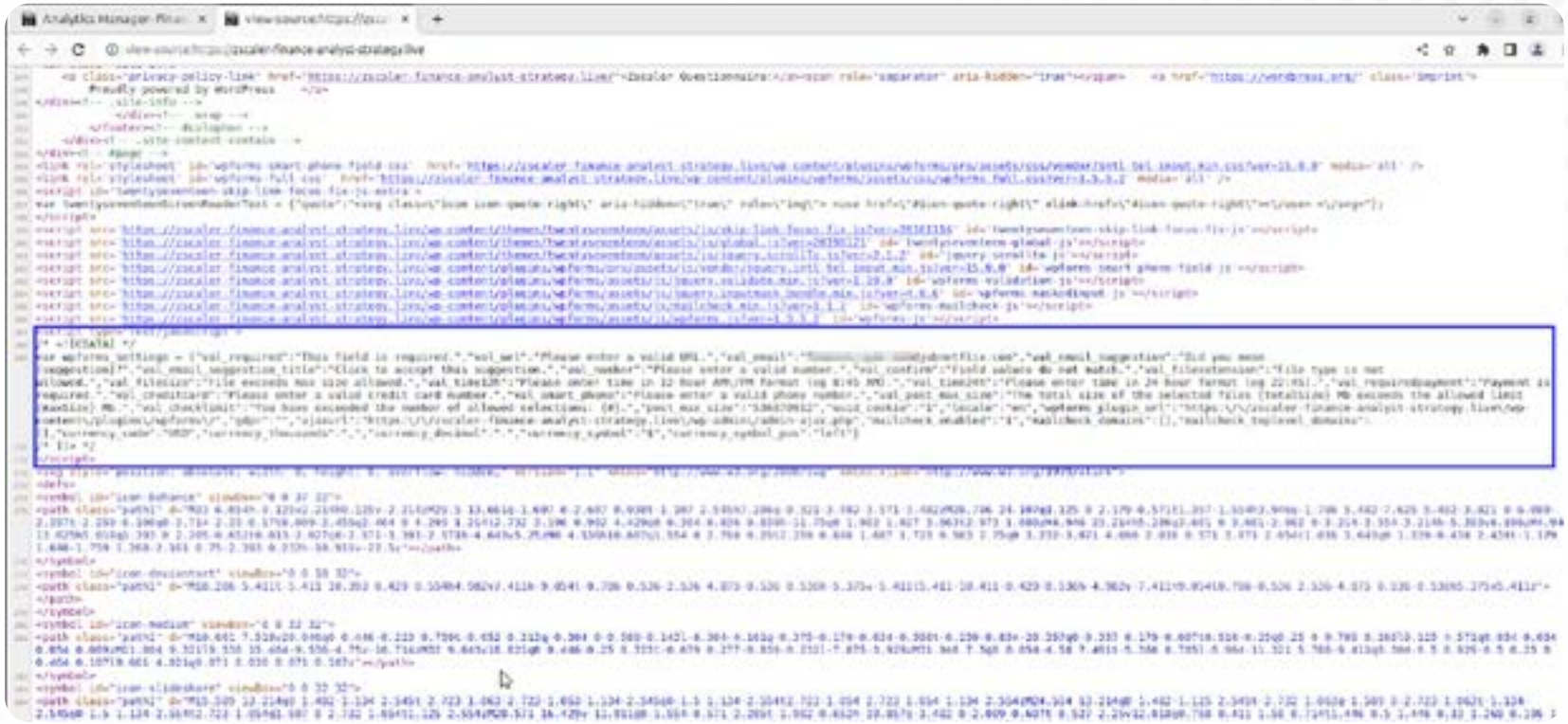


Figura 13: codice sorgente dell'e-mail di reclutamento fittizia

Attacchi di phishing AiTM (Adversary-in-the-Middle)

Scopri di più sugli attacchi di phishing AiTM (Adversary-in-the-Middle).

Il team di ThreatLabz ha scoperto un nuovo ceppo sfruttato da una campagna di phishing su larga scala che utilizza tecniche di AiTM insieme a diverse tattiche di elusione. I tradizionali siti web di phishing che raccolgono le credenziali dell'utente non completano mai il processo di autenticazione con il server dell'effettivo provider del servizio di posta elettronica. Se l'MFA è abilitata, l'aggressore non sarà in grado di accedere all'account usando solo le credenziali rubate. Per aggirare l'MFA, gli utenti malintenzionati possono però utilizzare attacchi di phishing AiTM.

La Figura 14 mostra un frammento di codice di una pagina di phishing fornita da un server di phishing AiTM.

Figura 14: codice della pagina di phishing fornita dal server di phishing AiTM

Il server proxy AiTM dannoso modifica gli URL di una pagina di destinazione legittima con URL controllati dall'aggressore (Figura 15) e funge da intermediario tra la vittima e il server di destinazione.

Figura 15: URL controllati dall'aggressori e modificati dal server proxy AiTM

Il sottodominio originale (in verde), il nome del dominio originale (in blu, senza il TLD) e un ID univoco generato (in rosa) sono uniti con dei trattini e diventano un sottodominio sotto il dominio del sito di phishing (in arancione).

Abbiamo potuto constatare quanto sopra quando alcune richieste hanno raggiunto le vittime con modifiche non corrette, come si vede nella figura 16.

Figura 16: modifiche errate passate alla vittima del phishing

Il risultato è la divulgazione dell'indirizzo del server controllato dall'aggressore, come mostrato nella figura 17.

Figura 17: divulgazione dell'indirizzo del server controllato dall'aggressore

Attacchi di phishing BiTB (Browser-in-the-Browser)

Anche gli attacchi di phishing BiTB hanno registrato un incremento nel 2022. Questi attacchi simulano la finestra di una pagina di autenticazione all'interno di una pagina di phishing principale, che induce la vittima a credere di dover inserire le proprie credenziali SSO (Single Sign-On) per poter continuare a utilizzare il sito web.

Gli aggressori utilizzano una combinazione di HTML/CSS di base e frame inline (iframe) per creare una finestra pop-up fittizia che simula la tipica finestra pop-up di SSO dell'utente. Per un utente, può risultare del tutto impossibile distinguere una finestra pop-up autentica da una di phishing ben progettata.

La figura 18 mostra un esempio di attacco BiTB che utilizza una finestra di SSO falsa generata tramite HTML per colpire Steam, una popolare piattaforma di gaming.

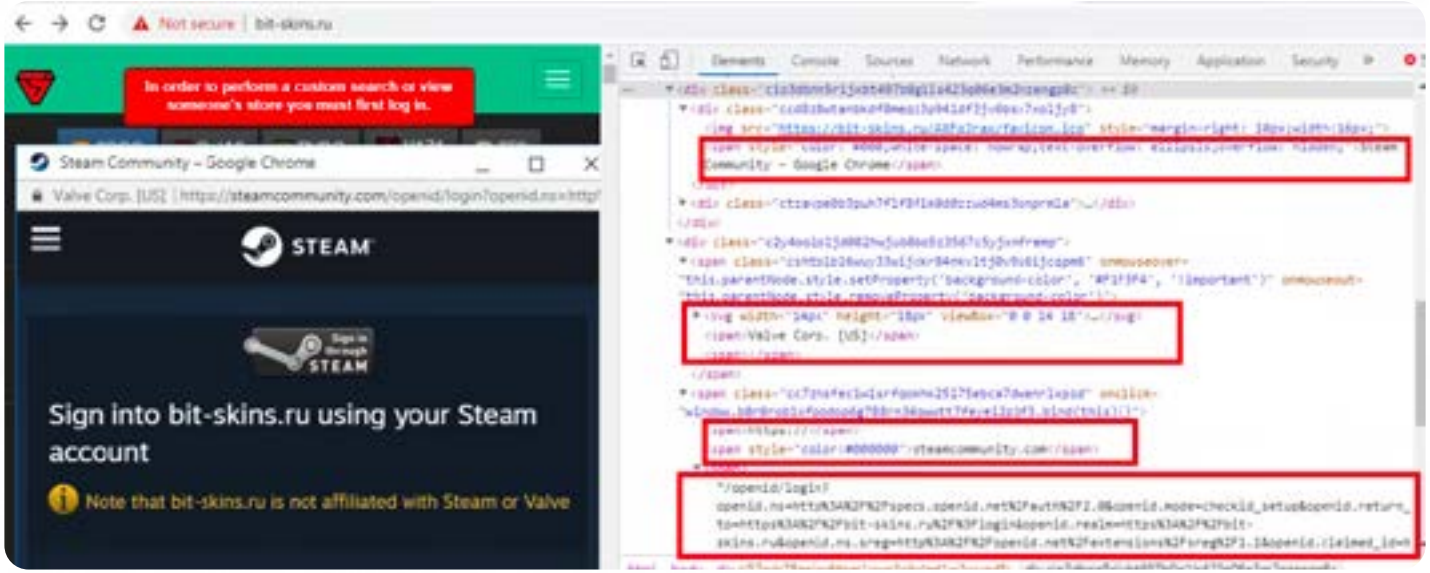


Figura 18: attacco BiTB o "picture-in-picture"

Utilizzo di servizi legittimi per ospitare siti web di phishing

Il team di ThreatLabz ha inoltre osservato che gli aggressori hanno utilizzato servizi di hosting legittimi per ospitare siti di phishing. Alcuni di questi siti includevano fornitori di hosting gratuito, come OOwebhostapp.com, servizi di condivisione di file, come transfer.sh, fornitori di servizi cloud, come amazonaws.com, e l'abbreviazione degli URL, sfruttando servizi come linkedin.com.

Nel corso del 2022, il team ha riscontrato che gli aggressori hanno utilizzato servizi DNS dinamici che consentono agli utenti di mappare un nome di dominio rispetto a un indirizzo IP variabile. Gli utenti utilizzano questi servizi principalmente per l'accesso remoto o l'hosting di siti web sulle reti domestiche.

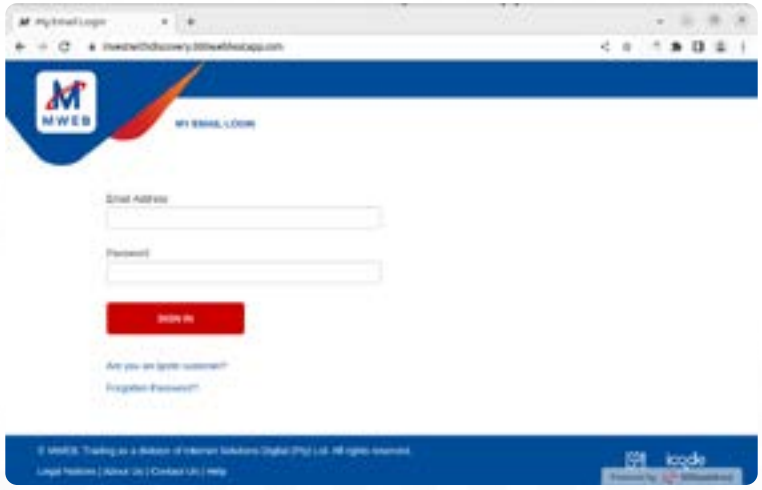


Figura 19: sottodomini DNS dinamici per l'hosting di pagine di phishing (esempio 1)

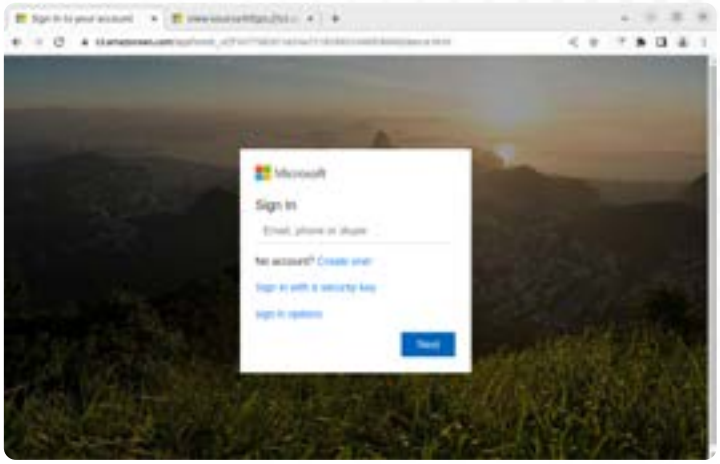


Figura 20: sottodomini DNS dinamici per l'hosting di pagine di phishing (esempio 2)

Gli aggressori possono inoltre utilizzare servizi DNS dinamici per ospitare siti web di phishing su computer o server compromessi senza indirizzi IP fissi.

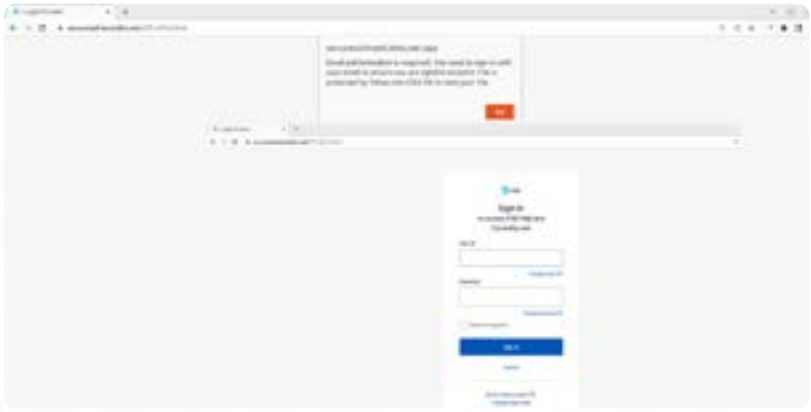


Figura 21: phishing di T&T ospitato utilizzando un DNS dinamico

Phishing che sfrutta il protocollo IPFS (InterPlanetary File System)

L'IPFS è un file system distribuito peer-to-peer, che consente agli utenti di archiviare e condividere file su una rete decentralizzata di computer. Rispetto ai tradizionali file system centralizzati, offre un modo più sicuro, resiliente ed efficiente di archiviare e distribuire i file.

Nel protocollo IPFS, i file sono divisi in blocchi più piccoli e distribuiti su più nodi di una rete, rendendo più difficile per un singolo punto di errore (SPOF) compromettere l'intero sistema. La Figura 22 mostra come appare il phishing basato su IPFS.

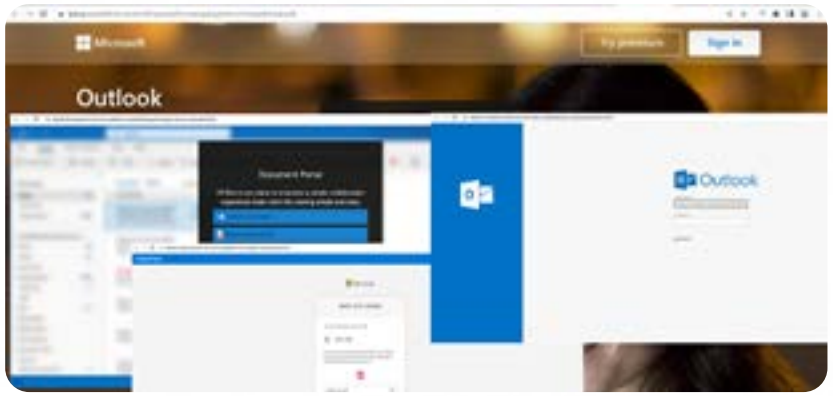


Figura 22: esempio di phishing basato su IPFS

Data la sua struttura peer-to-peer, è molto più difficile rimuovere una pagina di phishing ospitata su IPFS rispetto a una ospitata con un metodo più tradizionale.

Abbiamo inoltre riscontrato che gli aggressori hanno sfruttato Google Traduttore per far apparire i loro URL attendibili.

Figura 23: esempio di phishing IPFS che sfrutta Google Traduttore

Come illustrato nella figura 23, gli aggressori hanno sfruttato Google Traduttore su un sito di phishing ospitato su IPFS e in seguito hanno utilizzato la pagina per rubare le credenziali di DocuSign.

Utilizzo di WebSocket per l'esfiltrazione di dati con fingerprinting

Nel Report del 2022 di Zscaler ThreatLabz sul phishing, abbiamo parlato dei kit di phishing e dei framework di phishing open source. Kit e framework raggruppano e commercializzano gli strumenti necessari per lanciare rapidamente centinaia o addirittura migliaia di pagine di phishing convincenti ed efficaci, anche se l'aggressore è dotato di scarse competenze tecniche.

Alcuni di questi kit di phishing dispongono di una funzione chiamata "cloaking", una tecnica che consente di nascondere una reale pagina web di phishing a ricercatori e scanner di sicurezza pur continuando a esporla alle loro vittime. Il kit di phishing filtra le connessioni per ogni visitatore in base all'indirizzo IP, alle parole chiave dell'hostname, all'agente utente e altro ancora. A seconda della corrispondenza, fornirà una pagina benigna o una pagina di phishing, evitando così il rilevamento da parte dei ricercatori di sicurezza e degli strumenti anti-phishing che scansionano Internet alla ricerca di contenuti dannosi. Questi metodi di rilevamento tradizionali possono essere aggirati dagli aggressori utilizzando diverse tecniche di cloaking.

Quest'anno, abbiamo osservato una nuova caratteristica nelle tecniche di fingerprinting (creazione di impronte digitali) dei client. Ecco cosa succede quando un visitatore arriva su una pagina di phishing e viene sottoposto a fingerprinting:

1. L'utente naviga sulla pagina di phishing.
2. Il server restituisce un JavaScript per il fingerprinting del client, e il JavaScript carica l'impronta ottenuta tramite una connessione WebSocket.
3. Il server genera un cookie basato su quest'impronta e lo rinvia tramite WebSocket.
4. Il codice JavaScript aggiorna automaticamente la pagina con il cookie.
5. Se il cookie supera il controllo, l'utente viene reindirizzato alla pagina di phishing.

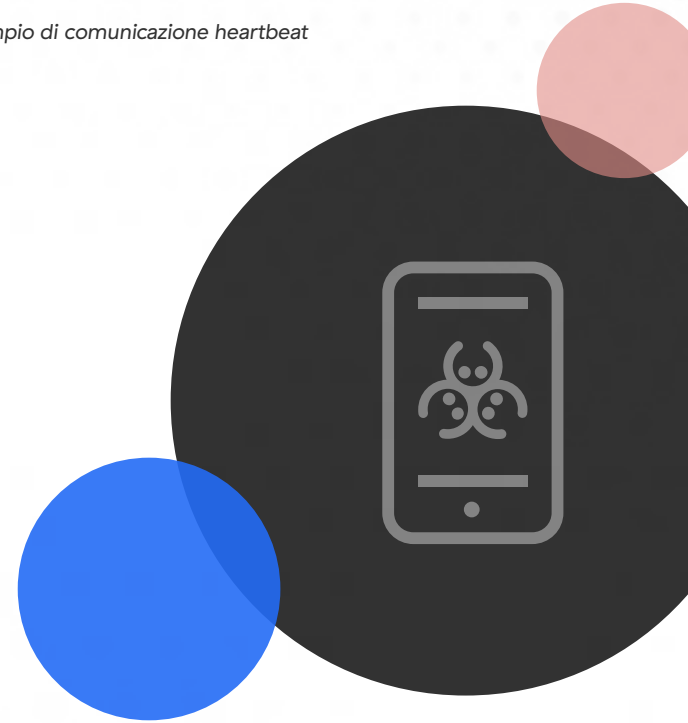
Il JavaScript di fingerprinting si basa su questo progetto open-source su GitHub.

```
{
 "type": "vdata",
 "data": {
  "languages": [
   "en-US"
  ],
  "cookieEnabled": true,
  "serviceWorker": true,
  "hardwareConcurrency": 48,
  "javaEnabled": false,
  "referrer": "",
  "etsl": 33,
  "battery": true,
  "hasChrome": false,
  "webXR": true,
  "mediaSession": true,
  "webgl": "ANGLE (Google, Vulkan 1.2.0 (SwiftShader Device (Subzero) (0x0000C0DE)), SwiftShader driver-5.0.0)",
  "timezone": "7",
  "platform": "Linux x86_64",
  "userAgent": "Mozilla/5.0 (X11; Ubuntu; Linux i686; rv:24.0) Gecko/20100101 Firefox/24.0",
  "appCodeName": "Mozilla",
  "appName": "Netscape",
  "language": "en-US",
  "deviceMemory": 8,
  "vendor": "Google Inc.",
  "visitorId": "6b3a518d3ab6051e32ce5098746b411e",
  "permissions": {
   "accelerometer": "prompt",
   "ambient_light_sensor": "unknown",
   "background_fetch": "unknown",
   "background_sync": "unknown",
   "bluetooth": "unknown",
   "camera": "prompt",
   "clipboard_write": "unknown",
   "device_info": "unknown",
   "display_capture": "unknown",
   "geolocation": "prompt",
   "gyroscope": "prompt",
   "magnetometer": "prompt",
   "microphone": "prompt",
   "midi": "prompt",
   "nfc": "unknown",
   "notifications": "prompt",
   "persistent_storage": "unknown",
   "push": "prompt",
   "speaker_selection": "unknown",
   "speaker-selection": "unknown",
   "device-info": "unknown",
   "background-fetch": "prompt",
   "background-sync": "prompt",
   "persistent-storage": "prompt",
   "ambient-light-sensor": "unknown",
   "clipboard-write": "prompt",
   "display-capture": "prompt"
  },
```


Figura 24: dati di fingerprinting di una macchina

Questa tecnica può essere interrotta monitorando la comunicazione WebSocket e filtrando i dati di fingerprinting. Il kit di phishing può impostare la comunicazione di comando e controllo (C2) per ricevere comandi dai server di phishing tramite WebSocket, attraverso una tecnica definita comunicazione heartbeat, in cui l'aggressore invia e riceve dati dal dispositivo della vittima.

Figura 25: esempio di comunicazione heartbeat



Utilizzo dei servizi di compilazione di moduli web per raccogliere credenziali

Abbiamo inoltre riscontrato che gli aggressori abusano dei servizi che aiutano gli utenti a raccogliere informazioni tramite moduli. FormSubmit, ad esempio, è un servizio web che consente di impostare e gestire con facilità moduli HTML per i siti web. Le organizzazioni possono utilizzarlo per creare moduli personalizzati con vari campi di inserimento, come caselle di testo, caselle di controllo, pulsanti di opzione, elenchi a discesa e upload di file, per poi inviare i dati del modulo a un indirizzo e-mail o a un URL di webhook specifico.

L'esempio della figura 26 mostra il modo in cui gli aggressori abusano dei servizi di moduli per raccogliere credenziali senza dover configurare nessun server.

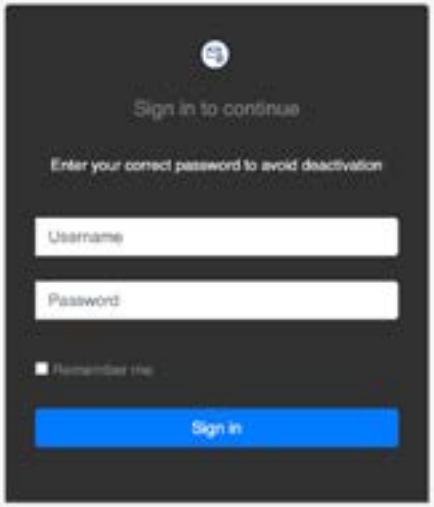


Figura 26: esempio di modulo

L'azione nel modulo è "https://submit-form[.]com/Qz1kGknr".

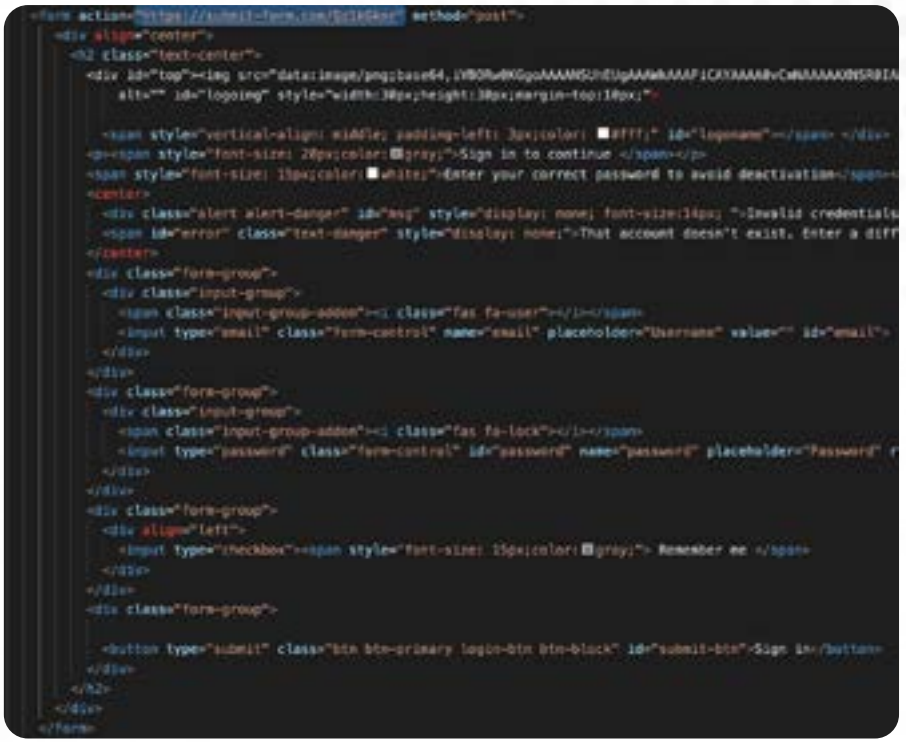


Figura 27: modalità attraverso cui l'aggressore sfrutta il servizio di creazione di moduli per intercettare le informazioni

Phishing che sfrutta HTML smuggling e file SVG

L'HTML smuggling è una tecnica che consente agli aggressori di aggirare i controlli di sicurezza della rete, incorporando codice dannoso all'interno di un HTML apparentemente benigno e consegnando payload dannosi a un sistema di destinazione. Spesso, gli schemi di rilevamento analizzano e rilevano i JavaScript, ed è per questo che gli aggressori utilizzano l'HTML smuggling per distribuire vari tipi di malware.

Gli utenti malintenzionati spesso spostano il codice di HTML smuggling nel formato SVG (Scalable Vector Graphics), un formato grafico vettoriale basato sull'XML, utilizzato per creare grafiche bidimensionali che possono essere ridimensionate senza perdere risoluzione, e modificano i file SVG con editor di testo e software grafici.

Gli aggressori possono utilizzare JavaScript per manipolare gli elementi e gli attributi SVG e creare diverse animazioni, come oggetti che si muovono, colori che cambiano e transizioni. Impiegando JavaScript, le animazioni SVG possono essere interattive, per consentire agli utenti di interagire con la grafica e attivare diverse animazioni.

Solitamente, le soluzioni di rilevamento non controllano il JavaScript all'interno degli SVG, il che rende questi file molto interessanti per gli aggressori.

Strumenti e tecniche di phishing

Online sono disponibili diverse applicazioni o estensioni del browser che vengono utilizzate dagli aggressori per copiare un sito web legittimo e modificare il codice di esfiltrazione dei dati per rubarli. Ecco alcuni esempi:

- **HTTrack,** un'applicazione molto utilizzata
- **singlefile,** un'estensione di Google Chrome
- **Webscrapbook,** un'estensione open source del browser
- **Save Page WE**, un'estensione di Google Chrome

Phishing basato sull'iframe

Un iframe è un elemento HTML che consente agli sviluppatori web di incorporare un altro documento HTML all'interno di una pagina web. Crea una sorta di "cornice nella cornice", in cui il contenuto del documento incorporato viene visualizzato all'interno di un riquadro rettangolare nella pagina. Incorporando contenuti di phishing in un iframe, gli aggressori possono riuscire a eludere il rilevamento.

Un iframe può essere utilizzato per il phishing in diversi modi:

1. Iframe annidato
2. Iframe di sfondo
3. Iframe frontale, come BiTB

Inoltre, ci aspettiamo che inizieranno a comparire anche gli "iframe come componenti", un metodo in cui diversi iframe possono essere combinati per generare una pagina di phishing, dove un iframe è una parte della pagina. Il primo iframe può essere ad esempio utilizzato per raccogliere un nome utente (figura 28):

Figura 28: iframe per la raccolta del nome utente

Il secondo iframe viene utilizzato per raccogliere una password (figura 29):

Figura 29: iframe per la raccolta della password

Infine, la pagina di phishing combina i due iframe (figura 30):

Figura 30: pagina di phishing con gli iframe combinati

Phishing basato su WebAssembly

Il WebAssembly è un formato di istruzioni binarie per una macchina virtuale che viene eseguito nei browser web moderni. Fornisce un formato bytecode portabile e low-level che può essere eseguito a velocità quasi nativa, ed è quindi adatto all'esecuzione di applicazioni sul web in cui le prestazioni sono di fondamentale importanza.

WebAssembly risolve i limiti di JavaScript come linguaggio per le applicazioni web, e il suo codice può essere scritto in vari linguaggi, come C++, Rust e Go, per poi essere compilato nel formato bytecode di WebAssembly.

Phishing basato sull'area geografica

Gli aggressori che vogliono colpire utenti all'interno di particolari aree geografiche o che parlano determinate lingue possono usare API di terze parti e servizi specifici per identificare i loro obiettivi.

Geo Targetly è un servizio che consente agli utenti di personalizzare i contenuti del proprio sito web in base alla posizione geografica dei visitatori. Per definire i contenuti visualizzati, è possibile creare regole personalizzate basate su fattori come indirizzi IP, impostazioni linguistiche e fusi orari.

Gli aggressori utilizzano proprio questo servizio come tecnica di cloaking per lanciare attacchi phishing.

Utilizzo di Punycode o di un indirizzo IP non standard negli URL per evitare il rilevamento

Un indirizzo IP è semplicemente un numero di 32 bit che può essere rappresentato con una quantità diversa di cifre. La quantità standard è di quattro cifre, ma esistono anche indirizzi IP a una, due o tre cifre, e ogni cifra può essere rappresentata utilizzando una base diversa (binaria, ottale, decimale, esadecimale). Rappresentando un indirizzo IP in modo non standard, gli aggressori possono riuscire a eludere il rilevamento, ma questa strategia può essere mitigata normalizzando gli indirizzi IP.

Phishing basato sul marcatore hash nell'URL

Il "marcatore hash" in un URL indica la parte dell'URL che viene dopo il simbolo del cancelletto (#). Conosciuto anche come identificatore di frammento, o fragment identifier, questo simbolo identifica una sezione specifica all'interno di una pagina web, come un'intestazione di sezione o un paragrafo, e consente all'utente di andare direttamente in quella sezione facendo clic su un link o un segnalibro.

Il contenuto dopo il simbolo "#" non viene inviato al server, quindi le modifiche all'hash non comportano l'aggiornamento della pagina. Questa funzione viene spesso utilizzata nelle applicazioni a pagina singola e nei contenuti web dinamici.

Gli aggressori hanno trovato due nuovi modi per sfruttare questo sistema:

1. Rappresentare le informazioni dell'utente con l'hash.
    - Gli indirizzi e-mail sono i più comuni. Quando viene visualizzata la pagina di autenticazione, l'indirizzo e-mail dell'utente viene inserito in modo automatico per ingannarlo.
2. Generare pagine di phishing specifiche in base all'hash in grado di contraddistinguere gli utenti.

IA e phishing

I recenti progressi nella tecnologia dell'IA, come ChatGPT, rendono più facile per gli aggressori sviluppare codice dannoso, generare attacchi BEC (Business Email Compromise), creare malware polimorfi e altro ancora. Abbiamo provato a generare una pagina di phishing di autenticazione utilizzando ChatGPT e, dopo solo tre semplici interazioni, lo strumento ha generato questa pagina web:

Figura 31: pagina di phishing generata da ChatGPT

Con un po' più di impegno, un aggressore potrebbe aggiungere uno sfondo e applicare modifiche, in modo da farla sembrare una vera pagina di autenticazione.

Previsioni per il 2024

1. **Gli attacchi che sfruttano l'IA saranno sempre più diffusi** con la scoperta di nuovi ambiti di applicazione per questi servizi da parte degli aggressori. Si prevede che ci saranno truffe più sofisticate che sfrutteranno diversi canali di comunicazione, come e-mail, SMS e siti web. Inoltre, i tentativi di phishing registreranno un brusco aumento, in quanto gli aggressori usufruiranno dell'intelligenza artificiale per lanciare attacchi più coordinati ed efficaci contro gruppi più numerosi di persone.

2. **Le soluzioni di phishing-as-a-service continueranno a evolversi;** i fornitori di questi servizi offriranno modelli di phishing personalizzati, un accesso a database più ampi di potenziali vittime e tecniche di social engineering sempre più avanzate. Potrebbero inoltre offrire servizi aggiuntivi, come l'installazione di malware, l'hosting e l'analisi. Inoltre, gli stessi saranno in competizione tra loro per offrire un valore aggiunto, con modelli di tariffazione accessibili e un'assistenza clienti 24 ore su 24 e 7 giorni su 7. Questo potrebbe portare a un incremento degli attacchi di phishing su piccola scala, ed è fondamentale rimanere sempre informati sulle ultime minacce e sulle tendenze del phishing.

3. **Gli attacchi indirizzati ai dispositivi mobili saranno sempre più diffusi,** in quanto gli aggressori si concentreranno sullo sfruttamento di questa nostra dipendenza. Svilupperanno contenuti più adatti ai dispositivi mobili, come applicazioni e siti web ottimizzati, e malware, tra cui spyware e trojan per l'accesso remoto. Inoltre, escogiteranno nuovi modi per estorcere denaro alle vittime e trarre profitti.

4. **L'MFA bombing e gli attacchi AitM aumenteranno,** in quanto gli utenti malintenzionati troveranno il modo di aggirare le misure di sicurezza basate sull'MFA. L'MFA bombing si basa sull'inondare le vittime di richieste di autenticazione, mentre gli attacchi AitM intercettano la sessione della vittima dopo che questa si è autenticata con l'MFA. Gli aggressori impiegheranno tecniche avanzate, come l'intelligenza artificiale, per prevedere e generare codici di verifica o identificare modelli di comportamento degli utenti da sfruttare per ottenere l'accesso. Per proteggersi da questi attacchi, è importante utilizzare password forti, attivare l'autenticazione a due fattori e monitorare gli account per accorgersi di eventuali attività sospette.

5. **Gli attacchi personalizzati diventeranno più difficili da rilevare,** perché gli aggressori svilupperanno tecniche di ricognizione avanzata per raccogliere informazioni sulle potenziali vittime. Queste informazioni verranno utilizzate per creare e-mail di phishing su misura, che appariranno più autorevoli e convincenti, accrescendone le probabilità di successo. Man mano che gli aggressori diventeranno sempre più sofisticati nell'uso della personalizzazione, per gli utenti risulterà molto più complesso identificare ed evitare gli attacchi di phishing.

Migliora le difese contro il phishing

Le statistiche di settore rivelano che un'organizzazione media riceve ogni giorno dozzine di e-mail di phishing, con un impatto finanziario significativo dovuto alle perdite causate dagli attacchi malware e ransomware, che anno dopo anno accrescono i costi medi degli attacchi di phishing riusciti. Affrontare tutte le minacce descritte in questo report è un compito gravoso e, sebbene non sia possibile eliminare completamente il rischio di subire un attacco di phishing, è comunque possibile ridurre le probabilità che un'organizzazione venga colpita.

Le basi per ridurre il rischio di attacchi di phishing:

Best practice: formazione sulle tematiche relative alla sicurezza

Le campagne di phishing registrano elevati tassi di successo perché prendono di mira gli utenti, ed è sufficiente che l'esca riesca a ingannare un solo dipendente distratto affinché l'attacco riesca. Uno studio del 2020 condotto dalla Stanford University ha rivelato che quasi l'88% delle violazioni dei dati è causato da un errore umano. Il report rivela inoltre che i giovani dipendenti uomini sono i più vulnerabili alle truffe di phishing e che, in tutti i dati analizzati, la distrazione è la principale causa di errore. Ecco perché la formazione per incrementare la consapevolezza degli utenti finali è fondamentale per prevenire le violazioni della sicurezza, e tenere una sessione una volta all'anno non è sufficiente. Tutti i membri dell'organizzazione devono essere istruiti su come riconoscere le minacce di phishing ed essere diffidenti di fronte alle richieste di informazioni o ai messaggi che inducono a fare clic su link presenti in e-mail, siti web, SMS, applicazioni e telefonate non affidabili.

L'implementazione di un programma di formazione continua sulle tematiche relative alla sicurezza e la conduzione di simulazioni di phishing periodiche sono fondamentali per sviluppare una cultura vigile e una forte consapevolezza del problema. Queste attività consentono di fornire una formazione tempestiva alle persone che hanno bisogno di maggiore supporto per identificare i tentativi di phishing e modificare i loro comportamenti rischiosi. Un altro modo per ridurre il numero di incidenti di phishing è quello di migliorare la segnalazione delle e-mail sospette di phishing da parte degli utenti, in modo da ridurre il tempo necessario ai team di sicurezza per rimuovere le minacce dalle altre caselle di posta in arrivo. Una soluzione potrebbe essere quella di inserire un pulsante "Segnala phishing" direttamente nella casella di posta.

ThreatLabz consiglia inoltre di implementare programmi di formazione in linea con la guida della Cybersecurity Infrastructure Security Agency (CISA) statunitense, che suggerisce agli utenti finali di prestare attenzione ai seguenti indicatori:

- **Indirizzi sospetti dei mittenti.** L'indirizzo e-mail di un mittente può imitare un'azienda esistente, e i criminali informatici utilizzano spesso indirizzi che assomigliano molto a quelli di aziende reali, alterando o omettendo alcuni caratteri.
- **Saluti e firme generiche.** Un messaggio di saluto generico, come "Gentile cliente" o "Signore/signora", o la mancanza di informazioni di contatto nel blocco della firma sono forti indicatori di phishing. Un'organizzazione attendibile, normalmente, si rivolge al destinatario per nome e fornisce le proprie informazioni di contatto.
- **Collegamenti ipertestuali e siti web emulati.** Passando il cursore sui link presenti nel corpo dell'e-mail, se il testo che appare non corrisponde al link stesso, significa che potrebbe essere stato emulato. I siti web dannosi possono sembrare identici a siti legittimi, ma gli URL possono presentare variazioni nell'ortografia o domini diversi (ad esempio ".com" invece di ".net"). Inoltre, i criminali informatici possono utilizzare un servizio di abbreviazione degli URL per nascondere la reale destinazione del collegamento.
- **Ortografia e layout.** La scarsa qualità della grammatica e della sintassi, errori di ortografia e formattazione incoerente sono altri indicatori tipici di un possibile tentativo di phishing. Le organizzazioni rispettabili dispongono di personale dedicato che produce, verifica e corregge le bozze della corrispondenza con i clienti.
- **Allegati sospetti.** Un'e-mail non richiesta che induce un utente a scaricare e ad aprire un allegato è una modalità comune di consegna di malware. Un criminale informatico può far credere alla vittima che l'azione richiesta sia urgente per convincerla a scaricare o ad aprire un allegato senza prima esaminarlo.

Best practice: controlli di sicurezza

I team responsabili della sicurezza devono tenere conto del fatto che i dipendenti e gli altri utenti cadranno inevitabilmente preda di tentativi di phishing, ecco perché devono essere adottate misure di protezione per rilevare e mitigare i danni. Le principali protezioni includono:

- **Scansione delle e-mail.** La posta elettronica è di gran lunga il vettore di phishing più comune, ed è quindi fondamentale disporre di un servizio di scansione delle e-mail cloud che le ispezioni prima che raggiungano il perimetro aziendale e fornisca protezione in tempo reale contro i link dannosi e l'emulazione dei nomi di dominio.
- **Segnalazione.** Spesso, gli attacchi di phishing tentano di colpire il maggior numero possibile di utenti finali di un'organizzazione per accrescere le probabilità di successo. Per bloccare i mittenti e i link dannosi più rapidamente, è bene consentire agli utenti finali di segnalare i tentativi di phishing, idealmente con un pulsante "Segnala" integrato nel client di posta elettronica. è importante delineare le procedure da seguire per investigare e rispondere agli incidenti di phishing, che dovrebbero anche includere la segnalazione alle autorità competenti, in modo da aiutare il governo a combattere i truffatori e a bloccare gli attacchi contro altre organizzazioni.
- **Autenticazione a più fattori.** L'autenticazione a più fattori (MFA) rimane una delle difese più importanti contro il phishing. Con la sua implementazione, infatti, una password non è sufficiente per compromettere un account. Le app di autenticazione, come Okta Verify o Google Authenticator, sono particolarmente efficaci e forniscono una difesa aggiuntiva contro le tattiche di MitM che possono intercettare i messaggi SMS.
- **Ispezione del traffico cifrato.** Più del 95% degli attacchi utilizza i canali cifrati, che spesso non vengono ispezionati; in questo modo, è molto più semplice bypassare i controlli di sicurezza, persino per gli aggressori meno sofisticati. Le organizzazioni devono quindi ispezionare tutto il traffico, indipendentemente dal fatto che sia cifrato o meno, per impedire agli aggressori di compromettere i propri sistemi.
- **Software antivirus.** Gli endpoint devono essere protetti con antivirus aggiornati periodicamente per identificare e bloccare i file dannosi e impedirne lo scaricamento.
- **Protezione dalle minacce avanzate.** L'antivirus è in grado di bloccare le minacce note, ma gli aggressori creano costantemente nuove varianti sconosciute di malware in grado di eludere gli strumenti di rilevamento basati sulle firme. Ecco perché è utile distribuire una sandbox inline per mettere in quarantena e analizzare i file sospetti, e utilizzare l'isolamento del browser per isolare i contenuti web potenzialmente dannosi senza interrompere i flussi di lavoro degli utenti finali.
- **Filtraggio degli URL.** è possibile limitare il rischio di subire attacchi di phishing sfruttando il filtraggio degli URL, che utilizza le policy per gestire l'accesso alle categorie più rischiose di contenuti web, come i domini appena registrati.
- **Applicazione delle patch.** è bene assicurarsi che applicazioni, sistemi operativi e strumenti di sicurezza siano sempre aggiornati con le ultime patch, per ridurre le vulnerabilità e garantire l'adozione delle misure di protezione più recenti.
- **Architettura zero trust.** Per quanto sia importante mettere in atto controlli di prevenzione, è altrettanto fondamentale adottare controlli che limitino i danni in caso di attacco riuscito. Ecco perché è bene implementare la segmentazione granulare, applicare l'accesso a privilegi minimi e monitorare costantemente il traffico per individuare gli aggressori che potrebbero aver compromesso l'infrastruttura.
- **Feed di intelligence sulle minacce.** I feed di intelligence sulle minacce si integrano con gli strumenti di sicurezza esistenti per fornire un arricchimento automatico del contesto e consentire una migliore rilevazione e la risoluzione più rapida delle minacce di phishing. Questi feed forniscono inoltre un contesto aggiornato sugli URL segnalati, l'estrazione di indicatori di compromissione (IOC), nonché tattiche, tecniche e procedure (TTP) per supportare il processo decisionale e l'assegnazione delle priorità.

Best practice: come identificare una pagina di phishing

Le pagine di phishing possono essere identificate individuando gli indicatori delle tattiche più comuni impiegate dagli aggressori per ingannare utenti e motori di sicurezza e le scorciatoie di cui spesso usufruiscono per generare nuove pagine. Inoltre, la creazione di nuovi siti di phishing aumenta durante le festività e altri eventi isolati. Ad esempio, durante la pandemia, il settore della sicurezza informatica ha assistito alla proliferazione di siti web fittizi a tema COVID-19, che avevano l'obiettivo di ingannare le vittime emulando organizzazioni sanitarie e siti web per ordinare kit di tamponi e forniture mediche. Per rilevare le minacce di phishing più recenti, è importante rimanere al corrente delle ultime ricerche sul tema e utilizzare informazioni di intelligence concrete con indicatori aggiornati, da utilizzare per definire le regole di rilevamento e i flussi di lavoro di risposta.

Di seguito è riportata una panoramica dei vari indicatori che dovrebbero richiamare l'attenzione dell'utente (e dei suoi strumenti anti-phishing):

L'intera pagina è basata su una singola immagine. Gli aggressori usano anche il phishing basato su immagini, in cui un'intera pagina web è costituita da un'immagine di sfondo, che è una copia di una pagina legittima. L'unico altro componente della pagina è un modulo web per raccogliere le credenziali. Si tratta di una tecnica molto comune, utilizzata per colpire in particolare le banche.

La pagina non ha titolo.

La pagina ha un ancoraggio vuoto per i link critici. Quando copiano i contenuti dalle pagine legittime, le pagine di phishing utilizzano spesso ancoraggi vuoti per le pagine importanti, come Aiuto, FAQ e così via.

La pagina ha un certificato autofirmato.

La pagina sembra essere un client webmail generico. Gli aggressori usano spesso pagine di webmail generiche per rubare le credenziali delle e-mail, imitando siti come Webmail, Zimbra, ecc.

La pagina non è criptata. Una richiesta di accesso su una pagina "http" è sospetta e andrebbe segnalata.

La pagina viene reindirizzata più volte prima di raggiungere una pagina con richiesta di accesso.

La pagina contiene HTML smuggling. Con l'HTML smuggling, gli aggressori nascondono un BLOB JavaScript dannoso codificato all'interno di un allegato di un'e-mail, che viene poi assemblato dal browser. In questo modo, gli aggressori possono bypassare i filtri delle e-mail. L'HTML smuggling, accompagnato da una richiesta di autenticazione, rappresenta un comportamento altamente sospetto.

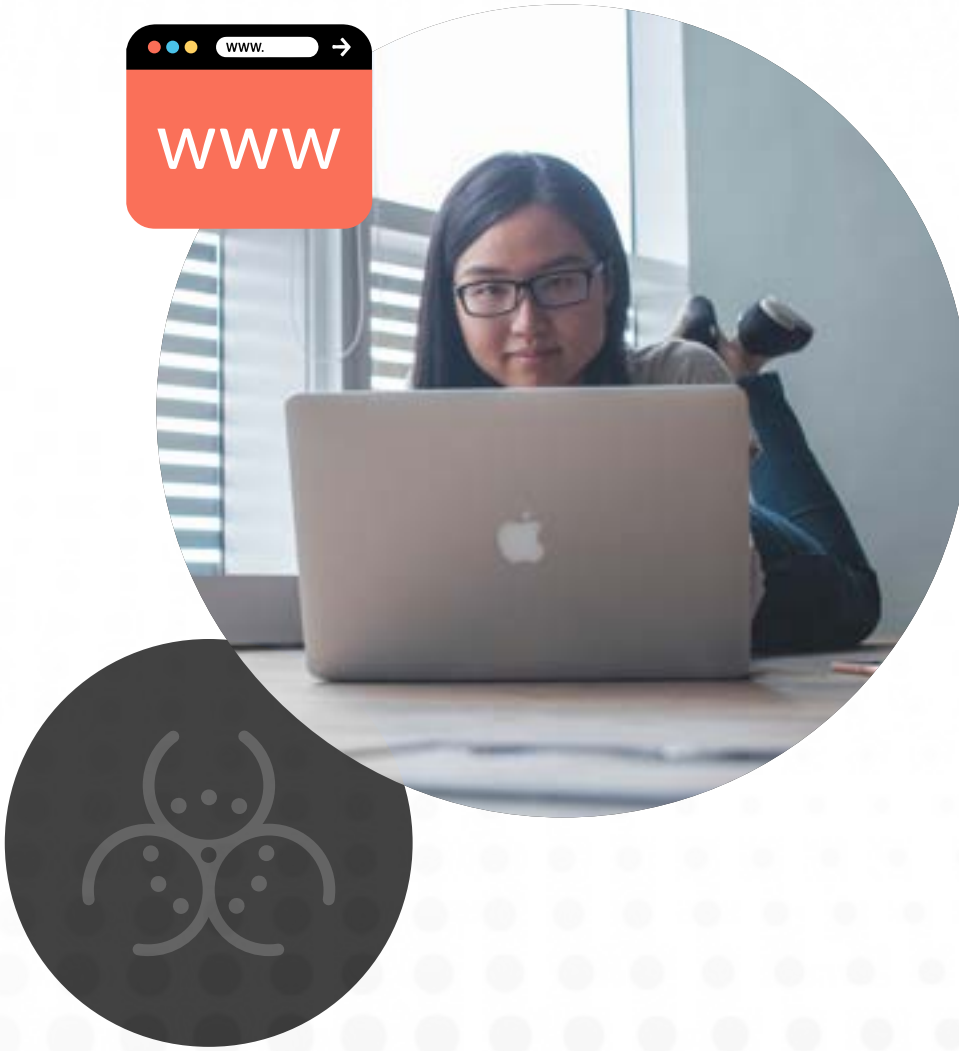
La pagina contiene tag offuscati. Gli operatori di phishing possono offuscare dei campi, come titolo, copyright, ecc.

La pagina sostituisce i caratteri chiave con omografi. Gli omografi, ovvero caratteri simili ad altri, vengono usati impropriamente nelle pagine di phishing per evitare il rilevamento. Questa tecnica sfrutta le somiglianze dei caratteri appartenenti a script di caratteri diversi per ingannare gli utenti e i motori di sicurezza che cercano di abbinare i modelli ASCII.

In che modo Zscaler Zero Trust Exchange è in grado di mitigare gli attacchi di phishing

Nell'ambito della sicurezza, la compromissione dell'utente è una delle sfide più difficili da affrontare. L'organizzazione deve implementare controlli per prevenire il phishing nell'ambito di una più ampia strategia zero trust, che consenta di rilevare le violazioni attive e ridurre al minimo i danni causati da quelle andate a buon fine. Zscaler Zero Trust Exchange™ è una soluzione costruita su un'architettura zero trust olistica che aiuta a bloccare il phishing nei seguenti modi:

- **Prevenendo le compromissioni:** grazie all'ispezione SSL completa su larga scala, all'isolamento del browser e al controllo degli accessi basato su policy per impedire l'accesso a siti web sospetti.
- **Eliminando il movimento laterale:** collegando gli utenti direttamente alle app, e non alla rete, per limitare il raggio di azione di un potenziale incidente.
- **Bloccando gli utenti compromessi e le minacce interne:** se un aggressore riesce a ottenere l'accesso al sistema di identità dell'azienda, Zero Trust Exchange previene i tentativi di sfruttamento delle app private attraverso l'ispezione inline ed è in grado di individuare gli aggressori più sofisticati sfruttando la tecnologia di deception integrata.
- **Bloccando la perdita dei dati:** ispezionando i dati in movimento e quelli inattivi per evitare potenziali furti da parte di aggressori attivi.



Prodotti correlati di Zscaler

Zscaler Internet Access™ aiuta a identificare e a bloccare le attività dannose instradando e ispezionando tutto il traffico Internet attraverso Zero Trust Exchange. Zscaler blocca:

- **URL e IP** osservati nel cloud Zscaler e provenienti dalle fonti open source e commerciali di intelligence sulle minacce integrate in modo nativo. Sono incluse anche le categorie di URL ad alto rischio definite da policy comunemente utilizzate per il phishing, come i domini osservati o attivati di recente.
- **Firme IPS** sviluppate dall'analisi di ThreatLabz condotta su kit e pagine di phishing.
- **Nuovi siti di phishing** identificati tramite la scansione dei contenuti che sfruttano il rilevamento basato su intelligenza artificiale e machine learning.

Advanced Threat Protection blocca tutti i domini C2 conosciuti.

Advanced Firewall estende la protezione C2 a tutte le porte e i protocolli, comprese le destinazioni C2 emergenti.

Browser Isolation genera un gap sicuro tra gli utenti e le categorie web dannose effettuando il rendering dei contenuti sotto forma di immagini, per eliminare la fuga di dati e la distribuzione di minacce attive.

Advanced Cloud Sandbox evita la distribuzione di malware sconosciuti con i payload di seconda fase.

Zscaler Private Access™ protegge le applicazioni limitando il movimento laterale, sfruttando l'accesso a privilegi minimi, la segmentazione da utente ad app e l'ispezione completa inline del traffico delle app private.

Zscaler Deception™ rileva e blocca gli aggressori che tentano di spostarsi lateralmente o di incrementare i propri privilegi attirandoli con esche sotto forma di server, applicazioni, directory e account degli utenti.

I prossimi passi da intraprendere

Scopri i rischi critici che insidiano l'intero ambiente cloud pubblico con Zscaler Security Risk Assessment. Ricevi un inventario completo delle risorse cloud, un quadro chiaro dei rischi per la sicurezza del cloud pubblico, una panoramica sull'allineamento dell'azienda rispetto agli standard di riferimento per la conformità e linee guida da seguire per intraprendere azioni correttive.

Informazioni su ThreatLabz

ThreatLabz è il team di ricerca sulla sicurezza di Zscaler. Questo team di esperti è responsabile della ricerca di nuove minacce e della protezione costante delle migliaia di aziende che utilizzano la piattaforma globale di Zscaler. Oltre alla ricerca sui malware e all'analisi del comportamento, i membri del team si occupano della attività di ricerca e sviluppo di nuovi prototipi per la protezione contro le minacce avanzate sulla piattaforma Zscaler, e conducono regolarmente controlli di sicurezza interni per garantire che i prodotti e l'infrastruttura di Zscaler siano in linea con gli standard di conformità. Sul suo portale, ThreatLabz pubblica regolarmente analisi approfondite sulle minacce nuove ed emergenti: research.zscaler.com.

Non perderti le ultime novità sulle ricerche di ThreatLabz. Iscriviti alla nostra newsletter Trust Issues oggi stesso.

Informazioni su Zscaler

Zscaler (NASDAQ: ZS) accelera la trasformazione digitale in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. Zscaler Zero Trust Exchange™ protegge migliaia di clienti dagli attacchi informatici e dalla perdita dei dati, collegando in modo sicuro utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in oltre 150 data center a livello globale, Zero Trust Exchange, basata sul SASE, è la più grande piattaforma di cloud security inline del mondo.

Per saperne di più, visita zscaler.it o seguici su Twitter @zscaler.

Appendice

La classificazione degli attacchi di phishing

Gli attacchi di phishing possono essere classificati in vari modi e possono includere diverse tecniche. Gli aggressori stanno inoltre adattando i loro approcci per ingannare utenti sempre più esperti ed eludere gli strumenti di difesa. Qui di seguito illustreremo le definizioni e le caratteristiche dei più comuni attacchi di phishing.

Gli elenchi riportano le descrizioni di diversi metodi di attacco fisici e il rischio che questi attacchi rappresentano per le organizzazioni. Gran parte di questo report si concentra sulle minacce di phishing virtuali, che per essere attuate richiedono una connessione a Internet. Una caratteristica indicativa delle truffe di phishing online è che, in genere, richiedono agli utenti di inviare informazioni o scaricare malware tramite uno dei seguenti metodi:

- **Link:** un utente fa clic su un link dannoso che lo indirizza su un sito di phishing, un file ospitato o un malware.
- **Richiesta:** a un utente viene richiesto di inviare informazioni sensibili che portano al furto dei suoi dati.
- **Allegato:** un utente apre un allegato che contiene un software dannoso.

Nel pianificare gli investimenti da effettuare quest'anno per ridurre gli incidenti legati al phishing, vanno considerati i seguenti tipi di attacchi di phishing.

Dalla a alla Z: i tipi più comuni di attacchi di phishing

1. **Angler phishing:** gli aggressori si spacciano per un servizio di assistenza clienti che intende risolvere questioni relative ai commenti negativi su un'azienda che sono stati pubblicati sui social media, prendendo di mira i clienti insoddisfatti, in particolare quelli delle banche.
2. **Phishing AitM (Adversary-in-the-Middle):** gli aggressori imitano le azioni di una vittima ignara per ottenere le sue credenziali di accesso e i cookie di sessione.
3. **Baiting phishing:** in modo analogo a un attacco basato su trojan, gli aggressori utilizzano offerte allettanti, nomi di file o dispositivi per attirare i curiosi in trappola.
4. **Phishing BitB (Browser-in-the-Browser):** gli aggressori visualizzano una finestra dannosa del browser all'interno di un'altra finestra del browser, per imitare un dominio legittimo e replicare finestre pop-up di accesso che sembrano essere di provider di autenticazione terzi.
5. **Phishing CEO fraud o BEC (Business E-mail Compromise):** gli aggressori colpiscono i dipendenti delle aziende sfruttando account dirigenziali compromessi per inviare fatture false o richieste di pagamento tramite bonifico bancario o altri modi.
6. **Phishing via chat o IM:** gli aggressori utilizzano la messaggistica istantanea per trasmettere truffe all'interno delle app, in genere impiegando collegamenti URL dannosi.
7. **Clone phishing:** gli aggressori creano messaggi e-mail duplicati che sembrano provenire da fonti attendibili, con lievi modifiche e allegati o link dannosi.

8. **Phishing di credential harvesting (o raccolta di credenziali):** gli aggressori creano pagine di autenticazione false o inviano e-mail di phishing che simulano delle richieste di login legittime per rubare nomi utente e password alle ignare vittime.
9. **Phishing basato sui documenti cloud:** gli aggressori inviano documenti dannosi da fonti cloud popolari, come Google Drive, Box o OneDrive, per aggirare gli strumenti di sicurezza tradizionali e renderne più difficile l'individuazione da parte dei team di sicurezza.
10. **E-mail phishing:** gli aggressori inviano messaggi di posta elettronica modificati tramite tecniche di social engineering spacciandosi per marchi noti, con risorse allegate o collegamenti URL dannosi, con l'intento di rubare informazioni o distribuire malware.
11. **Evil twin phishing:** gli aggressori simulano una rete Wi-Fi pubblica attendibile per osservare l'attività online delle vittime e rubare i dati che attraversano il punto di accesso dannoso.
12. **Phishing basato su HTTPS:** gli aggressori utilizzano il protocollo cifrato HTTPS (Hypertext Transfer Protocol Secure) per ingannare gli utenti e indurli a fare clic su collegamenti URL dannosi.
13. **Phishing di malvertising (o pubblicità fraudolenta):** gli aggressori utilizzano script nelle pubblicità per inviare contenuti indesiderati direttamente ai computer delle vittime.
14. **MFA bombing:** gli aggressori ingannano gli utenti con credenziali compromesse e li spingono a verificare una richiesta di MFA illegittima, effettuata in realtà dall'aggressore stesso. Questi attacchi sono solitamente caratterizzati da un flusso continuo di richieste di MFA, talvolta accompagnate da una chiamata, un SMS o un'e-mail fasulli, che inducono l'utente a verificare inconsapevolmente o accidentalmente una delle richieste.
15. **Phishing MiTM (Man-in-the-Middle):** gli aggressori prendono di mira gli utenti di un server o di un sistema specifico acquisendo i dati in transito, come credenziali, cookie o informazioni sul conto bancario, imitando i servizi online attraverso server proxy.
16. **Pharming o phishing basato sulla cache del DNS:** gli aggressori reindirizzano i visitatori a un sito dannoso, alterando l'indirizzo IP di un sito web legittimo nei server DNS (Domain Name System) compromessi, oppure inviando un'e-mail di phishing con un codice dannoso che reindirizza la vittima al sito ogni volta che inserisce un qualsiasi URL dal proprio computer.
17. **Phishing basato su codice QR:** gli aggressori utilizzano codici QR che, se scansionati dallo smartphone della vittima, conducono a siti web dannosi o scaricano malware sul dispositivo.
18. **Phishing basato su ransomware:** gli aggressori inviano e-mail con allegati o link dannosi che, se cliccati, scaricano il ransomware sul computer della vittima e richiedono il pagamento di una somma di denaro in cambio di una chiave di decifrazione.
19. **Phishing di reverse tunneling:** gli aggressori utilizzano un server remoto per creare un tunnel SSH inverso verso il computer della vittima che consente loro di sfruttare il dispositivo per vari scopi, come l'installazione di malware o il furto di dati sensibili, continuando a rimanere nascosti per evitare il rilevamento.
20. **Phishing basato sui motori di ricerca:** gli aggressori prendono di mira i consumatori creando siti di e-commerce fittizi indicizzati dai motori di ricerca con interessanti sconti su prodotti in evidenza, e possono apparire come pop-up di carattere stagionale o contenere false recensioni retrodatate. Le vittime possono inconsapevolmente condividere i propri dati personali, le informazioni bancarie, i numeri di carta di credito o persino pagare per prodotti fittizi. Per prolungare l'esistenza di questi siti, i truffatori si sono spinti anche a fornire false informazioni sulla spedizione e sul tracciamento e persino prodotti a basso costo.

21. **Smishing:** gli aggressori utilizzano i messaggi di testo (SMS) per trasmettere truffe, in genere impiegando collegamenti URL dannosi. Il mittente del messaggio appare come un marchio noto o un conoscente del destinatario.
22. **Spear phishing:** gli aggressori organizzano campagne che utilizzano informazioni pubblicamente disponibili per colpire le persone che lavorano per organizzazioni specifiche. Queste e-mail ingannevoli possono contenere informazioni reali e sembrare richieste interne legittime per indurre i destinatari a eseguire un'azione desiderata.
23. **Tailgating:** gli aggressori entrano fisicamente in un'area riservata seguendo una persona autorizzata. Questa forma di attacco è classificata come phishing se qualcuno cade vittima di trappole di social engineering (come nei casi in cui si consente a qualcuno di entrare perché sta trasportando pacchi di grandi dimensioni) e permette agli aggressori di accedere senza essere sottoposti a verifica.
24. **Phishing basato su USB:** gli aggressori installano fisicamente o inviano agli obiettivi unità USB contenenti eseguibili dannosi, che si caricano quando la chiave USB viene collegata a un qualsiasi endpoint vulnerabile.
25. **Vishing:** gli aggressori effettuano telefonate con intento malevolo e utilizzano tecniche di social engineering per indurre i destinatari a compiere un'azione, come trasferire denaro o rivelare informazioni personali.
26. **Watering hole phishing:** gli aggressori prendono di mira i membri di specifici gruppi che solitamente sono più propensi a visitare un determinato sito, che è stato compromesso dall'aggressore o appositamente creato per lanciare l'attacco.
27. **Whaling:** gli aggressori prendono di mira dirigenti e personalità di alto profilo utilizzando informazioni disponibili pubblicamente. Essi impiegano tecniche di social engineering per colpire il bersaglio e indurlo a rivelare segreti commerciali confidenziali da utilizzare per scopi fraudolenti o a eseguire altre azioni che possono essere utilizzate per lo scopo degli aggressori.

La tecnologia da sola non è in grado di contrastare il phishing. Ecco perché le organizzazioni devono seguire l'evoluzione delle truffe di phishing per osservare il modo in cui i cambiamenti nella consapevolezza culturale possono riuscire a mitigare tecniche specifiche nel corso del tempo. Comprendere i diversi tipi di truffa può aiutare i professionisti della sicurezza a istruire i dipendenti su come adottare un approccio scettico e zero trust di fronte a opportunità, richieste di verifica o notifiche push apparentemente legittime. Quando si delinea una strategia volta a ridurre gli incidenti di phishing, è consigliabile includere le seguenti tipologie di truffe più comuni:

Le principali categorie di truffe di phishing

Le truffe cloud emulano servizi di condivisione di file o di archiviazione cloud. Come esche impiegano richieste di accesso false e notifiche fittizie sugli account.

Le truffe ai **consumatori** emulano marchi di e-commerce. Come esche utilizzano notifiche fittizie degli account e richieste false di iscrizione o di riscossione di vantaggi.

Le truffe **commerciali** emulano servizi generici come FedEx. Come esche utilizzano notifiche sul tracciamento delle spedizioni o richieste di pagamento.

Le truffe **aziendali** emulano aziende specifiche. Come esche utilizzano notifiche false sugli account, aggiornamenti aziendali, attività delle risorse umane e false richieste di pagamento di fatture.

Le truffe di **dating** emulano individui in cerca di appuntamenti su una piattaforma online. Come esche utilizzano profili falsi, messaggi, Mi piace e follower fittizi.

Le truffe relative ai **servizi finanziari** emulano istituti finanziari noti. Come esche per colpire gli individui, utilizzano notifiche false sugli account o avvisi di sicurezza fittizi.

Le truffe **governative** emulano le agenzie governative, come l'Agenzia delle Entrate. Come esche utilizzano richieste fittizie di benefit, sussidi e richieste per pagamenti insoluti.

Le truffe basate sulle **offerte di lavoro** si presentano come aziende fittizie e reali alla ricerca di nuovi dipendenti. Sfruttano esche come candidature, offerte e annunci di lavoro falsi.

Le truffe basate su **notifiche push o browser** emulano le notifiche web del browser. Come esche utilizzano falsi promemoria per l'installazione di aggiornamenti, notifiche di messaggi e pubblicità sui prodotti.

Le truffe basate sui **social media** emulano piattaforme social o utenti. Come esche impiegano account finti o falsificati, messaggi privati, avvisi o notifiche sull'account e avvisi di sicurezza fittizi.

Le truffe **tecniche** emulano servizi generali o marchi noti. Impiegano esche come notifiche sugli account, messaggi di errore e aggiornamenti software.

Experience your world, secured.™

Informazioni su Zscaler

Zscaler (NASDAQ: ZS) accelera la trasformazione digitale in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. Zscaler Zero Trust Exchange™ protegge migliaia di clienti dagli attacchi informatici e dalla perdita di dati, collegando in modo sicuro utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in oltre 150 data center a livello globale, Zero Trust Exchange, basata su SASE, è la piattaforma di cloud security inline più grande del mondo. Per saperne di più, visita il sito www.zscaler.it.

+1 408.533.0288

Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134

zscaler.it