ThreatLabz–Report: Phishing 2023

ThreatLabz–Report: Phishing 2023

Inhalt

Kurzfassung

Phishing-Angriffe werden immer mehr zur Bedrohung, da sich Cyberkriminelle zunehmend raffinierter Methoden bedienen, die ihre Erkennung und Blockierung erschweren.

Bei der Analyse von 280 Milliarden Transaktionen und 8 Milliarden blockierten Angriffen pro Tag verzeichnete das ThreatLabz-Team von Zscaler für 2022 eine Zunahme der versuchten Phishing-Angriffe um 47,2 % im Vergleich zu 2021 — ein Aufwärtstrend, der sich voraussichtlich auch 2023 fortsetzen wird.

Auch die Verwendung von auf dem Schwarzmarkt erworbenen Phishing-Kits und Chatbot-KI-Tools wie ChatGPT setzt sich immer mehr durch und macht es Angreifern leicht, zielgerichtete Phishing-Kampagnen zu entwickeln. Damit können User noch leichter manipuliert und zur Preisgabe ihrer Zugangsdaten bewegt werden, wodurch sie sich selbst und ihre Organisation für Angriffe anfällig machen.

Mit der Verbreitung von KI- und PaaS-Angeboten haben Cyberkriminelle es einfacher denn je, Institutionen zu kompromittieren und auf vertrauliche geschäftliche, personenbezogene und Finanzdaten zuzugreifen, um sie zu erpressen. Wenngleich viele Organisationen bereits robuste Infrastrukturen zur Gewährleistung der Cybersicherheit aufgebaut haben, macht die aktuelle Bedrohungslage eine Neubewertung dieser Infrastrukturen erforderlich. Dabei ist insbesondere zu erwägen, inwieweit ein Zero-Trust-Ansatz effektiven Schutz bieten kann.

Dieser Report soll Sie mit den Social-Engineering- und Coding-Strategien hinter Phishing-Angriffen vertraut machen und Sie so in die Lage versetzen, kostspielige Sicherheitsverstöße künftig zu verhindern. Wir liefern Ihnen detaillierte Einblicke in aktuelle Phishing-Trends und Erkenntnisse, die das ThreatLabz-Team im Laufe des letzten Jahres gesammelt hat, sowie Best-Practice-Empfehlungen zum Schutz Ihrer Organisation vor den sich ständig weiterentwickelnden Phishing-Techniken.

Haupterkenntnisse für 2022

Die Anzahl der versuchten Phishing-Angriffe nahm von 2021 auf 2022 um 47,2 % zu.

Microsoft-Marken wie OneDrive und SharePoint waren 2022 neben der Kryptobörse Binance und illegalen Streaming-Services am stärksten betroffen.

Standorte in den USA, in Großbritannien/Nordirland, den Niederlanden, Russland und Kanada wurden besonders häufig ins Visier genommen.

Der Bildungssektor war 2022 das beliebteste Phishing-Ziel von Cyberkriminellen mit einem Zuwachs von **576 %**. Die Angriffe auf die Einzel- und Großhandelsbranche, den Spitzenreiter von 2021, gingen um **67 %** zurück.

Der Anteil von COVID-bezogenen Angriffen mit Markenimitation, die 2021 noch **7,2 %** aller beobachteten Phishing-Maschen ausmachten, ging 2022 auf **3,7 %** zurück.

KI-Tools haben maßgeblich zur Zunahme von Phishing-Angriffen beigetragen, indem sie die technischen Eintrittsbarrieren für Cyberkriminelle verringern und ihnen Zeit und Ressourcen sparen.

Angreifer gehen zunehmend zum Phishing über Anrufe oder Sprachnachrichten (Vishing) über, um Opfer zum Öffnen schädlicher Anhänge zu verleiten.

Mithilfe komplexer AiTM-Angriffe (Adversary-in-the-Middle) gelingt es Bedrohungsakteuren, die Multifaktorauthentifizierung (MFA) zu umgehen.

Recruitment-Maschen, die Arbeitssuchende ins Visier nehmen, nehmen an Häufigkeit zu.

Häufigste Ziele von Phishing-Angriffen 2022

Das ThreatLabz-Team von Zscaler hat Daten aus verschiedenen Ländern, Branchen, Marken und Plattformen analysiert, um die häufigsten Ziele für Phishing-Angriffe im Jahr 2022 zu ermitteln.

Phishing-Angriffe nach Ländern 2022

Folgende zehn Länder waren am stärksten von Phishing-Angriffen betroffen:

1. Vereinigte Staaten von Amerika
2. Vereinigtes Königreich
3. Niederlande
4. Russland
5. Kanada
6. Singapur
7. Deutschland
8. Frankreich
9. Japan
10. China

Die USA, die das Ranking der beliebtesten Phishing-Ziele seit jeher anführen, sind auch in diesem Jahr auf Position eins zu finden. Unsere Analyse ergab, dass über 65 % aller versuchten Phishing-Angriffe in den USA stattfanden — im Vorjahr waren es 60 %. Die versuchten Phishing-Angriffe auf Ziele in Großbritannien nahmen um 269 % zu.

Mehrere Länder verzeichneten im Jahr 2022 eine Zunahme der versuchten Phishing-Angriffe — allen voran Kanada mit einem Anstieg um 718 %. Einige ThreatLabz-Experten führen diesen Anstieg auf die gleichzeitige Zunahme von Angriffen auf Ziele im Bildungswesen zurück. Angriffsversuche auf Ziele in Russland und Japan nahmen um 198 % bzw. 92 % zu. Ungarn verzeichnete jedoch einen deutlichen Rückgang der Phishing-Angriffe um 90 %. Die Anzahl der Angriffe auf Ziele in Singapur ging ebenfalls um fast 48 % zurück.

Der Rückgang der Phishing-Angriffe auf Ziele in Singapur ist möglicherweise auf die verschärften staatlichen Cybersicherheitsmaßnahmen zurückzuführen, insbesondere die Initiativen der Cyber Security Agency (CSA). Diese Behörde stellt Privatpersonen und Unternehmen Richtlinien und Ratschläge zum Schutz vor Cyberbedrohungen bereit und setzt zusammen mit der Personal Data Protection Commission (PDPC) Datenschutzgesetze und -vorschriften durch.

Abb. 1: Phishing-Angriffe nach Ländern 2022

Versuchte Phishing-Angriffe nach Branchen 2022

Der Bildungssektor verzeichnete 2022 einen Anstieg der versuchten Phishing-Angriffe um 576 %, was ihn vom achten Platz unter den am stärksten betroffenen Branchen auf den ersten katapultierte und den letztjährigen Spitzenreiter, die Einzel- und Großhandelsbranche, auf Rang zwei verwies. Insbesondere in den USA nutzten Phishing-Angreifer offensichtlich die 2022 eingeleiteten Verfahren zur Rückzahlung von Studentendarlehen und Anträge auf Schuldenerlass aus. Sicherheitslücken bei der Bereitstellung von Fernunterricht dürften ebenfalls zur Zunahme der Angriffe beigetragen haben. Die Finanz- und Versicherungsbranche verzeichnete 2022 ebenfalls einen Anstieg der Phishing-Angriffe um 273 %.

Versuchte Phishing-Angriffe auf Ziele in der Gesundheitsbranche nahmen ebenfalls stark zu — von knapp 31 Millionen auf über 114 Millionen.

Patienten, die im ersten Jahr der COVID-19-Pandemie routinemäßige medizinische Vorsorgeuntersuchungen verschoben hatten, nahmen ihre Behandlungen 2022 wieder auf, meldeten sich bei ihren Online-Konten an und interagierten möglicherweise mit Phishing-Angreifern, die sich als Gesundheitsdienstleister oder Krankenversicherungen ausgaben. Darüber hinaus nutzen Ransomware-Angreifer zunehmend Phishing-Taktiken, um die Daten von Gesundheitsdienstleistern zu kompromittieren.

Im positiven Sinne gab es 2022 in anderen Branchen einen Rückgang der Phishing-Angriffe zu vermelden — so im Einzel- und Großhandel um 67 % und im Dienstleistungssektor um 38 %. Der rückläufige Trend im Einzel- und Großhandel ist wahrscheinlich auf eine Abschwächung des Konsumverhaltens nach den massiven Online-Einkäufen von 2021 zurückzuführen.

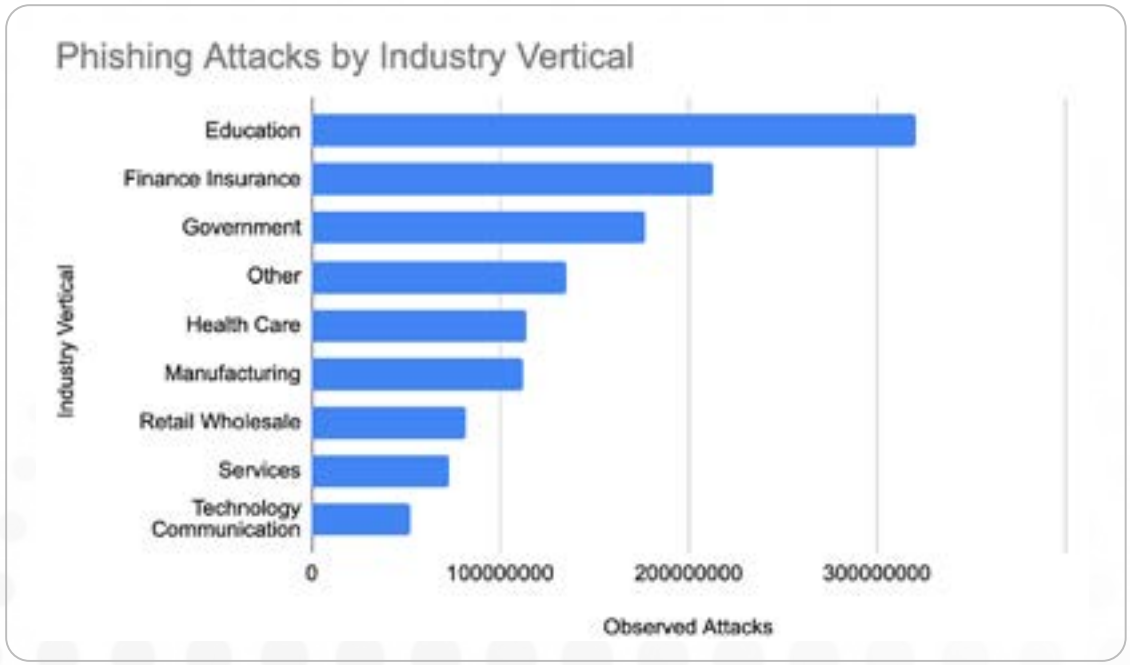
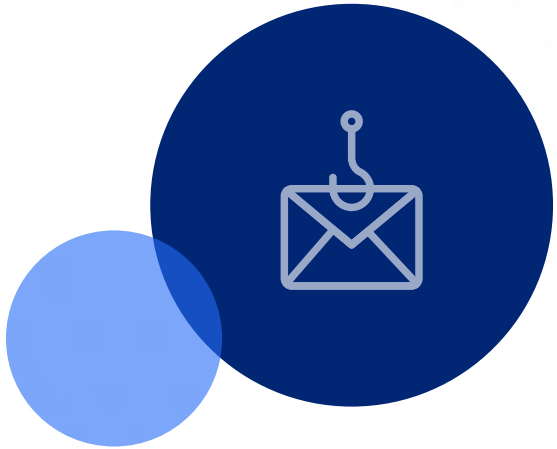


Abb. 2: Phishing-Angriffe nach Branchen 2022



Marken, die 2022 bei Phishing-Angriffen am häufigsten imitiert wurden

Phishing-Angreifer nutzen häufig Verbrauchertrends aus, indem sie sich als Vertreter beliebter Marken ausgeben, um User zu täuschen. Zu den am häufigsten imitierten Marken gehören Produktivitätstools, Kryptowährungsbörsen, illegale Streaming-Websites, Social-Media-Plattformen und Messaging-Services, Finanzinstitute, Websites von Behörden und Logistikdienstleister.

Microsoft war auch 2022 wieder die am häufigsten imitierte Marke mit einem Anteil von knapp 31 % der beobachteten Angriffsversuche. Weitere 17 % entfielen auf die Microsoft-Marke OneDrive, fast 4 % auf SharePoint und weitere 1,7 % auf Microsoft 365. Die Analyse von Zscaler ergab, dass Angreifer 2022 zum Versenden von Malware über Phishing-E-Mails zunehmend OneNote ausnutzten, das in OneDrive und andere Microsoft-Produkte integriert werden kann. Seit Microsoft im Juli 2022 Makros standardmäßig in allen Microsoft-365- bzw. Office-Anwendungen deaktiviert hat, hat auch die Verbreitung von Malware mittels schädlicher makrofähiger Dokumente an Bedeutung verloren.

Auf die Kryptowährungsbörse Binance entfielen 17 % der Angriffe mit Markenimitation, wobei sich Phisher als vermeintliche Kundenvertreter von Banken oder P2P-Unternehmen ausgaben. Illegale Streaming-Websites machten weitere 13,6 % der Angriffe aus und erreichten Spitzenwerte bei sportlichen Großereignissen wie der Fußball-Weltmeisterschaft im November und Dezember 2022.

Phishing-Angriffe mit COVID-Bezug bleiben weiterhin akut, jedoch ging ihre Bedeutung im Vergleich zum Vorjahr zurück. Der Anteil von COVID-bezogenen Angriffen mit Markenimitation, die 2021 7,2 % aller beobachteten Phishing-Maschen ausmachten, betrug 2022 nur noch 3,7 %.

Folgende Marken wurden 2022 bei Phishing-Angriffen am häufigsten imitiert:

1. Microsoft
2. OneDrive
3. Binance
4. Illegale Streaming-Websites
5. SharePoint
6. COVID-19-Hilfen
7. Behörden
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

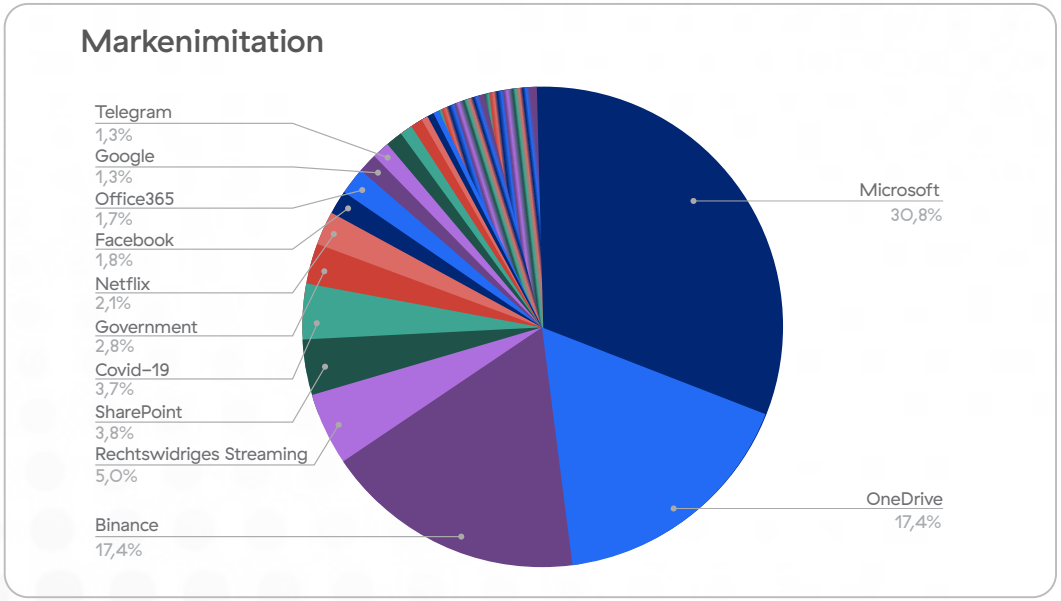


Abb. 3: Marken, die bei Phishing-Angriffen am häufigsten imitiert wurden

Wichtigste verweisende Domains 2022

Häufig nutzen Angreifer vertrauenswürdige Domains aus, um Opfer zu manipulieren und sie auf Phishing-Websites umzuleiten. Dabei schalten sie z. B. Werbeanzeigen in Medienkanälen oder auf Suchplattformen wie Google und Bing, veröffentlichen Inhalte in Unternehmensforen und Online-Marktplätzen wie Walmart und Amazon oder missbrauchen Filesharing-Plattformen/-Dienste wie Evernote, Dropbox und GitHub.

Durch Analysieren der verweisenden Domains konnten wir ermitteln, welche Domains am häufigsten für Angriffe missbraucht werden. 2022 zählten dazu u. a. Video-Streaming-Websites, Krypto-Börsen und andere Finanz-Websites, Website- und Formularersteller, Websites, die usergenerierte Inhalte hosten, und Suchmaschinen.

Folgende 20 Domains wurden am häufigsten für Verweise missbraucht:

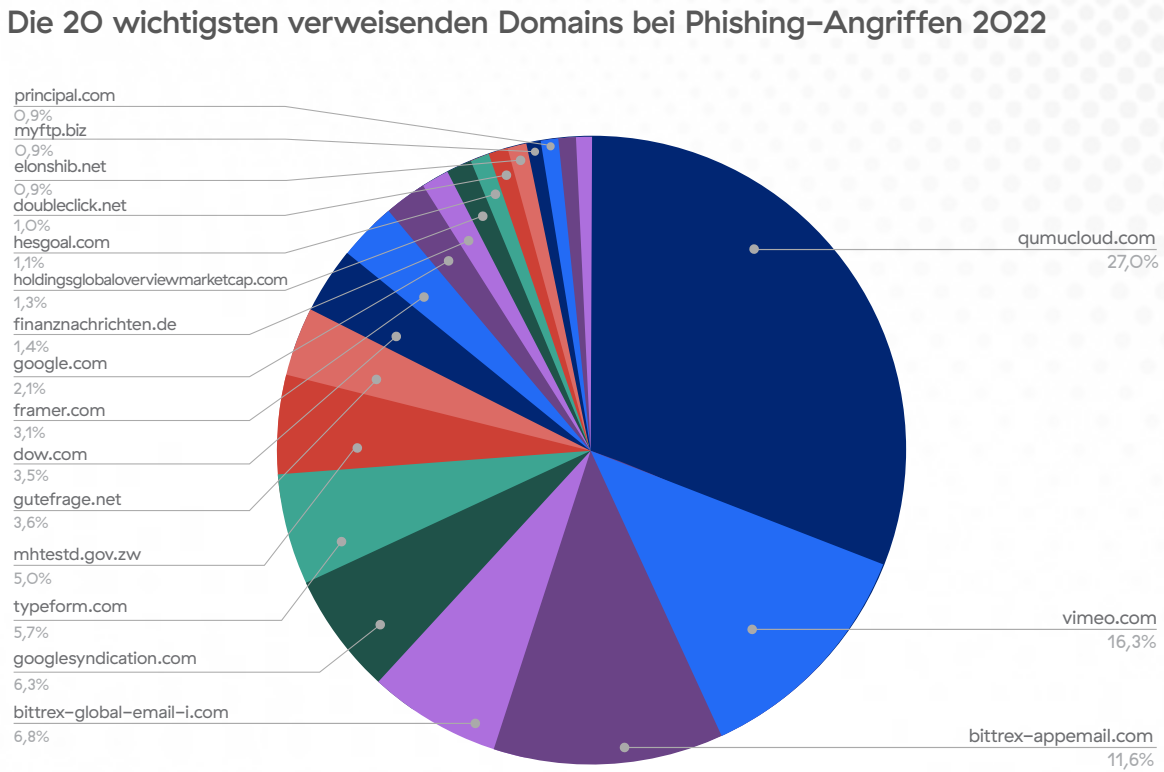


Abb. 4: Die häufigsten verweisenden Domains bei Phishing-Angriffen 2022

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

Ausnutzung autonomer Systeme für Angriffe 2022

Als autonomes System (AS) wird ein Netzwerk bzw. eine Gruppe von Netzwerken mit einer einzigen Routing-Richtlinie bezeichnet. Jedes AS hat eine eindeutige numerische Kennung, die sogenannte ASN. Im Rahmen dieser Analyse überprüfte das ThreatLabz-Team von Zscaler die ASNs, die für das Hosten der Phishing-Infrastruktur verantwortlich waren.

Unsere Analyse ergab, dass 39 % der 2022 beobachteten Phishing-Angriffe über Hosting-Websites erfolgten (gegenüber 50,6 % im Vorjahr), 53 % über ISPs (gegenüber 39,2 % im Jahr 2021) und 8 % über Unternehmensdomains.

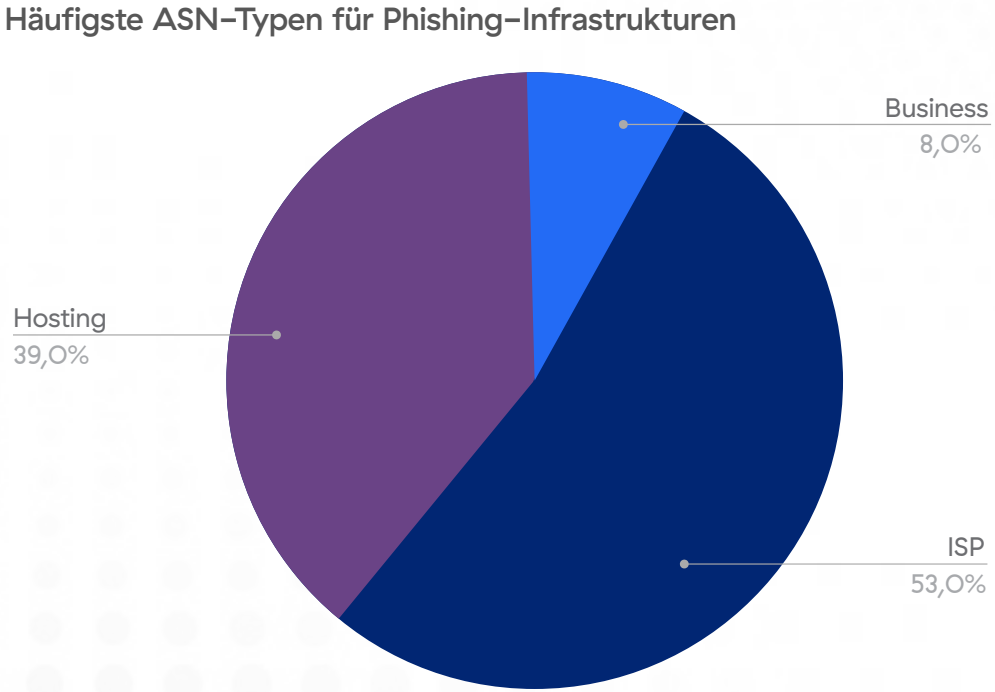


Abb. 5: ASNs für Phishing-Infrastrukturen

Phishing-Trends

Die Taktiken und Ansätze, die Bedrohungsakteure bei Phishing-Kampagnen einsetzen, werden von Jahr zu Jahr raffinierter und komplexer. Damit Ihre Organisation entsprechend gewappnet ist und Ihre Sicherheitsbeauftragten den Angreifern immer einen Schritt voraus sind, ist es uns wichtig, Sie über aktuelle Bedrohungstrends auf dem Laufenden zu halten. Nachstehend werden daher die wichtigsten Erkenntnisse aus den 2022 beobachteten Phishing-Trends vorgestellt.

Vishing-Angriffe

Als Vishing-Angriffe werden Phishing-Kampagnen mittels Sprachnachrichten bezeichnet, die Opfer zum Öffnen schädlicher Anhänge verleiten sollen. Mitte 2022 versandten Bedrohungsakteure schädliche E-Mails mit Sprachnachrichten an User verschiedener Organisationen in den USA, um ihre Anmeldedaten für Microsoft 365 und Outlook zu stehlen.

In unserer Analyse haben wir weitere Phishing-Kampagnen mit betrügerischen Sprachnachrichten in E-Mail-Anhängen beobachtet (siehe unten):

Abb. 6: E-Mail, wie sie im Rahmen einer Vishing-Kampagne versendet wird

Die .html-Datei enthält unkenntlich gemachtes JavaScript:

Abb. 7: Quellcode einer Vishing-E-Mail mit verstecktem JavaScript

Die Aufschlüsselung des Quellcodes zeigt, dass er User, die die Datei öffnen, auf einen von Angreifern kontrollierten Server umleiten würde:

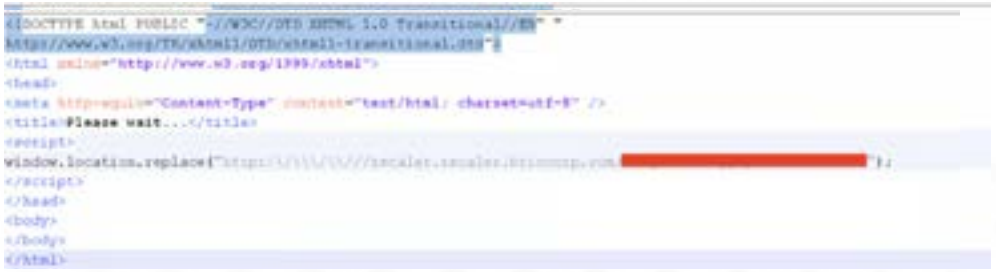


Abb. 8: Quellcode einer Vishing-E-Mail mit aufgeschlüsseltem JavaScript

Der User wird dann zu einer gefälschten Microsoft–Seite weitergeleitet:

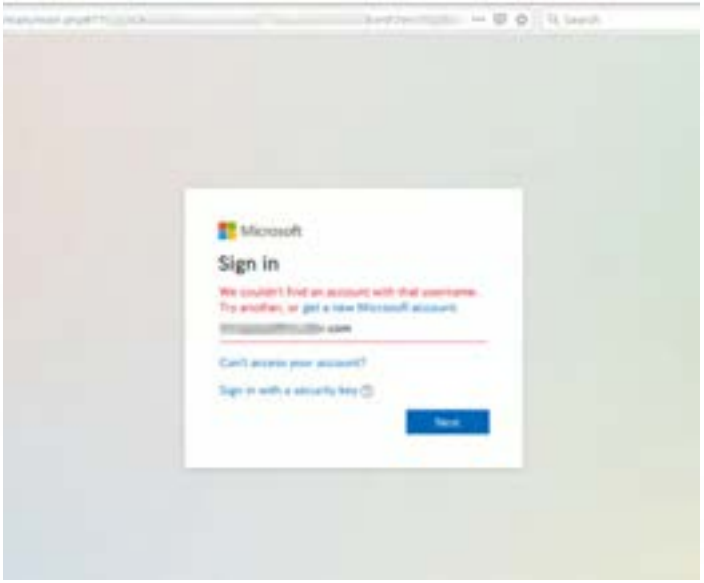


Abb. 9: Landingpage einer Vishing–Kampagne

ThreatLabz deckte auch eine Betrugsmasche mittels Sprachanrufen auf, bei dem ein Bedrohungsakteur sich gegenüber einem Unternehmensmitarbeiter als Vorgesetzter ausgibt. Zunächst erhält das Opfer einen Telefonanruf mit einer vorab aufgezeichneten Grußformel, dann wird der Anruf beendet. Anschließend erhält das Opfer vom Betrüger eine Nachricht, der Vorgesetzte habe Probleme mit der Netzwerkverbindung, und wird aufgefordert, die Kommunikation per Textnachricht fortzusetzen. Der Betrüger versucht dann, das Opfer dazu zu bringen, Bankverbindungen des Unternehmens preiszugeben oder Geld zu überweisen.

Um zu verhindern, dass Mitarbeiter Phishing–Betrügern auf den Leim gehen, müssen sie entsprechend darin geschult werden, nur über offizielle Kanäle der Organisation miteinander zu kommunizieren und ständig vor potenziellen Bedrohungen auf der Hut zu sein.

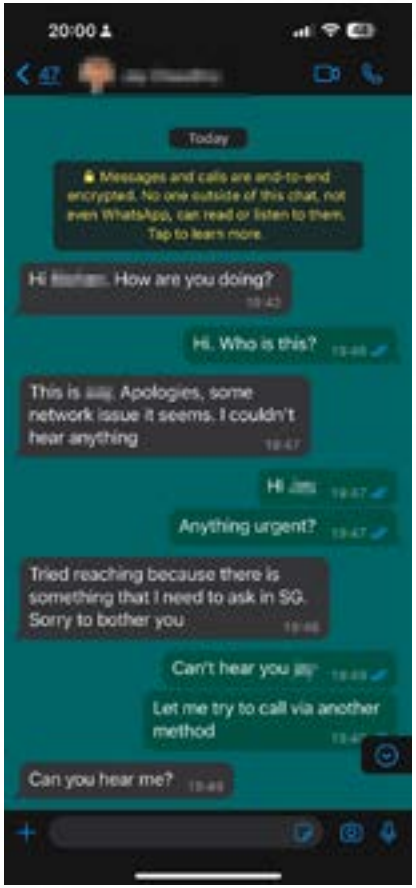


Abb. 10: Textnachricht im Rahmen einer Vishing–Kampagne

Recruitment–bezogene Betrugsmaschen

Im Jahr 2022 verzeichnete ThreatLabz eine Zunahme gezielter Angriffe auf Arbeitssuchende, bei denen verschiedene Betrugsmaschen zum Einsatz kamen. Dabei wurden erfundene Stellenausschreibungen, Websites oder Portale und Formulare verwendet, um Arbeitssuchende zu ködern.

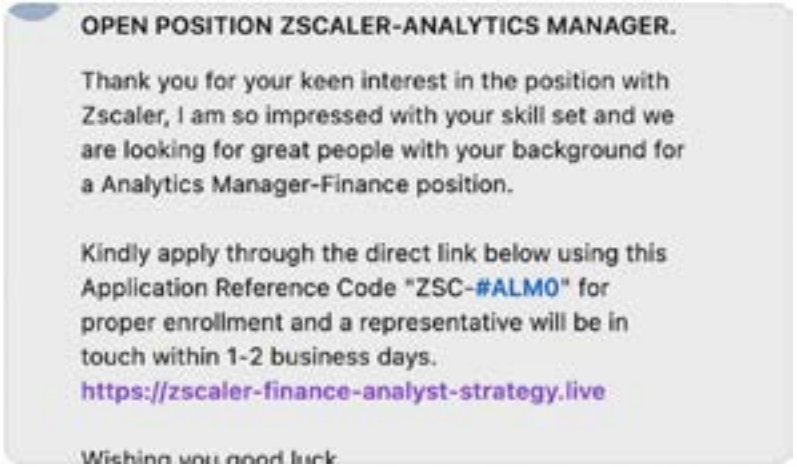


Abb. 11: Gefälschte LinkedIn–Werbung mit Phishing–URL

In diesem Beispiel hat der Angreifer eine gefälschte LinkedIn–Werbung mit einer Phishing–URL veröffentlicht. Die URL leitet potenzielle Opfer vorgeblich zu einem Stellenangebot weiter.

Sobald sich das Opfer auf die Stelle bewirbt, kommuniziert der Angreifer mit ihm und vereinbart ein Bewerbungsgespräch auf Skype, bei dem sich der Angreifer als Personalbeauftragter ausgibt.

Abb. 12: Gefälschte Recruitment–E–Mail

Die Analyse des Quellcodes zeigt, dass er Code zum Exfiltrieren von Kreditkartendaten beinhaltet.

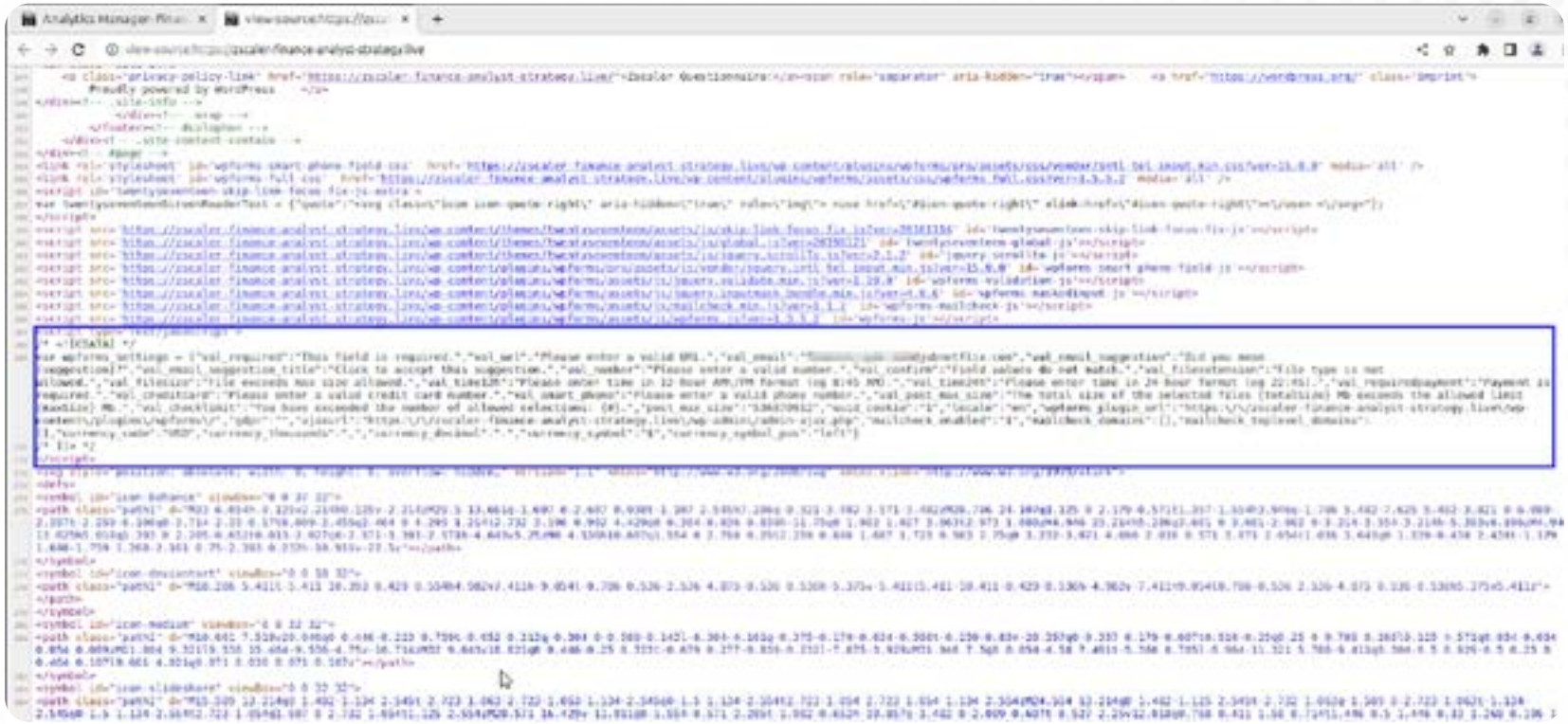


Abb. 13: Quellcode für betrügerische Recruitment–E–Mail

AiTM–Phishing–Angriffe (Adversary–in–the–Middle)

Hier finden Sie weitere Informationen zu AiTM–Phishing–Angriffen (Adversary–in–the–Middle).

Das ThreatLabz–Team fand einen neuen Stamm einer groß angelegten Phishing–Kampagne, die AiTM–Techniken zusammen mit verschiedenen Umgehungstaktiken verwendet. Herkömmliche Phishing–Websites, die Anmeldedaten von Usern erfassen, schließen den Authentifizierungsprozess niemals über den Server des eigentlichen E–Mail–Anbieters ab. Wenn der User Multi–Faktor–Authentifizierung (MFA) aktiviert hat, verhindert dies, dass sich der Angreifer nur mit den gestohlenen Zugangsdaten beim Konto anmelden kann. Teilweise setzen Angreifer AiTM–Phishing zur Umgehung der MFA ein.

Abb. 14 zeigt ein Codeschnipsel einer Phishing–Seite, das von einem AiTM–Phishing–Server ausgeliefert wird.

Abb. 14: Quellcode einer Phishing–Seite, der vom AiTM–Phishing–Server ausgeliefert wird

Der AiTM–Proxyserver ersetzt die URLs auf einer legitimen Zielseite mit vom Angreifer kontrollierten URLs (siehe Abb. 15) und fungiert als Vermittler zwischen dem Opfer und dem Zielserver.

Abb. 15: Vom Angreifer kontrollierte URLs, die vom AiTM–Proxyserver geändert wurden

Die ursprüngliche Subdomäne (in Grün), der ursprüngliche Domänenname (in Blau, ohne die TLD) und eine generierte eindeutige ID (in Rosa) werden durch Bindestriche miteinander verbunden und als Subdomäne unter der Domäne der Phishing–Site (in Orange) eingerichtet.

Wir konnten diese Taktik aufdecken, als Anfragen mit inkorrekten Änderungen an Opfer weitergeleitet wurden (siehe Abb. 16).

Abb. 16: Inkorrekte Änderungen, die an das Phishing–Opfer weitergegeben wurden

Dadurch wurde die vom Angreifer kontrollierte Serveradresse offengelegt (siehe Abb. 17).

Abb. 17: Offenlegung der vom Angreifer kontrollierten Serveradresse

BiTB–Phishing–Angriffe (Browser–in–the–Browser)

Der Einsatz von BiTB–Phishing–Angriffen nahm 2022 ebenfalls zu. Dabei wird ein Anmeldeseitenfenster innerhalb einer Phishing–Hauptseite simuliert, um das Opfer zur Eingabe seiner SSO–Anmeldedaten (Single–Sign–On) zu verleiten.

Angreifer verwenden eine Kombination aus einfachem HTML/CSS und Inline–Frame (iFrame), um ein gefälschtes Popup–Fenster zu erstellen, das das gewohnte SSO–Popup–Fenster des Users simuliert. Für User ist es fast unmöglich, ein echtes Popup von einer gut gemachten Phishing–Fälschung zu unterscheiden.

Abbildung 18 zeigt ein Beispiel für einen BiTB–Angriff auf die beliebte digitale Spieleplattform Steam mit einem gefälschten SSO–Fenster, das mittels HTML generiert wurde.

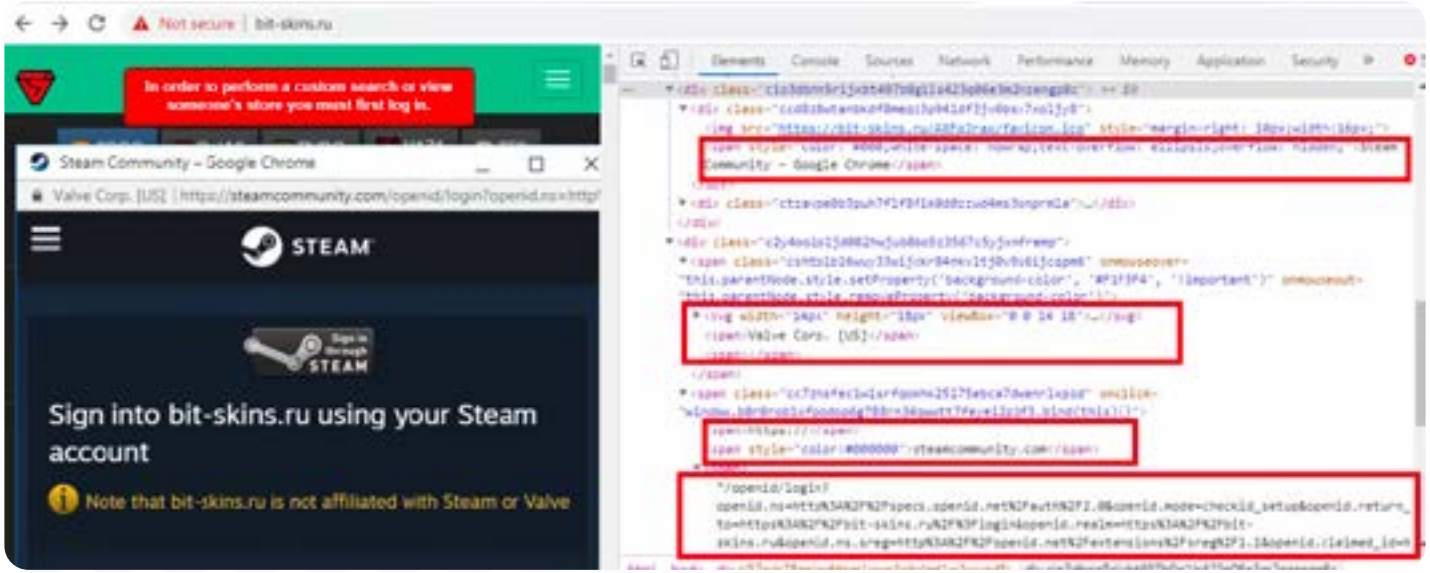


Abb. 18: BiTB–Angriff

Missbrauch legitimer Services zum Hosten von Phishing–Websites

Teilweise wurden bei den vom ThreatLabz–Team analysierten Angriffen legitime Hosting–Dienste zum Hosten von Phishing–Websites missbraucht. Betroffen waren Anbieter von kostenlosen Hosting–Diensten wie OOwebhostapp.com ebenso wie Filesharing–Services wie transfer.sh, Cloud–Service–Anbieter wie amazonaws.com und Kurzlink–Dienste, die u. a. über LinkedIn bereitgestellt werden.

Ebenfalls wurden Angriffe beobachtet, die dynamische DNS–Dienste ausnutzten. Diese Dienste, die die Zuordnung von Domänennamen zu sich ändernden IP–Adressen unterstützen, werden von Usern hauptsächlich für den Remotezugriff oder das Hosten von Websites in Heimnetzwerken verwendet.

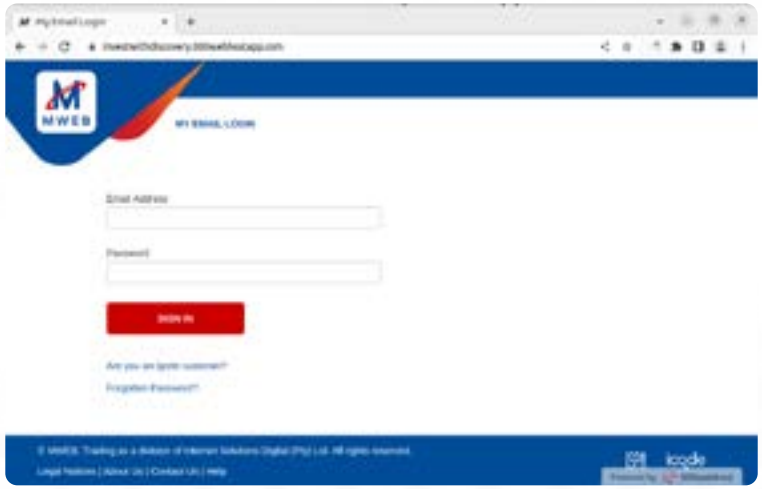


Abb. 19: Missbrauch dynamischer DNS–Subdomänen zum Hosten von Phishing–Seiten (Beispiel 1)

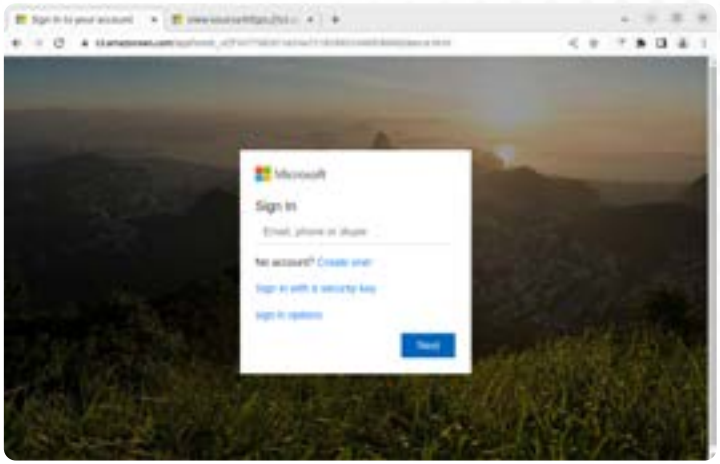


Abb. 20: Missbrauch dynamischer DNS–Subdomänen zum Hosten von Phishing–Seiten (Beispiel 2)

In manchen Fällen wurden dynamische DNS–Dienste auch dazu missbraucht, Phishing–Websites auf kompromittierten Computern oder Servern ohne feste IP–Adressen zu hosten.

Abb. 21: T&T–Phishing–Website, die mit dynamischem DNS gehostet wird

Phishing–Angriffe über das InterPlanetary File System (IPFS)

IPFS ist ein distribuiertes Peer–to–Peer–Dateisystem, das es Usern ermöglicht, Dateien in einem dezentralen Netzwerk von Computern zu speichern und gemeinsam zu nutzen. Im Vergleich zu herkömmlichen zentralisierten Dateisystemen stellt es eine sicherere, robustere und effizientere Möglichkeit zum Speichern und Verteilen von Dateien bereit.

Im IPFS werden Dateien in kleinere Blöcke aufgeteilt und auf mehrere Nodes in einem Netzwerk verteilt, wodurch das Risiko verringert wird, dass ein Single Point of Failure das gesamte System kompromittiert. Abbildung 22 zeigt, wie das IPFS für Phishing–Angriffe missbraucht werden kann.

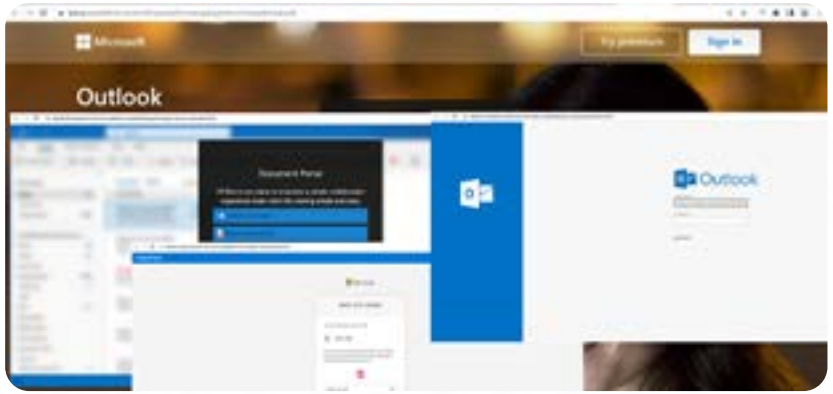


Abb. 22: Beispiel für IPFS–Phishing

Aufgrund der Peer–to–Peer–Konstruktion ist die Entfernung einer über das IPFS gehosteten Phishing–Seite mit sehr viel größeren Schwierigkeiten verbunden als beim Hosting mit herkömmlichen Methoden.

In anderen Fällen nutzten Phishing–Angreifer Google Translate, um ihre URLs legitim erscheinen zu lassen.

Abb. 23: Beispiel für einen IPFS–Phishing–Angriff, bei dem Google Translate ausgenutzt wird

Abbildung 23 zeigt, wie Angreifer Google Translate auf einer im IPFS gehosteten Phishing–Website einsetzten und die Seite dann zum Phishing von DocuSign–Anmeldedaten verwendeten.

Exfiltration von Daten mit Fingerabdruck über WebSockets

Im Phishing-Report des ThreatLabz-Teams für 2022 haben wir das Thema Phishing-Kits und quelloffene Phishing-Frameworks bereits angesprochen. Mit diesen Kits und Frameworks werden die erforderlichen Tools gebündelt und vermarktet, um auch ohne technische Vorkenntnisse schnell Hunderte oder Tausende überzeugender und effektiver Phishing-Seiten zu starten.

Teilweise verfügen diese Phishing-Kits über eine Funktion namens „Cloaking", mit der Angreifer Phishing-Webseiten vor Sicherheitsexperten und Scannern verbergen können, sie jedoch für die Opfer sichtbar bleiben. Das Phishing-Kit filtert Verbindungen für jeden Besucher basierend auf IP-Adresse, Schlüsselwörtern für Hostnamen, User-Agent usw. Auf der Grundlage der Ergebnisse wird entweder eine harmlose Seite oder eine Phishing-Seite bereitgestellt, wodurch die Erkennung durch Sicherheitsexperten und Anti-Phishing-Tools vermieden wird, die das Internet nach schädlichen Inhalten durchsuchen. Bedrohungsakteure setzen unterschiedliche Cloaking-Techniken zur Umgehung solcher Erkennungsmethoden ein.

Erstmals haben wir in diesem Jahr den Einsatz einer neuen Technik des Client-Fingerprinting beobachtet. Wenn ein Besucher auf einer Phishing-Seite landet und mit einem Fingerabdruck versehen wird, werden folgende Vorgänge durchgeführt:

1. Der Benutzer surft auf der Phishing-Seite.
2. Der Server generiert ein JavaScript, um einen Fingerabdruck des Clients zu erstellen, der dann über eine WebSocket-Verbindung hochgeladen wird.
3. Der Server generiert anhand des Fingerabdrucks ein Cookie und sendet das Cookie über WebSocket zurück.
4. Der JavaScript-Code aktualisiert die Seite automatisch mit dem Cookie.
5. Der User wird auf die Phishing-Seite umgeleitet, sofern die Cookies die Kontrollen erfolgreich durchlaufen.

Das JavaScript zum Erstellen der Fingerabdrücke basiert auf diesem Open-Source-Projekt auf 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"
  },
```


Abb. 24: Fingerabdruckdaten einer Maschine

Als effektive Abwehrmaßnahme gegen diese Technik empfiehlt sich die Überwachung der WebSocket–Kommunikationen und die Filterung von Fingerabdruckdaten. Manche Phishing–Kits richten C2–Kommunikationen (Command–and–Control) ein, um Befehle von Phishing–Servern über WebSocket zu empfangen. Hierbei kommt eine als Heartbeat–Kommunikation bezeichnete Technik zum Einsatz, die es dem Angreifer ermöglicht, Daten zum und vom Gerät des Opfers zu senden und zu empfangen.

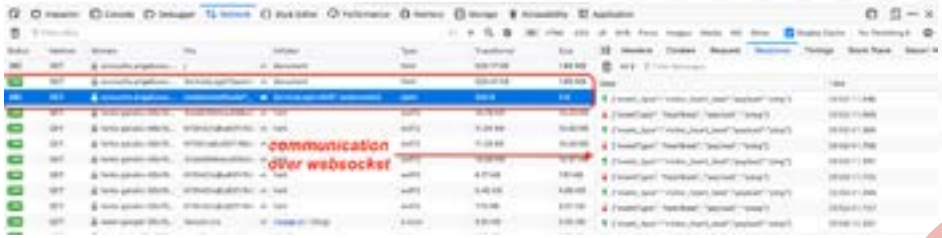
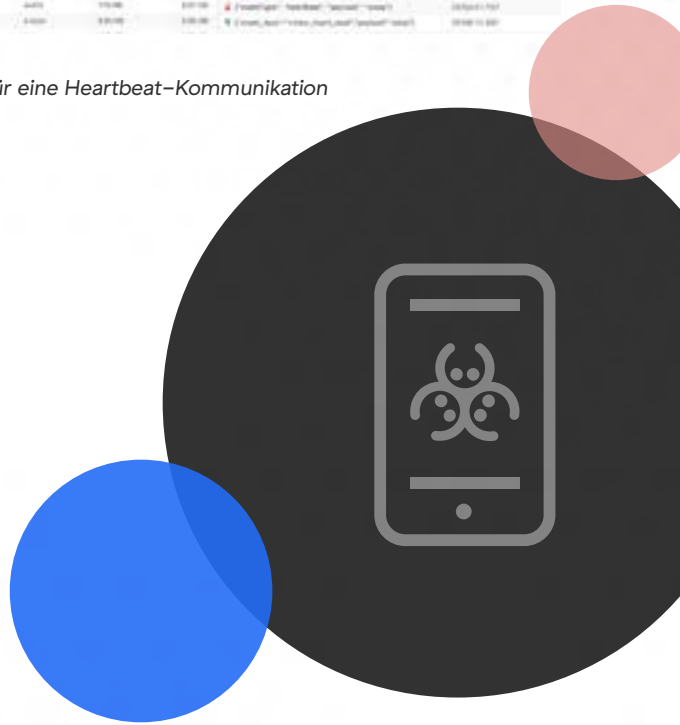


Abb. 25: Beispiel für eine Heartbeat–Kommunikation



Missbrauch webbasierter Formulare zum Erfassen von Anmeldedaten

Es wurden auch Angriffe beobachtet, bei denen Bedrohungsakteure Services missbrauchten, die die Erfassung von Daten über Formulare unterstützen. FormSubmit z. B. ist ein webbasierter Service, der eine einfache Möglichkeit bietet, HTML–Formulare für Websites einzurichten und zu verwalten. Organisationen können damit benutzerdefinierte Formulare mit verschiedenen Eingabefeldern wie Kontrollkästchen, Textfelder, Optionsfelder, Dropdown–Listen und Datei–Uploads erstellen und die Formulardaten dann an eine bestimmte E–Mail–Adresse oder Webhook–URL senden.

Das Beispiel in Abbildung 26 zeigt, wie Angreifer Services zur Formularerstellung missbrauchen können, um Anmeldedaten zu stehlen, ohne Server einrichten zu müssen.

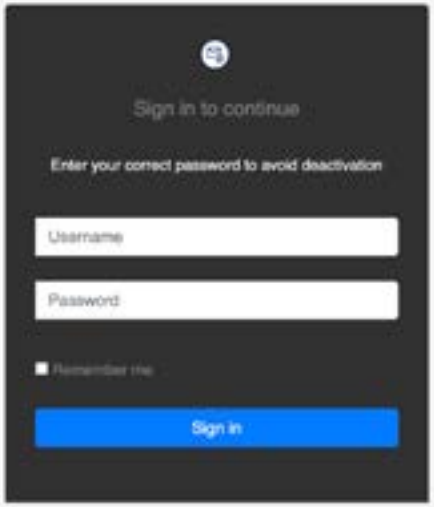


Abb. 26: Beispiel für ein Formular

Die „Aktion“ für dieses Formular lautet „https://submit–form[.]com/Qz1kGknr“.

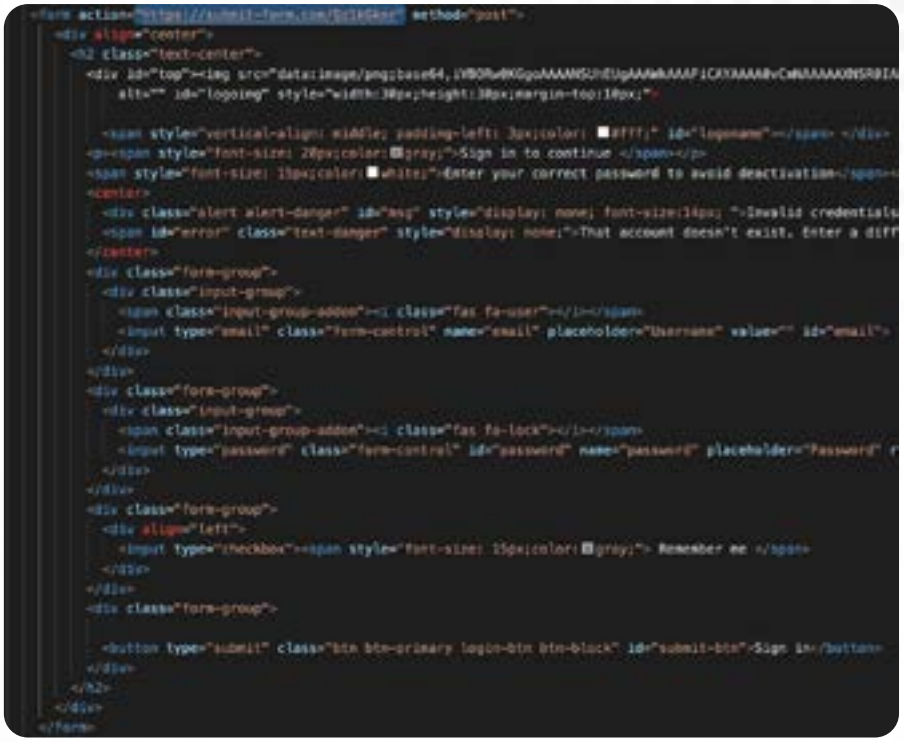


Abb. 27: Der Angreifer missbraucht den Formularservice zum Abfangen von Daten

Phishing-Angriffe mit HTML-Schmuggel und SVG-Dateien

HTML-Schmuggel ist eine Technik, mit der Angreifer Netzwerksicherheitskontrollen umgehen, indem sie Schadcode in scheinbar harmlosen HTML-Code einbetten und dann schädliche Payloads an ein Zielsystem übermitteln. Verdächtiges JavaScript wird bei der Bedrohungserkennung zumeist gescannt und erkannt, weswegen Bedrohungsakteure alle möglichen Arten von Malware vermehrt über HTML-Schmuggel ausliefern.

Angreifer verschieben häufig HTML-Schmuggelcode in Scalable Vector Graphics (SVG), ein auf XML basierendes Format zum Erstellen zweidimensionaler Grafiken, die sich ohne Auflösungsverluste skalieren lassen. Zur Bearbeitung der SVG-Dateien setzen sie Texteditoren und Grafiksoftware ein.

Angreifer können die Elemente und Attribute der SVG-Dateien mithilfe von JavaScript manipulieren, um verschiedene Animationen hinzuzufügen, z. B. Objekte zu bewegen, Farben zu ändern oder Übergänge zu erstellen. Mit JavaScript können SVG-Dateien interaktiv gestaltet werden, sodass User mit den Grafiken interagieren und verschiedene Animationen auslösen können.

Diese Methode bietet sich als attraktive Option für Angreifer an, da Sicherheitslösungen zur Bedrohungserkennung JavaScript innerhalb von SVG-Dateien normalerweise nicht überprüfen.

Phishing–Tools und –Techniken

Es sind verschiedene eigenständige Anwendungen oder Browser–erweiterungen online verfügbar, mit denen Angreifer legitime Websites kopieren und entsprechenden Code einbetten können, um Daten zu stehlen. Dazu gehören u. a.:

- **HTTrack,** eine weit verbreitete eigenständige Anwendung
- **singlefile,** eine Erweiterung für Google Chrome
- **Webscrapbook,** eine quelloffene Browsererweiterung
- **Save Page WE**, eine Erweiterung für Google Chrome

Phishing–Angriffe mittels iFrames

Ein iFrame ist ein HTML–Element, mit dem Webentwickler ein anderes HTML–Dokument in die aktuelle Webseite einbetten können. Es erstellt einen „Rahmen im Rahmen“, in dem der Inhalt des eingebetteten Dokuments in einem rechteckigen Feld auf der aktuellen Seite angezeigt wird. Bedrohungsakteuren gelingt es immer wieder, Kontrollmechanismen zu umgehen, indem sie Phishing–Inhalte in einen iFrame einbetten.

Es gibt verschiedene Möglichkeiten, iFrames für Phishing–Angriffe zu verwenden:

1. Verschachtelter iFrame
2. iFrame als Hintergrund
3. iFrame als Vordergrund (etwa bei BiTB–Angriffen)

Darüber hinaus gehen wir davon aus, dass auch „iFrames als Komponenten“ zunehmend relevant werden. Bei dieser Methode werden mehrere iFrames kombiniert, um eine Phishing–Seite zu generieren. In diesem Beispiel wird der erste iFrame zum Erfassen des Passworts verwendet (siehe Abb. 28):

Abb. 28: iFrame zum Erfassen von Benutzernamen

Der zweite iFrame wird zum Erfassen des Passworts verwendet (siehe Abb. 29):

Abb. 29: iFrame zum Erfassen von Passwörtern

Im letzten Schritt kombiniert die Phishing–Seite die beiden iFrames (siehe Abb. 30):

Abb. 30: Phishing–Seite mit kombinierten iFrames

WebAssembly-Phishing

WebAssembly ist ein binäres Anweisungsformat für eine virtuelle Maschine, die in heutigen Webbrowsern ausgeführt wird. Als portables Low-Level-Bytecode-Format, das mit nahezu nativer Geschwindigkeit ausgeführt werden kann, eignet es sich insbesondere für die Ausführung Performance-kritischer Anwendungen im Web.

WebAssembly wurde entwickelt, um die Einschränkungen von JavaScript bei der Ausführung von Webanwendungen zu umgehen. Der Code kann in verschiedenen Sprachen wie C++, Rust und Go geschrieben und dann in das Bytecode-Format von WebAssembly kompiliert werden.

Länderspezifische Phishing-Angriffe

Bedrohungsakteure, die gezielt User in bestimmten Ländern oder Sprachgebieten ins Visier nehmen, nutzen zur Identifizierung potenzieller Opfer teilweise APIs und entsprechende Services von Drittanbietern.

Geo Targetly ist ein Service, mit dem User die Inhalte ihrer Websites entsprechend dem geografischen Standort ihrer Besucher personalisieren können, indem sie benutzerdefinierte Regeln basierend auf Faktoren wie IP-Adressen, Spracheinstellungen und Zeitzonen erstellen.

Es überrascht nicht, dass Angreifer diesen Service als Cloaking-Technik zur Tarnung von Phishing-Inhalten missbrauchen.

Umgehen von Sicherheitskontrollen durch Ausnutzung von Punycode oder nicht standardmäßigen IP-Adressen in URLs

Eine IP-Adresse ist eine 32-Bit-Zahl, die durch unterschiedlich lange Ziffernfolgen dargestellt werden kann. Standardmäßig bestehen IP-Adressen aus vier Ziffern. Es gibt jedoch auch ein-, zwei- oder dreistellige IP-Adressen, wobei jede einzelne Ziffer mit einer anderen Basis (binär, oktal, dezimal, hexadezimal) dargestellt werden kann. Wenn Phishing-Angreifer eine IP-Adresse auf nicht standardmäßige Weise darstellen, kann sie Kontrollmechanismen umgehen. Um dies zu verhindern, empfiehlt sich die Normalisierung von IP-Adressen.

Phishing-Angriffe mittels „Hash in URLs“

Als „Hash“ wird der Abschnitt einer URL bezeichnet, der nach dem „#“-Symbol folgt. Ein Hash dient zur Identifizierung eines bestimmten Bereichs innerhalb einer Webseite, wie z. B. einer Abschnittsüberschrift oder eines einzelnen Absatzes, und ermöglicht es Usern, durch Anklicken eines Links oder Lesezeichens direkt zu diesem Bereich zu navigieren. Alternativ ist auch der Begriff „Fragmentbezeichner“ geläufig.

Die Zeichenkette, die nach dem „#“-Symbol folgt, wird nicht an den Server gesendet, sodass Änderungen am Hash keine Seitenaktualisierung auslösen. Diese Funktion wird häufig bei Single-Page-Anwendungen und dynamischen Webinhalten verwendet.

Phishing-Angreifer haben zwei neue Methoden gefunden, sie sich zunutze zu machen:

1. Darstellen von User-Daten als Hash.
   - E-Mail-Adressen sind am häufigsten betroffen. Auf der Anmeldeseite wird die E-Mail-Adresse automatisch ausgefüllt, um den User zu täuschen.
2. Generieren spezifischer Phishing-Seiten basierend auf dem Hash, die sich gezielt an einzelne User richten.

KI und Phishing

Aktuelle Fortschritte in der KI–Technologie wie ChatGPT machen es Angreifern sehr viel einfacher, Schadcode zu entwickeln, BEC–Angriffe (Business Email Compromise) zu generieren, polymorphe Malware zu erstellen usw. Wir haben selbst den Versuch unternommen, mit ChatGPT eine Phishing–Anmeldeseite zu generieren. Nach nur drei einfachen Interaktionen generierte das Tool diese Webseite:

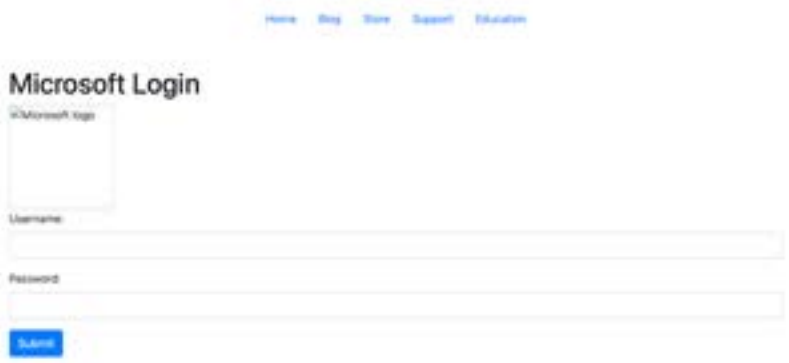


Abb. 31: Von ChatGPT generierte Phishing–Seite

Mit geringem Zusatzaufwand könnte ein Angreifer einen Hintergrund hinzufügen und ihn so bearbeiten, dass er wie eine echte Anmeldeseite aussieht.

Prognosen für 2024

1. **KI-basierte Angriffsmethoden werden immer häufiger zum Einsatz kommen,** je mehr neue Anwendungsfälle Bedrohungsakteure für diese Dienste entdecken. Rechnen Sie also mit der Auslieferung zunehmend raffinierter Phishing-Inhalte über verschiedene Kommunikationskanäle wie E-Mail, SMS und Websites. Außerdem sollten Sie auf eine rapide Zunahme versuchter Phishing-Angriffe vorbereitet sein, da immer mehr Akteure KI für besser koordinierte und effektivere Angriffe auf größere Personengruppen nutzen werden.

2. **Ebenfalls ist von der Weiterentwicklung der Phishing-as-a-Service-Angebote auszugehen,** wobei Anbieter sich insbesondere auf anpassbare Phishing-Vorlagen, Zugriff auf größere Datenbanken potenzieller Opfer und erweiterte Social-Engineering-Techniken spezialisieren dürften. Zusätzlich werden voraussichtlich Leistungen wie Malware-Installation, Hosting und Analysen angeboten. Dabei ist zu beachten, dass diese Anbieter darum konkurrieren, ein optimales Preis-Leistungs-Verhältnis mit erschwinglichen Preismodellen und einem rund um die Uhr verfügbaren Kundensupport bereitzustellen. Das wird eventuell zu einer Zunahme kleinerer Phishing-Angriffe führen — umso wichtiger ist es für Organisationen, sich über alle aktuellen Bedrohungen und Trends auf dem Laufenden zu halten.

3. **Auch gezielte Angriffe auf Mobilanwendungen und -geräte werden vermutlich zunehmen,** da Angreifer nur allzu gerne bereit sind, unsere Abhängigkeit von diesen Geräten auszunutzen. Entsprechend können Sie davon ausgehen, dass Phishing-Inhalte — Anwendungen, Websites und Malware, darunter insbesondere Spyware und Remotezugriff-Trojaner — künftig noch häufiger für Mobilgeräte optimiert werden. Ebenfalls steht zu erwarten, dass Phishing-Angreifer neue Möglichkeiten erschließen, aus der Erpressung ihrer Opfer Gewinn zu schlagen.

4. **MFA-Bombing und AitM-Angriffe stellen ebenfalls ein wachsendes Risiko dar,** da Angreifer laufend neue Wege finden, MFA-Sicherheitsmaßnahmen zu umgehen. Beim MFA-Bombing werden Opfer mit einem Strom von Authentifizierungsaufforderungen bombardiert. Bei AitM-Angriffen wird die Sitzung des Opfers abgefangen, nachdem es sich erfolgreich über MFA authentifiziert hat. Angreifern stehen heute fortschrittliche KI-basierte Techniken zur Verfügung, mit denen sich Verifizierungscodes vorhersagen bzw. generieren oder Muster im User-Verhalten identifizieren lassen, die für den Zugriff ausgenutzt werden. Zum Schutz vor diesen Angriffen ist es wichtig, sichere Passwörter zu verwenden, die Zwei-Faktor-Authentifizierung zu aktivieren und User-Konten auf verdächtige Aktivitäten zu überwachen.

5. **Personalisierte Angriffe werden in Zukunft noch schwerer erkennbar,** da Angreifer immer raffiniertere Aufklärungstechniken entwickeln, um Informationen über potenzielle Opfer zu sammeln. Anhand dieser Informationen werden dann individualisierte Phishing-E-Mails erstellt, die legitim und überzeugend wirken und eine entsprechend hohe Erfolgsquote aufweisen. Je gewitzter die Angreifer bei der Verwendung von Personalisierungstechniken vorgehen, desto schwieriger wird es für User, Phishing-Angriffe zu erkennen und zu vermeiden.

Abwehr von Phishing-Angriffen verbessern

Aus Branchenstatistiken geht hervor, dass ein durchschnittliches Unternehmen täglich Dutzende von Phishing-E-Mails erhält, wobei die finanziellen Auswirkungen immer größer werden, da die durch Malware- und Ransomware-Angriffe verursachten Verluste die durchschnittlichen Kosten von Phishing-Angriffen Jahr für Jahr in die Höhe treiben. Die Abwehr aller in diesem Report beschriebenen Bedrohungen ist eine kaum lösbare Aufgabe. Zwar lässt sich das Risiko von Phishing-Bedrohungen nicht vollständig eliminieren. Die vorgestellten Erkenntnisse und Empfehlungen sollen Sie jedoch dabei unterstützen, das Risiko erfolgreicher Phishing-Angriffe auf Ihre Organisation zu minimieren.

Grundlegende Maßnahmen zur Minderung des Risikos von Phishing-Angriffen:

Best Practices: Schulungen zum Sicherheitsbewusstsein

Phishing-Kampagnen haben vor allem deswegen so hohe Erfolgsquoten, weil sie auf User abzielen und es ausreicht, wenn ein einziger abgelenkter Mitarbeiter einen Fehler macht und in die Falle tappt. Eine Studie der Stanford University von 2020 ergab, dass fast 88 % der Datenpannen durch menschliches Versagen verursacht wurden. Der Report zeigt auch, dass junge männliche Mitarbeiter am anfälligsten für Phishing sind und dass in allen demografischen Gruppen Ablenkung die Hauptursache für Fehler ist. Aus diesem Grund sind Schulungen zum Sicherheitsbewusstsein für Enduser entscheidend, um Sicherheitsverletzungen zu verhindern. Diese dürfen jedoch nicht nur einmal im Jahr, sondern müssen kontinuierlich durchgeführt werden. Alle Mitarbeiter eines Unternehmens müssen über die Risiken aufgeklärt werden, Phishing-Angriffen zum Opfer zu fallen, und lernen, nicht vertrauenswürdige E-Mails, Websites, Textnachrichten, Anwendungen und Anrufe zu erkennen, damit Anmeldedaten nicht leichtfertig preisgegeben und Links nicht einfach angeklickt werden.

Kontinuierliche Schulungen zum Sicherheitsbewusstsein und regelmäßige Phishing-Simulationen sind unverzichtbar, um Mitarbeiter zu sensibilisieren und ihr Risikobewusstsein zu stärken. So können Personen, die zusätzliche Unterstützung benötigen, um Phishing-Versuche zu erkennen und ihr Risikoverhalten zu ändern, rechtzeitig geschult werden. Daneben sollten Organisationen adäquate Maßnahmen ergreifen, um die Meldung verdächtiger Phishing-E-Mails durch User zu verbessern, damit Sicherheitsteams entsprechende Bedrohungen schneller aus den Posteingängen anderer Mitarbeiter entfernen können. Hier empfiehlt sich die Einrichtung einer Schaltfläche zum Melden von Phishing-Versuchen direkt im Posteingang.

ThreatLabz empfiehlt außerdem, den Leitfaden der US Cybersecurity Infrastructure & Security Agency (CISA) bei Schulungen zum Sicherheitsbewusstsein zu befolgen. Dort wird Endusern geraten, auf folgende Indikatoren zu achten:

- **Verdächtige Absenderadresse.** Die Adresse des Absenders kann der eines seriösen Unternehmens zum Verwechseln ähnlich sein. Cyberkriminelle verwenden oft solche E-Mail-Adressen, bei denen sich nur einzelne Zeichen unterscheiden oder weggelassen werden.
- **Allgemeine Grußformeln und Signaturen.** Sowohl eine allgemeine Grußformel — z. B. „Sehr geehrter Kunde“ oder „Sehr geehrte Damen und Herren“ — als auch das Fehlen von Kontaktinformationen in der Signatur sind deutliche Hinweise auf eine Phishing-E-Mail. Eine vertrauenswürdige Organisation spricht User normalerweise mit Namen an und führt die eigenen Kontaktinformationen auf.
- **Gefälschte Hyperlinks und Websites.** Wenn man den Mauszeiger auf Links im Text der E-Mail bewegt und die Links nicht mit dem angezeigten Text übereinstimmen, ist der Link möglicherweise gefälscht. Schädliche Websites können einer seriösen Website zum Verwechseln ähnlich sehen, aber die URL kann anders geschrieben sein oder eine andere Domain verwenden (z. B. .com statt .net). Außerdem verwenden Cyberkriminelle möglicherweise einen Service zum Verkürzen von URLs, um die eigentliche Zielseite zu verschleiern.
- **Rechtschreibung und Layout.** Schlechte Grammatik und Satzstruktur, Rechtschreibfehler und inkonsistente Formatierung sind weitere Indikatoren für einen möglichen Phishing-Versuch. Seriöse Institutionen haben meist engagierte Mitarbeiter, die die Korrespondenz mit Kunden Korrektur lesen.
- **Verdächtige Anhänge.** Eine unerwartete E-Mail, in der ein User aufgefordert wird, einen Anhang herunterzuladen und zu öffnen, ist eine gängige Methode, um Malware zu übertragen. Cyberkriminelle behaupten häufig, dass es sich um dringende oder wichtige Angelegenheiten handelt, um User dazu zu bringen, einen Anhang herunterzuladen oder zu öffnen, ohne ihn vorher zu prüfen.

Best Practices: Sicherheitskontrollen

Sicherheitsteams müssen berücksichtigen, dass Mitarbeiter und andere Enduser unweigerlich Opfer von Phishing-Versuchen werden. Entsprechend müssen Schutzmaßnahmen eingesetzt werden, um den Schaden zu erkennen, einzudämmen und zu beheben, und zwar insbesondere:

- **E-Mail-Scans:** E-Mails sind am häufigsten von Phishing betroffen. Daher ist ein Cloud-basierter Service zum Scannen von E-Mails, der E-Mails überprüft, bevor sie den Perimeter erreichen — mit Echtzeitschutz vor schädlichen Links und gefälschten Domainnamen — von entscheidender Bedeutung.
- **Meldung von Angriffen:** Phishing-Angreifer nehmen oft eine hohe Anzahl von Endusern innerhalb einer Organisation ins Visier, um die Wahrscheinlichkeit eines erfolgreichen Angriffs zu erhöhen. Um verdächtige Absender und Links möglichst schnell zu blockieren, sollten Sie Endusern eine einfache Option zum Melden versuchter Phishing-Angriffe bereitstellen, am besten über eine in ihrem E-Mail-Client integrierte Schaltfläche. Unternehmen sollten Richtlinien zur Untersuchung von und Reaktion auf Phishing-Vorfälle implementieren, einschließlich der Meldung solcher Vorfälle an Behörden, um die Regierung bei der Bekämpfung von Betrügern zu unterstützen und Angriffe auf andere Organisationen zu verhindern.
- **Multi-Faktor-Authentifizierung:** MFA ist nach wie vor eine der wichtigsten Schutzmaßnahmen gegen Phishing. Mit MFA reicht ein Passwort allein nicht aus, um ein Konto zu kompromittieren. Die Authentifizierung mit Apps wie Okta Verify oder Google Authenticator ist besonders effektiv und bietet zusätzlichen Schutz gegen MiTM-Angriffe, die SMS-Nachrichten abfangen können.
- **Überprüfung des verschlüsselten Traffics:** Mehr als 95 % aller Angriffe erfolgen über verschlüsselte Kanäle, die oft nicht überprüft werden, sodass selbst mäßig erfahrene Angreifer Sicherheitskontrollen leicht umgehen können. Unternehmen müssen den gesamten Traffic überprüfen, unabhängig davon, ob er verschlüsselt ist oder nicht, um Angreifer daran zu hindern, ihre Systeme zu kompromittieren.
- **Antivirus-Software:** Endgeräte sollten durch regelmäßig aktualisierte Antivirus-Programme geschützt werden, um schädliche Dateien zu finden und zu verhindern, dass sie heruntergeladen werden.
- **Advanced Threat Protection:** Antivirus-Software ist zwar wichtig, um bekannte Bedrohungen zu stoppen. Angreifer sind jedoch in der Lage, neue, unbekannte Malware-Varianten zu entwickeln, die von signaturbasierten Tools nicht erkannt werden. Daher empfiehlt sich der Einsatz einer Inline-Sandboxing-Lösung, die verdächtige Dateien unter Quarantäne stellt und analysiert, sowie die Verwendung einer Browser-Isolation-Lösung, die potenziell schädliche Webinhalte abstrahiert, ohne die Workflows der Enduser zu beeinflussen.
- **URL-Filterung:** Das Risiko eines erfolgreichen Phishing-Angriffs lässt sich mit URL-Filtern einschränken, die mithilfe von Richtlinien den Zugriff auf die riskantesten Kategorien von Webinhalten verwalten, wie z. B. neu registrierte Domains.
- **Regelmäßiges Patching:** Unternehmen sollten Anwendungen, Betriebssysteme und Sicherheitstools mit aktuellen Patches auf dem neuesten Stand halten, um Sicherheitsrisiken zu verringern und sicherzustellen, dass die neuesten Schutzmaßnahmen umgesetzt werden.
- **Zero-Trust-Architektur:** Es ist zwar wichtig, Kontrollen zur Verhinderung von Phishing einzurichten. Ebenso wichtig ist es jedoch, Kontrollen einzuführen, die den Schaden begrenzen, den ein erfolgreicher Phishing-Angriff verursachen kann. Deshalb sollte eine granulare Segmentierung implementiert, minimale Zugriffsrechte erzwungen und Traffic kontinuierlich überwacht werden, um Bedrohungsakteure zu finden, die die Infrastruktur möglicherweise kompromittiert haben.
- **Feeds zu Bedrohungsdaten:** Diese Feeds lassen sich in vorhandene Sicherheitstools integrieren und bieten eine automatische Kontextanreicherung, um Phishing-Bedrohungen schneller erkennen und beheben zu können. Bedrohungsfeeds liefern aktualisierten Kontext zu gemeldeten URLs, extrahierten Indicators of Compromise (IOCs) sowie Taktiken, Techniken und Verfahren für Entscheidungsfindung und Priorisierung.

Best Practices: Woran erkennt man eine Phishing-Seite?

Es gibt eine Reihe von Erkennungsmerkmalen, die Hinweise auf die Taktiken geben, mit denen Bedrohungsakteure User und Sicherheitsengines austricksen. Häufig lassen sich Phishing-Seiten auch daran erkennen, dass bei ihrer Erstellung bestimmte Schritte ausgelassen wurden. Die Anzahl neuer Phishing-Websites nimmt im Zusammenhang mit Feiertagen und anderen ungewöhnlichen Ereignissen zu. Während der Pandemie beobachteten Sicherheitsexperten beispielsweise eine rapide Zunahme gefälschter Websites, die vorgaben, von medizinischen Organisationen bzw. Anbietern von COVID-19-Tests, PSA oder Arzneimitteln und Medizinprodukten zu stammen. Um auch neue Phishing-Bedrohungen zu erkennen, müssen Unternehmen unbedingt ständig auf dem Laufenden bleiben und ihre Erkennungsregeln und Reaktionsmaßnahmen anhand von verwertbaren Analyseergebnissen aktualisieren.

Insbesondere sollten Sicherheitsexperten (bzw. ihre Anti-Phishing-Tools) vor folgenden Erkennungsmerkmalen auf der Hut sein:

Die gesamte Seite basiert auf einem einzigen Bild. Beim bildbasierten Phishing basiert die gesamte Seite auf einem Hintergrundbild, das eine Kopie einer legitimen Webseite ist. Als einzige weitere Komponente enthält die Seite ein Webformular zur unrechtmäßigen Erfassung der gestohlenen Anmeldedaten. Dies ist eine sehr verbreitete Technik, die vor allem bei Angriffen auf Banken zum Einsatz kommt.

Die Seite hat keinen Titel.

Wichtige Links sind mit einem leeren Anker verknüpft. Auf Phishing-Seiten, deren Inhalte von legitimen Seiten kopiert wurden, finden sich häufig leere Anker zur Verknüpfung von wichtigen Seiten wie Hilfe, FAQs usw.

Die Seite hat ein selbstsigniertes Zertifikat.

Die Seite sieht aus wie ein generischer Webmail-Client. Phishing-Akteure verwenden häufig generische Webmail-Clients und imitieren Websites wie Webmail, Zimbra usw., um User zur Eingabe von Anmeldedaten zu veranlassen.

Die Seite ist nicht verschlüsselt. Eine Anmeldeaufforderung auf einer „http"-Seite ist verdächtig und sollte als riskant gemeldet werden.

Die Seite leitet den User mehrmals weiter, bevor eine Anmeldeaufforderung angezeigt wird.

HTML-Schmuggel. Als HTML-Schmuggel wird eine Methode zum Umgehen von E-Mail-Filtern bezeichnet. Dabei wird ein JavaScript-Blob mit schädlichem Code in einem E-Mail-Anhang versteckt und dann vom Browser zusammengesetzt. HTML-Schmuggel im Zusammenhang mit einer Anmeldeaufforderung ist als höchst verdächtig einzustufen.

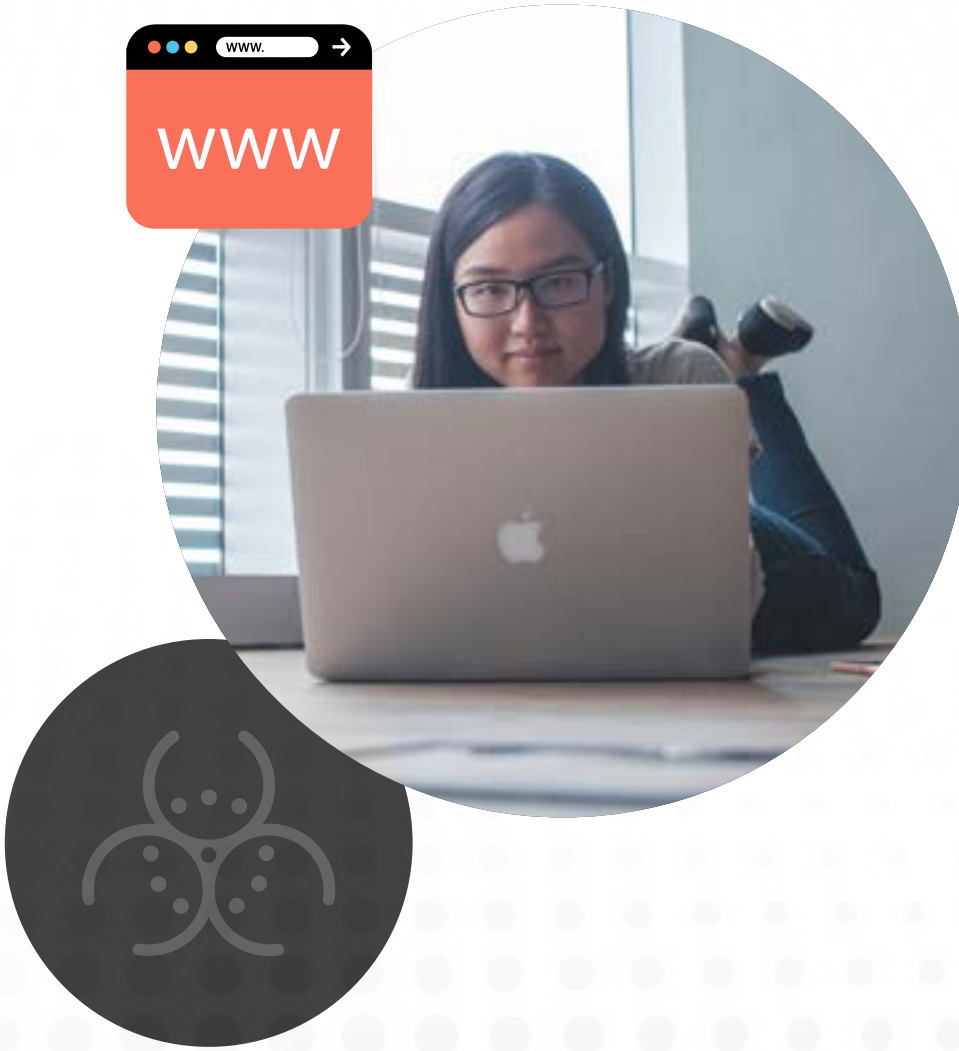
Die Seite enthält unkenntlich gemachte Tags. Phishing-Akteure machen Felder wie Titel, urheberrechtliche Hinweise usw. möglicherweise unkenntlich.

Buchstaben werden durch Homoglyphen ersetzt. Homoglyphen sind Schriftzeichen, die anderen Buchstaben oder Zahlen täuschend ähnlich sehen. Auf Phishing-Seiten werden insbesondere Homoglyphen aus anderen Alphabeten dazu verwendet, Schutzmechanismen und Sicherheitsengines zu umgehen, die auf die Erkennung von ASCII-Kodierung geschult sind.

Vorteile der Zscaler Zero Trust Exchange zur Abwehr von Phishing-Angriffen

Der Schutz des Unternehmens vor Angriffen, bei denen User zum Zugriff auf schädliche Links verleitet werden, stellt Sicherheitsbeauftragte vor enorme Herausforderungen. Bewältigen lassen sie sich nur durch die Implementierung entsprechender Kontrollmechanismen zur Abwehr von Phishing-Angriffen im Rahmen einer umfassenden Zero-Trust-Strategie, die es Ihrer Organisation ermöglicht, aktive Sicherheitsverletzungen zu erkennen und das Schadenspotenzial erfolgreicher Angriffe zu minimieren. Die Zscaler Zero Trust Exchange™ basiert auf einer ganzheitlichen Zero-Trust-Architektur, die Organisationen mit leistungsstarken Funktionen bei der Abwehr von Phishing-Angriffen unterstützt:

- **Sie verhindert Kompromittierungen durch Zugriff auf verdächtige Websites:** Durch komplette SSL-Überprüfung auch bei hohem Traffic-Volumen, Browser Isolation und richtlinienbasierte Kontrollen werden Zugriffe auf riskante Websites verhindert.
- **Sie lässt keine lateralen Bewegungen zu:** Indem User direkt mit Anwendungen und nicht mit dem Netzwerk verbunden werden, wird das Schadenspotenzial im Falle eines erfolgreichen Angriffs begrenzt.
- **Sie blockiert kompromittierte Konten und Insider-Bedrohungen:** Wenn es einem Angreifer gelingt, sich Zugang zu den Anmeldedaten von Mitarbeitern zu verschaffen, verhindert die Zero Trust Exchange den Zugriff auf unternehmensinterne Anwendungen. Mithilfe der integrierten Deception Technology werden auch geschickte Angreifer entlarvt.
- **Sie verhindert Datendiebstähle:** Daten werden bei der Übertragung und im Ruhezustand überprüft, um ihren Diebstahl im Zuge eines laufenden Angriffs zu verhindern.



Weitere relevante Produkte von Zscaler

Zscaler Internet Access™ unterstützt die Erkennung und Blockierung von Angriffen, indem der gesamte Internet-Traffic durch die Zero Trust Exchange geleitet und überprüft wird. Folgende Traffic-Typen werden blockiert:

- **URLs und IPs**, die in der Zscaler Cloud beobachtet und als verdächtig eingestuft wurden bzw. in nativ integrierten Open-Source- und kommerziellen Datenbanken verzeichnet sind. Dazu gehören URL-Kategorien, die in den Richtlinien als hochriskant definiert sind und häufig für Phishing-Angriffe verwendet werden — z. B. neu beobachtete und neu aktivierte Domains.
- **IPS-Signaturen**, die von ThreatLabz aus der Analyse von Phishing-Kits und -Seiten ermittelt wurden.
- **Neuartige Phishing-Websites**, die durch Inhaltsscans mit KI/ML-Erkennung identifiziert werden.

Advanced Threat Protection blockiert alle bekannten Command-and-Control-Domains.

Advanced Firewall erweitert den Command-and-Control-Schutz auf alle Ports und Protocols, einschließlich neuer, bislang unbekannter Ziele.

Browser Isolation isoliert User durch einen undurchdringlichen Air Gap vom Internet. Web-Inhalte werden als gestochen scharfer Bilderstrom angezeigt und das Risiko von Datenverlusten und aktiven Bedrohungen ausgeschaltet.

Advanced Cloud Sandbox verhindert die Auslieferung unbekannter Malware in der zweiten Phase.

Zscaler Private Access™ schützt Anwendungen, indem durch Mikrosegmentierung von User-to-App-Verbindungen und kompletter Inline-Überprüfung des Traffics von unternehmensinternen Anwendungen die laterale Bewegungsfreiheit von Angreifern eingeschränkt wird.

Zscaler Deception™ ködert und entlarvt Angreifer beim Versuch, sich lateral durchs Netzwerk zu bewegen bzw. sich erweiterte Zugriffsberechtigungen zu verschaffen, mit Decoys, die echten Servern, Anwendungen, Verzeichnissen und User-Konten täuschend ähnlich sehen.

Die nächsten Schritte

Zscaler stellt ein Tool zur Risikobewertung bereit, das kritische Risiken in Ihrer gesamten öffentlichen Cloud-Umgebung aufdeckt. Sie erhalten ein vollständiges Inventar Ihrer Cloud-Ressourcen, ein klares Bild aller damit verbundenen Sicherheitsrisiken, einen Überblick über Ihren aktuellen Status in Bezug auf die Erfüllung von Compliance-Benchmarks sowie umsetzbare Anleitungen zur Behebung etwaiger Probleme.

Über ThreatLabZ

ThreatLabz ist als Forschungsabteilung von Zscaler für die Früherkennung neuer Bedrohungen zuständig. Dieses erstklassige Team sorgt dafür, dass die Tausenden von Organisationen, die weltweit mit der globalen Zscaler-Plattform arbeiten, jederzeit geschützt sind. Neben der Erforschung und Verhaltensanalyse von Malware-Bedrohungen tragen die ThreatLabz-Experten auch zur Entwicklung neuer Prototypen für Advanced Threat Protection auf der Zscaler-Plattform bei und führen regelmäßig interne Revisionen durch, um sicherzustellen, dass Zscaler-Produkte und -Infrastrukturen die geltenden Sicherheitsstandards erfüllen. Detaillierte Analysen neuer Bedrohungen werden regelmäßig unter research.zscaler.de veröffentlicht.

Gerne informieren wir Sie über aktuelle Forschungsergebnisse der ThreatLabz-Experten. Am besten melden Sie sich gleich bei unserem Newsletter an!

Über Zscaler

Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, stabiler und sicherer arbeiten können. Die Zscaler Zero Trust Exchange™ schützt tausende Kunden mittels sicherer Verbindungen zwischen Usern, Geräten und Anwendungen an jedem beliebigen Standort vor Cyberangriffen und Datenverlusten. Als weltweit größte Inline-Cloud-Sicherheitsplattform wird die SASE-basierte Zero Trust Exchange in über 150 Rechenzentren auf der ganzen Welt bereitgestellt.

Weitere Informationen finden Sie unter zscaler.de — oder folgen Sie uns auf Twitter @zscaler.

Anhang

Kategorisierung von Phishing-Angriffen

Es gibt verschiedene Arten von Phishing-Angriffen, die unterschiedliche Angriffstechniken umfassen. Dabei ist jedoch zu beachten, dass Angreifer ihre Ansätze laufend anpassen, um besser informierte User zu täuschen und aktualisierte Abwehrmechanismen zu umgehen. Im Folgenden stellen wir gängige Definitionen und Merkmale von Phishing-Angriffen vor.

In den folgenden Listen wurden mehrere Beschreibungen physischer Angriffsmethoden und der sehr realen Bedrohung berücksichtigt, die sie für Unternehmen darstellen. Der Großteil dieses Reports konzentriert sich jedoch auf virtuelle Phishing-Angriffe, die nur mit einer Internetverbindung ausgeführt werden können. Ein typisches Merkmal von Online-Phishing ist, dass User in der Regel aufgefordert werden, Informationen einzugeben oder Malware über eine der folgenden Methoden herunterzuladen:

- **Link:** Der User klickt auf einen Link zu einer Phishing-Website, schädlichen Datei oder Malware-Installation.
- **Aufforderung:** Der User wird zur Eingabe vertraulicher Daten aufgefordert, die dann gestohlen werden.
- **Anhang:** Der User öffnet einen Anhang, der schädliche Software enthält.

Bei der Ressourcenplanung für Investitionen in die Abwehr von Phishing-Angriffen sollten Sie die nachstehend aufgeführten Angriffsarten berücksichtigen.

A bis Z: Gängige Methoden bei Phishing-Angriffen

1. **Angler-Phishing:** Angreifer nehmen gezielt unzufriedene Kunden — insbesondere Bankkunden — ins Visier, geben sich als Mitarbeiter des Kundensupports aus und bieten Unterstützung bei der Klärung negativer Kommentare über ein Unternehmen auf Social-Media-Plattformen an.
2. **AitM-Phishing (Adversary-in-the-Middle):** Angreifer imitieren die Online-Aktivitäten eines ahnungslosen Opfers, um an dessen Anmeldedaten und Sitzungscookies zu gelangen.
3. **Baiting (Köder-Phishing):** Ähnlich wie bei einem Trojaner-Angriff wird versucht, neugierige User mit verlockenden Angeboten, Dateinamen oder Geräten in eine Falle zu locken.
4. **Browser-in-the-Browser-Phishing (BitB):** Angreifer zeigen ein gefälschtes Browser-Fenster innerhalb eines Browser-Fensters einer vertrauenswürdigen Domain an. Oft werden Pop-up-Anmeldefenster repliziert, die aussehen, als ob sie von Drittanbietern wie Google, Facebook, Apple und Microsoft stammen.
5. **CEO Fraud oder Business Email Compromise (BEC):** Die Angriffe richten sich gegen Unternehmensmitarbeiter. Dabei werden kompromittierte Konten von Führungskräften genutzt, um gefälschte Rechnungen mit der Bitte um Zahlung per Banküberweisung oder anderen Zahlungsmethoden zu senden.
6. **Chat- oder IM-Phishing:** Angreifer verbreiten Phishing-Inhalte über Sofortnachrichten innerhalb von Anwendungen, in der Regel mit schädlichen URL-Links.
7. **Clone-Phishing:** Angreifer erstellen Duplikate von E-Mail-Nachrichten, die scheinbar aus vertrauenswürdigen Quellen stammen, mit geringfügigen Änderungen und schädlichen Anhängen oder Links.

8. **Credential Harvesting:** Angreifer erstellen gefälschte Anmeldeseiten oder senden Phishing-E-Mails, die legitime Anmeldeaufforderungen imitieren, um Opfer zur Preisgabe von Benutzernamen und Passwörtern zu bewegen.
9. **Doc Clouding:** Angreifer stellen schädliche Dokumente über gängige Cloud-Quellen wie Google Drive, Box, GitHub, Amazon S3 oder OneDrive bereit, um herkömmliche Sicherheitstools zu umgehen und die Erkennung der Bedrohung zu erschweren.
10. **E-Mail-Phishing:** Angreifer senden Social-Engineering-E-Mails, in denen sie sich als Vertreter bekannter Marken ausgeben, mit schädlichen URL-Links oder Anhängen, die darauf ausgelegt sind, Daten zu stehlen oder Malware zu verbreiten.
11. **Evil-Twin-Phishing:** Angreifer imitieren ein vertrauenswürdiges öffentliches WLAN-Netzwerk, um die Online-Aktivitäten der Opfer zu beobachten und Daten zu stehlen, die den gefälschten Zugangspunkt durchlaufen.
12. **HTTPS-Phishing:** Angreifer missbrauchen das verschlüsselte „Hypertext Transfer Protocol Secure", um arglose User zum Anklicken schädlicher URL-Links zu verleiten.
13. **Malvertising-Phishing:** Unerwünschte Inhalte werden über Skripte in Anzeigen direkt auf die Computer der Opfer übertragen.
14. **MFA-Bombing:** Angreifer verleiten User mithilfe kompromittierter Zugangsdaten dazu, eine gefälschte MFA-Aufforderung des Angreifers zu verifizieren. Diese Angriffe sind in der Regel durch einen kontinuierlichen Strom von MFA-Aufforderungen gekennzeichnet, manchmal begleitet von gefälschten Anrufen, Textnachrichten oder E-Mails, die den User dazu bringen sollen, unwissentlich oder versehentlich eine der Aufforderungen zu verifizieren.
15. **Man-in-the-Middle-Phishing (MITM):** Diese Angriffe zielen auf User eines bestimmten Servers oder Systems ab und erfassen Daten während der Übertragung, einschließlich Zugangsdaten, Cookies, Bankkontoinformationen usw., durch Imitation von Online-Services, indem Traffic über Proxy-Server geroutet wird.
16. **Pharming- oder DNS-Cache-Angriffe** leiten Besucher auf eine bösartige Website um, indem sie die IP-Adresse einer legitimen Website in den kompromittierten DNS-Servern (Domain Name System) ändern oder eine Phishing-E-Mail mit schädlichem Code versenden, der das Opfer auf die Website leitet, wenn es eine URL über seinen Computer eingibt.
17. **QR-Code-Phishing:** Angreifer setzen QR-Codes ein, die zu schädlichen Websites weiterleiten oder Malware auf das Gerät herunterladen, wenn sie vom Smartphone des Opfers gescannt werden.
18. **Ransomware-Phishing:** Angreifer senden E-Mails mit schädlichen Anhängen oder Links, die beim Anklicken Ransomware auf den Computer des Opfers herunterladen und eine Lösegeldzahlung im Austausch für einen Entschlüsselungscode zur Wiederherstellung der Daten verlangen.
19. **Reverse-Tunnel-Phishing:** Angreifer verwenden einen Remote-Server, um einen Reverse-SSH-Tunnel zum Computer des Opfers zu erstellen. Dieser ermöglicht es ihnen, den Computer für verschiedene Zwecke auszunutzen, z. B. zum Installieren von Malware oder Diebstahl vertraulicher Daten, und sich dabei vor dem Opfer versteckt zu halten.
20. Bei **Suchmaschinen-Phishing** werden gefälschte Online-Shopping-Websites verwendet, die von Suchmaschinen angezeigt werden. Diese Websites bieten beträchtliche Preisnachlässe auf bestimmte Produkte an, erscheinen aber als Pop-ups oder enthalten gefälschte, zurückdatierte Bewertungen. Opfer können unwissentlich persönliche Daten, Bankinformationen und Kreditkartennummern preisgeben oder sogar für gefälschte Waren bezahlen. Die Betrüger gehen sogar so weit, dass sie gefälschte Versanddaten und Informationen zur Sendungsverfolgung verschicken oder gar billige „Alibi-Ware" liefern, um die Website länger unbehelligt betreiben zu können.

21. **Smishing:** Angreifer verbreiten betrügerische Inhalte per Textnachricht (SMS), in der Regel mit schädlichen URL-Links. Die Nachricht stammt vermeintlich von einem bekannten Unternehmen oder einem Bekannten des Empfängers.
22. **Spear-Phishing:** Bei diesen Angriffen handelt es sich um organisierte Kampagnen, bei denen öffentlich zugängliche Informationen genutzt werden, um Personen anzusprechen, die für bestimmte Organisationen arbeiten. Diese betrügerischen E-Mails enthalten möglicherweise echte Informationen und sehen wie legitime interne Anfragen aus, um die Empfänger zur Durchführung der gewünschten Aktion zu verleiten.
23. **Tailgating:** Angreifer verschaffen sich physischen Zugang zu einem eingeschränkten Bereich, indem sie einer befugten Person mit Zugangsberechtigung folgen. Diese Angriffsform wird dann als Phishing eingestuft, wenn jemand auf den Social-Engineering-Trick des Angreifers (z. B. Mitführen mehrerer großer Pakete) hereinfällt und ihm ohne Überprüfung Zutritt gewährt.
24. **USB-Phishing:** Diese Angriffe beinhalten das physische Einschleusen oder Versenden von USB-Geräten mit schädlichen ausführbaren Dateien, die beim Anschließen an ein anfälliges Endgerät geladen werden.
25. **Vishing:** Bei diesen Angriffen handelt es sich um böswillige Telefonanrufe oder Sprachnachrichten, wobei das Opfer mithilfe von Social-Engineering-Techniken zur Überweisung von Geld oder Preisgabe personenbezogener Daten gedrängt wird.
26. **Watering-Hole-Phishing:** Diese Angriffe zielen auf Mitglieder bestimmter Gruppen ab, bei denen die Wahrscheinlichkeit hoch ist, dass sie eine bestimmte Website besuchen, die vom Angreifer kompromittiert oder eigens erstellt wurde.
27. **Whaling:** Diese Angriffe zielen auf Führungskräfte und hochrangige Personen ab und nutzen öffentlich zugängliche Informationen, um die Zielperson dazu zu bringen, vertrauliche Geschäftsgeheimnisse preiszugeben, die für betrügerische Zwecke verwendet werden können, oder eine andere Aktion durchzuführen, die zur Erreichung der Ziele des Bedrohungsakteurs genutzt werden kann.

Phishing ist ein komplexes Problem, das sich nicht allein durch Technologie lösen lässt. Wir empfehlen Organisationen, unbedingt die Entwicklung im Zeitverlauf nachzuverfolgen, um festzustellen, inwieweit bestimmte Techniken aufgrund von Veränderungen in der Wahrnehmung von/Sensibilisierung für Phishing-Maschen weniger wirksam werden. Je besser Sicherheitsexperten sich mit populären Betrugsmaschen der Angreifer auskennen, desto effektiver können sie Mitarbeiter darin schulen, im Umgang mit vermeintlichen Geschäftschancen, Verifizierungsaufforderungen oder Push-Benachrichtigungen die gebotene Skepsis an den Tag zu legen. Bei der Entwicklung einer unternehmensspezifischen Strategie zur Verringerung von Phishing-Vorfällen sollten Sie insbesondere folgende gängige Betrugsmaschen berücksichtigen:

Häufigste Phishing-Maschen nach Kategorien

Cloud-Betrüger geben sich als File-Sharing-Dienste oder Cloud-Speicherdienste aus und verwenden Köder wie gefälschte Zugriffsanfragen und Kontobenachrichtigungen.

Bei **Verbraucherbetrug** geben sich Angreifer als E-Commerce-Unternehmen aus und verwenden Köder wie gefälschte Kontobenachrichtigungen und Mitgliedschaften oder Vergünstigungen.

Bei **kommerziellem Betrug** geben sich Cyberkriminelle z. B. als Versandunternehmen aus und ködern mit Benachrichtigungen zur Sendungsverfolgung und Zahlungsaufforderungen.

Bei Betrugsmaschen mit **Markenbezug** geben sich Angreifer als Vertreter bestimmter Unternehmen aus und ködern mit gefälschten Kontobenachrichtigungen, Unternehmensmeldungen, Personalaufgaben und Zahlungsaufforderungen für Rechnungen.

Dating-Betrüger geben sich als Menschen aus, die über eine Online-Plattform nach einem Partner suchen, und ködern mit gefälschten Profilen, Nachrichten, Likes und Followern.

Bei Betrugsmaschen im Bereich **Finanzdienstleistungen** geben sich Cyberkriminelle als bekannte Finanzinstitute aus und ködern User mit gefälschten Kontobenachrichtigungen oder Sicherheitswarnungen.

Bei **behördenbezogenen** Phishing-Maschen geben sich Betrüger als Vertreter des Finanzamts oder anderer staatlicher Behörden aus und ködern mit gefälschten Leistungsansprüchen, Hilfskrediten und Mahnungen.

Im Zusammenhang mit **Stellenangeboten** geben sich Betrüger als falsche oder auch echte Unternehmen aus, die angeblich neue Mitarbeiter einstellen möchten, und nutzen dazu gefälschte Stellenausschreibungen, Bewerbungen und Stellenangebote.

Bei gefälschten **Push-Benachrichtigungen oder Browser-Betrug** werden Webbrowser-Benachrichtigungen verwendet und Köder wie Erinnerungen an die Installation von Updates, Benachrichtigungen und Produktwerbung eingesetzt.

Social-Media-Betrüger geben sich als Betreiber oder User von Social-Media-Plattformen aus und ködern ihre Opfer mit gefälschten oder manipulierten Konten, privaten Nachrichten, Kontowarnungen oder -benachrichtigungen und Sicherheitsmeldungen.

Bei **technikbezogenen** Betrugsmaschen geben sich Cyberkriminelle als allgemeine Services oder bekannte Unternehmen aus und nutzen Köder wie Kontobenachrichtigungen, Fehlermeldungen und Software-Updates.

Experience your world, secured.™

Über Zscaler

Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, resilienter und sicherer arbeiten können. Die Zscaler Zero Trust Exchange™ schützt tausende Kunden mittels sicherer Verbindungen zwischen Usern, Geräten und Anwendungen überall vor Cyberangriffen und Datenverlust. Die SASE-basierte Zero Trust Exchange ist weltweit in 150 Rechenzentren verfügbar und ist somit die größte Inline-Cloud-Sicherheitsplattform der Welt. Weitere Informationen finden Sie unter www.zscaler.de.

+1 408 533 0288

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

zscaler.de