proofpoint.

BERICHT

Der Faktor Mensch 2023

Eine Analyse der Cyber-Angriffskette

proofpoint.com/de

Einführung

Nach zwei Jahren mit Pandemie-bedingten Störungen fühlte sich das Jahr 2022 für viele wie eine Rückkehr zum „Business as usual“ an. Das trifft auf jeden Fall auch für Cyberkriminelle auf der ganzen Welt zu. Nachdem die medizinischen und wirtschaftlichen COVID-19-Programme nach und nach heruntergefahren wurden, mussten die Angreifer sich wieder auf ihre gewohnten Methoden zurückbesinnen. Dazu schärften sie ihre Social-Engineering-Kompetenzen, erweiterten ihre Tools und suchten nach neuen Möglichkeiten an unerwarteten Stellen.

All das hat zu einem Schub an Kreativität geführt. Die Cyber-Angriffskette – und die Bedrohungslandschaft insgesamt – hat erhebliche Entwicklungen an mehreren Fronten erlebt. Dazu gehören die Standardisierung raffinierter Techniken zur Umgehung von Multifaktor-Authentifizierung sowie Bedrohungen, die sich ausschließlich auf den Charme und die Überzeugungskraft der Angreifer verlassen. Und da Microsoft Maßnahmen zur Eindämmung des Office-Makro-Missbrauchs getroffen hat, stehen die Kriminellen unter Druck, Innovationen zu entwickeln und mit neuen Methoden zu experimentieren.

Doch ganz gleich, welche Taktiken oder Techniken die Angreifer einsetzen, sind ihre Opfer auch nur Menschen. Cyberangreifer nehmen gezielt Menschen ins Visier und nutzen deren Schwächen aus. Letztlich handeln Menschen einfach nur menschlich. Deshalb ist der Schutz der Anwender vor Cyberbedrohungen eine so wichtige und faszinierende Herausforderung.

INHALT

Die wichtigsten Erkenntnisse

13 Millionen

TOAD-Nachrichten erreichten in der Spitze mehr als 13 Millionen im Monat

x12

Die Zahl der Konversationsangriffe über Mobilgeräte stieg um den Faktor 12

Emotet erreichte wieder die Chart-Spitze und versendete mehr als

25 Millionen Nachrichten

94 %

der Cloud-Mandanten wurden jeden Monat kompromittiert

Die Nutzung von Office-Makros erlebte einen drastischen Rückgang, nachdem Microsoft Funktionen zur Blockierung bereitstellte

Top 5

Mit einer neuen Distributionsmethode gelangte SocGholish in die Top 5 der häufigsten Malware-Versionen

nach Nachrichtenvolumen

MFA-Umgehung

machte mehr als eine Million Nachrichten pro Monat aus

Informationen zu diesem Bericht

Seit mehr als 20 Jahren schützt Proofpoint Menschen und Daten vor Cyberangriffen. In dieser Zeit führten unsere Forschungen uns zu einer einfachen aber wichtigen Beobachtung: Für heutige Cyberbedrohungen sind Menschen – und nicht Technologien – die wichtigste Variable.

Der *Bericht zum Faktor Mensch* wirft in diesem Jahr einen genauen Blick auf die neuesten Entwicklungen in der Bedrohungslandschaft und konzentriert sich dabei auf die Kombination aus Technologie und Psychologie, die Cyberangriffe heute so gefährlich macht.

Inhalt dieses Berichts

Dieser Bericht stellt die Bedrohungen vor, die im Jahr 2022 bei Proofpoint-Bereitstellungen auf der ganzen Welt entdeckt, abgewehrt und behoben wurden. Damit basiert er auf einem der größten und vielfältigsten Datensätze in der Cybersicherheitsbranche.

Wir konzentrierten uns in erster Linie auf Bedrohungen, die zu einer umfassenderen Angriffskampagne und somit zu einer Serie von Aktionen gehören, die von einem Angreifer zum Erreichen eines Ziels durchgeführt werden. Manchmal können wir diese Kampagnen einem bestimmten Bedrohungsakteur zuordnen. Dieser Prozess wird als Attribution bezeichnet.

Umfang

Die Daten in diesem Bericht stammen aus dem Proofpoint Nexus Threat Graph und wurden aus Proofpoint-Bereitstellungen auf der ganzen Welt erhoben. Jeden Tag analysieren wir mehr als 2,6 Milliarden E-Mails, 49 Milliarden URLs, 1,9 Milliarden Anhänge, 28 Millionen Cloud-Konten, 1,7 Milliarden verdächtige SMS-Nachrichten und vieles mehr. Insgesamt erheben wir dabei Billionen Datenpunkte auf allen wichtigen digitalen Kanälen.

Dieser Bericht deckt den Zeitraum vom 1. Januar bis 31. Dezember 2022 ab. Die genannten konkreten Kampagnen wurden von unserem weltweiten Bedrohungsforscher-Netzwerk unmittelbar beobachtet. Kampagnen werden definiert als eine Reihe zusammenhängender Aktivitäten, die von einem einzigen Angreifer durchgeführt werden, um ein bestimmtes Ziel zu erreichen.

In einigen wenigen Fällen waren die Daten für das ganze Jahr entweder nicht verfügbar oder verfälschten unsere Aussage. Daher weisen wir gesondert darauf hin, wenn wir einen kürzeren Zeitrahmen oder eine andere Datenquelle gewählt haben.

ABSCHNITT 1

Die aktuelle Bedrohungslandschaft

TA542:

Der Bedrohungsakteur hinter der Malware Emotet. Finanziell motiviert und bekannt für extrem umfangreiche E-Mail-Kampagnen.

TA511:

Eine finanziell motivierte Cybercrime-Gruppe, die für umfangreiche Kampagnen gegen verschiedenste Branchen bekannt ist. Im Laufe der Zeit wurde TA511 bei der Nutzung unterschiedlicher Malware-Familien beobachtet.

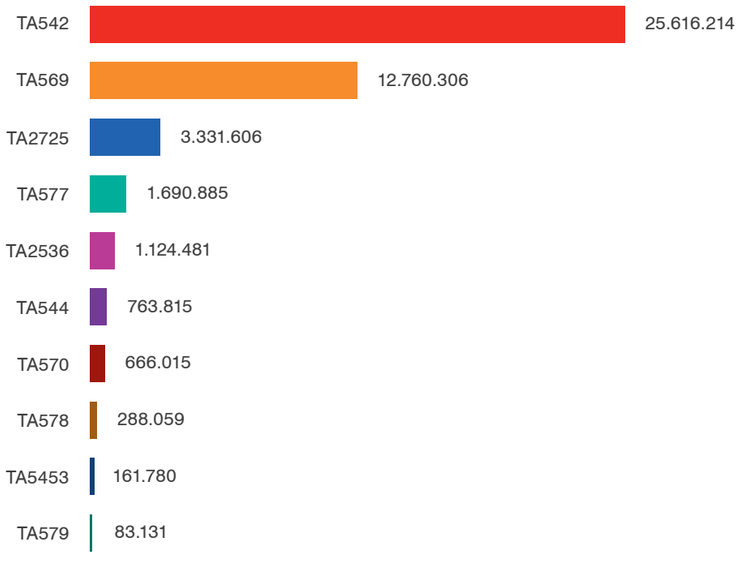
Einige Dinge ändern sich nie. Bei einigen Aspekten erlebte das Jahr 2022 enorme Veränderungen in der Bedrohungslandschaft: Angriffsketten wurden vielfältiger, Verbreitungsmechanismen wurden in kurzer Abfolge getestet und verworfen und Bedrohungsakteure lernten, dass Raffinesse und Geduld eine erfolgreiche Kombination ist.

Doch im Gegensatz zu den Techniken und Taktiken, die sich im Laufe des Jahres zum Teil rasant entwickelten, gab es bei den wichtigsten Akteuren deutlich weniger Veränderungen.

Leader und Loser

Trotz eines erratischen Jahres behielt **TA542**, der Betreiber von Emotet, den Status als aktivster Bedrohungsakteur der Welt. Die Rückkehr an die Spitze erfolgte nur ein Jahr, nachdem Strafverfolgungsbehörden das Botnet im Januar 2021 stillgelegt hatten. Die Abwesenheit von Emotet im letzten Jahr wurde von einer anderen Gruppe genutzt, um zum ersten Mal nach drei Jahren in Folge an die Spitze aufzusteigen. Gleichzeitig schafft es **TA511** – der nach Aufkommen größte Akteur im letzten Jahr – nicht einmal mehr in die aktuellen Top 10 und erreicht den 12. Platz.

Bedrohungsakteure nach Nachrichtenvolumen



TA2541:

Eine persistente Cybercrime-Gruppe, die meist die Luftfahrt-, Transport- und Verteidigungsbranche angreift.

TA577:

Eine überaus aktive Cybercrime-Gruppe, die seit 2020 überwacht wird. Als einer der berüchtigsten Qbot-Partner ist die Gruppe bekannt dafür, verschiedenste Branchen zu attackieren.

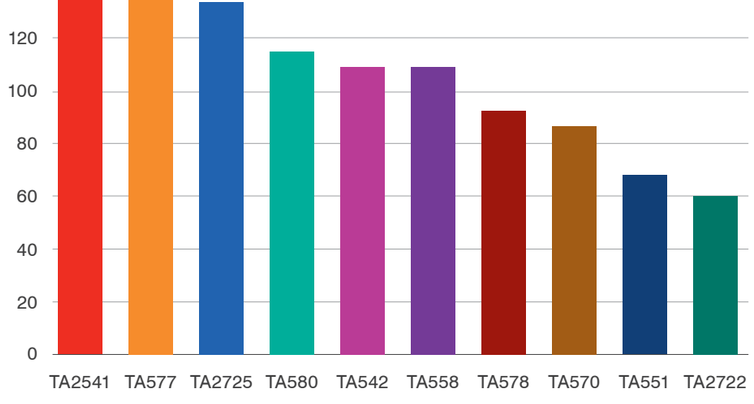
Vermittler für den Erstzugriff:

Cybercrime-Gruppen, die sich darauf spezialisieren, Ransomware-Akteuren Zugriff auf kompromittierte Systeme zu verschaffen.

Unsere Forscher identifizieren Bedrohungsakteure anhand von Mustern in der täglichen Flut schädlicher E-Mails. Wenn sie Aktivitäten durch einen bekannten Akteur finden, werden diese Nachrichten in eine Kampagne gruppiert, die meist durch eine gemeinsame Social-Engineering-Strategie oder Technik definiert wird.

Eine nützliche alternative Sicht ist die Einstufung von Akteuren nach der Anzahl ihrer diskreten Kampagnen anstatt lediglich nach ihrem Nachrichtenvolumen. Durch diesen Ansatz können wir sehen, welche Gruppen im Laufe des Jahres am aktivsten waren und wie sie ihre Taktiken und Köder verändern.

Bedrohungsakteure nach Kampagnenvolumen



Die beiden Top-Akteure in diesem Diagramm, **TA2541** und **TA577**, stellen interessante Gegensätze dar. TA2541 konzentriert sich ausschließlich auf die Branchen Luft-/Raumfahrt, Reisen und Verteidigung. Anders als viele andere ignoriert diese Gruppe in ihren Ködern aktuelle Ereignisse oder saisonale Themen und setzt stattdessen auf sorgfältig gestaltetes und branchenspezifisches Social Engineering.

Im Gegensatz dazu wählt TA577 eine gänzlich andere Herangehensweise. Als bekannter **Vermittler für den Erstzugriff** greift diese Gruppe verschiedenste Regionen sowie Branchen an und hat im Laufe der Jahre sehr unterschiedliche Malware verteilt.

Finanziell motivierte Akteure:

Cyberkriminelle, die es in erster Linie auf Geld abgesehen haben, sei es durch direkten Diebstahl oder die Monetarisierung gestohlener Daten und Anmeldeinformationen.

APT-Akteure:

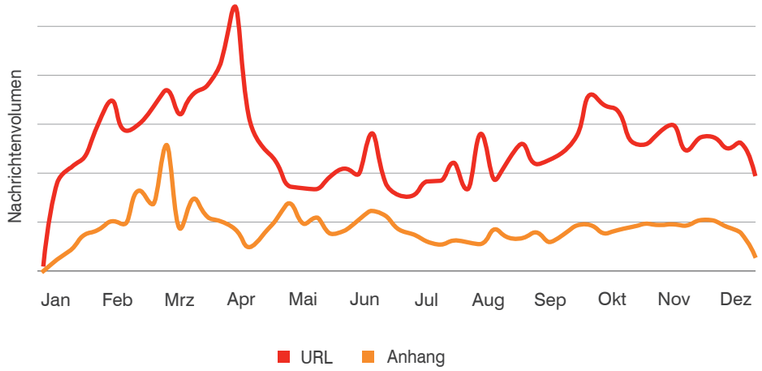
Akteure, die mit hochentwickelten hartnäckigen Bedrohungen (Advanced Persistent Threats) in erster Linie nationale Interessen unterstützen. In einigen seltenen Fällen sind APT-Akteure mit finanziell motivierten Aktivitäten beschäftigt.

Emotet:

Ein überaus aktives Malware-Botnet. Abgesehen von einem Zeitraum im Jahr 2021, als Emotet von Strafverfolgungsbehörden stillgelegt wurde, war dies die am weitesten verbreitete Malware.

Verlinkt oder angehängt?

Die Aufteilung in URLs und Anhänge zur Bedrohungsverteilung ist im Jahresvergleich unverändert geblieben. Auch wenn es einige wenige Zeiträume gab, in denen die Trends sich annäherten, machten URLs drei Viertel aller Gesamtbedrohungen aus.



Wenn wir Kampagnenbedrohungen in **finanziell motivierte** und **APT-Akteure** (Advanced Persistent Threat, hochentwickelte hartnäckige Bedrohung) unterteilen, sehen wir unterschiedliche Ansätze – APT-Akteure nutzen viel seltener Anhänge.

Während URLs gleichzeitig als häufigster Verbreitungsmechanismus für Cyberkriminalität dienen, ist die Verteilung gleichmäßiger. Einiges davon lässt sich auf den Einfluss einer Handvoll großer Akteure zurückführen. Wie wir im Kapitel „Im Blickpunkt: **Emotet**“ auf Seite 27 zeigen, hängt TA542 sehr an... Anhängen.

FormBook:

Diese Malware-as-a-Service wird seit 2016 in Foren verkauft. Die Preise sind vergleichsweise günstig, daher ist FormBook bei Angreifern sehr beliebt und wird für verschiedenste Angriffe mit ganz unterschiedlichen Social-Engineering-Taktiken und Übertragungsmethoden verwendet.

NetSupport:

Ein legitimes Remote-Zugriffs-Tool, das heute von vielen Cyberkriminellen missbraucht wird.

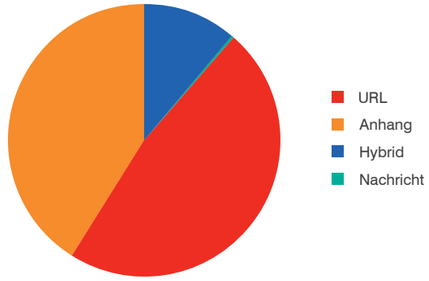
AgentTesla:

Eine weit verbreitete Stealer-Malware, die auch als Loader für sekundäre Schaddaten agiert.

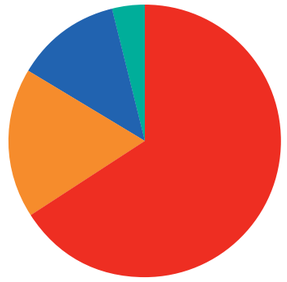
SocGholish:

Eine Malware für den Erstzugriff, die ausschließlich per Drive-by-Download von infizierten Websites verteilt wurde.

Verteilungsart: Cyberkriminalität

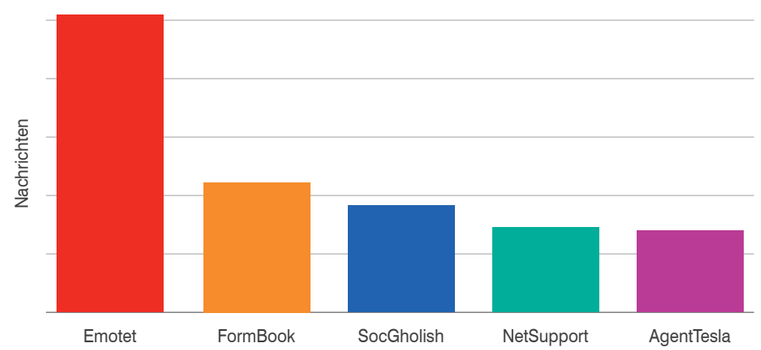


Verteilungsart: APT



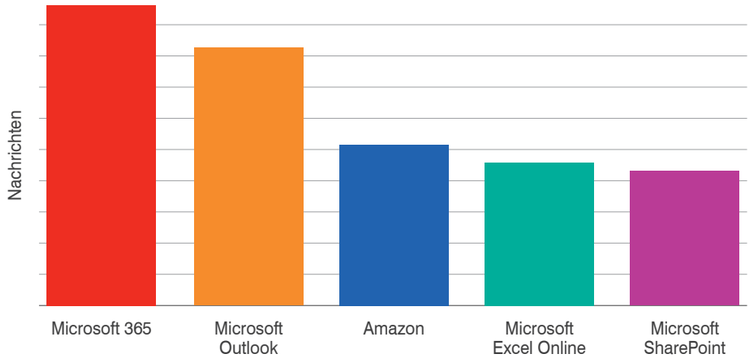
Häufigste Malware

Da TA542 der nach Aufkommen stärkste Bedrohungsakteur ist, überrascht es kaum, dass Emotet an der Spitze der Malware-Tabelle zu finden ist. Standard-Malware, die von verschiedenen Bedrohungsakteuren eingesetzt wird, belegt drei der vier weiteren Plätze (**FormBook**, **NetSupport** und **AgentTesla**). Doch der Aufstieg von **SocGholish** ist bemerkenswert. (Wir gehen im Kapitel „Im Blickpunkt: SocGholish“ auf Seite 22 im Detail darauf ein.)



Häufigste Köder

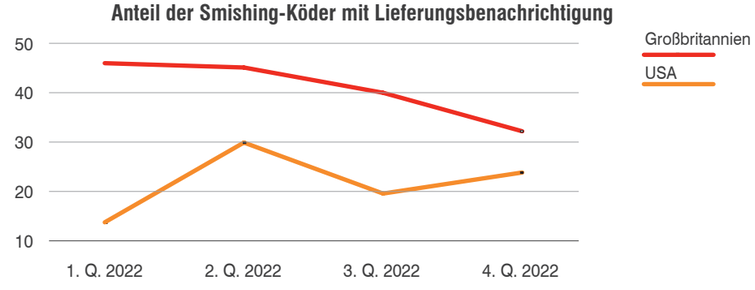
Der Missbrauch bekannter Marken und unseres Vertrauens darin ist eine der einfachsten Formen von Social Engineering. Und wieder einmal haben die Cyberkriminellen einen klaren Favoriten, wenn es um Markenmissbrauch geht.



Microsoft-Produkte und -Services belegen vier der Top 5-Positionen bei missbrauchten Marken (unter allen Bedrohungen), wobei Amazon den anderen Platz einnimmt. Bei den von unseren Forschern untersuchten Kampagnen war Amazon dabei die am häufigsten missbrauchte Marke, doch Microsoft belegt immer noch die übrigen vier Plätze.

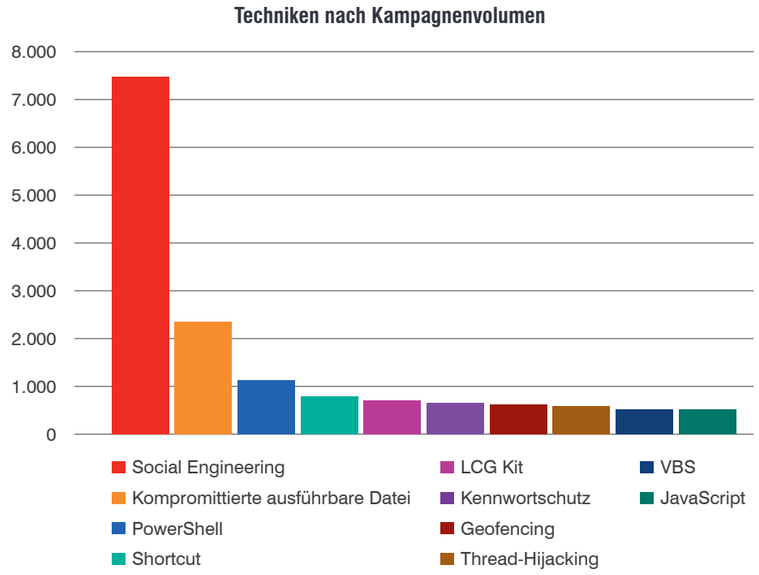
Als unsere Forscher den Fokus auf die Themen der schädlichen Nachrichten richteten, stellten sie fest, dass Begriffe wie „payment“ (Zahlung), „order“ (Bestellung), „invoice“ (Rechnung) und „purchase“ (Kauf) am häufigsten verwendet wurden.

Im Mobilgerätebereich war der häufigste Smishing-Betreff – Benachrichtigungen über Paketlieferungen – in den USA sowie in Großbritannien am häufigsten anzutreffen. Doch nachdem andere Ködertypen in Großbritannien zulegten, ging der Gesamtanteil der lieferungsbezogenen Smishing-Nachrichten zurück.



Häufigste Techniken

Als vor fast zehn Jahren der erste *Bericht zum Faktor Mensch* erschien, war eines unserer wichtigsten Anliegen, die zentrale Rolle von Social Engineering bei den meisten Cyberangriffen zu vermitteln. Bis heute ist das die häufigste von unseren Forschern entdeckte Technik. Die meisten von uns klassifizierten Angriffen umfassten zu einem gewissen Grad auch psychologische Manipulation.



Social Engineering lässt sich unbegrenzt skalieren – und die einzige Beschränkung ist die Raffinesse der Angreifer. Und selbst ohne die Nutzung von Malware oder technischen Exploits können die Folgen eines erfolgreichen Social-Engineering-Angriffs verheerend sein.

Identitätskrise

Unabhängig davon, ob Angreifer auf Phishing oder Malware-Verbreitung setzen, scheuen sie keine Mühen, um an Anmeldedaten für Unternehmensnetzwerke und -geräte zu gelangen. Es lohnt sich also, darüber nachzudenken, warum diese Zugriffe so wertvoll sind.

Anmeldeinformationen sind gleichbedeutend mit Anwenderidentitäten. Sobald Ihre Kombination aus Anmeldename und Kennwort kompromittiert wurde, kann der Angreifer sich gegenüber den entsprechenden Systemen mit Ihrer Identität ausweisen. Aktuelle Untersuchungen von Identitätsrisiken zeigten, wie leicht kompromittierte Identitäten zum Problem werden können.

Wie wir bei vielen Unternehmen feststellen, entstehen durch falsch konfigurierte Administratorkonten oder Schatten-Administratoren weitere Risiken für Anmeldedatendiebstahl. Lokale Administratoren werden von Lösungen zur Verwaltung privilegierter Zugriffe häufig nicht berücksichtigt. Zudem sind einige Administratorkonten den IT-Abteilungen gänzlich unbekannt, da die Berechtigungen entweder falsch zugewiesen wurden oder nach einer Änderung der Rolle nicht zurückgenommen wurden. Bis zu 40 % dieser Schatten-Administratoridentitäten können in einem einzigen Schritt missbraucht werden und erlauben beispielsweise das Zurücksetzen des Domain-Kennworts zur Erhöhung von Berechtigungen. Zudem zeigte sich, dass 13 % der Schatten-Administratoren bereits über Domain-Administratorberechtigungen verfügten.

Die Situation ist für Malware-Verbreiter ebenfalls günstig. Wie wir festgestellt haben, enthält jeder sechste Endpunkt eine Form von ausnutzbarem Identitätsrisiko. Etwa 10 % der Endpunkte haben ein ungeschütztes privilegiertes Kontokennwort, wobei 26 % dieser gefährdeten Konten zu Domain-Administratoren gehören. Es ist also nicht schwer zu erkennen, warum ein erfolgreicher Erstzugriff zu Domain-weiten Angriffen wie Ransomware-Infektionen oder Datendiebstahl führen kann.

1 von 6
Endpunkten ist gefährdet

TA471:

Ein Akteur, der hochentwickelte hartnäckige Bedrohungen zur Spionage bei Unternehmen und Behörden einsetzt.

TA416:

Eine APT-Gruppe, die mit China in Verbindung steht.

TA453:

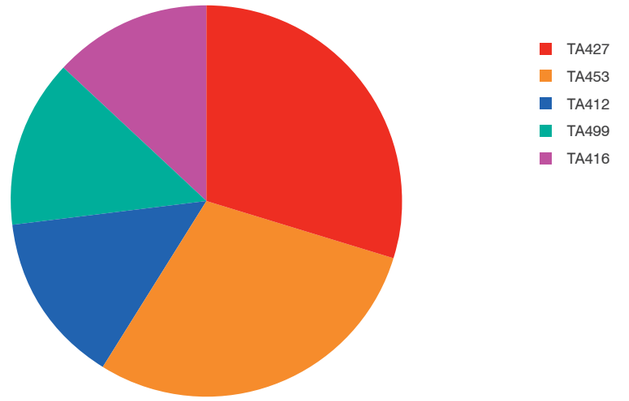
Eine APT-Gruppe, die im Auftrag der Iranischen Revolutionsgarde Spionage betreibt.

APT im Rampenlicht

Die im vorherigen Kapitel erwähnten Köderthemen zeigen, dass die vorherrschenden Motive immer noch finanzieller Art sind. Das zeigt sich darin, dass nur ein winziger Teil unserer Kunden von staatlich unterstützten APT-Akteuren angegriffen wird (und noch weniger werden von Gruppen attackiert, die mit einer der großen Weltmächte in Verbindung stehen).

Da das Volumen von APT-Aktivitäten im Vergleich zu finanziell motivierter Cyberkriminalität gering ist, kann ein einziger Ausreißerangriff übergroße Auswirkungen auf unsere Daten haben. Dies war im Jahr 2022 der Fall, als eine einzige große Kampagne den Akteur **TA471** an die Spitze des Diagramms des APT-Nachrichtenvolumens katapultierte. Das Nachrichtenvolumen kann jedoch auch in die Irre führen. Unsere Forscher geben als Kennzahlen für APT-Aktivitäten daher bevorzugt die Häufigkeit und Anzahl der Kampagnen an. So gesehen war **TA416**, eine Gruppe mit Verbindung zur chinesischen Regierung, einer der aktivsten APT-Akteure. Ganz konkret fanden unsere Forscher umfangreiche neue Kampagnen von TA416, die mit dem Beginn des Russland-Ukraine-Krieges zusammenhingen und gegen europäische diplomatische Einrichtungen für Flüchtlings- und Migrationshilfe gerichtet waren.

APT-Akteure nach Kampagnenvolumen



Für viele APT-Aktivitäten sind Präzision und Geduld entscheidend. Viele Akteure tauschen über einen Zeitraum von Wochen oder gar Monaten harmlose Nachrichten mit ihren Zielen aus, um Vertrauen aufzubauen. Diesem Muster folgen die meisten Aktivitäten von **TA453**, der zweitaktivsten APT-Gruppe des letzten Jahres, wobei die Gruppe in einigen Kampagnen mehrere Personen imitiert. Typische Ziele dieses Akteurs, der mit der Iranischen Revolutionsgarde in Verbindung stehen soll, sind Akademiker, Dissidenten, Journalisten und andere politische Einflussnehmer. Im vergangenen Jahr griff TA453 jedoch auch Forscher in den Bereichen Medizin und Luft-/Raumfahrt an.

ABSCHNITT 2

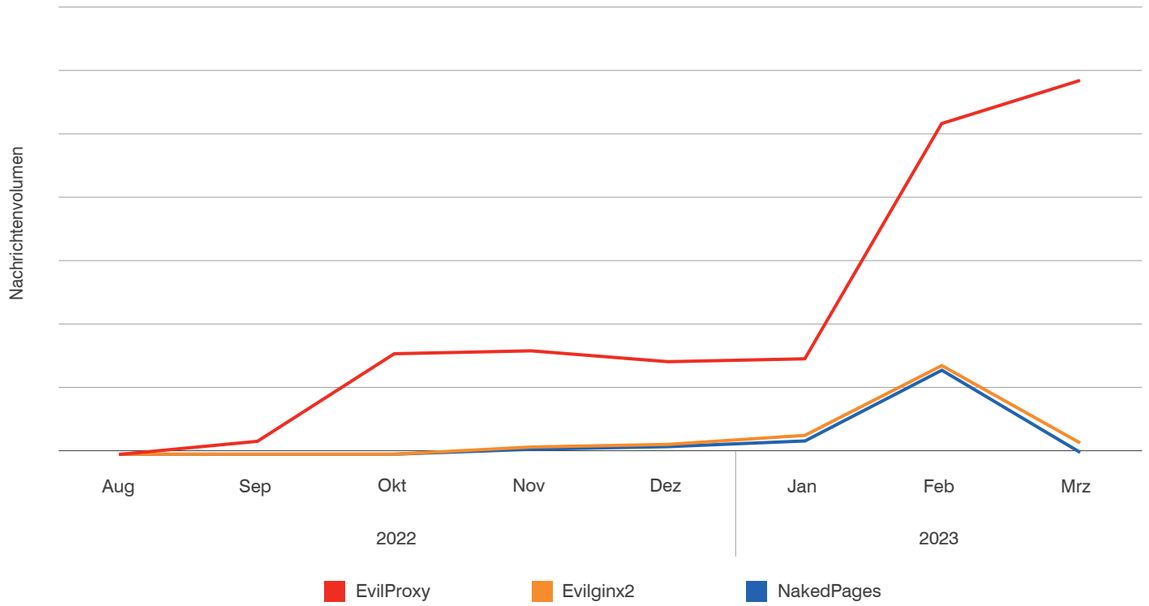
Neue Entwicklungen

Im Verlauf des Jahres 2022 setzten sich in der Bedrohungslandschaft mehrere technische und taktische Innovationen durch. Jede einzelne von ihnen markiert eine gefährliche Eskalation, seien es bislang unzugängliche Tools, die frei verfügbar werden, oder der breite Einsatz neuer Manipulationsmethoden.

Umgehung von Multifaktor-Authentifizierung

Viele Anwender gehen davon aus, dass eine aktive Multifaktor-Authentifizierung (MFA) ihre Konten und Daten zuverlässig schützt. Schließlich müssten Cyberkriminelle nicht nur an Ihre Anmeldedaten gelangen, sondern auch den zweiten Authentifizierungsfaktor kompromittieren, also Ihr Mobilgerät, den Telefonanschluss oder einen Token-Generator.

Doch beim Tauziehen zwischen Angriff und Verteidigung behält nur selten eine Seite länger die Überhand. Anfang 2022 entdeckten unsere Forscher eine neue Entwicklung in der Welt der Phishing-Kits. Mithilfe solcher Standardtools können selbst Kriminelle ohne Technikkenntnisse eine Phishing-Kampagne starten. Phishing-Kits sind keine neue Erscheinung. In den letzten Jahren hat sich der Markt von einem Lizenzmodell hin zu Betreibern entwickelt, die vollständig gehostetes Phishing-as-a-Service anbieten. Und im Jahr 2022 erhielten Phishing-Kits eine gefährliche neue Funktion: die Umgehung von MFA.



EvilProxy:

Eine Phishing-as-a-Service-Plattform mit erweitertem Funktionsumfang.

Evilginx2:

Ein Red-Team-Tool mit erweitertem Funktionsumfang, das Reverse-Proxy-Angriffe auf Mehrfaktor-Authentifizierung erlaubt.

NakedPages:

Ein Standard-Phishing-Kit mit erweitertem Funktionsumfang, das Reverse-Proxy-Angriffe auf Mehrfaktor-Authentifizierung erlaubt.

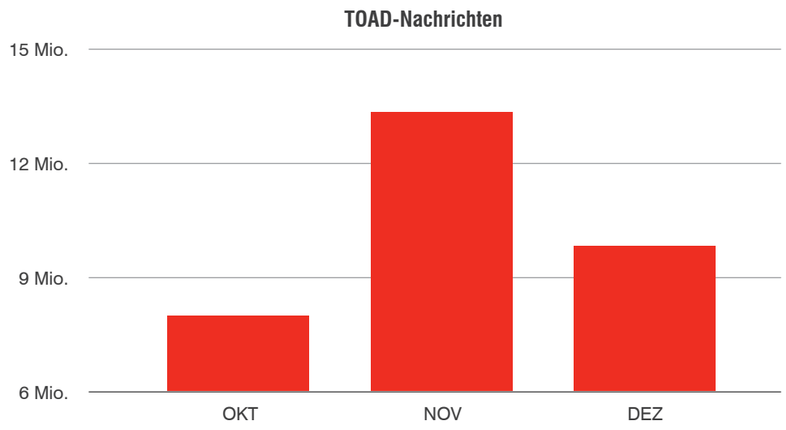
Im vierten Quartal 2022 entdeckten wir Angriffe mit drei bekannten Frameworks zur MFA-Umgehung: **EvilProxy**, **Evilginx2** und **NakedPages**. Zusammengenommen stehen diese Techniken für hunderttausende schädliche Nachrichten im Monat, wobei EvilProxy auch 2023 äußerst aktiv ist.

MFA ist immer noch ein zentraler Teil der gestaffelten Verteidigung und wird als Best Practice empfohlen. Doch die Zunahme dieser Techniken sollte als dringende Warnung verstanden werden, dass Angreifer versuchen, alle verfügbaren Assets in die Finger zu bekommen – auch Ihre MFA-Token.

Der TOAD kommt per Telefon

Im letzten Jahr berichteten wir über eine Zunahme bei TOAD-Angriffen (Telephone-Oriented Attack Delivery, Attacken per Telefon), eine neue Technik, die auf umfangreiche Interaktionen zwischen Angreifer und Opfer setzt. Die erste Stufe einer TOAD-Attacke ist gewöhnliches Social Engineering, beispielsweise in Form einer gefälschten Abonnementrechnung, mit der die Opfer davon überzeugt werden sollen, bei einer Telefon-Hotline anzurufen. Anstatt mit dem Kundendienst bekommen die Opfer es jedoch mit Cyberkriminellen zu tun. Im Laufe des Anrufs nutzen die Kriminellen verschiedene Taktiken und leiten die Opfer zum Beispiel an, ihnen Fernzugriff auf ihre Computer zu gewähren oder Malware herunterzuladen.

In diesem Jahr erweiterten wir unsere Systeme mit Funktionen, die TOAD-Angriffe automatisch erkennen, was uns ein deutlicheres Bild von der Verbreitung dieser Technik gibt.



BazaCall:

Ein frühes prominentes Beispiel für Telefonangriffe (Telephone-Oriented Attack Delivery), die Opfer mit der mittlerweile stillgelegten BazaLoader-Malware angriffen.

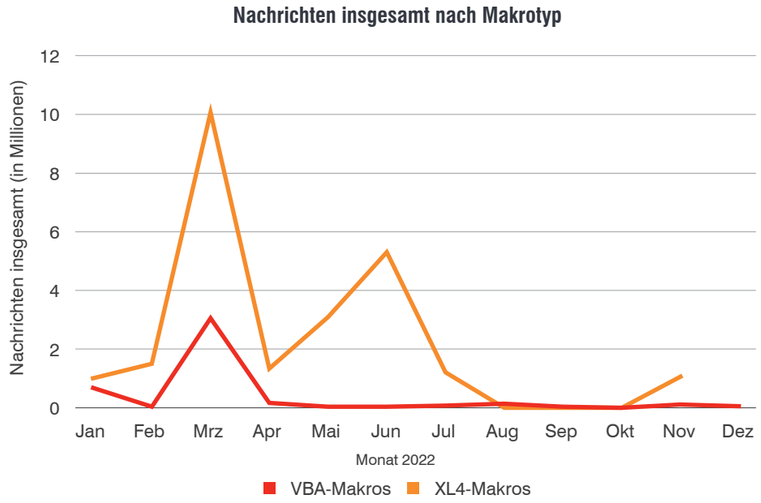
Dadurch können wir auch Millionen TOAD-Nachrichten im Monat erkennen und beseitigen. Und obwohl sie teilweise von bekannten Angreifern wie der **BazaCall**-Gruppe stammen, die im letzten Jahr gefälschte Film-Streaming-Websites und erfundene Justin Bieber-Touren anbot, spricht das enorme Volumen für den Einsatz durch weniger raffinierte Gruppen.

TOAD-Angriffe werden nicht wieder verschwinden, sodass Security-Awareness-Programme entsprechend angepasst werden sollten.

Erzwungene Evolution

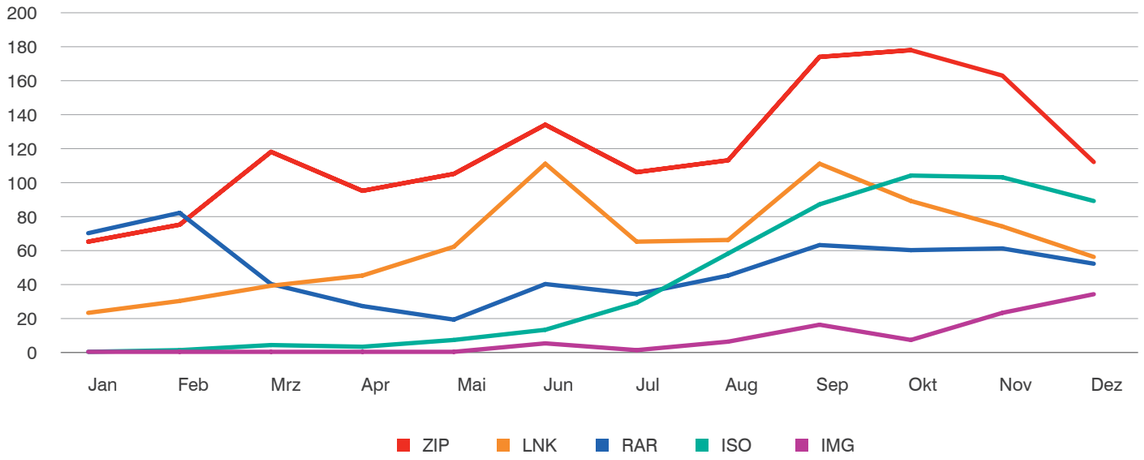
Cyberkriminelle sind innovationsgetrieben, doch das machen sie nicht zum Spaß. Wenn sich eine Taktik oder Technik als erfolgreich erweist, bleiben sie dabei, bis die Verteidiger ein Gegenmittel finden. Ein typisches Beispiel dafür ist die Nutzung von Office-Makros für die Malware-Übertragung. Die Technik selbst ist seit fast 20 Jahren bekannt – lange genug, dass Microsoft sich endlich dazu entschied, etwas gegen den Missbrauch zu unternehmen.

Im Laufe des Jahres 2022 änderte Microsoft die Methode, wie die eigenen Produktivitätsanwendungen mit Dateien aus dem Internet umgehen. Dadurch fällt es Cyberkriminellen deutlich schwerer, Malware mithilfe von Office-Dokumenten zu verteilen.



Das Aufkommen von Nachrichten mit Office-Makros ging daraufhin erheblich zurück, wobei zwei Spitzen bei VBA und XL4 auf Emotet-Aktivitäten zurückzuführen sind. Im Gegenzug kam es zu einer Zunahme bei anderen Dateitypen, als die Cyberkriminellen mit neuen Techniken experimentierten.

Dateityp nach Kampagnenzahl

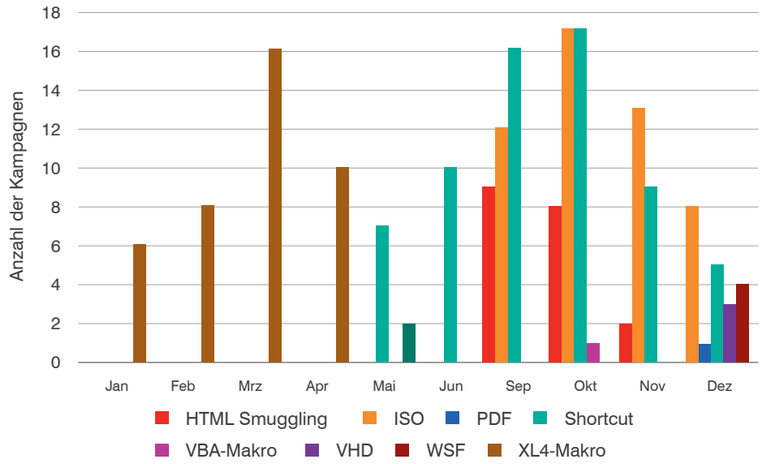


Der Bedrohungsakteur TA577 bietet ein gutes Beispiel für diese Evolution in der Praxis. Als überaus aktiver Qbot-Partner ist TA577 in den Top 5 nach Nachrichten- sowie dem Kampagnenvolumen vertreten. Im Jahr 2022 wechselte die Gruppe von Makros zu neuen Techniken und nutzte Dateitypen wie PDF, ISO und VHD (Virtual Hard Disk).

DAS ENDE DER MAKROS

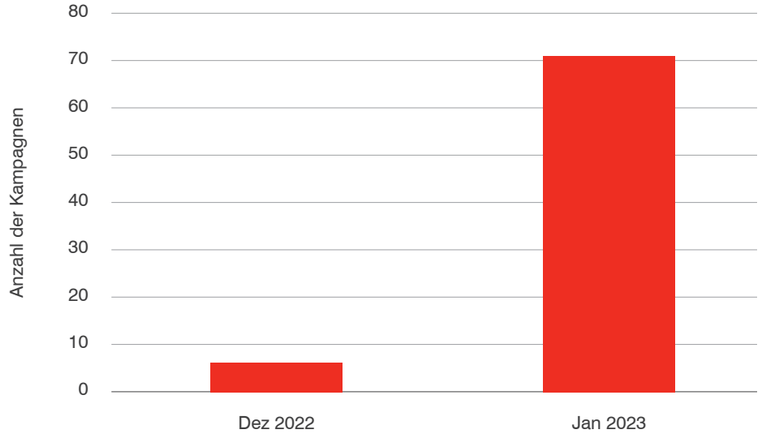
Da Office-Makros nicht mehr als zuverlässiger Malware-Übertragungsweg zur Verfügung standen, wechselten Bedrohungsakteure zu Dateitypen wie PDF, ISO und VHD (Virtual Hard Disk).

Von TA577 verwendete Techniken (2022)



Doch das Ende der Office-Makros bedeutet nicht, dass die Angreifer Microsoft den Rücken kehren. Ende des Jahres stellten unsere Forscher eine plötzliche Zunahme bei den Kampagnen fest, die Microsoft OneNote missbrauchen. Nach einem enormen Kampagnenaufkommen Anfang 2023 gab Microsoft Pläne zur Verbesserung der Sicherheitsmaßnahmen für Dateien bekannt, die in OneNote-Dokumenten eingebettet sind.

Anzahl der Kampagnen mit OneNote



Im Blickpunkt: SocGholish

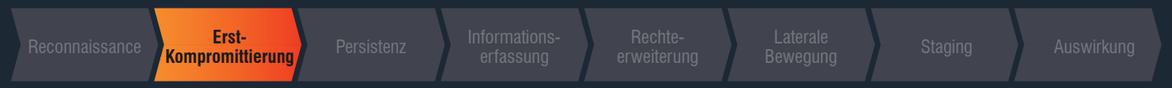
Eine der bemerkenswertesten Bedrohungen des Jahres war SocGholish, eine ausschließlich von der Cybercrime-Gruppe **TA569** verteilte Malware. Unter den von uns überwachten aktivsten Bedrohungsakteuren kam TA569 gleich an zweiter Stelle nach TA542/Emotet. Und unter den Malware-Familien, die in schädlichen E-Mails verteilt werden, hatten nur Emotet und die Standard-Malware **FormBook** ein höheres Nachrichtenvolumen.

TA569:

Eine Cybercrime-Gruppe, die für die Kompromittierung von Content-Management-Servern zur Verteilung von SocGholish bekannt ist. Als Vermittler für den Erstzugriff gibt es Verbindungen der Gruppe mit WastedLocker und möglicherweise mit anderen Ransomware-Akteuren.

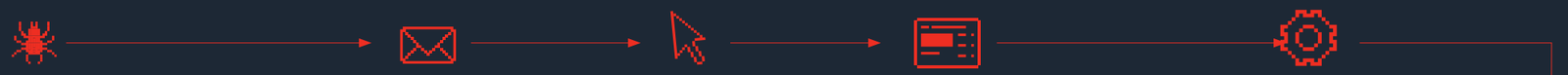
Die Angriffskette

Die Cyber-Angriffskette ist ein Modell, das den typische Ablauf der meisten Bedrohungen beschreibt. Auch wenn jeder Angriff in gewisser Weise einmalig ist, folgen die meisten einer typischen Abfolge. Nachfolgend vergleichen wir den Ablauf der Erst-Kompromittierung zweier großer Malware-Familien.



Angriffskette von SocGholish: Erst-Kompromittierung

Im Gegensatz zu den meisten Malware-Familien, die in diesem Bericht vorgestellt werden, gelangt SocGholish nicht per E-Mail-URL oder -Anhang zu seinen Opfern, sondern überwiegend über E-Mails von legitimen Versendern. Bei SocGholish handelt es sich um eine „Drive-by-Malware“, die auf infizierten Websites mit gefälschten Browser-Update-Warnungen darauf wartet, dass die Opfer sie herunterladen.



Infizieren des Hosts

Malware kann von infizierten Websites verteilt werden. Dazu nutzt der Angreifer eine Schwachstelle auf der Website oder einer Website-Komponente aus, z. B. Werbeblöcke oder eingebettete Assets.

Legitime E-Mail

Die Betreiber infizierter Websites wissen oft nicht, dass sie SocGholish hosten, und senden weiter E-Mails an die Anwender.

Klick auf die URL

Wenn Empfänger auf einen Link zu einer Website mit SocGholish klicken, riskieren sie eine Infektion.

Gefälschtes Browser-Update

SocGholish zeigt den Anwendern meist eine Popup-Benachrichtigung und fordert sie zum Herunterladen und Installieren eines „Browser-Updates“ auf, das in Wirklichkeit eine Malware ist.

SocGholish ist installiert

Wenn Anwender die Aufforderung des gefälschten Updates befolgen, wird SocGholish auf ihrem Computer installiert.

Ransomware oder andere nachfolgende Aktivitäten

Angriffskette von Emotet: Erst-Kompromittierung

Vergleichen wir diese Angriffskette mit Emotet-basierten Angriffen, die einem klassischeren Muster folgt.

E-Mail

Die meisten Malware-Exemplare werden durch schädliche E-Mails mit Links oder über Anhänge verteilt.

Mit Anhang

Die Gruppe hinter Emotet ist mittlerweile der einzige im großen Maßstab agierende Bedrohungsakteur, der Office-Makro-Anhänge nutzt.

Anhang wird geöffnet

Damit eine E-Mail-Bedrohung wirklich gefährlich wird, muss der Empfänger zuerst den Anhang öffnen.

Interaktion mit Anhang

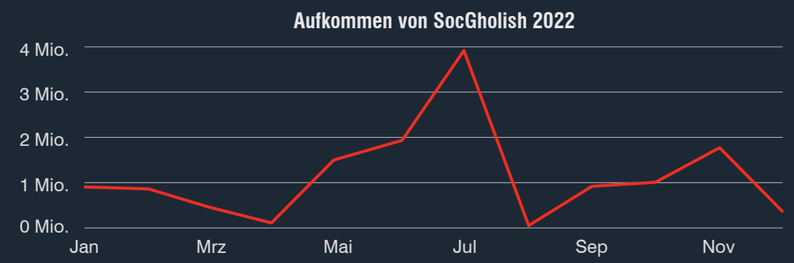
Nachdem der Anhang geöffnet wurde, muss der Empfänger meist noch etwas weiter gehen, bevor die Bedrohung wirksam wird. Im Fall von Emotet muss das Opfer üblicherweise noch auf eine Schaltfläche klicken, um Office-Makros zu aktivieren.

Emotet ist installiert

Wenn Empfänger den schädlichen Anhang aktivieren, wird Emotet heruntergeladen und auf ihrem Computer installiert.

In diesem Jahr verteilte TA569 Malware über einige Websites mit sehr hohem Besucherverkehr, darunter beispielsweise für einen kurzem Zeitraum einige lokale und nationale Nachrichtenseiten. Während dieser Zeit wurden alle E-Mails mit einem Link zu einer infizierten Website (z. B. tägliche Newsletter, Meldungen zu topaktuellen Nachrichten oder externe Zusammenfassungen) als potenzielles SocGholish-Infektionsrisiko gekennzeichnet.

Im konkreten Fall der Nachrichten-Websites konnten Administratoren die Quelle der Infektion identifizieren und entfernten das schädliche Skript innerhalb weniger Stunden. Doch viele andere Websites, die SocGholish hosten, sind sich ihrer Infektion nicht bewusst. Die Sachlage wird dadurch verkompliziert, dass TA569 die Injektionen auf den infizierten Websites aktiviert und deaktiviert, was das Identifizieren der betroffenen Hosts zusätzlich erschwert.



Doch während das E-Mail-Aufkommen von SocGholish in etwa dem anderer bekannter Malware-Familien entspricht, gibt es einen großen Unterschied hinsichtlich der Verbreitung dieser Bedrohung. Das Wissen über diesen Unterschied ist nicht nur für den Schutz vor SocGholish wichtig – er liefert auch wertvolle Einblicke darin, wie Social Engineering in ganz unterschiedlichen Bereichen der Entscheidungsfindung wirksam werden kann.

Raffiniertes Social Engineering

SocGholish ist eine interessante Fallstudie, da die Angriffskette sowohl aktive als auch passive Formen von Social Engineering enthält. Ganz deutlich ist das beim gefälschten Browser-Update, das die Computerkenntnisse der Anwender ausnutzt, um sie zur Installation von schädlicher Software zu überzeugen. Doch abgesehen von dieser allzu offensichtlichen Manipulation gehen unsere Forscher davon aus, dass TA569 auch ein subtileres Ziel verfolgt.

Die Geduld der Anwender mit den Systemen und Tools zu untergraben, die eigentlich für ihren Schutz gedacht sind, erscheint ambitioniert. Gleichzeitig haben einige Bedrohungsakteure bereits Erfahrungen damit gesammelt. In einer der größten Datenschutzverletzungen des letzten Jahres erlangten die Angreifer Zugriff auf die Systeme ihrer Opfer, indem sie konkrete Anwender mit MFA-Push-Anforderungen auf deren Mobilgerät bombardierten. Wenn diese Anwender ausreichend genervt waren, klickten sie irgendwann auf „Ja“, um den Anmeldeversuch zu authentifizieren. Was ursprünglich der Verteidigung diente, entwickelte sich so zu einer Schwachstelle, einfach weil der Angreifer sie zu einer Störung umfunktioniert hatte.

Im Fall von SocGholish ist es möglich, dass hohe E-Mail-Volumen von legitimen Quellen, die als schädlich markiert werden, die Anwender zum Safelisting bestimmter Websites motivieren. Schlimmer noch wird es aber, wenn die Empfänger anfangen, die E-Mail-Warnungen gänzlich zu ignorieren. Wenn eines von beidem geschieht, führt der Erfolg von TA569 dazu, dass alle Cyberkriminellen profitieren.

TA2536:

Eine seit langem aktive finanziell motivierte Cybercrime-Gruppe, die zum ersten Mal im Jahr 2015 beobachtet wurde. Verteilt üblicherweise schädliche Office-Dokumente.

LokiBot:

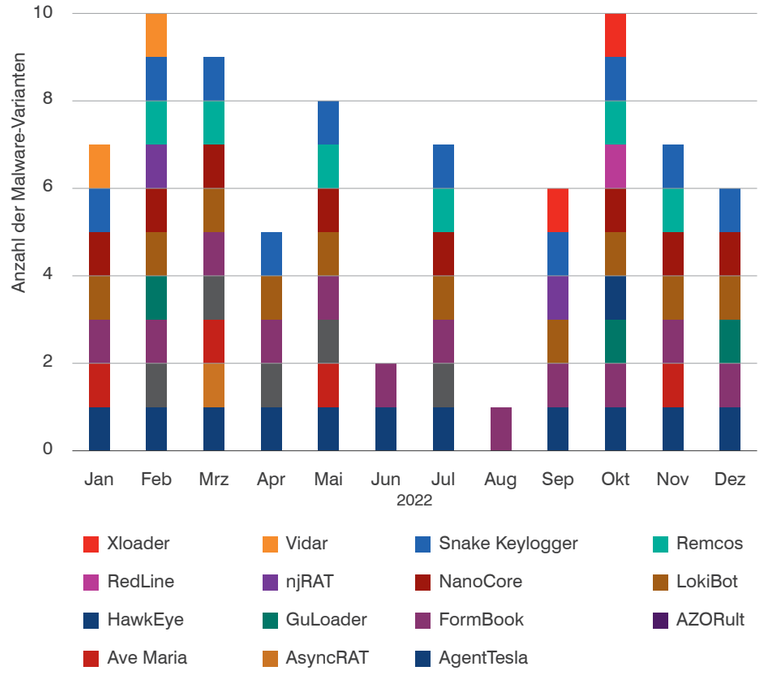
Gängige Stealer-Malware, die zum ersten Mal im Jahr 2016 beobachtet wurde und auch als Backdoor für sekundäre Infektionen genutzt wird.

Schnelle Iteration

Die Fluktuationen in der Bedrohungslage sind eine ständige Herausforderung für Sicherheitsteams und Forscher. Die agilsten Bedrohungsakteure ändern regelmäßig ihre Social-Engineering-Strategien und Malware-Payloads, damit sie als bewegliches Ziel schwerer zu treffen sind.

Ein gutes Beispiel für diese Tendenz im Jahr 2022 war die Cybercrime-Gruppe **TA2536**, die wir seit 2015 verfolgen. TA2536 nutzt Standard-Malware, die im Laufe des Jahres 15 verschiedene Payloads verteilte. Die Informationsdiebe AgentTesla und **LokiBot** tauchten häufig in den Kampagnen der Gruppe auf, doch wie das Diagramm unten zeigt, kamen ansonsten sehr unterschiedliche Payloads zum Einsatz.

TA2536: Verwendete Malware nach Monat



Pig Butchering:

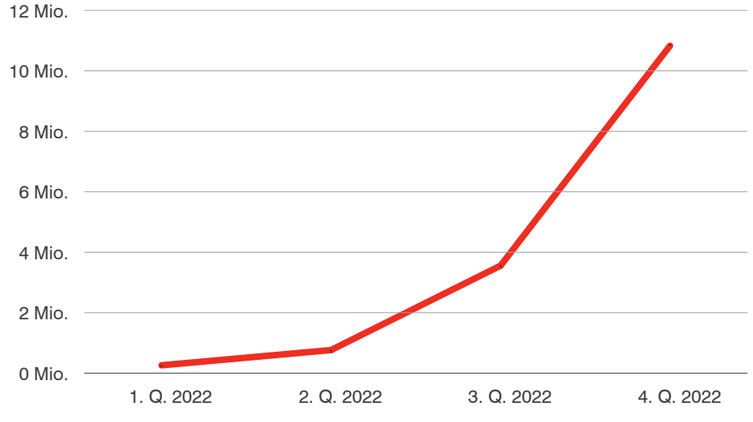
Eine Form von Konversationsbedrohung, bei der harmlose Nachrichten ausgetauscht werden, bevor der Angreifer Geld von seinen Opfern erbeutet, indem er sie davon überzeugt, in gefälschte Kryptowährungs-plattformen zu investieren.

Plaudern mit Angreifern

Cyberangriffe und Cyberschutz sind typischerweise sehr technische Disziplinen, doch die wichtigsten Entwicklungen des Jahres 2022 waren überhaupt nicht technischer Natur. Konversationsangriffe sind schon eine ganze Weile in der Bedrohungslandschaft vertreten. APT-Angreifer sind beispielsweise bekannt dafür, dass sie viel Zeit und Mühe darauf verwenden, Vertrauen bei ihren Opfern aufzubauen, bevor sie deren Anmeldedaten oder andere vertrauliche Informationen stehlen. Doch unsere Daten zeigen, dass es im Verlauf des Jahres zu einer erheblichen Zunahme bei Konversationsangriffen durch finanziell motivierte Akteure kam.

Für den Mobilbereich stellte unsere Cloudmark-Abteilung während der ersten Jahreshälfte einen Anstieg um den Faktor 12 fest. Durch diese enorme Zunahme bei diesen Angriffen, zu denen Romance Scams (Betrug mit Kontaktanzeigen), gefälschte Stellenanzeigen und **Pig Butchering**-Kryptowährungsbetrug gehören, wurden Konversationsangriffe in einigen Branchen zur häufigsten Angriffsform. Selbst ohne Berücksichtigung der vereinfachten Missbrauchsmeldung in iOS zeigen die Daten im Mobilbereich eine erhebliche Verschiebung zu Konversationsansätzen.

Berichte über Konversationsbedrohungen: USA



2,5 Mrd. USD
Verluste aufgrund von Kryptowährungsbetrug 2022

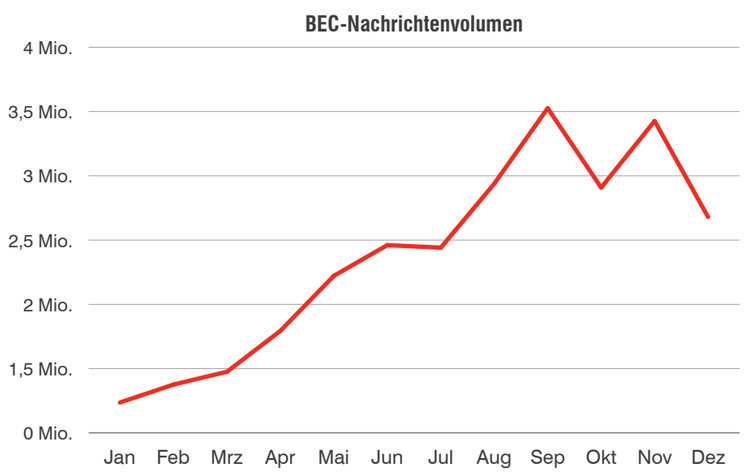
2,7 Mrd. USD
Verluste durch BEC-Angriffe auf US-Unternehmen

34 Mio. USD
Verluste durch Ransomware

Diese Angriffe verursachen erhebliche Kosten. Der aktuelle *Internet Crime Report* des FBI spricht von Verlusten in Höhe von 2,5 Milliarden US-Dollar durch Kryptowährungsbetrug[1], wobei Pig Butchering zu den besonders auffälligen Methoden gehört. Und die Verluste sind nicht nur finanzieller Natur. Konversationsangriffe sind deshalb erfolgreich, weil das Opfer eine emotionale Beziehung zum Angreifer aufbaut. Bei Romance Scam und Pig Butchering kann die Erkenntnis, dass dieses Vertrauen missbraucht wurde, ebenso verheerend sein wie der finanzielle Verlust.

Business Email Compromise (BEC)

Auch wenn das für Pig Butchering und Romance Scam typische informelle Geplauder in E-Mails seltener anzutreffen ist, fallen bestimmte über APT hinausgehende E-Mail-Bedrohungskategorien durchaus in dieses Muster. Die meisten BEC-Angriffe (Business Email Compromise, auch als Chefmasche bezeichnet) nutzen weder Phishing noch Malware. Stattdessen setzen die Angreifer auf Social Engineering und andere Täuschungsmethoden, um sich unerkannt in normale Geschäftskommunikation einzuklinken und gefälschte Rechnungen, Überweisungsaufträge oder ähnliches zu versenden.



BEC ist eine scheinbar niederschwellige Bedrohung, die weitaus weniger Aufmerksamkeit erhält als Ransomware und Datenlecks. Doch laut dem *Internet Crime Report* des FBI kostete BEC amerikanische Unternehmen im vergangenen Jahr 2,7 Milliarden US-Dollar, wobei die weltweiten Zahlen sicherlich deutlich höher liegen werden. Im Vergleich dazu betrugen die Verluste von Ransomware-Opfern etwas mehr als 34 Millionen US-Dollar.

1. FBI: „Internet Crime Report 2022“ (Bericht zu Internetkriminalität 2022), März 2023.

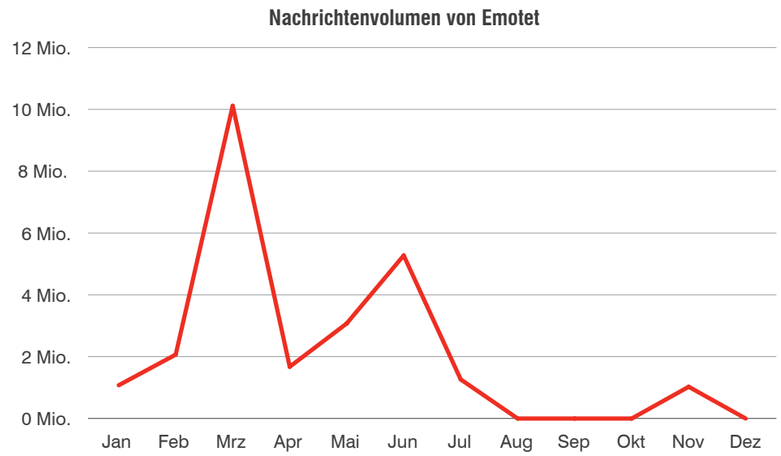
Conti:

Früher die gefährlichste Ransomware-Gruppe der Welt. Die Gruppe löste sich 2022 auf, nachdem viele interne Dokumente auf Twitter veröffentlicht wurden. Untersuchungen deuten darauf hin, dass viele in Verbindung mit Conti stehende Personen sich anderen Gruppen angeschlossen haben und weiterhin im Cybercrime-Ökosystem aktiv sind.

Im Blickpunkt: Emotet

Im Januar 2021 legten Strafverfolgungsbehörden das Emotet-Botnet still: Sie führten Verhaftungen durch und beschlagnahmten Gelder sowie Technik. Damit wurde die aktivste Malware zwar über Nacht offline genommen, doch der Optimismus nach dieser Operation erwies sich als verfrüht. Im vergangenen November meldete sich Emotet wieder auf der Bühne zurück und begann mit dem Versand neuer Kampagnen. Unabhängige Berichte aus der Zeit zogen eine Verbindung zwischen der Rückkehr von Emotet und Aktivitäten der Ransomware-Gruppe **Conti**, die ihre primäre Erstzugriffs-Malware konsolidierte.

Die Emotet-Aktivitäten im Jahr 2022 waren erratisch. Die einzigen beiden bemerkenswerten Aktivitätsspitzen fanden im März und Juni statt, während das Botnet im August, September, Oktober und Dezember komplett inaktiv war. Trotz dieses Verhaltensmusters verschickte TA542, die Gruppe hinter Emotet, im letzten Jahr mehr schädliche E-Mails als alle anderen von uns überwachten Bedrohungsakteure.



DIE VERBINDUNG ZWISCHEN EMOTET UND CONTI

Die @ContiLeaks bestätigten Annahmen über eine enge Zusammenarbeit von Conti und Emotet. Nachdem Conti alle Aktivitäten einstellte, kann es bei Emotet zu Turbulenzen gekommen sein.

Eine mögliche Erklärung für die Ruhephasen von TA542 ist das Schicksal der Ransomware-Gruppe Conti. Ende Mail 2022 gab die Gruppe Pläne zur Einstellung ihrer Aktivitäten bekannt, nachdem große Mengen interner Daten der Gruppe auf Twitter veröffentlicht wurden. Die @ContiLeaks bestätigten Annahmen über eine enge Zusammenarbeit von Conti und Emotet. Nachdem Conti ihre Aktivitäten einstellte, kann es bei Emotet intern zu Turbulenzen gekommen sein.

Ebenso ist es jedoch auch gut möglich, dass Emotet einfach auf einen günstigen Zeitpunkt wartete. Die Gruppe ist ein Sonderfall unter den im großen Maßstab agierenden Bedrohungsakteuren und verteilt ihre Malware beispielsweise vornehmlich als E-Mail-Anhang, statt dem allgemeinen Trend zu URL-basierten Angriffen zu folgen. Dennoch führte auch Emotet testweise kleinere Kampagnen mit URL-Versand durch. Das deutet darauf hin, dass die Gruppe – ebenso wie viele andere große Akteure – sich Zeit dabei lässt, diesen Veränderungen zu folgen.

ABSCHNITT 3

Opportunistische Angriffe

HILFSORGANISATIONEN IM VISIER

Eine wahrscheinlich staatlich unterstützte Phishing-Kampagne richtete sich gegen Mitarbeiter, die mit der Koordination von Flüchtlingen des Russland-Ukraine-Krieges betraut waren. Eine Woche später wurde der mit China in Verbindung stehende Angreifer TA416 dabei beobachtet, wie er ähnliche Hilfsmaßnahmen ins Visier nahm.

Einer der wichtigsten Faktoren bei Social Engineering ist die Aktualität. Köder, die sich auf aktuelle Ereignisse beziehen oder zeitlich knappe Entscheidungen fordern, bringen die Opfer dazu, einige ihrer üblichen Vorsichtsmaßnahmen über Bord zu werfen. In den letzten Jahren bot COVID-19 den Angreifern einen reichhaltigen Fundus an Schlagzeilen und Behördenentscheidungen, die sie in ihren Ködern verarbeiten konnten. Nachdem die Pandemie in diesem Jahr in vielen Ländern in den Hintergrund getreten ist, suchten die Cyberkriminellen opportunistisch nach anderen Möglichkeiten.

Russland-Ukraine

Als der Russland-Ukraine-Krieg Ende Februar losbrach, sagten einige Kommentatoren ein Jahr mit beispiellosen Cyberkonflikten voraus. Glücklicherweise ist das nicht eingetreten. Die politischen, wirtschaftlichen und humanitären Umwälzungen boten mehreren APT-Akteuren jedoch Chancen, die sie nicht ignorieren konnten.

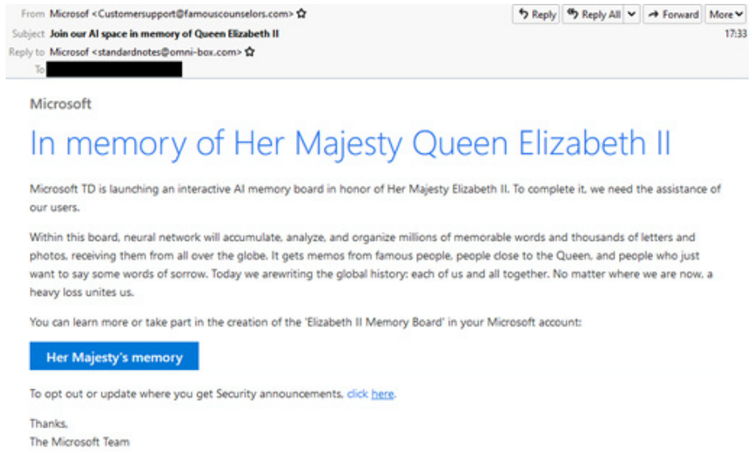
Innerhalb weniger Tage nach der Invasion deckten unsere Forscher einen wahrscheinlich staatlich unterstützten Angriff auf, der kompromittierte Anmeldedaten von ukrainischen Militärangehörigen nutzte. Die Kampagne richtete sich gegen europäische Behördenmitarbeiter, die mit logistischen Aufgaben oder der Flüchtlingskoordination betraut waren. Nur eine Woche später wurde der mit China in Verbindung stehende Angreifer TA416 dabei beobachtet, wie er ähnliche Hilfsmaßnahmen ins Visier nahm.

PROFITE MIT DER KRONE

Ein Köder gab sich als Teil eines „digitalen Gedenkbuchs“ aus und leitete die Opfer zu einer Website, die deren Anmeldedaten erfasste.

Queen Elizabeth II.

Während internationale Konflikte den staatlich unterstützten Angreifern zahlreiche Möglichkeiten boten, waren finanziell motivierte Cyberkriminelle weniger wählerisch. Im September bot der Tod von Queen Elizabeth II. einem Bedrohungsakteur die Gelegenheit, eine ungewöhnliche Phishing-Kampagne zu starten. Der Köder gab sich als Teil eines „digitalen Gedenkbuchs“ aus, das von Microsoft entwickelt wird. Wenn die Anwender per Klick teilnehmen wollten, wurden sie zu einer URL weitergeleitet, die ihre Anmeldedaten erfasste.


From Microsof <Customersupport@famouscounselors.com>
Subject Join our AI space in memory of Queen Elizabeth II
Reply to Microsof <standardnotes@omni-box.com>
To [redacted]
Reply Reply All Forward More
17:33

Microsoft

In memory of Her Majesty Queen Elizabeth II

Microsoft TD is launching an interactive AI memory board in honor of Her Majesty Elizabeth II. To complete it, we need the assistance of our users.

Within this board, neural network will accumulate, analyze, and organize millions of memorable words and thousands of letters and photos, receiving them from all over the globe. It gets memos from famous people, people close to the Queen, and people who just want to say some words of sorrow. Today we arewriting the global history: each of us and all together. No matter where we are now, a heavy loss unites us.

You can learn more or take part in the creation of the 'Elizabeth II Memory Board' in your Microsoft account:

Her Majesty's memory

To opt out or update where you get Security announcements, click here.

Thanks,
The Microsoft Team

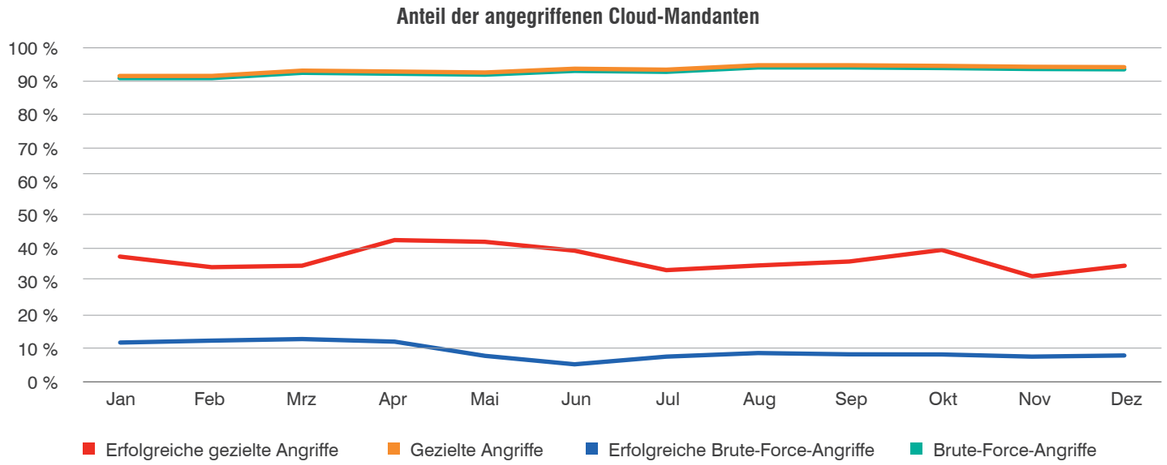
Silicon Valley Bank

Der Zusammenbruch der Silicon Valley Bank (SVB) im März zeigt eindrucksvoll, wie schnell Cyberangreifer sich eine Krise zu Nutze machen können. Innerhalb weniger Stunden nachdem US-Behörden die Kontrolle über die ins Straucheln geratene Bank übernommen hatten, fanden unsere Forscher dutzende frisch registrierte Doppelgänger- und Typosquatting-Domains. Und praktisch sofort gingen bei SVB-Kunden gezielte schädliche E-Mails ein, die zu Geldüberweisungen oder illegalen Aktivitäten aufforderten.

ABSCHNITT 4

Finstere Machenschaften in der Cloud

Im letzten Jahr berichteten wir darüber, wie die Allgegenwärtigkeit von Cloud-Infrastrukturen zu einer erheblichen Zunahme von Bedrohungen gegen Cloud-Mandanten geführt hat. Dieser Trend hat sich so weit fortgesetzt, dass jetzt Cloud-Bedrohungen selbst allgegenwärtig geworden sind.



62 %

der angegriffenen Cloud-Mandanten wurden erfolgreich kompromittiert

Das durchschnittliche Aufkommen an Brute-Force-Angriffen stieg um

400 %

(Anfang 2023 im Vergleich zum monatlichen Durchschnitt 2022)

Im Jahr 2022 wurden bis zu 98 % der überwachten Mandanten mit einem gezielten oder per Brute Force durchgeführten Cloud-Angriff attackiert. Teilweise waren die Angriffe so häufig, dass jeden Monat 94 % der überwachten Mandanten attackiert wurden. Diese Konstanz ist mit den Angriffen per E-Mail und über Mobilgeräte vergleichbar.

Bei den gezielten Angriffen gegen Cloud-Mandanten waren 62 % erfolgreich, wobei die monatliche Erfolgsrate bei etwa 20 % lag. Das sind etwas weniger als der Monatsdurchschnitt im vergangenen Jahr (24 %). Wahrscheinlich haben Cloud-Administratoren auf die wachsende Gefahr reagiert und Maßnahmen zum Schutz ihrer Systeme und Anwender ergriffen.

Ein anderer Grund für die sinkende Erfolgsrate kann die Außerbetriebnahme einiger veralteter E-Mail-Protokolle durch Microsoft sein. Der Wegfall dieser weniger sicheren Optionen hat zur Mitte des Jahres zu einem Rückgang bei erfolgreichen Brute-Force-Angriffen geführt. Die Effektivität der gezielten Angriffe hat jedoch nicht nachgelassen. Die abnehmende Effektivität der Brute-Force-Angriffe hat die Angreifer möglicherweise motiviert, das Angriffsvolumen deutlich zu erhöhen. Anfang 2023 stieg die Zahl der Brute-Force-Angriffe – und insbesondere der Password-Spraying-Attacken – laut unseren Daten von monatlich durchschnittlich 40 Millionen auf fast 200 Millionen. Dennoch ist es eher unwahrscheinlich, dass die sinkende Effektivität langfristig dazu führen wird, dass Angreifer andere Techniken und Vektoren nutzen.

14 %

der erfolgreichen Cloud-Angriffe im zweiten Halbjahr 2022 führten nach der Kompromittierung direkt zu Aktivitäten mit schädlichen E-Mails

13 %

der erfolgreichen Cloud-Angriffe führten zu Aktivitäten mit schädlichen Dateien

11 %

der Unternehmen autorisierten eine schädliche externe Anwendung

Aktivitäten nach dem Zugriff

Sobald ein Cloud-Mandant kompromittiert wird, haben die Bedrohungsakteure mehrere Optionen. Mit einem einzigen Satz Anmeldedaten erhalten sie häufig Zugriff auf E-Mails, Dokumentspeicher und andere Single Sign-On-Services, was schwerwiegende Folgen nach sich ziehen kann. Bei den beobachteten Cloud-Mandanten, die im zweiten Halbjahr des letzten Jahres einen erfolgreichen Angriff verzeichnet hatten, stellten mindestens 14 % nach dem Zugriff schädliche E-Mail-Aktivitäten fest. Thread-Hijacking und Nachahmung gehören zu den wichtigsten Tools in den Playbooks von BEC- und Supply-Chain-Angriffen. Böswillige Postfach-Zugriffe können daher nicht nur für das angegriffene Unternehmen, sondern auch für dessen Kunden und Partner Folgen haben.

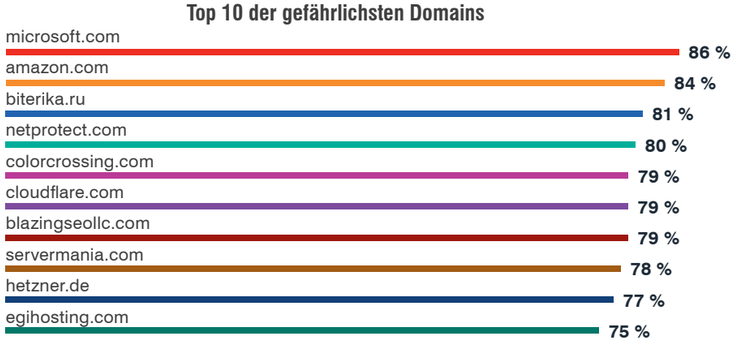
Die Aktivitätsraten bei schädlichen Dateien waren ähnlich und betrafen im Jahr 2022 etwa 13 % der attackierten Mandanten. Zu den Dateiaktivitäten gehören nicht nur Datendiebstahl, sondern auch das Hochladen von schädlichen Dateien, die Malware oder Phishing-Bedrohungen enthalten, oder das Manipulieren vorhandener Dokumente wie Zahlungsdaten von Lieferanten).

Die Fähigkeit der Angreifer, sich dauerhaft in der kompromittierten Umgebung festzusetzen, erweist sich bei Cloud-basierten Angriffen als immer größere Herausforderung. Viele Angreifer richten neue Postfach-Regeln wie Weiterleitungen ein oder manipulieren die Faktoren für die Multifaktor-Authentifizierung, sodass auch dann ein gewisser Zugang erhalten bleiben, wenn der unmittelbare Zugriff erkannt und gesperrt wird. In anderen Fällen autorisieren Angreifer schädliche OAuth-Anwendungen, um die Langlebigkeit und Persistenz des Zugriffs zu steigern. Laut einer konservativen Schätzung haben mindestens 11 % aller Unternehmen im vergangenen Jahr eine schädliche externe Anwendung autorisiert.

Traffic-Quellen

Wie die in diesem Bericht erläuterten Köder bereits gezeigt haben, ist die Nutzung legitimer Infrastrukturen eine bewährte und zuverlässige Technik von Social-Engineering-Akteuren. Dieser Ansatz spielt jedoch auch bei der Verbreitung vieler Cloud-basierter Angriffe eine wichtige Rolle. Etwa 80 % aller Unternehmen verzeichneten im vergangenen Jahr Brute-Force-Angriffe, die von Microsoft-, Amazon- und Cloudflare-Infrastrukturen ausgingen. Während sich Bedrohungen von anderen Domains in dieser Liste wahrscheinlich leicht per Blocklist sperren lassen, zeigen Cloud-Giganten wie Microsoft, Amazon und Cloudflare (deren Infrastrukturen unzählige geschäftskritische Services hosten) die Grenzen regelbasierter Schutzmaßnahmen.

Top 10 der gefährlichsten Domains



Fazit

Ganz gleich, wo Angreifer nach neuen Taktiken suchen: Für den Schutz vor zukünftigen Bedrohungen benötigen Sie einen personenzentrierten Ansatz. Wenn Ihre Anwender das Unerwartete erwarten, werden sie eine Bedrohung leichter erkennen und die Angriffskette unterbrechen können – ganz gleich, ob der Angriff über eine perfekt gestaltete Phishing-Seite oder über eine raffinierte Textnachricht erfolgt, die scheinbar von einem alten Freund gesendet wurde.

Cyberangriffe lassen sich nicht vermeiden. Es ist jedoch möglich, sie mit den richtigen Ansätzen, Tools und Richtlinien unter Kontrolle zu bringen. Verwenden Sie daher eine Lösung, die Ihnen zeigt, wer wie angegriffen wird und ob die angegriffene Person geklickt hat.

Errichten Sie eine zuverlässige Abwehr zum Schutz vor E-Mail-Betrug. E-Mail-Betrug lässt sich häufig nur schwer erkennen. Investieren Sie daher in eine Lösung, die E-Mails basierend auf benutzerdefinierten Quarantäne- und Blockierungsrichtlinien verwaltet. Ihre Lösung sollte externe ebenso wie interne E-Mails analysieren, da Angreifer möglicherweise kompromittierte Konten missbrauchen, um Anwender in Ihrem Unternehmen zu täuschen.

Schützen Sie Cloud-Konten vor Übernahmen und schädlichen Apps. Angreifer sind äußerst agil und können im Nu ihre Taktik ändern. Daher muss jeder Eintrittspunkt in Ihre Systeme abgedeckt sein.

Arbeiten Sie mit einem Anbieter für Bedrohungsdaten zusammen. Für kleinere, gezielte Angriffe benötigen Sie erweiterte Bedrohungsinformationen. Implementieren Sie eine Lösung, die mithilfe von statischen und dynamischen Techniken Angriffs-Tools, -Taktiken und -Ziele aufdeckt und daraus Erkenntnisse zieht.

Bedrohungsakteure sind besser ausgerüstet, kreativer und stärker motiviert als je zuvor. Um sie stoppen zu können, benötigen Sie einen mehrschichtigen, personenzentrierten Ansatz, der die gesamte Angriffskette abdeckt.

Wenn Sie mehr darüber erfahren möchten, wie Proofpoint Ihre Mitarbeiter vor hochentwickelten E-Mail-Angriffen und identitätsbezogenen Bedrohungen schützen kann, besuchen Sie proofpoint.com.

WEITERE INFORMATIONEN

Möchten Sie mehr darüber erfahren, wie Sie mit Proofpoint Einblicke in Ihre Schwachstellen sowie Ihre Risiken durch Angriffe und Anwenderberechtigungen erhalten und wie sie mit einer personenzentrierten Cybersicherheitsstrategie minimieren können? Dann besuchen Sie **proofpoint.com/de**.

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. ist ein führendes Unternehmen für Cybersicherheit und Compliance. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter 75 Prozent der Fortune-100-Unternehmen, setzen auf die personenzentrierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter **www.proofpoint.de**.

proofpoint.

0400-014-04-01