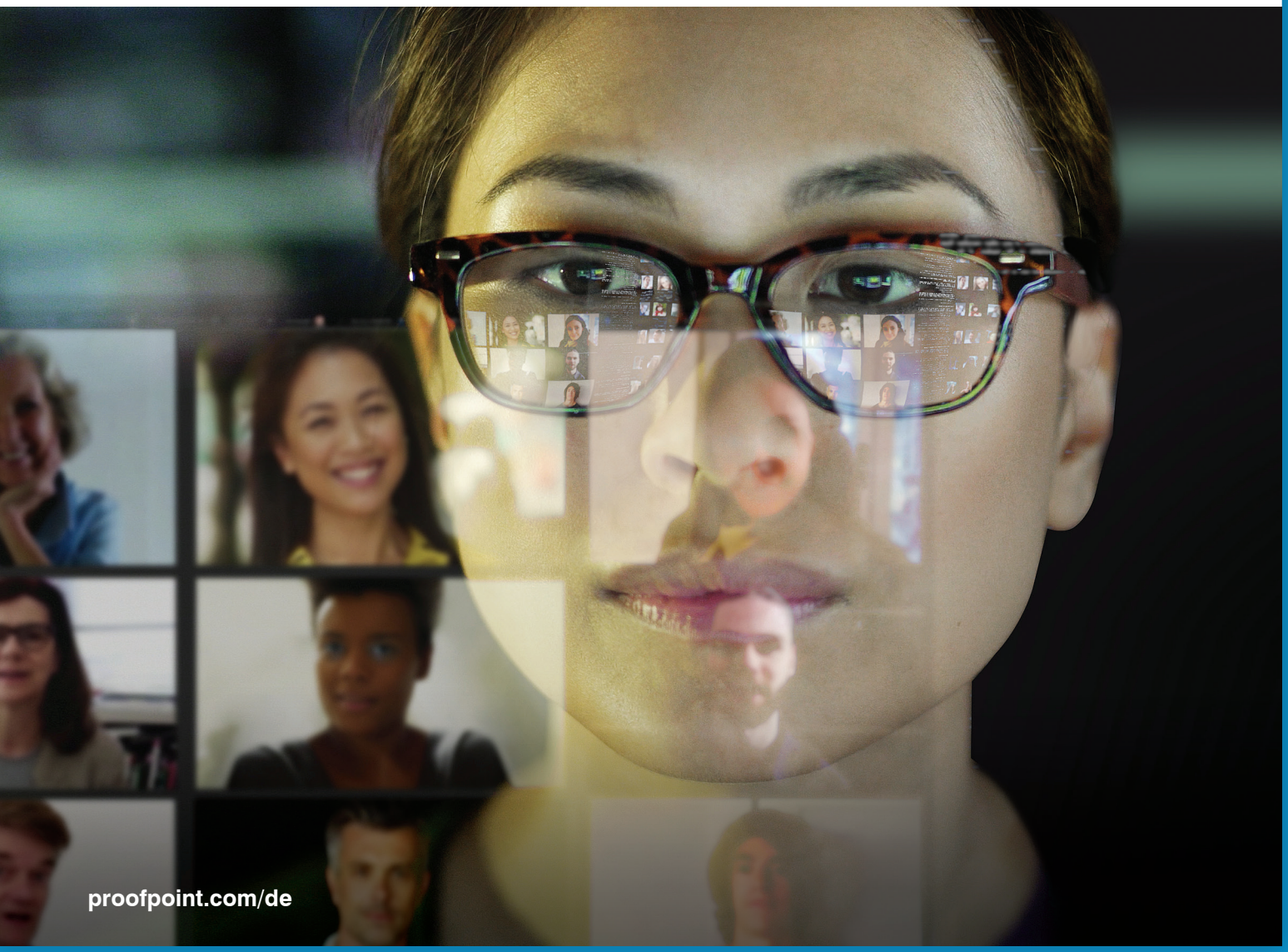
proofpoint.

BERICHT

Der Faktor Mensch 2021

Cybersicherheit, Ransomware und E-Mail-Betrug in einem Jahr, das die Welt veränderte



proofpoint.com/de

Einführung

Die tragischen, umwälzenden und historischen Veränderungen des Jahres 2020 wurden unzählige Male dokumentiert. Doch während Unternehmen auf der ganzen Welt ihre ersten vorsichtigen Schritte in Richtung Normalzustand unternehmen, bietet „das verlorene Jahr“[1] noch immer wertvolle Lektionen – insbesondere im Bereich der Cybersicherheit.

Während die weltweite Pandemie die beruflichen und privaten Abläufe auf den Kopf stellte, sahen die Cyberangreifer ihre Chance gekommen. Sie nutzten die plötzlich ungewohnten Arbeitsumgebungen sowie die Angst, Unsicherheit und Zweifel aus, um Anwender zu täuschen und Unternehmen zu kompromittieren. Und jetzt, im Jahr 2021, beobachten wir, wie Cyberkriminelle ihre Vorteile voll ausnutzen und unzählige Ransomware-Angriffe gegen große Unternehmen und kritische Infrastrukturen richten.

Auch wenn die Menschen wieder in die Büros, Fabriken, Ladengeschäfte und Ausstellungsräume zurückkehren, werden einige Trends aus der Zeit der Pandemie wahrscheinlich bleiben. Viele Arbeitnehmer werden einen Hybrid-Ansatz wählen und ihre Arbeitszeit zwischen Home Office und dem Arbeitgeber aufteilen. Verteilte Teams werden regions- und länderübergreifend arbeiten. Der Wechsel beim E-Commerce, der Cloud und weiteren Bereichen, der bereits vor der Pandemie im Gange war, hat sich weiter beschleunigt.

Ganz gleich, wie die Welt nach dem Ende der COVID-Pandemie aussehen wird, bleibt der Schutz der Menschen, ihrer Arbeitsplätze und ihrer Arbeitsweise eine ständige Herausforderung.

Informationen zu diesem Bericht

Seit der ersten Ausgabe im Jahr 2014 basiert der Bericht „Der Faktor Mensch“ auf dem einfachen Prinzip, dass Menschen – und nicht Technologien – die kritischste Variable bei aktuellen Cyberbedrohungen sind.

Seit damals ist der scheinbare Widerspruch zu einem weithin anerkannten Fakt geworden. Cyberangreifer nehmen gezielt Menschen ins Visier und nutzen deren Schwächen aus. Letztlich sind Menschen *einfach menschlich*.

Um aktuelle Bedrohungen und Compliance-Risiken effektiv zu verhindern, zu erkennen und darauf zu reagieren, müssen IT-Sicherheitsexperten die personenbezogenen Dimensionen der Anwenderrisiken kennen: Schwachstellen, Angriffe und Berechtigungen. Praktisch betrachtet werden Antworten auf diese Fragen benötigt:

- Wo liegen die größten Schwachstellen der Anwender?
- Wie nutzen Angreifer das aus?
- Wie groß ist die potenzielle Gefahr für Daten, wenn privilegierter Zugriff auf Daten, Systeme und andere Ressourcen kompromittiert wird?

Der richtige Umgang mit diesen Fragen, die die *menschlichen Faktoren* der Cybersicherheit beschreiben, steht im Mittelpunkt einer modernen Verteidigung.

Inhalt dieses Berichts

Dieser Bericht stellt die drei Facetten von Anwenderrisiken im Detail vor. Hier erfahren Sie, wie die außergewöhnlichen Ereignisse des Jahres 2020 sowie der dadurch ausgelöste historische Wandel die Bedrohungslandschaft fundamental verändert haben. Der Bericht untersucht die Veränderungen des Bedrohungsökosystems und die Bedeutung für uns alle. Außerdem erfahren Sie, wie personenzentrierter Schutz die Anwender widerstandsfähiger macht, Angriffe abwehrt und Berechtigungen verwaltet.

Dieser Bericht stellt die Bedrohungen vor, die im Jahr 2020 bei Proofpoint-Bereitstellungen 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 gehören, oder auf eine Serie von Aktionen, 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. Wie jedoch im Kapitel **„Die Kunst und Wissenschaft der Attribution“ auf Seite 27** ausgeführt wird, ist das nicht immer möglich.

Umfang

Die Daten in diesem Bericht stammen aus dem Proofpoint Nexus-Bedrohungsdiagramm und wurden aus Proofpoint-Bereitstellungen auf der ganzen Welt erhoben. Wir analysieren täglich mehr als 2,2 Milliarden E-Mails, 35 Milliarden URLs, 200 Millionen Anhänge, 35 Millionen Cloud-Konten und mehr – insgesamt Billionen Datenpunkte aus allen wichtigen digitalen Kanälen.

Dieser Bericht deckt den Zeitraum vom 1. Januar bis 31. Dezember 2020 ab. Sofern nicht anders angegeben, wurden die aufgeführten Bedrohungen direkt von unserem weltweiten Bedrohungsforscher-Netzwerk beobachtet und mit einer Angriffskampagne in Verbindung gebracht. Als Angriffskampagne definieren wir eine Reihe von Aktionen, mit denen Angreifer ein bestimmtes Ziel erreichen wollen.

Für Abschnitt 3 zu Berechtigungen berichteten 300 Kunden über ihre Insider Threat Management-Warnungen, was die Formen von Berechtigungsmissbrauch verdeutlicht, die ihnen die meisten Sorgen bereiten. Wir verglichen die Warnungen von Februar 2020 bis Januar 2021 (auf der Höhe der Pandemie) mit denen von Oktober 2019 bis Januar 2020.

[1] *The Economist*: „2020: The year that wasn’t“ (Das verlorene Jahr), November 2020.

Inhaltsverzeichnis

Die wichtigsten Erkenntnisse

Dies sind einige der wichtigsten Erkenntnisse des diesjährigen Berichts.

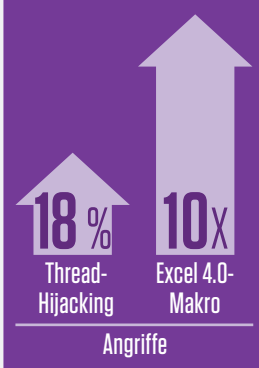
Mehr als **48 Mio. Nachrichten enthielten Malware,** die **als Einstiegspunkt für Ransomware-Angriffe dienen konnte**.

Während die Welt mit COVID-19 beschäftigt war, nutzten Angreifer die Situation nach Kräften aus. **Pandemiebezogene Köder waren häufiger als solche mit Bezug zu anderen aktuellen Ereignissen oder Nachrichten.** Fast jeder überwachte Bedrohungsakteur nutzte im Jahr 2020 mindestens einmal pandemiebezogene Inhalte.

Fast **10 % aller schädlichen Kampagnen-E-Mails** versuchten, Emotet-Malware zu verteilen. Vor ihrer Stilllegung im Januar 2021 im Zuge einer konzertierten Strafverfolgungsaktion wurde die Emotet-Infrastruktur anderen Gruppen zur Miete überlassen. Diese kriminellen Akteure nutzten sie zur Verteilung von Ransomware und anderen Malware-Typen.

Fast **25 % aller Angriffskampagnen** versteckten Malware in komprimierten ausführbaren Dateien, die nur durch die Interaktion des Empfängers ausgeführt werden.

Anmeldedaten-Phishing gegen Verbraucher und Unternehmen war der häufigste Angriffstyp und machte fast zwei Drittel aller schädlichen Nachrichten aus – mehr als alle anderen Angriffe zusammen. Anmeldedaten-Phishing ermöglicht die Kompromittierung von Konten, die für weitere Angriffe genutzt werden können, z. B. Datendiebstahl und BEC (Business Email Compromise).



Techniken, die vom Empfänger eine Interaktion mit einem Anhang oder direkt mit dem Angriff erfordern, haben erheblich zugenommen. **Thread-Hijacking-Angriffe haben im Vergleich zum Vorjahr um 18 % zugenommen.** Angriffe mit kennwortgeschützten Dateien erfolgten fast fünf Mal häufiger. Das Aufkommen an **Excel 4.0-Makroangriffen ist um mehr als das Zehnfache gestiegen.**

Mehr als ein Drittel der Menschen, die mit Angriffskampagnen mit Steganografie attackiert wurden, haben auf die schädliche E-Mail geklickt – die höchste Trefferquote unter allen Angriffstechniken.

>50X Angriffe, die auf CAPTCHA-Techniken setzen, erzielten **mehr als 50 Mal so viele Klicks** wie im Jahr zuvor.

Die Angriffskampagnen des Bedrohungsakteurs TA542 (der mit dem Emotet-Botnet in Verbindung gebracht wird) verleiteten **die meisten Anwender zum Klicken**. Die Zahlen verdeutlichen die Effektivität dieser Angreifer sowie das enorme E-Mail-Volumen der jeweiligen Kampagnen.

Da die Anwender plötzlich zu Hause eingesperrt sind und das Arbeiten im Home Office zum Normalzustand geworden ist, **hat sich bei Unternehmen die Wahrnehmung berechtigungsbasierter Risiken verändert**. **Die Zahl der Unternehmen, die DLP-Warnungen für die folgenden Aktivitäten festlegen, stieg erheblich** im Vergleich zur Zeit vor der Pandemie:

- Nutzung von USB-Geräten
- Kopieren großer Dateien und Ordner (insbesondere zu ungewöhnlichen Zeiten)
- Analyse von Dateifreigabediensten
- Mögliche Aktivitäten zur Umgehung von Tools zur Anwenderüberwachung

TOP 5 der Kontrollen für DLP und Insider-Bedrohungen, die von Kunden festgelegt wurden:

1. Verbinden mit unzulässigem USB-Gerät
2. Kopieren von Ordnern oder großen Dateien
3. Hochladen vertraulicher Dateien ins Web
4. Öffnen einer Textdatei, die Kennwörter enthalten könnte
5. Herunterladen einer Datei mit potenziell schädlichen Erweiterungen

Aufbau dieses Berichts

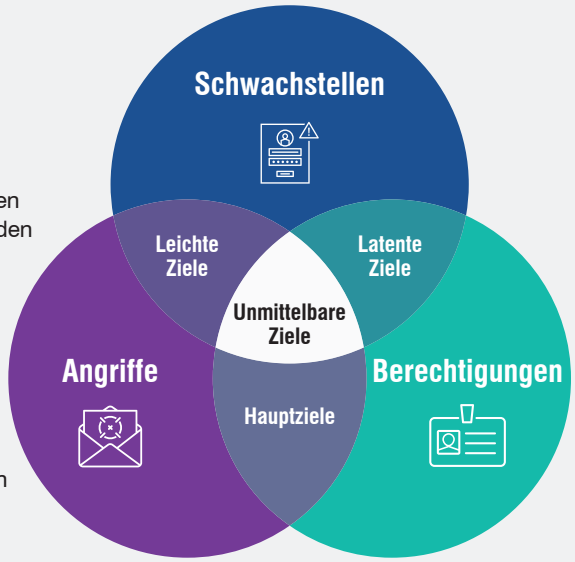
In der Cybersicherheit werden Risiken definiert als: *Bedrohungen* x *Schwachstellen* x *Folgen* +/- *Sicherheitskontrollen*

Dieser Bericht beleuchtet jede dieser Facetten im Hinblick auf unser personenzentriertes Anwenderrisiko-Modell – Schwachstellen, Angriffe (Bedrohungen) und Berechtigungen (Folgen) – und gibt Empfehlungen dazu, wie die jeweiligen Probleme behoben werden können.

Ebenso wie jeder Mensch einzigartig ist, sind auch sein Wert für die Cyberangreifer und das Risiko für den Arbeitgeber individuell.

Menschen haben ihre ganz eigenen digitalen Gewohnheiten und **Schwachstellen**. Sie werden mit unterschiedlichen Mitteln und wechselnder Intensität **angegriffen** und verfügen jeweils über ganz eigene **Zugriffsberechtigungen** für Daten, Systeme und Ressourcen.

Diese miteinander verknüpften Faktoren bestimmen das individuelle Gesamtrisiko eines Anwenders.



Schwachstellen

Die erste Schwachstelle der Anwender ist ihr digitales Verhalten – wie sie arbeiten und worauf sie klicken.

Viele Mitarbeiter arbeiten vielleicht im Home Office oder haben über ihre privaten Geräte Zugriff auf geschäftliche E-Mails. Oder sie nutzen Cloud-basierte Dateispeicher und installieren Drittanbieter-Add-Ons für ihre Cloud-Anwendungen. Und einige von ihnen sind besonders empfänglich für die E-Mail-Phishing-Taktiken der Angreifer.

Angriffe

Nicht alle Cyberangriffe sind gleich. Auch wenn jeder einzelne Angriff potenziell gefährlich ist, sind einige schädlicher, gezielter oder raffinierter als andere.

„Standard"-Bedrohungen, die in großer Masse versendet werden, mögen häufiger sein als raffiniertere Bedrohungstypen, sie sind jedoch bekannt und können leichter blockiert werden. (Das sollte jedoch kein Grund sein, sie zu unterschätzen, da sie ebenso großen Schaden anrichten können.)

Andere Bedrohungen kommen vielleicht nur bei einigen wenigen Angriffen zum Einsatz, können jedoch eine größere Gefahr darstellen, da sie raffinierter sind oder extrem zielgerichtet hinsichtlich der adressierten Personen sind.

Berechtigungen

Bei den Berechtigungen werden alle potenziell hochwertigen Assets erfasst, auf die Menschen Zugriff haben (z. B. Daten, finanzielle Befugnisse, wichtige Kontakte). Die Ermittlung dieses Risikoaspekts ist unverzichtbar, da er den potenziellen Gewinn für Angreifer repräsentiert – und das Unternehmen bei einer Kompromittierung schädigt.

Die Position des Anwenders im Organigramm ist natürlich ein wichtiger Faktor bei der Bewertung der Berechtigungen. Sie ist jedoch nicht der einzige Faktor – und häufig noch nicht einmal der wichtigste. Für die Angreifer kann jeder ein lohnenswertes Ziel darstellen, der ihnen nützlich ist.

Aufeinandertreffen von Risikofaktoren

Erhöhte Risiken in jeder dieser drei Kategorien sind ein Grund zur Sorge und in den meisten Fällen auch für zusätzliche Sicherheitsmaßnahmen. Zwei oder mehr erhöhte Risikostufen sind ein Hinweis auf ein dringendes Sicherheitsproblem.

Diese vier Anwenderkategorien zeigen, welchen Einfluss Kombinationen aus Schwachstellen, Angriffen und Berechtigungen auf Ihr Gesamtrisiko haben:

- **Latente Ziele:** Anwender mit umfangreichen Berechtigungen, die gleichzeitig anfälliger für Phishing-Köder sind, warten förmlich auf eine Kompromittierung. Diese Anwender haben nicht immer Spitzenpositionen im Unternehmen. Selbst die Zugriffsrechte untergeordneter Mitarbeiter in der Personalabteilung, dem Gebäudemanagement und der Verwaltung können sich in den falschen Händen als gefährlich erweisen. Selbst wenn sie derzeit noch nicht auf dem Radar der Angreifer sind, handelt es sich um leichte Ziele.
- **Leichte Ziele:** Mit häufig angegriffenen Anwendern, die sich als anfällig für Bedrohungen erweisen, haben Angreifer leichtes Spiel. Eine schnelle Reaktion und Eindämmung kann den Schaden bei Anwendern mit geringen Berechtigungen in Grenzen halten. Mit einem erfolgreichen Angriff kann ein Bedrohungsakteur jedoch einen Brückenkopf etablieren, um an Anwender zu gelangen, die Berechtigungen für wertvollere Daten, Systeme und Ressourcen besitzen.
- **Hauptziele:** Das Risiko durch gezielt angegriffene Anwender mit umfangreichen Berechtigungen kann mit Security Awareness-Schulungen und empfohlenen digitalen Vorgehensweisen minimiert werden. Menschen in dieser Kategorie erleben zahlreiche Angriffe – von denen nur einer erfolgreich sein muss, um dem Unternehmen schwerwiegenden Schaden zuzufügen.
- **Unmittelbare Ziele:** Anwender mit einer hohen Gefährdung in allen drei Risikofaktoren sind unmittelbare und kritische Schwachstellen. Daher sollten sie mit größter Priorität behandelt werden.

ABSCHNITT 1

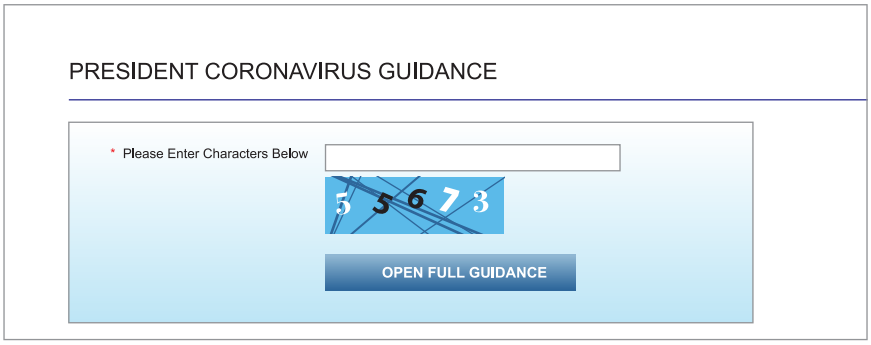
Schwachstellen

Eine andere Betrachtungsweise von Schwachstellen ist die Frage: „Wenn meine Anwender in einem Cyberangriff attackiert werden, wie groß ist die Wahrscheinlichkeit, dass er erfolgreich ist?“

Einige der erfolgreichsten Angriffstechniken des Jahres 2020 waren äußerst gezielt und wurden in Kampagnen eingesetzt, die manchmal nur eine Handvoll E-Mails umfassten.

STEGANOGRAFIE, also das Verbergen von schädlichem Code in Bildern und anderen Dateitypen, kam nur in einigen gezielten Kampagnen zum Einsatz. Doch die Technik erwies sich als äußerst effektiv und verleitete drei von acht Empfängern zum Klicken.* Von einer solchen Antwortrate können die meisten Angreifer – ganz zu schweigen von E-Mail-Marketern – nur träumen.

CAPTCHA-Techniken, die visuelle Puzzles zur Unterscheidung von Menschen und Maschinen nutzen, erreichten im Vergleich zum Vorjahreszeitraum mehr als 50 Mal so viele Klicks. Während die Gesamtantwortrate nur bei bescheidenen 5 % lag – was bei den meisten E-Mail-Marketing-Kampagnen immer noch ein enormer Erfolg wäre –, fielen erheblich mehr Anwender auf diese Technik herein als 2019.



Screenshot einer CAPTCHA-Abfrage bei einem COVID-bezogenen Angriff im Mai.

Es ist unklar, warum mehr Anwender auf diese beiden Techniken hereinfielen. Möglicherweise sind Mitarbeiter im Home Office aufgrund der Belastungen des Jahrs 2020 stärker abgelenkt und überlastet. Es ist aber auch möglich, dass einige durch die neuen Remote-Kontrollen darauf eingestellt waren, die CAPTCHA-Frage als normale Sicherheitsfrage zu betrachten.

STEGANOGRAFIE

Angreifer nutzen diese Technik zum Verbergen ihrer Schaddaten in scheinbar harmlosen Dateien wie Fotos und Audioclips. Üblicherweise sind die Schaddaten in sonst ungenutzten Datenblöcken kodiert, die Anwender nicht zu sehen bekommen und die sich mit Datei- und Sandbox-basierten Tools nur schwer erkennen lassen. Nachdem die verborgenen Daten auf die Computer der Opfer gelangt sind, werden sie dekodiert und aktiviert.

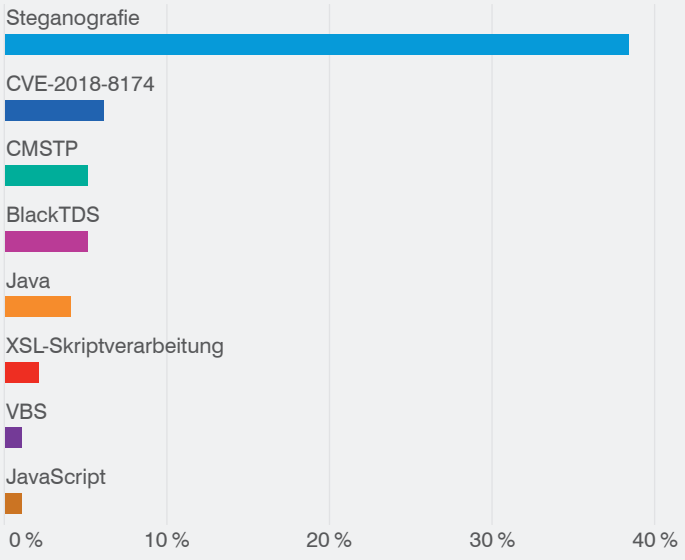
CAPTCHA

Meist werden CAPTCHA-Techniken als Maßnahme zur Betrugsabwehr eingesetzt. Dabei sollen Anwender eine Aufgabe ausführen, die für Menschen leicht und für Computer schwierig ist. Auf diese Weise wird sichergestellt, dass tatsächlich eine Person und nicht ein automatisierter Bot auf die Website zugreift. Cyberangreifer nutzen diese Technik auf ähnliche, aber böswillige Weise. Mit einer CAPTCHA-Abfrage stellen sie sicher, dass ihre Malware auf dem System eines echten Anwenders ausgeführt wird – und nicht in einer Sicherheits-Sandbox, die ihre schädlichen Aktivitäten beobachten kann. Mithilfe dieser Technik lässt sich auch feststellen, in welchem Land der Anwender lebt (anhand der IP-Adresse), um Angriffe auf Menschen in bestimmten Ländern oder Regionen durchzuführen.

* Bei Kampagnen, die einem Akteur zugeordnet werden konnten.

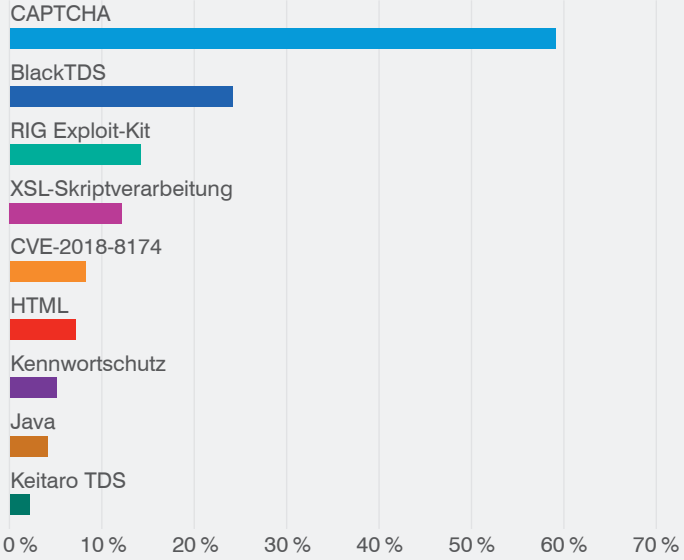
Techniken mit den meisten Klicks pro Nachricht*

Steganografie erwies sich in den wenigen gezielten Kampagnen, die diese Technik nutzen, als hocheffektiv. Angriffe, die die Windows-Schwachstelle CVE-2018-8174 ausnutzten, waren ebenfalls effektiv und wurden in größeren und häufigeren Kampagnen genutzt.



Veränderung im Jahresvergleich (Anzahl der durchschnittlichen Klicks, 2020 und 2019 im Vergleich)*

CAPTCHA-Techniken, die Sicherheitstools unterlaufen, indem sie menschliche Interaktionen erfordern, generierten im Jahr 2020 mehr als 50 Mal so viele Klicks wie im Vorjahr. Sie kamen in mehreren großen Kampagnen zum Einsatz.



TA542

Vor der Stilllegung im Januar 2021 war TA542 aufgrund umfangreicher Kampagnen mit der Malware-Familie Emotet zu einem der aktivsten Bedrohungsakteure geworden. Die Gruppe attackierte mehrere Branchen weltweit und verschickte dabei täglich Hunderttausende oder sogar Millionen von Nachrichten.

Emotet kompromittiert infizierte Systeme nicht nur, sondern startet von dort aus neue Angriffe. Zudem integriert die Malware die Systeme in ein zombieartiges Netzwerk aus mehr als einer Million gleichermaßen infizierten Rechnern, bekannt als Botnet. Andere Cyberkriminelle nutzten die Botnet-Infrastruktur von TA542 für verschiedenste Angriffe.

TA576

Dieser Bedrohungsakteur beschränkt sich meist auf steuerbezogene Angriffe. Er startete im Jahr 2020 nur zwei Angriffe – beide jedoch mit einem enormen Umfang.

TA407

Dieser auch als Silent Librarian, Cobalt Dickens und Mabna Institute bezeichnete Bedrohungsakteur agiert aus dem Iran. Er hat Universitäten in Nordamerika und Europa angegriffen, um an geistiges Eigentum zu gelangen. Im Jahr 2018 beschuldigten US-Behörden neun mutmaßliche Mitglieder der Gruppe des Diebstahls von Daten im Wert von 3,4 Milliarden US-Dollar.

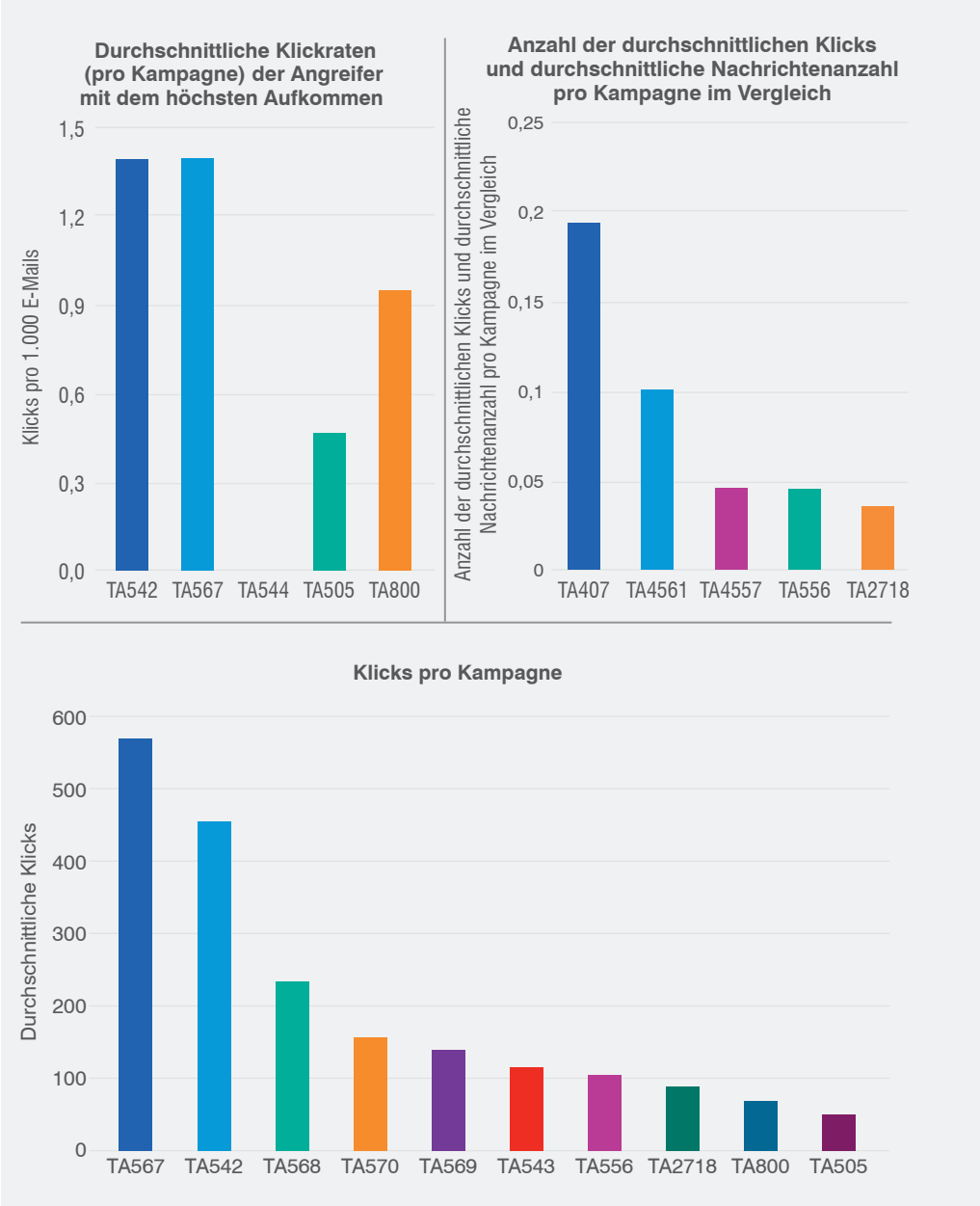
In jedem Fall verloren die Bedrohungsakteure keine Zeit, anfällige User anzugreifen.

Ein Angreifer, den wir als **TA542** bezeichnen und der 2020 für das höchste Angriffsaufkommen verantwortlich war, erzielte 454 Klicks pro Angriffskampagne und damit eine Trefferquote von etwa 0,1 %. Was ihr an Effektivität fehlte, machte sie durch schieres Volumen wett. (Mehr zu diesem berüchtigten Bedrohungsakteur in **Abschnitt 2: Angriffe**.) **TA576**, ein weiterer Akteur mit hohem Angriffsvolumen, erreichte mit 568 Klicks pro Kampagne eine ähnliche Trefferquote.

Einige der „effektivsten“ Angreifer, die höchste Trefferquoten erreichen, gehörten zu denen mit dem geringsten Nachrichtenaufkommen.

Beispielsweise erreichte der Angreifer **TA407** im Jahr 2020 einen Klick pro fünf E-Mails, was eine der größten Erfolgsquoten unter den von uns beobachteten Bedrohungsakteuren ist. Der Bedrohungsakteur ging äußerst selektiv vor und versendete 2020 in weniger als 100 Kampagnen nur jeweils einige Dutzend E-Mails.

Die Gruppe ist für ihre raffinierten Social-Engineering-Techniken bekannt. Beispielsweise nutzen die E-Mail-Kampagnen den Markenauftritt von Universitäten, professionelle Websites und normale Schulaktivitäten (z. B. Bibliotheksverlängerungen), um die Opfer zur Eingabe von Kontodaten zu verleiten.



Anwender auf der Probe: Fehlerquoten bei Phishing-Simulationen

Eine weitere Möglichkeit zur Ermittlung der Anfälligkeit sind simulierte Phishing-Angriffe. Diese Testübungen können zeigen, auf welche Köder und Taktiken die Empfänger unter realen Bedingungen am wahrscheinlichsten hereinfallen werden.

Unser jährlicher **„State of the Phish"-Bericht** analysierte, wie Anwender innerhalb der 12 Monate des Jahres 2020 auf mehr als 60 Millionen simulierte Phishing-E-Mails reagierten. Durch den Vergleich der durchschnittlichen Fehlerquoten – also des Anteils der Anwender, die auf einen Köder hereingefallen sind – erfahren Sie, wie und wo Anwender am anfälligsten sein können.

Die wichtigsten Erkenntnisse:

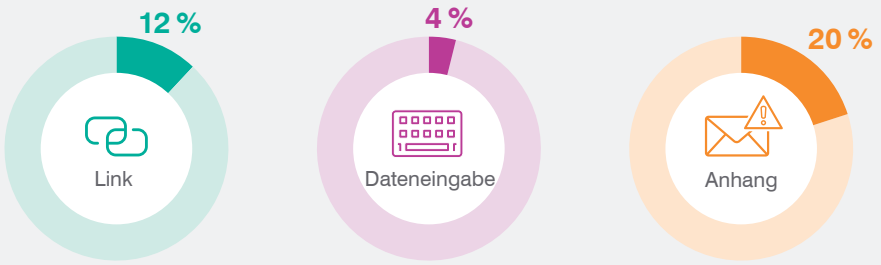
Fehlerquoten nach Vorlagenart

Jede „Phishing"-E-Mail basiert auf einer Vorlage, mit der Unternehmen eine Vielzahl von Angriffstypen, -themen und -ködern imitieren können. Auch wenn die Vorlagen ebenso vielfältig wie reale Bedrohungen sind, fallen sie in drei grundlegende Kategorien:

- Link (enthalten eine gefährliche URL, die zu Malware und schädlichen Websites führt)
- Dateneingabe (führen die Anwender zu einer gefälschten Anmeldeseite, die Anmeldedaten und andere personenbezogene Daten stehlen soll)
- Anhang (enthalten eine schädliche Datei)

Im Durchschnitt[2] klickte ein Fünftel der Anwender auf E-Mails mit Anhang. Das ist der höchste Wert unter den drei Vorlagentypen und zudem höher als bei den anderen beiden Typen zusammen.

Phishing-Vorlagen-Typen: Durchschnittliche Fehlerquoten



2 Um größere Unternehmen weniger stark zu gewichten, haben wir die Werte nach Kunden statt nach einzelnen Anwendern gemittelt.

Fehlerquoten nach Branche

Anfälligste Branchen

Die Fehlerquoten in simulierten Phishing-Angriffen deuten auch darauf hin, dass Anwender in einigen Branchen überdurchschnittlich anfällig sind.

Beispielsweise fielen Anwender in Unternehmen aus dem Entwicklungsbereich, der Telekommunikation, Bergbau und dem Bildungssektor eher auf einen Köder herein. Am anderen Ende des Spektrums standen Empfänger aus den Branchen Gastgewerbe/Freizeit und Unterhaltung/Medien, die am seltensten klickten.

(Hinweis: Jede in dieser Tabelle aufgeführte Branche umfasst Daten von mindestens 15 Unternehmen sowie mindestens 150.000 simulierten Phishing-Angriffen.)

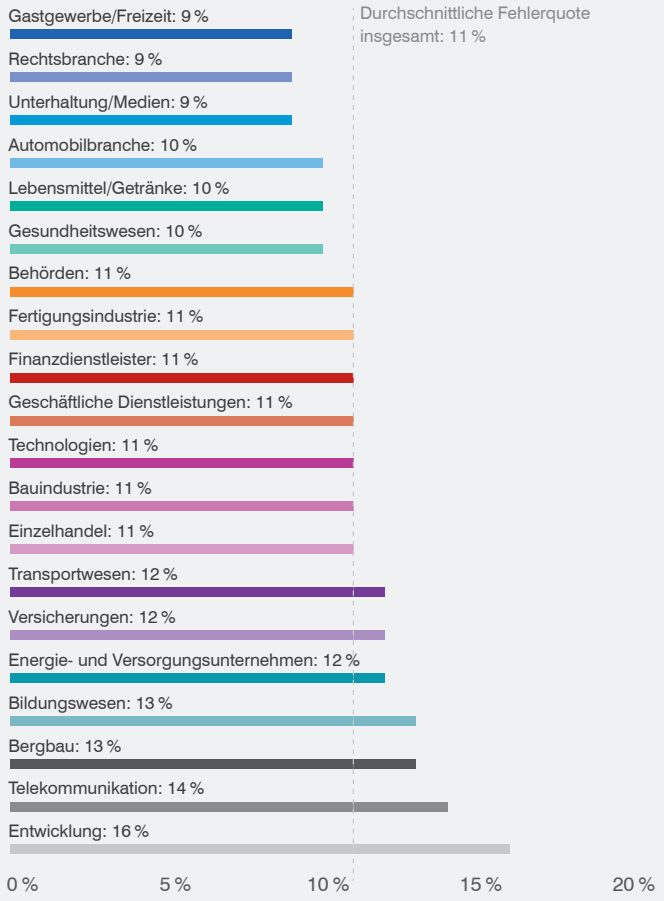
Anfälligste Branchen

Die branchenspezifischen Fehlerquoten allein zeigen nicht, bei welchen Rollen und Teams möglicherweise Probleme auftreten. Angreifer nehmen häufig konkrete Posteingänge und E-Mail-Aliase ins Visier. Fehlerquoten auf Abteilungsebene bieten einen detaillierten Überblick über potenzielle Schwachstellen im Unternehmen.

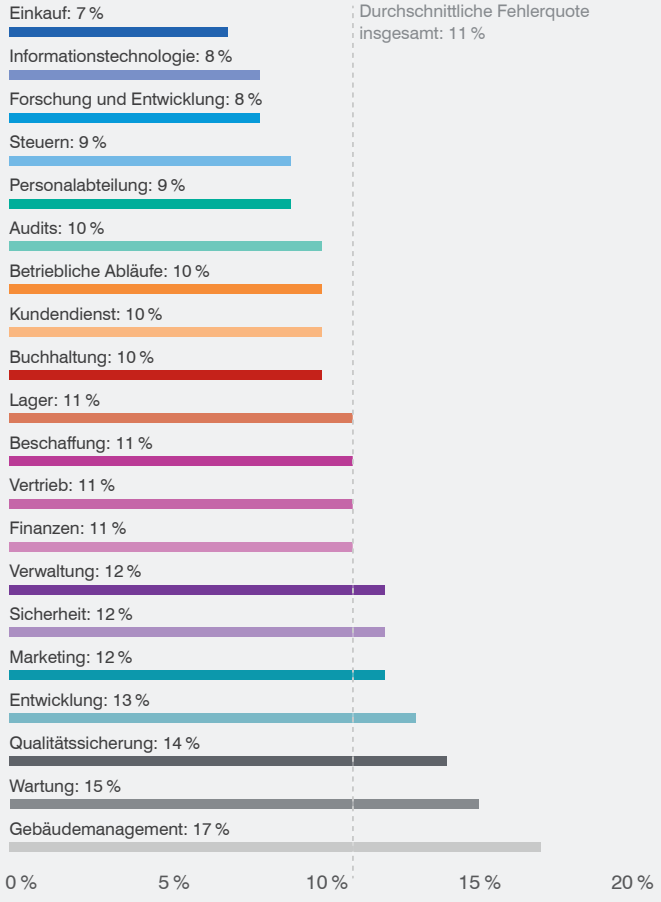
Die Abteilungen für Einkauf, IT, Forschung und Entwicklung, Steuern, Personal und Audits fielen am seltensten auf simulierte Phishing-E-Mails herein. Im Gegensatz dazu wurde in den Abteilungen Gebäudemanagement, Wartung, Qualitätskontrolle und Technik am häufigsten geklickt.

(Hinweis: Jede in dieser Tabelle aufgeführte Branche umfasst Daten von mindestens 15 Unternehmen sowie mindestens 150.000 simulierten Phishing-Angriffen.)

Durchschnittliche Fehlerquote nach Branche



Durchschnittliche Fehlerquote nach Abteilung



ABSCHNITT 2

Angriffe

Zahl von Ransomware-Angriffen steigt

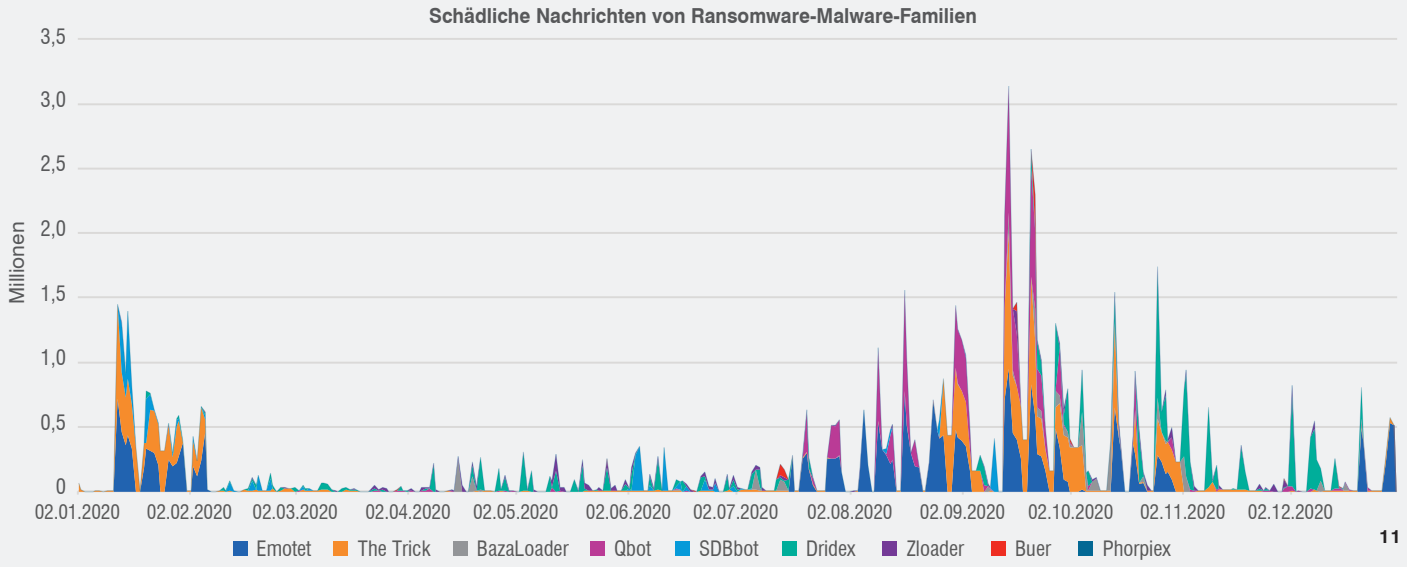
RANSOMWARE
Diese Malware-Form sperrt die Daten der Opfer per Verschlüsselung und fordert ein Lösegeld (englisch „ransom“) für den Entschlüsselungsschlüssel.

Laut den Zahlen der US-Regierung[3] stieg die Zahl der **RANSOMWARE**-Angriffe im letzten Jahr um 300 %. Im ersten Halbjahr 2021 erlangte das Problem mit den Angriffen auf Colonial Pipeline, JBS Foods und die IT des irischen Gesundheitssystems (Health Service Executive, HSE) noch größere Aufmerksamkeit. Dies zeigte, dass Ransomware-Gruppen kritische Infrastrukturen auf der ganzen Welt schädigen können.

Ransomware-Angreifer setzen weiterhin auf E-Mails, doch seit dem ersten Auftauchen von Locky in Millionen Postfächern im Jahr 2016 hat sich viel geändert. So gelangt Ransomware nicht mehr als primärer Payload per E-Mail-Kampagnen auf die Systeme, sondern wird häufiger durch bereits vorhandene Malware heruntergeladen und über kompromittierte RDP (Remote Desktop Protocol)- oder VPN (virtuelles privates Netzwerk)-Zugriffe übertragen. E-Mails spielen jedoch weiterhin eine zentrale Rolle, da die Malware in der ersten Angriffsphase auf diese Weise auf die Systeme gelangt und die Voraussetzung für die Verbreitung der Ransomware schafft.

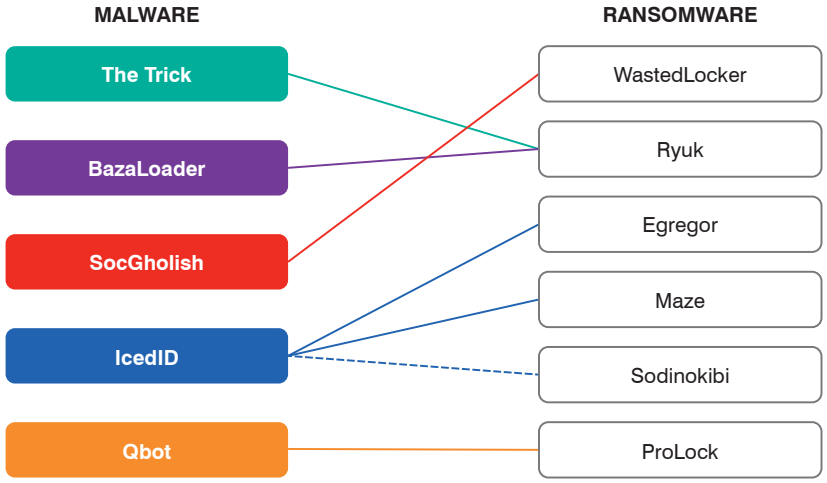
Die Cyberkriminellen, die für diese Loader und Trojaner verantwortlich sind, fungieren anschließend als Access Broker oder Berater und gewähren Ransomware-Gruppen gegen Gewinnbeteiligung Backdoor-Zugriff auf infizierte Systeme. Statt auf große Verbreitung und kleine Lösegeldsummen setzen die Ransomware-Angreifer jetzt häufig auf „Big Game Hunting“, d. h. auf große Unternehmen, die mehr zu verlieren haben und eher zu Zahlungen bereit sind.

3 James Rundle und David Uberti (*Wall Street Journal*): „How Can Companies Cope with Ransomware?“ (Wie können Unternehmen Ransomware abwehren?), Mai 2021.



Durch diese Strategieänderung beobachten wir in unserem E-Mail-Gateway nur wenig Ransomware. Gleichzeitig machte allein die Variante mit dem Namen Avaddon im Jahr 2020 ganze 95 % aller Erstphase-Ransomware-Paylaods aus. Dennoch wurden mehrere gängige Erstphase-Payloads beobachtet (z. B. The Trick, Dridex und Qbot), die als Einstiegspunkte für spätere Ransomware-Infektionen dienten. Laut unseren Daten gehörten diese drei Varianten zu den Bedrohungen mit dem höchsten Volumen. Insgesamt beobachteten wir im Jahr 2020 mehr als 48 Millionen Nachrichten mit Malware, die den späteren Download von Ransomware oder anderen sekundären Schaddaten ermöglicht.

Es gibt keine einfache direkte Beziehung zwischen der Erstzugriffs-Malware und der letztendlich eingesetzten Ransomware. Doch unsere Beobachtungen und die anderer Forscher[4] legen einige häufige Verbindungen nahe.



Beispiele für Erstzugriffs-Schaddaten, die von Bedrohungsakteuren übertragen wurden, und die nach dem Erstzugriff verbreitete Ransomware.

Während das Netzwerk der Beziehungen zwischen kriminellen Syndikaten komplex ist, ist die Reihenfolge der Ereignisse bei einem typischen, per E-Mail ausgelösten Ransomware-Angriff sehr geradlinig: Nach der Erstinfektion durch einen Bank-Trojaner oder Loader sind Sie für Ransomware-Gruppen anfällig, die es auf lukrative Ziele abgesehen haben. Für die meisten Unternehmen besteht also der beste Schutz vor Ransomware in der Vermeidung der Erstinfektionen.

Mit anderen Worten: Wenn Sie die Loader blockieren, blockieren Sie die Ransomware.

4 Clifford Krauss (*The New York Times*): „How the Colonial Pipeline Became a Vital Artery for Fuel“ (So wurde Colonial Pipeline zur Treibstoff-Lebensader), Mai 2021.

Obwohl die Bedrohungsakteure wahlbezogene Themen als Köder erst einsetzten, als die Wahl im Herbst 2020 bereits im vollem Gange war, griffen sie dennoch das gesamte Jahr über Organisationen an, die mit der Wahl in Verbindung standen.

„Battleground States“: Angriffe während der US-Wahlen

Die meisten Sicherheitsforscher gingen davon aus, dass Cyberangreifer die US-Wahl im Jahr 2020 für ihre Zwecke nutzen würden. So könnten einige von ihnen Falschinformationen verbreiten, während andere das Thema als Social-Engineering-Köder in E-Mail-Bedrohungen einsetzen würden.

Und genau das ist auch passiert. Obwohl die Bedrohungsakteure wahlbezogene Themen als Köder erst einsetzten, als die Wahl im Herbst 2020 bereits im vollem Gange war, griffen sie dennoch das gesamte Jahr über Organisationen an, die mit der Wahl in Verbindung standen.

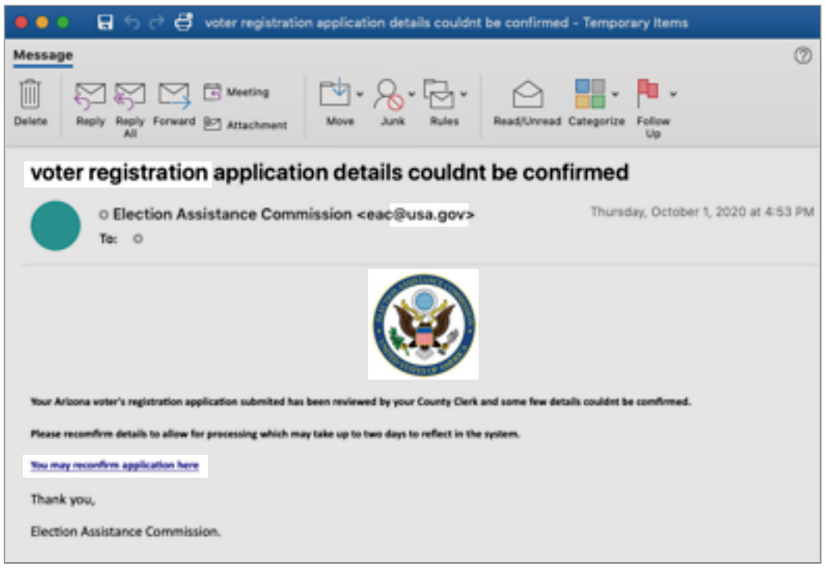
Finanziell motivierte Cyberkriminelle und staatlich unterstützte Bedrohungsakteure nahmen Organisationen ins Visier, die sowohl direkt als auch indirekt mit der Wahl in Verbindung standen. Davon betroffen waren alle Regierungs- und Politikebenen: von lokalen, bundesstaatlichen und staatlichen Einrichtungen bis hin zu sogenannten „Political Action Committees“ (PACs, Lobbygruppen für politische Kandidaten).

Zahlreiche Branchen wurden mit politischen und wahlbezogenen Köderthemen in den USA angegriffen. Die Zahl der Attacken mit US-Wahlthemen erreichte im Oktober 2020 ihren Höchstwert und ging nach der Wahl am 3. November wieder stark zurück. Folgende Themen fanden dabei Verwendung:

- Der Gesundheitszustand des damaligen Präsidenten Donald Trump
- Die Organisation der US-Demokraten „Democratic National Committee“ (DNC)
- Die US-Behörde „Election Assistance Commission“
- Wählerregistrierung

WICHTIGE MERKMALE:

- Nutzung von Themen, die oft starke Emotionen auslösen
- Nachahmung der E-Mail-Domäne der US-Behörde Election Assistance Commission
- Siegel des US-Präsidenten soll offiziellen Charakter verstärken
- Enthält schädliche, als Registrierungs-Webseite getarnte URL



E-Mail-Köder, der die US-Behörde Election Assistance Commission nachahmt.

THREAD-HIJACKING
Nachdem ein E-Mail-Konto übernommen wurde, hat ein Angreifer vollen Zugriff auf den Posteingang des Opfers und kann auf frühere und laufende E-Mail-Threads mit einer schädlichen E-Mail antworten. Da die Empfänger den Absender kennen und ihm vertrauen – und dazu noch in aktivem Kontakt zu der Person standen – kann diese Technik sehr wirkungsvoll sein.

Einige Malware-Familien können für Social Engineering nun im großen Maßstab Thread-Hijacking automatisieren.

EMOTET
Vor der Abschaltung der Infrastruktur im Jahr 2021 war Emotet die weltweit am häufigsten verteilte Malware. Die Gruppe war eine der ersten, die sich vom Diebstahl von Bank-Anmeldedaten abwendeten und auf die Tätigkeit als Access Broker für andere kriminelle Elemente umschwenkten, darunter auch Angreifer, die Dridex und Qbot verteilen.

URSNIF
Ursnif ist ein verbreiteter Bank-Trojaner, der sich aus einer Malware-Familie namens Gozi entwickelte, deren Quellcode 2015 geleakt wurde. Ursnif ist die beliebteste mehrerer aus Gozi entstandenen Varianten, zu denen beispielsweise Dreambot, ISFB und Papras gehören.

So werden E-Mail-Threads missbraucht

In einer Kampagne wurden Beamte ins Visier genommen, die für die Durchführung der Wahlen und die Planung der Wahl-Infrastruktur verantwortlich waren. Dabei nutzten die Angreifer eine Methode namens **THREAD-HIJACKING**.

In einigen Malware-Kampagnen – wie **EMOTET** und einigen **URSNIF**-Angriffen – werden E-Mails automatisch in laufende E-Mail-Threads eingefügt. So funktioniert die Technik:

1. Die Malware scannt E-Mails in einem kompromittierten Posteingang.
2. Wenn „re:“ als Betreffzeile identifiziert wurde, erstellt sie eine Nachricht, die an die anderen Empfänger im E-Mail-Thread geschickt wird und scheinbar vom kompromittierten Anwender im Thread kommt.
3. Da die E-Mail von jemanden zu stammen scheint, dem die anderen Teilnehmer vertrauen – und mit dem es bereits Aktivitäten gab – fallen die Empfänger häufiger darauf rein.

Proud Boys

In einer ungewöhnlichen E-Mail-Kampagne in Verbindung mit den US-Wahlen ahmten die Angreifer die gewaltbereite rechtsextreme Gruppe Proud Boys nach und griffen als Demokraten registrierte Wähler in Florida an.

E-Mails mit Betreffzeilen wie „Vote for Trump or else!“ (Wähle Trump, sonst passiert was!) drohten den Empfängern mit Gewalt, sollten sie der Aufforderung nicht nachkommen. Enthalten war ein Link zu einem vermeintlich von den Proud Boys stammenden Video mit einer Person, die angeblich gerade Stimmzettel zur Wählerregistrierung und Briefwahl für Bürger von Alaska ausfüllt. Die Kampagne stand mit ihren offenen Gewaltandrohungen im krassen Gegensatz zu den typischen Cyberbedrohungsaktivitäten zum Thema Wahl.

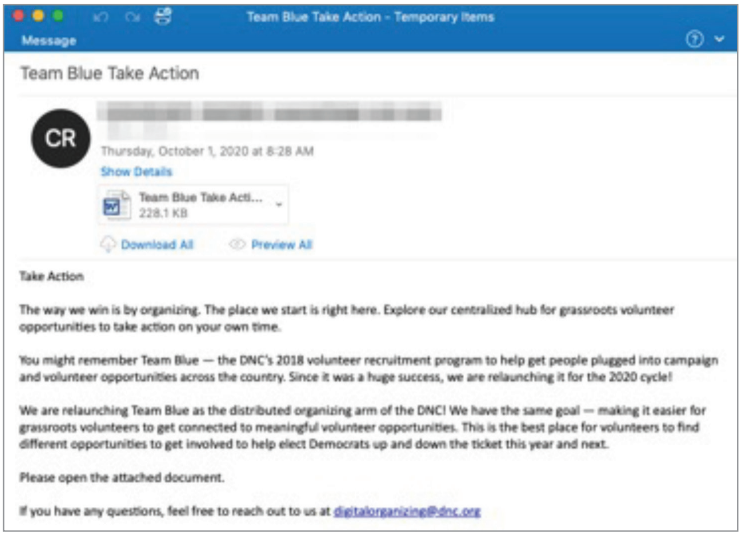
Die Proud Boys-Mitglieder sind zwar für ihre gewaltsamen Angriffe gegen die Linke bekannt, doch geben Behörden und Sicherheitsfirmen an, dass die E-Mails in Wirklichkeit von staatlich unterstützten Angreifern im Iran stammen.

Emotet profitiert vom Wahlfieber

Auch Emotet – die vom E-Mail-Aufkommen her größte Bedrohung des Jahres – verwendete im Oktober 2020 Köder mit dem Thema Wahl. TA542 (der Bedrohungsakteur hinter Emotet) führte folgende wahlbezogene Aktionen durch:

- **Nachahmung** des DNC
- Aufforderung der Empfänger zur Freiwilligenarbeit
- Unterstützung zur politischen Organisierung

(Weitere Informationen zu Emotet erfahren Sie auf **Seite 27 im Abschnitt „Wer ist wer in der Bedrohungslandschaft: Die wichtigsten Bedrohungsakteure“**)



Ein Emotet-Angriff, der mit dem Thema Wahl ködert.

Emotet griff keine bestimmten Personen oder Unternehmen an, die in den Wahlprozess involviert waren, sondern nutzte das Interesse an den Wahlen und den damit verbundenen Ereignissen für Köder, die auf ein breites Publikum in vielen Branchen abzielten.

COVID-19: So nutzten Angreifer die Pandemie für ihre Zwecke

Die COVID-19-Pandemie hat das Arbeits- und Privatleben der meisten Menschen auf den Kopf gestellt. Das Wissen um die Angriffstaktiken in dieser neuen und fremden Umgebung – und möglichst auch der Angreifer – ist ein wichtiges Teil des Cybersicherheits-Puzzles.

Bedrohungsakteure verwenden sehr häufig aktuelle Ereignisse als E-Mail-Köder, doch im Jahr 2020 kam es wohl zum ersten Mal dazu, dass sich alle Angreifer zur selben Zeit auf dieselben Themen konzentrierten. Als die Welt mit gespannter Aufmerksamkeit auf Neuigkeiten zur Pandemie blickte, schwenkte das gesamte Ökosystem der Cyberkriminellen geschlossen auf die gleichen thematischen Inhalte um.

Praktisch alle Bedrohungsakteure nutzten nun COVID-19 als bevorzugten Social-Engineering-Köder, seien es Spammer, Nutzer von **STANDARD-MALWARE**, Cyberkriminelle mit großen Kampagnen oder **ADVANCED PERSISTENT THREATS** (APTs). Wir registrierten beinahe 250 Millionen schädliche Nachrichten mit COVID-19-Bezug – und weitere Milliarden, die aus breiter angelegten Angriffen und Spam stammten.

STANDARD-MALWARE

Der Begriff Standard-Malware steht für häufig genutzte, öffentlich verfügbare Tools, die von vielen Angreifern eingesetzt werden. Standard-Malware sollte zwar von Sicherheitstools erkannt und blockiert werden, doch nutzen Angreifer sie oft auf geschickte Weise und in großen Mengen. Sie können zudem genauso viel Schaden wie hochentwickelte und gezielte Bedrohungen verursachen.

ADVANCED PERSISTENT THREATS (APTS)

Die auch als hochentwickelte andauernde Bedrohungen bezeichneten APTs betreiben typischerweise Spionage im Auftrag einer Regierung, obwohl auch hochentwickelte Cyberkriminelle in diese Kategorie fallen können. Die Angriffe können zu Diebstahl von geistigem Eigentum, zur Plünderung von Konten und zur Schädigung von Daten und Systemen führen.

Missbrauch einer Gesundheitskrise

Die COVID-19-Pandemie war ein gutes Beispiel dafür, dass Cyberangreifer ihre Taktiken innerhalb kürzester Zeit anpassen, um die Angst, Unsicherheit und Zweifel der Opfer auszunutzen.
Dies ist eine Zeitachse der wichtigsten Meilensteine dieser weltweiten Gesundheitskrise sowie der Reaktion der Bedrohungsakteure.

Bekannt gewordene Angriffe

19. Januar

Angriffe gegen Anwender in Japan nutzen COVID-19-Köder, um die Empfänger zum Öffnen infizierter Microsoft Word-Dokumente zu verleiten. Die E-Mails sind Teil einer größeren Kampagne zur Verteilung der Emotet-Malware-Familie.

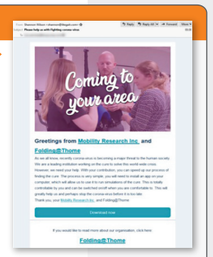
10. Februar

COVID-19-bezogene E-Mail-Köder an Ziele in Japan.

E-Mails an Empfänger im stark betroffenen Italien versprachen aktuelle Informationen zur Pandemie. Sie umfassten einen Microsoft Word-Anhang mit einer URL, die zu einer Phishing-Seite für Anmeldedaten-Diebstahl führte.

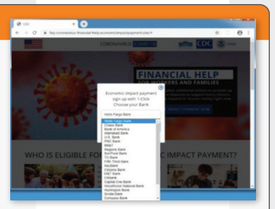
7. März

Menschen in den USA werden mit E-Mails vorgeblich von „Mobility Research Inc“ angegriffen, die um Hilfe zur Suche nach einem Heilmittel um die Teilnahme bei Folding@Thome baten.
Der Inhalt imitiert das legitime Folding@Home-Projekt, das ungenutzte Rechenzyklen auf Anwender-Computern für medizinische Forschung nutzt. Doch statt die COVID-19-Forschung mit der echten Folding@Home-Anwendung zu unterstützen, führt ein Klick auf die URL zur RedLine-Malware, die Anmeldedaten stiehlt und andere Malware herunterlädt.



April

US-Einwohner werden mit Phishing-E-Mails scheinbar vom „Federal Reserve System“ angegriffen, die auf eine offiziell aussehende Website verweisen und zur Eingabe von Banking-Anmeldedaten auffordern, um die Unterstützungsgelder zu erhalten. Die Website war auf den Diebstahl von Anmeldedaten für die meisten großen US-Banken ausgerichtet.



19. Januar 2021

E-Mails an Einwohner der USA und Kanadas versprechen Impfdosen mit dem Pfizer-BioNTech-Impfstoff. Ein Klick auf die URL führt zu einer gefälschten Microsoft 365-Authentifizierungsseite, die Anmeldedaten stehlen soll.

Pandemiebezogenes E-Mail-Aufkommen

Meilensteine der Pandemie

JANUAR

9
Die Weltgesundheits-organisation (WHO) informiert über die geheimnisvolle Coronavirus-Lungenentzündung in Wuhan, China.

20
Drei US-Flughäfen – JFK, San Francisco und Los Angeles – beginnen mit dem Untersuchen ankommender Reisender auf das Coronavirus.

21
Das US-amerikanische CDC (Centers for Disease Control) bestätigt den ersten Coronavirus-Fall der USA.

31
Die WHO ruft einen weltweiten Gesundheitsnotfall aus.

FEBRUAR

3
Die USA rufen einen öffentlichen Gesundheitsnotfall aus.

25
Laut CDC nähert sich COVID-19 einem Pandemiestatus.

MÄRZ

6
21 Passagiere eines kalifornischen Kreuzfahrtschiffes werden positiv getestet.

11
Die WHO erklärt COVID-19 zur Pandemie.

13
Die USA erklären COVID-19 zum nationalen Notfall und geben Milliarden US-Dollar an Notfallhilfen frei. Einreisesperre für Nicht-US-Bürger aus Europa tritt in Kraft.

19
Kalifornien ruft den ersten landesweiten Lockdown aus.

26
Der US-Kongress beschließt den CARES Act mit 2 Billionen USD zur Unterstützung von Krankenhäusern, kleinen Unternehmen und lokalen Behörden. Das Gesetz tritt am nächsten Tag in Kraft.

APRIL

11
Die ersten Unterstützungs-schecks werden in den Bankkonten der US-Empfänger eingezahlt.

29
Erste Tests des National Institutes of Health (NIH) zeigen frühe erfolg-versprechende Ergebnisse für Remdesivir.

MAI

1
Remdesivir erhält FDA-Notzulassung.

28
Die USA verzeichnen mehr als 100.000 COVID-19-Tote.

JUNI

JULI

22
Die US-amerikanischen Health and Human Services (HHS) und das US-Verteidigungs-ministerium geben Vertrag mit Pfizer und BioNTech für 100 Millionen COVID-19-Impfdosen bekannt.

27
Moderna-Impfstoff beginnt Phase-3-Tests.

AUGUST

7
Verhandlungen zum zweiten Unterstützungspaket geraten ins Stocken.

SEPTEMBER

8
Die University of Oxford und AstraZeneca stoppen Phase-3-Tests ihres Impfstoffs aufgrund einer vermuteten starken Nebenwirkung bei einem Teilnehmer.

21
Johnson & Johnson beginnt Phase 3 der Impfstofftests

OKTOBER

2
Donald und Melania Trump werden positiv auf COVID-19 getestet; Trump wird in Krankenhaus eingewiesen.

12
Johnson & Johnson stoppen Phase-3-Impfstofftests nach unerwarteter Krankheit eines Teilnehmers.

15
Anzahl der Fälle in den USA steigen erstmalig seit Anfang August auf 60.000 neu gemeldete COVID-19-Infektionen.

23
Unabhängig voneinander nehmen AstraZeneca und Johnson & Johnson ihre Impfstofftests wieder auf.

NOVEMBER

16
Die US-amerikanische FDA (Food and Drug Administration) verkündet baldige Notzulassung von Pfizer- und Moderna-Impfstoffen.

DEZEMBER

11
FDA beschließt Notzulassung für Pfizer/BioNTech-Impfstoff.

14
Sandra Lindsay, Krankenschwester auf einer Intensivstation, ist die erste geimpfte US-Bürgerin.

18
FDA beschließt Notzulassung für Moderna-Impfstoff.

29
Zweite Runde der US-Unterstützungs-schecks erreicht die Empfänger.

JANUAR

INFEKTIONSVEKTOR
Ein Infektionsvektor ist der Übertragungskanal eines Angriffs. E-Mail ist der am häufigsten genutzte Infektionsvektor bei modernen Cyberangriffen.

SCHADDATEN
Schaddaten sind die Malware, die die Angreifer letztlich auf das betroffene System übertragen wollen. Sie unterscheiden sich von jeglichem schädlichen Code, der genutzt wird für den Erstzugriffspunkt ins System, für Übertragungstechniken oder für die Social-Engineering-Taktiken, mit denen Menschen zum Herunterladen oder Aktivieren der Schaddaten verleitet werden.

Die COVID-19-Pandemie war die größte Krise für die öffentliche Gesundheit der letzten hundert Jahre. Durch die schnelle Ausbreitung des Virus auf der ganzen Welt mussten sich Unternehmen aller Art anpassen. Schnell führten sie neue Richtlinien und Technologien ein und bewegten sich dabei auf einem schmalen Grat zwischen der Sicherheit der Arbeitnehmer und dem Überleben des Unternehmens.

Auch die Bedrohungsakteure passten sich der Situation schnell an. Durch die Angst und Verunsicherung über die gesundheitliche und wirtschaftliche Sicherheit in Kombination mit einem überstürzten Wechsel zur Arbeit im Home Office entstanden ideale Bedingungen für effektivere Cyberangriffe. Mitte März 2020 setzten etwa 80 % der von uns täglich gescannten Bedrohungen auf COVID-19-Themen.

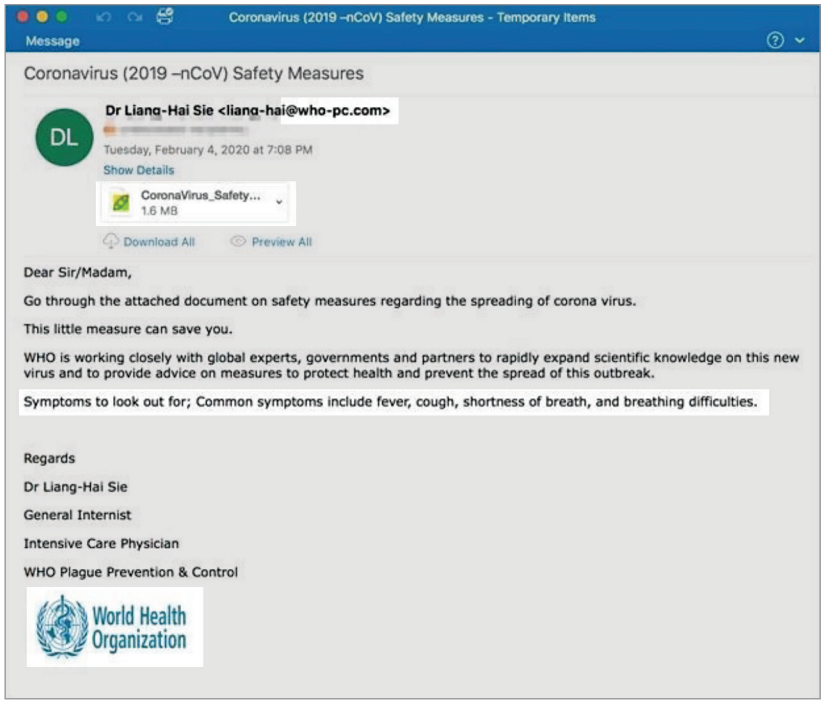
Die **INFEKTIONSVEKTOREN**, **SCHADDATEN** und das aggregierte Nachrichtenaufkommen dieser Bedrohungen blieben dabei größtenteils unverändert. Die Bedrohungsakteure verbreiteten weiterhin die gleichen Malware- und Phishing-Kampagnen in den gewohnten Zeitabständen und Mengen. Neu hinzu kamen eine gestresste Belegschaft und die Störung der gewohnten Betriebsabläufe. Das Ergebnis war eine größere Angriffsfläche, die wiederum für höhere Infektionsraten sorgte.

Frühlingserwachen

Zu Beginn der Pandemie sollten die Köder vor allem eine emotionale Reaktion hervorrufen. Viele lockten ihre Opfer mit Neuigkeiten zu geänderten Unternehmensrichtlinien, behördlichen Vorgaben und geeigneten Schutzmaßnahmen. Zum Beispiel wurde die Weltgesundheitsorganisation (WHO) nachgeahmt und die Opfer mit Informationen über das Virus geködert.

WICHTIGE MERKMALE:

- Verwendung der Doppelgänger-E-Mail-Domäne soll WHO-Erklärung imitieren
- Schädlicher Anhang soll mit Dateiname Thema verstärken
- Grundlegende Informationen zu COVID-19, um Nachricht glaubwürdiger erscheinen zu lassen
- WHO-Logo dient zur besseren Tarnung



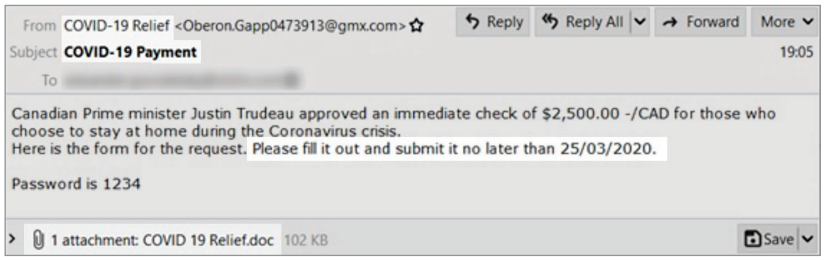
Phishing-E-Mail, in der die WHO nachgeahmt wird.

Dem Geld folgen

Während Regierungen über Konjunkturhilfen sprachen, die einen wirtschaftlichen Zusammenbruch verhindern sollten, nutzten Cyberkriminelle die Gelegenheit und köderten ihre Opfer mit vermeintlichen Geldzahlungen an die Bevölkerung und Unternehmen.

WICHTIGE MERKMALE:

- Nutzung von Display Name-Spoofing und einer auffälligen Betreffzeile, um Aufmerksamkeit der Empfänger mit Versprechen von Finanzhilfen zu wecken
- Angegebene Frist soll Opfer unter Zeitdruck setzen
- Schädlicher Anhang soll mit Dateiname Thema Finanzhilfen verstärken



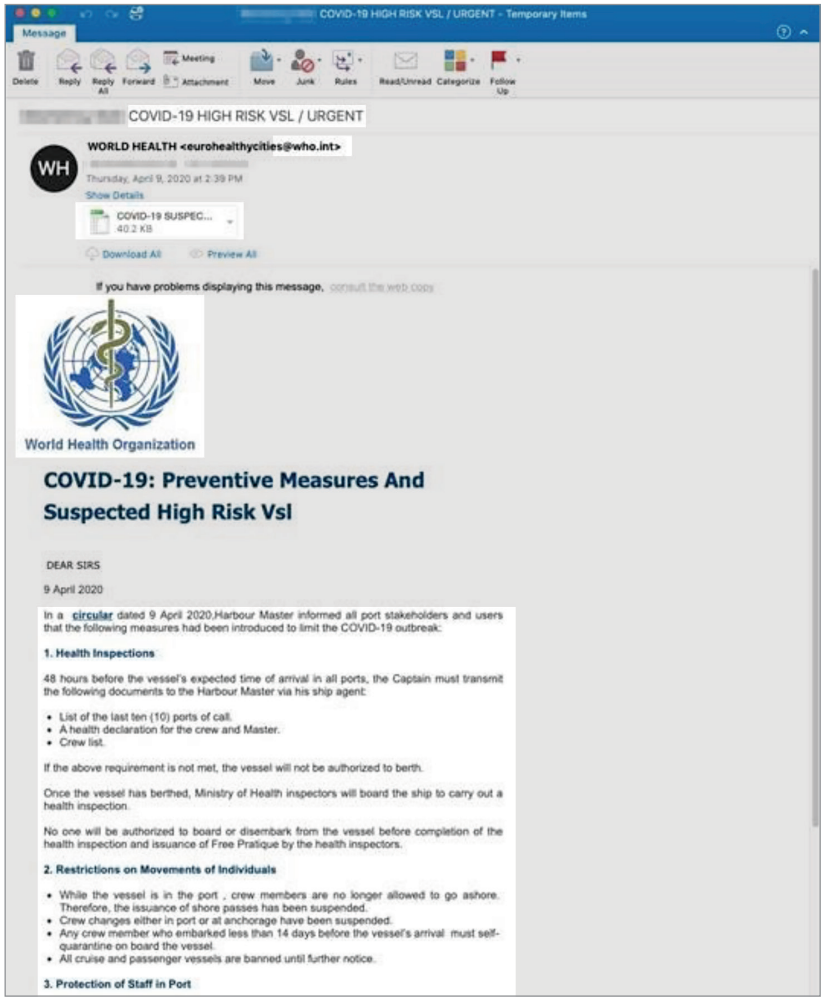
Phishing-E-Mail zu angeblichen Corona-Finanzhilfen.

Die goldenen Regeln

Als anschließend die Regierungen damit begannen, neue Richtlinien und Vorschriften zu erlassen, fanden sich in den Ködern Themen rund um die Einhaltung dieser Regeln wieder.

WICHTIGE MERKMALE:

- Lesern wird Gefühl des Zeitdrucks und Risikos suggeriert, um sie zu instinktivem Handeln zu bewegen
- Nachgeahmte E-Mail-Domäne der WHO
- Schädlicher Anhang soll mit Dateinamen Gefühl der Angst und Gefahr verstärken
- Nutzung des WHO-Logos, um offiziellen Eindruck zu erwecken
- Reale Informationen über COVID-19 sollen scheinbare Autorität der E-Mail verstärken



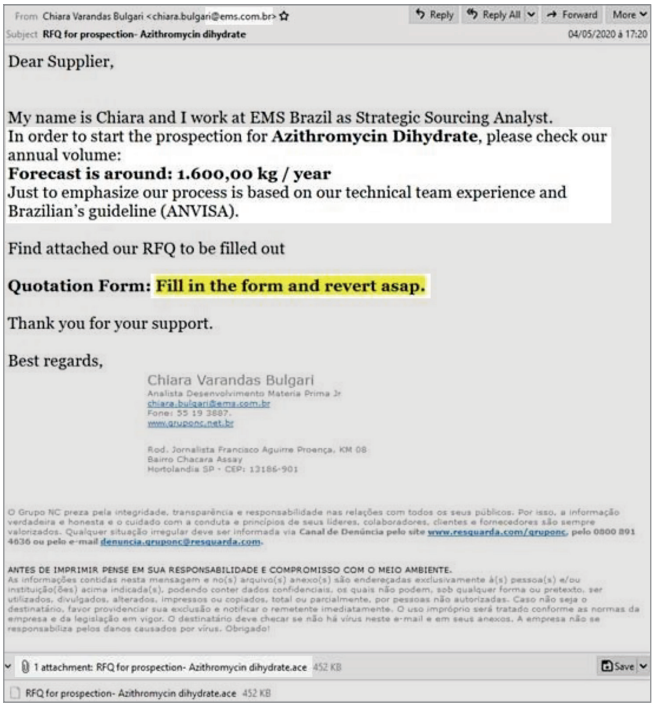
Phishing-E-Mail, die angeblich von der WHO stammt und Informationen über COVID-19 verbreitet.

Taktiken vermehren sich parallel zur Ausbreitung des Virus

Mit zunehmender Ausbreitung wirkte sich die Pandemie auf beinahe alle Menschen und Lebensbereiche aus. Dabei wurden auch die Köder der Angreifer vielfältiger und esoterischer – die Opfer wurden mit gefälschten Benachrichtigungen zu Lebensmittellieferungen, COVID-19-Behandlungsaussichten und Neuigkeiten zu Stellenstreichungen getäuscht.

WICHTIGE MERKMALE:

- Nachgeahmte E-Mail-Domäne von EMS, dem größten Arzneimittelhersteller Brasiliens
- Auf aktuelle Ereignisse bezogene, emotionsgeladene Betreffzeile soll Aufmerksamkeit der Leser wecken
- Empfänger werden aufgefordert, schnell zu handeln, um bewussten Nachdenken zu vermeiden
- Enthält schädlichen Anhang, der als normales Geschäftsformular getarnt ist



From: Chiara Varandas Bulgari <chiara.bulgari@ems.com.br>
Subject: RFQ for prospection- Azithromycin dihydrate
04/05/2020 à 17:20

Dear Supplier,

My name is Chiara and I work at EMS Brazil as Strategic Sourcing Analyst.
In order to start the prospection for **Azithromycin Dihydrate**, please check our annual volume:
Forecast is around: 1.600,00 kg / year
Just to emphasize our process is based on our technical team experience and Brazilian's guideline (ANVISA).

Find attached our RFQ to be filled out

Quotation Form: Fill in the form and revert asap.

Thank you for your support.

Best regards,

Chiara Varandas Bulgari
Analista Desenvolvimento Materia Prima Jr
chiara.bulgari@ems.com.br
Fone: 55 19 3887...
www.grupoNC.net.br

Rod. Jornalista Francisco Aguirre Proença, KM 08
Bairro Chacara Assay
Hortolandia SP - CEP: 13186-901

O Grupo NC preza pela integridade, transparência e responsabilidade nas relações com todos os seus públicos. Por isso, a informação verdadeira e honesta e o cuidado com a conduta e princípios de seus líderes, colaboradores, clientes e fornecedores são sempre valorizados. Qualquer situação irregular deve ser informada via **Canal de Denúncia pelo site www.resguarda.com/gruponc**, pelo 0800 891 4636 ou pelo e-mail **denuncia.gruponc@resguarda.com**.

ANTES DE IMPRIMIR PENSE EM SUA RESPONSABILIDADE E COMPROMISSO COM O MEIO AMBIENTE.
As informações contidas nesta mensagem e no(s) arquivo(s) anexo(s) são endereçadas exclusivamente à(s) pessoa(s) e/ou instituição(ões) acima indicada(s), podendo conter dados confidenciais, os quais não podem, sob qualquer forma ou pretexto, ser utilizados, divulgados, alterados, impressos ou copiados, total ou parcialmente, por pessoas não autorizadas. Caso não seja o destinatário, favor providenciar sua exclusão e notificar o remetente imediatamente. O uso impróprio será tratado conforme as normas da empresa e da legislação em vigor. O destinatário deve checar se não há vírus neste e-mail e em seus anexos. A empresa não se responsabiliza pelos danos causados por vírus. Obrigado!

1 attachment: RFQ for prospection- Azithromycin dihydrate.ace 452 KB
RFQ for prospection- Azithromycin dihydrate.ace 452 KB

Phishing-E-Mail, die vermeintlich Informationen zur Behandlung von COVID-19 enthält.

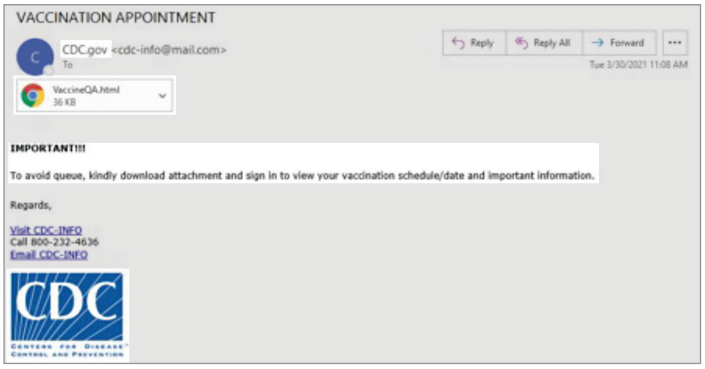
Neues Jahr, ähnliche Themen

Im Jahr 2021 hat sich die Situation in Bezug auf die Pandemie und die globale Reaktion darauf verbessert. Dennoch nutzen Bedrohungsakteure weiterhin COVID-19-bezogene Themen und ahmten zum Beispiel Informationen rund um die Vergabe von Impfterminen nach.

Ganz gleich, was 2021 noch bereithält, COVID-19 wird wahrscheinlich weiterhin ein häufig genutztes und wirkungsvolles Thema für Cyberangriffe bleiben.

WICHTIGE MERKMALE:

- Nutzung von Display Name-Spoofing zur Nachahmung einer von der CDC verschickten E-Mail
- Angehängte HTML-Datei ist eine Webseite für Anmeldedaten-Phishing
- Versprechen von schnellem Zugang zu damals knapper Ressource (in diesem Fall der COVID-19-Impfstoff)
- CDC-Logo dient zur besseren Tarnung



VACCINATION APPOINTMENT
CDC.gov <cdc-info@mail.com>
To
Reply Reply All Forward
Tue 3/30/2021 11:08 AM
VaccineQA.html
36 KB

IMPORTANT!!!

To avoid queue, kindly download attachment and sign in to view your vaccination schedule/date and important information.

Regards,

Visit CDC-INFO
Call 800-232-4636
Email CDC-INFO

CDC
CENTERS FOR DISEASE CONTROL AND PREVENTION

Phishing-E-Mail zum Anmeldedatendiebstahl ahmt CDC nach.

ANMELDEDATEN-PHISHING
Beim Anmeldedaten-Phishing werden die Opfer dazu gebracht, ihre Kontoanmeldedaten anzugeben. Die Angreifer erlangen somit Zugriff auf Bankkonten, persönliche Informationen, Unternehmenskonten und mehr. Anmeldedaten-Phishing läuft üblicherweise über E-Mails ab, in denen die unterschiedlichsten Social-Engineering-Techniken zum Einsatz kommen können. Die Angreifer geben sich als vertrauenswürdige Marke oder eine Person aus dem Unternehmen der Opfer aus und verschicken eine E-Mail, die einen Link zu einer gefälschten Anmeldeseite enthält. Geben Anwender ihre Benutzernamen und Kennwörter ein, übernehmen die Angreifer mit diesen Informationen die Konten der Opfer.

BUSINESS EMAIL COMPROMISE (BEC)
Angriffe, bei denen Bedrohungsakteure vertrauenswürdige Kollegen, Führungskräfte oder Anbieter mit Hilfe einer Reihe von Techniken nachahmen. Der Absender bittet den Empfänger zum Beispiel, Geld zu überweisen, eine Rechnung zu begleichen, Gehaltszahlungen umzuleiten, Bankverbindungen zu ändern oder vertrauliche Informationen herauszugeben.

BEC-Angriffe sind schwer zu erkennen, weil sie weder Malware noch schädliche URLs enthalten, die mit standardmäßiger Cyberabwehr analysiert werden könnten. Stattdessen verleiten die BEC-Angreifer ihre Opfer mit Hilfe von Identitätstäuschung und anderen Social-Engineering-Techniken dazu, Handlungen im Namen des Angreifers auszuführen.

Angriffstypen

ANMELDEDATEN-PHISHING bei Verbrauchern und Unternehmen war die mit Abstand häufigste Angriffsform und trat häufiger auf, als alle anderen Formen zusammengenommen. 2020 machte Anmeldedaten-Phishing mehr als die Hälfte aller E-Mail-Bedrohungen aus.

Der Diebstahl von Benutzernamen und Kennwörtern kann zu Finanzbetrug, Cyber-Spionage und vielem mehr führen.

Andere Angriffstypen richteten sich zum Beispiel gegen Finanzsysteme, luden weitere Malware herunter, kaperten infizierte Systeme für Botnets und stahlen vertrauliche Informationen.

BEC

Die E-Mail-Betrugsmethode **BUSINESS EMAIL COMPROMISE** (BEC, auch Chefmasche genannt) gehört zu den Bedrohungen, die die größten finanziellen Schäden bei Unternehmen aller Größen und in allen Branchen verursacht. Laut dem vom FBI geführten Internet Crime Complaint Center betrugen die Kosten dieser Angriffe für Unternehmen und Einzelpersonen allein im Jahr 2020 etwa 1,8 Milliarden US-Dollar. Das sind 44 % aller gemeldeten Verluste durch Cyberkriminalität – mehr als die meisten anderen Arten von Cyberkriminalität.[5]

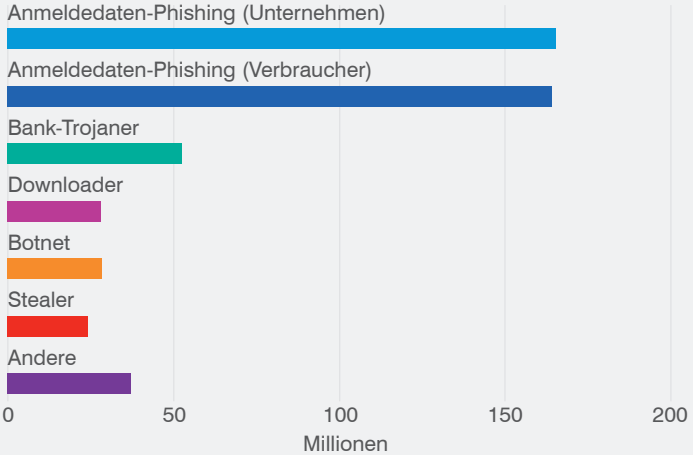
Bei Proofpoint verfolgen wir einen personenzentrierten Ansatz zum Schutz vor BEC, der aus einem dreistufigen **Framework** besteht:

- Identität: für wen sich die Akteure ausgeben
- Täuschung: die von ihnen verwendeten Techniken
- Thema: die aufgetretene Betrugskategorie

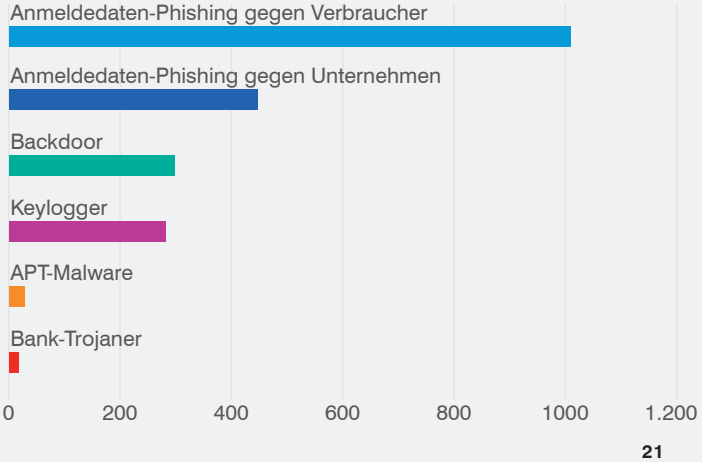
Täuschungen werden üblicherweise in zwei Kategorien eingeteilt: Nachahmung und Kompromittierungstechniken. Nachahmung definieren wir als einen Angriff, in dem der Akteur einen oder mehrere E-Mail-Header manipuliert, um den Absender zu verschleiern. Eine Kompromittierung ist ein Angriff, bei dem ein Angreifer Zugang zu einem legitimen Postfach erlangt.

5 FBI: „2020 Internet Crime Report“ (Bericht zu Internetkriminalität 2020), März 2021.

Angriffstypen nach Nachrichtenaufkommen (2020)
Anmeldedaten-Phishing gegen Unternehmen und Verbraucher war der bei weitem häufigste Angriffstyp.



Veränderung (2020 und 2019 im Vergleich)



Unser Framework legt einen besonderen Schwerpunkt auf Köderthemen, denn sie liefern verwertbare Bedrohungsdaten, einschließlich der dabei eingesetzten unterschiedlichen Betrugsarten wie **Rechnungsbetrug**, die Umleitung von Gehaltszahlungen und Erpressung.

In erfolgreichen BEC-Methoden werden Social-Engineering-Taktiken eingesetzt, beispielweise wird der Anzeigename geändert bzw. ein bestimmter Tonfall oder Anhänge werden genutzt, um eine Nachricht glaubwürdiger erscheinen zu lassen.

Bei einem im Jahr 2020 beobachteten relativ raffinierten Betrugsversuch setzte ein Bedrohungsakteur, den wir unter dem Kürzel TA2520 führen, Social Engineering in mehreren Kampagnen ein. Er ahmte dabei oft hochrangige Führungskräfte über Display Name-Spoofing nach und wies die Empfänger an, Geld für einen angeblichen Unternehmenskauf zu überweisen.

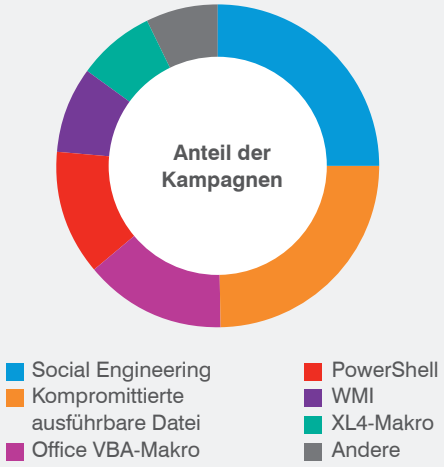
In diesen Betrugsversuchen ging es um Summen von mehr als einer Million US-Dollar, wobei häufig aktuelle Ereignisse einbezogen wurden. In einigen Nachrichten war beispielsweise die Rede von Einschränkungen durch COVID-19 und von einem Impfstoff, der für eine wirtschaftliche Erholung sorgen sollte.

Ein weiterer wichtiger Bedrohungsakteur im Jahr 2020 ist TA2519, der mehrstufige BEC-Angriffe durchführte. In der ersten Angriffsstufe konzentrierte sich der Bedrohungsakteur auf die Verbreitung von COVID-19-Ködern zur Verteilung von Malware, die die Anmeldedaten der Opfer stehlen sollte. In der zweiten Stufe nutzte TA2519 die gestohlenen Anmeldedaten, um die Konten der Opfer zu übernehmen und damit gefälschte Rechnungen an ein zweites Opfer zu schicken – eine Technik, die als Betrug mit Lieferantenrechnungen bekannt ist.

Gefälschte Rechnungen können so manipuliert werden, dass sie den Anschein erwecken, sie kämen von einer beliebigen Person, zum Beispiel von einem Kollegen oder einem unbekannten Dritten. Am erfolgversprechendsten ist offenbar das Ausnutzen von Beziehungen zu Lieferanten, also zu Unternehmen, die Produkte oder Dienstleistungen verkaufen. Letztendlich können solche Angriffe die Unternehmen Zehntausende bis mehrere Millionen US-Dollar kosten.

Anteil der Kampagnen

Eine schädliche E-Mail kann mehrere Techniken enthalten, z. B. Social Engineering, das die Anwender zum Herunterladen und Öffnen eines kompromittierten Anhangs verleiten soll.



Angriffstechniken

Bedrohungsakteure setzen ein breites Spektrum an Techniken ein, um Sicherheitskontrollen zu umgehen und die Opfer dazu zu bringen, einen Angriff auszulösen und die Zielsysteme zu infizieren. Eine Gemeinsamkeit ist dabei der Einsatz von Social-Engineering-Taktiken.

Dabei verwenden sie beispielsweise auffällige Betreffzeilen, glaubhafte Handlungsaufforderungen und gezielte Vorgehensweisen, um die Empfänger zu einer Reaktion zu bewegen. Wie bereits im **Abschnitt „COVID-19: So nutzten Angreifer die Pandemie für ihre Zwecke“ auf Seite 15** beschrieben, war das beliebteste Thema im Jahr 2020 die Pandemie.

Im Folgenden werden einige andere wichtige Trends erläutert.

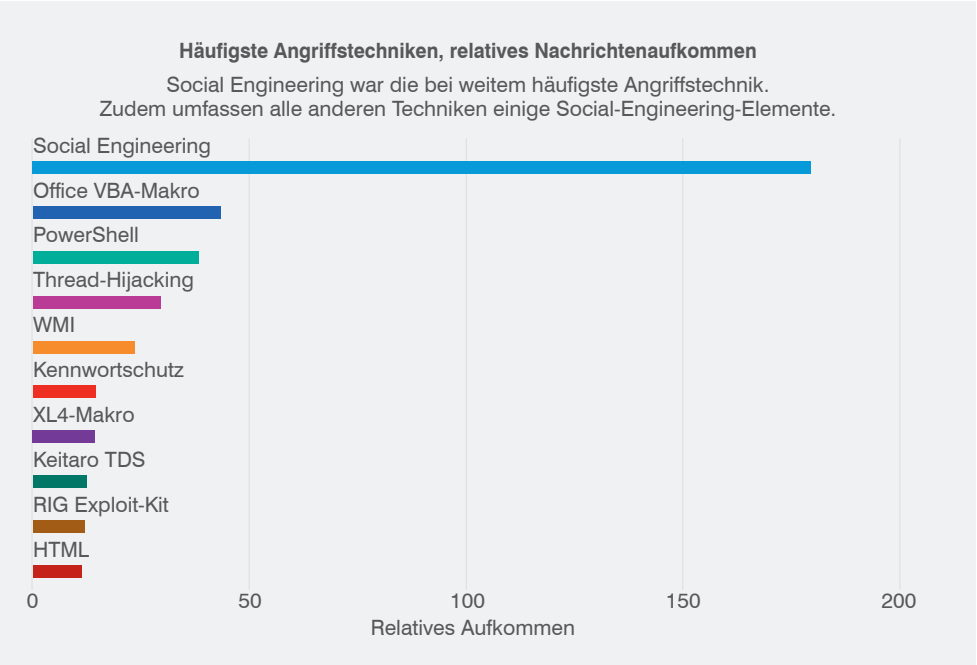
Komprimierte ausführbare Dateien

Beinahe ein Viertel der Angriffskampagnen setzte komprimierte ausführbare Dateien ein, um Malware zu verbergen. Bei dieser Methode muss das Opfer mit einem schädlichen Anhang (z. B. einer PowerPoint-Präsentation oder einer Excel-Arbeitsmappe) interagieren, um die Schaddaten auszuführen. Da das schädliche Skript erst ausgeführt wird, wenn jemand die Datei entsperrt, werden automatisierte Malware-Erkennungsfunktionen effektiv umgangen.

Excel 4.0

Im Laufe des Jahres 2020 nutzten Bedrohungsakteure **zunehmend** Excel 4.0-Makros (XL4) zur Verteilung von Malware. Dabei verwendeten sie etwas weniger häufig Office Visual Basic for Applications-Makros. (Trotzdem bleibt Letzteres eine sehr viel häufiger genutzte Technik.)

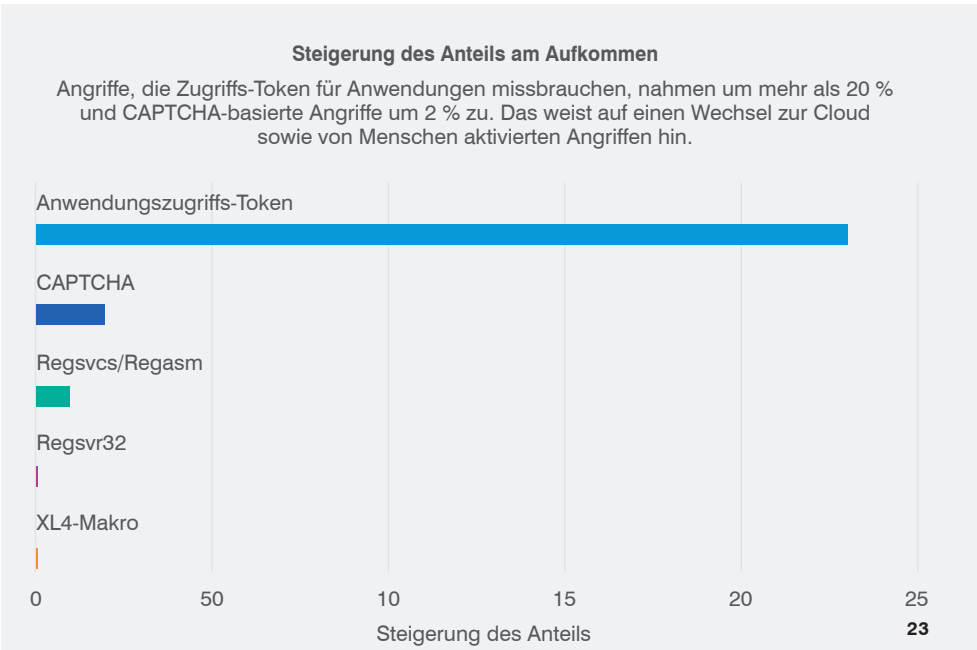
XL4-basierte Angriffe nutzen eine Reihe alter Excel-Funktionen, daher ist ein plötzlicher Anstieg dieser Technik eventuell überraschend. Eine Erklärung sind die begrenzten Erkennungsmöglichkeiten für XL4 in modernen Sicherheitssystemen. Obwohl Microsoft immer noch XL4-Makros unterstützt, empfiehlt der Software-Riese seinen Kunden **dringend**, auf die neueste VBA-Version umzusteigen.



CAPTCHA

Angriffe mit CAPTCHA-Techniken stiegen 2020 stark an. (Wie schon in **Abschnitt 1: „Schwachstellen“ auf Seite 6** erwähnt, waren Anwender für diese Technik anfälliger als im Jahr 2019.)

Der finanziell motivierte Bedrohungsakteur TA564 verwendet diese Methode oft in Malware-Kampagnen gegen Organisationen in Kanada. Mittels CAPTCHA prüft der Angreifer vor einer Aktion, ob sich das Opfer in der Zielregion befindet. Ist dies nicht der Fall, wird der Angriff gestoppt.



BANK-TROJANER
Dieser Malware-Typ stiehlt traditionell die Online-Banking-Anmeldedaten von Kunden. Dies erfolgt meist dadurch, dass der Browser des Opfers auf eine gefälschte Version der Bank-Website umgeleitet oder ein gefälschtes Anmeldeformular in die echte Website injiziert wird. In jüngster Zeit dienten viele Bank-Trojaner auch als Vorstufe zu medienwirksamen Ransomware-Angriffen.

LOADER/DOWNLOADER
Loader-Malware lädt zusätzlichen Schadcode aus dem Internet herunter. Viele verschiedene Malware-Typen wie Bank- und Remote-Zugriffs-Trojaner verfügen nun über diese Funktion. Dropper haben Ähnlichkeiten mit Loadern, doch statt zusätzlichen Code herunterzuladen, entschlüsseln und starten sie den Code, der mit den Malware-Schaddaten anfangs übertragen wurde.

DRIDEX
Der modulare Bank-Trojaner Dridex, der von den Bedrohungsakteuren „Evil Corp" entwickelt und kontrolliert wird, verschwand 2019 von der Bildschirmfläche und tauchte 2020 wieder auf. Die Malware ist eng mit der anschließenden Bereitstellung von Bitpaymer/Doppelpaymer-Ransomware verbunden.

QBOT
Qbot ist ein modularer Trojaner, dessen Funktionen seit der ersten Nutzung im Jahr 2007 stetig erweitert wurden. Wie die anderen hier aufgeführten Bank-Trojaner fungiert Qbot nun hauptsächlich als Informationsdieb und Loader für nachfolgende Schaddaten wie Cobalt Strike.

ZLOADER
Zloader ist ein älterer Bank-Trojaner, dessen Nutzung im Jahr 2020 mit aktualisierten Varianten sprunghaft anstieg. Er wird weiterhin aktiv weiterentwickelt und von vielen Angreifern genutzt.

REMOTE-ZUGRIFFS-TROJANER
Remote-Zugriffs-Trojaner bieten Angreifern die administrative Kontrolle eines infizierten Systems. Üblicherweise besitzen sie weniger hochentwickelte Funktionen, doch können sie kompromittierte Systeme überwachen sowie zusätzliche Malware herunterladen und ausführen.

Angriffstools

BANK-TROJANER, die Finanzdaten stehlen und als **LOADER** für andere Malware agieren können, gehörten zu den am häufigsten verwendeten Malware-Typen, die von Bedrohungsakteuren verteilt wurden. Zu den wichtigsten Familien gehören **DRIDEX**, **QBOT** und **ZLOADER**.

Zwar gingen die Aktivitäten des Emotet-Botnets im Jahr 2020 drastisch zurück – die Gruppe blieb jedoch weiterhin eine der aktivsten. (Weitere Informationen zu Emotet finden Sie in **„Malware-Fallstudie: Emotet im Jahr 2020" auf Seite 28** sowie in **„Malware-Metamorphose: Warum Bezeichnungen öfter eine andere Bedeutung haben können" auf Seite 26**.)

Die RATtenjagd gewinnen

Beinahe ein Viertel der Malware-Kampagnen nutzte **REMOTE-ZUGRIFFS-TROJANER** (RATs). Bedrohungsakteure können mittels RATs die Kontrolle über den Rechner der Betroffenen übernehmen und Bankdaten stehlen, Informationen sammeln und sich in der kompromittierten Umgebung ausbreiten. Beispiele für bekannte RATs sind Ave Maria, NanoCore RAT und Remcos.

Obwohl 2020 viele RAT-Kampagnen geführt wurden, waren sie weniger wirkungsvoll als Kampagnen, in denen andere Malware-Familien zum Einsatz kamen. Die Anwender klickten oder reagierten häufiger auf E-Mails mit Emotet, Malware-Backdoors und Bank-Malware.

Eine Lektion in Sachen Ransomware: Angreifer nehmen Schulen im Jahr des Distanzunterrichts ins Visier

Genau wie Mitarbeiter in Unternehmen waren auch Schüler und Studenten, Eltern, Lehrer und Schulen durch die Pandemie gezwungen, über das Internet miteinander zu kommunizieren. Der Unterrichtsbetrieb wurde per Videokonferenz-Software wieder aufgenommen und Schüler, Studenten und Lehrkräfte tauschten sich allein über digitale Ressourcen aus.

Die Bedrohungsakteure stellten sich schnell auf die neue Situation ein. Sie nutzten den Umbruch für ihre Zwecke und setzten unterrichtsbezogene Themen oder andere Schulressourcen als Köder ein, um damit Malware zu verteilen und in vielen Fällen den Distanzunterricht zu behindern.

In einer Kampagne vom Oktober 2020 ahmten die Angreifer Eltern oder Aufsichtspersonen nach, die im Namen der Schüler eine Arbeit einreichen wollten.[6] In der E-Mail stand, das Kind hätte technische Probleme. Das schädliche Dokument im E-Mail-Anhang übertrug Cryptme, eine simple Ransomware-Variante, die Dateien auf den Rechnern der Betroffenen verschlüsselt.

6 **https://www.nbcnews.com/tech/security/parents-end-chain-ransomware-hit-kids-schools-rcna646**

E-Mail, die angeblich von einem Elternteil stammt.

2020 stiegen Ransomware-Angriffe sprunghaft an. Da Schüler und Studenten gezwungen sind, vor ihren Bildschirmen zu lernen, führen diese Angriffe zu großen Beeinträchtigungen in einer bereits angespannten Lernumgebung.

Schulen **bleiben weiterhin ein Ziel** für Cyberkriminelle. Wir gehen davon aus, dass sich dies auch im Jahr 2021 fortsetzt.

Anstieg an Cobalt-Aktivitäten

Oft missbrauchen Bedrohungsakteure Software-Tools, die wie RATs funktionieren und für legitime Anwendungsfälle von IT-Abteilungen, Sicherheitstestern und fortgeschrittenen Anwendern eingesetzt werden. Einige sind sogar in Anwendersysteme integriert und ermöglichen es den Angreifern, die Ressourcen einzusetzen, die bereits im Zielsystem vorhanden sind. (Diese Taktik wird „Living-off-the-Land“ genannt.)

Ein Beispiel dafür ist Cobalt Strike, ein kommerzielles Sicherheitstool, das Unternehmen helfen soll, Schwachstellen durch simulierte Angriffe aufzudecken. (Diese Methode ist als „Red Team“-Übung bekannt, in der eine Person im Auftrag des Unternehmens die Rolle eines Cybereindringlings übernimmt.)

Allerdings nutzen immer mehr Bedrohungsakteure das Tool für echte Angriffe. 2020 stieg die Anzahl der Bedrohungen, die Cobalt Strike als primäre Schaddaten verteilten, sprunghaft um 161 % an.

Andere Sicherheitsforscher beobachten die gleichen Trends, da immer mehr Bedrohungsakteure Open-Source-Hackingtools verwenden. Zum Beispiel verschickte TA572 Rechnungs-E-Mails mit schädlichen Excel- und Word-Dokumenten, die mittels Microsoft Excel 4.0-Makros (XL4) Cobalt Strike herunterluden.

Malware-Metamorphose: Warum Bezeichnungen öfter eine andere Bedeutung haben können

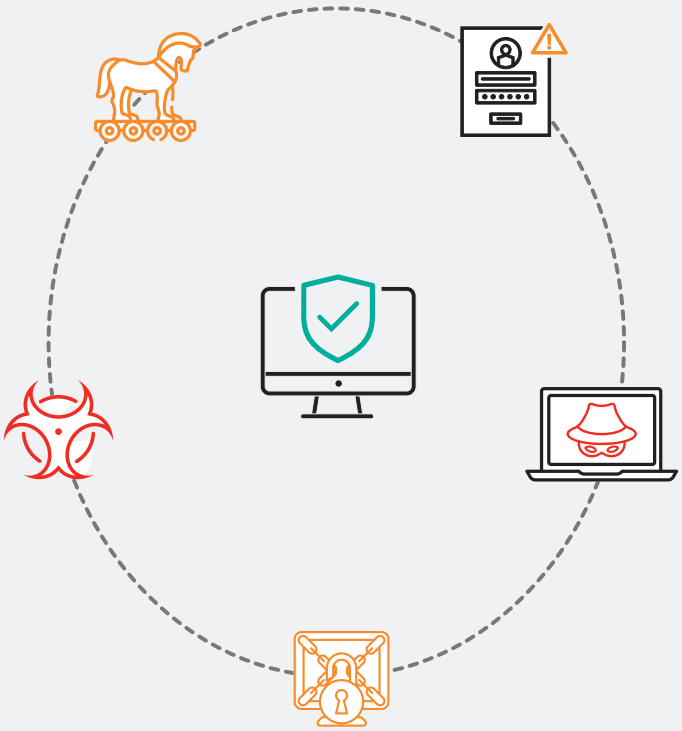
Das Klassifizieren von Malware kann Ihnen helfen, das Ausmaß und die Art einer Bedrohung zu verstehen, die gegen Ihre Anwender gerichtet ist, doch liefern diese Bezeichnungen nicht immer ein vollständiges Bild. Angreifer entwickeln Malware-Familien weiter und nutzen sie auf unerwartete Weise. Und wie bei einer Schauspielertruppe, in der ein Schauspieler im Krankheitsfall für einen anderen einspringt, werden Malware-Tools oft ausgetauscht und je nach Bedarf miteinander kombiniert.

Die gemeinsame Nutzung unterschiedlicher Malware-Familien ist eine langjährige Praxis, die für die Angreifer einen wichtigen Zweck erfüllt. Sie sind dadurch flexibel und können für jede Angriffsphase genau das richtige Tool einsetzen. Zudem sorgt der Ansatz für Redundanz und ermöglicht es den Angreifern, sich weiterhin in einer Umgebung aufzuhalten, selbst wenn Teile der Malware bereits erkannt wurden. Und nicht zuletzt verlängert das die Lebensdauer älterer Malware, die wahrscheinlich von Sicherheits-Gateways erkannt würde – aber nicht, wenn sie auf einen bereits infizierten Rechner heruntergeladen wird.

Ein Beispiel dafür ist Emotet, der vielseitig einsetzbare und weit verbreitete Malware-Service, der als „die weltweit gefährlichste Malware“ galt, bevor seine Infrastruktur im Januar durch internationale Bemühungen der Strafverfolgungsbehörden abgeschaltet wurde. Emotet wurde 2014 zum ersten Mal entdeckt und diente als einfacher Bank-Trojaner für den Diebstahl von Kontoanmeldedaten bei einer kleinen Gruppe von Personen in Deutschland und Österreich.

Nicht lange danach wurden der Schadsoftware Downloader-Funktionen hinzugefügt, die Emotet zu einem nützlichen Tool zum Download sekundärer Malware machten. Im Laufe der Zeit sorgten weitere Funktionen dafür, dass die Malware für Angreifer von größerem Nutzen sowie schwerer zu erkennen war, sich schneller ausbreiten konnte und sich auf einfachere Weise erweitern ließ.

Später entwickelte sie sich zu einem vielseitig einsetzbaren Botnet – einem Netzwerk infizierter Rechner, das wie eine Zombie-Armee weltweit für ein breites Spektrum an Angriffen genutzt werden konnte.



Wer ist wer in der Bedrohungslandschaft: Die wichtigsten Bedrohungsakteure

2020 haben wir 69 aktive Bedrohungsakteure identifiziert. Basierend auf dem Nachrichtenaufkommen werden im Folgenden die aktivsten von ihnen näher untersucht. Wie die meisten Angreifer, die Nachrichten in großen Mengen verschicken, werden alle fünf Bedrohungsakteure von Forschern als „finanziell motiviert" bezeichnet, d. h. sie konzentrieren sich auf Finanzverbrechen.

Die Kunst und Wissenschaft der Attribution

Egal ob im Internet oder in der Realität – diese Frage wird bei jedem Verbrechen gestellt: *Wer war es*? Für Sicherheitsforscher ist die Antwort nicht immer eindeutig.

Jeder Angriff hinterlässt eine Spur digitaler Brotkrumen, z. B. die von der Malware genutzten IP-Adressen von Command-and-Control-Servern, Malware-Metadaten, die in E-Mail-Ködern verwendeten Schriftarten und Sprachen, Verhaltensweisen, Konfigurationseinstellungen und andere Hinweise. Forscher tragen diese Anhaltspunkte zusammen und suchen nach Mustern zwischen Angriffen, um sich ein Bild davon zu verschaffen, wer hinter einem Angriff steckt. Bedrohungsforscher nennen diesen Vorgang Attribution.

Wir kategorisieren Bedrohungsakteure nach ihren Kampagnen und Verhaltensweisen und nicht nach Nationalität oder Organisation, obwohl einige von ihnen auch durch andere Forschungsteams und Strafverfolgungsbehörden zugeordnet werden. Eine eindeutige Attribution ist jedoch nicht immer möglich.

Der Grund: Das Ökosystem der Cyberkriminellen ist unüberschaubar und stark fragmentiert.

Einige cyberkriminelle Organisationen funktionieren wie Franchises. Fortgeschrittene **BEDROHUNGSAKTEURE** entwickeln die Malware-„Produkte" und stellen sie dann über eine passende Infrastruktur als leicht zu bedienende Pakete oder Services zur Verfügung. Interessierte Cyberkriminelle können diesen Service dann für ihre Angriffe mieten. Sie bezahlen für einen bestimmten Zeitraum oder bekommen für jede erfolgreiche Kompromittierung einen Anteil an der Beute. In anderen Fällen handeln sie als Verteiler, die die Malware über E-Mails versenden und mit einer Provision für jede erfolgreiche Infizierung vergütet werden.

Da verschiedene Cyberkriminelle oftmals die gleichen Tools und Infrastrukturen nutzen, können Forscher einen Angriff nicht immer einem bestimmten Bedrohungsakteur zuordnen. Die Analyse der Angriffe, die wichtigen Bedrohungsakteuren zugeordnet werden können – wie wir das in diesem Bericht tun – bleibt dennoch ein wichtiger Teil des Sicherheitspuzzles.

BEDROHUNGSAKTEUR
„Bedrohungsakteur" ist ein von Bedrohungsforschern verwendeter Begriff, der einen Angreifer oder eine Gruppe von Angreifern bezeichnet. Dazu zählen zum Beispiel staatlich unterstützte Angreifer, organisierte Cyberkriminelle und gelegentlich Hacktivisten.

TA542

Hierbei handelt es sich um die cyberkriminelle Gruppe hinter dem berüchtigten Emotet-Botnet. Obwohl das Botnet 2020 für fünf Monate **still** war, entfielen beinahe 10 % des schädlichen E-Mail-Datenverkehrs weltweit auf die Aktivitäten dieser Gruppe. Internationalen Strafverfolgungsbehörden gelang es im Januar 2021, Emotet zu zerschlagen und die mutmaßlichen Mitglieder der Gruppe zu verhaften. Seitdem wurde beinahe keine Aktivität mehr verzeichnet.

Malware-Fallstudie: Emotet im Jahr 2020

Emotet wurde 2014 als einfacher Bank-Trojaner entdeckt und entwickelte sich bis 2020 zu einem der berüchtigsten Malware-Botnets.

Im Februar 2020 stellte Emotet seine Aktivitäten für fünf Monate ein und nahm sie im Juli wieder auf. Trotz des Ausfalls blieb Emotet die aktivste Bedrohung im Jahr 2020.

Emotet war für ein massives E-Mail-Aufkommen mit weltweiter Verteilung bekannt. Dabei kamen **mehrere Köderthemen** zum Einsatz, die in einigen Fällen zeitlich mit globalen Ereignissen zusammenfielen, darunter auch COVID-19.

Im **Oktober 2020**, einen Monat vor der Wahl des US-Präsidenten, setzte Emotet politische Themen als Phishing-Köder ein. Dabei griff Emotet Organisationen in Nordamerika, Europa, Ostasien und Ozeanien an. In der zweiten Phase wurden die Malware-Familien Qbot und The Trick genutzt.

War die Gruppe einmal in die Umgebung eines Opfers eingedrungen, verkaufte sie den Zugang an andere Bedrohungsakteure, die das System weiter kompromittierten (z. B. mit Ransomware-Angriffen, die Störungen und Kosten verursachten).

MALVERTISING
Beim Malvertising wird Schadcode in Online-Werbung eingebettet. Diese Werbung erscheint häufig auf legitimen und vertrauenswürdigen Webseiten, sodass es schwierig ist, sie am Gateway oder Endgerät zu blockieren.

TA567

Dieser Bedrohungsakteur nutzt böswillige Werbung, auch bekannt als **MALVERTISING**, die über Keitaro, ein legitimes Datenverkehr-Verteilungssystem (Traffic Distribution System, TDS) verbreitet wird. Keitaro hilft Werbetreibenden, Online-Anzeigen gezielt einzusetzen, indem Anwender auf die richtigen Webseiten geleitet werden. Statt schädliche E-Mails zu verwenden, nutzt TA567 das Keitaro-Datenverkehr-Verteilungssystem, um schädliche Inhalte über harmlose Werbung zu verteilen, damit die Malware auf legitime Websites gelangt. An sich ungefährliche E-Mails können Links zu Websites enthalten, die mit dieser kompromittierten Werbung infiziert wurden. Dadurch erhält Proofpoint Einblick in die Aktivitäten des Angreifers. Diese Bedrohungen nutzen häufig Geofencing-Techniken, um schädliche Werbung an bestimmte Regionen anzupassen.

TA544

Dieser Cyberkriminelle stiehlt Geld mit Hilfe von Bank-Trojanern und anderer Malware. Auf die Gruppe entfielen fast 4 % des weltweiten E-Mail-Aufkommens. TA544 verwendet üblicherweise Microsoft Office-Anhänge mit schädlichen Makros und bringt die Empfänger dazu, die Anhänge zu öffnen, wodurch die Makros ausgeführt und Schaddaten heruntergeladen werden. Ihre Angriffe richten sich gegen mehrere Branchen in verschiedenen Ländern, darunter Italien und Japan.

THE TRICK

Seit dem ersten Auftreten im Jahr 2016 hat sich dieser Bank-Trojaner zu einem vielseitigen Tool entwickelt, das andere Malware herunterladen, sich in einem Netzwerk ausbreiten, sich selbst aktualisieren und mehr tun kann.

BAZALOADER

BazaLoader wurde zuerst im April 2020 entdeckt und wird genutzt, um andere Malware herunterzuladen. Obwohl sie relativ neu ist, konnten wir mindestens sechs Varianten der Malware beobachten – ein Zeichen dafür, dass sie aktiv weiterentwickelt wird.

TA505

Dieser einflussreiche Bedrohungsakteur ist für die Durchführung schädlicher E-Mail-Kampagnen in einem bisher beispiellosen Umfang bekannt. Die Gruppe ändert regelmäßig ihre Taktiken, Techniken und Prozeduren (TTPs) und gilt in der Cyberkriminalitätsszene als **Trendsetter**. TA505 ist bei den Zielen nicht wählerisch und greift eine breite Palette an Branchen und Ländern an. 2020 konzentrierte sich die Gruppe bei ihren Angriffen hauptsächlich auf die USA, Kanada und deutschsprachige Teile Europas. Obwohl ihre Aktivitäten bisweilen Evil Corp. (einer cyberkriminellen Gruppe in Russland) zugeordnet werden, führen wir TA505 als separaten Bedrohungsakteur.

TA800

Dieser Bedrohungsakteur verteilt Banking-Malware und Malware-Loader, zum Beispiel **THE TRICK** (auch bekannt als TrickBot) und **BAZALOADER**. Diese Loader sind eng mit Ransomware-Angriffen der zweiten Phase verbunden, in denen Conti bzw. Ryuk eingesetzt werden. Die Gruppe war eine der ersten Bedrohungsakteure, die BazaLoader im April 2020 nutzten – Monate vor anderen Gruppen. Ihre Angriffe richten sich gegen ein breites Spektrum an Branchen in Nordamerika und machen etwa 2 % des gesamten schädlichen E-Mail-Aufkommens aus.

ABSCHNITT 3

Berechtigungen

Mithilfe einer Analyse der Berechtigungen lässt sich feststellen, wie viel Schaden ein erfolgreicher Angriff verursachen würde. Durch die Kompromittierung eines Anwenders mit umfangreichen Berechtigungen erhalten Angreifer Zugriff auf vertrauliche und wertvolle Informationen.

Bedrohungen durch Insider sind eine weitere Form des Berechtigungsmissbrauchs. Dabei spielt es keine Rolle, ob die betreffenden Anwender böswillig oder fahrlässig gehandelt haben oder kompromittiert wurden. Bei vielen Unternehmen fand praktisch über Nacht ein Wechsel ins Home Office statt, was die Überwachung und Behebung von Insider-Bedrohungen erschwerte.

Daher liegt der Fokus verstärkt auf potenziellen Gefahren wie USB-Geräten, dem Kopieren großer Dateien und Ordner (insbesondere zu ungewöhnlichen Zeiten), der Analyse von Dateifreigabediensten sowie Aktivitäten, mit denen sich Tools zur Anwenderüberwachung umgehen lassen. Die Zahl der Unternehmen, die DLP-Warnungen für die folgenden Aktivitäten festlegen, stieg erheblich im Vergleich zur Zeit vor der COVID-19-Pandemie:

Häufigste Warnungen bei der Abwehr von Insider-Bedrohungen

AKTION	RANG	VERÄNDERUNG GEGENÜBER 2019
Anschließen eines nicht gelisteten USB-Geräts	1	▲
Kopieren großer Dateien oder Ordner	2	▲
Exfiltrieren einer überwachten Datei ins Internet per Upload	3	▼
Öffnen einer Klartextdatei, die Kennwörter enthalten könnte	4	▲
Herunterladen von Dateien mit potenziell schädlichen Erweiterungen	5	▼
Kopieren großer Dateien oder Ordner außerhalb der üblichen Zeiten	6	▲
Exfiltrieren einer Datei auf nicht gelistetes USB-Gerät	7	▼
Installation von Hacker- oder Spoofing-Tools	8	▼
Zugriff auf Cloud-Dienste für Upload und Freigabe	9	▲
Öffnen des ObservelT-Agenten-Ordners	10	▲

Schlussfolgerung und Empfehlungen

Aktuelle, auf menschliches Verhalten zielende Bedrohungen können nur mit personenzentriertem Schutz abgewehrt werden.

Angreifer sehen die Welt nicht als Netzwerkdiagramm, sondern als Organigramme, Verbindungen, Beziehungen und Zugriffsmöglichkeiten.

Verwenden Sie daher eine Lösung, die Ihnen zeigt, wer wie angegriffen wird und ob die angegriffene Person geklickt hat. Berücksichtigen Sie dabei das individuelle Risiko der einzelnen Anwender, einschließlich der Informationen dazu, wie sie angegriffen werden, auf welche Daten sie zugreifen können und wie leicht sie sich täuschen lassen.

Wir empfehlen folgende Maßnahmen für personenzentrierten Schutz:

Schwachstellen

Die meisten Cyberangriffe sind nur dann erfolgreich, wenn Menschen darauf hereinfallen. Das Schließen von Schwachstellen beginnt mit Schulungen zur Sensibilisierung für Sicherheit und mit risikobasierten Kontrollen. Wir empfehlen folgende Maßnahmen:

- **Schulen Sie Ihre Anwender darin, schädliche E-Mails zu erkennen und zu melden.** Mit regelmäßigen Schulungen und simulierten Angriffen lassen sich viele Angriffe stoppen und die Menschen identifizieren, die besonders gefährdet sind. Die besten Simulationen imitieren reale Angriffstechniken. Wählen Sie daher eine Lösung, die hierfür aktuelle Trends und neueste Bedrohungsdaten einbezieht.
- **Gehen Sie davon aus, dass Anwender früher oder später auf eine Bedrohung klicken werden.** Angreifer finden immer neue Möglichkeiten, den Faktor Mensch auszunutzen. Suchen Sie nach einer Lösung, die Bedrohungen mithilfe zusätzlicher Sicherheitsebenen für Ihre anfälligsten Anwender neutralisiert.
- **Isolieren Sie riskante Websites und URLs.** Halten Sie riskante Webinhalte von Ihrer Umgebung fern, Eine solche Web-Isolierungstechnologie ist ein wichtiger Schutz für E-Mail-Konten, die von mehreren Personen genutzt werden und daher nur schwer mit Mehrfaktor-Authentifizierung abgesichert werden können. Außerdem können Sie auf diese Weise das private Surfverhalten sowie die Webmail-Services Ihrer Anwender isolieren.

Angriffe

Cyberangriffe lassen sich nicht vermeiden. Es ist jedoch möglich, sie mit den richtigen Ansätzen, Tools und Richtlinien unter Kontrolle zu bringen. Dies sind unsere Empfehlungen zur Verhinderung, Erkennung und Abwehr von Angriffen:

- **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.
- **Verhindern Sie Ransomware, indem Sie die Erstinfektion verhindern.** Die Verbreiter von Ransomware richten ihre Angriffe heute bevorzugt gegen lohnenswerte Ziele, die bereits mit einem Trojaner oder Loader infiziert wurden. Wenn Sie diese verbreiteten Malware-Formen abwehren, können Sie verhindern, Oper eines Malware-Angriffs zu werden.
- **Schützen Sie Cloud-Konten vor Übernahmen und schädlichen Apps.**
- **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.

Berechtigungen

Alle Cyberangreifer haben es auf Daten, Systeme und anderen Ressourcen abgesehen. Je mehr Berechtigungen das Opfer besitzt, desto umfangreicher die Zugriffsmöglichkeiten der Angreifer – und desto größer ist der potenzielle Schaden. Wir empfehlen folgende Maßnahmen, mit denen Sie Berechtigungen verwalten und sicherstellen können, dass diese nicht missbraucht werden:

- **Stellen Sie ein System zur Abwehr von Insider-Bedrohungen bereit**, mit dem Sie böswillige, fahrlässige und kompromittierte Anwender verhindern, erkennen und kontrollieren können. Dies ist das häufigste Szenario für Berechtigungsmissbrauch, auf das möglichst in Echtzeit reagiert werden sollte.
- **Nutzen Sie Tools für die schnelle Reaktion auf potenziellen Berechtigungsmissbrauch**, mit denen Sie herausfinden können, was vor, während und nach dem Zwischenfall geschehen ist und welche Absichten der Anwender hatte – ohne die üblichen False Positives.
- **Setzen Sie Sicherheitsrichtlinien durch** und nutzen Sie dazu bei Bedarf Anwenderschulungen, Echtzeit-Erinnerungen und Blockierungen.

Proofpoint kann Sie bei der Analyse und Behebung von Schwachstellen, Angriffen und Berechtigungsmissbrauch unterstützen – mit einem personenzentrierten Ansatz, der auch die größten aktuellen Herausforderungen für Sicherheit und Compliance bewältigt. Weitere Informationen dazu erhalten Sie unter **www.proofpoint.com/de**.

WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter **proofpoint.com/de**.

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) 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 mehr als die Hälfte der Fortune-1000-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.

0400-005-01-01 07/21