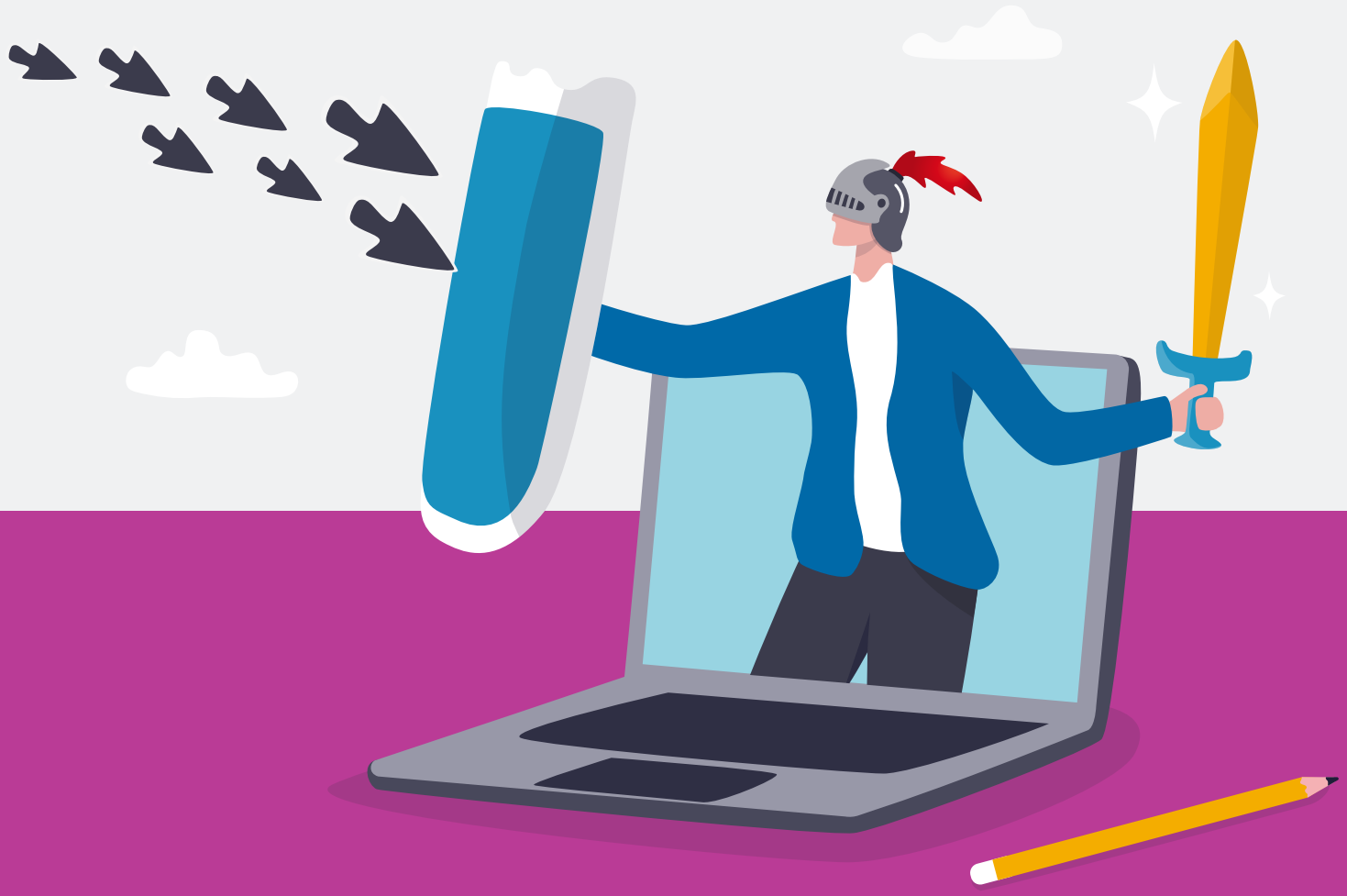
proofpoint.

E-BOOK

5 reale Cyberangriffe und wie sie gestoppt wurden

Teil 2: Technische Angriffe



Einleitung

Cyberkriminelle sind raffiniert und hochmotiviert – und sie haben allen Grund dazu. Ihre Branche wächst und bietet hohe Rendite bei geringem Risiko. Schätzungen zufolge werden die Kosten durch Cyberkriminalität bis zum Jahr 2027 auf erschreckende 23,8 Billionen US-Dollar pro Jahr steigen.[1]

Mit der Aussicht auf derart hohe Gewinne scheinen der Kreativität bei modernen Cyberangriffen keinerlei Grenzen gesetzt. Neue und raffinierte Malware-, Phishing- und Social-Engineering-Taktiken schießen jeden Tag wie Pilze aus dem Boden, während die Verteidiger in einer Art Katz-und-Maus-Spiel versuchen, sie zu stoppen. Auch wenn es scheinbar nahezu unbegrenzte Bedrohungsvarianten gibt, haben sie doch grundlegende Gemeinsamkeiten: Sie kommen per E-Mail und sie nehmen den Menschen ins Visier.

In dieser E-Book-Reihe stellen wir einige der derzeit heimtückischsten E-Mail-Angriffe vor, von denen viele mehrere Sicherheitstools umgehen konnten, bevor wir sie entdeckten. Um zu verdeutlichen, wie es dazu kommen konnte, werden wir die einzelnen Angriffe detailliert erläutern, den genauen Ablauf beleuchten und aufzeigen, wie die Cyberkriminellen menschliche Schwachstellen ausgenutzt haben. Anschließend erläutern wir, wie Proofpoint den jeweiligen Angriff stoppen konnte.

Im ersten Teil haben wir uns mit Angriffen befasst, die auf Social Engineering basieren, während es nun um technischere Angriffe geht.

1 Weltwirtschaftsforum: „2023 Was a Big Year for Cybercrime – Here's How We Can Make Our Systems Safer“ (2023 war für Cyberkriminelle sehr erfolgreich: So können wir unsere Systeme besser schützen), Januar 2024.

Inhaltsverzeichnis

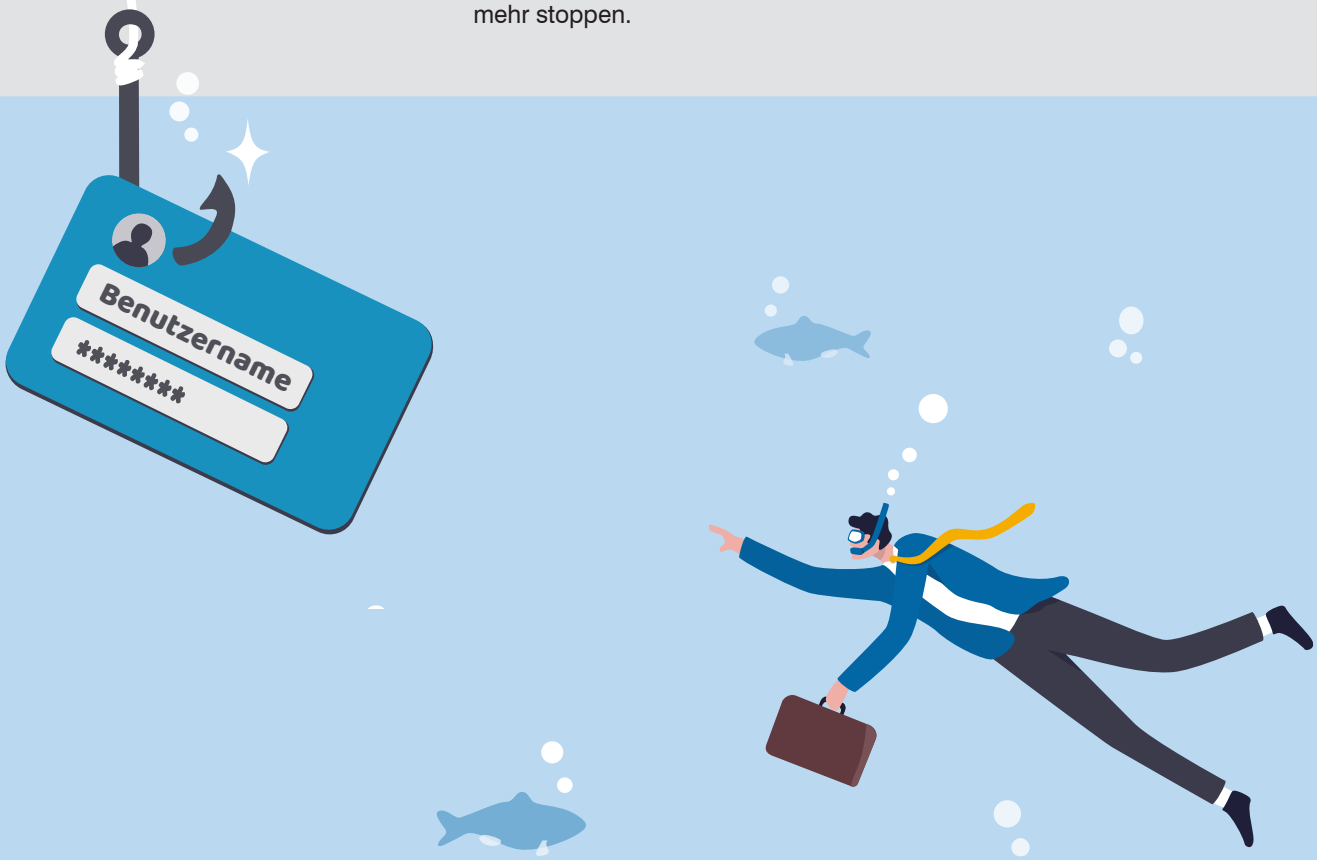
ABSCHNITT 1

Phishing-Toolkit EvilProxy

EvilProxy ist ein Phishing-Toolkit, das Anwender-Anmeldedaten und Token für Multifaktor-Authentifizierung (MFA) stehlen kann.

Dazu schaltet sich das Toolkit hinter eine legitime Website. Wenn sich Anwender mit einer Phishing-Webseite verbinden, wird ihnen eine gefälschte Anmeldeseite angezeigt, die wie das echte Anmeldeportal aussieht und sich auch so verhält. Sobald sie sich anmelden, erfasst EvilProxy ihre Anmeldedaten sowie die Authentifizierungstoken der Sitzung, sodass die kriminellen Akteure sich im Namen der Anwender anmelden und MFA-Schutzmaßnahmen umgehen können.

EvilProxy und andere Bedrohungen, die MFA umgehen, werden von kriminellen Akteuren immer häufiger als Reaktion auf verbesserte Sicherheitskontrollen genutzt. Herkömmliche Ansätze auf Basis von IP-Adressen- oder URL-Reputation können diese Bedrohungen nicht mehr stoppen.



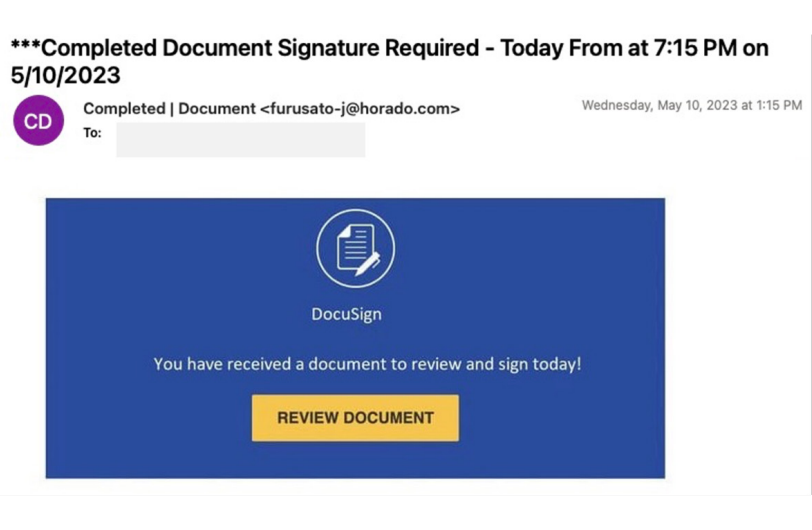
Das Szenario

Während einer Risikoanalyse für E-Mail-Sicherheit entdeckte Proofpoint bei einem Technologieunternehmen mit 1.500 Kunden einen laufenden EvilProxy-Angriff. Das Unternehmen nutzte bereits ein anderes E-Mail-Sicherheitstool, das diese Attacke jedoch nicht erkannt hatte.

Ablauf des Angriffs

Nachfolgend ein genauerer Blick auf den Ablauf dieses Angriffs:

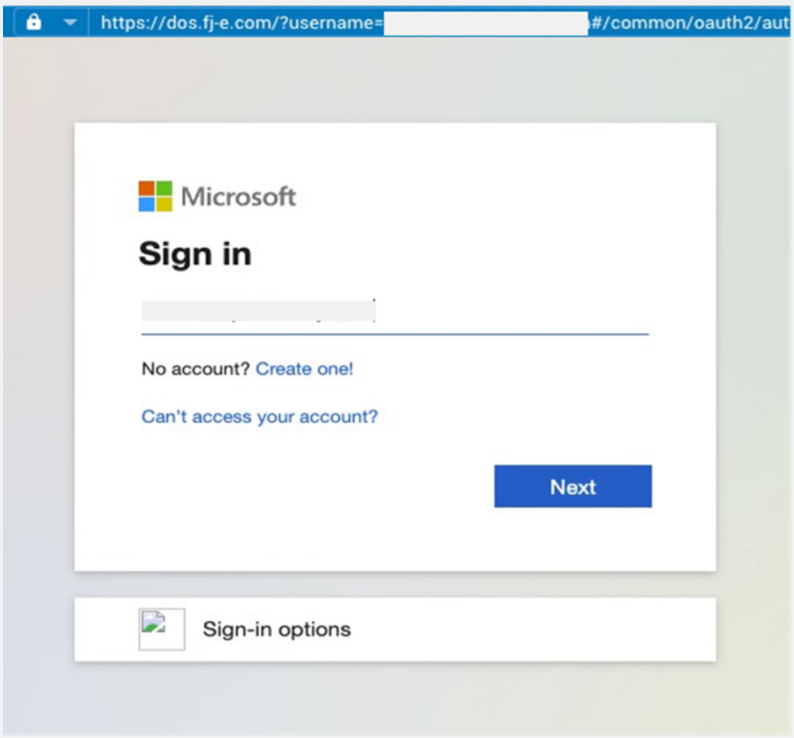
1. **Die betrügerische Nachricht.** Der Angriff begann mit einer E-Mail, die wie eine echte DocuSign-Benachrichtigung aussah, in der die Empfänger um die Unterzeichnung eines Dokument gebeten wurden. Die scheinbar harmlose Nachricht war jedoch das Einfallstor für einen raffinierten Cyberangriff.



Die gefälschte E-Mail, die der Kunde zu Beginn erhielt.

2. **Die schädliche URL.** Wenn die Empfänger auf die eingebettete URL klickten, wurden sie auf ihre eigene Microsoft-Anmeldeseite geleitet, hinter die jedoch ein Proxy-Server der Angreifer geschaltet war. Hier wurden die Anwender aufgefordert, ihre Anmeldedaten einzugeben.

3. **Das EvilProxy-Phishing-Framework.** Die treibende Kraft hinter dem Angriff. Die Angreifer nutzten eine Reverse-Proxy-Technik, um die Anmeldeversuche der Anwender über die richtige Microsoft-Anmeldeseite abzufangen. Auf diese Weise konnten sie unbemerkt MFA-Token und Anmeldedaten erfassen.



Die schädliche Microsoft-Anmeldeseite.

4. **Aushebelung der MFA-Verifizierung.** Mithilfe der MFA-Codes sowie der Anmeldedaten erlangten die Angreifer ungehinderten Zugriff auf die kompromittierten Konten. Da sie die MFA-Verifizierung umgehen konnten, stand ihnen die Unternehmensumgebung offen.

Wie Proofpoint die Bedrohung erkannt hat

Proofpoint nutzt hochentwickeltes Machine Learning (ML) zum Entschlüsseln des Kontexts eingehender Nachrichten und Analysieren des Inhalts auf potenzielle Bedrohungen. Wir analysieren den E-Mail-Text sowie den Kontext und können so feststellen, ob eine E-Mail harmlos, schädlich oder verdächtig ist. Außerdem untersuchen wir die typischen Sendemuster des Absenders. Falls in der E-Mail verdächtige Payloads enthalten sind, übermittelt Proofpoint sie zur genaueren Analyse an eine Sandbox. Dadurch können wir selbst bislang unbekannte schädliche Inhalte aufdecken.

In diesem Szenario stellte Proofpoint fest, dass die E-Mail-Nachricht aus mehreren Gründen verdächtig war. Erstens erhielt der Empfänger normalerweise keine E-Mails von diesem Absender. Außerdem verlangte der Absender vom Empfänger, eine Aktion vorzunehmen (auf die URL klicken). Da wir nicht sofort feststellen konnten, ob die URL harmlos oder schädlich ist, wurde sie zur Sicherheit in der Sandbox analysiert.

Beim Aufrufen der URL zeigte sich, dass durch Umleitungen versucht wurde, böswillige Absichten zu verbergen. Unser URL-Modul ließ sich davon nicht beirren und stellte fest, dass die Umleitung zu einer Webseite führte, die einer Microsoft-Anmeldeseite täuschend ähnlich sah. Anhand des Verhaltens dieser Webseite konnte Proofpoint ein URL-Framework aufdecken, das mithilfe eines Proxy-Dienstes die Anmeldedaten und MFA-Antworten von Anwendern in Echtzeit stehlen konnte – ein Verhalten, das für EvilProxy typisch ist. Durch das Abfangen der Anmeldedaten und MFA-Antworten in Echtzeit ist es Bedrohungsakteuren selbst bei aktiviertem MFA-Schutz schnell möglich, Zugriff auf ein Anwenderkonto zu erlangen.

Malicious URLs

Credential phish caught by machine learning engine

URL	https://bs.serving-sys.com/Serving/adServer.bs?cn=brd&PluID=0&Pos=45940487&EyeblasterID=1086486580&clk=&ctick=4849&rtu=https%3A%2F%2Fdse54net.web.app/
Rule	dc890227-7740-11e9-8d93-12ba71d80a0c

phishing url

URL	https://bs.serving-sys.com/Serving/adServer.bs?cn=brd&PluID=0&Pos=45940487&EyeblasterID=1086486580&clk=&ctick=4849&rtu=https%3A%2F%2Fdse54net.web.app/
Rule	2930c017-0415-11eb-bab7-12ba71d80a0c

Detected by rule e7461bcaf73c18c64b12ed7fbb7283e6

URL	https://bs.serving-sys.com/Serving/adServer.bs?cn=brd&PluID=0&Pos=45940487&EyeblasterID=1086486580&clk=&ctick=4849&rtu=https%3A%2F%2Fdse54net.web.app/
Rule	behavior_e7461bcaf73c18c64b12ed7fbb7283e6

Redirect Chain

A URL with multiple redirects was visited

URL	https://doc.yg-r.com/?username=redacted_email&auth=1-0.79432671181593

Zusammenfassung der von Proofpoint gemachten Beobachtungen, die zur Einstufung der E-Mail als Bedrohung geführt haben.

Behaviors

Malicious content dropped during execution

Rule	behavior_d27be4c0bb9ef4dc79fb5309c19e5b3d

ETPRO Suricata IDS Alerts

Rule	behavior_286b6c09e0dc5b5fc7664b918c773cae

SocGholish redirect domain: trademark.jgieslaclarca.com

Rule	behavior_800bd3bcf9c9fc40f2ce1212d47b0b76

SocGholish compromised script detected: http://jc.efleasing.com/wp-content/plugins/elementor/assets/lib/swiper/swiper.min.js?ver=5.3.6

Rule	behavior_800bd3bcf9c9fc40f2ce1212d47b0676

Erkennung des EvilProxy-Phishing-Frameworks durch Proofpoint.

ABSCHNITT 2

SocGholish-Angriff

SocGholish ist eine Malware-Familie, die mindestens seit 2018 im Umlauf und bis heute sehr erfolgreich ist. Aufgrund sehr unterschiedlicher Ausführungsphasen, Voraussetzungsprüfungen und Verschleierungsroutinen gehört sie zu den am schwersten fassbaren Malware-Familien. Bislang sind keine Details dazu bekannt, wie die Malware ihre Ziele auswählt, mit welcher Logik sie Erkennungen vermeidet und welche Zwischenphasen sie konkret nutzt, was sie noch geheimnisvoller macht.

Grundsätzlich erfolgt ein SocGholish-Angriff in vier Phasen:

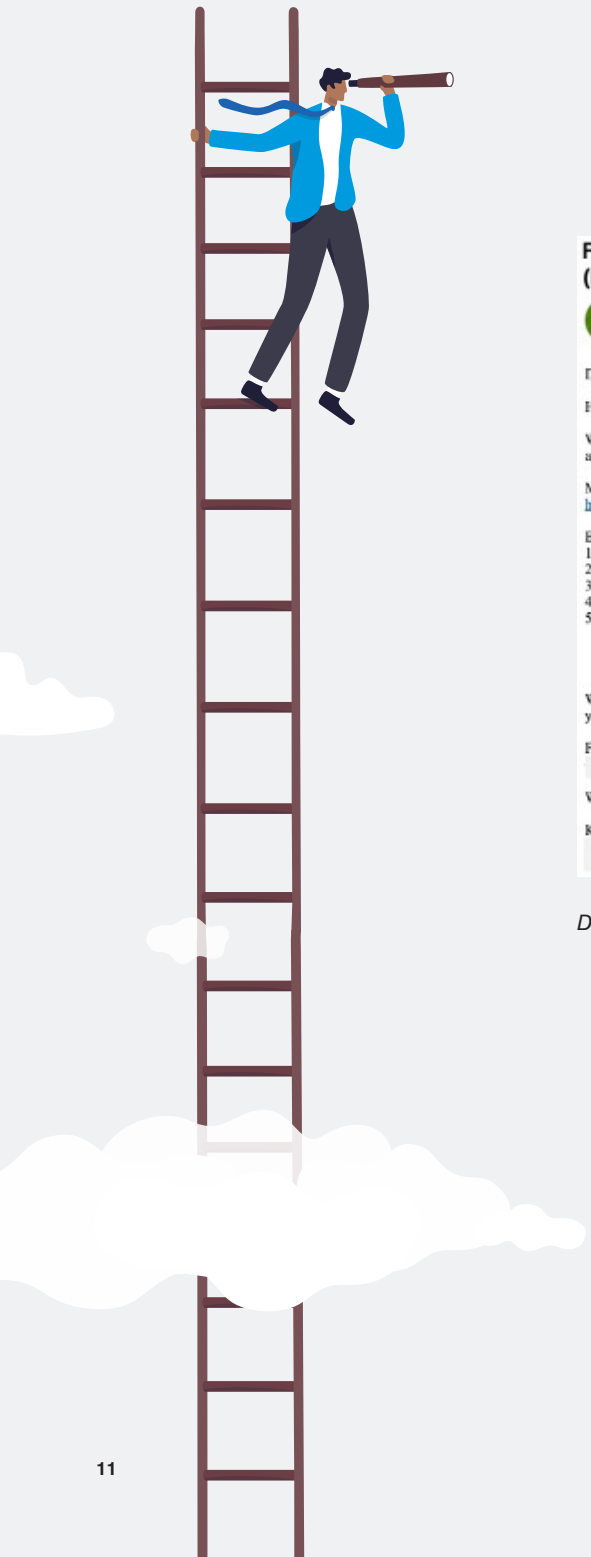
Phase 1: Schädliche Injektionen
Ein Bedrohungsakteur kompromittiert eine legitime Website und injiziert schädlichen JavaScript-Code, der Profile von Anwendern erstellt, um ideale Kandidaten für weitere Angriffe zu finden.

Phase 2: SocGholish-Download
Wenn ein Anwender bestimmte Kriterien erfüllt, versucht der JavaScript-Code, ihm SocGholish unterzuschieben, oft getarnt als gefälschtes Browser-Update. Falls der Anwender darauf klickt, wird SocGholish auf sein Gerät heruntergeladen.

Phase 3: Nach Hause telefonieren
Anschließend baut die Malware einen Kommunikationskanal zu C&C-Proxys (Command-and-Control) auf, um weitere Anweisungen zu erhalten.

Phase 4: Nachfolgende Malware und Infektion
SocGholish setzt die Profilerstellung auf dem Anwendergerät fort und kontaktiert danach die C&C-Server, um nachfolgende Malware herunterzuladen, meist Remote-Zugriffs-Trojaner oder Ransomware.

Der Schutz vor SocGholish ist ausgesprochen schwierig. Die Malware ist weit verbreitet und kann selbst die fortschrittlichsten E-Mail-Sicherheitstools unterlaufen. Innerhalb eines einzigen Monats des Jahres 2023 stellte Proofpoint fest, dass SocGholish in tausenden Fällen den Sicherheitsmaßnahmen entgehen konnte.



Das Szenario

Während einer Risikoanalyse für E-Mail-Sicherheit entdeckten wir bei einem Technologieunternehmen mit 4.000 Anwendern einen laufenden SocGholish-Angriff. Die vorhandene E-Mail-Sicherheitslösung hatte die Bedrohung nicht erkannt.

Ablauf des Angriffs

Nachfolgend ein genauerer Blick auf den Ablauf dieses Angriffs:

1. **Die ursprüngliche Nachricht.** Anwender erhielten eine E-Mail mit der Einladung, ein Paper zur Veröffentlichung in einem bekannten Wissenschaftsjournal einzureichen. Dabei war die E-Mail selbst weder schädlich, noch stammte sie von einem Bedrohungsakteur. Wie für SocGholish-Kampagnen typisch, kam schädlicher Code erst ins Spiel, als der Anwender auf die kompromittierte – aber legitime – Website gelangt war.

Follow up: Paper Invitation: [Environment and Social Psychology] (Indexed in Scopus) is Open for Submission

TS

To:

Thursday, June 29, 2023 at 6:05 AM

Dear

Hope this mail finds you well.

We were wondering if you have received our paper invitation for the journal *Environment and Social Psychology*. We are writing to inquire if you are interested in submitting a paper for publication in this journal.

More information can be found on the website:
https://esp.apacsci.com/index.php/esp/index

Benefits of publishing with ESP:
1.Open access (unlimited and free access for readers).
2.Indexed by the Scopus, NLB, Portico, and other databases.
3.Fast Publication combined with thorough peer review.
4.As indicated on the website, the APC of USD 1250 in 2023 applies to submitted papers.
5.We will provide discount for early bird submission:
*Early Bird Submission before July 31, 2023: 90%
*Early Bird Submission before August 31, 2023: 60%
*Early Bird Submission before September 30, 2023: 50%

We cordially invite you to submit a paper. In addition, we would appreciate it if you could recommend this journal to your colleagues. If you are interested, please kindly let us know.

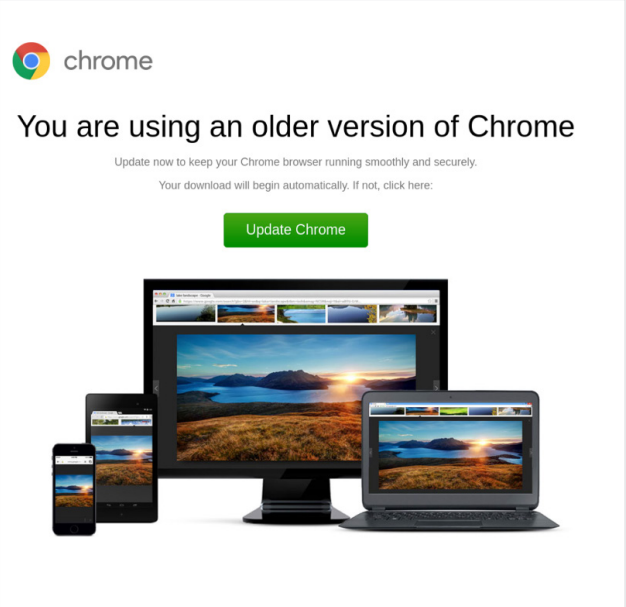
For any questions regarding technical issues or applying discount, please feel free to contact

We look forward to hearing from you.

Kind regards,

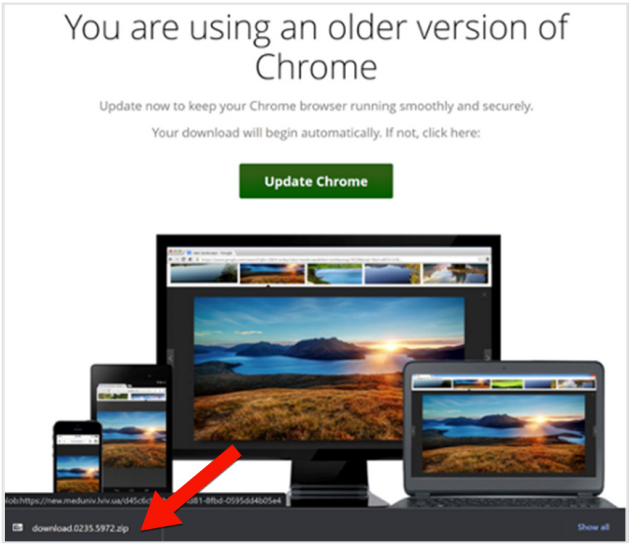
Die ursprüngliche E-Mail, die bei unserem Kunden einging.

2. **Die kompromittierte URL.** Sobald der Anwender auf die URL in der E-Mail geklickt hat, startete der am Ziel injizierte JavaScript-Code die Profilerstellung, um festzustellen, ob dieser Anwender sich für weitere Angriffe eignete. Einigen Anwendern wurde eine ganzseitige Popup-Meldung angezeigt, die sie zur Aktualisierung ihres Browsers aufforderte.



Die gefälschte Aufforderung zum Aktualisieren des Browsers.

3. **Installation von SocGholish.** Nachdem das Update-Paket heruntergeladen wurde, erstellte SocGholish ein Profil des Geräts, seiner Konfiguration und seiner Zugriffsmöglichkeiten. SocGholish kontaktierte dann C&C-Proxys für weitere Anweisungen und mögliche nachfolgende Malware.



Die vom gefälschten Browser-Update heruntergeladene Datei.

Schwierigkeiten bei der Erkennung dieser Bedrohungen

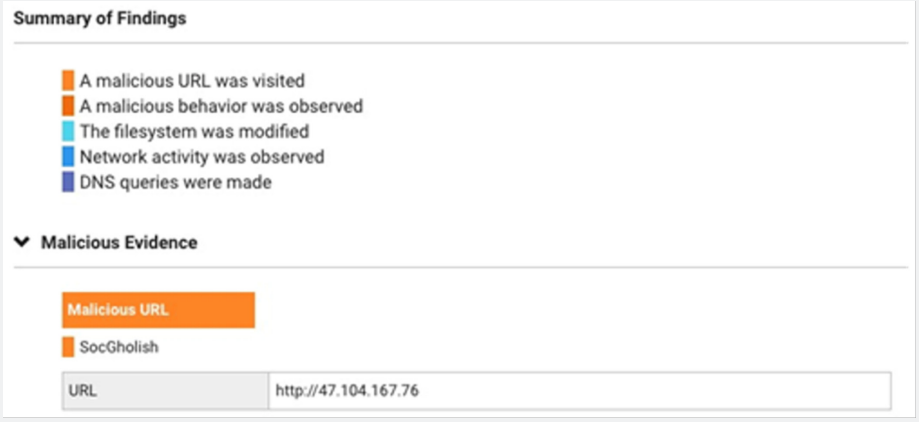
Die meisten E-Mail-Sicherheitstools können schädlichen JavaScript-Code erkennen, doch SocGholish ist von Natur aus gut getarnt. Insbesondere fällt es vielen E-Mail-Sicherheitstools schwer, die Profilerstellungstechniken der Malware zu erkennen, d. h. die Überprüfung der IP-Adresse, des Betriebssystems, des Browsers sowie der lokalen Sprache. Tools, die ausschließlich auf Anomalieerkennung setzen, haben Probleme mit Angriffen wie SocGholish, da sowohl die E-Mail-Nachricht als auch die URL legitim sind.

SocGholish nutzt zudem Taktiken zum Erkennen und Umgehen von Sandbox-Analysen. Wenn die Malware eine simulierte Umgebung wie eine Bedrohungsanalyse-Sandbox erkennt, wird sie nicht aktiv. Auch E-Mail-Sicherheitstools, die Bedrohungen mit KI/ML analysieren, haben bei der Erkennung von SocGholish Schwierigkeiten, da die E-Mail-Nachricht selbst nicht schädlich ist und aufgrund früherer Sendemuster auch nicht als ungewöhnlich eingestuft wird.

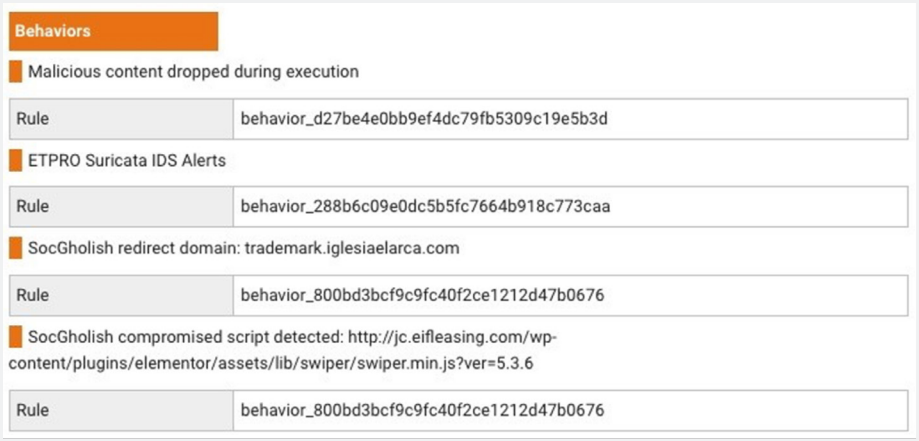
Wie Proofpoint die Bedrohung erkannt hat

Proofpoint erkennt mithilfe umfangreicher URL-Analysen verschiedene verdächtige, für SocGholish typische Verhaltensweisen wie Profilerstellung. Durch die Analyse von Netzwerkaktivitäten können wir Malware identifizieren, die mit C&C-Proxys kommuniziert. Zudem können wir eine weitere bei SocGholish beobachtete Taktik aufdecken: die Umleitung an einen DNS-Dienst und den Missbrauch kompromittierter Skripte.

In diesem Szenario entdeckte Proofpoint mehrere ungewöhnliche Sendemuster und schloss die URLs in eine Sandbox ein, bevor Anwender darauf klicken konnten. Die vorausschauende Sandbox-Analyse bestimmter URLs ist ein Alleinstellungsmerkmal von Proofpoint, durch das wir neue und bislang unbekannte URL-Bedrohungen aufdecken können.



Der Forensik-Bericht im Proofpoint TAP-Dashboard zeigt Aktivitäten, die auf einen SocGholish-Angriff hinweisen.



Der Forensik-Bericht im Proofpoint TAP-Dashboard zeigt konkrete Verhaltensweisen, die auf einen SocGholish-Angriff hinweisen.

Proofpoint priorisiert häufige und gründliche URL-Scans. Der Bedrohungsakteur TA569, der in Verbindung mit SocGholish beobachtet wird, ist für seine persistente Kontrolle von Websites bekannt, die er mit Injektionen angegriffen hat. Wir haben Vorfälle beobachtet, bei denen bereinigte Webseiten mit ähnlichen oder unterschiedlichen Injektionen erneut kompromittiert wurden.

Daher isolieren wir URLs proaktiv in Sandbox-Umgebungen, selbst nachdem sie als sicher oder sauber eingestuft wurden. Durch kontinuierliche Überwachung können wir sicherstellen, dass potenzielle Kompromittierungen oder Missbrauchsversuche sofort aufgedeckt werden.

ABSCHNITT 3

Phishing mit QR-Codes

Beim QR-Code-Phishing wird der Ansatzpunkt des Angriffs von der geschützten E-Mail-Umgebung zum Anwender-Mobilgerät verschoben, das häufig weit weniger sicher ist.

Bei QR-Codes wird die URL nicht im E-Mail-Text angezeigt, sodass die meisten E-Mail-Sicherheitsscans unwirksam sind. Zudem wird die Entschlüsselung von QR-Code-Betrug mithilfe von Texterkennung (Optical Character Recognition, OCR) schnell ressourcenintensiv und lässt sich nur schwer skalieren.

Das Szenario

Proofpoint konnte vor Kurzem einen solchen Angriff auf ein Landwirtschaftsunternehmen mit mehr als 16.000 Mitarbeitern aufdecken. Ein Bedrohungsakteur hatte einen Phishing-Köder erstellt, der wie die Gehaltsinformationen eines Mitarbeiters aussah. In der E-Mail wurde der Mitarbeiter aufgefordert, einen QR-Code mit seinem Mobilgerät einzuscannen, um auf die Informationen zuzugreifen, anstatt auf einen Link zu klicken. Der QR-Code führte zu einem gefälschten SharePoint-Anmeldebildschirm, der die Anmeldedaten des Mitarbeiters abfragte.

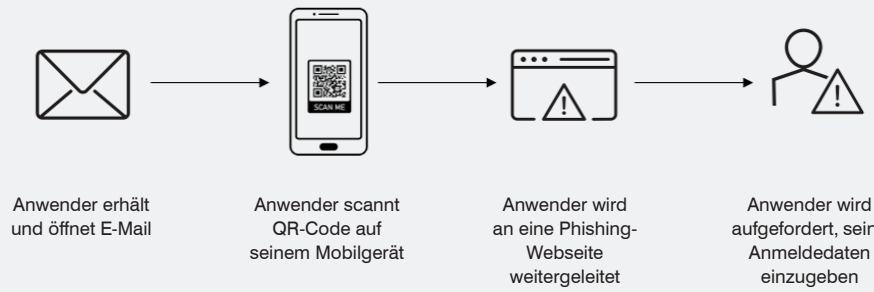
Ablauf des Angriffs

Nachfolgend werfen wir einen Blick auf den Ablauf des Angriffs:

1. **Die betrügerische Nachricht.** Der Mitarbeiter erhielt eine E-Mail, die scheinbar von der Personalabteilung seines Arbeitgebers stammte und angeblich Gehaltsinformationen enthielt.

Diese schädliche E-Mail wurde von Proofpoint blockiert, noch bevor sie den Posteingang des Anwenders erreichte. (Hinweis: Aus Sicherheitsgründen haben wir den schädlichen QR-Code ersetzt und verlinken stattdessen auf Proofpoint.com. Der übrige E-Mail-Inhalt ist ein teilweise unkenntlich gemachter Screenshot der Originalnachricht.)

2. **Abfolge des QR-Code-Angriffs.** Der Mitarbeiter wurde aufgefordert, den QR-Code mit seinem Mobilgerät zu scannen.



Typische Abfolge des QR-Code-Angriffs.

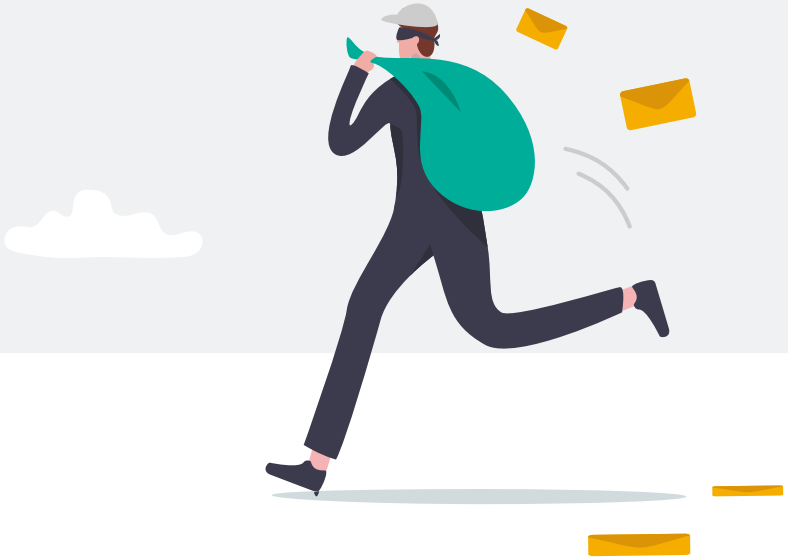
3. **SharePoint-Phishing-Köder.** Nachdem der Mitarbeiter die URL dekodiert hatte, wurde mit einem gefälschten SharePoint-Anmeldebildschirm versucht, ihn zum Eingeben seiner Anmeldedaten zu verleiten.

Dekodierter QR-Code, der den Anwender zur SharePoint-Phishing-Seite weiterleitet.

Schwierigkeiten bei der Erkennung dieser Bedrohungen

Fakt ist, dass die Phishing-URL in einem QR-Code sich nicht leicht extrahieren und scannen lässt und die Allgegenwärtigkeit von QR-Codes ein weiteres Problem darstellt. Die meisten harmlosen E-Mail-Signaturen enthalten Logos, in Bilder eingebettete Links zu sozialen Netzwerken und sogar QR-Codes, die zu legitimen Websites führen. Das Vorhandensein eines QR-Codes ist also kein sicheres Anzeichen für Phishing.

Häufig versuchen Sicherheitstools, diese Bedrohungen allein durch die Auswertung ungewöhnlicher Sendemuster zu stoppen. Dies ist jedoch eine schwache Basis für die Einstufung einer Nachricht und kann dazu führen, dass harmlose E-Mails als schädlich klassifiziert werden. Das ist vor allem bei solchen E-Mail-Sicherheitstools der Fall, die Bedrohungen nach der Zustellung abzuwehren versuchen.



Wie Proofpoint die Bedrohung erkannt hat

Proofpoint nutzt eine hochentwickelte Kombination von Indikatoren und Analysestufen, um zwischen manipulierten und harmlosen QR-Codes zu unterscheiden. Wir erstellen Analysen und Profile für folgende Faktoren:

- Absender
- Sendemuster
- Beziehung zwischen Absender und Empfänger basierend auf ihrer früheren Kommunikation

Anhand dieser Indikatoren können wir verdächtige Absender identifizieren und feststellen, ob sie gegen ein etabliertes Profil verstoßen. Unsere Systeme hatten vorher nie festgestellt, dass der Absender aus diesem Beispiel mit diesem Unternehmen oder Empfänger kommuniziert hat.

Indikatoren, die Proofpoint zur Einstufung der Nachricht als Bedrohung verwendet hat.

Wir nutzen jedoch nicht nur ungewöhnliche Sendemuster. Proofpoint kombiniert viele weitere Indikatoren, um die Art und Metonymie des E-Mail-Inhalts festzustellen und so die Anzahl der False Positives zu reduzieren. (Eine Metonymie ist ein Wort oder eine Phrase, um etwas anderes darzustellen, z. B. das Weiße Haus für die US-amerikanische Regierung. Mit diesen Analysen können wir die Absichten des Absenders feststellen, unabhängig davon, welche Wörter er nutzt.)

Dazu überprüfen wir den E-Mail-Verlauf des Absenders und führen eine linguistische und semantische Analyse des E-Mail-Textes durch. Dank dieses Ansatzes konnten wir Formulierungen in der E-Mail entdecken, mit denen der Empfänger aufgefordert wurde, Aktionen durchzuführen – in diesem Fall einen QR-Code mit seinem Mobilgerät scannen.

Abgesehen von der Verhaltens- und Sprachanalyse entdeckten wir außerdem Täuschungsversuche in den Nachrichtenheadern. Bedrohungsakteure versuchen häufig, vertrauenswürdige Einrichtungen oder andere Mitarbeiter zu imitieren, um das Vertrauen der Nachrichtenempfänger zu gewinnen. In diesem Fall erstellten die Bedrohungsakteure E-Mail-Header, die scheinbar von der Personal- und der Finanzabteilung des Arbeitgebers stammten.

Wir gingen sogar noch einen Schritt weiter und analysierten den QR-Code. Mithilfe der OCR- und Bilderkennungstechnologie in unseren Erkennungsmodulen konnten wir die im QR-Code versteckten schädlichen URLs scannen und aufdecken. Wir extrahierten URLs sowie Text und konnten so sicherstellen, dass alle wichtigen E-Mails zugestellt werden, während schädliche Nachrichten blockiert oder unschädlich gemacht werden.

ABSCHNITT 4

MFA-Manipulation

Manipulationen der Multifaktor-Authentifizierung (MFA) stellen für Cloud-Plattformen eine erhebliche Bedrohung dar. Bei dieser raffinierten Technik infiltrieren Bedrohungsakteure ihre eigene MFA-Methode in ein kompromittiertes Cloud-Konto.

Bedrohungsakteure haben mehrere Möglichkeiten zum Umgehen von MFA, eine davon sind AiTM-Angriffe (Adversary-in-the-Middle). Dabei fügt der Bedrohungsakteur einen Proxy-Server zwischen das Opfer und die Website ein, bei der er sich anmelden möchte. Dadurch kann er das Anwenderkennwort sowie das Session-Cookie stehlen.

Für den Anwender gibt es kein Anzeichen, dass er gerade angegriffen wird – er meldet sich scheinbar vollkommen normal bei seinem Konto an. Die Angreifer haben jedoch alles, was sie zum Etablieren von Persistenz benötigen, d. h. sie behalten Zugriff selbst dann, wenn die gestohlenen MFA-Anmeldedaten gesperrt oder für ungültig erklärt werden.

MFA-Manipulationsangriffe kommen nach einer Cloud-Kontoübernahme zum Einsatz – und wir beobachten diese Art von Angriff erschreckend häufig. Im Jahr 2023 stellten Proofpoint-Forscher fest, dass fast alle Unternehmen (96 %) mit Cloud-basierten Attacken angegriffen wurden. Außerdem wurden 60 % erfolgreich kompromittiert und verzeichneten mindestens ein übernommenes Konto.

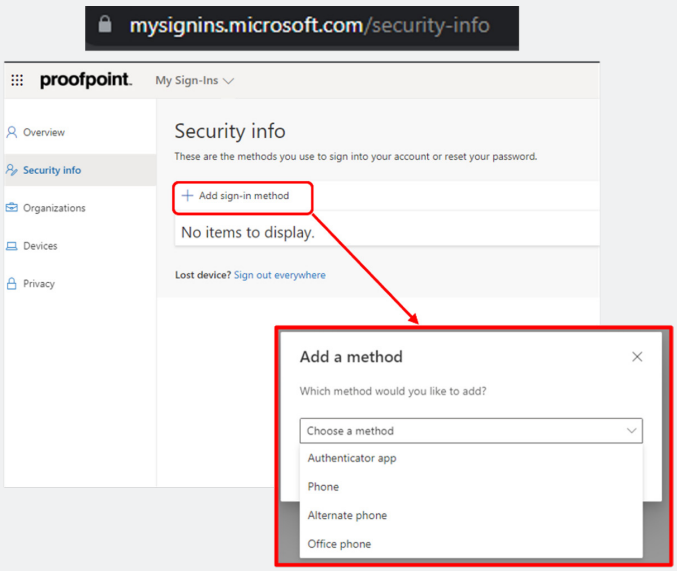
Das Szenario

Proofpoint konnte eine Reihe von MFA-Manipulationsangriffen auf eine große Immobiliengesellschaft abfangen. In einem Fall gelangt es den Bedrohungsakteuren mit einem AiTM-Angriff, die Anmeldedaten des Finanzcontrollers des Unternehmens sowie dessen Session-Cookie zu stehlen. Anschließend meldeten sie sich beim Geschäftskonto des Anwenders an und führten 27 unbefugte Zugriffsaktivitäten durch.

Ablauf des Angriffs

Nachfolgend ein genauerer Blick auf den Ablauf dieses Angriffs:

1. **Sicherung eines Brückenkopfes.** Bedrohungsakteure nutzen die native Funktion „Meine Anmeldungen“ zum Hinzufügen ihrer eigenen MFA-Methoden, mit denen sie Microsoft 365-Konten kompromittieren. Wir beobachteten, dass die Angreifer ihre eigene Authenticator-Anwendung mit Benachrichtigung und Code registrierten, nachdem sie im Rahmen eines automatisierten Angriffs Zugriff auf das gekaperte Konto erlangt hatten. Dadurch konnten sie sich einen Brückenkopf in der angegriffenen Cloud-Umgebung sichern.



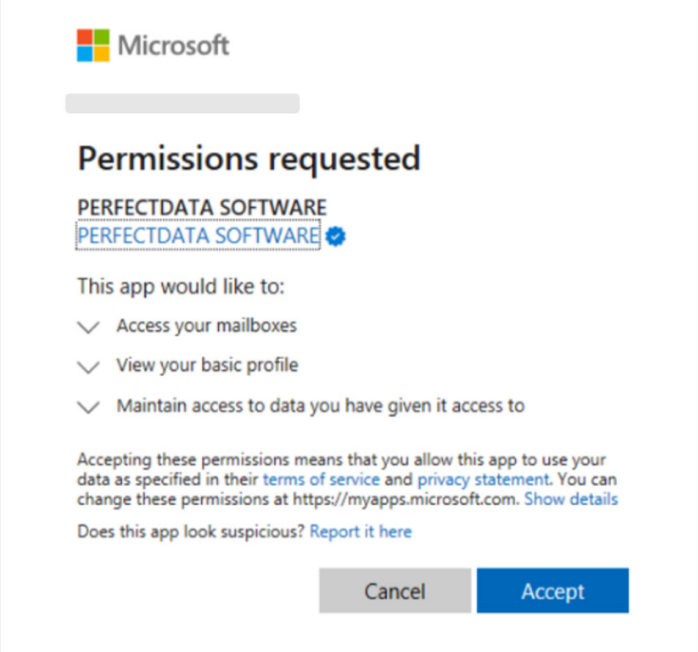
Der typische MFA-Manipulationsablauf mit der Microsoft-Funktion „Meine Anmeldungen“.

2. **Kombination von Angriffstaktiken.** Die Angreifer nutzten einen sehr raffinierten Angriff, bei dem sie MFA-Manipulation mit dem Missbrauch der OAuth-Anwendung kombinierten. Kurz gesagt nutzt ein Angreifer beim OAuth-Missbrauch eine Drittanbieter-Anwendung zum Diebstahl von Daten, Verteilen von Malware oder Anrichten von Schäden.

3. **Erlangen von dauerhaftem Zugriff.** Angreifer nutzen zudem eine missbrauchte Anwendung, um selbst dann Persistenz zu gewährleisten, nachdem ihr Erstzugriff auf ein kompromittiertes Konto unterbunden wurde. In diesem Fall autorisierten die Angreifer die scheinbar harmlose Anwendung PERFECTDATA SOFTWARE, um dauerhaften Zugriff auf das Anwenderkonto und die Systeme sowie seine Ressourcen und Anwendungen zu erhalten. Für diese Anwendung forderten die Angreifer die folgenden Berechtigungen an:

    - Dauerhafter Vollzugriff auf das Anwenderpostfach
    - Offline-Zugriff auf Daten
    - Zugriff auf das Anwenderprofil

Wenn diese Berechtigungen gewährt wurden, hatten die Angreifer ungehinderten und kontinuierlichen Zugriff auf vertrauliche Daten. Es wäre für sie kein Problem, Bedrohungen an interne oder externe Anwenderkonten zu verteilen.



Die Berechtigungsanfrage für die Anwendung PERFECTDATA SOFTWARE mit Details zu den angeforderten Berechtigungen.

Schwierigkeiten bei der Erkennung dieser Bedrohungen

Diese mehrstufigen Schritte missbrauchen legitime Cloud-Funktionen und fügen sich nahtlos in reguläre Aktivitäten ein, sodass sie klassischen Sicherheitsmaßnahmen häufig entgehen. Andere Anbieter sind derart auf isolierte Ereignisse konzentriert, dass sie Schwierigkeiten haben, Verbindungen zu ziehen.

Wie Proofpoint die Bedrohung erkannt hat

Proofpoint untersucht mithilfe verschiedener Strategien, z. B. anhand interner Bedrohungsdaten-Feeds sowie Analysen des Anwenderverhaltens (User and Entity Behavior Analytics, UEBA), wie die Angreifer in die Umgebung gelangt sind und wie sie nach der Kompromittierung vorgegangen sind.

Unsere nächsten Schritte bestanden darin, die Behebung der schädlichem Sessions zu automatisieren und die gefährliche Anwendung PERFECTDATA SOFTWARE zu sperren. Dadurch konnte das Sicherheitsteam der Immobiliengesellschaft sofortige Behebungsmaßnahmen starten.

Außerdem wurde das Unternehmen während der Untersuchung dieses Zwischenfalls von den Cloud-Bedrohungsforschern von Proofpoint beraten. Dank ihrer Hilfe konnte sichergestellt werden, dass alle vom Angreifer kontrollierten MFA-Methoden dauerhaft entfernt wurden und in Zukunft kein Risiko mehr bestand.

Die Details zur gesperrten Drittanbieter-Anwendung.

ABSCHNITT 5

Mehrstufiger QR-Code-Angriff

Bei einem QR-Code-Angriff wird der schädliche QR-Code meist in eine E-Mail eingebettet. Vor Kurzem haben sich Angreifer jedoch eine neue und noch raffiniertere Vorgehensweise ausgedacht. Bei diesen mehrstufigen Angriffen wird der schädliche QR-Code in einem scheinbar harmlosen angehängten PDF-Dokument versteckt.

Um die automatisierte Erkennung zu erschweren und klassische E-Mail-Sicherheitstools auszumanövrieren, nutzen die Angreifer Umgehungstaktiken wie CAPTCHAs auf der Landing Page. Dadurch ist es für Tools mit klassischer URL-Reputationserkennung äußerst schwer, solche Bedrohungen zu identifizieren.

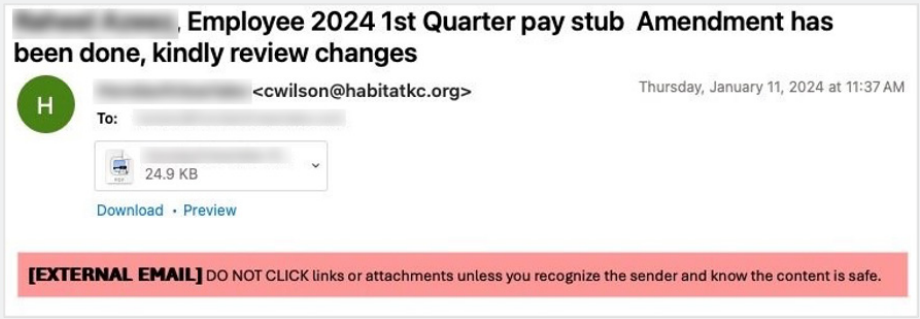
Das Szenario

Vor Kurzem führte Proofpoint eine Bedrohungsbewertung bei einem US-Automobilhersteller mit 11.000 Angestellten durch und fand eine dieser Bedrohungen. Die vorhandenen Sicherheitstools des Unternehmens – ein API-basiertes E-Mail-Sicherheitstool sowie die systemeigene Sicherheitslösung – sollten angeblich QR-Codes scannen können, stuften jedoch beide die E-Mail als harmlos ein und leiteten sie an den Endnutzer weiter.

Die Bedrohung: Wie lief der Angriff ab?

Nachfolgend ein genauerer Blick auf den Ablauf dieses Angriffs:

1. **Täuschender Köder.** Die E-Mail wirkte täuschend echt und forderte dringend zur Abgabe der Steuererklärung auf, was den Empfänger dazu verleitete, eine angehängte PDF-Datei zu öffnen.

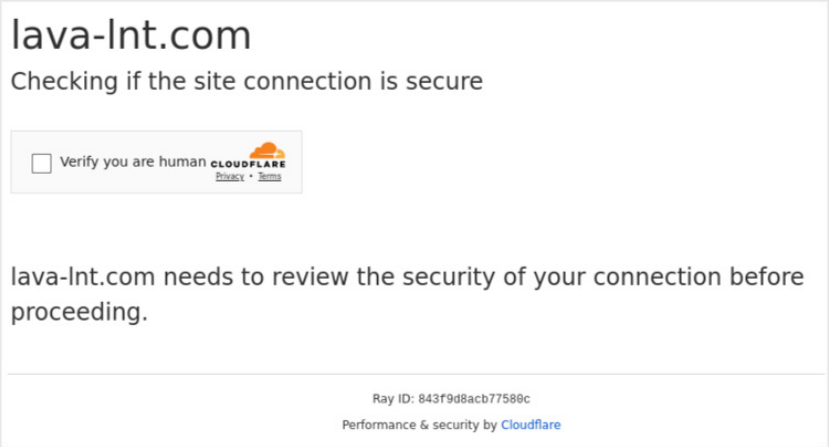


Ursprüngliche E-Mail an den Endnutzer.

2. **Schädlicher QR-Code in der PDF-Datei.** Im Gegensatz zu früheren QR-Code-Angriffen war die schädliche URL in der E-Mail nicht direkt sichtbar, sondern in der angehängten PDF-Datei verborgen. Angesichts der Verbreitung von QR-Codes wurde der Empfänger deshalb nicht misstrauisch.

Die angehängte PDF-Datei mit dem eingebetteten QR-Code (unkenntlich gemacht).

3. **Cloudflare-CAPTCHA-Abfrage.** Der Angreifer beschränkte sich jedoch nicht nur auf eine Täuschungsebene, sondern nutzte eine Cloudflare-CAPTCHA-Abfrage auf der Landing Page der QR-Code-URL, um die dahinter liegende Bedrohung weiter zu verbergen. Mit diesem Schritt sollten Sicherheitstools unterlaufen werden, die sich auf URL-Reputationsanalysen beschränken.



Cloudflare-CAPTCHA-Abfrage auf der Landing Page der QR-Code-URL.

4. **Letzte Stufe – Anmeldedaten-Phishing.** Nach dem Bestätigen der CAPTCHA-Abfrage führte der schädliche QR-Code zu einer Phishing-Landing Page, auf der die Anmeldedaten erfasst wurden. Durch den Diebstahl der Anmeldedaten können Bedrohungsakteure auf ein Anwenderkonto zugreifen und weitere interne Angriffe durchführen. Ebenso sind jedoch auch externe Angriffe möglich, bei denen sie Partner oder Lieferanten mit BEC-Attacken (Business Email Compromise) täuschen.

Schwierigkeiten bei der Erkennung dieser Bedrohungen

Beim Aufdecken von QR-Code-Bedrohungen sind OCR (Optical Character Recognition) und andere QR-Code-Scantechniken unverzichtbar. Sie sind jedoch lediglich der Mechanismus, mit dem die versteckte URL extrahiert wird, und können nicht zwischen legitimen oder schädlichen QR-Codes unterscheiden.

Viele Tools, darunter auch die beim Automobilhersteller vorhandenen E-Mail-Sicherheitstools, lesen angeblich QR-Codes und extrahieren die URL zur Analyse. Sie können jedoch keine URLs in einem eingebetteten Bild in einem Anhang scannen.

Wie Proofpoint die Bedrohung erkannt hat

Nur wenige Tools führen URL-Tiefenanalysen in großem Maßstab durch, so wie Proofpoint das kann. Wir kombinieren QR-Code-Scans mit mehrschichtigen Erkennungstechnologien, die auf hochentwickelte KI und ML setzen. Da wir die URL und ihr Verhalten analysieren, verstehen wir den Kontext von E-Mail-Nachrichten und erkennen raffinierte URL-Bedrohungen, die anderen Tools entgehen.

Mit diesen Methoden konnten wir diese Bedrohung erkennen und stoppen:

QR-Code-Scans: Proofpoint konvertierte Bilder mithilfe von QR-Code-Scans in ein maschinenlesbares Format und konnte so die verborgene URL zur weiteren Analyse extrahieren. Unsere QR-Code-Scans unterstützen PDF-Dateien, E-Mail-Text, Bilder, Microsoft Word-Dateien und viele andere Formate.

Verhaltensindikatoren: Proofpoint analysierte das Anwenderverhalten, den E-Mail-Kontext sowie das Thema der E-Mail und fand Muster, die auf eine wahrscheinliche Gefährlichkeit der E-Mail hinwiesen.

URL-Sandbox-Analysen: Nach dem Extrahieren der URL in einer Sandbox konnte Proofpoint visuelle Elemente, Weiterleitungen, Endpunktprozesse, Netzwerkaktivitäten, DNS-Aufrufe sowie CPU- und Speicherprozesse analysieren. Dabei können wir auch Umgehungstaktiken wie CAPTCHAs erkennen. Selbst wenn die URL harmlos erscheint (obwohl Verhaltensindikatoren auf gefährliche Aktivitäten hinweisen), überwachen und überprüfen wir sie weiterhin, um spätere Kompromittierungen oder Angriffsversuche festzustellen.

ABSCHNITT 6

Fazit

Alle diese Betrugstaktiken zeigen deutlich, warum zuverlässige und mehrschichtige Cybersicherheitsmaßnahmen unverzichtbar sind.

Um mit der Entwicklung solcher Bedrohungen Schritt zu halten, benötigen Sie einen umfassenden Ansatz zum Schutz vor personenzentrierten Bedrohungen:

- **Erkennen Sie Bedrohungen vor der Zustellung.** Sie können Ihre Anwender nur schützen, wenn Sie schädliche Nachrichten blockieren, bevor sie zugestellt werden. Untersuchungen von Proofpoint haben gezeigt, dass jeder siebte Anwender schädliche E-Mails innerhalb von einer Minute nach der Zustellung anklickt. Wählen Sie deshalb ein Tool, das ML-gestützte Algorithmen und erweiterte Bedrohungsdaten kombiniert, um komplexe Bedrohungen zu identifizieren und zu blockieren.
- **Schulen Sie Ihre Anwender.** Ihre Mitarbeiter, Auftragnehmer und Partner sind die erste Verteidigungslinie Ihres Unternehmens. Stellen Sie sicher, dass sie Security-Awareness-Schulungen zu allen Arten von Angriffen erhalten. Erinnern Sie sie daran, ungewöhnliches Verhalten von E-Mail-Absendern umgehend zu melden.
- **Führen Sie regelmäßig Audits durch.** Anhand von Audits lassen sich potenzielle Schwachstellen in Ihrer Umgebung einfacher identifizieren. Achten Sie auf Unregelmäßigkeiten in Ihren Konfigurationen und Zugriffsprotokollen.
- **Richten Sie Ihr System für die Überwachung von Konfigurationsfehlern ein.** Suchen Sie dabei nicht nur nach fehlerhaften Konfigurationen, sondern aktivieren Sie auch die automatische Behebung, damit unerlaubte Änderungen rechtzeitig und schnell korrigiert werden. Dadurch verhindern Sie, dass Angreifer Persistenz aufbauen können.
- **Erstellen Sie einen Plan für die Reaktion auf Zwischenfälle.** Definieren Sie mehrere Angriffsszenarien und legen Sie fest, wie Sie diese untersuchen und beheben werden. Testen Sie, wie effektiv Ihr Plan tatsächlich ist, indem Sie regelmäßige Simulationen durchführen.

Die nächsten Schritte

Der Schutz Ihres Unternehmens ist angesichts der zunehmenden E-Mail-Bedrohungen wichtiger denn je. Schützen Sie Ihr Unternehmen, Ihre Mitarbeiter und Ihre Kunden mit einem proaktiven Ansatz vor komplexen Angriffen wie Ransomware, BEC und Anmeldedaten-Phishing.

Mit der Risikoanalyse für E-Mail-Sicherheit von Proofpoint erhalten Sie einen umfassenden Überblick sowie wertvolle Erkenntnisse zu Angriffsrisiken und erfahren, wer mit E-Mail-basierten Bedrohungen angegriffen wird.

Warten Sie nicht zu lange, bis Sie Ihre E-Mail-Sicherheit testen. Kontaktieren Sie Proofpoint, um eine kostenlose **Risikoanalyse für E-Mail-Sicherheit** zu vereinbaren.

MEHR ERFAHREN

Weitere Informationen finden Sie unter **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 85 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.

0503-007-04-01 08/24