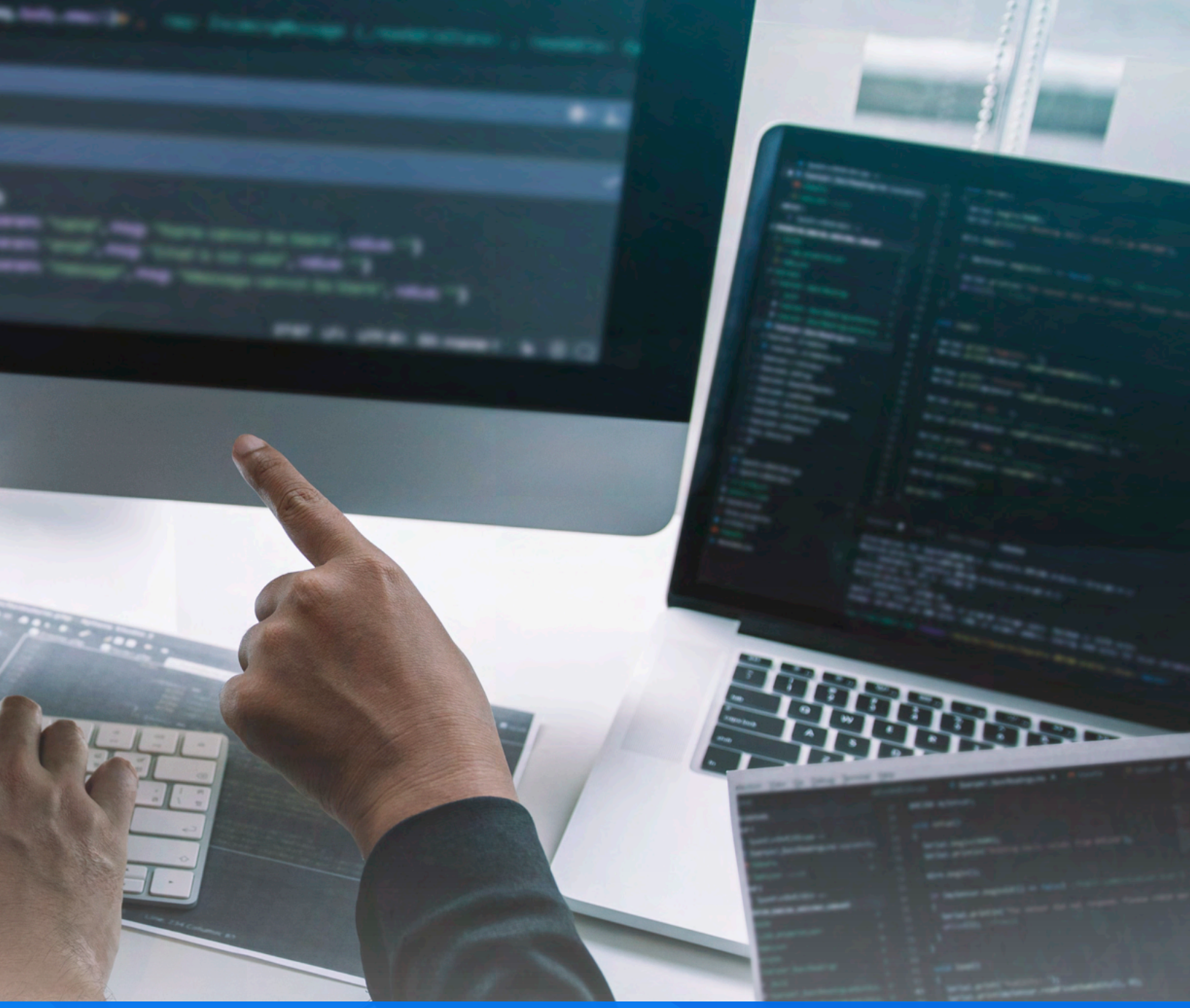

REPORT ZUM

Status verschlüsselter Angriffe

REPORT (2021)

zscaler™

INHALTSVERZEICHNIS

Ist HTTPS-Traffic sicher?

Die Sicherheit von Unternehmensdaten scheint weitgehend missverstanden zu werden. HTTPS (also TLS, früher SSL) ist der Branchenstandard für Verschlüsselung, der Daten während der Übertragung schützt. Aufgabe dieses Standards ist es, Inhalte vor den neugierigen Blicken Unbefugter zu schützen. Dieses Protokoll ist jedoch nur ein Hilfsmittel. Die Verschlüsselung bedeutet nicht, dass auch der Inhalt selbst sicher ist. Malware kann genauso leicht verschlüsselt und übertragen werden wie legitime Dateien – und in der Tat werden mehr als 80 Prozent aller Malware über diese Kanäle übertragen.

Wem diese Idee offensichtlich erscheint, dem sei Folgendes gesagt: In den meisten Unternehmen wird nicht der gesamte verschlüsselte Traffic überprüft.Viele überprüfen verschlüsselten Traffic überhaupt nicht. Doch warum überprüfen Unternehmen ihn nicht, wenn der Großteil des Traffics über verschlüsselte Kanäle versendet wird? Und eine noch wichtigere Frage: Was übersehen sie dabei?

Wie sich herausstellt, eine ganze Menge. Zwischen Januar und September 2021 blockierte Zscaler 20,7 Milliarden Bedrohungen über HTTPS. Dies entspricht einer Zunahme von mehr als 314 Prozent gegenüber den 6,6 Milliarden blockierten Bedrohungen im Jahr 2020, was im Vergleich zum Vorjahr bereits ein Anstieg von fast 260 Prozent war.

Cyberkriminelle werden in ihren Angriffstaktiken immer versierter und haben von den im Dark Web verfügbaren Affiliate-Netzwerken und As-a-Service-Tools profitiert. Dies hat zu einer explosionsartigen Zunahme raffinierter Angriffe geführt, die Sicherheitsteams nachts wachhalten. Besonders Ransomware hat Unternehmen auf der ganzen Welt mit aufsehenerregenden Angriffen beeinträchtigt, die Schäden in Höhe von zweistelligen Millionen Dollar verursacht haben. Die Verschlüsselung von Malware ist ein trivialer Schritt in der Angriffssequenz.

Angesichts der Zunahme von Ransomware – sowie einer Reihe anderer Bedrohungskategorien – und der Fortführung von hybriden und ortsunabhängigen Arbeitsmodellen müssen Unternehmen den gesamten Traffic on premise und außerhalb überprüfen, um ihr Unternehmen bestmöglich zu schützen. Leider ist eine solche Prüfung äußerst ressourcenintensiv. Der Versuch, dies in großem Umfang mit hardwarebasierten Legacy-Sicherheitstools wie Firewalls der nächsten Generation zu tun, ist fast unmöglich und kann für eine effektive Überprüfung fünf- bis siebenmal so viele Geräte erfordern, wenn die Leistung nicht beeinträchtigt werden soll. Infolgedessen lassen viele Unternehmen zumindest einen Teil ihres verschlüsselten Traffics ungeprüft passieren. Das ist ein großes Problem – und wir werden hier erläutern, wie groß es genau ist.

Angriffe über verschlüsselte Kanäle haben von 2020 bis 2021 um **314 %** zugenommen.

Haupterkenntnisse

Die Zscaler Zero Trust Exchange beherbergt das größte Sicherheits-Dataset der Welt. Es wurde aus über 300 Billionen Signalen und 160 Milliarden täglichen Transaktionen aufgebaut– mehr als das 15-Fache des täglichen Google-Suchvolumens. ThreatLabz, das Expertenteam von Zscaler für Bedrohungsanalysen, analysierte diese Daten in den ersten neun Monaten des Jahres 2021 und beurteilte in diesem Zeitraum die Bedrohungen im verschlüsselten Traffic. Die folgende Analyse gibt aufschlussreiche Einblicke in verschlüsselte Angriffe. Zu den Haupterkenntnissen gehören:

- **Bedrohungen über HTTPS haben zugenommen:** Zscaler hat im zweiten Jahr in Folge einen Anstieg von mehr als 314 Prozent der Bedrohungen in verschlüsseltem Traffic gegenüber dem Vorjahr festgestellt.
- **Technologieunternehmen sind ein großes Ziel:** Angriffe auf Technologieunternehmen sind im Vergleich zum Vorjahr um 2.344 Prozent gestiegen; Angriffe auf Einzel- und Großhandelsunternehmen nahmen um 841 Prozent zu.
- **Kritische Dienste bekommen eine Schonfrist:** Das Gesundheitswesen war 2020 das größte Ziel, die Anzahl der Bedrohungen ist jedoch deutlich gesunken. Dies war ebenso der Fall bei Angriffen auf staatliche Einrichtungen. Nach großen Angriffen, wie dem auf Colonial Pipeline, erhöhte sich die Aufmerksamkeit der Strafverfolgungsbehörden, was diese Branchen als Ziele weniger attraktiv machte.
- **Das Vereinigte Königreich und die USA sind Hauptziele verschlüsselter Angriffe:** Unter den fünf am stärksten betroffenen Ländern sind außerdem Indien, Australien und Frankreich.
- **Taktiken ändern sich:** Malware ist um 212 Prozent und Phishing um 90 Prozent gestiegen, während Kryptomining-Malware um 20 Prozent zurückgegangen ist. Dies spiegelt eine allgemeine Verschiebung der Angriffstrends wider, bei der Ransomware immer beliebter wird.
- **Schutz des Unternehmens mit Zero Trust:** Die beste Möglichkeit, sich vor verschlüsselten Bedrohungen zu schützen, ist die Verwendung einer Cloud-Proxy-basierten Zero-Trust-Architektur. Sie reduziert die Angriffsfläche und ermöglicht eine Überprüfung des gesamten ein- und ausgehenden Traffics – inline und im großen Maßstab.

Angriffe auf Technologieunternehmen haben um das 20-Fache **zugenommen**

Zum Schutz des Großteils des Internet-Traffics wird moderne Verschlüsselungstechnologie eingesetzt, einschließlich SSL (Secure Sockets Layer) und dessen Nachfolger TLS (Transport Layer Security). Die Verschlüsselungsraten für legitimen Traffic steigen ebenso wie für schädlichen Traffic. Zscaler blockierte im Jahr 2021 über einen Zeitraum von neun Monaten mehr als 20,7 Milliarden Bedrohungen.

Die Verschlüsselung bietet Angreifern gleich mehrere Vorteile: Verschlüsselter Traffic wird von Sicherheitsteams nicht nur seltener überprüft, ein Fingerprinting verschlüsselter Dateien ist auch viel schwieriger, sodass Malware unentdeckt eingeschleust werden kann.

Es gibt verschiedene Angriffsarten, die Kriminelle im verschlüsselten Traffic verstecken können. Malware ist mit fast 91 Prozent der Angriffe die mit Abstand wichtigste Kategorie.

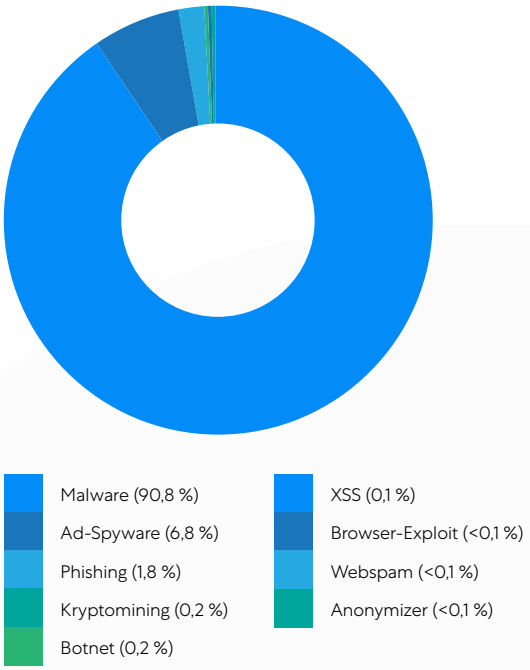

Abbildung 1: *Häufigkeit der Angriffe über verschlüsselte Kanäle*

Malware macht **91 %** der Angriffe aus

Andere Angriffstypen nehmen jedoch zu. Ad-Spyware, Browser-Exploits, Malware, Phishing und Botnet-Angriffe haben im Jahr 2021 gegenüber 2020 zugenommen. Die einzigen Angriffstypen, die einen Rückgang verzeichneten, waren Kryptomining (Computer werden zum Fördern von Kryptowährungen übernommen), Cross-Site-Scripting oder XSS (schädlicher Code wird in legitime Websites eingespeist) und Anonymizer-Angriffe (Proxys werden eingesetzt, um die Verfolgung des Angreifers zu erschweren). Die Beliebtheit von Kryptomining-Angriffen sinkt, da Ransomware in den letzten Jahren zu einer lukrativeren Option geworden ist. Ransomware ist in diesem Report in der Kategorie Malware enthalten.

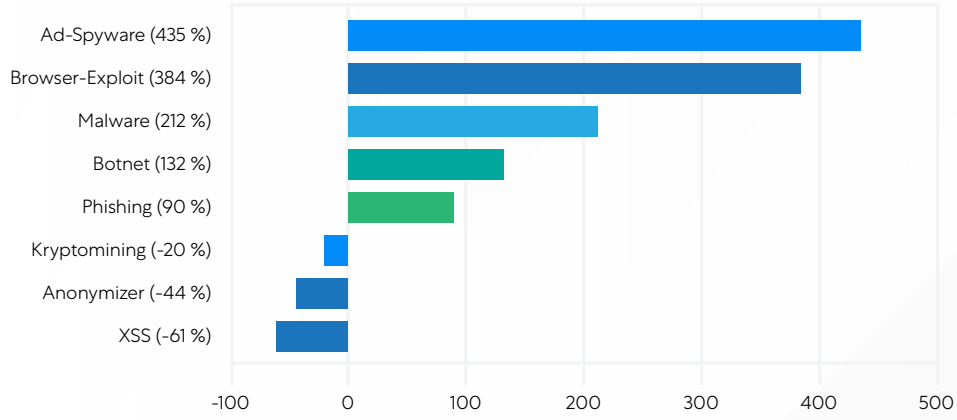

Abbildung 2: *Jährliche Änderung der Angriffe über verschlüsselte Kanäle*

Webangriffe

Im Internet existiert eine Vielzahl schädlicher Websites, wozu auch solche mit einem HTTPS-Präfix gehören. Die mangelnde Hygiene des Internets ermöglicht es Bedrohungen, lange Zeit zu verweilen: Zscaler beobachtete mehr als 13.000 Angriffe von mit Coinhive infizierten Websites, obwohl Coinhive bereits vor über zwei Jahren ausgeschaltet wurde. Eine der häufigsten Web-Angriffskategorien, die HTTPS ausnutzen, sind JavaScript-basierte Skimmer wie **Magecart**, die zum Diebstahl von Web-Zahlungsdaten verwendet werden.

Familie	Angriffe	Typ
Nicehash	5.644.273	Cryptomining
Magecart	2.573.304	Skimming von Zahlungsdaten
Adload	1.626.905	Web Spam
Covid19	972.223	Schadprogramm
Webshell	934.873	Schadprogramm
Coinhive	13.670	Cryptomining

Infizierte Websites können noch **Jahre** nach ihrer Einführung im Internet verweilen.

Phishing

Phishing ist nach wie vor eine beliebte Taktik, bei der User dazu verleitet werden, auf Links in E-Mails zu klicken, die versteckte Malware enthalten. Alle E-Mail- und Filesharing-Dienste sind anfällig für Angriffe. Die Beliebtheit von Microsoft 365 machte es 2021 jedoch bei Weitem zum beliebtesten Ziel – die Zscaler Plattform blockierte innerhalb eines Beobachtungszeitraums von neun Monaten über 15 Millionen Angriffsversuche.

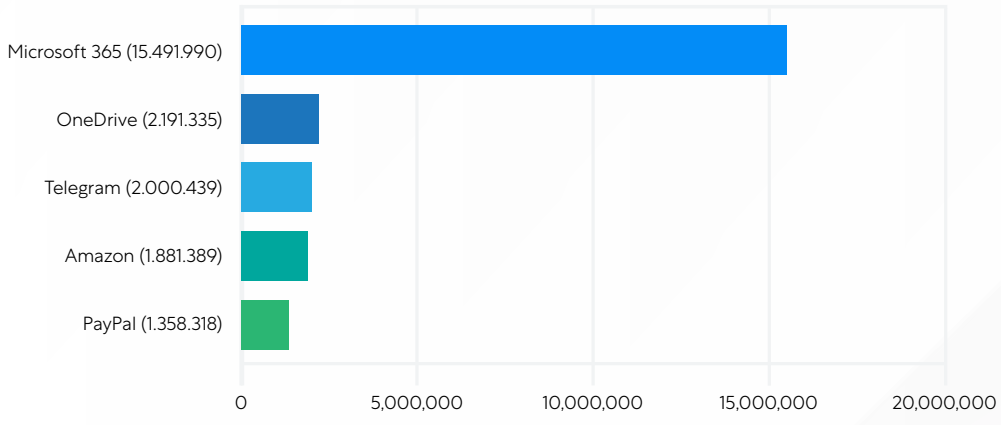

Abbildung 3: *Verschlüsselte Phishing-Angriffe*

Schadprogramm

Malware war im Jahr 2021 die wichtigste Angriffskategorie. Malware wird in der Regel über einen infizierten Link in einer E-Mail oder auf einer Website heruntergeladen. Die meisten Unternehmen verfügen zwar über einen gewissen Schutz vor Malware, die Angreifer verbessern jedoch stetig ihre Techniken und entwickeln neue Malware-Varianten, die in der Lage sind, Fingerprinting-Technologien zu umgehen. Natürlich bemerken Unternehmen, die ihren verschlüsselten Traffic nicht überprüfen, selbst bekannte Malware erst dann, wenn sie in ihre Systeme eingeschleust wurde. Die im Folgenden aufgelisteten Malware-Familien waren im Jahr 2021 weit verbreitet. Dieser Report enthält in einem späteren Teil technische Fallstudien über vier dieser Familien, in denen die Angriffssequenzen veranschaulicht werden.

Familie	Malware-Angriffe
njRAT	355.753
Ursnif	336.540
Azorult	199.334
Hancitor	137.421
Emotet	58.867
Qakbot	30.199
Smokeloader	4.269

Persönlich identifizierbare Informationen (PII) sind das **wichtigste Ziel** von Datendiebstahlversuchen.

Datendiebstahl

Angreifer nutzen verschlüsselte Kanäle nicht nur, um Systeme zu infiltrieren – sie nutzen verschlüsselte Kanäle auch zur Datenexfiltration. Die am häufigsten exfiltrierten Datentypen sind nationale Identifikationsmerkmale und Steuernummern, wie Aadhar (Indien), TFN (Australien), Sozialversicherungsnummern (USA) und BSN (Niederlande). Kreditkarten- und Finanzinformationen bilden das zweitbeliebteste Ziel, gefolgt von geistigem Eigentum und medizinischen Daten. Die nachstehende Grafik zeigt die Datendiebstahlversuche über nur drei Monate.

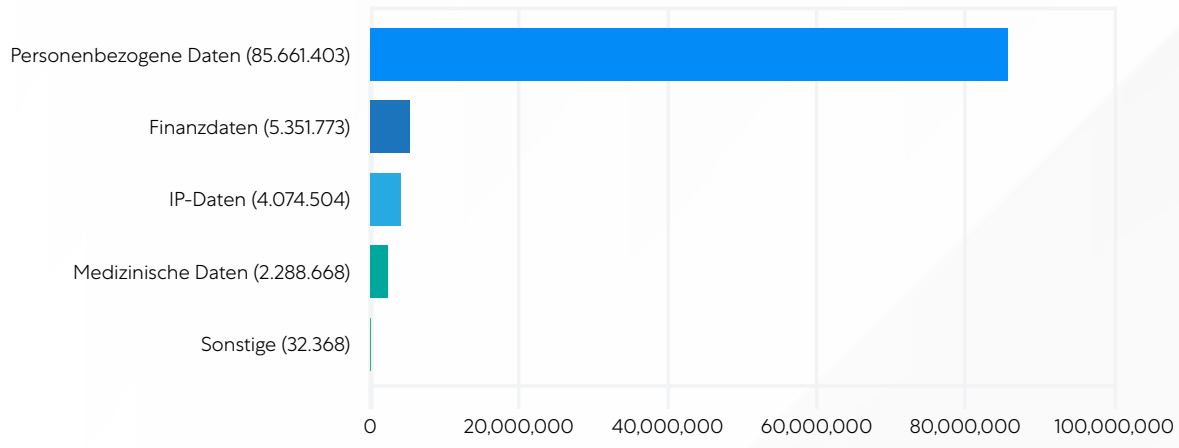

Abbildung 4: *Datendiebstahlversuche*

Command-and-Control-Aktivität

Command-and-Control-Server (C&C) werden aus verschiedenen Gründen eingesetzt, z. B. zum Ausführen von Payloads in der zweiten Phase eines gezielten Angriffs, zum Exfiltrieren von Daten und zum Steuern von Rechnern in Botnets. Botnets sind Netzwerke aus Geräten, die sich in der Kontrolle eines Angreifers befinden und einen groß angelegten, koordinierten Angriff ermöglichen. Bisher wurden Botnets u. a. für DDoS-Angriffe (Distributed Denial of Service), Diebstahl von Finanzdaten, Fördern von Kryptowährungen und gezieltes unbefugtes Eindringen verwendet.

Angreifer nutzen eine Reihe von Tools, um Callbacks auf ihre C&C-Server durchzuführen. Einige dieser Tools, wie Smoke Loader und Gumblar, sind Bots, die speziell zu diesem Zweck entwickelt wurden. Bei anderen, wie Cobalt Strike und PoshC2, handelt es sich um Tools für Penetrationstests, die von den Angreifern umfunktioniert wurden. Nachstehend wird die Häufigkeit der Callback-Versuche mithilfe dieser Tools dargestellt:

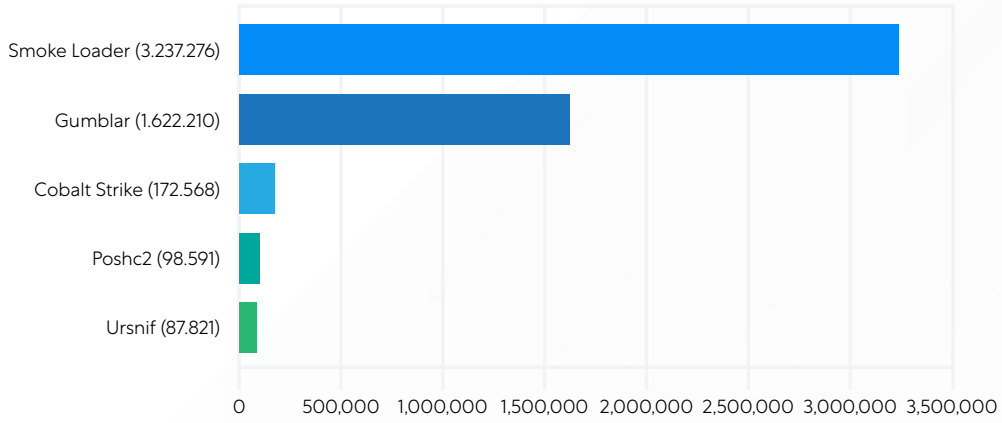

Abbildung 5: *Command-and-Control-Aktivität*

Angreifer interagieren mit fast **70 Prozent** der verschlüsselten, mit dem Web verbundenen Anwendungen.

Credential Stuffing und Exploit-Aktivität

Doch nicht nur Malware wird über verschlüsselten Traffic verbreitet. Angreifer nutzen diese Kanäle auch für von Menschen initiierte Angriffsversuche, bei denen verschlüsselte Anwendungen ausgenutzt werden.

Das ThreatLabz-Team sammelt mithilfe der Zscaler-Deception-Technologie außerdem Informationen aus einem weltweit eingesetzten Netz aus Decoys, um die Taktiken, Techniken und Verfahren der Angreifer zu untersuchen. Decoy-Assets dienen als Köder für Angreifer und werden von legitimen Usern nicht genutzt. Jede Interaktion mit ihnen ist also ein Zeichen für bösartige Aktivität. Die Erkenntnisse von ThreatLabz:

1. Es wurde mit fast 70 Prozent aller SSL-verschlüsselten Anwendungs-Decoys interagiert. Dies lässt darauf schließen, dass aller Wahrscheinlichkeit nach Angriffsversuche auf 70 Prozent der SSL-verschlüsselten Anwendungen vorliegen.
2. Bei mit dem Internet verbundenen Decoy-Webanwendungen waren 48 Prozent der Angriffe auf Zugangsdaten an E-Mail- und VPN-Decoys gerichtet.
    - E-Mail-Decoys waren ein beliebtes Ziel für Angriffsversuche mit gestohlenen Zugangsdaten.
    - Bei VPN-Decoys wurden Versuche zur Ausnutzung neu offengelegter CVE-Schwachstellen in VPN-Produkten festgestellt.
3. Die am häufigsten beobachtete Technik war die Suche nach „.git“-Dateien, wahrscheinlich mit dem Ziel, nach falsch konfigurierten Webservern zu suchen, um den Quellcode offenzulegen. Diese Technik gibt es zwar schon seit einiger Zeit, sie ist aber immer noch sehr beliebt für Ausspähversuche vor einem Angriff.

Angriffe auf Mobilgeräte

Smartphones und Tablets sind nach wie vor ein beliebtes Ziel für Angreifer, die sie mithilfe gefälschter Anwendungen ausnutzen. Nach der anfänglichen Infektion nutzen viele der neuen und verbreiteten mobilen Malware-Varianten SSL-Netzwerkkommunikation für ihre Command-and-Control-Aktivitäten, darunter das Abrufen von Payloads oder das Empfangen von Befehlen für schädliche Aktivitäten und Datenexfiltration. Es wurde festgestellt, dass Malware-Familien wie Hydra, Joker und das neu entdeckte GriftHorse für ihre Aktivitäten nach einer Infektion SSL ausnutzen.

Malware: GriftHorse

Die vor Kurzem aufgetauchte Android-Malware-Kampagne GriftHorse hat weltweit mehr als 10 Millionen Opfer mit einer Diebstahlsumme in Höhe eines schätzungsweise dreistelligen Euro-Millionenbetrags gefordert. Nach der Infektion werden Opfer dazu verleitet, eine Telefonnummer einzusenden, um einen Preis zu erhalten. Ohne Wissen des Opfers wird die Telefonnummer für das Abonnement eines Premium-SMS-Dienstes angemeldet, wodurch die Telefonrechnung des Opfers mit mehr als 30 Euro pro Monat belastet wird. Der Trojaner kommuniziert in drei Phasen mit C&C-Servern und nutzt SSL für Aktivitäten nach der Infektion.

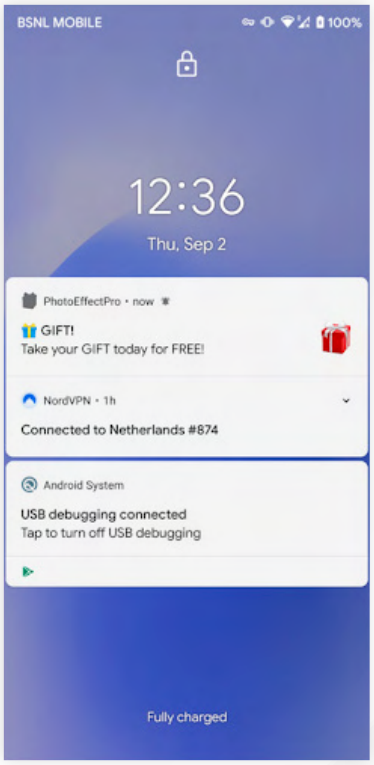

Abbildung 6: *GriftHorse-Malware-Angriff*

Malware: Joker

Joker ist eine der bekanntesten Malware-Familien, die über den Google Play Store auf Android-Geräte abzielt. Zscaler blockierte fast 22.000 Callback-Versuche der Joker-Malware über TLS, das es für Command-and-Control-Aktivitäten nutzt. Trotz der öffentlichen Bekanntheit dieser Malware findet sie anhand von Änderungen an Code, Ausführungsmethoden oder Payload-Abruftechniken immer wieder den Weg in den offiziellen App-Marktplatz von Google. Joker ist eine Art von Spyware und wurde entwickelt, um SMS-Nachrichten, Kontaktlisten und Geräteinformationen zu stehlen und das Opfer für Premium-WAP-Services (Wireless Application Protocol) anzumelden.

Malware: Hydra

Hydra ist eines der beliebtesten und leistungsfähigsten Beispiele für Banking-Malware. Zu den Funktionen gehört das Screencasting, also die Aufzeichnung von Aktivitäten, die im Laufe der Zeit auf dem Bildschirm des Users stattfinden. Hydra ist auch in der Lage, Remote-Anwendungen zu installieren, die es Angreifern ermöglichen, infizierte Geräte zu beobachten und zu kontrollieren. Dies macht Hydra zu einer ernsthaften Bedrohung. Hydra nutzt SSL-Zertifikate für Command-and-Control-Aktivitäten.

Branche

Ein Vergleich der Jahre 2021 und 2020 zeigt große Unterschiede zwischen den einzelnen Branchen. In sieben der in unserer Studie betrachteten Branchen kam es zu mehr Angriffen über verschlüsselte Kanäle. Bei zweien sank die Zahl der Angriffe, darunter das Hauptziel des vergangenen Jahres: das Gesundheitswesen.

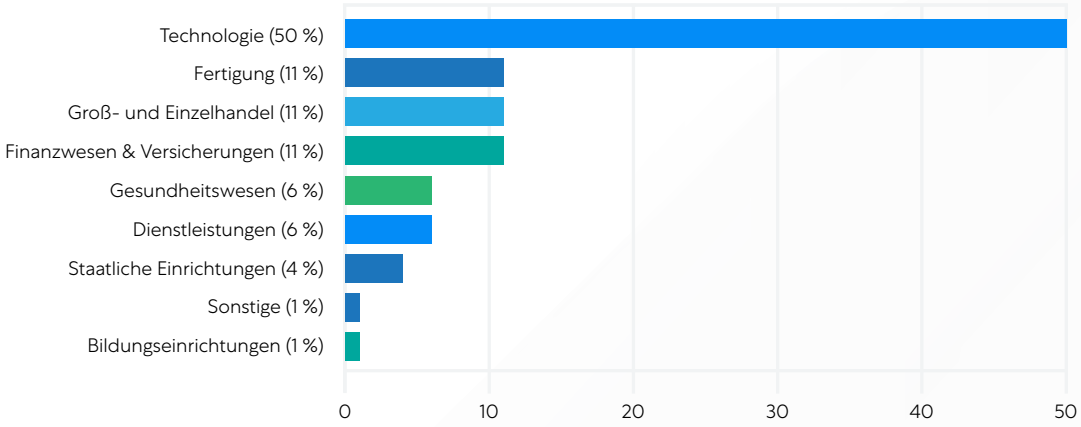

Abbildung 7: *Angriffsvolumen nach Branche*

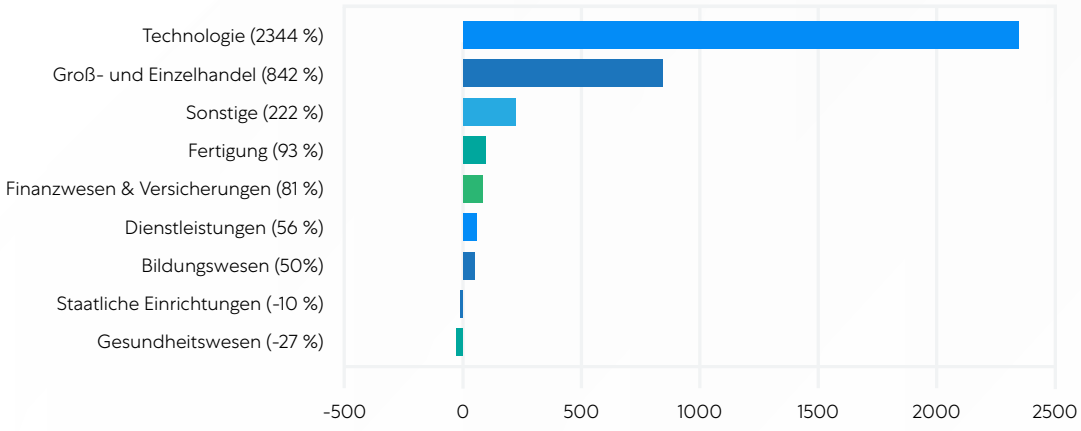

Abbildung 8: *2021 gegenüber 2020: Angriffe nach Branche*

Starker Anstieg der Angriffe in den Branchen Technologie und Einzelhandel

Angriffe auf Technologieunternehmen haben sich um das 23-Fache erhöht und machen nun mehr als die Hälfte der beobachteten Angriffe aus. Malware ist für die Technologiebranche ein sehr viel größeres Problem als für andere Branchen. Die hohe Abhängigkeit von Technologie bei nahezu allen Geschäftsfunktionen bietet Angreifern eine große Angriffsfläche. Dies wurde durch die plötzliche Notwendigkeit verschärft, Remote-Mitarbeiter mit Ressourcen zu unterstützen – von Remote-Konnektivität bis hin zu Telekonferenzen, SaaS-basierten Anwendungen und Workloads in öffentlichen Clouds.

Technologieunternehmen sind auch aufgrund ihrer Rolle in der Lieferkette anderer Unternehmen attraktive Ziele. Ein erfolgreicher Lieferkettenangriff kann Angreifern Zugriff auf Hunderte oder sogar Tausende nachgeschaltete Opfer verschaffen, wie die Fälle von Kaseya, SolarWinds und anderen zeigen.

Auch der Groß- und Einzelhandel hatte mit einer achtfachen Steigerung der Angriffsraten ein extrem schlechtes Jahr. Im Jahr 2020 machte er nur 3,5 Prozent der Angriffe aus, 2021 stieg dieser Anteil jedoch auf 11 Prozent. Schädliche Inhalte nahmen deutlich zu, darunter Skimmer, bösartige JavaScripts und Malware-Payloads, die über TLS-Kanäle auf Einzelhandels- und E-Commerce-Anbieter abzielen.

Während die Welt zur Normalität zurückkehrt und Unternehmen sowie öffentliche Veranstaltungen rund um den Globus erneut öffnen, arbeiten viele Mitarbeiter weiterhin in relativ unsicheren Umgebungen. Der Zugang zu kritischen Kassensystemen ist für Cyberkriminelle äußerst attraktiv, da er ihnen die Tür zu hohen Gewinnen öffnet.

Angriffe auf Gesundheitswesen und staatliche Einrichtungen gehen zurück

Die Angriffe auf Organisationen im Gesundheitswesen, die 2020 das Hauptziel darstellten, sind 2021 um 27 Prozent zurückgegangen. Angriffe auf staatliche Einrichtungen waren ebenfalls um 10 Prozent rückläufig. Große Ransomware-Angriffe, die sich auf kritische Dienste ausgewirkt haben, wie der Angriff auf SolarWinds, der Angriff auf Colonial Pipeline und der Ransomware-Angriff auf die irische Gesundheitsbehörde, haben die Aufmerksamkeit der höchsten Strafverfolgungsbehörden auf sich gezogen. Deshalb sind diese kritischen Branchen für Angreifer derzeit weniger attraktiv. Darüber hinaus haben einige Ransomware-Familien versprochen, während der Pandemie keine Angriffe auf das Gesundheitswesen und andere kritische Dienste zu unternehmen – obwohl sie dieses Versprechen nicht ganz eingehalten haben.

Region

Die fünf Länder, die am häufigsten Ziel von verschlüsselten Angriffen geworden sind, sind das Vereinigte Königreich, die USA, Indien, Australien und Frankreich:

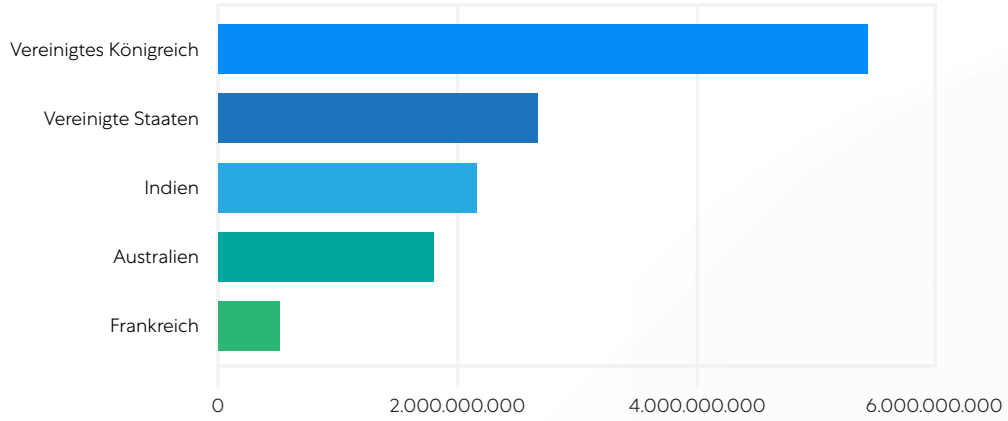

Abbildung 9: *Am meisten angegriffene Länder*

Bei jedem dieser Länder handelt es sich um ein großes Technologiezentrum und die Angriffsraten sind mit der allgemeinen Zunahme der auf diesen Sektor gerichteten Angriffe gestiegen. ThreatLabz beobachtete Angriffe in 255 verschiedenen Ländern weltweit, darunter auch in kleinen Ländern, die nicht zu den üblichen Zielen gehören. Darunter befanden sich über 7,5 Millionen Angriffe auf Inseln in der Karibik sowie auf die Färöer Inseln, St. Bartholemy und die Falklandinseln. Dies ist das Ergebnis des vermehrten ortsunabhängigen Arbeitens, aufgrund dessen Mitarbeiter von abgelegenen Standorten aus arbeiten.

Europa, angeführt von einer massiven Angriffsrate im Vereinigten Königreich, war insgesamt das Ziel der meisten Angriffsversuche über verschlüsselte Kanäle:

Region	Graf
Europa	7.234.747.361
APAC	4.925.542.601
Nordamerika	2.778.360.051
Südamerika	226.320.069
Afrika	146.865.982
Mittlerer Osten	137.494.862
Mittelamerika	127.354.294
Karibik	7.543.056
Antarktis	16.144

Das Work-from-Anywhere-Konzept hat für eine Erweiterung der geografischen Reichweite von Cyberangriffen gesorgt.

Mit dem Wechsel zu neuen digitalen Arbeitsmodellen müssen Unternehmen zunehmend sicherstellen, dass ihre Assets und der Traffic zu diesen Assets sicher sind. Darüber hinaus ist die Erkenntnis entscheidend, dass Verschlüsselung allein keine Sicherheit bietet: Verschlüsselte Kanäle werden von Angreifern genauso häufig verwendet wie unverschlüsselte Kanäle.

Fazit: **Der gesamte Traffic muss überprüft werden!**

Veraltete Tools machen eine vollständige Überprüfung zu einem kostspieligen und leistungsmindernden Unterfangen. Außerdem können Vorschriften, die unterschiedliche Richtlinien für verschiedene Datentypen vorschreiben, dies ebenfalls zu einer mühsamen Aufgabe machen. Es gibt jedoch bewährte Strategien, mit denen Unternehmen ihren verschlüsselten Traffic in großem Umfang überprüfen können – ohne Beeinträchtigung der Systemleistung oder Verursachung von Compliance-Konflikten. Wir empfehlen:

- Entschlüsselung, Entdeckung und Abwehr von Bedrohungen im gesamten HTTPS-Traffic mit einer Cloud-nativen Proxy-basierten Architektur, die den gesamten Traffic für jeden User überprüfen kann.
- Isolierung unbekannter Angriffe und Schutz vor Patient-Zero-Malware mit einer KI-gesteuerten Sandbox, die im Gegensatz zu Firewall-basierten Passthrough-Ansätzen verdächtige Inhalte zur Analyse aufbewahrt.
- Konsistente Sicherheit für alle User und alle Standorte, sodass alle User stets über dasselbe hohe Sicherheitsniveau verfügen, ob zu Hause, am Hauptsitz oder unterwegs.
- Verringern Sie die Angriffsfläche durch Zero Trust sofort, wodurch eine laterale Ausbreitung nicht mehr möglich ist. Apps sind für Angreifer unsichtbar und autorisierte User greifen direkt auf benötigte Ressourcen zu, nicht auf das gesamte Netzwerk.

Die Lösung erfordert Skalierbarkeit und Leistung. Beides kann nur durch eine Cloud-native, Proxy-basierte Architektur wie Zscaler Zero Trust Exchange™ bereitgestellt werden. Eine Cloud-basierte Sicherheitsplattform erfüllt die Anforderungen an Entschlüsselung und Überprüfung durch die elastische Skalierung von Rechenressourcen und bietet eine einheitliche Policy-Durchsetzung über mehrere Standorte hinweg. Eine mehrschichtige, tiefgreifende Abwehrstrategie, welche die Angriffsfläche verringert und eine vollständige HTTPS-Überprüfung zur Aufdeckung versteckter Bedrohungen bietet, ist unerlässlich, um den Schutz von Unternehmen zu gewährleisten.

Die beste Möglichkeit zur Abwehr verschlüsselter Bedrohungen besteht in der Überprüfung des verschlüsselten Traffics im Rahmen einer ganzheitlichen Zero-Trust-Sicherheitsstrategie.

SO WEHRT DIE ZSCALER ZERO TRUST EXCHANGE VERSCHLÜSSELTE BEDROHUNGEN AB

Zero-Trust-Strategien und -Architekturen sind das wirksamste Mittel, um Unternehmen vor sich rasch wandelnden Cyberbedrohungen zu schützen. Zero Trust geht davon aus, dass zu jedem Zeitpunkt ein aktiver Angriff vorliegt und die Infrastruktur bereits beeinträchtigt wurde. Auf der Grundlage dieser Annahme werden Sicherheitskontrollen eingerichtet, die den Erfolg eines mutmaßlichen Angriffs verhindern.

Die meisten erweiterten Angriffe erfolgen in drei unterschiedliche Phasen. Die Angriffe beginnen mit der anfänglichen Kompromittierung eines mit dem Internet verbundenen Endgeräts oder Assets. Daraufhin breitet der Angreifer die Malware lateral aus, um das System auszuspähen und im Netzwerk Fuß zu fassen. Zum Schluss ergreift der Angreifer Maßnahmen zur Erreichung seiner Ziele, bei denen es sich in der Regel um die Exfiltration von Daten handelt. Die Zscaler Zero Trust Exchange reduziert das Risiko in jeder dieser drei Angriffsphasen auf ganzheitliche Weise, da sie in jeder Phase mehrere Sicherheitskontrollen bereitstellt:

Schutz vor Kompromittierung
Schutz von Usern, Servern, Workloads und IoT/OT durch Minimierung der Angriffsfläche und Überprüfung des gesamten Traffics.

Schutz vor lateralen Bewegungen
Angreifer werden daran gehindert, sich im Netzwerk zu bewegen und hochwertige Ziele ausfindig zu machen.

Verhinderung von Datendiebstahl
Überprüfung aller mit dem Internet verbundenen Daten, um Datenverluste im Internet und die Ausnutzung nicht verwalteter Geräte zu verhindern.

Anfängliche Kompromittierung: Zur Verhinderung des ersten Zugriffs muss zunächst die Anzahl von Einstiegspunkten in das Ökosystem reduziert werden. Es muss eine Prüfung der Angriffsfläche erfolgen, aktuelle Sicherheits-Patches müssen installiert und mögliche Fehlkonfigurationen korrigiert werden. Außerdem sind mit dem Internet verbundene Anwendungen zu vermeiden – stattdessen sollten sie hinter einem Cloud-Proxy verborgen sein, der die Verbindung vermittelt. Dadurch haben Angreifer nur eine Tür in das System hinein und aus dem System heraus zur Verfügung, die überwacht werden kann. Wie wir bereits mehrfach empfohlen haben: Der gesamte Traffic sollte überprüft werden. Es ist davon auszugehen, dass nichts und niemandem vertraut werden kann. Zscaler führt im Rahmen seiner Service-Plattform eine HTTPS-Überprüfung im großen Maßstab durch. Bei einer Zunahme Ihres Traffics wird die Kapazität sofort bedarfsgerecht angepasst. Es gibt also keine Appliances, die bemessen, bestellt oder versandt werden müssen.

Laterale Ausbreitung: Mit Zero Trust gibt es kein „vertrauenswürdiges Netzwerk". Sie müssen annehmen, dass jede Person, die Zugriff auf Anwendungen hat, böswillige Absichten hat, und dementsprechend den Schaden, der von einer Person angerichtet werden kann, begrenzen. Eine Mikrosegmentierung reduziert den Zugriff selbst für authentifizierte User. Die Zero-Trust-Zugriffslösung von Zscaler, Zscaler Private Access™, verbindet User direkt mit der benötigten Anwendung, ohne je das Netzwerk zu gefährden. Sie erzeugt dadurch ein Eins-zu-eins-Segment, das von der Zero Trust Exchange vermittelt und authentifiziert wird. Das ist Zero-Trust-Segmentierung in Reinform und sehr viel weniger komplex als eine regelbasierte Netzwerksegmentierung, wie sie durch Legacy-Technologien vorgenommen wird. Zscaler verwendet außerdem Täuschungstechnologie, um Angreifer mit strategisch platzierten Decoys zu ködern. So werden Sicherheitsteams informiert, dass ein Angreifer versucht, sich lateral zu bewegen oder das Netzwerk auszuspähen.

Command-and-Control-Callback (C&C): Sobald die Malware installiert ist, versucht sie in der Regel, Kontakt mit einem Command-and-Control-Server (C&C) aufzunehmen. Dieser Kontakt ermöglicht es Angreifern, Rechner zu übernehmen, zusätzliche Befehle zu erteilen, weitere Malware herunterzuladen oder Daten zu stehlen. Die Überprüfung des ausgehenden Traffics ist ebenso wichtig wie die des eingehenden Traffics, um diese Kommunikation zu unterbrechen und sensible Daten zu schützen. Zscaler kann verschlüsselte Daten in beide Richtungen prüfen und setzt elegante Funktionen zum Schutz vor Datenverlust ein, um jeglichen schädlichen ausgehenden Traffic zu erkennen und zu stoppen.

Zscaler Zero Trust Exchange wehrt die gesamte Angriffssequenz ab und bietet eine HTTPS-Überprüfung in großem Maßstab mit einem mehrschichtigen Ansatz, der Inline-Bedrohungsüberprüfung, Sandboxing und Data Loss Prevention sowie eine breite Palette zusätzlicher Abwehrfunktionen umfasst. Darüber hinaus sorgt der Cloud-Effekt von Zscaler dafür, dass alle auf der globalen Plattform identifizierten Bedrohungen automatisch zum Schutz aller Zscaler-Kunden aktualisiert werden. Ihre eigene Sicherheitslage wird also durch die Beiträge aller Zscaler-Kunden auf der ganzen Welt ständig verbessert. Die Zscaler Zero Trust Exchange, angetrieben durch die weltweit größte Security-Cloud, beschleunigt die Unternehmenstransformation. User und Anwendungen werden standortunabhängig durch kontextbasierte Identitätsprüfung und Policy-Durchsetzung zuverlässig geschützt.

ThreatLabz beobachtete 2021 die im Folgenden aufgelisteten neuen und verbreiteten Malware-Familien, die TLS nutzen.

njRAT

355.753 beobachtete Blockierungen zum Download über TLS.

Zusammenfassung

njRAT, auch bekannt als Bladabindi, ist ein im .Net-Framework entwickelter Remote-Access-Trojaner (RAT), der dem Remote-Angreifer vollständige Kontrolle über das infizierte System sowie eine Reihe von Funktionen bietet. Er kann die Tastatureingaben des Users protokollieren, Daten von kompromittierten Rechnern stehlen und Daten an einen Remote-Server exfiltrieren. Erstmals beobachtet wurde dieser Trojaner im Juni 2013.

Die Malware verwendet eine oder alle der folgenden Techniken, um unentdeckt zu bleiben:

1. Verschleierung mit bekannten Packern, wie ConfuserX usw.
2. Anti-Virtualisierung: Prüfung der Präsenz von „vboxservice.exe“, „vboxtray.exe“, „vmtoosd.exe“, „SDBIE.DLL“ usw.
3. Überprüfung auf Analysetools: Prüfung von Prozessen wie processviewer.exe, processhacker.exe usw.

Verbreitungsstrategie

Angreifer nutzen verschiedene Strategien wie E-Mail- und Web-Angriffsvektoren zur Verbreitung von njRAT. Zu den beliebtesten Angriffsvektoren gehören:

- Einsatz von Exploit-Kits wie Lord EK und Rig EK.
- Makrobasierte MS Office-Dateien, die als E-Mail-Anhänge versendet oder unter einer URL gehostet werden.

Persistenz

Für die Persistenz nutzt die Malware einen oder beide der folgenden Mechanismen:

1. Autorun-Registrierungseintrag unter HKCU\Software\Microsoft\Windows\CurrentVersion\Run oder HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
2. Kopieren der Malware selbst in den Autostartordner

Netzwerk

njRAT verwendet einen dynamischen DNS-Service für Command-and-Control-Server (C&C) und kommuniziert mit einem benutzerdefinierten TCP-Protokoll über einen konfigurierbaren Port. Aktuell wurde beobachtet, dass njRAT v2.0 die URL cdn.discordapp.com zum Ablegen der Payload nutzt, die das HTTPS-Protokoll verwendet. Filebin.net, das auch HTTPS verwendet, wurde ebenfalls genutzt, um sich als gecracktes Spiel auszugeben.

Smoke Loader

ThreatLabz registrierte 4.269 blockierte Downloads und 3.237.276 blockierte Callbacks über TLS.

Zusammenfassung

Smoke Loader tauchte 2011 erstmals aus dem russischen Cybercrime-Untergrund auf. In diesem Jahr ist Smoke Loader 10 Jahre alt geworden und immer noch aktiv. Smoke Loader wird in erster Linie als Downloader verwendet, um zusätzliche Malware herunterzuladen und auszuführen. Smoke Loader ist ein kriminelles Toolkit, das einen Bot und ein PHP-basiertes C&C-Panel sowie ein Benutzerhandbuch enthält. Diese Malware wird häufig im Dark Web verkauft und bietet für 1.650 USD ein Malware-Komplettpaket.

Ausweichtechniken

Smoke Loader durchläuft häufig Prozesslisten, um einen Prozess zur Einspeisung zu finden, und verwendet die Propagate-Injection-Methode, um Code in explorer.exe zu integrieren. Die Malware ist zudem mit mehreren Anti-VM-Tricks ausgestattet. Zum Beispiel prüft sie, ob der Pfad der ausführbaren Datei die Zeichenfolge [A-F0-9]{4}.vmt enthält und sucht auch nach allen laufenden Prozessen, um die Zeichenfolgen „qemu-ga.exe“, „qga.exe“, „windanr.exe“, „vboxservice.exe“, „vboxtray.exe“, „vmtoosd.exe“, „pr_toos.exe“, „vbox“ und „vmmemc“ zu finden. Werden eine oder mehrere dieser Zeichenfolgen gefunden, wird die Binärdatei beendet. Es wird auch nach laufenden Prozessnamen wie „procmon.exe“, „ProcessHacker.exe“, „Wireshark.exe“ und vielen anderen gesucht. Wird einer dieser Prozesse gefunden, wird die Binärdatei beendet.

Persistenzmechanismus

Die Malware generiert eine eindeutige ID für jeden Opfercomputer, die auf einer Verkettung des Computernamens, einer fest kodierten statischen Nummer (die sich von Kampagne zu Kampagne unterscheidet) und der Seriennummer des Systemlaufwerks basiert. Die ID wird dann als MD5-Hash der verketteten Zeichenfolge generiert und wiederum mit der MD5-Seriennummer ergänzt. Die Malware verwendet diese eindeutige ID für mehrere Zwecke, nämlich zum Erstellen von zufälligen Dateinamen für zwei abgelegte Dateien – die erste ist eine Kopie der ausführbaren Datei von Smoke Loader und die zweite ist eine lnk-Datei, die im Autostartordner erstellt und als geplante Aufgabe aufgerufen wird.

Netzwerkkommunikation

Die C&C-Domains werden mit einfachen XOR-Operationen verschlüsselt. Daraufhin sendet Smoke Loader eine POST-Anforderung an den C&C-Server. Die Payload wird mit RC4 verschlüsselt, bevor sie gesendet wird. Die POST-Anforderung liefert eine „404 Not Found“-Antwort, enthält aber eine Payload im Antwortkörper. Smoke Loader hat sich zu einem beliebten Downloader für verschiedene Malware-Familien entwickelt und lädt Malware wie Avemaria herunter, die auf pastebin.com gehostet wird. Sie funktioniert über HTTPS und eine ähnliche Kommunikation ist auch bei anderer abgelegter Malware zu beobachten, die HTTPS verwendet.

QakBot

30.199 beobachtete Blockierungen zum Download über TLS.

Zusammenfassung

QakBot ist ein Banking-Trojaner, auch bekannt als Qbot oder Pinkslipbot, der seit 2007 aktiv ist. Sein Hauptziel ist der Diebstahl von Bankdaten. Er wird über Spam-E-Mails verteilt und verleitet die User zum Herunterladen schädlicher Anhänge oder zum Anklicken schädlicher Links. Ein heruntergeladenes Dokument bzw. eine heruntergeladene Skriptdatei lädt die Haupt-Payload von Qakbot im infizierten System weiter herunter.
In einigen Fällen wird Qakbot über Exploit-Kits verbreitet und durch andere Malware wie TrickBot heruntergeladen. QakBot hat sich im Laufe der Zeit weiterentwickelt und verfügt heute über zusätzliche Funktionen, z. B. Web-Injektionstechniken zum Stehlen von Anmeldedaten, Kreditkartennummern, Sozialversicherungsnummern, E-Mail-Adressen und Tastatureingaben. Außerdem verfügt er über Backdoor-Funktionen.

Persistenzmechanismus

QakBot stellt Persistenz her, indem er einen RUN-Schlüssel am Ort des Autostarts erstellt und die Malware bei jedem Login ausführt. Außerdem werden geplante Aufgaben erstellt, um die Payload einmal um 5:33 Uhr auszuführen und die geplante Aufgabe nach der Ausführung zu löschen.

> *HKEY_USERS\Software\Microsoft\Windows\CurrentVersion\Run\{zufallsgeneriert}*
> *C:\Windows\SysWOW64\schtasks.exe 'C:\Windows\system32\schtasks.exe' /Create /RU 'NT AUTHORITY\SYSTEM' /tn {zufallsgeneriert}/tr '\'% AppData%\Roaming\Microsoft\{zufallsgeneriert}\{zufallsgeneriert.exe}\' /I {zufallsgeneriert}' /SC ONCE /Z /ST 05:33 /ET 05:45*

Netzwerkkommunikation

In einer der Kampagnen lädt JavaScript das aktualisierte QakBot-Formular *ebook[.]w3wvg.com/datacollectionservice.php3* herunter und führt es aus. Die heruntergeladene Payload ist verschlüsselt und das Skript entschlüsselt sie. Daraufhin wird sie im System abgelegt und die folgenden Informationen werden vom Computer des Opfers gestohlen:

- IP-Adresse
- Host Name
- Benutzername
- OS-Version
- Bankzugangsdaten

Die Malware verwendet WebInject, um die Kommunikation zwischen dem Rechner des Opfers und den Bank-Websites zu verändern, und stiehlt die Anmeldedaten. Um über Transport Layer Security mit dem Command-and-Control-Server zu kommunizieren, wie im folgenden Screenshot dargestellt, verwendet QakBot statt Secure Sockets Layer einen TLS-Handshake.

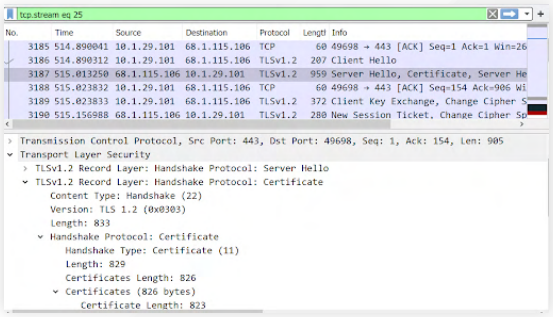

Abbildung 10: *QakBot verwendet TLS-Handshake*

Solarmarker

Zusammenfassung

Die als Solarmarker/Jupyter Infostealer/Yellow Cockatoo/Polazert bekannte Malware ist ein sehr modularer Infostealer und Keylogger. Die Malware verpackt sich in der Regel mit bekannten potenziell unerwünschten Anwendungen (PUAs), z. B. PDFSam, und nutzt im Allgemeinen Innopack, um sich als legitime Programmdatei zu verpacken. Eine Infektion mit Solarmarker wird in der Regel mit SEO-Poisoning erreicht. Dabei handelt es sich um eine alte Technik, bei der die Opfer mit einem Köder zum Herunterladen von Dateien aus dem Internet verleitet werden. Der Download des Malware-Pakets erfolgt über HTTPS.

Ausweichtechniken

Diese Malware wird mit Installationsprogrammen wie MSI und Innopack verbreitet. Dadurch wird die Größe des ursprünglichen Vektors auf über 50 MB erhöht, was größer ist als die Übermittlungsgröße einiger Malware-Repositorys und Sandboxen. MSI wird auch verwendet, um Endpunkterkennung und Antivirenlösungen zu umgehen, da es weniger verdächtig ist, wenn MSI PowerShell ausführt, als wenn eine EXE ein PowerShell-Skript ausführt.

Persistenzmechanismus

In neueren Kampagnen legt die Malware eine .lnk-Datei im User-Verzeichnis Startmenü\Programme\Autostart ab. Ist die .lnk-Datei in diesem Verzeichnis abgelegt, wird sie beim Start ausgeführt und die Backdoor gestartet.

Netzwerkkommunikation

Solarmarker wird über das TLS-Protokoll eingeschleust und über SEO-Poisoning verteilt. Da diese Malware in der Regel zusammen mit anderen Installationsprogrammen gebündelt ist, wird ihre Netzwerkkommunikation durch die Kommunikation der legitimen Packer etwas verschleiert. Die meisten Programme verwenden TLS und HTTPS, während die schädliche Kommunikation über HTTP mit POST-Anforderungen erfolgt. Die IP-Adresse ist in der Binärdatei vorhanden. Die Userdaten werden, wie unten dargestellt, in einer JSON-Datei gesendet.

```
"{\"action\":\"ping\",\"",
Deimos.a.a(new char[]
{
    'h',
    'w',
    'i',
    'd'
}),
"\":\"",
A_0.g,
"\",\"pc_name\":\"",
Deimos.a.h(),
Deimos.a.b(),
"\",\"os_name\":\"",
Deimos.a.e(),
Deimos.a.b(),
"\",\"arch\":\"",
Deimos.a.f() ? "x64" : "x86",
Deimos.a.b(),
"\",\"rights\":\"",
Deimos.a.d() ? "Admin" : "User",
Deimos.a.b(),
"\",\"version\":\"",
A_0.a,
"\",\"",
```

Abbildung 11: *Über eine JSON-Datei gesendete Userdaten*

BlackMatter

Zusammenfassung

Die Verbreitung von BlackMatter begann im Juli 2021. Die Betreiber der BlackMatter-Ransomware verwenden doppelte Erpressungstechniken und sind dafür bekannt, gestohlene sensible Daten der Opfer auf ihrer Website zu veröffentlichen, wenn das Lösegeld nicht bezahlt wird. Sie bieten RaaS (Ransomware-as-a-Service) an und schalteten eine Anzeige in einem Forum, in der sie Vermittler suchten, die einen ersten Zugang zu kompromittierten großen Netzwerken bereitstellen können – die BlackMatter-Betreiber bezahlen die Vermittler für den Netzwerkzugang. BlackMatter-Ransomware verwendet Kombinationen von RSA+ Salsa20 im Verschlüsselungsprozess. Diese Ransomware fügt nach der Verschlüsselung„. {zufällige alphanumerische Zeichenfolge}“ an die Dateien an. Sie legt die Lösegeldforderung „{zufällige alphanumerische Zeichenfolge}.README.txt“ ab.

Ausweichen und Verschleierung

BlackMatter-Ransomware löscht Schattenkopien auf dem Computer eines Opfers, um eine Systemwiederherstellung zu verhindern. Sie beendet produktivitätsrelevante Prozesse wie Outlook, Oracle und Notepad, sodass die Ransomware weitere Dateien verschlüsseln kann. Nach der Ausführung erhöht sie auch die Berechtigungen über eine COM-Schnittstelle. Sie nutzt Zeichenfolgenobfuskation und verwendet eine dynamische Win32-API-Auflösungstechnik.

Netzwerkkommunikation

BlackMatter sammelt Informationen wie Bot-Version, Bot-ID, Hostname, Benutzername, Festplatteninformationen, Betriebssystem, Systemarchitektur und verschlüsselte Dateiinformationen. Die Malware kommuniziert über HTTPS und verwendet TLS zur Verschlüsselung, wie im folgenden Screenshot dargestellt. Wenn die Payload nicht über HTTPS kommunizieren kann, wird HTTP zur Kommunikation mit dem Command-and-Control-Server verwendet.

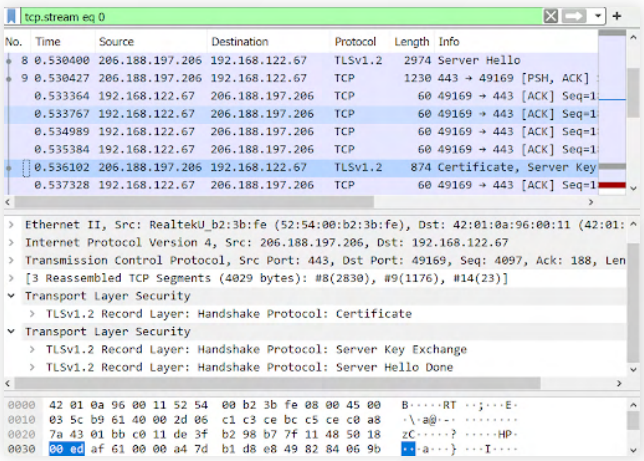

Abbildung 12: *BlackMatter verwendet TLS für die Verschlüsselung*

REvil/Sodinokibi

Zusammenfassung

Die REvil-Ransomware, auch als Sodinokibi bekannt, wurde erstmals im April 2019 entdeckt und über Spam-E-Mails, Exploit-Kits und kompromittierte RDP-Konten verbreitet; Sodinokibi nutzt auch häufig Sicherheitslücken in Oracle WebLogic aus. Sodinokibi verschlüsselt jede Datei und fügt .{zufällige alphanumerische Zeichenfolge} an die Dateien an. Die Verschlüsselung erfolgt mit einer Kombination aus Salsa20- und ECDH-basierten Key-Exchange-Algorithmen. Die Ransomware legt die Lösegeldforderung „{zufallsgenerierte alphanumerische Zeichen}-readme.txt“ ab und ändert den Bildschirmhintergrund im infizierten System.

Ausweichen und Verschleierung

REvil kann UAC-Umgehungstechniken dazu verwenden, um Funktionen mit erhöhten Berechtigungen im Kontext des aktuellen Prozesses auszuführen. REvil verwendet außerdem verschiedene Windows-APIs, um die auf dem Computer installierte Standardsystemsprache zu bestimmen und die bösartigen Aktivitäten nur durchzuführen, wenn die Systemsprache nicht in der vorkonfigurierten Whitelist vorhanden ist. Solche Sprachprüfungen werden häufig von Ransomware-Stämmen durchgeführt, um zu verhindern, dass Opfer in bestimmten Regionen infiziert werden.

Netzwerkkommunikation

REvil sammelt Details zum Benutzernamen, Hostnamen, Domänennamen, dem Tastaturlayout, Betriebssystem, den Laufwerksinformationen, der CPU-Architektur und dem Verschlüsselungsschlüssel des Opfersystems und sendet diese Informationen über HTTPS an seinen Command-and-Control-Server. Die Liste der Domänen ist in der in die Payload eingebetteten Konfiguration enthalten.

Microsoft Office 365

Wir haben beobachtet, wie legitime Hosting-Sites und Online-Code-Editoren wie glitch.me, Codesandbox, Workers Cloudflare und andere für das Hosting von Phishing-Inhalten missbraucht werden. Diese Websites stellen die Phishing-Seiten über HTTPS bereit und unterstützen eine schnelle Webentwicklung. Nachfolgend werden einige Beispiele für solche Phishing-Websites aufgeführt.

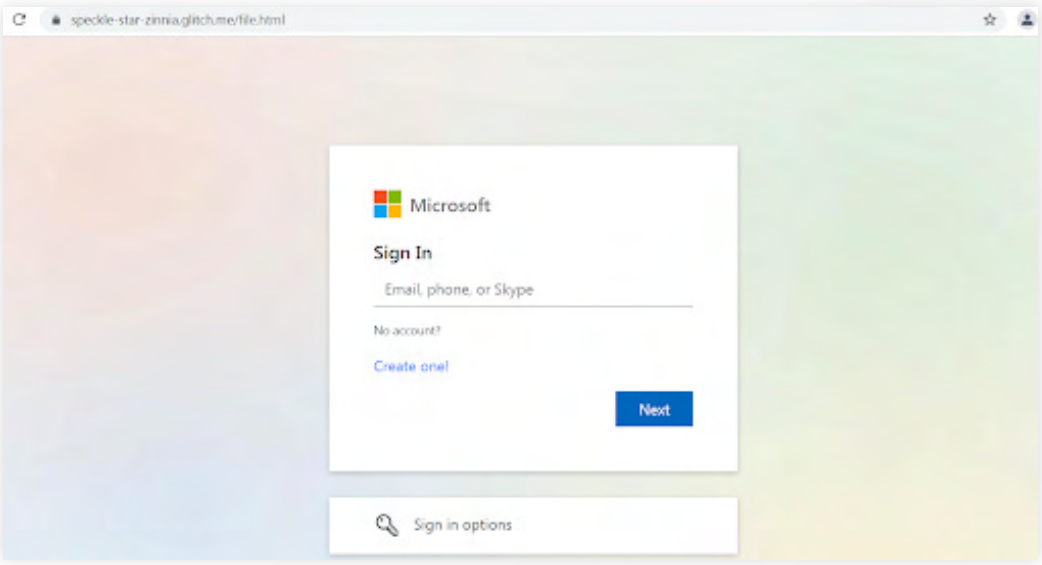

Abbildung 13: *Beispiel für eine Phishing-Website*

Diese Phishing-Seiten verwenden eine mehrschichtige Verschleierung und einige Teile des Quellcodes wurden mit einer Mischung aus JavaScript-Obfuskatoren und Base64-Kodierung verschleiert.

Abbildung 14: *Beispiel für eine mehrschichtige Obfuskation*

Unten wird ein weiteres Beispiel für eine mehrschichtige Obfuskation dargestellt.

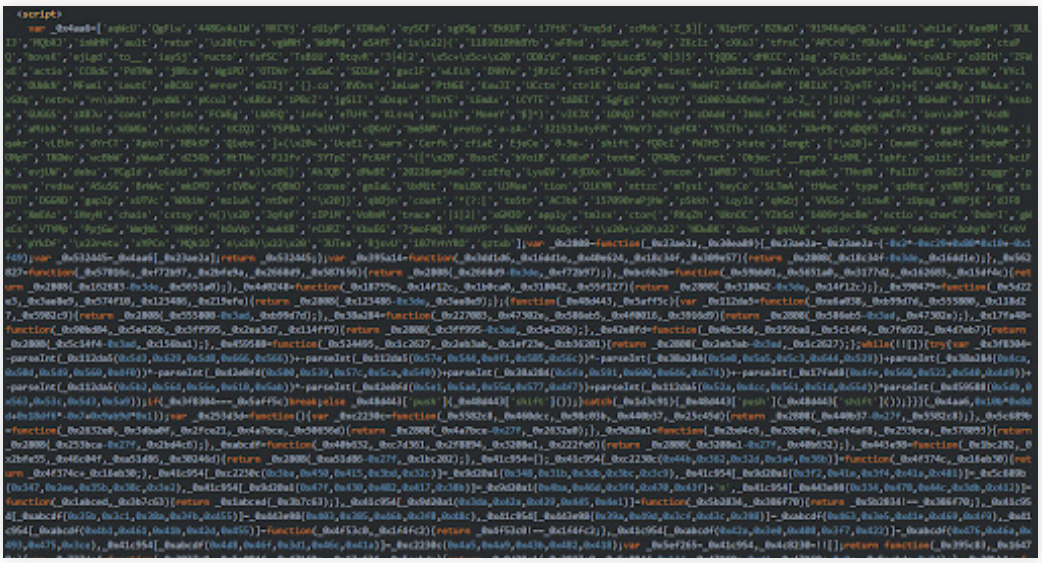

Abbildung 15: *Beispiel für eine mehrschichtige Obfuskation*

Diese Phishing-Websites führen auch ein Fingerprinting von IP-Adressen durch und leiten auf eine legitime Microsoft-Website weiter, wenn die IP-Adresse zu einer der im folgenden Screenshot aufgeführten Unternehmen gehört.

```
$.ajax({
        type: "GET",
        url:'https://pro.ip-api.com/json/?key=tPiZVEq18Ne6eQ1&fields=66846719',
        dataType: "json",
        success: function (res) {
        var e833200 = res.as + " " + res.asname + " " + res.isp;
          if (
          e833200.toLowerCase().indexOf("phish".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("Paypal".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("namecheap".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("Google".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("Amazon".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("M247".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("AVAST".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("Kaspersky".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("BullGuard".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("Wintek Corporation".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("McAfee".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("commodo".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("bitdefender".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("Contina".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("Symantec".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("fireeye".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("NetCraft".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("YandexBot".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("barracuda".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("mimecast".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("appriver".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("proofpoint".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("urlscan".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("urlredirectresolver".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("urlresolver".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("bingbot".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("bot".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("trendmicro".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("spam".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("crawler".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("mozilla".toLowerCase()) >= 0
          || e833200.toLowerCase().indexOf("msnbot".toLowerCase()) >= 0
```

Abbildung 16: *Liste der Unternehmen*

Amazon

Wir haben Fälle von Amazon-Phishing über HTTPS beobachtet. Einer dieser Fälle wird im nachstehenden Screenshot dargestellt. Es ist erkennbar, dass die Zustellregion auf die Vereinigten Staaten voreingestellt wurde. Dies liefert einen Einblick in Bezug auf das Ziel der Phishing-Kampagne.

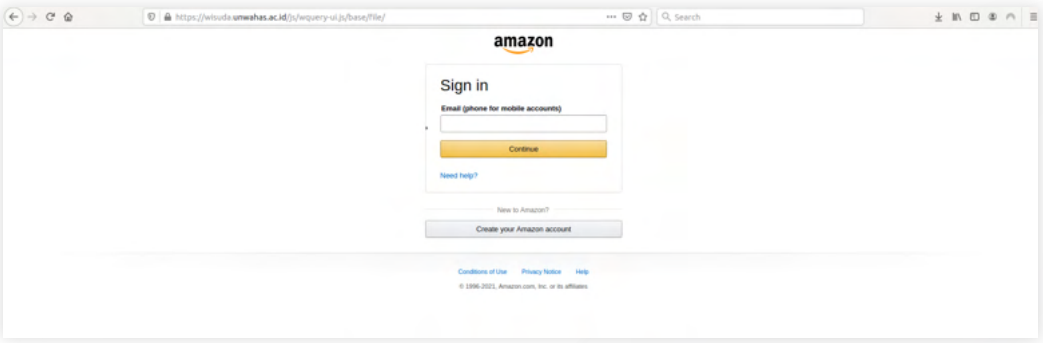

Abbildung 17: *Beispiel für Amazon-Phishing über HTTPS*

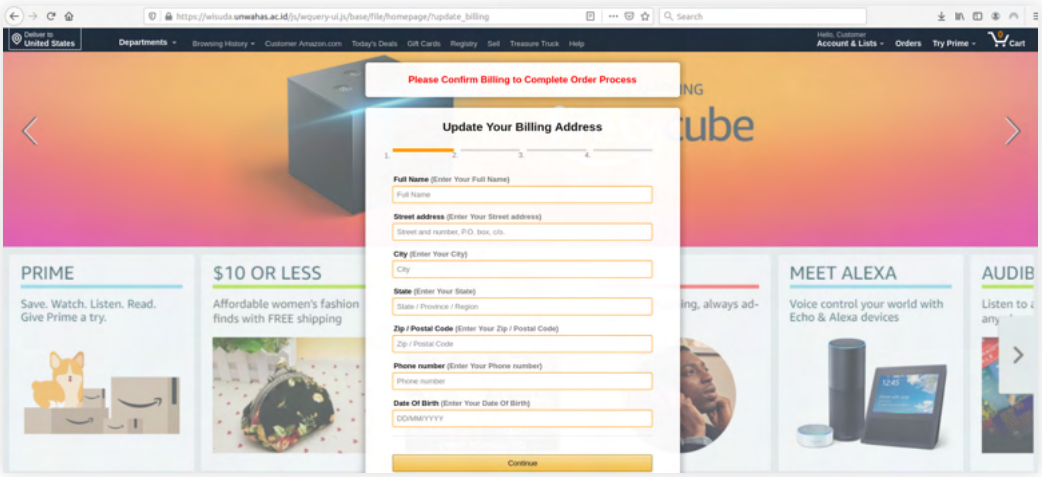

Abbildung 18: *Beispiel für Amazon-Phishing über HTTPS*

Die vom Angreifer verunstaltete Seite an der Adresse der Amazon-Phishing-Hosting-Website wird unten dargestellt.

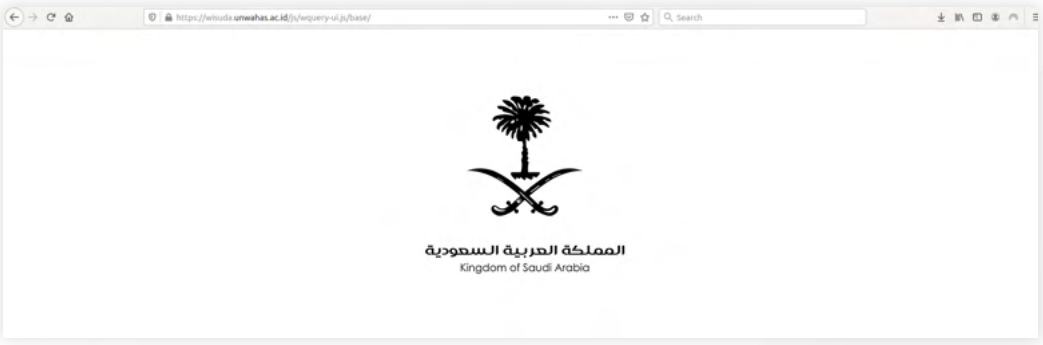

Abbildung 19: *Vom Angreifer verunstaltete Seite*

OneDrive

Wir konnten beobachten, wie Angreifer OneDrive-Phishing-Seiten über HTTPS bereitstellen. Diese wurden von kompromittierten Websites bereitgestellt, auf denen die Phishing-Inhalte gehostet wurden. Der Quellcode liegt in einfacher hexadezimalen Codierung vor, um von Phishing-Inhalts-Scannern unentdeckt zu bleiben.

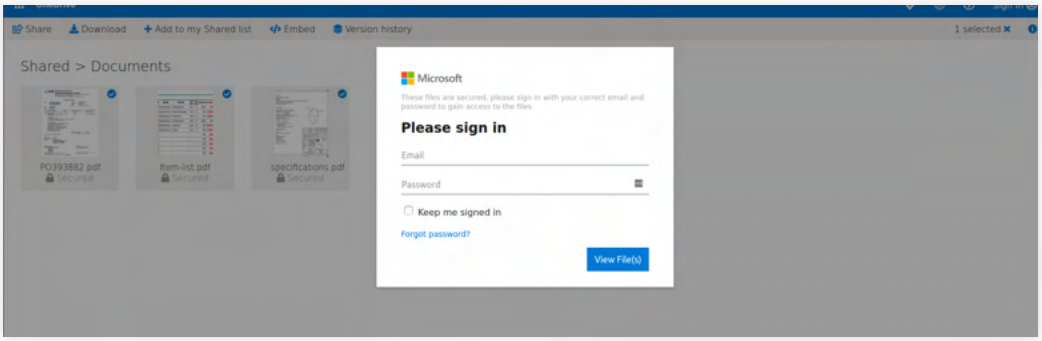

Abbildung 20: *Beispiel für OneDrive-Phishing über HTTPS*

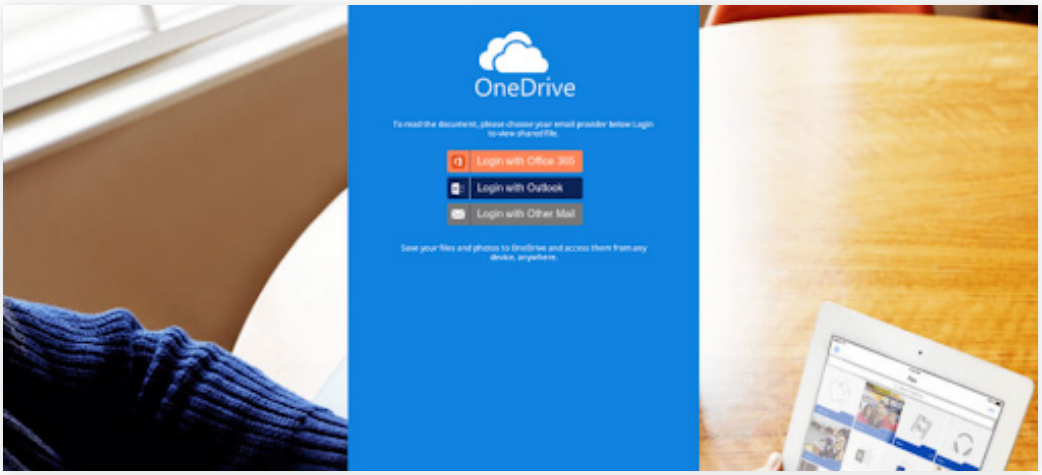

Abbildung 21: *Beispiel für OneDrive-Phishing über HTTPS*

Abbildung 22: *Codierter Teil des Quellcodes*

Telegram

Wir haben Fälle von inoffiziellen Telegram-Web-Clients festgestellt, die HTTPS verwenden. Diese Web-Clients können keine Sicherheit garantieren. Diese Phishing-Seiten fragen die Telefonnummer des Users ab und senden ein einmaliges Passwort an die Telefonnummer des Users. Sobald der User das einmalige Passwort auf der inoffiziellen Website eingibt, verwendet der Web-Client die API von Telegram, um User-Inhalte abzurufen und stellt diese dem User bereit. Dabei gibt es keine Garantie dafür, wie die Nachrichten, Kontaktliste und anderen Details des Users von den bösartigen Web-Clients verwendet werden. Nachfolgend wird ein Beispiel für eine solche Website aufgeführt.

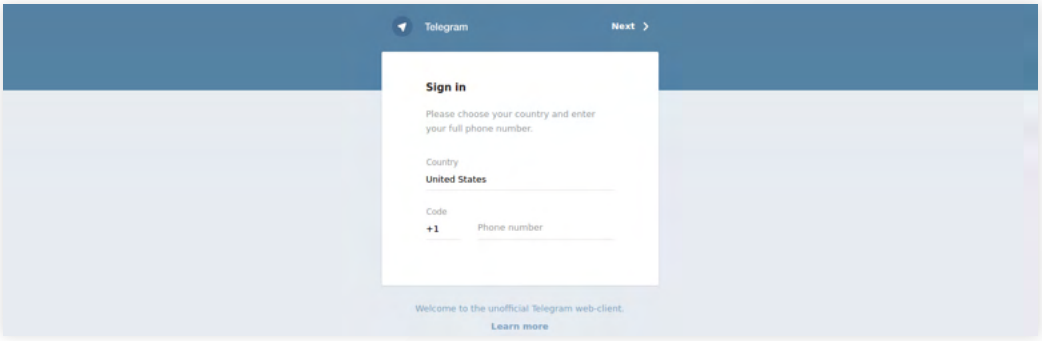

Abbildung 23: *Beispiel für inoffiziellen Telegram-Web-Client, der HTTPS verwendet*

Der Gründer von Telegram empfahl zur Gewährleistung der Sicherheit die Verwendung der offiziellen Telegram-App.

Abbildung 24: *Beispiel für OneDrive-Phishing über HTTPS*

PayPal

Wir haben PayPal-Phishing-Aktivitäten über HTTPS beobachtet. In dem unten dargestellten Fall verfügt eine Shopping-Website über eine kompromittierte PayPal-Zahlungsoption.

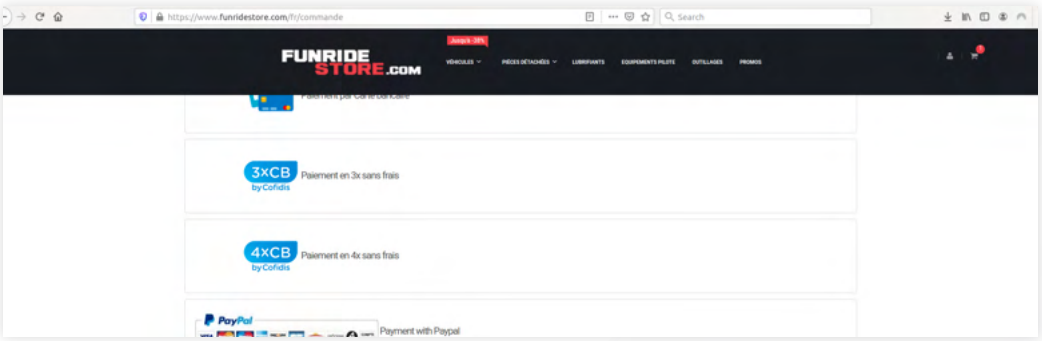

Abbildung 25: *Beispiel für PayPal-Phishing-Aktivität über HTTPS*

Wenn der User Artikel in den Warenkorb legt, werden Versand- und Kontaktinformationen abgefragt. Nach Eingabe der Daten werden dem User verschiedene Zahlungsoptionen angeboten. Der hier dargestellte PayPal-Zahlungslink ist kompromittiert. Wenn der User die PayPal-Option auswählt, wird er zu der unten dargestellten Phishing-Seite weitergeleitet.

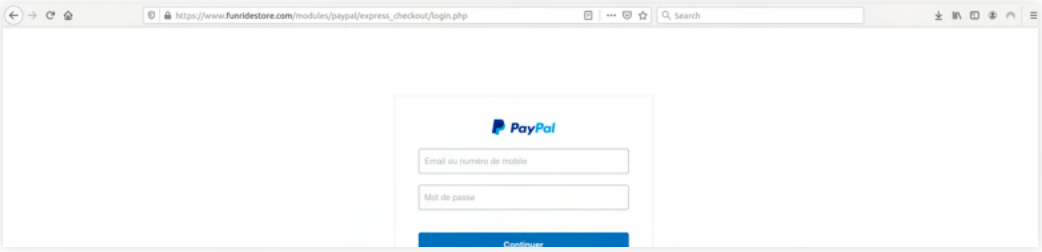

Abbildung 26: *PayPal-Phishing-Seite*

Bei Eingabe der PayPal-Zugangsdaten wird der User zur legitimen PayPal-URL weitergeleitet, wo er sich anmelden und den Kauf abschließen kann.

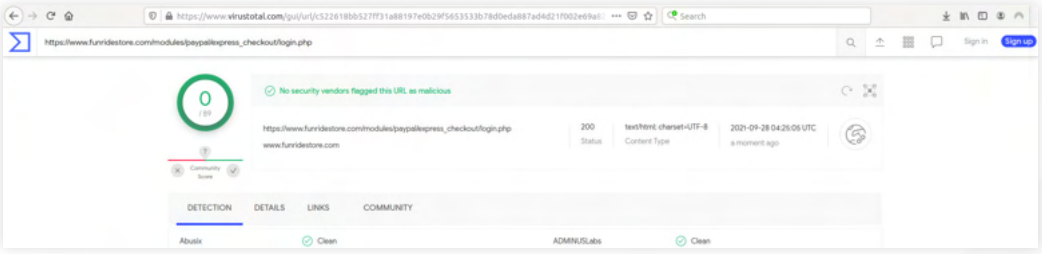

Abbildung 27: *PayPal-Phishing-Seite*

Hierbei handelt es sich um ein interessantes Beispiel für Social Engineering. Auf einer legitimen Shopping-Seite wurde der PayPal-Phishing-Link dort platziert, wo die Kunden einen legitimen Link erwarten würden. Die Kreditkartenzahlungslinks verweisen auf legitime URLs und nur der PayPal-Link wurde kompromittiert.

Wir beobachten häufig, dass Angreifer bei gezielten Angriffen Tools wie Cobalt Strike, Mimikatz, LaZagne und andere einsetzen, um eine laterale Ausbreitung, Datenexfiltration und andere C&C-Aktivitäten durchzuführen. Cobalt Strike ist bei solchen gezielten Angriffen nach wie vor eines der am häufigsten verwendeten Tools.

Cobalt Strike

Es wurden 24.410 blockierte Downloads und 172.568 blockierte Callbacks über TLS beobachtet.

Zusammenfassung

Cobalt Strike ist ein kommerzielles Tool für Adversary Simulation und Red-Team-Einsätze. Es handelt sich um eine voll funktionsfähige Software mit vordefinierten und konfigurierbaren Command-and-Control-Profilen (C&C), die eine Änderung des Verhaltens und der Netzwerkindikatoren ermöglichen, um Taktiken, Techniken und Verfahren unterschiedlicher Malware-Familien zu simulieren, die bei realen Angriffen verwendet werden. Obwohl es sich dabei um ein legitimes kommerzielles Tool handelt, wird es immer wieder von Angreifern bei echten Angriffen eingesetzt. Verschiedene APT-Gruppen, wie die folgenden, verwenden bekanntermaßen das Cobalt-Strike-Framework:

- APT19
- DarkHydrus
- CopyKittens
- APT32
- Cobalt Group
- APT29
- Leviathan
- FIN6

Cobalt Strike ist eine dateilose Malware und unterstützt mehrstufigen Shellcode, der für unterschiedliche Zwecke verwendet werden kann.

Netzwerkkommunikation

Cobalt Strike kann anhand einer Funktion namens „Malleable C&C Profiles“ so konfiguriert werden, dass es über ein oder mehrere Protokolle kommuniziert:

- DNS (TXT-, A- und AAAA-Datensätze)
- HTTP/HTTPS
- SMB (benannte Pipes)
- TCP

Ausweichtechniken

Cobalt Strike wird oft als letzte Payload abgelegt, die auch benannte Pipes verwendet. Dabei handelt es sich um Sockets, die die Kommunikation zwischen Prozessen oder sogar Hosts ermöglichen. Zu den Post-Exploit-Funktionen von Cobalt Strike gehören Keylogger, Mimikatz und Screenshot-Module.

Laterale Ausbreitung mit gestohlenen Zugangsdaten

Cobalt Strike nutzte gestohlene Zugangsdaten, um über Server Message Block (SMB) mit einer Remote-Netzwerkfreigabe zu interagieren, sich über das Remote Desktop Protocol (RDP) bei einem Computer anzumelden und sich bei einem Dienst anzumelden, der speziell für die Annahme von Remote-Verbindungen entwickelt wurde, etwa Telnet, SSH und VNC.

PoshC2

Es wurden 98.591 blockierte Callbacks über TLS beobachtet.

PoshC2 ist ein Proxy-bewusstes C&C-Framework, das Penetrationstester bei Red Teaming, Post-Exploit und lateraler Ausbreitung unterstützt.

PoshC2 ist hauptsächlich in Python3 geschrieben. Das vorkonfigurierte PoshC2 umfasst Programme in PowerShell/C# und Python2/Python3 zum Einschleusen sowie Payloads mit Quellcode in PowerShell v2 und v4, C++ und C#. Diese ermöglichen C&C-Funktionen auf einer Vielzahl von Geräten und Betriebssystemen, u. a. Windows, *nix und OSX.

PoshC2 kann mit SharpSocks verwendet werden, das ein C#-Reverse-HTTPS-Tunneling-Socks-Proxy ermöglicht, sodass der C&C-Traffic über HTTPS laufen kann.

Ursnif

Es wurden 336.540 blockierte Downloads und 87.821 blockierte Callbacks über TLS beobachtet.

Zusammenfassung

Ursnif (auch bekannt als Gozi) ist ein Bank-Trojaner. Es gibt aber Varianten, die Komponenten wie Backdoors, Spyware, File Injectors und mehr enthalten. Er wurde erstmals 2006 entdeckt und ist seitdem ununterbrochen aktiv. Die Malware wird anhand von länderspezifischen Phishing-Kampagnen verbreitet.

Persistenzmechanismus

Ursnif verwendet zwei Mechanismen, um Persistenz zu erzeugen:

1. Erstellen einer neuen geplanten Aufgabe (mit dem Namen „Power<zufälliges_Wort>“ (z. B. PowerSgs)).
2. Sollte dies aus irgendeinem Grund nicht gelingen, verwendet die Malware den Registrierungsschlüssel „HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run“, um Persistenz über einen Neustart des Systems zu gewährleisten.

Netzwerkaktivität

Sobald die Malware auf dem Rechner Fuß gefasst hat, startet sie ihren Haupt-Arbeitsthread, der den C&C-Server kontinuierlich nach Befehlen abfragt. Diese Malware sammelt Userinformationen wie „User“, „Server“ und „ID“ als Hash-Werte sowie „Uptime“, ein Zeitwert, der angibt, wie lange das Gerät bereits läuft. „DNS“ ist der Computername, und „whoami“ ist der vollständige Username. Die Malware nutzt in einigen Fällen HTTPS, um ihren C&C-Server zu kontaktieren und Daten an ihn zu übertragen.

Dridex

Es wurden 50.088 blockierte Downloads und 11.167 blockierte Callbacks über TLS beobachtet.

Zusammenfassung

Dridex, auch als Bugat und Cridex bekannt, ist ein Trojaner, der sich auf den Diebstahl von Bankzugangsdaten spezialisiert hat.Er tauchte erstmals 2011 auf und wurde im Laufe der Jahre weiterentwickelt. Er wurde in mehreren Phishing-Kampagnen eingesetzt, die Microsoft Word- und Excel-Dokumente als Payloads verwendeten.

Ausweichtechniken

Dridex wird durch das Cutwail-Botnet oder das RIG-Exploit-Kit verbreitet. Dridex ist auch für Phishing-Kampagnen bekannt, die auf aktuellen Ereignissen basieren, z. B. dem SpaceX-Start.

Netzwerkkommunikation

Die Dridex-Dokumenten-Payload enthält C&C für die nächste Stufe. Der C&C-Server wird über HTTPS kontaktiert, um eine DLL-Datei (Dynamic Link Library) herunterzuladen. Dabei handelt es sich um die endgültige Payload, die den User infiziert und weitere C&C-Server kontaktiert. Eine Variante von Dridex, die auch als DoppelDridex bekannt ist, hat in ihren jüngsten Kampagnen damit begonnen, cdn.discordapp.com und Slack als C&C-Server zu verwenden, der die DLL-Datei enthält.

Zscaler überprüft den gesamten SSL-Traffic – ohne Beeinträchtigung der Performance oder Bedenken im Hinblick auf die Compliance. Erfahren Sie anhand unseres Tools zur **Analyse der Internet-Bedrohungslage**, ob Sie SSL-/TLS-Traffic überprüfen können.

Über ThreatLabZ

ThreatLabZ ist die Abteilung für Sicherheitsforschung von Zscaler. Das erstklassige Team ist dafür verantwortlich, neue Bedrohungen aufzuspüren und sicherzustellen, dass Tausende von Organisationen, die die globale Plattform von Zscaler nutzen, permanent geschützt sind. Neben der Erforschung von Malware und der Erstellung von Verhaltensanalysen beschäftigen sich die Teammitglieder auch mit der Erforschung und Entwicklung neuer Prototypmodule für den erweiterten Schutz vor Bedrohungen auf der Zscaler-Plattform und führen regelmäßig interne Sicherheitsüberprüfungen durch, um zu gewährleisten, dass Produkte und Infrastruktur von Zscaler den Sicherheitsstandards entsprechen. ThreatLabZ veröffentlicht regelmäßig detaillierte Analysen von neuen und aufkommenden Bedrohungen auf seinem Portal: **research.zscaler.com**.

Über Zscaler

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

zscaler™