Report zum Status verschlüsselter Angriffe 2022

Inhaltsverzeichnis

Einführung

Ist verschlüsselter Traffic wirklich sicher? Nicht immer.

Bei HTTPS handelt es sich um ein Kommunikationsprotokoll, das Schutz für Daten während der Übertragung von einem Webserver an einen Browser bietet. In den Anfängen des Internets wurde HTTPS ausschließlich bei der Übertragung sensibler Daten genutzt, doch inzwischen sind die Vorteile der Verwendung von HTTPS zum Schutz aller Daten allgemein bekannt. Bei verschlüsseltem Traffic kann es sich um verschiedenste Informationen handeln: einen Usernamen und ein Passwort, eine Kreditkartennummer — oder sogar um Malware.

Da HTTPS zum Standard für die Übertragung von Daten über das Internet geworden ist, haben sich User und Organisationen bereits an das kleine Schloss in ihrer Browserleiste gewöhnt. Somit sind auch Angreifer dazu gezwungen, HTTPS zu verwenden, um keinen Verdacht zu erregen — das Protokoll schützt also nicht nur sensible Userdaten, sondern kann auch dazu dienen, schädlichen Code zu verbergen. Verschlüsselter Traffic wird von Sicherheitsteams nicht nur seltener überprüft, sondern ein Fingerprinting verschlüsselter Dateien ist auch viel schwieriger, sodass Malware unentdeckt eingeschleust werden kann.

Tatsächlich werden Gefahren oft übersehen. Zwischen Oktober 2021 und September 2022 blockierte Zscaler 24 Milliarden Bedrohungen über HTTPS. Dies entspricht einer Zunahme von mehr als 20 % gegenüber den 20,7 Milliarden blockierten Bedrohungen im Jahr 2021, was im Vorjahresvergleich bereits damals einen Anstieg um fast 314 % darstellte.

Cyberkriminelle entwickeln ihre Taktiken stetig weiter, um nicht entdeckt zu werden und aktuelle Trends, wie etwa hybride Arbeit, zu ihrem Vorteil zu nutzen. Auch ist es dank Malware- und Ransomware-as-a-Service so einfach wie nie, auf den fahrenden Zug aufzuspringen. Eigenen Code schreiben oder die Infrastruktur einrichten zu können, ist nicht länger erforderlich, um eine Ransomware-Kampagne zu starten und durchzuführen. Alles, was Cyberkriminelle benötigen, ist im Dark Web als Service zu finden.

Organisationen müssen den gesamten Traffic überprüfen — sowohl On- als auch Off-Premise — damit verschlüsselte Bedrohungen nicht ins Unternehmen eingeschleust werden können. Leider ist ein solches Vorgehen unglaublich ressourcenintensiv. Eine Überprüfung des Traffics in großem Maßstab ist mit herkömmlichen hardwarebasierten Sicherheitstools nahezu unmöglich. Mitunter ist die fünf- bis siebenfache Anzahl von Firewalls der nächsten Generation erforderlich, um verschlüsselten Traffic effektiv und ohne Leistungseinbußen zu prüfen. Infolgedessen lassen viele Organisationen zumindest einen Teil des verschlüsselten Traffics ungeprüft passieren und setzen sich damit einem erheblichen Risiko aus.

Haupterkenntnisse

Die Zscaler Zero Trust Exchange beherbergt die größte Sicherheitsdatenbasis der Welt, die aus über 300 Billionen Signalen und 260 Milliarden täglichen Transaktionen aufgebaut wurde. ThreatLabz, das Expertenteam von Zscaler für Bedrohungsanalysen, untersuchte diese Daten von Oktober 2021 bis September 2022. Die folgende Analyse gibt aufschlussreiche Einblicke in verschlüsselte Angriffe. Zu den Haupterkenntnissen gehören:

Bei mehr als 85 % der Angriffe werden inzwischen verschlüsselte Kanäle in verschiedenen Phasen der Kill Chain (Phishing, Malware-Bereitstellung, C&C-Aktivitäten usw.) verwendet. Im Vorjahr waren es noch 80 %.

Bedrohungen über HTTPS haben zugenommen: Zscaler hat im Vergleich zum Vorjahr einen Anstieg der Bedrohungen im verschlüsselten Traffic um 20 % festgestellt.

Die Fertigungsbranche ist eines der Hauptziele: Verschlüsselte Bedrohungen, deren Angriffsziele Fertigungsbetriebe sind, haben im Vergleich zum Vorjahr um **239 % zugenommen**.

Weniger verschlüsselte Bedrohungen im Einzelhandel und in Behörden: Der Einzelhandel verzeichnete seit dem letzten Jahr einen Rückgang der verschlüsselten Bedrohungen um **63 %**, bei Behörden sank diese Zahl um **40 %**.

Die USA und Indien sind Hauptziele verschlüsselter Angriffe: Unter den fünf am stärksten betroffenen Ländern sind außerdem Südafrika, das Vereinigte Königreich und Australien.

Es gibt immer mehr verschlüsselte Angriffe und sie werden immer raffinierter: Zscaler fand und blockierte 2022 jedeArt von Bedrohung häufiger im SSL/TLS-Traffic als 2021.

Zero Trust ist die beste Verteidigung gegen verschlüsselte Bedrohungen: Eine Cloud-Proxy-basierte Zero-Trust-Architektur minimiert die Angriffsfläche und ermöglicht eine Inline-Überprüfung des gesamten Traffics im großen Maßstab.

Überblick über verschlüsselte Bedrohungen

Moderne Verschlüsselungsmethoden, einschließlich Secure Sockets Layer (SSL) und dessen Nachfolger Transport Layer Security (TLS), werden weltweit eingesetzt, um den Großteil des Internet-Traffics zu schützen. Laut Google sind 95 % des dort generierten Traffics verschlüsselt. Die Verschlüsselungsraten für legitimen Traffic steigen ebenso wie für schädlichen Traffic.

Schon das dritte Jahr in Folge stieg die Anzahl verschlüsselter Bedrohungen, die von Zscaler blockiert wurden — sowohl gemessen am Gesamtvolumen als auch am prozentualen Anteil. Das zeigt deutlich, dass Cyberkriminelle zunehmend auf neue Taktiken umsteigen.

Im Jahr 2022 blockierte Zscaler in einem Zeitraum von neun Monaten 24 Milliarden Bedrohungen, eine Steigerung von 20 % gegenüber 2021. Bei mehr als 85 % dieser Angriffe kamen verschlüsselte Kanäle zum Einsatz.

Es gibt verschiedene Arten von Bedrohungen, die Cyberkriminelle im verschlüsselten Traffic verbergen können. Malware ist immer noch die bei weitem am häufigsten anzutreffende Bedrohungskategorie, auch wenn der Anteil dieser Angriffe von 90,8 % auf 89,8 % gesunken ist. Auch Ransomware ist eine Form der Malware und aus gutem Grund eine der wichtigsten Prioritäten von CISOs auf der ganzen Welt. Allein Ransomware-Angriffe haben im Vergleich zum Vorjahr um 80 % zugenommen.

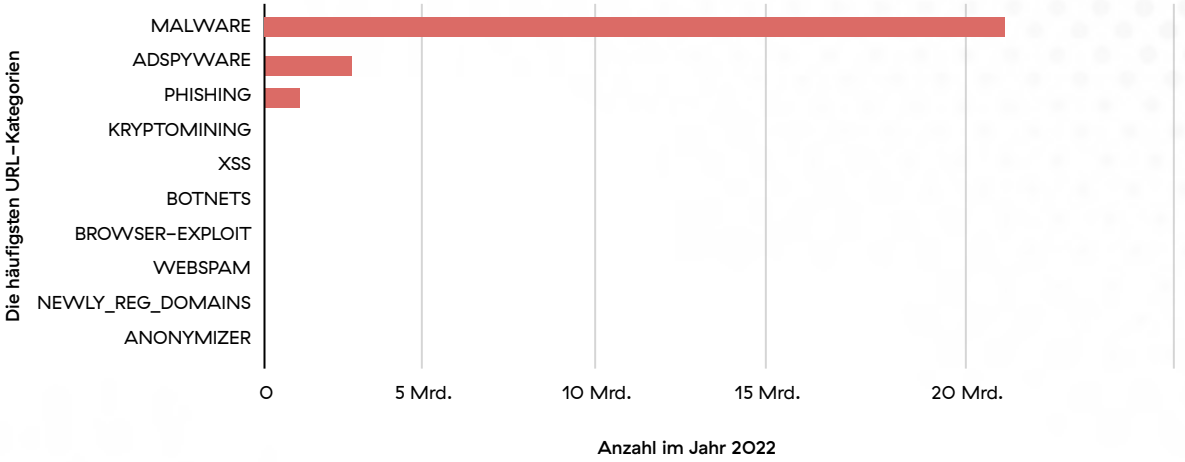
Es gibt immer mehr verschlüsselte Angriffe und sie werden immer raffinierter: Zscaler fand und blockierte 2022 jede Art von Bedrohung häufiger im SSL/TLS-Traffic als 2021. Einige der weniger verbreiteten Kategorien, wie Webspam und Browser-Exploits, machen zwar weniger als 0,1 % aller Angriffe aus, wachsen jedoch am schnellsten. Die Anzahl der Webspam-Angriffe stieg beispielsweise um 1.642 % an.

Phishing über verschlüsselte Kanäle nahm im Vergleich zum Vorjahr um 89 % zu. Aus unserem aktuellen Report zu Phishing-Angriffen geht aber hervor, dass im Jahr 2022 nur 29 % mehr Phishing-Angriffe auftraten, was darauf hindeutet, dass die Nutzung verschlüsselter Kanäle bei dieser Kategorie erheblich zunimmt. Dieser Trend ist wahrscheinlich auf die weite Verbreitung von Phishing-Kits und Phishing-as-a-Service-Modellen zurückzuführen, mithilfe derer Angreifer auch mit geringem technischem Know-how ausgefeilte Angriffe durchführen können.

Trotz des Preiseinbruchs von Kryptowährungen im Jahr 2022 und rückläufiger Gewinne für Miner bleibt Kryptojacking die vierthäufigste Bedrohung und verzeichnete ein deutliches Wachstum von 144 % im Vergleich zum Vorjahr, nachdem 2021 noch ein Rückgang zu beobachten war.

Methodik: Analyse von 24 Milliarden blockierten Bedrohungen über SSL- und TLS-Kanäle von Oktober 2021 bis September 2022 in der Zscaler Cloud.

Verschlüsselte Angriffe nach Typ



2022 im Vergleich zu 2021:	
WEBSPAM	1641,65 %
BROWSER-EXPLOIT	188,63 %
KRYPTOMINING	144,44 %
PHISHING	89,07 %
XSS	81,27 %
MALWARE	13,98 %
AD-SPYWARE	6,47 %
BOTNETS	3,49 %

Die häufigsten Bedrohungskategorien

Malware: 89,9 % der Angriffe

Im Jahr 2022 war Malware die mit Abstand am häufigsten auftretende Bedrohungskategorie. In der Regel wird sie von Usern verbreitet, die über Links in E-Mails oder Websites schädliche Payloads herunterladen. Zwar verfügen die meisten Organisationen über eine Art Malware-Schutz, doch Angreifer entwickeln ihre Techniken stetig weiter und entwerfen neue Malware-Varianten, die in der Lage sind, auf Zuverlässigkeit basierte Erkennungstechnologien zu umgehen.

Daher können Organisationen, die verschlüsselten Traffic nicht überprüfen, Malware erst identifizieren, nachdem ihre Systeme bereits infiziert sind. Im Folgenden sind die häufigsten Malware-Familien aufgeführt, die im Jahr 2022 entdeckt wurden.

Cyberkriminelle verbergen zwar die verschiedensten Bedrohungen im verschlüsselten Traffic, doch Malware ist nach wie vor die am häufigsten eingesetzte Kategorie. Schädliche Skripte und Payloads, die während der gesamten Angriffssequenz verwendet werden, machen fast 90 % der verschlüsselten Bedrohungen aus, die im Jahr 2022 blockiert wurden.

ChromeLoader verwendet PowerShell, um dem Chrome-Browser eines Users eine bösartige Erweiterung hinzuzufügen. Diese ändert die Webbrowser-Einstellungen des Users so, dass schädliche Werbung für gefälschte Werbegeschenke, Umfragen, nicht jugendfreie Spiele oder Dating-Seiten angezeigt und die Suchanfragen des Users weitergegeben werden.

Gamaredon, auch bekannt als Primitive Bear, Shuckworm oder Actinium, ist ein russischer APT, der auf ukrainische Regierungsbehörden und kritische Infrastruktur abzielt. Die Multiplattform-Malware verschafft sich Zutritt, öffnet eine Backdoor, erstellt für spätere Angriffe Fingerabdrücke von Systemen und stiehlt wichtige Informationen.

AdLoad ist eine auf macOS abgestimmte Malware, die die integrierten macOS-Sicherheitstools und Antivirenprogramme von Drittanbietern umgeht. Sie ruft unsichere URLs auf und lädt unbemerkt unerwünschte Software herunter.

SolarMarker stiehlt vor allem Informationen und erstellt Backdoors. Die Malware wird hauptsächlich über SEO-Poisoning verbreitet, eine Angriffsmethode, bei der Cyberkriminelle bösartige Websites mit beliebten Schlüsselwörter erstellen und Techniken zur Suchmaschinenoptimierung einsetzen, damit sie möglichst weit oben in den Suchergebnissen platziert werden.

Manuscrypt ist ein Remote-Access-Tool (RAT), das auf Kryptowährungsbörsen und ähnliche Entitäten abzielt. Manuscrypt ist in der Lage, beliebige Befehle auszuführen, Systeme auszuspähen und Daten zu exfiltrieren.

Ad-Spyware: 6,3 % der Angriffe

Verschlüsselte Ad-Spyware stellt weiterhin eine Bedrohung für User dar. Der Anteil von Ad-Spyware an allen verschlüsselten Angriffen ist nur leicht gesunken — von 6,8 % im Jahr 2021 auf 6,3 % im Jahr 2022. Angreifer verbreiten Ad-Spyware, indem sie sie mit anderer Software kombinieren. Die User akzeptieren ahnungslos die Nutzungsbedingungen der Software, woraufhin die Ad-Spyware unbemerkt auf dem System installiert und der User von Pop-up-Anzeigen überhäuft wird. Zu den wichtigsten Ad-Spyware-Familien im Jahr 2022 gehören:

Popads ist ein legitimes Werbenetzwerk, das von Website-Publishern genutzt wird, um Einnahmen zu erzielen. Bestimmte Adware leitet jedoch zu Popads.net weiter und zeigt betrügerische Werbung auf dem Computer des Endusers an.

Searchprotect legt im Webbrowser des Users eine neue Startseite sowie Suchmaschine fest und hindert den User daran, diese Änderungen rückgängig zu machen. Öffnet der User einen neuen Browser-Tab, werden unzählige Werbe-Pop-ups eingeblendet, die nicht geschlossen werden können.

PremierOpinion zeigt Umfragen auf Shopping-Websites an. Es erfasst und überträgt die Aktivitäten des Users, einschließlich Surfverhalten, demografischer Daten und Anwendungsnutzung. PremierOpinion beeinträchtigt zudem die Browser- und CPU-Performance.

MindSpark modifiziert die Standard-Browsereinstellungen und ändert die Sucheinstellungen. Die Spyware ist auch in der Lage, die Browserleistung zu beeinträchtigen und konkurrierende Software zu blockieren. Außerdem kann MindSpark die Startseite des Users ändern und Pop-up-Anzeigen einblenden.

Phishing: 3 % der Angriffe

Phishing-Angriffe in verschlüsseltem Traffic haben sich von 1,8 % im Jahr 2021 auf 3 % im Jahr 2022 fast verdoppelt. Bei Phishing wird Social Engineering eingesetzt, um den Empfängern vorzugaukeln, dass es sich bei einer eingehenden E-Mail oder SMS um einen vertrauenswürdigen Absender, beispielsweise ein bekanntes Unternehmen, handelt. Das Ziel hinter dieser Methode ist es, den Empfänger zur Weitergabe vertraulicher Informationen oder zum Klicken auf einen Link zu bewegen, der versteckte Malware enthält.

Cyberkriminelle neigen dazu, sich als beliebte Marken auszugeben, um speziell User dieser Marke zu überlisten. Auch nutzen sie das öffentliche Interesse an aktuellen Themen wie COVID-19 aus. Da viele User weiterhin zumindest teilweise von zu Hause aus arbeiten und die COVID-19-Pandemie nach wie vor im Fokus steht, war es nicht überraschend, dass die Themen, die 2022 am häufigsten im Rahmen von Phishing-Angriffen genutzt wurden, denen des Jahres 2021 sehr ähneln.

Kryptomining und Kryptojacking: 0,5 % der Angriffe

Kryptomining-Software dient, wie der Name schon sagt, zum Schürfen von Kryptowährungen. In ähnlicher Weise wird Kryptojacking von Cyberkriminellen eingesetzt, um die Rechenleistung eines Zielsystems zu missbrauchen und im Namen des Angreifers Kryptowährungen zu generieren. Kryptojacking wirkt sich auf verschiedene Weise auf Organisationsnetzwerke aus: Unerwünschte und unerkannte Mining-Aktivitäten innerhalb von Netzwerken führen zu einem erhöhten Verschleiß der Organisationshardware, da sich die CPU-Zyklen erhöhen. Zudem beanspruchen diese Aktivitäten auch die Netzwerkbandbreite der Organisation und führen zu Performanceproblemen.

Kryptojacking erlebte im Jahr 2022 ein Comeback: Nach einem Rückgang im Jahr 2021 stieg die Zahl der Kryptojacking-Angriffe im vergangenen Jahr um 144 %. Es ist wahrscheinlich, dass Cyberkriminelle die Gelegenheit erkannt haben, die Rechenleistung der User auszunutzen, da diese zu einem hybriden Arbeitsmodell übergegangen sind und einen Teil der Zeit zu Hause und den anderen Teil im Büro arbeiten.

Zu den relevantesten Kryptojackern im Jahr 2022 gehören:

Xmrig ist ein Open-Source-Kryptojacker, der in andere Malware integriert werden kann. Xmrig selbst stiehlt keine sensiblen Informationen und verschlüsselt selbst auch keine Daten. Sein einziger Zweck besteht darin, Kryptowährungen zu schürfen, sodass er in erster Linie die Ressourcen seiner Opfer verbraucht.

ThetaToken ist eine Blockchain, die über ein dezentrales Netzwerk betrieben wird, in dem User Ressourcen und Videoinhalte teilen. Über die Plattform streamen User Videos, indem sie ihre Bandbreite und zusätzliche Rechenkapazitäten im Tausch gegen Belohnungen anbieten, die Theta Tokens genannt werden.

ElectrumStealer ist eine als Trojaner konzipierte Version des beliebten Bitcoin-Wallet-Service Electrum, der auf macOS abzielt. Er exfiltriert Passwörter und andere Daten auf einen Server, den die Cyberkriminellen im Electrum-Netzwerk kontrollieren.

Webmine ist wie Coinhive in Websites eingebettet. Mit dem JavaScript-Miner können Website-Publisher die CPU-Leistung ihrer User nutzen, um die Kryptowährung Monero zu schürfen.

CoinIMP ist ein JavaScript-Miner, der in Websites eingebettet ist. Mithilfe von CoinIMP haben User die Möglichkeit, Website-Publisher mit CPU-Ressourcen für ihre Inhalte zu bezahlen. Der Web-Miner wird normalerweise nicht von Antiviren- oder Adblocker-Software blockiert. Sollte dies dennoch passieren, reagieren die Entwickler sofort und arbeiten an einer Lösung.

XSS: 0,2 % der Angriffe

Cross-Site-Scripting (XSS) verzeichnete einen leichten Anstieg von 0,1 % der verschlüsselten Angriffe im Jahr 2021 auf 0,2 % im Jahr 2022. Bei einem XSS-Angriff schleusen Cyberkriminelle schädlichen Code in legitime Websites ein.

Versuchte Botnet-Rückrufe: 0,2 % der Angriffe

Die häufigsten über HTTPS blockierten Malware-Familien nach CnC-Aktivität

Ein Botnet ist ein Netzwerk von Computern, die mit Schadsoftware infiziert sind und zur Durchführung von Angriffen von einem Cyberkriminellen ferngesteuert werden. Der Anteil der von infizierten Systemen ausgehenden Botnet-Rückrufaktivitäten lag 2022 bei 0,2 % aller verschlüsselten Angriffe, nachdem er 2021 sprunghaft um 132 % gegenüber 2020 angestiegen war.

SmokeLoader ist ein Trojaner, den Cyberkriminelle in erster Linie nutzen, um andere Malware auf infizierten Systemen zu platzieren. Mithilfe von Plugins kann SmokeLoader allerdings auch erweitert werden, wodurch sich Informationen exfiltrieren lassen. Der Trojaner wird über Exploit-Kits und E-Mail-Kampagnen verbreitet und als scheinbar legitime Anwendung angeboten.

Gumblar ist ein Trojaner, der schädlichen JavaScript-Code in die Seiten einer Website oder den Webbrowser eines Users einschleust. Gumblar leitet die Google-Suche der User um und installiert dann über eine PDF-Schwachstelle bösartige Sicherheitssoftware.

RecordBreakerStealer ist eine weiterentwickelte Version von Raccoon Stealer. Der Infostealer wird als Malware-as-a-Service (MaaS) verkauft und ist darauf ausgelegt, Daten und Inhalte aus dem infizierten System zu exfiltrieren. Dank ihrer Einfachheit und des hervorragenden Support-Services ist die Malware bei Cyberkriminellen sehr beliebt.

Cobalt Strike ist eine kommerzielle Software für Penetrationstests, die sich vor allem an ethische Hacker richtet. Die Software wird jedoch auch von Cyberkriminellen eingesetzt, da sie eine Vielzahl von Funktionen bietet, die zur Durchführung verschiedener Angriffe genutzt werden können, von Ransomware-Operationen bis hin zu spionageorientierten Advanced Persistent Threats (APTs).

QuasarRAT ist ein voll funktionsfähiger Open-Source-RAT (Remote-Access-Trojaner), der hauptsächlich auf Microsoft Windows-Betriebssysteme abzielt. QuasarRAT ist seit mindestens 2014 auf GitHub verfügbar und bietet eine Vielzahl von Techniken und Funktionen, darunter einen integrierten Keylogger und die Option, Passwörter und Dateien von kompromittierten Computern abzurufen.

Occamy ist ebenfalls ein RAT, den Cyberkriminelle zum Eindringen in ein Zielsystem verwenden. Sobald er auf dem infizierten System platziert ist, kann Occamy verwendet werden, um u. a. Sicherheitsprogramme zu deaktivieren, Daten zu stehlen, den Host in ein Botnet einzuschreiben oder zusätzliche Malware auf dem System zu installieren. Occamy wird häufig über E-Mail-Spam-Kampagnen und Software-Cracks oder Keygens verbreitet, die aus dem Internet heruntergeladen werden.

Angriffe auf Mobil- und IoT-Geräte

Angreifer nutzen Mobil- und IoT-Geräte für eine Vielzahl bösartiger Aktionen, die von sehr gezielten Methoden wie dem Einschleusen von Malware auf Smartphones über die Umgehung von MFA bis hin zu unglaublich breit angelegten Botnet-Angriffen reichen, bei denen IoT-Geräte zur Durchführung umfangreicher DDoS- (Distributed Denial of Service), Scraping-, Kryptojacking- und Spam-Angriffe genutzt werden.

Angreifer verschaffen sich häufig über SMiShing, eine Form des Phishings, Zugriff auf Mobilgeräte. Dabei werden SMS-Nachrichten, schädliche mobile Websites und betrügerische Apps genutzt, die in App-Stores als legitime Anwendungen ausgegeben werden. Berichten von ThreatLabz zufolge kursierten in den zurückliegenden drei Monaten mehr als 50 bösartige Apps, die mehr als 500.000-mal heruntergeladen wurden und Malware-Familien wie Joker, Harly, Coper und Adfraud enthielten.

Hier eine Zusammenstellung der relevantesten Malware-Familien, die für Angriffe auf Mobilgeräte zum Einsatz kommen:

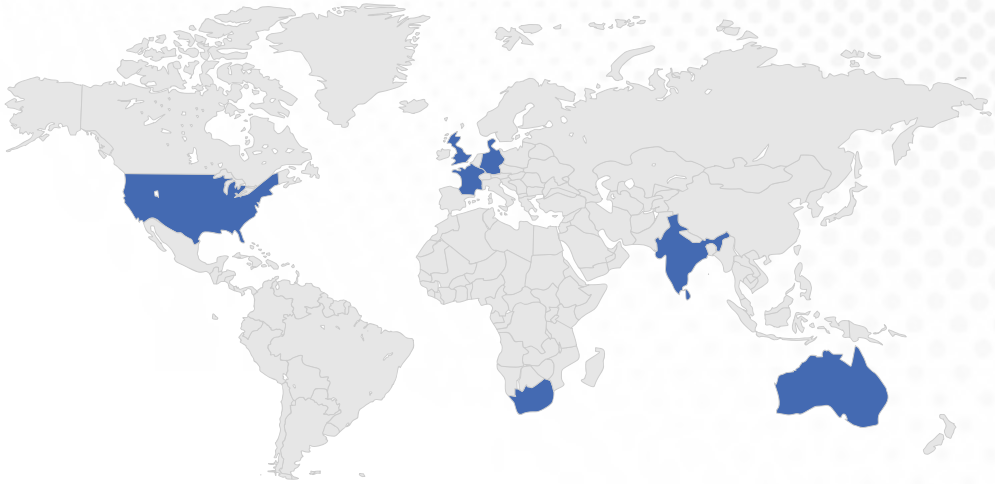
Multiverze ist eine Ransomware, die gezielt auf AndroidOS ausgerichtet ist. Sie verschlüsselt die Informationen auf dem Gerät des Users oder verhindert, dass es korrekt funktioniert. Dem User wird daraufhin eine Lösegeldforderung angezeigt, in der die Bedingungen genannt werden, unter denen die Daten entschlüsselt oder die ursprünglichen Funktionen wiederhergestellt werden.

Mirai ist ein Botnet, das Brute-Force-Techniken einsetzt, um IoT-Geräte über verschiedene Protokolle anzugreifen. Mirai nutzt zudem Schwachstellen in IoT-Geräten aus, die sich meist in Management Frameworks befinden. Ziel ist es, weitere Geräte zu infizieren und letztlich Remote-Code auszuführen. Die infizierten Geräte werden üblicherweise in Bots umgewandelt und sind daraufhin Teil einer größeren Botnet-Armee. Mirai ist seit Jahren eine der produktivsten Malware-Familien in diesem Bereich und verübte 2016 den größten DDoS-Angriff der Geschichte. Im Jahr 2021 stammten sogar 76 % aller von Zscaler blockierten Angriffe auf IoT-Geräte von dieser Malware-Familie.

Am stärksten betroffene Regionen

Die fünf Länder, die am häufigsten Ziel von verschlüsselten Angriffen geworden sind, sind die USA, Indien, Südafrika, das Vereinigte Königreich und Australien. Südafrika ist dabei ein Neuzugang, der 2022 an die Spitze der Rangliste aufgestiegen ist und Frankreich damit von den ersten fünf Plätzen verdrängt hat — 2021 nahm Frankreich noch den fünften Platz ein. Südafrika verzeichnete in diesem Jahr 3112 % mehr Angriffe über TLS- und SSL-Kanäle als im Vorjahr und war 2022 damit das Land mit den dritthöchsten Angriffszahlen.

Cyberkriminelle konzentrierten ihre Kampagnen auch auf Japan, die USA und Indien. In diesen Ländern nahm die Zahl der Angriffe im Vergleich zum Vorjahr um 613 %, 155 % bzw. 87 % zu.



Entwicklung der Angriffszahlen nach Land zwischen 2021 und 2022			
Südafrika	3112,33 %	Kanada	87,49 %
Japan	613,1 %	Indien	86,59 %
Russische Föderation	544,95 %	Spanien	84,46 %
Deutschland	352,37 %	Malaysia	56,66 %
Vereinigte Arabische Emirate	316,81 %	Vereinigtes Königreich	40,43 %
Singapur	185,73 %	Brasilien	32,21 %
Schweiz	162,75 %	Australien	–21,78 %
Vereinigte Staaten von Amerika	154,73 %	Philippinen	–24,32 %
Frankreich	146,22 %		
Niederlande	106,90 %		
Italien	103,13 %		

Hauptbranchen

Die Zahl der verschlüsselten Angriffe auf die Fertigungsbranche hat sich 2022 mehr als verdoppelt, wodurch nun der Technologiesektor nicht länger die Liste der am häufigsten betroffenen Branchen anführt. Angreifer beschäftigen sich offenbar gezielt mit der Fertigung, da diese Branche im Vergleich zu anderen ein besonderes lohnendes Ziel für Ad-Spyware ist. Sie ist neben dem Gesundheitswesen zudem eine der beiden Branchen, die mit Abstand von den meisten Phishing-Versuchen über verschlüsselte Kanäle betroffen ist. In der Fertigungsbranche hat sich in den letzten Jahren ein starker Wandel vollzogen und der Sektor hat weiterhin mit COVID-19-Beschränkungen und Engpässen in der Lieferkette zu kämpfen. Die Anwendungen, Produkte und Services, die zur Bewältigung dieser Herausforderungen neu eingeführt wurden, haben die Angriffsfläche deutlich vergrößert und zu neuen Sicherheitsrisiken geführt.

Das Bildungs- und das Gesundheitswesen verzeichneten im Jahr 2022 ebenfalls einen bemerkenswerten Anstieg verschlüsselter Angriffe. Im Bildungswesen stieg die Zahl der Angriffe im Vergleich zum Vorjahr um 132 %, wobei sie im vorherigen Jahr bereits um 50 % zugenommen hatte. Nach einem Anstieg von 27 % im Jahr 2020 belief sich die Steigerung im Gesundheitswesen 2022 auf 34 %.

Unterdessen gingen die Angriffe auf Technologieanbieter über TLS und SSL im Vergleich zum Vorjahr um 6 % zurück, nachdem diese Branche 2021 noch rund 50 % aller Angriffe verzeichnete. Zu den anderen Branchen, in denen die Angriffe über verschlüsselte Kanäle abnahmen, gehören der Einzelhandel mit —63 %, Behörden mit —40 % sowie der Finanz- und Versicherungssektor mit —5 %.

Der Einzelhandel verzeichnete im vergangenen Jahr einen Anstieg der verschlüsselten Angriffe um 842 %, was vermutlich auf den Umstand zurückzuführen ist, dass Cyberkriminelle die pandemiebedingten Veränderungen der Infrastruktur ausnutzten. Die Angriffe auf den Einzelhandel sind 2022 im Vergleich zu den Zahlen von 2020 immer noch stark erhöht, haben sich aber gegenüber dem massiven Anstieg von 2021 etwas normalisiert.

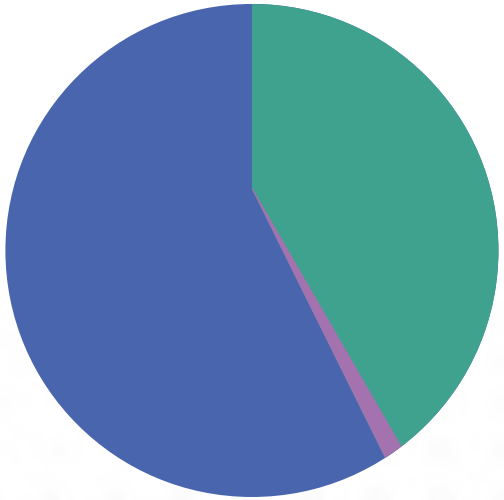
Angriffe auf Regierungsorganisationen gingen das zweite Jahr in Folge zurück: 2021 um 10 % und 2022 um 40 %. Die Strafverfolgungsbehörden sind gegen schwerwiegende Cyberangriffe auf Behörden und andere kritische Branchen vorgegangen, was sie zu weniger attraktiven Zielen für Kriminelle macht, die auf schnelles Geld aus sind.

Industriesektor	2022 im Vergleich zu 2021
Bildung	133,77 %
Finanzwesen/Versicherungen	—5,20 %
Öffentliche Hand	—39,60 %
Gesundheitswesen	33,92 %
Fertigung	239,10 %
Sonstiges	312,76 %
Einzel-/Großhandel	—63,45 %
Dienstleistungen	108,27 %
Technologie/Kommunikation	—6,24 %

SSL-Zertifikate im Vergleich

Obwohl alle SSL- und TLS-Zertifikate zur Verifizierung von Identitäten und Verschlüsselung von Verbindungen dienen, funktioniert die Überprüfung von Informationen bei den verschiedenen Zertifikatstypen auf unterschiedliche Weise.

Art des verwendeten Zertifikats



OV: 56,0 % DV: 42,8 % LW: 1,3 %

Domain Validation (DV) ist die günstigste, einfachste und schnellste Form der Validierung. Bei diesem Prozess wird die E-Mail-Domain des Antragstellers mit der WHOIS-Datenbank abgeglichen, um zu überprüfen, ob die Person, die das Zertifikat beantragt, die Domain betreibt, die durch das Zertifikat geschützt werden soll.

OV-Zertifikate (Organization Validation) sind teurer und schwieriger zu erhalten, da im Rahmen dieses Prozesses die Identität und der Sitz der Organisation überprüft wird.

EV-Zertifikate (Extended Validation) garantieren den höchsten Sicherheitsstandard, sind aber weit weniger verbreitet und kamen 2021 nur bei 21 % der Fortune-500-Unternehmen zum Einsatz. Wie bei den OV-Zertifikaten wird auch hier die Identität der Organisation überprüft, allerdings anhand eines strengeren Verfahrens, das neun zusätzliche Schritte umfasst. So soll sichergestellt werden, dass die Organisation auch wirklich die ist, für die sie sich ausgibt. Dies sind die teuersten und am schwierigsten zu erwerbenden Zertifikate und sie werden insbesondere von Unternehmen im Finanz-, Einzelhandels- und Technologiesektor eingesetzt, für die Vertrauen von größter Bedeutung ist.

Zscaler ThreatLabz fand heraus, dass für fast 99 % des schädlichen SSL-Traffics von Oktober 2021 bis Oktober 2022 entweder OV- oder DV-Zertifikate verwendet wurden. EV-Zertifikate machten lediglich 1,3 % des Traffics aus. Bemerkenswert ist, dass öfter Zertifikate verwendet wurden, die eine strengere Verifizierung erfordern, was darauf hindeutet, dass Angreifer immer häufiger legitime Websites vertrauenswürdiger Organisationen kompromittieren, um Angriffe auszuführen.

Prognosen

1. **Die zunehmende Nutzung von Malware-as-a-Service wird auch in Zukunft zu immer mehr Angriffen über verschlüsselte Kanäle führen.** Cyberkriminelle können jetzt einfach für leistungsstarke Malware und entsprechende Ressourcen bezahlen, mit denen sie unabhängig von ihren eigenen technischen Fähigkeiten ausgeklügelte Angriffe durchführen können. Da das As-a-Service-Modell weiter an Popularität gewinnt, werden auch immer mehr Angriffe Umgehungstaktiken, einschließlich Verschlüsselung, beinhalten.

2. **Organisationen mit Legacy-Infrastrukturen stehen vor schwierigen Entscheidungen.** Für die Überprüfung verschlüsselter Kanäle ist zehnmal so viel Rechenleistung erforderlich wie für die Überprüfung unverschlüsselter Kanäle. Die erhebliche Zunahme des verschlüsselten Traffics stellt Organisationen, die auf hardwarebasierte Sicherheit setzen, vor schwierige Entscheidungen hinsichtlich ihrer Kapazitätsplanung. Entweder verschwenden sie Geld für Firewalls, die für ihre Bedürfnisse viel zu umfangreich sind, oder sie riskieren, dass sie mangels Ressourcen nicht mehr den gesamten Traffic überprüfen können, der geprüft werden sollte.

3. **2023 wird es zu noch mehr verschlüsselten Angriffen kommen.** Cyberbedrohungen werden weiterhin vor allem über verschlüsselten Traffic verbreitet werden, da Angreifer ihre Taktiken stets an die gängigen Praktiken anpassen. Die Mehrheit des gesamten Traffics ist bereits heute verschlüsselt und somit ist in den nächsten Jahren mit einem Anstieg der verschlüsselten Bedrohungen zu rechnen, da neue Cyberkriminelle bestehende Kompetenzlücken schließen werden. Noch können Sie sich auf diese Situation vorbereiten: Erarbeiten Sie ein Sicherheitskonzept mit einer dauerhaften Strategie zum Schutz vor Bedrohungen, die sich im verschlüsselten Traffic verbergen.

4. **Die Exfiltration verschlüsselter Daten zu Erpressungszwecken wird zunehmen.** Da immer mehr Ransomware-Angreifer mehrere Taktiken anwenden, um ihre Opfer zu erpressen und zur Kasse zu bitten, ist mit einem zunehmenden Diebstahl sensibler Daten zu rechnen. Um Firewalls und andere Legacy-Sicherheitstechnologien zu umgehen, verschlüsseln Cyberkriminelle Datenbestände, bevor sie diese aus der Umgebung des Opfers ausschleusen.

5. **Sicherheitsstandards für verschlüsselten Traffic werden überarbeitet.** Vermutlich steht eine Aktualisierung der aufsichtsrechtlichen Rahmenbedingungen im Hinblick auf Sicherheitsstandards zur Analyse des verschlüsselten Traffics bevor. Weitere Debatten, die dieses Thema in den Mittelpunkt rücken, sind ebenfalls zu erwarten.

6. **Es wird schwieriger sein, Angriffe abzuwehren.** Im vergangenen Jahr machte die Hackergruppe Lapsu$ Schlagzeilen, die mit ungewöhnlich raffinierten Taktiken Organisationen infiltriert und wertvolle Daten schnell und rabiat exfiltriert hatte. Allein daran sollten Sicherheitsexperten und -verantwortliche deutlich erkennen, dass die bisherige Methode zur Entwicklung von Angriffsabwehrstrategien ausgedient hat: Ein Fokus auf geordnete lineare Abfolgen von Angriffsphasen mit zahlreichen zu erkennenden Ereignissen, bekannte Indikatoren und vorhersehbare Techniken ist keine gangbare Lösung mehr. Jetzt ist es an der Zeit, sich auf eine neue Welle potenzieller Bedrohungen vorzubereiten, die 2023 und in den darauffolgenden Jahren mit Sicherheit einsetzen wird. Dabei sollten Sie vor allem darauf achten, dass Ihre Abwehrmechanismen auf jede Phase des Angriffszyklus abgestimmt sind, sodass Bedrohungen in jeder dieser Phasen effektiv abgefangen werden können.

Notwendige Maßnahmen zum Verhindern verschlüsselter Angriffe

Die Daten sprechen für sich: Verschlüsselter Traffic beinhaltet Malware und andere Bedrohungen. Dieser Trend hat in den letzten Jahren ständig zugenommen und es besteht Grund zur Annahme, dass Cyberkriminelle den verschlüsselten Traffic weiterhin als Angriffsvektor nutzen werden. Die einzige Möglichkeit, verschlüsselte Bedrohungen zu unterbinden, besteht darin, den Traffic zu überprüfen — und zwar den gesamten.

Die Überprüfung von verschlüsseltem Traffic war nicht immer praktikabel. Veraltete Tools machen eine vollständige Überprüfung zu einem kostspieligen Unterfangen, das zudem die Performance beeinträchtigt. Außerdem können Regelungen, die unterschiedliche Richtlinien für verschiedene Datentypen vorschreiben, dies ebenfalls zu einer mühsamen Aufgabe machen. Es gibt jedoch bewährte Strategien, mit denen Organisationen ihren verschlüsselten Traffic in großem Maßstab überprüfen können — ohne Beeinträchtigung der Performance oder die Verursachung von Compliance-Konflikten. Wir sprechen folgende Empfehlungen aus:

- Setzen Sie auf eine Cloud-native, Proxy-basierte Architektur, um Traffic in großem Maßstab zu entschlüsseln und so Bedrohungen zu erkennen und abzuwehren.
- Nutzen Sie eine KI-basierte Sandbox, um unbekannte Angriffe unter Quarantäne zu stellen und Patient-Zero-Malware zu stoppen.
- Sorgen Sie für eine kontinuierliche Überprüfung des gesamten Traffics, unabhängig davon, ob sich User zu Hause, in der Zentrale oder unterwegs befinden, um konsistenten Schutz vor verschlüsselten Bedrohungen zu gewährleisten.

Beginnen Sie mit einem Zero-Trust-Ansatz, um laterale Bewegungen zu verhindern und somit die Angriffsfläche zu minimieren. Durch Zero Trust werden Anwendungen für Angreifer unsichtbar. Außerdem erhalten autorisierte User nur noch Zugriff auf Ressourcen, die sie wirklich benötigen, nicht mehr auf das gesamte Netzwerk.

Die Lösung erfordert Skalierbarkeit und Leistung. Beides kann nur durch eine Cloud-native, Proxy-basierte Architektur wie die Zscaler Zero Trust Exchange™ bereitgestellt werden. Nur eine Cloud-basierte Sicherheitsplattform erfüllt die Anforderungen an Entschlüsselung und Überprüfung durch die elastische Skalierung von Rechenressourcen und bietet eine einheitliche Richtliniendurchsetzung über mehrere Standorte hinweg.

Eine mehrschichtige, tiefgreifende Abwehrstrategie, die die Angriffsfläche verringert und eine vollständige HTTPS-Überprüfung zur Aufdeckung versteckter Bedrohungen bietet, ist unerlässlich, um den Schutz von Unternehmen zu gewährleisten.

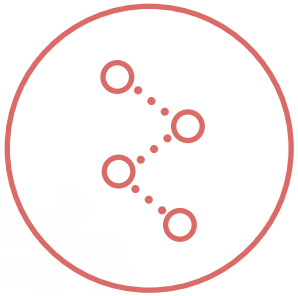
Abwehr verschlüsselter Bedrohungen durch die Zscaler Zero Trust Exchange

Niemand darf als vertrauenswürdig eingestuft werden — das ist der Leitgedanke hinter jeder Zero-Trust-Strategie und -Architektur. Bei der Implementierung von Sicherheitskontrollen wird davon ausgegangen, dass jeder User böswillige Absichten verfolgen könnte. Daher besteht das Ziel darin, die Angriffsfläche zu verringern, indem die Sichtbarkeit von und der Zugriff auf Netzwerkressourcen eingeschränkt werden.

Ein komplexer Angriff erfolgt häufig in vier Phasen. Die Angreifer führen zunächst eine Aufklärungsaktion im Internet durch, um nach Schwachstellen zu suchen und ihr Vorgehen zu planen. Dann dringen sie in das Netzwerk ein, oft durch einen Exploit, einen Brute-Force-Angriff auf eine erkennbare Ressource oder mithilfe von gestohlenen Anmeldedaten. Sobald sie sich innerhalb des Netzwerks befinden, bewegen sich die Cyberkriminellen lateral fort, weiten ihre Berechtigungen aus und setzen sich im Netzwerk fest. Schließlich verwirklichen die Angreifer ihre Ziele. In der Regel umfasst dies die Exfiltration von Daten. Die Zscaler Zero Trust Exchange bietet Sicherheitskontrollen in jeder dieser Angriffsphasen, um das Risiko ganzheitlich zu reduzieren.

Minimale Angriffsfläche

Präventive Verhinderung der Kompromittierung



Laterale Ausbreitung unterbinden

Datenverluste verhindern

Angriffsfläche finden: Innerhalb der gesamten Netzwerkumgebung gilt ein implizites Vertrauensprinzip. So beinhaltet die Zugangsberechtigung zu Netzwerken den Zugriff auf sämtliche Anwendungen, die sich dort befinden. Der gemeinsame Netzwerkkontext — etwa internetbasierte User, die sich über VPN verbinden, oder öffentlich sichtbare Workloads in einem beliebigen Netzwerk oder andere Optionen — ermöglicht ungehinderte Verbindungen mit allen Services. Entsprechend exponiert jede Zugriffsanfrage über ein gemeinsames Netzwerk den betreffenden Service als Angriffsfläche. Jeder mit dem Internet verbundene Service, einschließlich Firewalls, ob im Rechenzentrum, in der Cloud oder in einer Zweigstelle, kann entdeckt, angegriffen und ausgenutzt werden.

Anfängliche Kompromittierung: Zur Verhinderung des Erstzugriffs müssen Sie zunächst die Anzahl von Einstiegspunkten in Ihre Umgebung reduzieren. Die Angriffsfläche muss geprüft, 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. Darüber hinaus sollte — wie wir bereits mehrfach empfohlen haben — der gesamte Traffic überprüft werden. Es ist davon auszugehen, dass nichts und niemand vertrauenswürdig ist. 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 Bewegung: 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 C&C-Server aufzunehmen. Dieser Kontakt ermöglicht es Angreifern, Computer 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 effiziente Funktionen zum Schutz vor Datenverlust ein, um jeglichen schädlichen ausgehenden Traffic zu erkennen und zu stoppen.

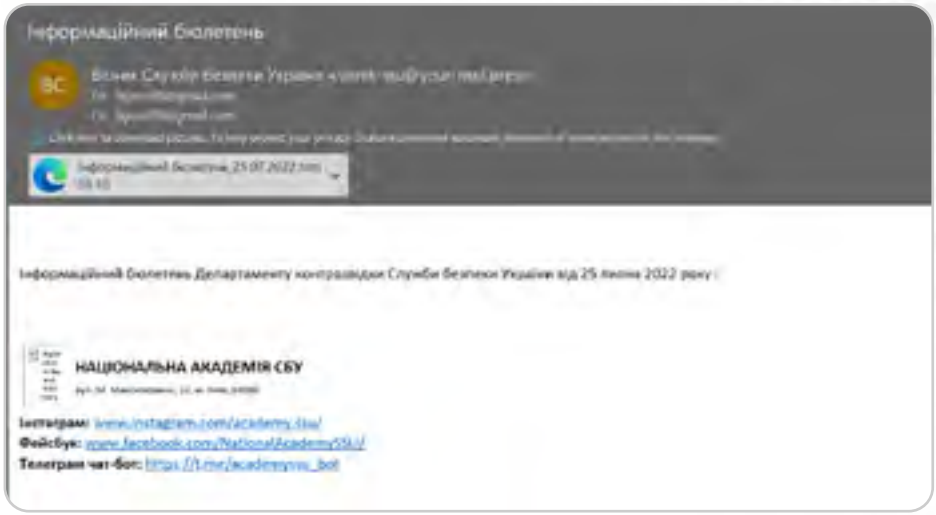
Die Zscaler Zero Trust Exchange wehrt die gesamte Angriffssequenz ab und bietet eine HTTPS-Überprüfung in großem Maßstab mit einem mehrschichtigen Ansatz, der Inline-Bedrohungsüberprüfung, Sandboxing und Data Loss Prevention sowie eine breite Palette zusätzlicher Abwehrfunktionen umfasst. Darüber hinaus sorgt der Cloud-Effekt von Zscaler dafür, dass alle auf der globalen Plattform identifizierten Bedrohungen automatisch zu einer Aktualisierung der Schutzmaßnahmen aller Zscaler-Kunden führen. Ihr eigener Sicherheitsstatus 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 Richtliniendurchsetzung zuverlässig geschützt.

Malware-Fallstudien

Gamaredon

Zusammenfassung

Die APT-Gruppe Gamaredon ist seit 2013 aktiv. Sie hatte es in der Vergangenheit vor allem auf die ukrainische Regierung abgesehen und damit die Spannungen zwischen Russland und der Ukraine verschärft. Sie erstellt maßgeschneiderte Malware mit eingebetteten komplexen Funktionen, mit denen sie die Daten der Opfer auf von Angreifern kontrollierte Server exfiltriert. Dabei kommen folgende Techniken zur Umgehung von Sicherheitstools zum Einsatz:



- Die Malware versucht, die Sandbox-Erkennung zu umgehen, indem sie die Ausführung der Malware mithilfe von Windows-APIs wie SleepEx und NTDelayExecution verzögert, bis die Sandbox-Analyse abgeschlossen ist. Zudem ködert sie Opfer mit Decoy-Dokumenten.

Bereitstellungsmechanismus

Angreifer verbreiten Gamaredon mithilfe verschiedener Strategien, beispielsweise über Phishing-E-Mails mit bösartigen Microsoft Office-Anhängen oder ISO-Dateien mit eingebetteten LNK-Dateien, die PowerShell-Skripts zum Herunterladen schädlicher Binärdateien enthalten.

Persistenz

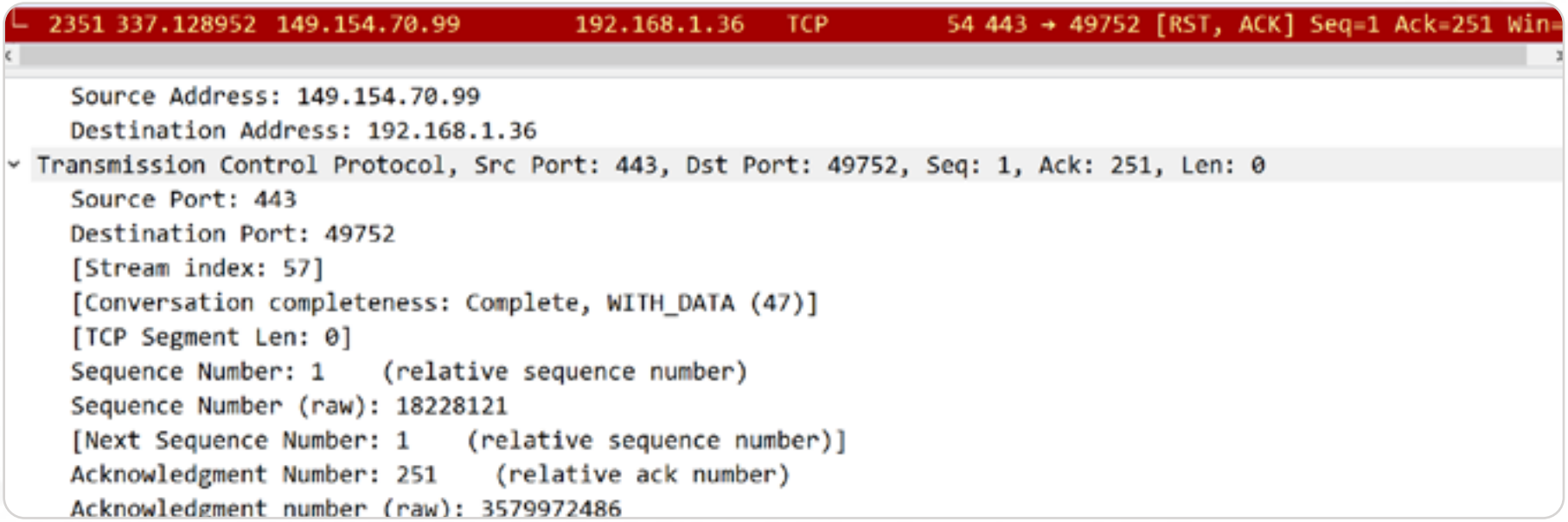
Hinsichtlich der Persistenz nutzt die Malware die beiden folgenden Mechanismen:

- In unserer Stichprobe überprüfte die Malware vor der Ausführung einer Aktion, ob Microsoft Office installiert ist.
- Sie führt Programme in regelmäßigen Abständen oder zu bestimmten Zeiten aus, um andere Aktionen mithilfe von Windows-Services zur Aufgabenplanung wie schtasks.exe vorzunehmen.

C:\Windows\SysWOW64\schtasks.exe schtasks /create /tn Adobe.exe_del /tr 'taskkill /f /im Adobe.exe' /sc daily /st 10:05

Netzwerk

In jüngsten Kampagnen haben wir festgestellt, dass Gamaredon-Domains von TIMEWEB-RU registriert sind und die Domain .ru verwenden. Die IP-Adresse ist in der Binärdatei enthalten und anstelle von Secure Sockets Layer (SSL) wird ein TLS-Handshake verwendet. Der TCP-Traffic ist in folgendem Schnappschuss zu sehen.



Lyceum

Zusammenfassung

Die seit 2017 aktive Gruppe Lyceum ist eine staatlich geförderte iranische APT-Gruppe, die es vor allem auf Organisationen in den Energie- und Telekommunikationsektoren des Nahen Ostens abgesehen hat. Lyceum nutzt eine neu entwickelte .NET-basierte DNS-Backdoor-Malware, bei der es sich um eine angepasste Version des Open-Source-Tools DIG.net handelt. DIG.net ist ein Open-Source-DNS-Resolver, der zur Abfrage des DNS-Servers und zur anschließenden Analyse der Antwort verwendet werden kann.

Bereitstellungsmechanismus

Hauptsächlich wird die Payload über einen Microsoft Office-Anhang bereitgestellt, in den ein bösartiges Makro eingebettet ist. Bei einer kürzlich analysierten Kampagne enthielt das entsprechende Microsoft Word-Dokument eine Vorlage mit Nachrichtenartikeln über militärische Angelegenheiten im Iran. Der Cyberkriminelle nutzte die Funktion AutoClose(), die beim Schließen des Dokuments ausgeführt wurde und daraufhin die DNS-Backdoor auf dem System platzierte.

Persistenz

Die Malware verwendet den STARTUP-Ordner, um Persistenz zu gewährleisten, und wird bei jedem Neustart des Systems ausgeführt. Sie generiert eine eindeutige BotID, die von dem aktuellen Microsoft Windows-Usernamen abhängt. Den Usernamen wandelt sie mit der Funktion CreateMD5() in sein MD5-Äquivalent um und parst die ersten acht Bytes des MD5 als BotID zur Identifizierung des Users und des von der Malware infizierten Systems.

Netzwerk

Die Malware nutzt eine DNS-Angriffstechnik —das sogenannte DNS-Hijacking —, bei der ein vom Angreifer kontrollierter DNS-Server die Antwort und Auflösung von DNS-Anfragen manipuliert. Durch die Verwendung des DNS-Protokolls für die Command-and-Control-Kommunikation (C2) entgeht die Schadsoftware der Entdeckung. Sie umfasst Funktionen wie den Upload/Download von Dateien und die Ausführung von Systembefehlen auf dem infizierten Computer durch den Missbrauch von DNS-Einträgen, einschließlich TXT-Einträgen für eingehende Befehle und Adresseinträgen für die Datenexfiltration. Die Malware richtet einen vom Angreifer kontrollierten DNS-Server ein, indem sie die IP-Adresse des Domainnamens erlangt, was wiederum eine DNS-Anfrage an die Domain auslöst, um die IP-Adresse aufzulösen. Nun wird diese IP-Adresse als der vom Angreifer kontrollierte DNS-Server für alle weiteren von der Malware initiierten DNS-Anfragen verwendet.

QuasarRAT

Zusammenfassung

QuasarRAT ist seit mindestens 2015 aktiv. Es handelt sich um einen legitimen, öffentlich verfügbaren RAT für Microsoft Windows. Angreifer nutzen QuasarRAT u. a. zur Steuerung von Remote-Desktops, zum Keylogging, zum Stehlen von Passwörtern, zum Beenden verschiedener Prozesse, zum Abrufen von Systeminformationen und zur Implementierung von Systemsteuerungsbefehlen. Es handelt sich um eine Client-Server-Anwendung, bei der alle Vorgänge auf der Client-Seite ausgeführt und vom Server verwaltet werden.

Bereitstellungsvektor

QuasarRAT wird über Spam-E-Mails, durch Backdooring, als gecrackte Software getarnt oder über andere Köder auf dem Computer des Opfers bereitgestellt.

Persistenz

- QuasarRAT nutzt die folgenden Methoden, um Persistenz auf dem Zielcomputer zu erreichen:
- Die Malware erstellt einen Mutex: QSR_MUTEX_[0-9A-Za-z]{18,}.
- Sie stellt sicher, dass der schädliche Inhalt nicht innerhalb der virtuellen Maschinen von Sicherheitsunternehmen ausgeführt wird, indem sie die öffentliche IP-Adresse des Computers überprüft.
- Sie platziert Dateien im AppData-Verzeichnis.
- Windows-Services verwendet sie zur Planung, um Aufgaben hinzuzufügen und zu ändern. Zum Beispiel:

‘C:\Windows\SysWOW64\schtasks.exe’ /create /
tn RtkAudioService64 /tr ‘C:\Users\user\btpanui\
SystemPropertiesPerformance.exe’ /sc Minute /mo 1 /F

Netzwerk

Bei der mit Quasar verschlüsselten Kommunikation wird ein AES-Algorithmus mit einem in der Client-Binärdatei fest kodierten Pre-shared Key verwendet. Es ist nicht möglich, AES-verschlüsselten Traffic auf Signaturmuster zu überprüfen. Allerdings können die charakteristischen Merkmale verschlüsselter Datenpakete genutzt werden, um den AES-verschlüsselten Traffic von Quasar zu erkennen — in diesem Fall die ersten vier Bytes der Payload, mit denen das erste Paket, das nach dem TCP-Handshake vom Server an den Client gesendet wird, identifiziert werden kann. Mithilfe dieses Pakets wird der Authentifizierungsprozess von Server und Client eingeleitet. Die ersten vier Bytes der TCP-Payload enthalten „40 OO OO OO“, was die Größe der folgenden Daten in Little Endian angibt.

Qakbot

Zusammenfassung

Qakbot, auch bekannt als QBot, QuackBot und Pinkslipbot, ist ein seit 2008 aktiver Trojaner, der Passwörter stehlen soll. Diese hartnäckige Bedrohung verbreitet sich über ein E-Mail-basiertes Botnet, das Antworten in aktive E-Mail-Threads einfügt. Cyberkriminelle haben es mit Qakbot auch auf Bankkunden abgesehen und verschaffen sich durch kompromittierte Anmeldedaten Zugriff, um Finanzvorgänge auszuspionieren und so wertvolle Informationen zu erhalten. Sie arbeiten auch kontinuierlich an neuen Bereitstellungsvektoren, um der Entdeckung zu entgehen.

Bereitstellungsvektor

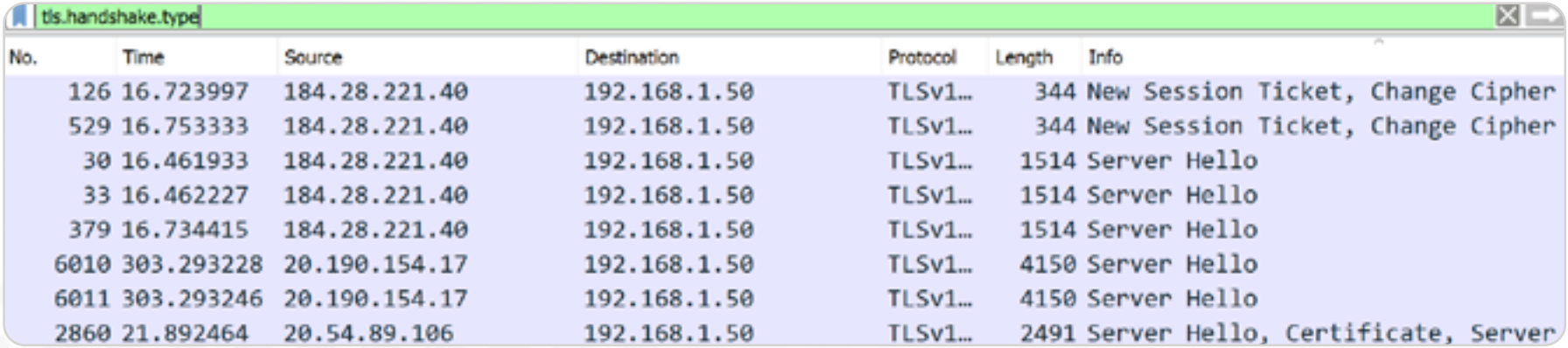
Qakbot stellt die Payload wie etwa XLM 4.0 über schädliche Microsoft Office-Anhänge bereit und verwendet geläufige Dateinamen mit gängigen Formaten wie Calculation-1517599969-Jan-24.xlsb, ClaimDetails-1312905553-Mar-14.xlsb oder Compensation-1172258432-Feb-16.xlsb.

Persistenz

- Folgendermaßen bleibt Qakbot persistent:
- Erstellen eines Mutex
- Erstellen eines Autostart-Registrierungsschlüssels
- Kopieren der Malware in das STARTUP- oder AppData-Verzeichnis des Systems
- Erstellen von Services zur Aufgabenplanung
- Einschleusen der Malware in legitime Microsoft Windows-Prozesse wie explorer.exe

Netzwerk

Mithilfe von WebInject verändert Qakbot die Kommunikation zwischen dem Zielcomputer und Banking-Websites und stiehlt die Anmeldedaten der Opfer. Qakbot nutzt HTTPS- oder SSL/TLS-Traffic ohne zugehörige Domains.

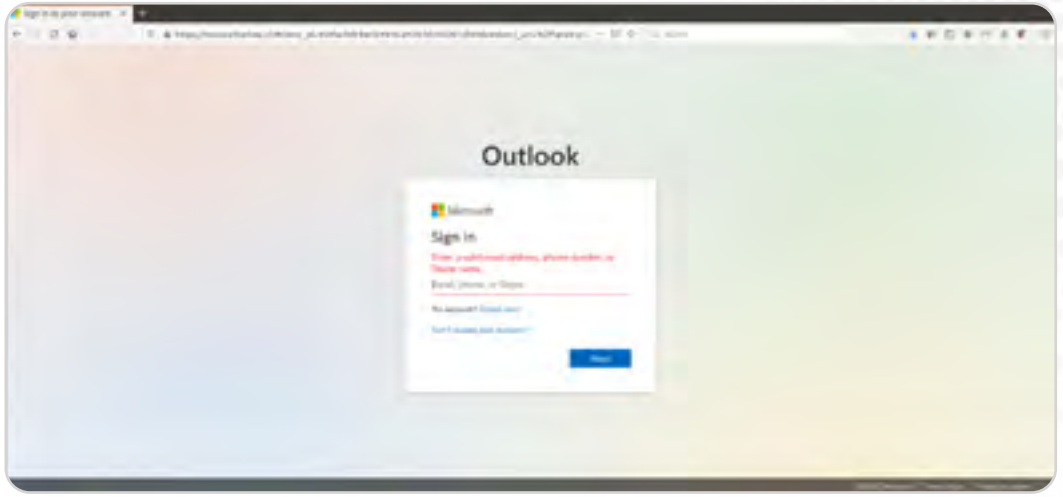


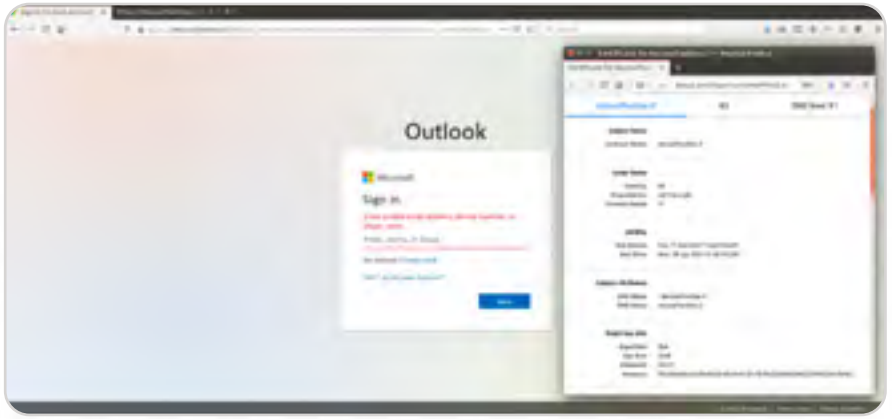
Phishing-Fallstudien

Microsoft-Phishing:

Zscaler ThreatLabz erfasste einen Fall von Domain-Squatting über HTTPS, wobei folgende Phishing-Website verwendet wurde:

Phishing-URL: https://micosoftonline[.]cf/

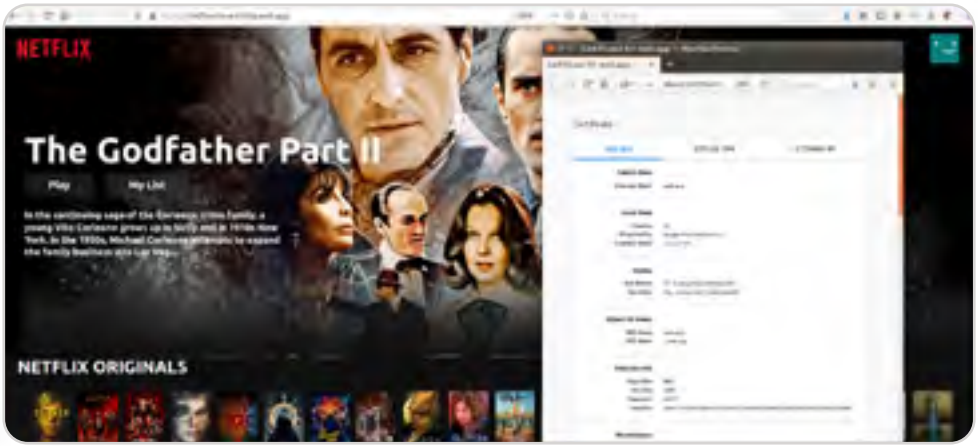




Netflix-Phishing:

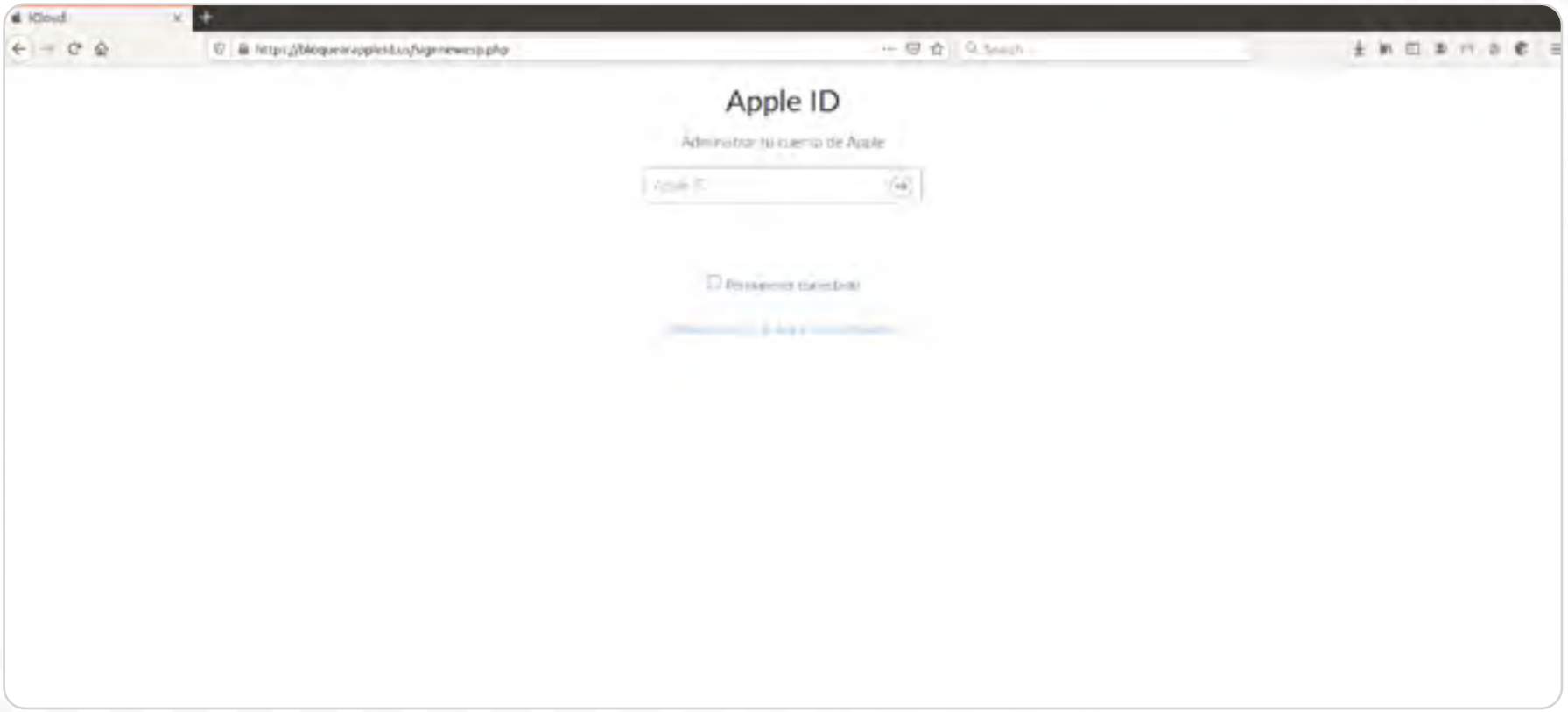
Wir haben auch einen Fall von Phishing beobachtet, bei dem Cyberkriminelle Netflix über HTTPS genutzt und Webhosting-Services wie web[.]app sowie Google Trust-Zertifikate missbraucht haben.

Phishing-URL: https://netflix-clone-7c60a.web[.]app/



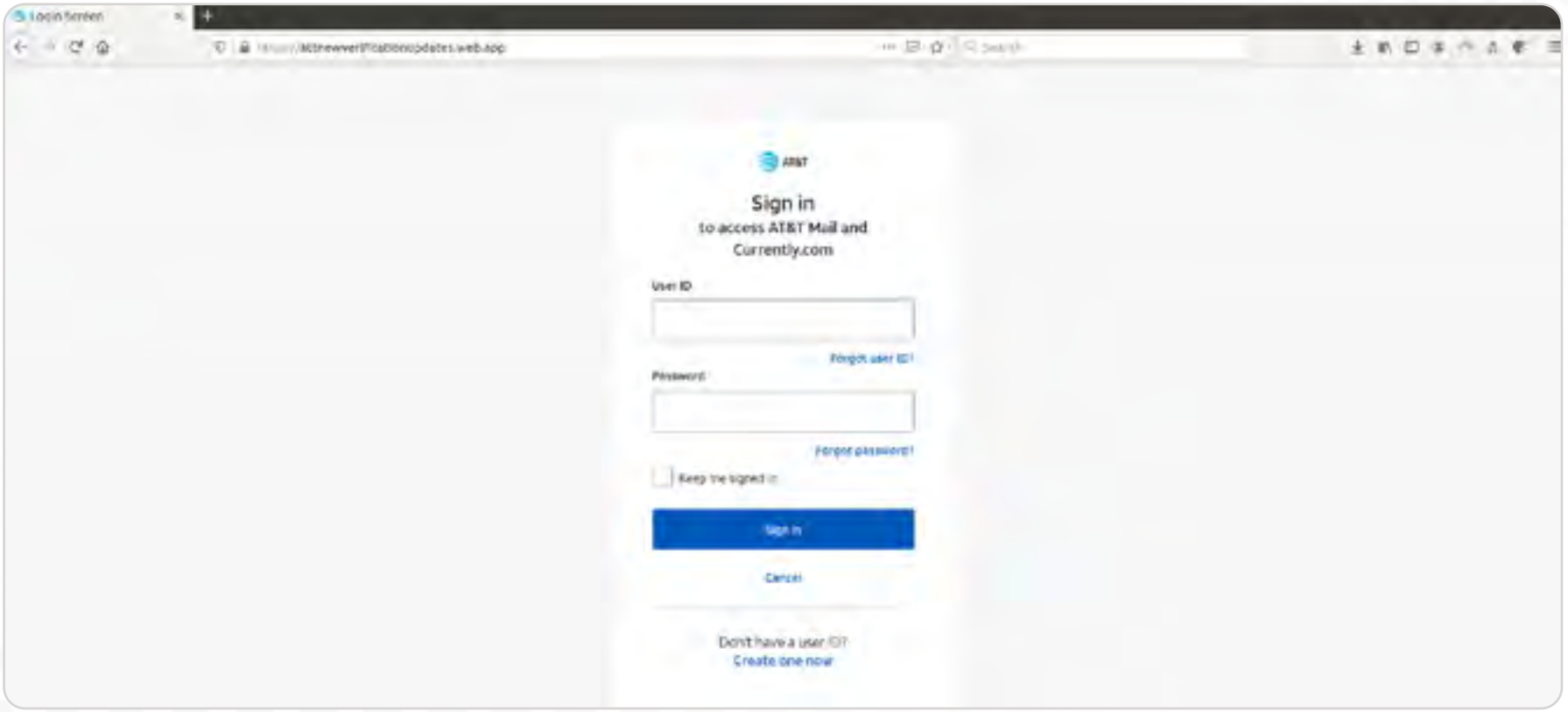
Apple-Login

Phishing-URL: https://bloquearappleid[.]us/signnewesp.php



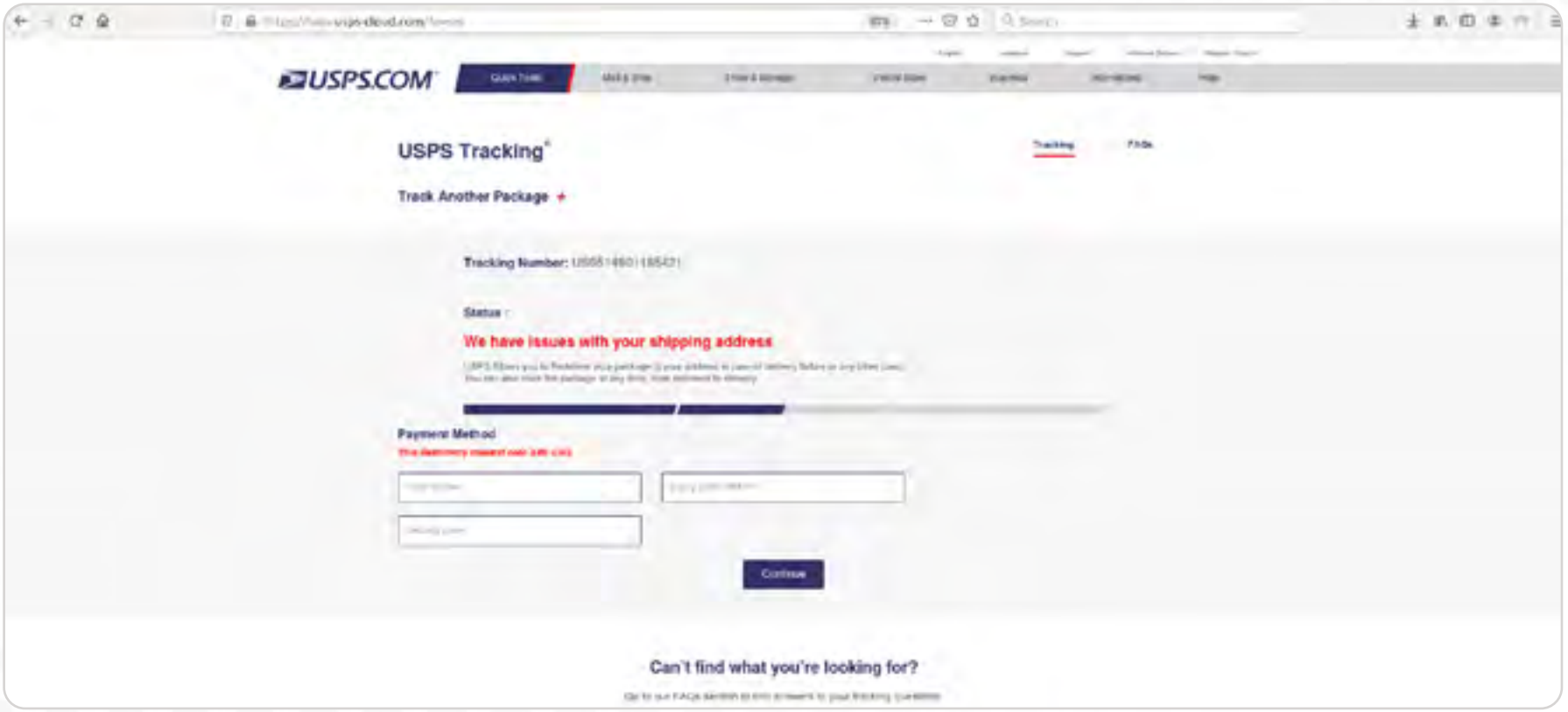
ATT-Phishing:

Phishing-URL: https://attnewverificationupdates[.]web[.]app/



USPS-Phishing:

Phishing-URL: https://faqs[.]ups-cloud[.]com/?a=sec

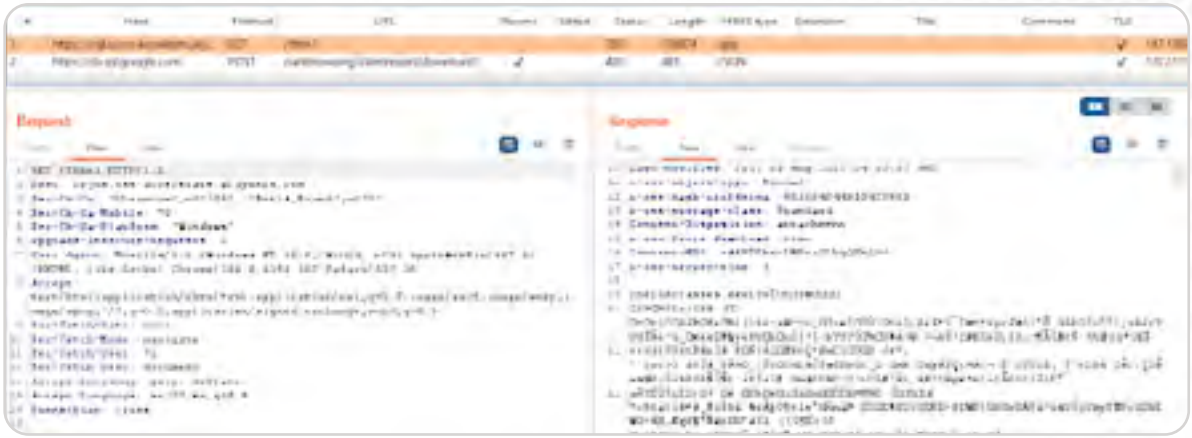


Fallstudien zu Angriffen auf Mobil- und IoT-Geräte

GriftHorse: Diese Malware dient dazu, Opfer für einen Premium-SMS-Service anzumelden, der über die Telefonrechnung abgerechnet wird und somit finanzielle Verluste verursacht. GriftHorse war zunächst eine Trick-Malware, die Payloads in nativem JS versteckte, um statische Überprüfungen zu umgehen.

Der Trojaner kommuniziert über einen sicheren SSL-Kanal mit C&C-Servern und kann so nach der Infektion Aktivitäten durchführen. Zur Tarnung und C&C-Kommunikation nutzt GriftHorse Facebook Deferred Deep Linking, Appsflyer und GitHub — auch über SSL.

Joker: Joker ist seit Jahren eine hartnäckige Malware, die gezielt auf die Android-Plattform ausgerichtet ist und User für Premium-Services über WAP oder Direktabrechnung anmeldet. Abgesehen von verschiedenen Techniken zur Tarnung innerhalb von Apps kommunizieren die C2-Server von Joker über SSL. Eine neue Variante agiert scheinbar nicht länger SDK-basiert, sondern verwendet einen kontrollierteren, SSL-Server-gestützten Ansatz mit Client-seitigem SSL-Pinning, um nicht entdeckt zu werden.



MaliBot: MaliBot ist eine neuartige Banking-Malware, die hauptsächlich auf Online-Banking-Kunden in Spanien und Italien abzielt. Es handelt sich um eine leistungsstarke Malware, die Anmeldedaten und Cookies stehlen sowie Codes für die mehrstufige Authentifizierung umgehen kann. MaliBot stiehlt vor allem Finanzdaten, Anmeldedaten, Krypto-Wallets sowie personenbezogene Daten und hat es zudem auf Finanzinstitute abgesehen. Die Malware ist in der Lage, infizierte Geräte über eine VNC-Server-Implementierung remote zu steuern.
Wir konnten mehrere C2-Aktivitäten von dieser Banking-Malware über einen sicheren Kanal beobachten.

Hydra: Hydra ist eine weitere verbreitete und voll funktionsfähige Banking-Malware. Unter anderem verfügt sie über Screencast-Funktionen, mit denen sich Aktivitäten des infizierten Geräts visualisieren lassen, und sie kann Anwendungen remote installieren. Diese Funktionen machen die Malware zu einer der größten Bedrohungen für Mobilgeräte. Hydra nutzt außerdem Let's Encrypt-SSL-Zertifikate für C&C-Aktivitäten. Bei einigen neueren Stichproben konnte festgestellt werden, dass auch Github zu diesem Zweck eingesetzt wird.

Medusa: Medusa ist ebenfalls ein bekannter Android-basierter Banking-Trojaner.
Er sammelt personenbezogene Informationen, verwendet Overlay und stiehlt Anmeldedaten auf der Grundlage von Befehlen der Angreifer. Die C2-Server von Medusa nutzen ebenfalls sichere Kanäle.

Über ThreatLabZ

ThreatLabz ist als Forschungsabteilung von Zscaler für die Früherkennung neuer Bedrohungen zuständig. Dieses Expertenteam sorgt dafür, dass tausende Organisationen, die die globale Zscaler-Plattform nutzen, jederzeit geschützt sind. Neben der Erforschung und Verhaltensanalyse von Malware tragen die ThreatLabz-Experten auch zur Entwicklung neuer Prototypen für den Schutz vor komplexen Bedrohungen auf der Zscaler-Plattform bei und führen regelmäßig interne Audits durch, um sicherzustellen, dass Zscaler-Produkte und -Infrastrukturen die geltenden Sicherheitsstandards erfüllen. Detaillierte Analysen neuer Bedrohungen werden regelmäßig unter research.zscaler.com veröffentlicht.

Gerne informieren wir Sie über aktuelle Forschungsergebnisse der ThreatLabz-Experten.
Am besten melden Sie sich gleich bei unserem Newsletter an!

Experience your world, secured.™

Über Zscaler

Zscaler (NASDAQ: ZS) beschleunigt die digitale Transformation, damit Kunden agiler, effizienter, resilienter und sicherer arbeiten können. Die Zscaler Zero Trust Exchange™ schützt tausende Kunden mittels sicherer Verbindungen zwischen Usern, Geräten und Anwendungen überall vor Cyberangriffen und Datenverlust. Die SASE-basierte Zero Trust Exchange ist weltweit in 150 Rechenzentren verfügbar und ist somit die größte Inline-Cloud-Sicherheitsplattform der Welt. Weitere Informationen finden Sie unter www.zscaler.de.

+1 408 533 0288

Zscaler, Inc. (Hauptsitz) • 120 Holger Way • San Jose, CA 95134, USA

zscaler.de