Report zum Status Verschlüsselter Angriffe 2020

Angriffe via SSL-/TLS-Verschlüsselung nehmen rasant zu laut der jährlichen Untersuchung des Zscaler™ ThreatLabZ-Teams

JANUAR – SEPTEMBER 2020

Inhalt

Über ThreatLabZ

ThreatLabZ ist das globale Security Research-Team von Zscaler. Das Team ist nicht nur für den Schutz von Zscaler-Kunden vor neuartigen Bedrohungen zuständig, sondern analysiert auch den gesamten Traffic in der Zscaler-Cloud. Dank des kombinierten Fachwissens in den Bereichen Cybersicherheit, Datenwissenschaft und KI/Machine Learning – im Verbund mit dem ausgewerteten Datenvolumen aus über 120 Milliarden Transaktionen pro Tag in der Cloud-Plattform Zero Trust Exchange™ von Zscaler – ist das ThreatLabZ-Team bestens aufgestellt, um fundierte Erkenntnisse zu Trends zu liefern.

Wenn ThreatLabZ eine neue Angriffskampagne oder Malware mit ungewöhnlichen Techniken oder Fähigkeiten entdeckt, detonieren die Forscher die betreffenden Dateien und analysieren den darin enthaltenen Code. So lässt sich präzise nachvollziehen, wie die Malware für Tarnung, Auslieferung von Payloads, Diebstahl, Kontrolle von Geräten, Ausspionieren der User sowie zur Vervielfältigung und Verbreitung programmiert wurde.

Die Ergebnisse der Analysen werden den Sicherheitsexperten und der Öffentlichkeit im **Zscaler-Research-Blog** vorgestellt.

Konkret zum Thema SSL-Trends haben die Forscher des ThreatLabZ kürzlich Bedrohungen aufgedeckt und analysiert, die sich verschlüsselte Kanäle zunutze machen. Einzelheiten lassen sich in folgenden Artikeln nachlesen:

- **Fake VPN Sites Deliver Infostealers (Gefälschte VPN-Seiten verbreiten Infostealer)**
- **Abuse of StackBlitz Tool to Host Phishing Pages (Missbrauch von StackBlitz-Tools für das Hosting von Phishing-Seiten)**
- **JavaScript Skimmers**
- **Higaisa Advanced Persistent Threat**

Um die Zscaler-Cloud in Aktion zu erleben, lassen sich auf dem **Cloud Activity Dashboard** die Anzahl der verarbeiteten Transkationen und abgewehrten Bedrohungen pro Sekunde ablesen.

Malware wird in SSL-Traffic verborgen.

Und zwar massenhaft – trotz des hartnäckigen, und weit verbreiteten Irrglaubens hinsichtlich SSL-Verschlüsselung, der Sicherheitsexperten immer wieder auf die Palme bringt: „Ich dachte, solange die Website SSL-Verschlüsselung verwendet, ist sie sicher."

Richtig ist, dass SSL-Verschlüsselung erfunden wurde, um Traffic vor unbefugten Blicken zu schützen. Findige Cyberkriminelle machen sie sich jedoch auch zum Einschmuggeln von Bedrohungen zunutze, sodass Verschlüsselung ohne gründliche Untersuchung selbst ein potenzielles Risiko darstellt.

SSL/TLS-Verschlüsselung ist der Branchenstandard zum Schutz von Daten bei der Übertragung – das wissen Angreifer genauso gut wie Sicherheitsexperten. Eben diese Kriminellen nutzen die branchenüblichen Verschlüsselungsmethoden selbst und umgehen herkömmliche Sicherheitsmechanismen, indem sie Malware in verschlüsseltem Traffic verbergen. Tatsächlich hat die Zscaler-Cloud im Zeitraum von Januar bis September insgesamt 6,6 Milliarden Sicherheitsbedrohungen abgewehrt, die sich in verschlüsseltem Traffic transportiert wurden. Das entspricht durchschnittlich 733 Millionen geblockten Bedrohungen im Monat und bedeutet einen Anstieg um fast 260 % gegenüber dem Vorjahreswert von 283 Millionen Bedrohungen pro Monat.

Die Untersuchung von verschlüsseltem Traffic ist für Unternehmen aller Größen und Branchen eine unverzichtbare Komponente ihrer Sicherheits- und Abwehrmechanismen. Herkömmliche, lokal installierte Sicherheitstools wie Next-Generation Firewalls bieten in aller Regel nicht die erforderliche Leistungsfähigkeit und Kapazität zur effektiven Entschlüsselung, Untersuchung und Wiederverschlüsselung des Traffics. Allein der Versuch, den gesamten SSL-Traffic durchleuchten würde, die Performance und damit auch die Produktivität komplett lahmlegen. Deswegen lassen viele Unternehmen ihren verschlüsselten Traffic zumindest teilweise ohne Untersuchung passieren. Dies betrifft insbesondere den Datenverkehr von Cloud-Anbietern und aus anderen als „vertrauenswürdig" eingestuften Quellen. Das ist ein fatales Manko. Unternehmen, die nicht den gesamten verschlüsselten Traffic überwachen, sind anfällig für darin verborgene Phishing-Angriffe, Malware usw. mit potenziell verheerenden Auswirkungen.

Im Zeitraum von Januar bis September **identifizierte und verhinderte die Zscaler-Cloud 6,6 Milliarden Bedrohungen**, die sich in verschlüsseltem Traffic verbargen.

In den ersten neun Monaten des Jahres 2020 analysierte das ThreatLabZ-Team den gesamten verschlüsselten Traffic in der Zscaler-Cloud nach Branchen aufgeschlüsselt. Es galt dadurch Erkenntnisse sowohl bezüglich des Gesamtvolumens an verschlüsseltem Traffic als auch der Bedrohungen zu gewinnen. Die wichtigsten Ergebnisse auf einen Blick:

- **Der Großteil des Internet-Traffics wird verschlüsselt:** 80 % des gesamten Datenverkehrs wird standardmäßig mit SSL/TLS verschlüsselt.
- **Explosionsartige Zunahme:** Die Anzahl der SSL-basierten Bedrohungen nahm in den vergangenen neun Monaten um 260 % zu; beschleunigt wurde dieser Trend durch die stark gewachsene Bedeutung Cloud-basierter Zusammenarbeit aufgrund der COVID-19-Pandemie.
- **Gesundheitswesen im Visier der Angreifer:** Insgesamt 1,6 Milliarden endeckte und abgewehrte Bedrohungen im verschlüsselten Traffic richteten sich gegen das Gesundheitswesen; an zweiter und dritter Stelle lagen Finanzwesen und Fertigungsbranche.
- **Zunehmender Missbrauch Cloud-basierter Filesharing-Dienste:** Über 30 % aller SSL-basierten Bedrohungen werden über Filesharing-Dienste wie Google Drive, OneDrive, AWS oder Dropbox eingeschmuggelt.
- **Versteckte Ransomware nimmt zu:** Über 5-mal mehr Ransomware wird im verschlüsselten Traffic übertragen.

SSL/TLS ist keine Sicherheitsgarantie: Warum verschlüsselter Traffic untersucht werden muss

Die Verschlüsselung von Internet-Traffic mit SSL (Secure Sockets Layer) und dem Nachfolger TLS (Transport Layer Security) gilt weltweit als Standard für die sichere Datenübertragung. Entsprechend wird heutzutage die überwältigende Mehrheit des Internet-Verkehrs verschlüsselt.[1] Problematisch daran ist, dass auch Cyberkriminelle sich die Verschlüsselung zunutze machen, um Malware und andere Bedrohungen unerkannt zu transportieren. Deswegen ist ein digitales Zertifikat keine Garantie mehr für die Vertrauenswürdigkeit des Traffics, der durch verschlüsselte Kanäle übertragen wird.

Cyberkriminelle haben raffinierte Angriffsketten entwickelt, die mit einer harmlos aussehenden Phishing-E-Mail beginnen, in der sich Malware oder eine andere Bedrohung verbirgt. Sobald der entsprechende Link von einem nichtsahnenden User angeklickt wird, geht der Angriff in die nächste Phase über – die Installation der Malware, die dann zur Exfiltration wertvoller Unternehmensdaten führt.

Richtig tückisch werden diese Angriffe dadurch, dass die ransportierte Malware oder andere Bedrohung selbst verschlüsselt wird, sodass sich ihre Dateistruktur komplett ändert. Cybersicherheitssysteme erkennen eingehende Bedrohungen anhand der Dateistruktur bzw. des „Fingerabdrucks" – bestimmte Strukturen werden automatisch blockiert. Durch jede Verschlüsselung wird der Datei jedoch ein völlig neuer Fingerabdruck verpasst, sodass die Sicherheitssysteme sie nicht als Bedrohung erkennen.

SSL-Unternsuchung ist die einzige wirksame Methode zur Abwehr schädlicher Dateien, die [über solche Dienste] übertragen werden, da Sicherheits-Engines naturgemäß keine Bedrohungen abwehren können, die sie nicht sehen.

[1] https://transparencyreport.google.com/https/overview?hl=de

Entwicklung des SSL-Traffics

Bei der Mehrzahl der Unternehmen hat sich die Erkenntnis durchgesetzt, dass die Verschlüsselung von Daten bei der Übertragung erforderlich ist, um sie vor unbefugten Blicken und Missbrauch zu schützen. Die Analyse ergab, dass der prozentuale Anteil des verschlüsselten Traffics im Bildungswesen am höchsten ist, gefolgt von der Fertigungsbranche, dem Finanz- und dem Gesundheitswesen. Die übrigen untersuchten Branchen – Einzel-/Großhandel, Dienstleistungen, Technologie/Kommunikation und öffentliche Verwaltung – lagen jedoch nur knapp dahinter. Branchenübergreifend lag der Anteil des verschlüsselten Traffics im Analysezeitraum von Januar bis September 2020 bei durchschnittlich 75 Prozent und erreichte Höchstwerte von über 80 Prozent.

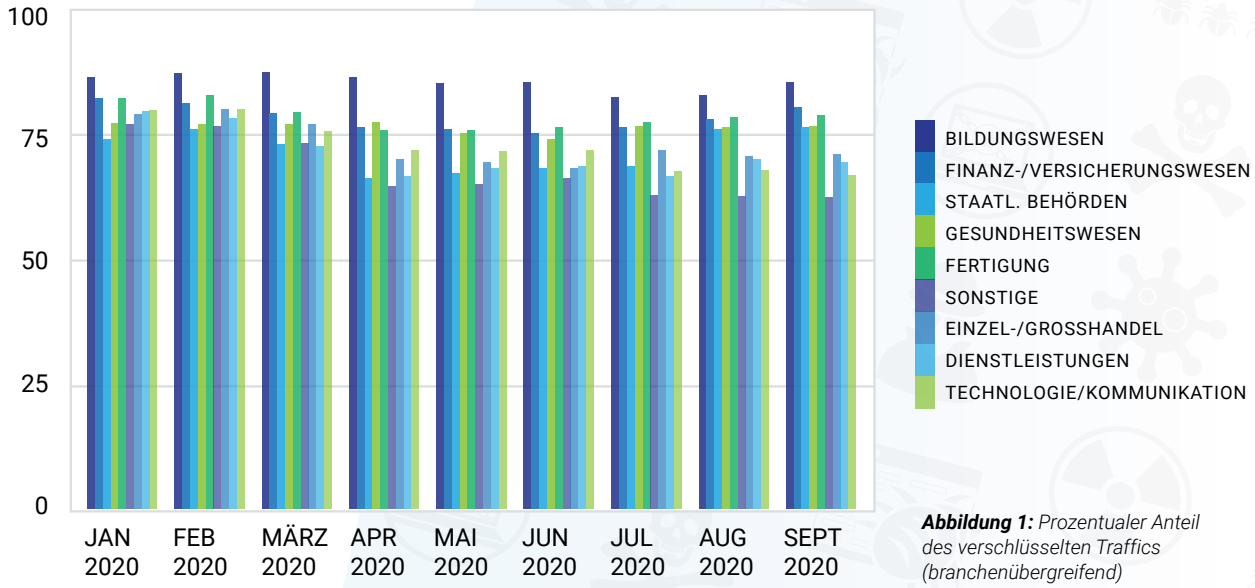


Abbildung 1: *Prozentualer Anteil des verschlüsselten Traffics (branchenübergreifend)*

Branchenübergreifend wurde ein hoher Anteil des Traffics verschlüsselt – entsprechend ist SSL/TLS-Üntersuchung für alle Unternehmen ein wichtiges Thema.

Die Recherche ergab, dass das Gesundheitswesen das beliebteste Angriffsziel durch verschlüsselte transportierte Malware ist. Im Zeitraum von Januar bis September 2020 richteten sich 25,5 % aller in der Zscaler-Cloud geblockten Advanced Threats im SSL-Datenverkehr gegen Unternehmen und Einrichtungen im Gesundheitswesen. Das Finanz-/Versicherungswesen war mit 18,3 % der blockierten Angriffe am zweitstärksten betroffen, gefolgt von Fertigungsunternehmen (17,4 %) und der öffentlichen Verwaltung (14,3 %).

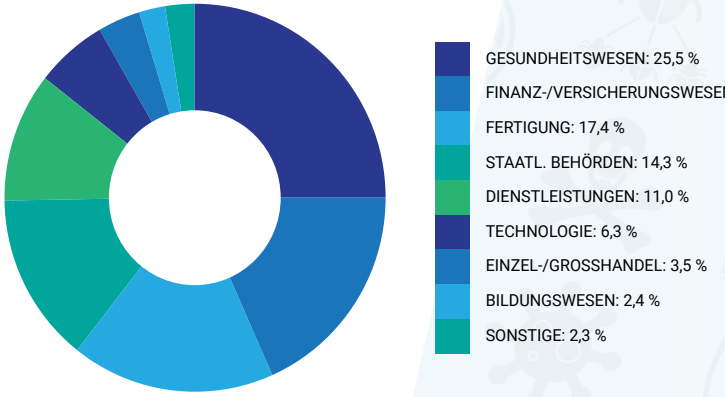


Abbildung 2: *Abgewehrte erweiterte Bedrohungen im verschlüsselten Traffic nach Branche*

Einrichtungen und Unternehmen aus dem Gesundheitswesen waren Angriffsziel Nr. 1 für Bedrohungen, die hinter SSL-Verschlüsselung verborgen wurde – und das, obwohl ihr reibungsloser Betrieb angesichts der globalen Pandemie wichtiger ist denn je. Angreifer haben die Pandemie zudem genutzt, um neue Kampagnen zu starten – mit gefälschten Websites für Nachrichten, Produkte und angebliche Heilmittel. Im ersten Quartal des Jahres 2020 nahmen COVID-bezogene Bedrohungen laut Angaben von ThreatLabZ um **30.000 Prozent** zu.

Schwerpunkt Gesundheitssektor

Im Analysezeitraum richteten sich mehr als 1,69 Milliarden Angriffsversuche im SSL-Traffic gegen den Gesundheitssektor, der damit so oft ins Visier genommen wurde wie keine andere Branche. Die überwältigende Mehrzahl der Angriffe auf diesen Sektor (84,2 Prozent) erfolgte über schädliche URLs. Diese URLs erreichen die User per E-Mail, SMS, Pop-ups oder Anzeigen auf Webseiten und veranlassen sie zum Herunterladen von Malware, Spyware oder Ransomware oder führen dazu, dass Konten gehackt werden.

Dass gerade das Gesundheitswesen immer wieder von Cyberkriminellen ins Visier genommen wird, liegt u. a. an den veralteten Systemen, die – bedingt durch langwierige Genehmigungsverfahren – in vielen Einrichtungen nach wie vor zum Einsatz kommen. Unzureichende Sicherheitskontrollen machen diese Systeme anfällig für bekannte Bedrohungen. Ohne vereinheitlichte Kontrollmechanismen sowie zentralisierten Überblick und Richtlinienverwaltung klaffen Lücken in den Sicherheitsmaßnahmen dieser Einrichtungen, die sie zum beliebten Angriffsziel für Cyberkriminelle machen.

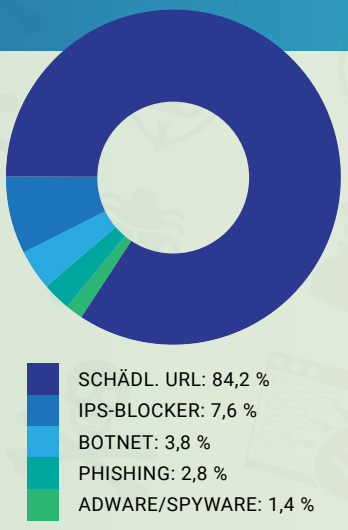


Abbildung 3: *Bedrohungen über verschlüsselte Kanäle gegen das Gesundheitswesen*

Angriffe werden immer raffinierter

Gefälschte Websites lassen sich oft daran erkennen, dass die URLs Rechtschreibfehler oder andere verdächtige Abweichungen enthalten, die sie von ihrem legitimen Vorbild unterscheiden. Allerdings sorgen Cyberkriminelle mit Techniken wie Domain-Squatting oder homographen Angriffen dafür, dass ihre Fälschungen echten Websites zum Verwechseln ähnlich sehen.

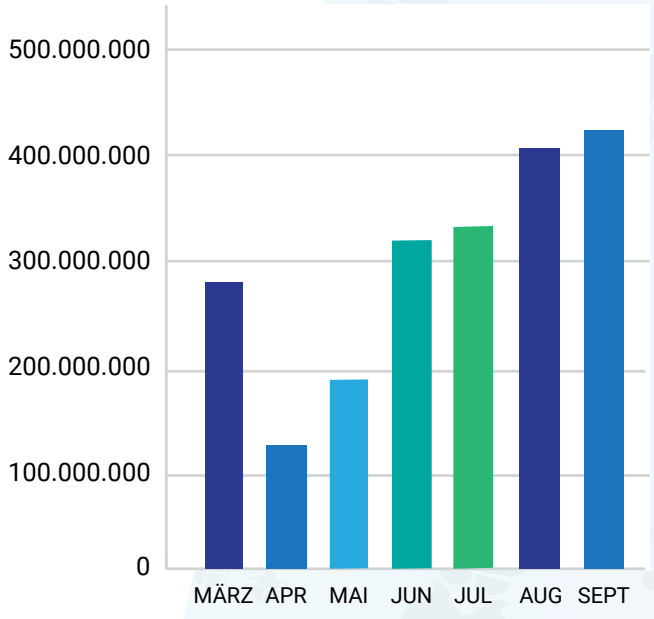
Als Domain-Squatting wird die Registrierung einer Top-Level-Domain bezeichnet, die sich auf den ersten Blick kaum von einer bekannten Marke unterscheiden lässt (z. B. gmali.com). Diese wird dann für Phishing-Angriffe, Diebstahl von Anmeldedaten oder zur Übertragung von Malware verwendet.

Homographe Angriffe funktionieren ähnlich wie Domain-Squatting. Hier beruht die Täuschung darauf, dass einzelne Buchstaben im Domainnamen durch ähnlich aussehende Schriftzeichen ersetzt werden (z. B. https://www.app1e.com).

Missbrauch von Cloud-Speicherdiensten

Cloud-Speicherdienste stellen ein zunehmend beliebtes Einfallstor für Angriffe dar. Solche Dienste eignen sich hervorragend für den sicheren Austausch von Dateien über SSL-basierte Übertragung im Internet. Da Cyberkriminelle aber wissen, dass die wenigsten Unternehmen über die erforderlichen Kapazitäten zur Untersuchung des gesamten SSL-Verkehrs verfügen, und zeitgleich, gängige Cloud-Dienste als vertrauenswürdig eingestuft werden, werden Angriffe gestartet, die scheinbar von diesen Diensten ausgehen.

Im Zeitraum von März bis September 2020 wehrte die Zscaler-Cloud **zwei Milliarden Bedrohungen** in verschlüsseltem Traffic ab. Bei der Mehrzahl der Bedrohungen handelte es sich um schädliche Inhalte, die in Google, AWS, Dropbox und OneDrive gehostet wurden. Die Anzahl dieser Bedrohungen verdoppelte sich von März bis September beinahe und machte knapp 30 Prozent aller Bedrohungen in SSL/TLS-Verschlüsselungen während dieses Zeitraums aus.



Von März bis September wehrte die Zscaler-Cloud **zwei Milliarden Bedrohungen** in SSL-Traffic aus Cloud-Speicherdiensten ab.

Abbildung 4: *Abgewehrte Bedrohungen in TLS/SSL-Traffic aus führenden Cloud-Speicherdiensten*

Abbildung 5 zeigt den Missbrauch von Cloud-Diensten zum Hosten und Übertragen von Malware. Die Malware-Payload (häufig eine Stage-1-Downloader-Datei) wird in einem oder mehreren Cloud-Speicherdiensten hochgeladen und die entsprechende URL dann im Rahmen einer E-Mail-Spam-Kampagne verbreitet. Durch Verwendung gängiger Dienste wie Google, Microsoft, Amazon und Dropbox erhöht sich die Wahrscheinlichkeit, dass die Empfänger den Link tatsächlich anklicken.

Auch die Wildcard-SSL-Zertifikate dieser Anbieter werden immer wieder von Cyberkriminellen missbraucht. Wenn Traffic von Cloud-Services als vertrauenswürdig eingestuft und ohne Untersuchung weitergeleitet wird haben Betrüger leichtes Spiel. Malware-Payloads in verschlüsseltem Traffic unterlaufen Sicherheitslösungen, auf Basis von URL-Filtern, die auf URL-Filtern basieren (Anti-Spamwächter, E-Mail-Schutz, Firewalls usw). **Eine Phishing-E-Mail mit einem Link zu einer schädlichen Datei, die in einem vertrauenswürdigen Cloud-basierten Dienst gehostet wird, kann herkömmliche E-Mail-Sicherheitslösungen umgehen.**

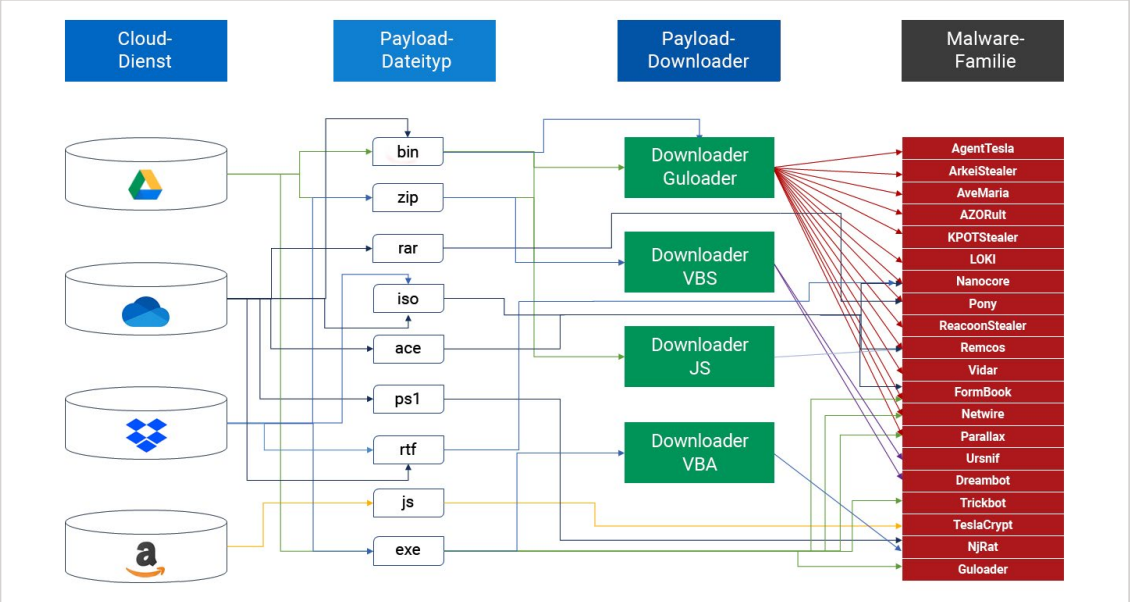


Abbildung 5: *Übertragung von Malware-Payloads über Cloud-Dienste*

Im folgenden Beispiel werden URLs aus dem Cloud-Speicherdienst OneDrive gezeigt. In diesem Beispiel handelt es sich bei den ersten beiden Links um schädliche URLs, die den User zum Herunterladen von Dateien aus den Malware-Familien „Trojan EdLoader" und „Backdoor LokiBot" veranlassen. Die dritte URL ist ein legitimer Link zur eigentlich gewünschten Datei. Die Subdomain und Uniform Resource Identifier (URI) werden als zufällige Zeichenfolgen angezeigt, sodass die Unterscheidung zwischen legitimen und schädlichen URLs unmöglich wird. SSL-Untersuchung ist die einzige wirksame Methode zur Abwehr schädlicher Dateien, die über solche Dienste übertragen werden, da Sicherheits-Engines naturgemäß keine Bedrohungen abwehren können, die sie nicht sehen.

Abbildung 6: *Zufällige Zeichenfolgen in Subdomains lassen keine Unterscheidung zwischen legitimen und schädlichen URLs zu*

Angriffe auf Mobilgeräte

Smartphones stellen ebenfalls beliebte Angriffsziele dar. Das Grundprinzip ist ähnlich wie beim Spoofing von Webseiten: gefälschte Apps, die legitim aussehen. Auf diese Weise gelingt es z. B. dem Bankentrojaner Cerberus – dessen Name und Symbol schwer von der Google-Play-App zu unterscheiden sind –, Android-Geräte zu infizieren. Sobald ein nichtsahnender User die gefälschte App anklickt, wird er in einer Benachrichtigung aufgefordert, Bedienungshilfen zu aktivieren. (Dabei handelt es sich um Tools zur barrierefreien Nutzung von Android-Geräten und -Apps.)

Diese Angriffsmethode beruht auf der Annahme, dass ein Großteil der User derartige Benachrichtigungen durch „Zulassen" wegklickt, ohne sie gründlich durchzulesen. In diesem Fall führt dies dazu, dass die App Lesezugriff auf die Inhalte anderer Apps auf dem Startbildschirm erhält und ohne Wissen des Users verschiedene Aktionen durchführen kann.

Die Malware kann Zugangsdaten u. a. für Bank-Apps, Gmail oder die Zwei-Faktor-Authentifizierung über die Google-Authenticator-App abgreifen und exfiltrieren. Außerdem kann sie ohne Wissen des Users Audio-Aufnahmen anfertigen oder Textnachrichten auslesen. Schlimmer noch: Nachdem der User die Aktivierung der Bedienungshilfen einmal zugelassen hat, verhindert die Malware ihre Deaktivierung und erschwert das Deinstallieren der App.

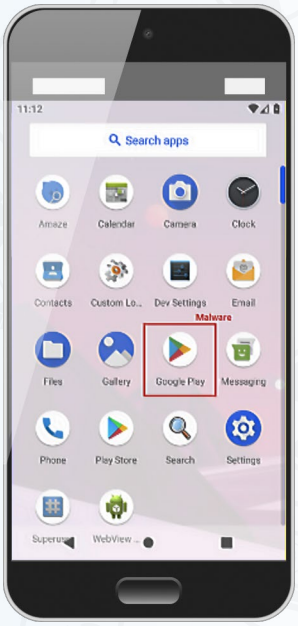


Abbildung 7: *Gefälschte Google-Play-App*

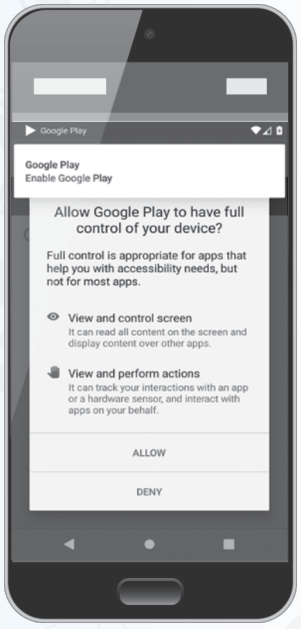
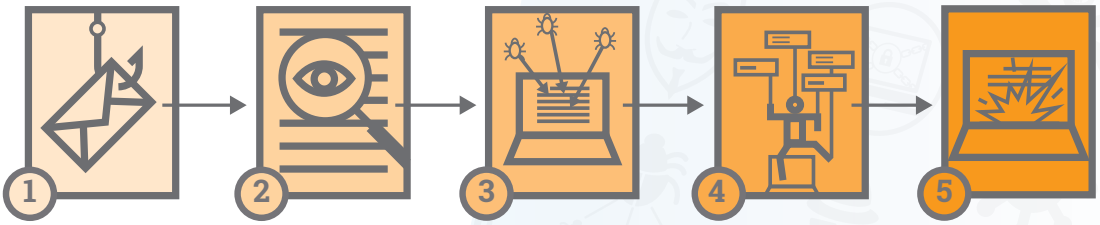


Abbildung 8: *Benachrichtigung auf gefälschter Google-Play-App*

Anatomie eines Angriffs



Delivery: Erfolgt oft mithilfe einer Phishing-E-Mail, in der sich ein Exploit oder eine Malware verbirgt. Die Malware wird durch Herunterladen bzw. Anklicken eines Links übertragen.

Exploitation: Nach erfolgreicher Übertragung sucht das Programm nach Schwachstellen im System, die es zur Ausführung des Code ausnutzen kann.

Installation: Malware wird auf das Gerät des Opfers geladen.

Command-and-Control (C&C) Callback: bezeichnet die Kommunikation der Malware mit C&C-Servern zum Einholen von Anweisungen oder für die Übertragung gestohlener Daten.

Detonation: In diesem Schritt kann die Malware weitere Schadprogramme installieren, Daten exfiltrieren oder andere Aktionen ausführen, die von dem C&C-Server programmiert werden.

Analyse der Angriffskette

Phishing

Phishing kommt in der Regel als erste Stufe eines mehrstufigen Cyberangriffs zum Diebstahl von Anmeldedaten zum Einsatz. Insgesamt wurden über **193 Millionen Phishing-Angriffe** analysiert, die im Zeitraum von Januar bis September 2020 über verschlüsselte Kanäle übertragen, aber von der Zscaler-Cloud erkannt und abgewehrt wurden. Diese Angriffsversuche wurden nach Branchen aufgeschlüsselt. Die Fertigungsbranche war mit 38,6 Prozent der versuchten Phishing-Angriffe am stärksten betroffen – wohl u. a. aufgrund der potenziell höheren Anfälligkeit durch heterogene IT-Infrastrukturen und -Systeme an unterschiedlichen Standorten. An zweiter Stelle folgt der Dienstleistungssektor, auf den 13,8 Prozent der Angriffsversuche entfielen.

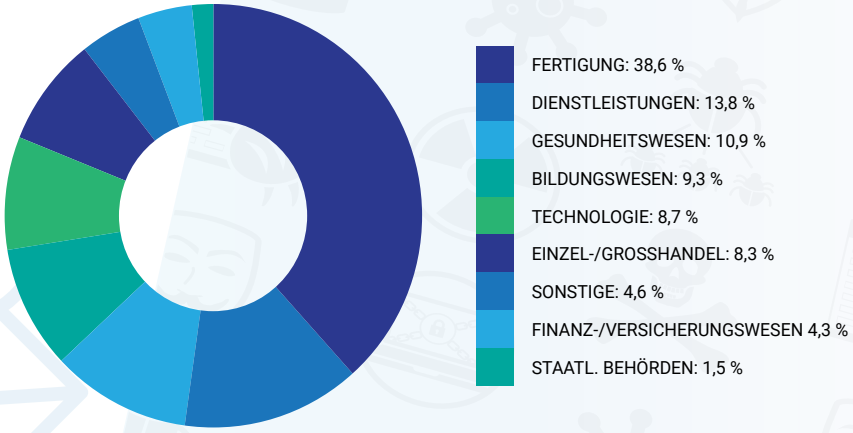


Abbildung 9: *Abgewehrte Phishing-Bedrohungen über verschlüsselte Kanäle nach Branche*

Missbrauch von Diensten und Marken für Phishing-Angriffe

Bei Phishing-Angriffen kommen häufig gefälschte Websites zum Einsatz, die der Website einer legitimen Marke täuschend ähnlich sehen. Konkret bedeutet das: Der User bekommt eine E-Mail, in der er aufgefordert wird, einen Link anzuklicken, der ihn zu einer gefälschten Website weiterleitet. Dort wird der User aufgefordert, Benutzernamen und Passwort oder andere Daten einzugeben, die von Cyberkriminellen für Angriffe missbraucht werden können.

Die Recherche hat ergeben, dass Microsoft häufiger ins Visier von Phishing-Angriffen gerät als jede andere Marke. Webbasierte Microsoft-Produkte wie Office 365, SharePoint und OneDrive werden von Cyberkriminellen immer wieder missbraucht, um Anmeldedaten von Unternehmenskunden zu stehlen. An zweiter Stelle folgten sogenannte „Tech Support"-Betrugsmaschen. Hierbei erhält der User eine Nachricht über einen angeblichen Hacker-Angriff auf sein Gerät, den der „Microsoft-Support" beheben wird– sobald der Nutzer seine Kreditkartendaten angegeben hat.

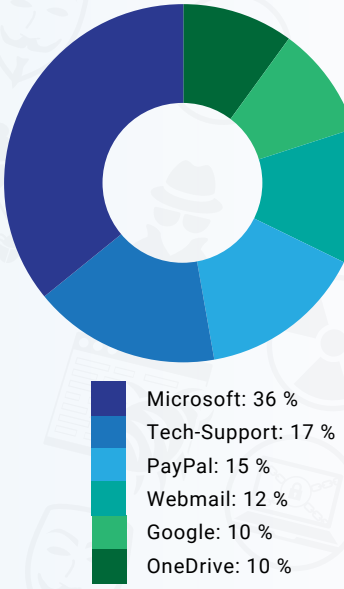


Abbildung 10: *Die am häufigsten für Phishing-Angriffe missbrauchten Marken und Dienste*

PayPal und Google zählten ebenfalls zu den Marken, die am häufigsten für Phishing-Angriffe missbraucht wurden. Die Spoofing-Websites sahen den echten täuschend ähnlich und waren nur schwer als Fälschungen zu erkennen.

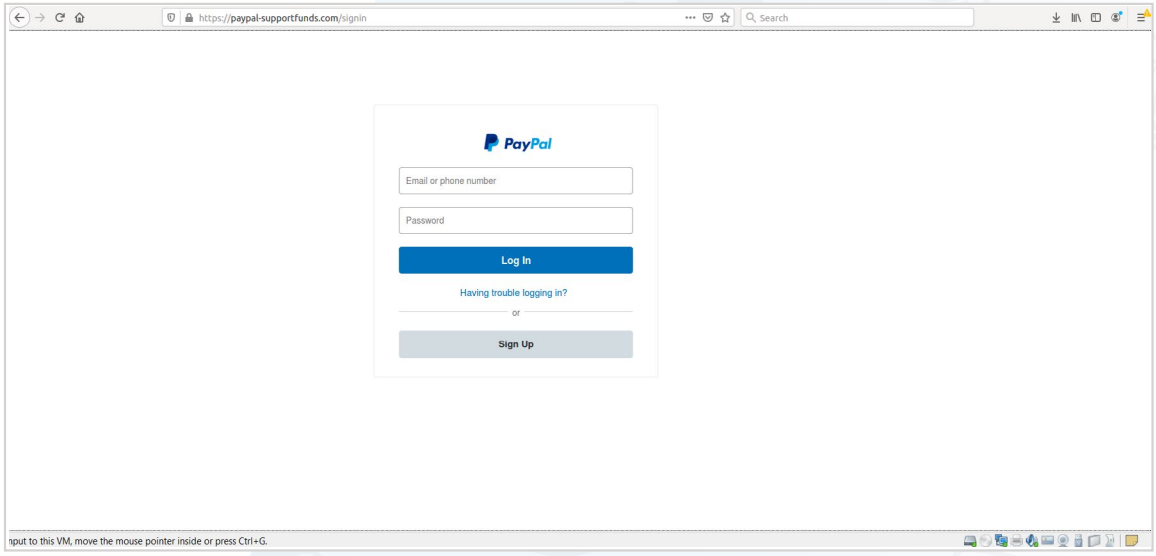


Abbildung 11: *Gefälschte PayPal-Website über HTTPS*

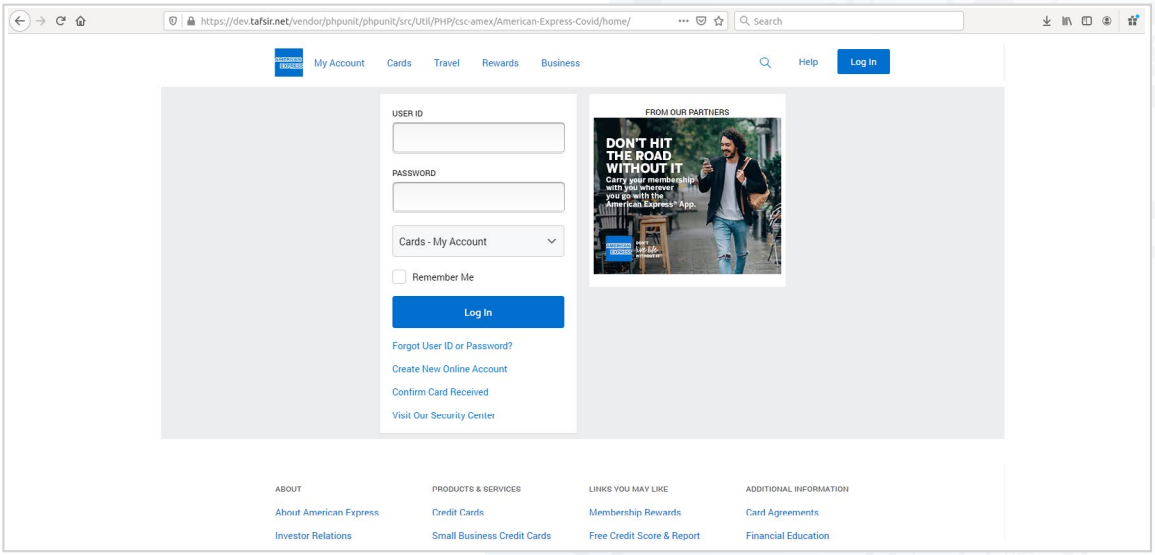


Abbildung 12: *Gefälschte American-Express-Website über HTTPS*

Netflix-Phishing-Angriff über HTTPS

Dass sich Streaming-Services wie Netflix während der Pandemie wachsender Beliebtheit erfreuen, ist Cyberkriminellen nicht entgangen. So werden auch Streaming-Dienste für Phishing-Angriffe missbraucht, die auf die Entwendung von Anmeldedaten abzielen. Die Fälschungen sind teilweise so geschickt, dass sie sich kaum von echten Webseiten unterscheiden (siehe Abb. 13).

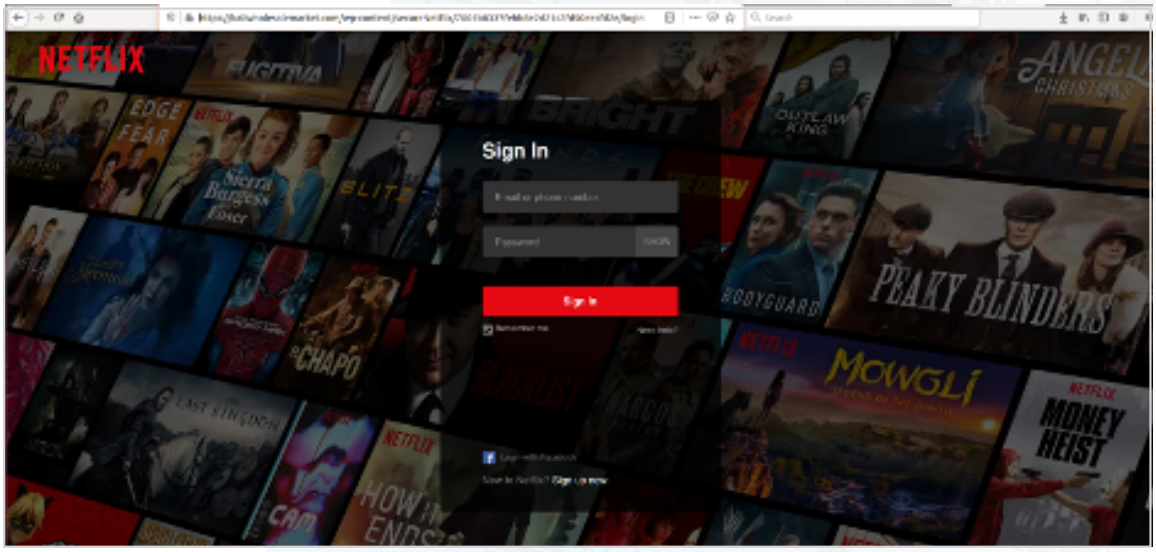


Abbildung 13: *Gefälschte Netflix-Seite*

„Tech Support“-Angriff über HTTPS auf Microsoft-User

In Abbildung 14 wird eine gefälschte Webseite für „Tech Support“-Angriffe auf Microsoft-Anwender dargestellt. Bei Anklicken der URL wird angezeigt, dass das HTTPS-Zertifikat von Microsoft verifiziert wurde. Die Verwendung dieses Zertifikats zeigt, dass die Angreifer eine weitere bekannte Marke – nämlich Azure – missbrauchen, um die Legitimität der Webseite vorzutäuschen.

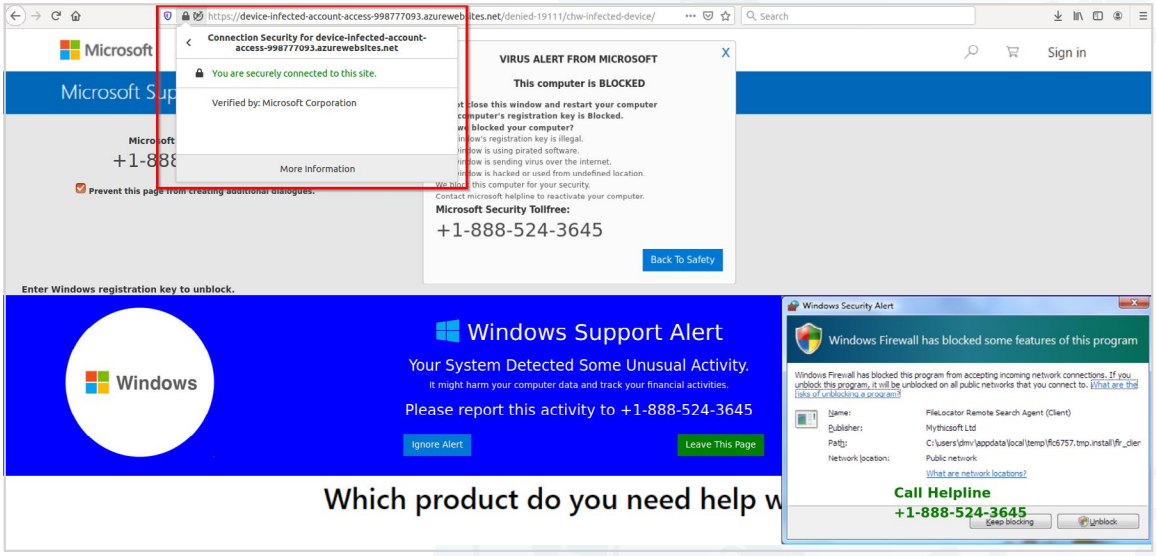


Abbildung 14: *„Tech Support“-Angriff über HTTPS auf Microsoft-Kunden*

Browser-Exploits

Mithilfe von Browser-Exploits machen sich Angreifer eine Sicherheitslücke im Betriebssystem zunutze, um die Browser-Einstellungen des Opfers ohne dessen Wissen zu ändern. Insgesamt wehrte die Zscaler-Cloud im Analysezeitraum über 658.000 Browser-Exploit-Bedrohungen ab, die sich hauptsächlich gegen die Fertigungsbranche (26,5 Prozent) und das Finanz-/Versicherungswesen (19,9 Prozent) richteten.

Die historisch bedingte Fragmentierung der Fertigungsbranche macht sie zu einem beliebten Angriffsziel für Cyberkriminelle. Häufig kommen bis heute an unterschiedlichen Standorten jeweils eigene IT-Infrastrukturen und heterogene Systeme zum Einsatz. Wie in anderen Branchen auch führt das Fehlen vereinheitlichter Kontrollmechanismen sowie zentralisierter Berichterstattung und Richtlinienverwaltung in den Sicherheitsmaßnahmen dieser Unternehmen zu Lücken, die Cyberkriminelle entsprechend ausnutzen.

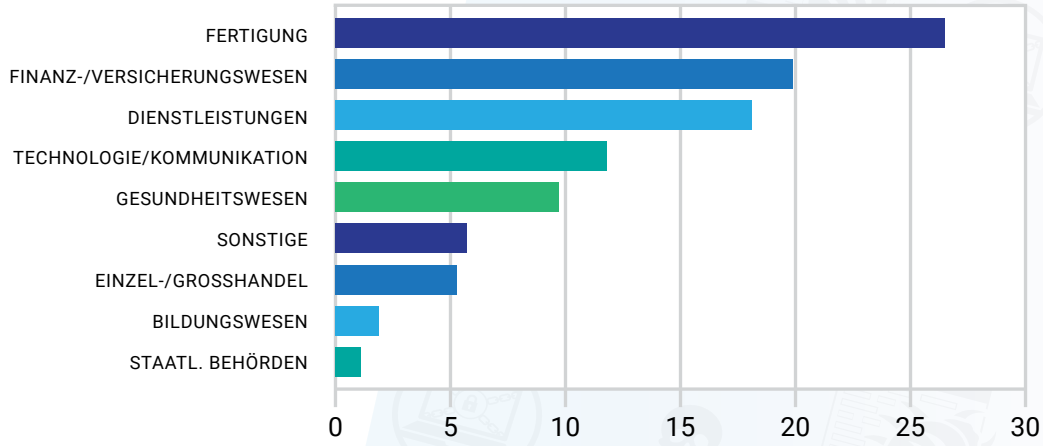


Abbildung 15: *Abgewehrte Browser-Exploits über verschlüsselte Kanäle nach Branche*

Ransomware

Seit März 2020 hat die Anzahl der über SSL/TLS-Kanäle übertragenen Ransomware-Angriffe, die von Zscaler ThreatLabZ abgewehrt wurden, um 500 Prozent zugenommen. Mit der Anzahl von Mitarbeitern, die im Homeoffice auf interne Anwendungen zugreifen, nahmen auch die Ransomware-Angriffe insbesondere auf Branchen zu, die sehr anfällig für Lösegeldforderungen sind.

Am häufigsten richteten sich Ransomware-Angriffe über verschlüsselte Kanäle gegen Unternehmen aus den Sektoren Technologie/Kommunikation (40,5 %) und Gesundheitswesen (26,5 %).

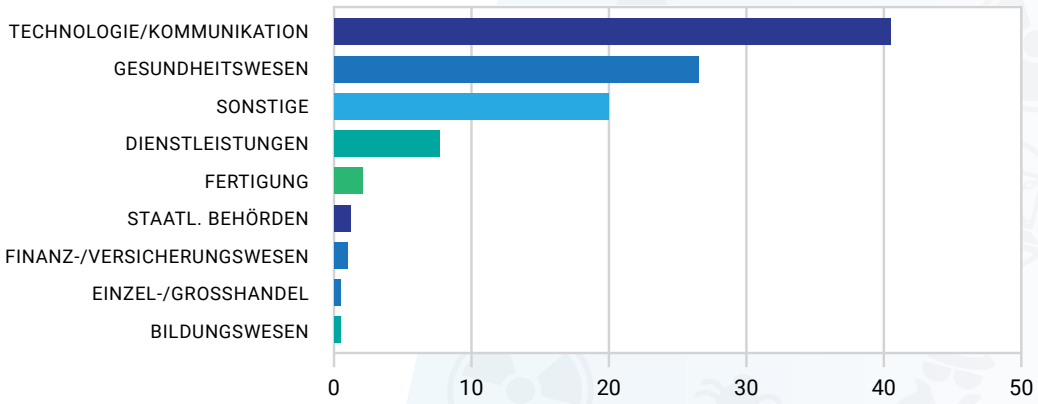


Abbildung 16: *Abgewehrte Ransomware-Angriffe über verschlüsselte Kanäle nach Branche*

Als besonders beliebt erwiesen sich hierbei Varianten aus den Ransomware-Familien FileCrypt/FileCoder, Sodinokibi, Maze und Ryuk. Neu ist, dass viele dieser Ransomware-Varianten im Laufe des vergangenen Jahres um eine Funktion zum Exfiltrieren von Daten ergänzt wurden. Zusätzlich zur Verschlüsselung der Daten ihrer Opfer sind Ransomware-Gangs damit in der Lage, sensible Daten zu exfiltrieren. Diese dienen den Angreifern quasi als Versicherungspolice: Selbst wenn das betroffene Unternehmen über noch so gute Backups verfügt, ist es zur Zahlung des Lösegeld gezwungen, um zu verhindern, dass die erbeuteten Daten offengelegt werden.

Malware

Durch Installation von Malware auf dem Gerät eines Users verschaffen sich Kriminelle dauerhaften Zugriff auf dieses Gerät. Ermöglicht wird die Installation häufig durch erfolgreiche Ausnutzung von Sicherheitslücken bzw. durch Social-Engineering-Angriffe. Dieser Angriffstyp wurde bei der Analyse der Forscher von Zscaler bei weitem am häufigsten beobachtet. Insgesamt wurden im Analysezeitraum über **2,6 Milliarden Malware-Bedrohungen** abgewehrt.

Malware-Angriffe richten sich besonders häufig gegen Unternehmen aus Branchen, in denen personenbezogene Daten verarbeitet werden. In dieser Analyse betraf dies vor allem das Gesundheits- sowie das Finanz-/Versicherungswesen mit 27,7 bzw. 19,6 Prozent der abgewehrten Malware-Angriffe über verschlüsselte Kanäle.

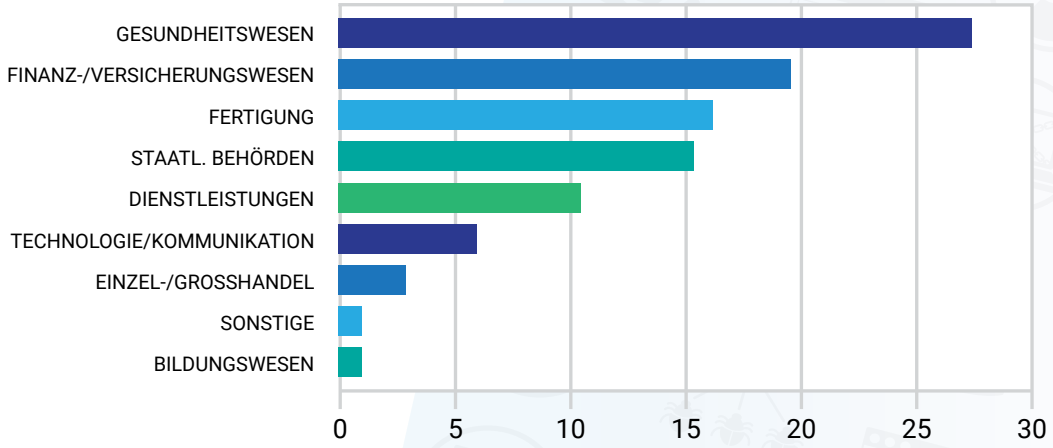


Abbildung 17: *Abgewehrte Malware-Angriffe über verschlüsselte Kanäle nach Branche*

C&C-Aktivität von Malware über verschlüsselte Kanäle

C&C-Kommunikation (Command-and-Control) ist ein weiterer Kernbestandteil der Angriffskette. Wenn die Malware sich erfolgreich der Erkennung entzogen hat und auf dem Gerät des Users installiert wurde, stellt sie die Kommunikation zum C&C-Server her. Häufig sind Malware-Payloads so programmiert, dass zur Aktivierung ihrer schädlichen Wirkung erst ein entsprechender Befehl vom Server erforderlich ist. Emotet und TrickBot zählten zu den Malware-Familien, die in dieser Analyse am häufigsten auftraten.

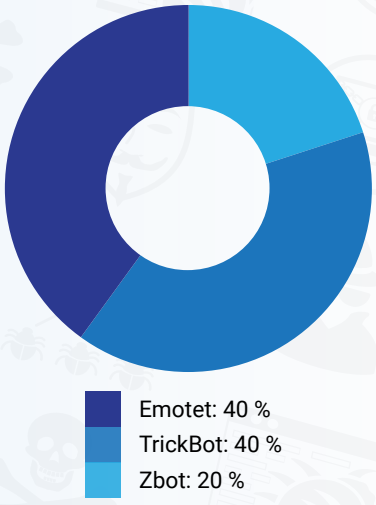


Abbildung 18: *Am häufigsten abgewehrte C&C-Aktivität über verschlüsselte Kanäle*

Neben Emotet und TrickBot wurden Aktivitäten von Ursnif und Unruy nachgewiesen. Emotet kam branchenübergreifend am häufigsten zum Einsatz. TrickBot folgte als zweithäufigste Malware bei Angriffsversuchen auf das Finanz-/Versicherungswesen sowie auf die öffentliche Verwaltung. Ursnif war besonders bei Angriffen auf das Gesundheitswesen und die Fertigungsbranche beliebt. Unruy lag bei Angriffsversuchen auf Bildungseinrichtungen an zweiter Stelle.

Diese Malware sollten Sie kennen

Emotet: Emotet wurde 2014 als Bankentrojaner in die Welt gesetzt. Inzwischen hat er sich zu einer branchenübergreifend stark verbreiteten Bedrohung entwickelt und wird hauptsächlich zum Spammen sowie zum Herunterladen von Malware im infizierten System eigesetzt. Nach Einschätzung der US-amerikanischen Cybersicherheitsbehörde (CISA) zählt Emotet zu den Malware-Familien, die im öffentlichen und im privaten Sektor **die höchsten Kosten und schwersten Schäden** verursachen. Emotet hat sich wohl auch aufgrund seiner modularen Struktur als sehr widerstandsfähig erwiesen. Aufgrund regelmäßiger Aktualisierungen entzieht er sich immer wieder der Erkennung.

TrickBot: TrickBot ist ein Nachfolger des Bankentrojaners Dyre und hat sich als einer der häufigsten und gefährlichsten Malware-Familien in der heutigen Bedrohungslandschaft durchgesetzt. TrickBot wird häufig in Kombination mit anderen Arten von Malware verwendet, teilweise als Erstinfektionsvektor zur Einleitung eines Angriffs oder zum Herunterladen weiterer Malware-Familien, um möglichst viel Profit aus einer Infektion zu schlagen.

Ursnif: Der Ursnif-Trojaner zählt zu den aktivsten und am häufigsten auftretenden Varianten der Malware-Familie „Gozi“ (auch als „Dreambot“ bekannt). Er wird zumeist durch Exploit-Kits, E-Mail-Anhänge und Links zu schädlichen URLs verbreitet.

Unruy: Unruy ist ein Trojaner, der zum Anzeigen und Anklicken unerwünschter Werbung dient, um Umsätze für die Hacker zu generieren. Er kommuniziert mit externen Hosts und richtet u. U. durch willkürliches Herunterladen und Ausführen von Dateien weiteren Schaden an.

Wirksame Abwehr verschlüsselter Bedrohungen

Voraussetzung für eine wirksame Abwehr ist zunächst die Erkenntnis, dass die SSL-Verschlüsselung keine Garantie für sicheren Traffic ist. Mit der Verbreitung der Verschlüsselung zum Schutz von Daten hat auch ihr Missbrauch durch Cyberkriminelle zugenommen, die darin ein probates Mittel zum Einschmuggeln von Angriffen sehen. Die Untersuchung von verschlüsseltem Traffic ist damit wichtiger als je zuvor. Die Mehrzahl der Unternehmen befolgt Sicherheits-Best-Practices und verschlüsselt ihren Internet-Traffic. Indes bieten herkömmliche Sicherheitstools wie Next-Generation Firewalls in aller Regel nicht die erforderliche Leistung und Kapazität zur Untersuchung des gesamten SSL-Traffics. Eine komplette Lahmlegung der Betriebs- und Arbeitsabläufe kann sich kein Unternehmen leisten. Deswegen lassen viele IT-Teams den verschlüsselten Traffic weitgehend ohne Scannen passieren.

Erschwerend kommt hinzu, dass der Umgang mit personenbezogenen Daten von Kunden, Patienten usw. strengen Vorschriften unterliegt. Unterschiedliche Richtlinien für die Untersuchung der verschiedenen Datentypen zu erstellen und standortübergreifend durchzusetzen, ist eine komplexe Aufgabe, die sich viele Unternehmen lieber sparen.

Wie lässt sich ein Unternehmen also vor den Gefahren schützen, die sich im verschlüsselten Traffic verbergen – und zwar ohne Leistungseinbußen? Wie gelingt es, den gesamten verschlüsselten Traffic sämtlicher User innerhalb und außerhalb des Netzwerks zu entschlüsseln und zu scannen – und zwar ohne Verstöße gegen die geltenden Datenschutzvorschriften?

- **Entschlüsseln, Erkennen und Abwehr von Bedrohungen im gesamten SSL-Traffic** mit einer Cloud-nativen proxybasierten Architektur, die den gesamten Traffic aller User überwacht.
- **Quarantäne unbekannter Bedrohungen und Abwehr von „Patient Zero"-Malware** mit KI-basierter Analyse verdächtiger Inhalte, die von herkömmlichen Firewalls womöglich durchgelassen würden.
- **Einheitlicher Sicherheitsstandard für alle User und alle Standorte**, damit sämtliche Mitarbeiter im Homeoffice, in der Firmenzentrale oder auch unterwegs gleichermaßen zuverlässig geschützt sind.
- **Sofortige Minimierung der Angriffsfläche** durch das „Zero Trust"-Grundprinzip, das von vornherein keine lateralen Bewegungen zulässt. Apps sind für die Angreifer unsichtbar, und befugte User greifen direkt auf die benötigten Ressourcen statt auf das gesamte Netzwerk zu.

Diese Lösung erfordert die Skalierbarkeit und Leistungsfähigkeit einer Cloud-nativen, Proxy-basierten Architektur wie der Zscaler Zero Trust Exchange.Eine Cloud-basierte Sicherheitsplattform wird den Anforderungen bezüglich Verschlüsselung und Untersuchung durch elastisch skalierbare Rechenleistung gerecht und gewährleistet standortübergreifend die konsistente Durchsetzung von Richtlinien. Zscaler bietet SSL-Untersuchung in skalierbarem Maßstab im Rahmen seiner Dienste-Plattform an. Bei Zunahme des Traffics werden die Kapazitäten umgehend bedarfsgerecht aufgestockt – ohne dass Hardware aufgerüstet, bestellt oder verschickt werden muss.

Keine Branche ist vor Sicherheitsbedrohungen gefeit. Je mehr Traffic verschlüsselt wird, desto unverzichtbarer wird die Untersuchung dieses Traffics. Eine mehrschichtige Defense-in-Depth-Strategie, die SSL-Untersuchung vollumfänglich unterstützt, ist eine unabdingbare Voraussetzung für die wirksame Abwehr der eskalierenden Bedrohungen, die sich im verschlüsselten Traffic verbergen.

Zscaler kann Ihren gesamten SSL-Traffic ohne Auswirkungen auf Leistung oder Compliance überwachen. Mit unserem **Online-Tool zur Analyse von Sicherheitslücken** können Unternehmen die Fähigkeit Ihres Unternehmens zur Untersuchung von SSL/TLS-Traffic prüfen.

Über ThreatLabZ

ThreatLabZ ist die für Sicherheitsthemen zuständige Abteilung von Zscaler. Das Team aus ausgewiesenen Experten ist zuständig für die Früherkennung neuartiger Bedrohungen und damit für die Sicherheit Tausender Unternehmen weltweit, die sich zum Schutz ihrer Daten auf die Zscaler-Plattform verlassen. Neben der Malware-Forschung und Verhaltensanalyse leisten die Teammitglieder einen wichtigen Beitrag zur Erforschung und Entwicklung neuer Prototyp-Module zur Erweiterung der Zscaler-Plattform. Die Durchführung interner Sicherheitsaudits zur Gewährleistung der Produkte- und Infrastrukturkonformität von Zscaler fällt ebenfalls in den Verantwortungsbereich des ThreatLabZ. Im Portal **research.zscaler.com** werden regelmäßig ausführliche Analysen neuer Bedrohungen veröffentlicht.

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, die über 150 Rechenzentren auf der ganzen Welt verteilt ist, ist die weltweit größte Inline-Cloud-Sicherheitsplattform. Informieren Sie sich unter zscaler.com oder folgen Sie uns auf Twitter **@zscaler**.

zscaler™