CISCO
SECURE

Kritische Bedrohungen im Radar

Eine Analyse der schwerwiegendsten Sicherheitsvorfälle

Muster im Verhalten von Cyberkriminellen erkennen

Hazel Burton

(Chefredakteurin)

Joe Walsh, Gitarrist von den Eagels, sagte einmal: „Im Laufe eines Lebens hat man den Eindruck, dass überall Anarchie und Chaos herrscht. Ein unvorhergesehenes Ereignis scheint auf das andere zu folgen. Wenn man aber später auf sein Leben zurückblickt, stellt man fest, dass das Chaos Ordnung hatte."

Leider konnten Cybersecurity-ExpertInnen diese Einsicht 2021 nicht teilen, denn sie hatten bzw. haben es immer noch mit zahlreichen schwerwiegenden Bedrohungen zu tun. Da wären z. B. die Log4j-Ransomware, die es auf kritische Infrastrukturen abgesehen hat, eine höhere Anzahl von gemeldeten Schwachstellen im Vergleich zum Vorjahr, dynamische Lieferkettenangriffe und Emotet, eine Malware, die wieder zum Leben erweckt wurde. Neben all diesen neu aufkommenden Bedrohungen gibt es außerdem noch die alltäglichen Risiken, die es einzudämmen gilt.

Um die wichtigen Bedrohungstrends im Jahr 2021 zu analysieren und Ordnung in das Chaos zu bringen, habe ich mich mit sechs ExpertInnen für Bedrohungserkennung und AnalystInnen von Cisco Secure zusammengeschlossen. Ich habe sie zu ihren Erkenntnissen bezüglich einer bestimmten Cybersicherheitsbedrohung bzw. zu einem bestimmten Vorfall in den vergangenen 12 Monaten befragt. Jede/r Einzelne wählte ein Thema aus, das uns fundierte Informationen zu den aktuellen Prioritäten der Angreifer liefert.

Zur zeitlichen Einordnung: Diese Inhalte wurden im Januar 2022 erstellt. Die Ereignisse in der Ukraine werden hier nicht abgedeckt. Aktuelle Informationen dazu finden Sie im Talos Threat Advisory Blog. Dieser wird kontinuierlich aktualisiert.

In diesem Bericht finden Sie auch Vorhersagen und Präzedenzfälle für das kommende Jahr. Nachdem das Jahr 2021 eher chaotisch ablief, war ich mir nicht ganz sicher, wie wir vorgehen sollten. Matt Olney, Director of Threat Intelligence and Interdiction bei Cisco Talos, teilte mir in einem Gespräch seine Einschätzung mit:

„Grob gesagt ist in den letzten fünf Jahren nichts passiert, was unseren Verteidigungsansatz grundlegend geändert hat. Jedes Jahr haben wir es im Durchschnitt mit ein oder zwei bedrohlichen, überraschend auftretenden Schwachstellen zu tun. In einem Wettlauf mit den Angreifern, die diese Schwachstellen ausnutzen möchten, versuchen wir als Sicherheitsverantwortliche, diese zu verstehen und entsprechende Schutzmaßnahmen zu treffen."

„Angriffe auf Lieferketten und Ransomware sind auf jeden Fall ein großes Problem und aus diesem Grund reagieren Regierungen weltweit verstärkt darauf."

Die Expertenanalyse in diesem Bericht liefert einen Überblick über die wichtige Rolle der Abwehr und die Funktionen, die wir in der Branche auf Basis eingehender Analysen des Verhaltens von Angreifern in der Vergangenheit entwickelt haben.

In diesem Bericht erfahren Sie von ExpertInnen, deren Aufgabe es ist, Muster von Cyberkriminellen zu erkennen, mehr über den Umgang mit kritischen Bedrohungen.

Inhalt

Colonial Pipeline:

Mehr gegen Ransomware tun als nur hoffen und beten

mit Matt Olney,
Director of Cisco Talos
Threat Intelligence and Interdiction

Warum haben Sie sich bei der Fülle an Vorfällen im Jahr 2021 gerade für den bei Colonial Pipeline entschieden?

Es gibt zwei Aspekte, die ich an dem Vorfall bei Colonial Pipeline interessant fand. Zum einen die globale Reichweite, zum anderen die Auswirkungen auf die Kraftstoffversorgung an der Ostküste der USA. Aufgrund des Angriffs erhöhte sich der politische Druck, was folglich dazu führte, dass die US-Regierung ihre Reaktion auf Ransomware-Aktivitäten beschleunigte.

Der zweite Aspekt ist die Reaktion der Angreifer. Die Situation war vergleichbar mit der Geschichte von Ikarus, der sich bei seinem Flug zu nah an die Sonne wagte. Die Angreifer wussten, dass sie mit dem Angriff auf eine kritische Infrastruktur eine Grenze überschritten hatten. Das Umfeld der Angreifer reagierte prompt mit massiven Maßnahmen.

Nach dem Angriff auf Colonial Pipeline hat sich sicherlich einiges geändert – bis heute.

Wann wurde der Ransomware-Angriff gestartet und wie hat man anfänglich darauf reagiert?

Um eines klarzustellen: Cisco war bei der Reaktion von Colonial Pipeline nicht involviert. Meine Informationen stammen alle aus der öffentlichen Berichterstattung.

An einem Freitagmorgen Anfang Mai wurde ein zuvor infiziertes Netzwerk bei Colonial Pipeline verschlüsselt. Im Grunde war der Zugriff auf das gesamte IT-Netzwerk nicht mehr möglich.

Kritische Infrastrukturumgebungen sind normalerweise in die Bereiche IT (Information Technology) und OT (Operational Technology) aufgeteilt. In diesen Bereichen befinden sich die industriellen Komponenten. Die Komponenten, die für die Pipeline, das Pumpen des Kraftstoffs und alle Monitoring-Aufgaben erforderlich sind, befinden sich in der OT-Umgebung.

Berichten zufolge gab es keine Auswirkungen auf die OT-Umgebung von Colonial Pipeline. Lediglich die IT-Umgebung war von der Verschlüsselung betroffen. Colonial zahlte umgehend das Lösegeld in Höhe von 75 Bitcoin, was zu diesem Zeitpunkt einem Gegenwert von circa 4,4 Millionen USD entsprach.

Sie mussten jedoch feststellen, dass das von den Angreifern bereitgestellte Entschlüsselungstool sehr langsam arbeitete, sodass es schneller ging, die Daten mit traditionellen Mitteln wiederherzustellen. Ich glaube nicht, die Verantwortlichen bei Colonial würden im Rückblick behaupten, die Zahlung des Lösegelds hätte sich gelohnt.

Berichten zufolge hatte sich Colonial Pipeline dazu entschieden, keinen Kraftstoff zu pumpen, da sie nicht in der Lage waren, die Kraftstofflieferungen nachzuverfolgen und in Rechnung zu stellen (da diese Funktion Teil der IT-Umgebung des Unternehmens ist). Und das, obwohl das OT-Netzwerk funktionsfähig und verfügbar war.

Die Verantwortlichen bei Colonial hatten Bedenken und man wollte prüfen, ob das OT-Netzwerk sicher ist. Colonial stellte den Betrieb der Pipeline innerhalb von einer Stunde nach der Verschlüsselung ein. Sechs Tage in Folge wurde kein Kraftstoff an die Ostküste gepumpt.

Colonial Pipeline Fakten und Zahlen

- Colonial Pipeline ist für 45 % der gesamten Kraftstofflieferungen an die Ostküste der USA verantwortlich.
- Die Pipeline hat eine Länge von fast 47.000 km.
- Das Lösegeld betrug 75 Bitcoin (ca. 4,4 Millionen USD).
- 87 % der Tankstellen in Washington D.C. hatten keinen Kraftstoff mehr.

Um die Tragweite dieser Entscheidung zu verdeutlichen: Colonial Pipeline ist für 45 % der Kraftstofflieferungen an die Ostküste verantwortlich. Von dem Lieferstopp waren nicht nur Autofahrer betroffen, sondern es gab auch Engpässe bei Erdgas und Treibstoffen für Flugzeuge.

Die allgemeine Öffentlichkeit reagierte größtenteils mit Panikkäufen. Als den Tankstellen langsam der Kraftstoff ausging, fingen die Verbraucher an, Vorräte zu horten, was die Situation noch verschlimmerte. Es gab auch einige Verbraucher, die alle möglichen Behälter mit Benzin füllten. Die Regierung gab eine Mitteilung heraus, in der sie die Bevölkerung davor warnte, Benzin in Plastiktüten abzufüllen.

Auch nachdem am folgenden Mittwoch der normale Betrieb wiederaufgenommen wurde, waren mehr als 10.000 Tankstellen an der Ostküste ohne Kraftstoff.

Auf die Biden-Regierung wurde verstärkt politischer Druck ausgeübt, Maßnahmen gegen den Versorgungsengpass zu ergreifen. Wenn die Situation länger angedauert hätte (Schätzungen gehen von weiteren drei bis vier Tagen aus), hätte dies weitreichende wirtschaftliche Folgen gehabt. Der Engpass hätte zu starken Beeinträchtigungen des Personentransports geführt und die Berufstätigen wären nicht mehr zu ihren Arbeitsplätzen gekommen.

Man machte sich ernsthafte Sorgen um die langfristigen Auswirkungen.

Was wissen wir über die Angreifer?

Dazu gibt es ein paar interessante Punkte.

Der Angriff sorgte sofort für viel Gesprächsstoff in den Untergrundforen und im Dark Web. Es gab Kommentare wie: „Das war bestimmt ein Fehler."

Mehrere Ransomware-Gruppen veröffentlichten Mitteilungen, in denen sie eine Beteiligung an dem Angriff auf Colonial Pipeline abstritten. Einige Gruppen gaben sogar formelle Richtlinien mit folgendem Inhalt heraus: „Diese Gruppe verübt keine Angriffe auf kritische Infrastrukturen oder Krankenhäuser."

In einigen Untergrundforen wurden sogar Regeln aufgestellt, welche die Werbung für Ransomware-Services untersagten. Auf diese Weise wollten sie sich der Aufmerksamkeit der Strafverfolgungsbehörden entziehen und vermeiden, mit Ransomware-Angriffen in Verbindung gebracht zu werden.

Dieser Trend hält seit vielen Monaten an. Den Angreifern war bewusst, dass dieser Vorfall zahlreiche Länder alarmiert hat und diese jetzt härter gegen Angreifer vorgehen würden.

Ich gehöre zur Ransomware Task Force (RTF). Diese wurde ins Leben gerufen, um umfassende Empfehlungen für internationale Regierungen und Privatunternehmen für den Umgang mit dieser Art von Bedrohung zu erstellen. Wenige Wochen vor dem Angriff auf Colonial haben wir unsere Erkenntnisse dazu geliefert. Unter anderem haben wir den Regierungen empfohlen, Ransomware als nationales Sicherheitsproblem zu behandeln.

In diesem Zusammenhang hat die Regierung Biden einige Verfügungen des Präsidenten schneller auf den Weg gebracht. Außerdem hat das U.S. Cyber Command seine Aktivitäten verstärkt und das FBI hat dafür gesorgt, dass einige Gelder, die mit Ransomware erpresst wurden, zurückbezahlt wurden.

80 % des in Bitcoin gezahlten Lösegelds wurde zurückbezahlt, allerdings hatte der Bitcoin zum Zeitpunkt der Rückzahlung erheblich an Wert verloren. Der Gegenwert betrug lediglich 2,2 Millionen USD.

Unmittelbar nach dem Angriff wurden Sie in einem Artikel folgendermaßen zitiert: „Es ist höchste Zeit, mehr gegen Ransomware zu tun als nur zu hoffen und zu beten." Warum haben Sie das gesagt?

Bis zu diesem Zeitpunkt haben sich die Regierungen hauptsächlich darauf konzentriert, Informationen weiterzugeben bzw. entsprechende Mitteilungen zu veröffentlichen. Sie verließen sich auf traditionelle Strafverfolgungsmethoden, um gegen Ransomware-Gruppen vorzugehen.

Leider war ihnen lange Zeit nicht bewusst, dass dieser Ansatz nicht zielführend ist. Die Anzahl der Festnahmen war sehr niedrig im Vergleich zu den katastrophalen Auswirkungen von Ransomware-Angriffen.

„Die Bedrohung durch Ransomware ist bei bestimmten Akteuren nach wie vor auf einem kritischen Niveau. Deshalb muss ihr der Status einer nationalen Sicherheitsbedrohung zugewiesen werden."

Das bedeutet, dass die Regierungen vollständig involviert werden müssen, um entsprechend zu reagieren. Das US Außenministerium, Finanzministerium, Cyber Command, Justizministerium und die entsprechenden Ministerien auf der ganzen Welt müssen aktiv eingreifen, da es sich um ein globales Problem handelt.

Die Veröffentlichung von Bulletins und Mitteilungen und die vereinzelte Verfolgung durch Strafbehörden, die oft irgendwo in Osteuropa im Sande verläuft, reicht nicht mehr aus.

Im Juli gab es einen weiteren Ransomware-Angriff auf eine Lieferkette, der von der REvil-Gruppe auf Kaseya verübt wurde. Welche Prognose können Sie, ausgehend von den diesjährigen Angriffen, zu der Natur von Ransomware- und Lieferkettenangriffen für das Jahr 2022 abgeben?

Die Reichweite, die ein Ransomware-Angriff auf Lieferketten haben könnte, hat schon immer große Sorgen hervorgerufen. 2017 gab es mit NotPetya schon einmal einen Ransomware-ähnlichen Vorfall, der auf eine Lieferkette abzielte. Es entstand ein weltweiter Schaden von über 10 Milliarden USD. Hierbei handelte es sich aber nicht um Ransomware, sondern um einen rein destruktiven Angriff, der von einem Nationalstaat unterstützt wurde. Der Angriff sollte nur wie ein Ransomware-Angriff aussehen.

„Aktuell sind Angriffe auf Lieferketten das größte Sicherheitsproblem. Ich kann mir nichts Beunruhigenderes vorstellen."

Das Unternehmen Kaseya stellt mittelständischen Unternehmen Services bereit. Hierzu haben sie administrativen Zugriff auf deren Netzwerke und Systeme. Das ist ein gefundenes Fressen für Angreifer. Das war wirklich eine ganz neue Art von Bedrohung.

Ich möchte nicht damit sagen, dass es sich um eine gängige Bedrohung handelt. Das Vorgehen ist sehr komplex, denn durch den simultanen Angriff auf mehrere Unternehmen, müssen die Angreifer verschiedene Entschlüsselungscodes für jede dieser Umgebungen bereitstellen. Wenn ein Unternehmen das Lösegeld zahlt und den Code erhält, müssen sie sicherstellen, dass nicht alles entschlüsselt wird.

Das ist meiner Meinung nach einer der Gründe, warum wir nicht mehr Angriffe dieser Art sehen. Außerdem verdienen Cyberkriminelle genügend Geld mit ihrer aktuellen Methode, nämlich Unternehmen einzeln zu erpressen.

Welchen Rat haben Sie für Personen, die für die Abwehr von Ransomware-Angriffen zuständig sind?

Früher haben wir z. B. Patches oder die Implementierung der Zweitfaktor-Authentifizierung empfohlen. Diese Maßnahmen sind war immer noch wichtig, aber am allerwichtigsten ist es, auf der Hut zu sein.

Gemeinsam mit unserem Cisco Talos Incident Response Team haben wir beobachtet, wie Angreifer Systeme mit Ransomware infiltrieren. An ihren Methoden hat sich nicht viel geändert. Selten gibt es einen völlig neuen Ransomware-Vorfall.

„Wenn Sie die Bedrohungslandschaft genau beobachten und Zeit und Geld in die Blockierung von Ransomware-Angreifern investieren, indem Sie beispielsweise gestohlene Anmeldeinformationen und spezielle Schwachstellen vermeiden, tun Sie schon viel, um den Angreifern einen Schritt voraus zu sein.“

Meistens ist ihnen das konkrete Ziel egal. Wichtig ist ihnen nur, Geld damit zu machen. Wenn Sie dafür sorgen, dass Ihr Unternehmen schwer angreifbar ist, stehen die Chancen gut, dass die Angreifer aufgeben und sich nach einer leichteren Beute umsehen.

Weitere Ressourcen:

Weitere Informationen zu neuen wichtigen Sicherheitsfunktionen für die Infrastruktur finden Sie im Artikel von Talos zum Angriff auf Colonial Pipeline.

Security Debt:

eine beliebte, neue Angriffsmöglichkeit

mit Dave Lewis
Advisory CISO, Cisco Secure

Was versteht man unter dem Begriff „Security Debt“ und warum wird es zunehmend zu einem Problem?

Den Begriff „Security Debt“ (Sicherheitsschulden) habe ich das erste Mal vor 20 Jahren verwendet, als ich für verschiedene Energieunternehmen tätig war. In vielen dieser Umgebungen wurden Systeme genutzt, die längst an Wert verloren haben, oder nicht ordnungsgemäß gewartet wurden. Infolgedessen gab es viele Angriffsziele.

Ich würde das Problem als technisches Defizit bezeichnen, das sich als Sicherheitsproblem manifestiert hat, entweder aufgrund von zeitlichen Faktoren, aufgrund von Nachlässigkeit oder einer Interaktion mit einem anderen System, das der Umgebung hinzugefügt wurde.

Gibt es ein Beispiel aus Ihrem beruflichen Umfeld, das die Security Debt näher beschreiben?

Ich kann Ihnen viele verschiedene Beispiele nennen. Nehmen wir ein ganz einfaches Beispiel. Ich arbeitete für ein Technologieunternehmen (nein, es war nicht Cisco). In der ersten Woche prüften wir alle Benutzernamen und Kennwörter im Unternehmen.

Es stellte sich heraus, das 10 Konten den „Super User“-Status hatten, obwohl die Benutzer längst nicht mehr für das Unternehmen arbeiteten. Die meisten hatten das Unternehmen innerhalb der letzten fünf Jahre verlassen. Eine Person war leider verstorben. Die Konten wurden jedoch während der letzten zwei Jahre benutzt.

Zum Glück wurden sie nicht für böswillige Aktivitäten verwendet. Auf Glück alleine sollte man sich aber bei einem Sicherheitsprogramm nie verlassen. Einblicke in die Aktivitäten in der Umgebung sind essenziell.

Wie manifestieren sich die Security Debt?

- Risiken werden in Kauf genommen, um sicherzustellen, dass Termine eingehalten werden.
- Der Kampf ums Budget steht dabei immer im Vordergrund.
- Patches werden nicht angewendet, da sich Systeme hinter einer Firewall befinden.

Wie könnte ein Angreifer die Security Debt in einem Unternehmen ausnutzen?

In vielen Unternehmen haben Angreifer ein leichtes Spiel. Beispielweise gibt es Schwachstellen, für die keine Patches installiert werden, da die Unternehmen nicht über die erforderlichen Kompetenzen verfügen oder keinen vertrauenswürdigen Dienstleister an ihrer Seite haben.

Manche Dinge werden auch einfach beiseite geschoben. Projekte werden implementiert, die nicht bis zum Ende durchdacht sind und denen ein Abschlusskonzept fehlt. Folglich werden einige dieser Projekte nach ihrer Laufzeit ohne Konzept weitergeführt, sodass leider Sicherheitsschwachstellen in der Umgebung entstehen.

Daraus ergeben sich unterschiedliche Angriffspunkte. Angreifer können Shodan oder Scanvorgänge nutzen. Oder sie zapfen einfach Open-Source-Quellen an, wie z. B. LinkedIn. Sie klicken sich dann durch verschiedene Lebensläufe und prüfen, ob jemand beispielsweise mit einem bestimmten Produkt gearbeitet hat.

Sie können dann eine Feinsuche nach Produkten durchführen, die möglicherweise in dieser Umgebung verwendet wurden, und diese dann mit den Schwachstellen vergleichen, die entweder veröffentlicht wurden oder die sie im Dark Web finden.

Was würden Sie Unternehmen mit Security Debt raten? Wie sollen sie damit umgehen?

Der Ansatz ist dreiteilig. Zuerst müssen Sie Ihre Hausaufgaben machen und ermitteln, welche Ressourcen und welche Benutzer sich in Ihrer Umgebung befinden und welche Anwendungen und Hardware diese verwenden. Sorgen Sie dafür, dass diese Bestände allgemein verfügbar sind.

Zweitens müssen Sie über ein Risikoregister verfügen, um die identifizierten Probleme nachzuverfolgen. Das Register dient aber nicht nur der Nachverfolgung. Sie können es bei Bedarf auch an Auditoren weitergeben. Die Auditoren können die identifizierten Probleme und die Roadmap für die Lösung solcher Probleme Ihrem Risikoregister entnehmen.

Als Drittes müssen Sie wiederholbare Prozesse definieren. Das ist die wichtigste Aufgabe. Wenn in einigen der Unternehmen, für die ich in der Vergangenheit gearbeitet habe, ein Problem auftrat, waren alle in heller Aufregung und versuchten fieberhaft herauszufinden, wer was tun muss.

„Stellen Sie sicher, dass es einen Prozess gibt, bei dem die zuständigen Personen identifiziert werden. So wissen Sie, wen Sie anrufen müssen, wenn etwas schief geht, und wer sich um welche Aufgaben kümmert."

Wichtig ist, dass Sie die Zuständigkeiten nicht bestimmten Personen zuordnen. Ordnen Sie sie einer bestimmten Rolle zu, damit das Problem trotz wechselnder Zuständigkeiten gelöst werden kann. Wenn etwas nicht so läuft wie geplant, sollte es einen Weg zur Lösung des Problems geben. Dafür müssen Rollen definiert werden.

Wie wirken sich die Security Debt auf andere Risikofaktoren aus?

Die Security Debt haben Auswirkungen auf Ihre Lieferkette, nicht nur im physischen Sinne, sondern auch in Bezug auf die Software.

„Wenn Ihre Anwendungen von Dritten erstellt werden, müssen Sie sicherstellen, dass sie einem definierten, wiederholbaren Prozess folgen, aus dem sich keine Schwachstellen in Ihrer Umgebung ergeben."

Ich habe das in der Vergangenheit in einigen Unternehmen erlebt. Es entstanden Sicherheitslücken im System, nicht weil jemand böswillige Absichten hatte, sondern weil niemand die Bibliotheken geprüft hat.

In Bezug auf die Umgebung würde ich immer einen analytischen Ansatz empfehlen. Fragen Sie sich, ob Sie die Systeme wirklich benötigen oder ob Sie beispielsweise bestimmte Hardware durch umfassende Upgrades ersetzen können. Außerdem können Sie mit einer Modernisierung der Technologie, welche die Latenz Ihrer Geräte klar verbessert, viele Sicherheitsprobleme vermeiden, die vielleicht schon vorher da waren.

Stellen Sie außerdem sicher, dass Sie einen Ansatz wählen, der die Sicherheit demokratisiert. Viele Unternehmen weltweit setzen heute auf hybride Arbeit und das wird in absehbarer Zukunft auch so bleiben.

Stellen Sie sicher, dass Sie Endnutzer unterstützen, damit sie sicher arbeiten können. Von MitarbeiterInnen sollte nicht erwartet werden, dass sie mit Tools arbeiten, die von Engineers für Engineers entwickelt wurden.

Weitere Ressourcen:

Weitere Informationen zum Umgang mit Security Debt, finden Sie im neuesten Duo Trusted Access-Bericht.

In der Security Outcomes-Studie, Teil 2 finden Sie stichhaltige Daten dazu, wie Unternehmen mit diesem Problem umgegangen sind.

Die wichtigsten Schwachstellen (an die sie vielleicht gar nicht denken)

mit Jerry Gamblin,
Director of Security Research,
Kenna Security (seit Kurzem Teil von Cisco)

Können Sie etwas darüber erzählen, wie Sie und Ihr Team gegen Schwachstellen vorgehen?

Wir bei Kenna überwachen alle veröffentlichten Schwachstellen genau und ordnen ihnen einen Risikowert zu, damit unsere Kunden wissen, auf was sie sich zuerst konzentrieren müssen.

Um Ihnen einen Überblick über die Bedrohungslage und den Anstieg der Sicherheitslücken zu geben: Dieses Jahr hatten wir es mit mehr als 20.000 neuen CVEs (Common Vulnerabilities and Exposures [Bekannte Schwachstellen und Risiken]) zu tun. Dies entspricht 55 CVEs pro Tag. Die Personaldecke der meisten Sicherheitsteams ist zu dünn für die Auswertung von 55 CVEs pro Tag oder mehr, um festzustellen, welche Schwachstellen ein Risiko für ihre Umgebung darstellen und welche nicht.

Gängige Schwachstellen-Frameworks erfordern häufig das Patching von Schwachstellen mit einem CVSS-Wert (Common Vulnerability Scoring System) von über 7,0. Das Problem dabei ist, dass wir es mit einem durchschnittlichen CVSS-Wert von 7,1 zu tun haben. Das bedeutet, dass für mindestens die Hälfte aller CVEs Patches installiert werden müssen.

Wir wissen, dass diese Problematik zunimmt (wir sagen nicht, dass sich die Lage verschlimmert, da die große Mehrheit der CVEs valide Schwachstellen sind). Zum Teil liegt das an der höheren Anzahl von Berichten und der verbesserten Transparenz. GitHub ist jetzt eine CNA (CVE Numbering Authority). Sie haben letztes Jahr die meisten CVEs für Open-Source-Projekte gemeldet.

Bestimmte Sicherheitslücken aus 2021 sind allgemein bekannt (z. B. Log4j und die Sicherheitslücken in Microsoft Exchange). Dennoch ist eine erhebliche Anzahl von kritischen Schwachstellen weniger bekannt. Sie bleiben oft unentdeckt.

Es gibt eine hohe Anzahl von Schwachstellen, die sich auf Open-Source-Projekte wie Chrome und Edge auswirken, und Sicherheitslücken in Windows wie z. B. die PrintNightmare-CVEs in diesem Sommer.

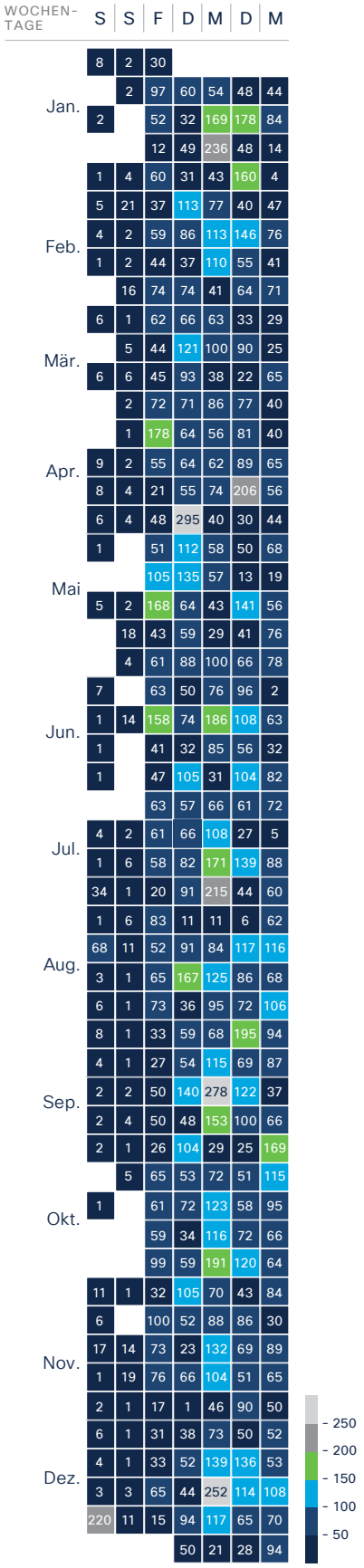
Zusammenfassung: CVEs im Jahr 2021

- Gesamtanzahl der CVEs: 20.129
- Durchschnittliche Anzahl der CVEs pro Tag: 55,3
- Durchschnittlicher CVSS-Wert: 7,1

Zusammenfassung: CVEs im Januar 2022

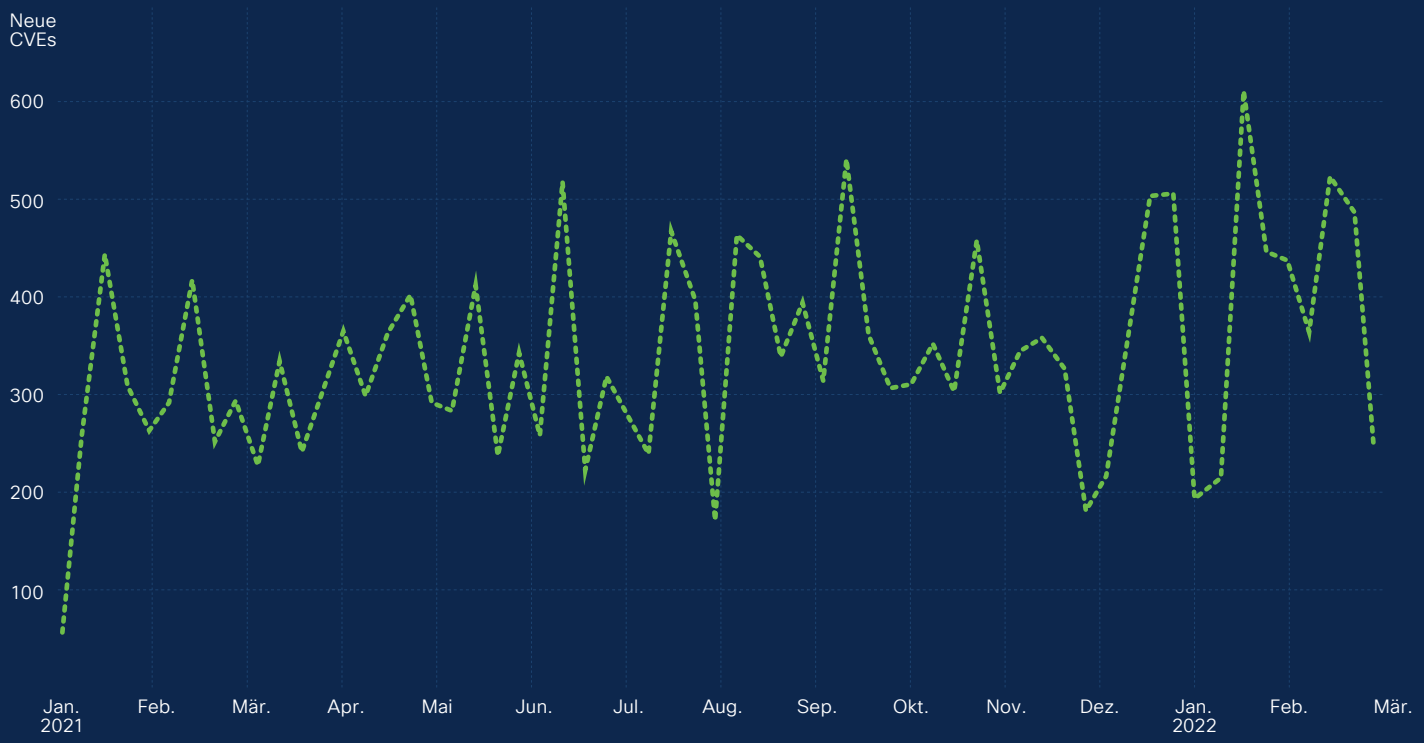
- Gesamtanzahl der CVEs: 2.020
- Durchschnittliche Anzahl der CVEs pro Tag: 65,16
- Durchschnittlicher CVSS-Wert: 6,86
- Anstieg im Januar 2021 (1.523): 32 % oder +497

CVEs pro Tag im Jahr 2021



Quelle: Kenna Security

Anzahl der CVEs pro Woche im Jahr 2021:



Quelle: Kenna Security

Häufig wird in den Medien über die Offenlegung von Sicherheitslücken nicht berichtet. Können Sie uns erläutern, warum man ihnen mehr Beachtung schenken sollte?

Das Management von Schwachstellen ist für die Verantwortlichen schwierig, denn oft mangelt es der Unternehmensführung am erforderlichen Interesse und es fehlen organisatorische Ressourcen. Dabei stellen die CVEs, die es nicht in die Schlagzeilen schaffen, oft das größte Risiko für Unternehmen dar.

Unter den mehr als 20.000 CVEs gibt es einige, denen die Medien starke Aufmerksamkeit schenken. Wahrscheinlicher ist es jedoch, dass Ihr Unternehmen mit schwerwiegenden CVEs konfrontiert ist, über die nicht in den Medien berichtet wurde.

Das Schwachstellenmanagement ist definitiv eine heikle Sache. Die Neuigkeiten kommen plötzlich, der Druck durch die Beteiligten steigt und Ihre Planung für die ganze Woche gerät durcheinander, wenn die Ressourcen, denen aber entsprechende Informationen fehlen, der Bedrohung oberste Priorität einräumen. Zu diesem Zeitpunkt kann eine risikobasierte Priorisierung (und eine Liste der Abhilfemaßnahmen) Sie dabei unterstützen, den Überblick über die wirklich wichtigen Dinge zu behalten.

Die Cybersecurity and Infrastructure Security Agency (CISA) zählt zu den einflussreichen Institutionen, die Unternehmen dazu auffordert, ihren Ansatz für die Beseitigung von Schwachstellen weiterzuentwickeln. Die CISA hat folgende verbindliche Richtlinie (22-01) in ihrem Bulletin im November 2021 veröffentlicht:

„Angreifer verlassen sich nicht auf rein kritische Schwachstellen, um ihre Ziele zu erreichen. Zu einigen der meist verbreiteten Angriffe mit verheerenden Folgen zählen mehrere Schwachstellen, deren Risiko als hoch, mittel oder sogar niedrig eingestuft wurde. ... Bekannte ausgenutzte Sicherheitslücken sollten bei der Beseitigung höchste Priorität haben.“

- CISA, Binding Operational Directive 22-01

Mit welchen Sicherheitslücken war Ihr Team 2021 beschäftigt? Können Sie einige der wichtigsten Bedrohungen nennen?

Wir haben viel Zeit für die Chrome V8-Engine aufgewendet. Dieses Jahr gab es bei Microsoft weitreichende Änderungen durch die Umstellung von Internet Explorer auf Microsoft Edge, einen Chromium-basierten Browser. Wir haben sichergestellt, dass unsere Kunden verstehen, was der Umstieg von einem Closed-Source- auf einen Open-Source-Browser bedeutet.

Auch Schwachstellen bei der Virtualisierung häufen sich. Diese Jahr zeigten sich mehr VMware ESXi-Schwachstellen mit hohem Risiko als in der Vergangenheit.

Außerdem gibt es neuerdings auch CEVs, die wir intern „Pile-on CEVs“ nennen (wir haben noch keinen wirklich passenden Begriff gefunden). Ein neues Basis-CVE wird veröffentlicht und innerhalb der nächsten paar Wochen gibt es eine Häufung von CVEs im Code. Beispiele für Pile-on CVEs sind Log4j und PrintNightmare, denen mehrere eindeutige CVEs zugeordnet sind.

In diesen Situationen empfiehlt es sich, den Fortschritt eines Anbieters bei der Beseitigung von RCE-Schwachstellen (Remotecodeausführung) zu kontrollieren, vor allem bei Schwachstellen mit großer Angriffsfläche (und möglichen weitreichenden Folgen).

Gibt es bestimmte Trends bei den Schwachstellen zu beobachten?

Das Problem mit den Sicherheitslücken wird aufgrund der Größe und des Ausmaßes dieses Jahr noch dringlicher. Mit dem Prophet-Framework von Facebook führen wir jede Nacht ein Modell aus. Wahrscheinlich wird es dieses Jahr mehr als 23.000 CVEs geben.

Außerdem sind nicht alle Bedrohungen durch den CVSS-Wert abgedeckt. Als wir unseren neuesten Priority to Prediction-Bericht veröffentlichten, machten wir Schlagzeilen, denn wir haben geschrieben, dass Twitter ein besserer Indikator für Sicherheitslücken ist.

In unserem Bericht steht auch, dass die Priorisierung von Schwachstellen mit einem Exploit-Code, der öffentlich verfügbar ist, 11-mal effizienter ist als CVSS, wenn es um die Minimierung von Schwachstellen geht.

Ein erwähnenswerter Trend ist auf alle Fälle, dass es sehr hilfreich ist bzw. das Risiko deutlich sinkt, wenn bekannte Sicherheitslücken priorisiert werden und Vorhersagen darüber getroffen werden, welche Ziele die Angreifer als nächstes im Visier haben könnten.

„Unternehmen müssen auf ein risikobasiertes Managementsystem für Schwachstellen umstellen, bei dem mögliche Ausführungen von Remote-Code analysiert werden oder geprüft wird, ob ein Exploit-Code vorhanden ist. Dieses Vorgehen ist unverzichtbar, um die wichtigsten Schwachstellen zu identifizieren, die möglicherweise Auswirkungen auf Ihr Unternehmen haben.“

Welchen Rat geben Sie den Sicherheitsverantwortlichen, um Schwachstellen leicht zu identifizieren und den Angreifern einen Schritt voraus zu sein?

Sie sollten niemals die automatische Ausführung von Patches deaktivieren. Ich kenne das Problem, da ich ganz am Anfang meiner Karriere in IT-Abteilungen im öffentlichen und privaten Sektor tätig war. Jeder möchte die automatische Ausführung von Patches deaktivieren, da man sich nicht sicher ist, ob die Patches laufende Prozesse beeinträchtigen. Wenn sie aktiviert ist, sind Sie aber besser geschützt.

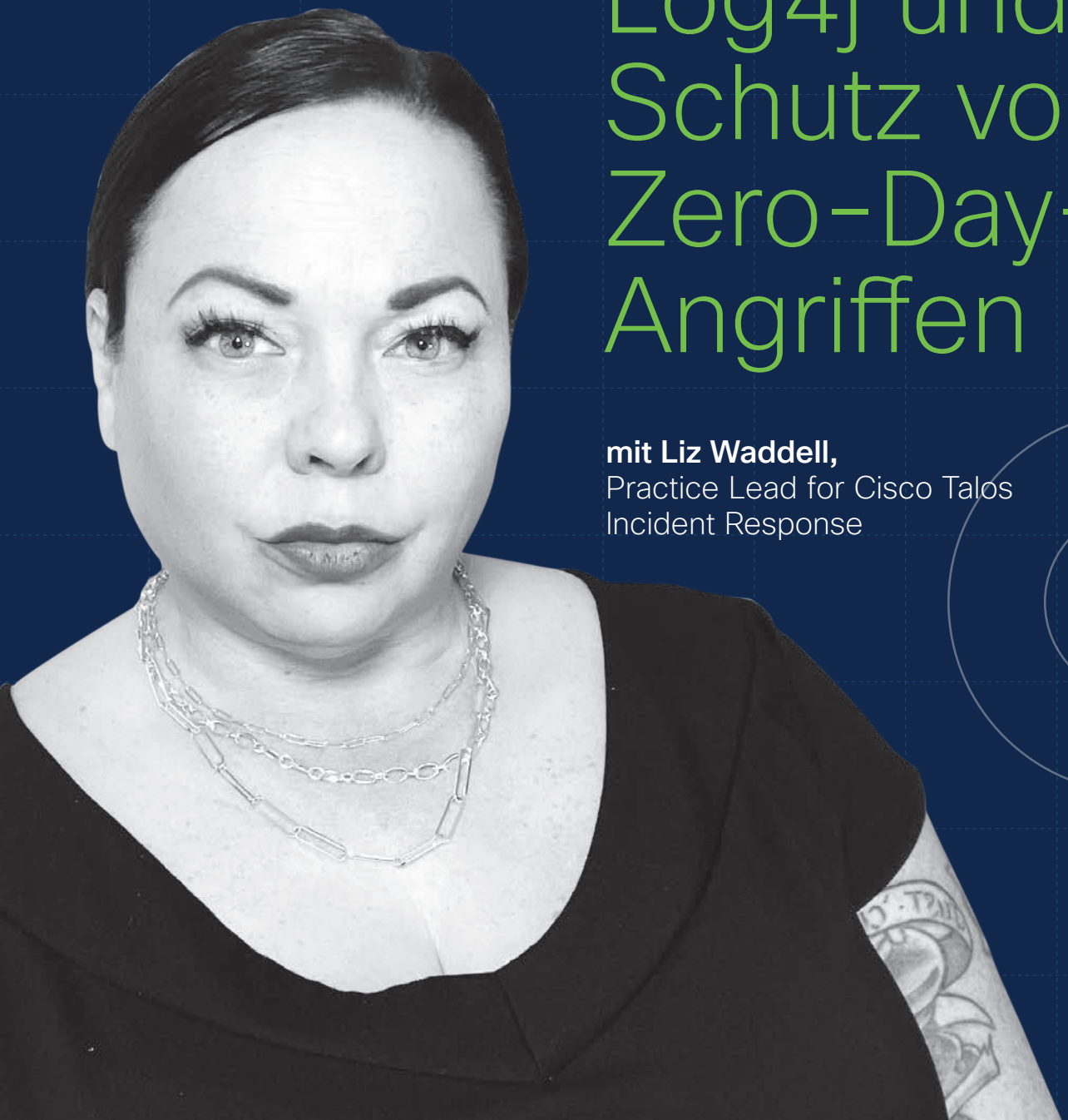
Verwenden Sie die automatische Ausführung für die Routinewartung, damit Ihnen mehr Zeit für die eingehende Untersuchung von Schwachstellen bleibt, für die Sie aufwändige Patches und Tests durchführen müssen.

Weitere Ressourcen:

Um bei Schwachstellen, die es vielleicht nicht in die Schlagzeilen schaffen, auf dem neuesten Stand zu bleiben, lesen Sie den Kenna Security-Blog. Hier finden Sie weitere Informationen.

Jerry Gamblin verfolgt ein persönliches Projekt, bei dem er täglich einen Abgleich auf CVE.ICU durchführt und Open-Source-Daten auf der Basis des CVE-Datensatzes analysiert.

Log4j und Schutz vor Zero-Day-Angriffen



mit Liz Waddell,
Practice Lead for Cisco Talos Incident Response

Das CTIR-Team (Cisco Talos Incident Response) war Ende 2021 wesentlich daran beteiligt, Kunden bei der Beseitigung von Log4j-Schwachstellen zu unterstützen. Betrachten wir zunächst, wie sich die Ereignisse im Zusammenhang mit Log4j entwickelt haben.

Am 24. November 2021 hat das Cloud-Security-Team von Alibaba eine Warnmeldung bezüglich einer RCE-Schwachstelle in Log4j2, einer Java-Protokollierungsbibliothek, an Apache herausgegeben. Das ist ein wichtiges Detail, auf das wir später noch zurückkommen werden.

Es gibt mindestens 1.800 eindeutige Code-Bibliotheken und Projekte, die in Cloud-Services und Endpunkte integriert sind, die über diese bestimmte Protokollierungsbibliothek verfügen. Als Log4j identifiziert wurde, war die Bedrohung durch diese Schwachstelle enorm ... doch erst, nachdem die Medien darüber berichtet hatten.

Am 30. November teilte ein anonymer Sicherheitsforscher mit dem Twitter-Handle @p0rz9 einen GitHub-Link zu einem Proof of Concept. Am Tag darauf wurden die ersten Berichte veröffentlicht, dass die Schwachstelle in Unternehmen auf der ganzen Welt ausgenutzt wurde.

Am 9. Dezember, als das Interesse der Öffentlichkeit immer größer wurde, wurde der erste Patch von Apache veröffentlicht. Danach konnten wir bei Cisco Talos beobachten, dass sich die Exploits häuften und seltsame Dinge passierten. Minecraft-User warnten vor der Ausführung von schädlichem Code auf Clients und Servern, auf denen die Java-Version des beliebten Spiels ausgeführt wird.

Am 10. Dezember haben wir die erste Ausgabe des Talos Blogs veröffentlicht. Dieser wird laufend aktualisiert. Es gab einen richtigen Hype um Sicherheitslücken. Es war unglaublich hektisch. Eine Nachricht nach der anderen prasselte auf uns ein.

Sicherheitsverantwortliche beschäftigten sich mit der Erkennung von Schwachstellen, Unternehmen wollten herausfinden, ob sie angreifbar waren, und ForscherInnen versuchten die Anzahl der Betroffenen zu ermitteln. Sie prüften alles, was sie finden konnten. Deshalb ist es so wichtig, eine zuverlässige Quelle zu haben, auf die sich Sicherheitsverantwortliche verlassen konnten. Jemand muss Ordnung in die Informationsflut bringen.

Log4j im Zeitverlauf

TALOS

24. November 2021
Das Cloud-Security Team von Alibaba meldet die Log4j2-RCE-Sicherheitslücke von Apache.

30. November 2021
Die Schwachstelle durch Github-Pull-Anforderung wird bekannt.

1. Dezember 2021
Erster Angriff wird gemeldet.

2. Dezember 2021
Erster von Cisco entdeckter Angriff.

9. Dezember 2021
Apache veröffentlicht den ersten Patch.

10. Dezember 2021
Liveschaltung des Cisco Talos Blog und erste Berichterstattung.
Großflächige Angriffe mit Bereitstellung von Minern werden entdeckt.

11. Dezember 2021
Aktivitäten im Zusammenhang mit dem Mirai-Botnet werden beobachtet und weitere Informationen veröffentlicht.

13. Dezember 2021
Cisco Talos findet Hinweise darauf, dass E-Mails als Angriffsvektor dienen. Verschleierte Identitäten und Protokolle werden missbräuchlich eingesetzt. Aktualisierung des Blogs und weitere Meldungen als Reaktion darauf.
Cisco veröffentlicht einen Warnhinweis zu Log4j2.

14. Dezember 2021
Apache bring weiteren Patch heraus (Patch 2.16.0) und empfiehlt allen Benutzern das Upgrade.
Cisco Talos entdeckt, dass Log4j2 in vielen Metadaten-Quellen eingebettet ist, einschließlich Bildern und Word-Dokumenten.
Aktualisierung des Blogs und weitere Meldungen.

18. Dezember 2021
Apache veröffentlicht zusätzlichen Patch (Patch 2.17.0) um neue Denial-of-Service-Sicherheitslücke zu schließen.

„Es gibt eine Sache, die wir aus der Vergangenheit gelernt haben: Es muss mehrere Patches für eine Anwendung mit Sicherheitslücken geben."

Log4j folgte diesem Muster und bis zum 18. Dezember wurden drei Patches veröffentlicht. Nach dem verheerenden Angriff auf SolarWinds im Jahr zuvor, gingen wir davon aus, dass es Weihnachten 2021 ähnliche Vorfälle geben würde. Die Anzahl der Kunden, die uns in der Weihnachtszeit wegen Log4j kontaktierten, war jedoch überschaubar, was jedoch nicht heißt, dass es überhaupt keine Vorfälle gab. Talos lagen entsprechende Informationen vor, dass Schwachstellen aktiv ausgenutzt wurden. Dazu gehörten Aktivitäten von Minern und anderen Angreifern mit finanziellen Motiven. Uns lagen Berichte zu Angriffen vor, die von Nationalstaaten ausgingen, und wir beobachteten großflächige Aktivitäten in unseren Honeypots und Telemetriequellen.

Am 5. Januar nahmen die Berichte über die Ausnutzung von Schwachstellen wieder zu, als der NHS (National Health Service) in Großbritannien Log4Shell-Schwachstellen auf seinen VMware Horizon-Servern meldete.

Incident Response von Talos für Zero-Day-Angriffe

Für Unternehmen, die 2022 mit Log4j und möglichen Zero-Day-Angriffen konfrontiert sind, ist unser 7-Punkte-Aktionsplan möglicherweise sehr hilfreich.

1 Hintergrund/Überblick über Bedrohungen

Wie brauchen eine einzige zuverlässige Informationsquelle, auf die sich unsere Kunden bei der Planung ihrer Abwehrstrategie verlassen können.

Wir veröffentlichen den Talos Blog, der kontinuierlich aktualisiert wird.

2 Umfang der Bedrohung

Wir möchten nicht nur wissen, welche Schwachstellen es gibt, sondern auch, inwiefern diese ausgenutzt werden können. Müssen wir uns Sorgen über CVE machen? Was Log4j und die Schwachstellen in Microsoft Exchange anbelangt, lautet die Antwort definitiv „Ja“.

Können Angreifer die Kontrolle über ein System übernehmen? Was können sie anschließend tun? Können sie sich lateral im System bewegen, Daten stehlen oder Ransomware implementieren?

Diese Antworten sind hilfreich für weitere forensische Untersuchungen möglicher Schwachstellen.

3 Wie kann ich feststellen, ob mein System anfällig ist?

Diese Frage wird am häufigsten gestellt.

Bei Schwachstellen wie Log4j fragen wir Sie zunächst, ob Sie wissen, auf welchen Systemen Log4j ausgeführt wird.

Es gibt immer mehrere Stellen, an denen eine Anwendung angreifbar ist und über Log4j-Sicherheitslücken verfügt. Überall dort, wo Anwendungen benutzergesteuerte Daten über Log4j protokollieren, lauern Gefahren.

Bedrohungsvektoren umfassen die Protokollierung von benutzergesteuerten URIs, eingehende Benutzer-Agents, POST-Parameter und von Benutzern bereitgestellte Dateien. In vielen Fällen gibt es mehrere Indirektionsebenen zwischen der Erfassung eines vom Benutzer beeinflussten Wertes und seiner Verwendung durch das Log4j-Framework. Dadurch steigt die Komplexität bei der Risikobewertung eines bestimmten Einfallstors.

Außerdem sind mögliche Auswirkungen nicht auf Ihr System allein beschränkt. Anbieter und Partner können ebenfalls betroffen sein. Genau aus diesem Grund waren wir so beunruhigt, als wir von diesem Exploit erfahren haben.

4 Wie weiß ich, ob mein System angegriffen wurde?

Es gibt verschiedene Ressourcen, über die Sie feststellen können, ob eine Schwachstelle im Unternehmen ausgenutzt wurde, und unser Team hat eine Liste mit Punkten, die alle abgehakt werden.

Einige Punkte beziehen sich auf Log4j. Andere Punkte sind allgemeine Dinge, die Sie beachten sollten. Hier sind einige Beispiele:

- Prüfen Sie die Protokolle von Perimeter-Sicherheitsgeräten (z. B. Firewalls, IDS/IPS) auf IOCs (Indicators of Compromise).
- Prüfen Sie RMI- und LDAP-Protokolle und -Ports am Netzwerkperimeter. Verwenden Sie ggf. Sperrlistenausnahmen für bekannte, vertrauenswürdige Kommunikation, die diese Protokolle verwendet.
- Prüfen Sie die Ereignisprotokolle des Betriebssystems auf verdächtige oder böswillige HTTP-Anfragen.
- Prüfen Sie die Webserverprotokolle auf zugehörige IOCs.
- Wir können auch Skripte einbeziehen, die unsere AnalystInnen (bzw. Kunden) verwenden, um zu prüfen, ob sich die Anwendung auf einem System befindet (z. B. Log4j-Bibliotheken).

5 Was, wenn es eine Schwachstelle gibt, die nicht ausgenutzt wurde?

Wir identifizieren gemeinsam nutzbare Inhalte zur Bedrohungseindämmung auf der Basis von aktuellen Richtlinien. Manchmal geben wir den Unternehmen den einfachen Rat, Patches auf dem System zu installieren. Beispiel Log4j: Deaktivieren Sie die JNDI (Java Naming and Directory Interface), indem Sie den neuesten Patch installieren. Oder wir prüfen andere Maßnahmen zur Bedrohungseindämmung, wenn das Installieren von Patches keine Option ist.

6 Was, wenn es eine Schwachstelle gibt, die ausgenutzt wurde?

Das hängt von der jeweiligen Situation im Unternehmen ab, aber im Falle von Log4j waren die Anweisungen ganz klar: Führen Sie die Schritte 1 bis 5 aus und aktivieren Sie den Incident-Response-Plan Ihres Unternehmens. Und rufen Sie uns an.

7 Indicators of Compromise

Es ist auf alle Fälle empfehlenswert, eine Liste von IOCs zu verwenden und aktuell zu halten. Alle Informationen diesbezüglich, einschließlich IOCs, finden Sie im Talos Blog. Zu den IOC-Typen gehören im Allgemeinen IPs, Domains, Benutzer-Agents oder spezielle Web Shell SHA-256-Hashes wie im Fall von Log4j.

Können Sie etwas zur Log4j-Lage zum Zeitpunkt der Berichterstellung (Februar 2022) sagen?

Wir haben festgestellt, dass die Log4Shell-Schwachstellen im NHS-System ausgenutzt wurden, um Web Shells zu erstellen. Leider können Angreifer Web Shells für unzählige schädliche Aktivitäten nutzen – Malware, Ransomware, Rickrolling und den Diebstahl von Anmeldeinformationen oder Daten.

Letztendlich lässt sich sagen, dass Angreifer mit Netzwerkzugriff auf ein betroffenes VMware-Produkt diese Schwachstellen ausnutzen können, um das Zielsystem vollständig zu kontrollieren.

Huntress zufolge gab es im Januar circa 25.000 VMware Horizon-Server, auf die der Zugriff über das Internet möglich war. Darüber hinaus wurden nach Angaben von Huntress auf vielen dieser Server keine Patches installiert.

Was erschwerend hinzukommt ist, dass einige dieser ausführbaren Dateien vom AV- und EDR-Monitoring ausgeschlossen sind. Wir und einige andere Sicherheitsunternehmen haben festgestellt, dass dieses Versäumnis von einigen Angreifern aktiv ausgenutzt wird.

So sieht es momentan aus. Hauptsächlich zielen die Angriffe auf VMware Horizon-Server ab.

Dennoch wird das Umfeld und das Dark Web von uns immer noch sorgfältig geprüft, um sicherzustellen, dass wir so effektiv wie möglich auf Änderungen und weitere Angriffe reagieren können.

Diese Anwendung ist in viele Lösungen integriert. Informationen zu aktuellen Erkenntnissen finden Sie im dedizierten Talos Blog.

Wird Log4j auch in diesem Jahr nennenswerte Auswirkungen haben?

Log4j wird auch 2022 große Auswirkungen haben. Das war schon beim Angriff auf VMware Horizon offensichtlich. Wir müssen auf alle Fälle so proaktiv wie möglich vorgehen, um die potenziellen Zugriffspunkte für Angreifer zu bestimmen, die diese Schwachstelle für einen Angriff auf Ihre Umgebung ausnutzen wollen.

Unternehmen müssen ihr System unbedingt auf andere Hinweise zu Aktivitäten prüfen, die bei der ursprünglichen Suche nach Bedrohungen vielleicht übersehen wurden. Gibt es Anzeichen einer lateralen Bewegung? Gibt es Anzeichen für eine Kompromittierung der Umgebung?

Haben Sie weitere Ratschläge, was Sicherheitsverantwortliche gegen diese Schwachstelle oder mögliche Zero-Day-Angriffe tun können?

Denken Sie bei jedem Zero-Day-Notfall daran, dass Exploits im Zusammenhang mit Schwachstellen nach ihrer Entdeckung zunehmen. Dokumentieren Sie sämtliche Erkenntnisse und aktualisieren Sie kontinuierlich Ihr System.

Ich wünschte, ich könnte konkret sagen, wie viel Zeit Sie einsparen, wenn Sie Informationen ordnungsgemäß dokumentieren. Wie Sie bereits wissen, haben ich viel Erfahrung in Kundenumgebungen. Sie müssen mir einfach glauben, dass Sie so wirklich enorm viel Zeit einsparen.

Weitere Ressourcen:

Mehr Informationen zu den Incident Response-Trends 2021 erhalten Sie im Cisco Talos Blog.

Wenden Sie sich in einem Notfall telefonisch an das Cisco Talos Incident Response Team unter folgender Nummer: USA: 1-844-831-7715 | Europa: (+44) 808-234-6353

Aktuelle Entwick-lungen bei Emotet

mit Artsiom Holub,
Senior Security Analyst,
Cisco Umbrella

Können Sie etwas zum Verlauf von Emotet in der Bedrohungslandschaft erzählen? Wie kam es, dass sich Emotet zu einer weit verbreiteten Bedrohung entwickelt hat?

Emotet ist wohl ziemlich einmalig in der Bedrohungslandschaft. 2015 trat es erstmals in Erscheinung – als reiner Banking-Trojaner. Zu diesem Zeitpunkt waren einige Trojaner im Umlauf, doch Emotet war anders, denn dahinter steckte ein sehr starkes Entwicklerteam. Das heißt, dass Emotet ständig weiterentwickelt wurde.

2016 wurde Emotet als Loader neu konfiguriert. 2017 wurde es dann als Loader-as-a-Service-Modell angeboten. In diesem Jahr startete Emotet durch die Koordination mit Malware wie TrickBot und QakBot voll durch.

In den Jahren 2018 bis 2019 grassierte diese Malware und das Trio aus Emotet, TrickBot und der Ryuk-Ransomware wurde für mehrere schwerwiegende Angriffe benutzt.

Das IT-Netzwerk in Frankfurt, eines der größten Finanzzentren in Europa, wurde durch einen Cyberangriff mit Emotet lahmgelegt. Aufgrund eines Malware-Angriffs kamen die kritischen Systeme der Stadt Allentown, Pennsylvania (USA), zum Erliegen. Der Angriff weitete sich massiv aus und kostete die Stadt fast 1 Million USD. Und bei einem Angriff auf das größte Landgericht in Berlin, Deutschland, wurden große Mengen an vertraulichen Daten gestohlen.

Um Ihnen ein Gefühl für das Ausmaß von Emotet und der zugehörigen Malware zu vermitteln: Cisco Umbrella hat 2019 bis zu 4 Millionen Anfragen pro Monat blockiert.

2020 wurde im Rahmen einer gemeinsamen Aktion der gesamten Sicherheitsbranche versucht, Emotet auszuschalten. Diese Aktion war einigermaßen erfolgreich und folglich war Emotet phasenweise inaktiv.

Doch die böswilligen Angreifer haben das lukrative Geschäft nicht so einfach aufgegeben. Anscheinend wollten sie mit der Unterbrechung ihrer Aktivitäten einer Entdeckung entgehen. Der Plan sah aber auch vor, gestärkt zurückzukehren.

Ende 2020 war Emotet wieder da – mit einem überarbeiteten Code und neuen Methoden, um Unternehmen mit schädlichen Payloads im großen Umfang zu schaden. Emotet entwickelte sich zu einem der ersten großen Loader mit Zugriff auf Netzwerke im privaten und öffentlichen Sektor.

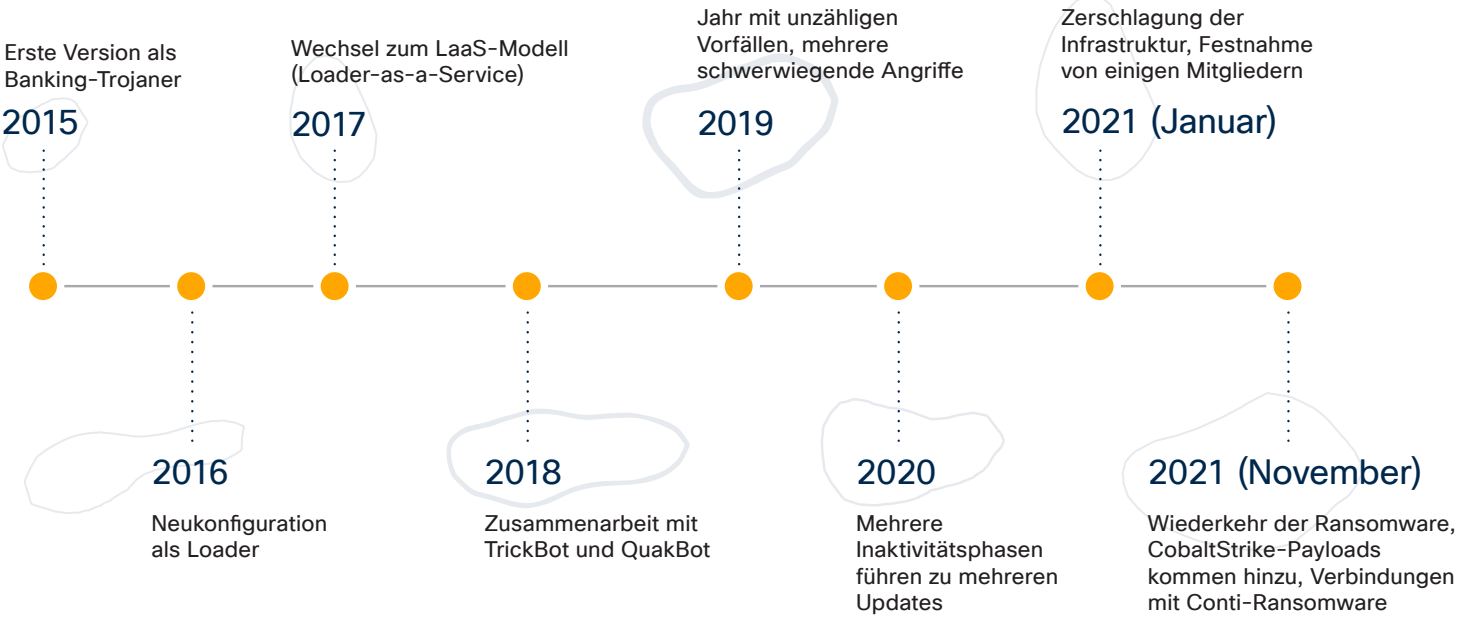
Was wurde 2021 gegen Emotet unternommen?

Im Januar hat man in Zusammenarbeit mit privaten und staatlichen Organisationen sowie im Rahmen einer Operation, die von Europol und Eurojust (European Union Agency for Criminal Justice Cooperation) geleitet wurde, die Aktivitäten von Emotet gestoppt. Ein großer Teil der zugehörigen Infrastruktur wurde zerstört.

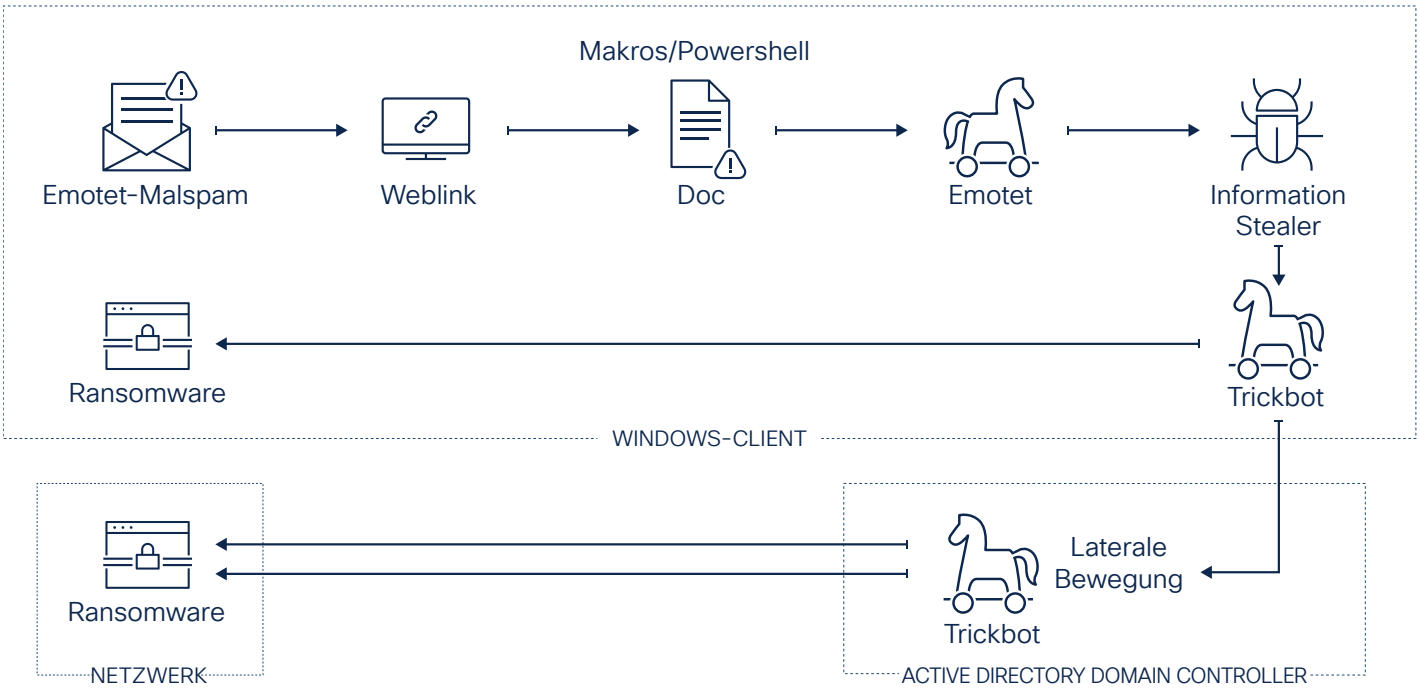
Im April hatte man Emotet von allen infizierten Geräten deinstalliert. Darüber hinaus gelang der Cyberpolizei in der Ukraine ein erfolgreicher Schlag gegen die Angreifer. Sie hatten mehrere Bandenmitglieder verhaftet, die an der Entwicklung von Emotet maßgeblich beteiligt waren.

Damals war die Hoffnung groß, dass Emotet für immer verschwunden bleibt. Doch leider war das nicht der Fall.

Entwicklung von Emotet



Emotet: Änderung der Kill Chain für Ransomware



Wie kam es, dass Emotet Ende 2021 zurückgekehrt ist?

Aufgrund der Natur der Aktivitäten und der Gewinne, die Cyberkriminelle mit dieser Malware einfahren konnten, erlebten wir die Rückkehr von Emotet. Emotet war wieder da – mit einer völlig neuen Infrastruktur, die sich bis heute kontinuierlich ausweitet.

Die Rückkehr von Emotet lässt auf einen Anstieg der Nachfrage nach solchen Operationen im Umfeld von Cyberkriminellen schließen. Es bedarf nur einiger gut organisierter krimineller Vereinigungen, um endlose Möglichkeiten für Emotet-Botnet-Entwickler zu schaffen.

Das Duo aus TrickBot und Emotet wurde von der Ryuk-Ransomware intensiv genutzt. Aktuell bieten sich Kriminellen durch Conti neue logische Möglichkeiten.

Conti organisiert gezielte Angriffe, um die Einnahmen zu maximieren. Wenn sich die Dinge in diese Richtung weiterentwickeln, d. h. TrickBot und Emotet zu einem exklusiven Medium für die Verteilung von Conti-Ransomware werden, werden sich diese Kampagnen höchstwahrscheinlich im kommenden Jahr noch ausweiten.

Könnten Sie das etwas näher ausführen? Können Sie auf der Basis der aktuellen Entwicklungen einschätzen, wie sich Emotet 2022 möglicherweise manifestieren wird?

„Es ist sehr gut möglich, dass sich Emotet 2022 zur größten Bedrohung entwickeln wird. Emotet ist ein leistungsstarker Loader, der wieder zum Leben erweckt wurde.“

Meine Einschätzung basiert auf dem Wissen, dass dieses Trio (Emotet, TrickBot und Ryuk) die gesamte Vorgehensweise erheblich geändert hat. Die Änderungen beschränken sich nicht nur auf diese Dreiergruppe, sondern gelten auch für alle anderen Ransomware-Betreiber. Das Dreiergespann wurde auch als Einstieg für Angriffe auf Lieferketten verwendet.

Die Bedrohung ist vielschichtig. Zunächst geht es darum, in Systeme einzudringen und sehr starke Profile der betroffenen Netzwerke zu erstellen. Als nächstes werden z. B. TrickBot und Cobalt Strike eingesetzt. Dies ist ein leistungsstarkes Tool für laterale Bewegungen, das die Kontrolle über das gesamte Netzwerk übernimmt.

Mit Conti als gut organisiertem Ransomware-Provider wird es 2022 wahrscheinlich groß angelegte Angriffe mit dieser bestimmten Kill Chain geben.

Welchen Rat haben Sie für Sicherheitsverantwortliche, damit diese ihre Unternehmen vor diesem Angriffstyp schützen können?

Es ist wie in allen Bereichen der Sicherheit: es gibt keine Universallösung, die Emotet stoppen wird. Setzen Sie auf einen mehrstufigen Ansatz, ermitteln Sie die schwächsten Glieder in Ihrem Netzwerk und führen Sie Sicherheitskontrollen für diese Schwachstellen durch.

„Als Analyst haben ich den Unternehmen immer geraten, sich auf ihre Abwehrstrategie zu konzentrieren, um laterale Bewegungen und Datenexfiltrationen in das Internet zu erkennen. Auf jeden Fall sollten Sie den ausgehenden Traffic auf Verbindungen zu Cyberkriminellen prüfen.“

Zu guter Letzt sollten Sie mithilfe aktueller Threat-Intelligence die Taktiken, Methoden und Verfahren (TTPs) von Angreifern ermitteln. Es mag sein, dass sich die Tools und Aktivitäten ändern, aber Cyberkriminelle setzen oft auf Verfahren, die sich bereits in der Vergangenheit bewährt haben.

Weitere Ressourcen:

Lesen Sie den Bericht von Cisco Umbrella: The modern cybersecurity landscape: Scaling for threats in motion.

Weitere Informationen zur Rückkehr von Emotet finden Sie im Cisco Talos Blog.

Die Zunahme von MacOS-Malware

mit Ashlee Benge,
Lead, Strategic Intelligence and Data Unification, Cisco Talos

Könnten Sie uns einige Hintergrundinformationen zu MacOS-Malware geben? Warum haben Sie sich gerade dieses Thema ausgesucht?

Das ist eines meiner persönlichen Interessensgebiete. Ich habe dieses Thema für diesen Bericht gewählt, weil wir meiner Meinung nach viel zu lange davon ausgegangen sind, dass MacOS unempfindlich gegen Malware ist. Diese Gerücht hält sich hartnäckig, seitdem es Mac gibt.

In der Sicherheitsforschung werden wir mit Informationen überflutet. Meine Aufgabe ist es, diese enormen Datenmengen zu durchforsten, um herauszufinden, ob sich das Verhalten von Angreifern geändert hat. Mit jeder Änderung beginnt die Jagd nach neuen Bedrohungen.

Und das war vor kurzem bei MacOS-Malware der Fall. MacOS wird immer attraktiver für Angreifer und 2021 haben wir einige neue MacOS-Malware-Typen entdeckt, die uns Sorgen bereiten.

Wir haben es verstärkt mit Malware zu tun, die entweder ausschließlich auf MacOS oder auf mehrere Betriebssysteme abzielt. Egal ob Linux, Windows oder MacOS: Angreifer können zur Kompromittierung all dieser Systeme die gleiche Malware benutzen.

Apple hat in den ersten zwei Monaten in 2022 zwei Fixes für Zero-Day-Sicherheitslücken auf iOS- und MacOS-Geräten herausgegeben. Durch diese Schwachstellen, die sich auf WebKit auswirken, erhöht sich für iOS- und MacOS-Nutzer das Risiko von Angriffen mit Remotecodeausführung.

Diese schwerwiegenden Sicherheitslücken können von Angreifern ausgenutzt werden, um ihre Präsenz in einem kompromittierten Netzwerk auszubauen. Alles hängt davon ab, was die Angreifer vorhaben, wenn sie erst einmal in das System eingedrungen sind.

Häufig erleben wir, dass sekundäre Malware herausgegeben und ausgeführt wird. Bei dieser Malware handelt es sich beispielsweise um Cryptochecker, Ransomware oder vielleicht Backdoors.

Backdoors können für den Diebstahl sensibler Daten benutzt werden, um Unternehmen zu erpressen oder anderweitig Schaden anzurichten. Angreifer können auch dafür sorgen, dass ein angegriffenes Gerät nicht mehr funktionsfähig ist, was zu Denial of Service und Betriebsunterbrechungen führt.

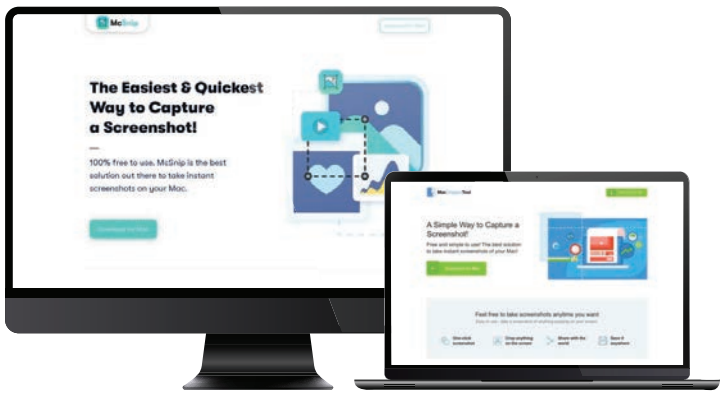
Können Sie uns ein Beispiel für eine auf MacOS ausgerichtete Malware geben, die Sie 2021 entdeckt haben?

Eine der interessantesten Entdeckungen im August 2021 war die Backdoor-Malware McSnip.

Unser Tag hat ganz normal begonnen – mit der Überwachung des Verhaltens von Angreifern und der Suche nach Änderungen, die uns bei der Identifizierung neuer Malware-Familien helfen könnten.

Wir entdeckten eine Änderung an einem vorhandenen Dropper-Verfahren. Dabei handelt es sich um Methoden einer bestimmten Gruppe von Malware-Angreifern, die versuchen, vor dem Angriff binäre Daten in das System einzuschleusen.

Wir konnten alle schadhafte Dateien, die wir dieser Kampagne zuordnen konnten, identifizieren und unschädlich machen. Dabei sind uns einige interessante Sachen aufgefallen.



Obwohl diese binären Daten in der Lage waren, sensible Daten zu exfiltrieren, wurden diese Funktionen nicht genutzt. Da schrillten bei uns alle Alarmglocken.

Wir stellten fest, dass im Fall von McSnip die schadhaften binären Dateien ein Screenshot-Tool imitierten, das direkt von einer Website heruntergeladen werden konnte anstatt über den legitimen App Store.

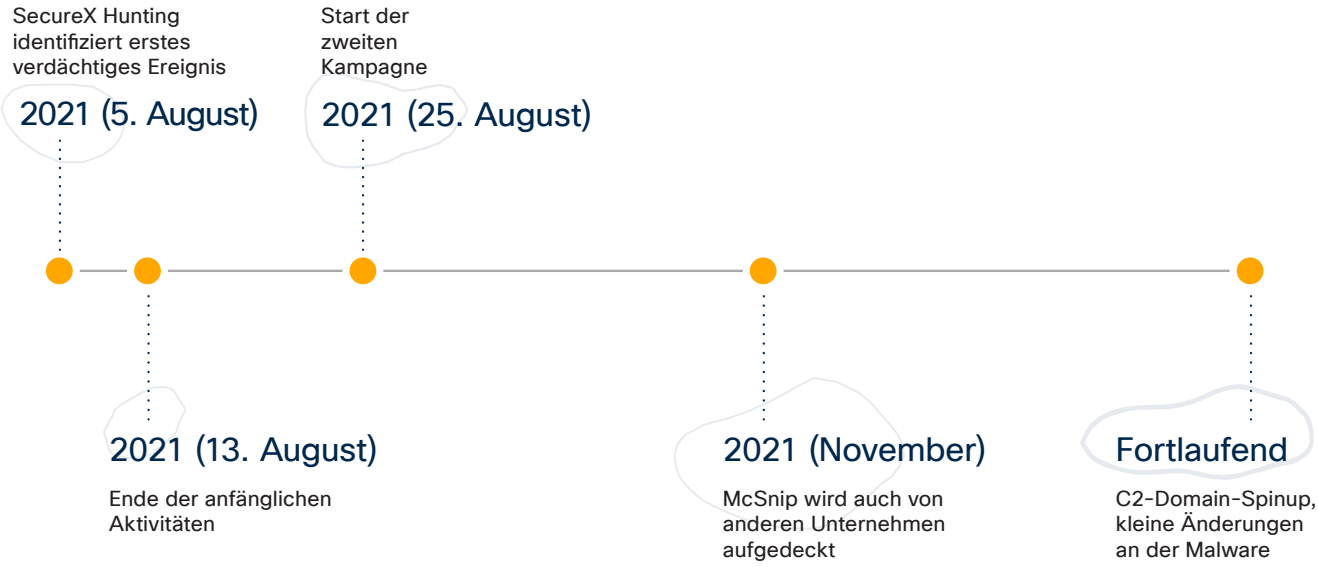
Wir entwickelten Hunts für diese Malware, um sicherzustellen, dass es keine aktiven Kampagnen gab. Bald danach ist die Anzahl der Versuche, Systeme mit der McSnip-Methode zu kompromittieren, zurückgegangen.

Ende November wurde McSnip auch von anderen Sicherheitsorganisationen aufgedeckt. Im selben Zeitraum wurde eine sekundäre Kampagne gestartet. Für die Malware vom August wurden kleine Updates durchgeführt, um diese neuen schadhaften Funktionen für die Datenexfiltration zu nutzen.

Die Testphase begann wohl im August. Die Angreifer, die hinter der Malware steckten, wollten testen, ob der Dropping-Mechanismus planmäßig funktioniert, und es gelang ihnen, binäre Dateien auf Zielgeräten abzulegen. Die eigentliche Kampagne wurde im November gestartet, als die Angreifer McSnip einsetzten, um Systeme aktiv zu kompromittieren.

McSnip wird immer noch genutzt, zumindest werden entsprechende Versuche unternommen. Die Angriffe sind willkürlich und richten sich gegen alle möglichen Kunden. Aufgrund unserer Anstrengungen zur Nachverfolgung der Malware und der Bemühungen meines Teams ist es uns gelungen, die tatsächliche Ausführung dieser schadhaften Dateien zu verhindern.

McSnip-Backdoor



Welchen Rat würden Sie Sicherheitsverantwortlichen zum Schutz ihrer Endpunkt in 2022 geben?

Der wichtigste Rat, den ich Unternehmen geben kann, ist, dass sie sich einen Überblick über ihre Angriffsfläche verschaffen. Dazu gehört die Bedrohungsmodellierung. Außerdem sollten sie sicherstellen, dass sie teamübergreifend kommunizieren, um wirklich zu verstehen, wo sich etwaige Schwachstellen befinden.

„Bei Endpunkten ist aktives Hunting sehr hilfreich. Suchen Sie nach Änderungen am Verhalten und an den Mustern und stellen Sie sicher, dass Sie sich nicht ausschließlich auf Dinge konzentrieren, die bereits bekannt sind. Halten Sie Ausschau nach unbekannten Mustern und Vorfällen, um mögliche Sicherheitslücken zu schließen.“

Weitere Ressourcen:

Weitere Informationen zur Bedrohungsmodellierung finden Sie auf der Ressourcen-Website „What is threat modelling?“.

Wie Cisco Secure helfen kann

Cisco Secure kann Sicherheitsverantwortliche dabei unterstützen, die Sicherheit zu erhöhen und die Integrität ihres Unternehmens vor unvorhersehbaren Bedrohungen oder Änderungen zu schützen. Wir arbeiten mit Kunden zusammen, um Sicherheitslücken zu schließen und künftige Ereignisse zu antizipieren. Gleichzeitig unterstützen wir Unternehmen dabei, ihre Investitionen in die Sicherheit des gesamten Unternehmens zu optimieren.

Cisco Secure kombiniert maschinengestützte Überwachung mit menschlichen Erkenntnissen – für umfassende Einblicke und die schnelle Erkennung von Bedrohungen. In Kombination mit der beispiellosen, aussagekräftigen Intelligence von Cisco Talos für bekannte und neue Bedrohungen bleiben die Sicherheitsverantwortlichen den Angreifern immer einen Schritt voraus. Weitere Informationen zu unserem Plattformansatz:

Cisco SecureX

Konsolidieren Sie Ihre Sicherheitsmaßnahmen an einem zentralen Ort – mit Cisco SecureX, unserer Cloud-nativen, integrierten Plattform.

Cisco SecureX ist eine integrierte und offene Lösung. Sie vereinfacht und vereinheitlicht die Sicherheit an einem zentralen Ort. Cisco SecureX erhöht die Sichtbarkeit und maximiert die betriebliche Effizienz – zum Schutz von Netzwerken, Endpunkten, Clouds und Anwendungen.

Cisco SecureX erkunden

Incident Response von Cisco Talos

Unser kundenorientiertes Incident Response Team hilft Unternehmen dabei, festzustellen, ob ihr System kompromittiert wurde. Falls ja, ermitteln wir, was genau passiert ist. Wir geben jedem Unternehmen entsprechende Anweisungen, damit sie so schnell wie möglich den Betrieb wiederaufnehmen können.

Im November 2021 wurde Cisco Talos Incident Response als führende Lösung im 2021 IDC MarketScape for Worldwide Incident Readiness Services genannt.

Weitere Informationen zu Cisco Talos Incident Response

Die richtige Cisco Secure-Lösung finden:

Secure Access Service Edge (SASE)

Kombination aus Netzwerk- und Sicherheitsfunktionen in einem Cloud-basierten Service.

Mehr über SASE erfahren

Secure Hybrid Work

Gewährleisten Sie sicheren Zugriff an allen Standorten, um das Arbeiten von überall aus zu ermöglichen.

Mehr über die Hybrid Work-Lösungen erfahren

Extended detection and response (XDR)

Steigerung der Produktivität mit einer Cloud-nativen Plattform mit integrierten Analytik- und Automatisierungsfunktionen

Mehr über XDR erfahren

Schutz vor Ransomware

Wehren Sie Angriffe über mehrere kritische Kontrollpunkte hinweg ab.

Mehr über Schutz vor Ransomware erfahren

Zero Trust

Finden Sie die richtige Balance zwischen Sicherheit und Nutzbarkeit sowie dem Schutz von Benutzern, Netzwerken und Anwendungen.

Mehr über Zero Trust erfahren

Weitere Ressourcen

Anmerkungen zum Thema Burnout

Was in diesem Bericht nicht fehlen darf, sind einige Anmerkungen zu den persönlichen Folgen für Sicherheitsverantwortliche. In unserem neuesten E-Book Wohlbefinden am Cybersecurity-Arbeitsplatz haben wir 20 Verantwortliche für Cybersicherheit gebeten, uns mitzuteilen, was sie zur Vermeidung von Burnout und zur Erhaltung ihrer psychischen Gesundheit tun. Sehen Sie sich auf alle Fälle das E-Book an, wenn Sie oder jemand, die/den Sie kennen, betroffen sind.

Optimale Umsetzung der fünf wichtigsten Sicherheitspraktiken

In der Cisco Security Outcomes-Studie, Teil 2 analysieren wir fünf wichtige Praktiken, die Ihnen beim Aufbau eines erstklassigen Cybersicherheitsprogramms helfen. In dem Bericht finden Sie praktische Hinweise für den Aufbau einer sicheren und effizienten Arbeitsumgebung.

Talos Newsletter zu Bedrohungsquellen

Abonnieren Sie Talos Threat Source. Hier erhalten Sie jede Woche die neuesten Informationen von Cisco Talos mit Hinweisen zu den größten Bedrohungen und aktuellen Nachrichten zum Thema Sicherheit.

Cisco Secure Blog

Lesen Sie den Cisco Security Blog mit Produktankündigungen von Cisco Secure, Branchen-News und innovativen Lösungsansätzen.

Podcast: Security-Erfolgsgeschichten

Im Security Stories-Podcast hören Sie einzigartige, inspirierende und oft auch amüsante Hintergrundgeschichten von Verantwortlichen im Bereich der Cybersicherheit.

Hauptgeschäftsstelle Nord- und Südamerika
Cisco Systems, Inc.
San Jose, CA

Hauptgeschäftsstelle Asien/Pazifik
Cisco Systems (USA), Pte. Ltd.
Singapur

Hauptgeschäftsstelle Europa
Cisco Systems International BV Amsterdam,
Niederlande

© 2022 Cisco und/oder Partnerunternehmen. Alle Rechte vorbehalten.


cisco
SECURE