Cisco 2016
Midyear Cybersecurity Report

Inhalt

ZUSAMMENFASSUNG UND WICHTIGSTE ERKENNTNISSE 2

EINFÜHRUNG 5

RANSOMWARE IM FOKUS: TOP-TREND IN DER CYBER-KRIMINALITÄT 6

Ransomware: Eine kaum abzustellende Geldmaschine 7

Die Entwicklung von Ransomware: Ein Trojaner verbreitet sich selbst 9

Sicherheitslücken 11

Trügerische Sicherheit: sichere Verbindungen 12

ZEIT ZUM OPERIEREN 13

Angriffsvektoren: Client-seitig 14

PDF- und Java-Angriffe werden seltener 14

Exploit-Kits setzen weiterhin auf Flash 15

Exploit-Kit versteckt sich hinter dem Tor-Netz 16

Angreifer erweitern ihre Kampagnen auf die Serverseite 16

JBoss: Angreifbare Infrastruktur bringt Zeitgewinn für kriminelle Operationen 18

Weltweites Spam-Aufkommen bleibt relativ konstant 19

Die Rückkehr der Blacklists? Umstieg der Angreifer auf HTTPS macht Untersuchungen ungleich schwerer 21

Malvertising-as-a-Service: Hochgradig effiziente Ausbreitung von Infektionen 23

Web-Angriffsmethoden: Alle Hebel stehen auf Ransomware 25

ZEIT ZUM ABSICHERN 26

Sicherheitsrisiko Patching-Lücke: Trotz schneller Verfügbarkeit werden Sicherheitsupdates nicht rechtzeitig installiert 27

Veraltete Infrastruktur: Ausbreitung von Ransomware macht das Schließen seit Langem bestehender Sicherheitslücken unabdingbar 30

Verschlüsselung: HTTPS-Datenverkehr bleibt 2016 zumindest vorerst konstant 35

TLS-Verschlüsselung macht zwar die Payload, nicht aber das Verhalten einer Malware unkenntlich 37

Bedrohungs-Erkennungszeit: Ein hitziges Wettrüsten ist im Gange 40

Incident-Response: Versäumnisse, die die Sicherheit durchlöchern 44

Unzureichende Netzwerkpflege: Ransomware-Ausbrüche im Gesundheitswesen stehen exemplarisch für ein branchenübergreifendes Problem 45

GLOBALE PERSPEKTIVEN UND SICHERHEITSEMPFEHLUNGEN 46

Blockierung von Web-Angriffen: Regionaler Überblick 47

Malware-Auftrittsrisiko im Branchenvergleich: Keine Branche ist gefeit 49

Geopolitisches Update: Politik und Wirtschaft auf der Suche nach Auswegen aus dem Datenschutz-Dilemma 50

Sicherheitsempfehlungen 52

Indicators-of-Compromise sind keine Threat-Intelligence 53

FAZIT 54

ÜBER CISCO 55

Mitwirkende am Cisco Midyear Cybersecurity Report 2016 55

Zusammenfassung und wichtigste Erkenntnisse

Wer sich Cyberkriminellen wirksam entgegenstellen will, muss ihnen schneller einen Riegel vorschieben.

In vielen Fällen haben Cyberkriminelle derzeit noch immer viel zu leichtes Spiel. Einfach, indem sie bekannte Sicherheitslücken ausnutzen, die Unternehmen und Endnutzer wider besseren Wissens nicht geschlossen haben, können sie oft mehrere Tage, Monate oder sogar noch länger unerkannt ihr Unwesen treiben. Unterdessen ringen Sicherheitsteams weiterhin darum, tiefere Einblicke in die Aktivitäten von Angreifern zu erhalten und die Zeit bis zur Erkennung („Time to Detection", TTD) von bekannten und neuen Bedrohungen zu verkürzen. Einige Fortschritte können sie zwar bereits für sich verbuchen, aber bis sie wirklich wirksam verhindern können, dass die Kriminellen ihre hochprofitablen Infrastrukturen aufziehen und teils mit verheerender Wucht zuschlagen, ist es noch ein weiter Weg.

Der Cisco® Midyear Cybersecurity Report 2016 bietet eine aktuelle Analyse der in unserem letzten Security Report identifizierten Trends und untersucht zudem weitere Entwicklungen, die nach den Erkenntnissen von Cisco Security Research im weiteren Verlauf dieses Jahres für die Sicherheitslandschaft von Bedeutung sein werden.

Unsere Beobachtungen zu den aktuellen Entwicklungen in der Schattenwirtschaft bestätigen: Cyberkriminelle konzentrieren ihre Anstrengungen auch weiterhin darauf, mit größtmöglicher Effektivität Gewinne zu generieren. Dafür hat sich Ransomware für sie als besonders wirksam erwiesen – ein Vehikel, mit dem sie bevorzugt Unternehmensnutzer ins Visier nehmen. Ransomware steht mit vielen der in diesem Report skizzierten Trends in der Bedrohungs- und Sicherheitslandschaft im Zusammenhang – von den Techniken, die Angreifer verwenden, um ihre Kampagnen zu fahren und ihre Aktivitäten zu tarnen, bis hin zu unseren Einschätzungen dazu, wie sich diese ernstzunehmende Bedrohung künftig entwickeln wird.

Weiterhin zeigen wir in diesem Report die zahlreichen Maßnahmen auf, die Unternehmen einsetzen sollten (und müssten), um ihre Bedrohungsabwehr zu stärken. So empfehlen unsere Sicherheitsforscher:

- Einen Incident-Response-Plan für eine schnelle Wiederaufnahme des normalen Geschäftsbetriebs nach einem Ransomware-Angriff formulieren (und auf seine Eignung testen)
- HTTPS-Verbindungen und SSL-Zertifikaten nicht blind vertrauen
- Patches für bekannte Sicherheitslücken in Software und Systemen, hierbei insbesondere auch in den für die Internet-Infrastruktur kritischen Routern und Switches, schnell installieren
- Nutzer besser über die Gefahren von Browser-Infektionen aufklären
- Besseres Verständnis davon gewinnen, was aussagekräftige Threat-Intelligence wirklich bedeutet

Der Report ist in vier Themenkomplexe gegliedert:

I. RANSOMWARE IM FOKUS: TOP-TREND IN DER CYBER-KRIMINALITÄT

Unsere Sicherheitsforscher beleuchten Entwicklungen, die auf eine künftig noch erheblich stärkere Zunahme von Angriffen mit Malware dieser Art hindeuten. Ebenfalls thematisiert wird der Zeitgewinn, der sich aufgrund von Sicherheitslücken in nicht aktualisierten oder veralteten Systemen für die Aktivitäten der Angreifer ergibt. Da Ransomware-Operationen zunehmend Unternehmensnutzer ins Visier nehmen, sollten Unternehmen zudem einen geschützten Speicherort für die Sicherung geschäftskritischer Daten einrichten und Maßnahmenpläne ausarbeiten, die nach einem Angriff schnellstmöglich eine Rückkehr zum normalen Geschäftsbetrieb ermöglichen.

II. ZEIT ZUM OPERIEREN

Dieser Abschnitt untersucht Client-seitige Angriffsvektoren, die Angreifern mehr Zeit und Möglichkeiten verschaffen, neue Innovationen zu entwickeln und ihre Kampagnen zu fahren. Die Zunahme von Schwachstellen in den Bereichen Verschlüsselung und Autorisierung legt nahe, dass Cyberkriminelle immer mehr die Vorteile von sicheren Verbindungen für sich erkennen. Ebenfalls diskutiert werden aktuelle Trends bei Exploit-Kits und Angriffsvektoren, darunter der zunehmende Einsatz von Server-Exploits als Mittel für den Zugriff auf umfangreichere Datensätze, sowie der Vormarsch von „Malvertising-as-a-Service", das Sicherheitsteams vor neue Herausforderungen stellt und zudem die Frage aufwirft, wer für den Schutz der Endnutzer verantwortlich ist.

III. ZEIT ZUM ABSICHERN

Dieser Abschnitt untersucht die Lücke zwischen den Aktivitäten von Angreifern und dem Aktivwerden von Sicherheitslösungen. So veröffentlichen die Hersteller nach Bekanntwerden einer Sicherheitslücke in ihren Produkten mittlerweile zwar schneller entsprechende Patches, die Nutzer installieren diese jedoch häufig nicht rechtzeitig. Daneben wird aufgezeigt, welche Fortschritte Cisco bei der Verkürzung der Bedrohungs-Erkennungszeit macht, und es werden Fakten herausgestellt, die das andauernde Wettrüsten zwischen Angreifern und Verteidigern deutlich machen. Ein weiteres Thema ist der zunehmende Trend bei Angreifern, ihre Kampagnen über HTTPS zu fahren und ihre Kommunikation mithilfe von Transport Layer Security (TLS) zu verschlüsseln.

IV. GLOBALE PERSPEKTIVEN UND SICHERHEITSEMPFEHLUNGEN

In diesem Abschnitt werden geopolitische Entwicklungen und deren Auswirkungen auf das Security-Umfeld analysiert, darunter die zunehmende Herausforderung für Regierungen, mit dem technischen Wandel Schritt zu halten, um Bedrohungen besser verstehen und die Kontrolle von Daten und den Zugriff darauf wirksam steuern zu können. Außerdem stellen wir Maßnahmen vor, mit denen der Spielraum von Angreifern eingegrenzt werden kann, und erläutern, welcher entscheidende Unterschied zwischen Indicators-of-Compromise (IOCs) und Threat-Intelligence besteht.

WICHTIGSTE ERKENNTNISSE

- Ransomware dominiert den Malware-Markt. Diese Bedrohung ist zwar nicht neu, doch mit keinem anderen Malware-Typ werden mittlerweile derart große Gewinne erzielt wie mit Ransomware. Ein immer beliebteres Ziel sind dabei Unternehmen, wie die starke Zunahme an Ransomware-Kampagnen zeigt, die in der ersten Jahreshälfte 2016 neben Einzelpersonen auch gezielt Unternehmensnutzer anvisierten. Wie sich außerdem zeigt, werden die Drahtzieher immer schneller und effektiver darin, die Reichweite ihrer Ransomware-Kampagnen zu maximieren und somit auch die Chancen auf hohe Gewinne deutlich zu erhöhen.
- Exploit-Kits, also die Hauptverantwortlichen für den Aufstieg von Ransomware, finden den Weg in ihre Zielsysteme auch weiterhin häufig über Sicherheitslücken in Adobe Flash. Bei einer Analyse des populären Nuclear-Exploit-Kits etwa verliefen 80 Prozent aller erfolgreichen Exploit-Versuche über Flash.
- Mit Sicherheitslücken in der Anwendungssoftware JBoss haben Angreifer einen neuen Vektor gefunden, über den sie z. B. Ransomware-Kampagnen fahren können. So waren durch Kompromittierungen über JBoss-Sicherheitslücken im Verlauf unserer Untersuchung erhebliche Einfallstore auf Servern entstanden.
- Zwischen September 2015 und März 2016 wurde ein fünffacher Anstieg von schädlichen Aktivitäten im Zusammenhang mit HTTPS-Datenverkehr registriert, in erster Linie zurückzuführen auf schädliche Ad-Injector-Software und Adware. Angreifer greifen zunehmend auf HTTPS-Verschlüsselung zurück, da sie so ihre Aktivitäten im Internet verbergen und ihre Operationen über längere Zeiträume ausweiten können.
- Obwohl die meisten großen Softwarehersteller praktisch sofort nach Bekanntwerden von Sicherheitslücken in ihren Produkten entsprechende Patches herausgeben, installieren viele Nutzer diese häufig nicht rechtzeitig. Dadurch entsteht häufig ein großes Zeitfenster, in dem Angreifer Exploits gegen diese Nutzer ausführen können.
- Um auf die Risiken von unzureichend gepflegter, veralteter Infrastruktur und nicht behobener Sicherheitslücken in Betriebssystemen aufmerksam zu machen, haben wir bei einer Stichprobe von Cisco Geräten untersucht, wie weit darauf vorhandene bekannte Sicherheitslücken zurückdatierten. 23 Prozent der Sicherheitslücken in diesen Geräten gingen bis in das Jahr 2011 zurück. Bei knapp 16 Prozent waren sogar Sicherheitslücken zu finden, die bereits seit 2009 bekannt waren.
- Eine eher geringe, aber dennoch wachsenden Zahl von Malware-Stichproben verschlüsselte ihren Netzwerkverkehr über Transport Layer Security (TLS), um ihre Aktivitäten zu verbergen. Dies gibt Grund zur Sorge, denn Deep-Packet-Inspection ist als Sicherheitstool in diesem Fall wirkungslos. Aussagekräftigere Erkenntnisse kann jedoch eine Kombination aus maschinellem Lernen und neuartigen Dateninterpretationsverfahren liefern.
- Cisco konnte die Bedrohungs-Erkennungszeit weiter reduzieren. Zwischen Dezember 2015 und April 2016 lag der TTD-Median bei ca. 13 Stunden – und damit deutlich unter dem inakzeptablen Branchenstandard von derzeit 100 bis 200 Tagen. Die Auf- und Abwärtsbewegungen der TTD in diesem Zeitraum unterstreichen die enorme Intensität des Wettrennens zwischen Angreifern, die laufend neue Bedrohungen ins Feld führen, und Verteidigern, die schnell mit wirksamen Maßnahmen dagegenhalten müssen.

Einführung

Betrachtet man die Art und Weise, wie Angreifer vorgehen, werden Systeme nach wie vor nicht angemessen geschützt. Die Strategien und Tools für die Abwehr von Angriffen wurden zwar weiterentwickelt, aber den Kriminellen bleibt noch immer zu viel Zeit für die Durchführung ihrer Operationen.

Das Problem: Die Nutzer sind angreifbar, weil es Sicherheitsteams an der nötigen Übersicht fehlt. Noch immer wird auf Punktlösungen vertraut und nach einem „Triage"-Ansatz Maßnahmen gegen Angriffe fallabhängig abgewogen, statt Sicherheit ganzheitlich anzugehen. Doch das spielt den Angreifern in die Hände.

Denn sie haben die Zeit auf ihrer Seite: Infrastruktur, Systeme und Geräte, die nicht angemessen gepflegt oder einfach vergessen wurden, können sie auf Sicherheitslücken sondieren, sich über diese im Netzwerk einnisten und sich lateral darin bewegen. Wenn sie dann Zugang zu Servern erhalten, können sie ihre Operationsbasis verbreitern und somit noch größere Profite einfahren.

„Verteidiger müssen die Möglichkeiten, die ihnen zur Verfügung stehen, besser nutzen. Wenn sie Patches für Sicherheitslücken schneller installieren und ihre Infrastruktur auf dem aktuellen Stand halten, können sie wissen, womit sie es zu tun haben, und lassen Angreifern somit nur noch begrenzten oder sogar gar keinen Spielraum mehr."

Trotz ihres zeitlichen Vorsprungs haben die Angreifer aber nur eine begrenzte Zahl von Möglichkeiten, in Netzwerke einzudringen. Die Verteidiger müssen nur die Möglichkeiten, die ihnen zur Verfügung stehen, besser nutzen. Wenn sie Patches für Sicherheitslücken schneller installieren und ihre Infrastruktur auf dem aktuellen Stand halten, können sie wissen, womit sie es zu tun haben, und lassen Angreifern somit nur noch begrenzten oder sogar gar keinen Spielraum mehr. Zudem können sie eine vollständige Übersicht über die Sicherheitslandschaft erhalten: ob Angreifer in ihr Netzwerk gelangt sind, wie ihnen dies gelungen ist, und welche Systeme die schädlichen Aktivitäten bemerkt (bzw. übersehen) haben.

Sicherheitsteams sind jedoch häufig damit überfordert, das Netzwerk auf so vielen Ebenen gleichzeitig abzusichern, und belassen es daher bei ihrem Triage-Ansatz. Für die Angreifer bedeutet das, sie haben alle ihre Vorteile auf ihrer Seite: Verteidiger, die selbst die einfachsten Eintrittswege nicht verschließen und Zeit, ihre Operationen bequem aufzuziehen. Daher ist Ransomware auch das perfekte Mittel für sie, diese Vorteile in Profite umzumünzen – ein Mittel, das nicht nur weiter auf dem Vormarsch, sondern auch immer schwieriger abzuwehren ist (siehe „Ransomware: Eine kaum abzustellende Geldmaschine" auf **Seite 7**).

Ransomware im Fokus: Top-Trend in der Cyberkriminalität

Ransomware im Fokus: Top-Trend in der Cyberkriminalität

Ransomware dominiert den Malware-Markt. Diese Bedrohung ist zwar nicht neu, doch mit keinem anderen Malware-Typ werden mittlerweile derart große Gewinne erzielt. In der ersten Jahreshälfte 2016 waren gegen Einzelpersonen und Unternehmensnutzer gerichtete Ransomware-Kampagnen größer angelegt und hatten eine größere Durchschlagskraft.

Die Erfolge der jüngsten Ransomware-Angriffe u. a. gegen zahlreiche Vertreter der Gesundheitsbranche, werden sehr wahrscheinlich weitere Kampagnen ähnlicher Art nach sich ziehen. Netzwerk- und serverseitige Sicherheitslücken öffnen Tür und Tor für im Verborgenen durchgeführte Ransomware-Kampagnen, die ganze Branchen ins Wanken bringen können.

Ransomware: Eine kaum abzustellende Geldmaschine

Ransomware ist in Duzenden Varianten in Umlauf, einige davon sind sprachspezifisch, allesamt sind sie hartnäckig. Die Innovatoren in diesem Bereich, insbesondere die Entwickler von Ransomware-Spielarten wie CryptoLocker und CryptoWall, haben die Effektivität ihrer Malware mit der Einführung von starken kryptografischen Verschlüsselungsverfahren drastisch verbessert. Beim Großteil der derzeit bekannten Ransomware lassen sich die Dateien nicht ohne Weiteres entschlüsseln, und so bleibt den Opfern meist nichts anderes übrig als der Lösegeldforderung nachzukommen.

Die Zahlung erfolgt üblicherweise über die Bitcoin-Kryptowährung, die der Ransomware-Branche auch ungewollt zum Aufschwung verholfen hat, da die Bitcoin-Nutzeradressen anonym bleiben. Ein weiteres Problem für Sicherheitsforscher ist die Tatsache, dass Ransomware-Transkationen praktisch komplett über das anonyme Tor-Netz laufen. Zudem können Bitcoins gestückelt werden, d. h. die Drahtzieher können ihr gesamtes Team mit einer einzigen Bitcoin-Einheit bequem auszahlen und praktisch nicht zurückverfolgt werden.

EIN NEUER VEKTOR FÜR RANSOMWARE

E-Mail und schädliche Online-Werbung (Malvertising) sind die primären Vektoren für Ransomware. Einige Angreifer nutzen mittlerweile jedoch auch netzwerk- und serverseitige Sicherheitslücken.

So wurde Anfang des Jahres eine groß angelegte Kampagne mit der Ransomware-Variante Samas/Samsam/MSIL.B/C („SamSam“) gegen das Gesundheitswesen gefahren, die über kompromittierte Server verbreitet wurde. Die Angreifer bewegten sich über diese Server lateral durch das Netzwerk und infizierten weitere Systeme, auf denen sie die Daten verschlüsselten, um Lösegeld zu erpressen.

Eintritt in die Unternehmensnetze verschafften sich die Drahtzieher mithilfe von JexBoss, einem Open-Source-Tool, mit dem Sicherheitslücken in JBoss-Anwendungsservern aufgespürt und ausgenutzt werden können. Anschließend verschlüsselten sie dann zahlreiche Windows-Systeme mit der SamSam-Ransomware.

„In Zukunft wird Ransomware das Internet noch weitaus stärker durchdringen, und es wird ihr deutlich schwerer beizukommen sein. Darauf sollten sich Unternehmen und Endnutzer jetzt einstellen, indem sie Sicherungskopien ihrer wichtigsten Daten erstellen und diese angemessen gegen Angriffe abschirmen."

Der SamSam-Angriff war in vielerlei Hinsicht vorprogrammiert, da viele Unternehmen JBoss-Server mit nicht gepatchten Sicherheitslücken in Betrieb haben (siehe „JBoss: Angreifbare Infrastruktur bringt Zeitgewinn für kriminelle Operationen" auf **Seite 18**). Bei einer Untersuchung im April 2016 konnten wir mindestens 2.100 JBoss-Server identifizieren, die bereits kompromittiert und für den Missbrauch durch einen Angreifer bereit waren. Alle betroffenen Unternehmen wurden darauf hingewiesen, dass sie diese Server umgehend vom Netz nehmen und aktualisieren sollten.

Angreifbare Internet-Infrastruktur ist ein allgegenwärtiges Problem, und zweifelsohne werden Cyberkriminelle diesen Kanal künftig noch ausgiebiger für verdeckte Malware-Kampagnen nutzen, die nicht nur einzelne Unternehmen, sondern ganze Branchen ins Visier nehmen (siehe „Veraltete Infrastruktur: Ausbreitung von Ransomware macht das Schließen seit Langem bestehender Sicherheitslücken unabdingbar", **Seite 30**).

EBENFALLS FRAGLICH: DIE DATENINTEGRITÄT

Opfer eines Ransomware-Angriffs sind in einer wenig beneidenswerten Position. Sie müssen darauf vertrauen, dass die Angreifer ihren Teil des „Deals" einhalten. Und obwohl Bezahlen die wohl einfachste (und einzige) Lösung zu sein scheint, ist es keineswegs gesichert, dass die Daten dann auch entschlüsselt werden. Tatsächlich sind sie im schlimmsten Fall sogar komplett verloren, wie dies etwa bei frühen Versionen einiger Ransomware-Varianten der Fall war, bei denen Bugs zu Dateiverlusten führten, auch wenn das Lösegeld bezahlt wurde.

Weiterhin besteht das Risiko, dass die Angreifer die Dateien manipulieren, solange diese unter ihrer Kontrolle sind. Je nachdem, um welche Art von Dateien es sich handelt (z. B. Krankenakten oder technische Pläne), können Manipulationen oder Datendiebstahl verheerende Folgen haben.

Zudem haben wir auch Fälle beobachtet, in denen ein- und dasselbe System mehrfach zum Opfer von Ransomware wurde. Teilweise wurde das Lösegeld dann beim zweiten Mal reduziert, dem Nutzer wurde also eine Art „Kundenrabatt" eingeräumt. Aber auch das Gegenteil war bisweilen der Fall: Zögerten die Nutzer etwa beim ersten Mal mit der Zahlung, wurde die Forderung erhöht.

Ransomware hat sich zu einem extrem effektiven und einträglichen Geschäftsmodell entwickelt, das kriminelle Kreise zweifelsohne noch ausgiebiger als Hauptquelle für leicht verdientes Geld nutzen werden. Dass von Unternehmen wesentlich größere Summen erpresst werden können als von Einzelnutzern, bedarf dabei keiner weiteren Erklärung. Ebenso wenig, dass auch die potenziellen Schäden und Kosten von Ransomware-Angriffen für Unternehmen oder Branchen um ein Vielfaches höher sind.

In Zukunft wird Ransomware das Internet noch weitaus stärker durchdringen, und es wird ihr deutlich schwerer beizukommen sein (siehe „Die Entwicklung von Ransomware: Ein Trojaner verbreitet sich selbst" auf **Seite 9**). Darauf sollten sich Unternehmen und Endnutzer jetzt einstellen, indem sie Sicherungskopien ihrer wichtigsten Daten erstellen und diese angemessen gegen Angriffe abschirmen. Zudem müssen die Daten schnell wiederhergestellt werden können – ein Vorgang, der gerade in Unternehmen häufig mit erheblichem Aufwand verbunden ist. Daher ist es entscheidend zu ermitteln, an welchen Stellen hierbei Probleme auftreten könnten. Und nicht zuletzt müssen Unternehmen dafür sorgen, dass alle bekannten Sicherheitslücken in ihrer Internet-Infrastruktur und ihren Systemen behoben werden.

Weitere Details zur SamSam-Kampagne und zu Sicherheitslücken in JBoss-Servern können Sie in den folgenden Blog-Beiträgen von Cisco Talos nachlesen:

„SamSam: The Doctor Will See You, After He Pays the Ransom"

„Widespread JBoss Backdoors a Major Threat"

Die Entwicklung von Ransomware: Ein Trojaner verbreitet sich selbst

Der SamSam-Angriff markiert einen Wendepunkt im Bereich der Erpressungstrojaner: Ransomware-Operationen infizieren nicht mehr nur Einzelnutzer, sondern gleich ganze Netzwerke (siehe **Seite 16**). Die Verbreitungsmethode ist dabei ebenso einfach wie effektiv, wird aber angesichts des Erfolgs von SamSam sicher noch weiterentwickelt werden, um noch schneller noch mehr Systeme zu erreichen und die Lösegeldzahlungen noch wirksamer erpressen zu können.

Mit Blick auf die aktuellen Entwicklungen ist zu erwarten, dass sich Ransomware in Zukunft selbst verbreiten wird. Und jeder sollte sich angemessen darauf vorbereiten, denn die Ransomware-Kampagnen gegen Vertreter des Gesundheitswesens Anfang des Jahres, bei denen die Angreifer Backdoors in JBoss-Servern ausnutzten, zeigen einmal mehr: Mit genügend Zeit zum Aufziehen ihrer Operationen finden Cyberkriminelle auch neue Wege, Netzwerke und Nutzer zu kompromittieren – einschließlich alter Sicherheitslücken, die längst geschlossen sein sollten.

Sich selbst verbreitende Malware ist dabei nichts Neues. Von Würmern und Botnets kennt man diese Technik seit Jahrzehnten. Doch viele dieser Bedrohungen sind noch immer weit verbreitet und nicht minder effektiv. Malware kann sich z. B. über folgende Wege selbst ausbreiten:

- **Nutzung einer Sicherheitslücke in einem weit verbreiteten Produkt:** Bereits in der Vergangenheit haben die erfolgreichsten Wurm-Typen Sicherheitslücken in Produkten genutzt, die im Internet weit verbreitet waren.
- **Replikation auf alle verfügbaren Laufwerke:** Einige Malware-Varianten erfassen lokale und Remote-Laufwerke, darunter auch Netz- und USB-Laufwerke, und kopieren sich anschließend auf diese, um sich weiter auszubreiten oder noch stärker Fuß zu fassen. Auf diesem Weg können auch Offline- und solche Systeme infiziert werden, die nicht über das öffentliche Internet erreichbar sind.
- **Infektion von Dateien:** Dabei hängt sich die Malware entweder am Anfang oder am Ende einer Datei an, dabei bevorzugt an ausführbare Dateien, die nicht von Windows SFC oder SFP (System File Checker/System File Protector) geschützt werden. Einige Würmer können sich aber auch an nicht ausführbare Dateien anhängen und sich von dort aus verbreiten.
- **Eingeschränkte Brute-Force-Aktivität:** Bei manchen Würmern wurde auch diese Methode bereits beobachtet.
- **Resiliente Command-and-Control-Infrastruktur:** Einige Würmer sind auf die gängigen Maßnahmen zum Lahmlegen von Command-and-Control-Infrastrukturen eingestellt und umgehen diese. Viele Würmer verwenden jedoch keine Command-and-Control-Infrastruktur, sondern eine einfache Standardaktion, um sich schnellstmöglich zu verbreiten.
- **Nutzung anderer Backdoors:** Einige Malware-Entwickler erkennen, ob ein System bereits von einer anderen Infektion befallen ist, und verbreiten ihre eigene Malware quasi im Fahrwasser der anderen Schadprogramme.

„Mit Blick auf die aktuellen Entwicklungen ist zu erwarten, dass sich Ransomware in Zukunft selbst verbreiten wird. Und jeder sollte sich angemessen darauf vorbereiten.“

DAS ERPRESSER-FRAMEWORK

Betrachtet man die aktuellen Neuerungen im Bereich der Erpressertrojaner, so werden künftige Generationen sehr wahrscheinlich auf ein modulares Softwaredesign setzen. Denn mit einer solchen Architektur – sie wird auch in vielen populären Open-Source-Suites für Penetrationstests eingesetzt – können bei Bedarf bestimmte Funktionen genutzt werden. So können die Angreifer effizienter operieren und ihre Taktik anpassen, falls eine Methode auffliegt oder sich als nicht effektiv erweist.

Wir erwarten, dass das Ransomware-Framework der nächsten Generation im Kern folgende Funktionen umfassen wird:

- Verschlüsselung von Standardspeicherorten für Benutzerdateien sowie die Möglichkeit, für jedes Opfer die zu verschlüsselnden Verzeichnisse und Dateitypen individuell zu definieren
- Markierung der Systeme und Dateien, die bereits verschlüsselt wurden
- Anweisungen für eine korrekte Zahlungsabwicklung über Bitcoins
- Möglichkeit zur Festlegung des zu zahlenden Betrags und Angabe von zwei Fristen: eine Zahlungsfrist, nach deren Ablauf die Forderung erhöht wird, und eine weitere Frist, nach deren Ablauf der Schlüssel für die Daten gelöscht wird

Daneben wird das Framework verschiedene Module unterstützen, mit denen die Ransomware entsprechend der anvisierten Umgebungen angepasst und abhängig von den verfügbaren Einfallstoren noch aggressivere Ausbreitungstechniken angewendet werden können. Einige Beispiele für solche Module:

VERBREITUNG ÜBER AUTORUN.INF AUF USB-SPEICHERMEDIEN

Ein Modul, welches das infizierte System nach zugeordneten lokalen und Remote-Laufwerken durchsucht, sich dann in bestimmte Bereiche auf diesen Laufwerken kopiert und Dateiattribute festlegt, die das Auffinden und Löschen dieser Kopien erschweren. Im nächsten Schritt würde eine „autorun.inf"-Datei auf diese Laufwerke geschrieben, über die die Schadprogramme künftig automatisch auf allen Computern ausgeführt werden, die sich mit dem Laufwerk verbinden.

EXPLOITS DER AUTHENTIFIZIERUNGSINFRASTRUKTUR

Dieses Modul würde versuchen, über Schwachstellen in gängigen Authentifizierungsinfrastrukturen an Anmeldeinformationen zu gelangen, die den Angreifern Zugriff auf andere Systeme verschaffen.

COMMAND-AND-CONTROL UND INFEKTIONS-REPORTING

Zukünftige Ransomware-Generationen könnten so konfiguriert sein, dass sie – um das Erkennungsrisiko zu reduzieren – die Command-and-Control-Aktionen nicht selbst ausführen. Ein solches Modul würde einen Beacon mit einer GUID (Globally Unique Identifier) an eine über gängige Protokolle und Dienste wie HTTP, HTTPS oder DNS erreichbare Command-and-Control-Domäne übertagen. Anschließend würde die Domäne diese GUIDs erfassen, um Statistiken zur Anzahl der in einem Zielnetzwerk infizierten und verschlüsselten Systeme zu erstellen. Mithilfe dieser Daten ließe sich die Effektivität von Kampagnen messen.

RATE LIMITER

Mit einem solchen Modul kann die Beanspruchung der Systemressourcen reduziert werden. So ist die Ransomware schwerer zu entdecken, wenn ihre CPU- und Netzwerknutzung auf ein Minimum reduziert wird.

BESCHRÄNKUNG AUF DIE ZIELADRESSE RFC 1918

Ein solches Modul würde Angriffe auf Zielhosts der für interne Netzwerke verwendeten Adresse RFC 1918 beschränken.

Mit einer sorgfältig geplanten Sicherheitsarchitektur und einem ebenso sorgfältigen Passwortmanagement lasst sich die laterale Bewegungsfreiheit der künftigen, sich selbst ausbreitenden Ransomware-Varianten jedoch erheblich einschränken. Detaillierte Empfehlungen zum Schutz vor der Ransomware der nächsten Generation finden Sie auf **Seite 52**.

Weitere Informationen zu den Entwicklungen im Bereich der Ransomware und zu den Möglichkeiten für Unternehmen, sich auf zukünftige Bedrohungen wie diese vorzubereiten, finden Sie im folgenden Blog-Beitrag von Cisco Talos:

„Ransomware: Past, Present, and Future"

Sicherheitslücken

Sicherheitslücken, die nicht zeitnah geschlossen werden, verschaffen Angreifern die Zeit, ihre Operationen in Gang zu setzen. Exploit-Kits, Ransomware oder auch Social-Engineering-Spam sind dabei ihre Mittel, um ungepatchte Systeme und veraltete Hardware anzugreifen und ihre Ziele zu erreichen.

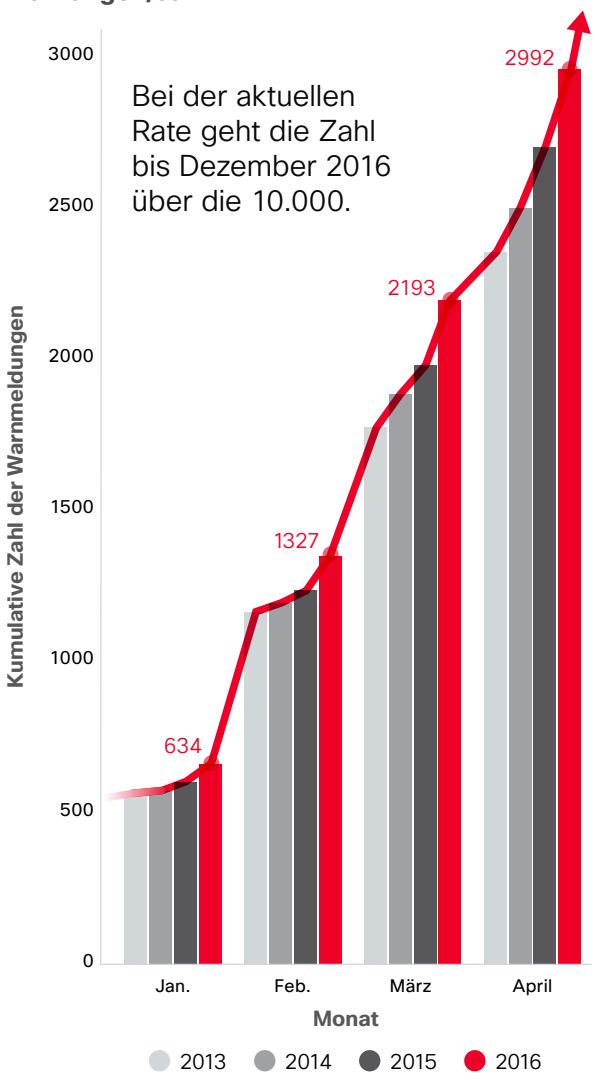
Sicherheitslücken sind das Einfallstor, das Angreifern die Möglichkeit zum Einbruch ins Netzwerk bietet. Wenn die Verteidiger an diesem Schnittpunkt ansetzen, indem sie Sicherheitslücken beheben, können sie diese Bedrohung erheblich mindern. Versäumen sie dies, werden Angreifer die Sicherheitslücken als Startrampe für ihre Kampagnen nutzen.

Seitens der Hersteller wird die Erkennung und Veröffentlichung von Sicherheitslücken mittlerweile verantwortungsvoller gehandhabt, etwa durch die Implementierung von Secure Development Lifecycle (SDL)-Prozessen. Wie auf **Seite 15** näher ausgeführt, beobachten jedoch auch Cyberkriminelle genau, welche Patches veröffentlicht werden, und rekonstruieren diese mittels Reverse-Engineering, um anhand dieser Erkenntnisse ihrerseits neue Ansätze zu entwickeln.

2016 ist die kumulative Zahl der Warnmeldungen in den ersten vier Monaten gegenüber der Gesamtzahl vom Vorjahr leicht gestiegen (Abbildung 1). Zurückzuführen ist dies vermutlich auf Veröffentlichungen von neuen Versionen der Software etwa von Microsoft oder Apple, gründlichere Code-Prüfungen und leistungsfähigere Code-Prüfungstools, sowie die bereits genannten SDL-Prozesse.

Die Prozesse zur Veröffentlichung und Behebung von Sicherheitslücken werden zwar laufend optimiert und weiterentwickelt, doch die Kriminellen setzen alles daran, diese Lücken mit immer umfangreicheren und komplexeren Angriffen wieder zu öffnen und die Reaktionsmöglichkeiten der Verteidiger zu untergraben. Daher müssen Angreifern auch diese Möglichkeiten entzogen werden. Und dafür ist die Behebung bekannt gewordener Sicherheitslücken und die Implementierung eines leistungsfähigen Patch-Managements entscheidend.

Abbildung 1: Kumulative Gesamtzahl der Warnungen/Jahr



Quelle: Cisco Security Research

„Die Prozesse zur Veröffentlichung und Behebung von Sicherheitslücken werden zwar laufend optimiert und weiterentwickelt, doch die Kriminellen setzen alles daran, diese Lücken mit immer umfangreicheren und komplexeren Angriffen wieder zu öffnen und die Reaktionsmöglichkeiten der Verteidiger zu untergraben.“

TRÜGERISCHE SICHERHEIT: SICHERE VERBINDUNGEN

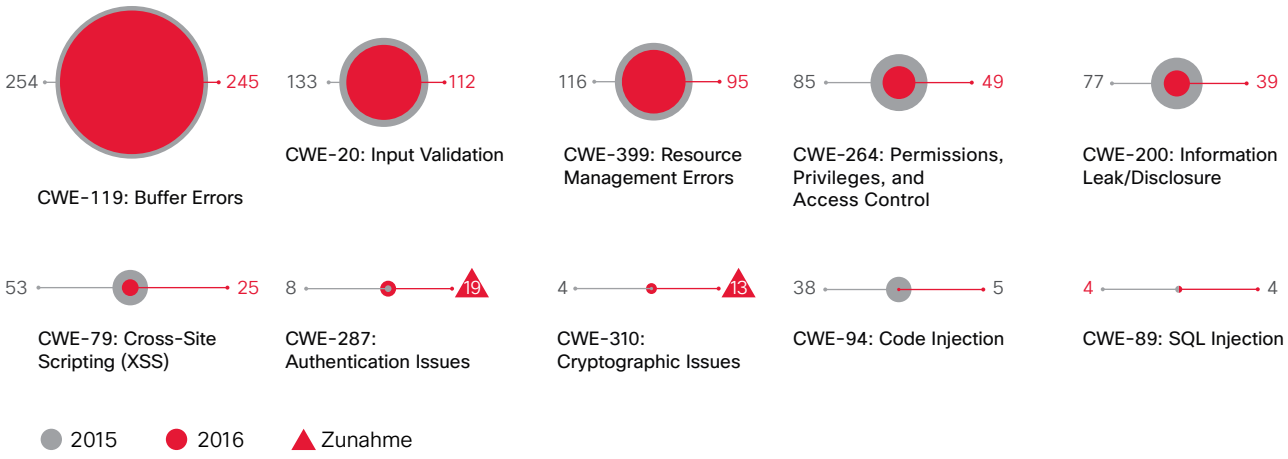
HTTPS-Verbindungen oder SSL-Zertifikate geben Nutzern das Gefühl, sie bewegten sich sicher im Cyberspace. Wie jedoch die zunehmende Zahl von Warnmeldungen mit Bezug auf Verschlüsselung und Authentifizierung nahelegt, können gesicherte Verbindungen von Angreifern leichter als gedacht kompromittiert werden. Die Sicherheit dieser Verbindungen ist also mehr als fragwürdig.

Wie in Abbildung 2 unten gezeigt, steigt die Zahl der in der Common Weakness Enumeration (CWE) festgehaltenen Authentifizierungs- und Kryptografieproblemen seit 2014 und 2015 stetig an. Allein zwischen Dezember 2015 und März 2016 wurden 19 Authentifizierungsprobleme und 13 kryptografische Probleme verzeichnet, was beinahe der Gesamtzahl des Vorjahres entspricht.

Zwar ist es positiv zu bewerten, dass Verbindungen zunehmend verschlüsselt und Informationen somit besser vor fremden Augen geschützt werden. Doch damit gehen auch Risiken einher. So steht auf der einen Seite die zusätzliche Komplexität von Verschlüsselungstools – und somit die Gefahr neuer Sicherheitslücken –, und auf der anderen Seite die nutzerseitige Erwartung einer Privatsphäre, die somit nicht mehr garantiert werden kann. Falsch umgesetzte Verschlüsselung bietet also eher das Gegenteil von Schutz.

Sichere Verbindungen erfordern eine komplexe Kette aus Prozessen und Tools. Jenseits der Zertifikate ist diese Kette jedoch mitunter fragwürdig. Denn zwischen den Verbindungen liegen Geräte wie VPN-Gateways, die möglicherweise nicht sicher sind. Und auch Websites, die sichere Verbindungen anzeigen, können bereits infiziert sein. Am Ende des Tages bedeutet das: Bei URLs, die durch das Vorhängeschloss-Symbol sichere Aktivitäten suggerieren, darf niemals von absoluter Sicherheit ausgegangen werden.

Abbildung 2: Zunahme Authentifizierungs- und Kryptografieprobleme, Dezember bis März



Quelle: Cisco Security Research

Zeit zum Operieren

Zeit zum Operieren

Der weitere Vormarsch von Ransomware sowie das Ausmaß der jüngsten Kampagnen machen deutlich: Je länger Cyberkriminelle ungestört ihre Operationen aufziehen und im Verborgenen ihre Kampagnen schmieden können, desto härter schlagen sie genau dann zu, wenn sich die größten Gewinne einstreichen lassen.

Kryptowährungen, das Tor-Netz sowie mittels HTTPS und Transport Layer Security (TLS) verschlüsselte Verbindungen verschaffen ihnen dabei die nötige Anonymität, während ihnen Exploit-Kit-Entwickler mit immer schnelleren Reverse-Engineerings von neuen Patches und mit Exploits von unkontrolliert öffentlich gewordenen Sicherheitslücken zusätzlichen Rückenwind geben. Daneben führen die Kriminellen nun eine hocheffiziente und schwer zurückverfolgbare neue Malvertising-Strategie ins Feld, mit der sie mehr Datenverkehr an kompromittierte Websites leiten können, um die Computer der Webnutzer zu infizieren und schließlich Ransomware-Angriffe zu starten.

Angriffsvektoren: Client-seitig

Angreifer nehmen sich traditionell bevorzugt die Client-Seite vor, da sie dort näher am Nutzer, also dem schwächsten Glied in der Sicherheitskette, operieren können. Zudem sind die Möglichkeiten, ihre Operationsbasis zu verbreitern auf Client-Seite geradezu unermesslich.

Dennoch scheinen sich Client-seitige Angriffsvektoren wie PDF-Dateien nach jahrelangem Wachstum zu stabilisieren. Dafür entdecken die Cyberkriminellen nun zunehmend die Serverseite für sich, da sie sich hier lateral durch die Netze bewegen und so ihre Position stärken können.

PDF- UND JAVA-ANGRIFFE WERDEN SELTENER

PDF und Java werden als Angriffsvektoren immer unpopulärer. Oracle hat im Januar 2016 die Einstellung des Browser-Plug-ins von Java angekündigt, da die Browser-Hersteller den Support für Plug-ins dieser Art nicht mehr fortsetzen wollen.[1] Stattdessen will sich Oracle künftig auf seine Java Web Start-Technologie konzentrieren, die ohne Plug-ins auskommt.

Mit der Einstellung des Browser-Plug-ins wird Java als Angriffsvektor weiter an Bedeutung verlieren. Sicherheitsforscher werden jedoch genau beobachten, ob die Angreifer ältere Bedrohungen weiterentwickeln und gegen die neue Java-Variante einsetzen. Sicherheitsverantwortliche und Unternehmen sollten Java mit Ausnahme der Websites, auf denen die Technologie unbedingt benötigt wird, grundsätzlich sperren.

[1] „Moving to a Plugin-Free Web", Java Platform Group, Januar 2016: **https://blogs.oracle.com/java-platform-group/entry/moving_to_a_plugin_free**.

PDF-Exploits gehen zwar ebenfalls zurück, sind aber noch immer in E-Mails anzutreffen, in denen die Empfänger dazu verleitet werden sollen, infizierte Anhänge zu öffnen. Um dabei die Erfolgsquote zu erhöhen, versehen die Spammer die Mails zudem mit Betreffzeilen, die auf aktuelle Meldungen oder saisonbedingte Ereignisse verweisen (mehr zum Thema Spam auf **Seite 19**).

Und auch Flash ist bei Exploit-Kit-Entwicklern weiterhin beliebt. Insgesamt werden Flash-Inhalte im Internet zwar allmählich weniger, doch bei vielen Online-Applikationen kommt Flash z. B. für Multimedia-Inhalte oder interaktive Werbung nach wie vor in großem Umfang zum Einsatz.

Alternativen wie HTML5 sind zwar langsam im Kommen, der Übergang erfolgt jedoch sukzessive. Solange Flash noch eine Rolle spielt, wird die Technologie daher auch ein Angriffsvektor bleiben.

EXPLOIT-KITS SETZEN WEITERHIN AUF FLASH

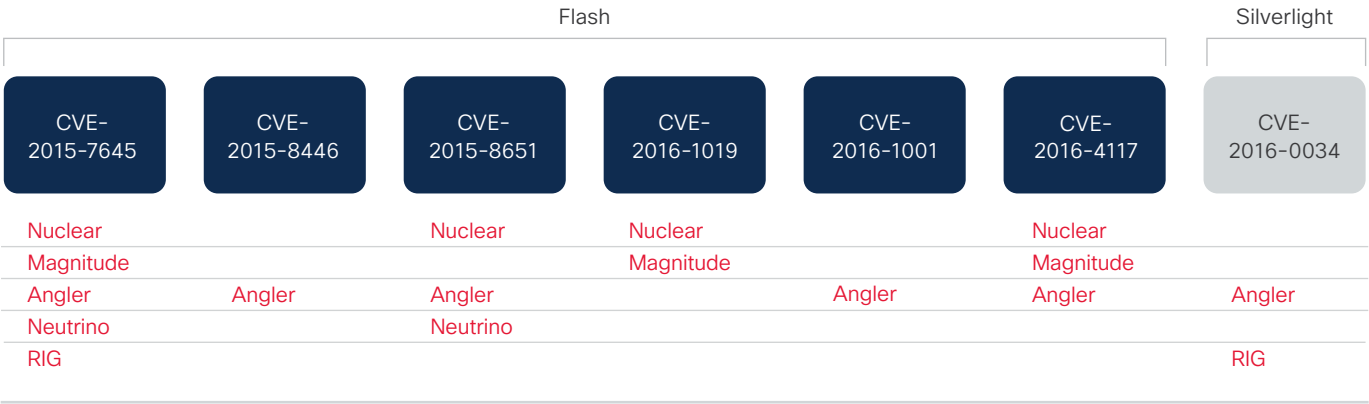
Exploit-Kits, also die Hauptverantwortlichen für den Aufstieg von Ransomware, finden den Weg in ihre Zielsysteme auch weiterhin häufig über Sicherheitslücken in Adobe Flash. Bei einer Analyse des populären Nuclear-Exploit-Kits etwa verliefen 80 Prozent aller erfolgreichen Exploit-Versuche über Flash.[2]

Adobe reagiert zwar schnell mit Patches auf die häufigen Veröffentlichungen von Sicherheitslücken in Flash, doch genauso verhält es sich mit der Reaktion der Angreifer. Sobald Adobe einen Patch herausbringt, rekonstruieren Exploit-Kit-Autoren diese mittels Reverse-Engineering. Exploits von Sicherheitslücken in Flash, die zur Remote-Code-Ausführung genutzt werden, lassen dann meist kaum eine Woche auf sich warten.

Nutzer und Administratoren können sich vor Bedrohungen wie diesen schützen, indem sie nicht benötigte Browser-Plug-ins deaktivieren oder entfernen. Zumindest aber sollten sie alle Flash-Updates direkt nach deren Veröffentlichung installieren.

Wie wichtig die Installation von Patches ist, machen die verschiedenen in Abbildung 3 aufgeführten Exploit-Kits deutlich, die aktuelle Sicherheitslücken in Flash und Microsoft Silverlight ausnutzen. Wenn Nutzer alle für diese Sicherheitslücken verfügbaren Patches installieren, können sie sich deutlich besser vor Ransomware schützen, die von Exploit-Kits ausgeliefert wird.

Abbildung 3: Von Exploit-Kits genutzte Sicherheitslücken



Quelle: Cisco Security Research

TEILEN

[2] „Threat Spotlight: Exploit Kit Goes International, Hits 150+ Countries", Cisco Talos Blog, 20. April 2016: **http://blog.talosintel.com/2016/04/nuclear-exposed.html**.

Exploit-Kit versteckt sich hinter dem Tor-Netz

Exploit-Kit-Entwickler sind äußerst kreativ dabei, ihre Tarnung zu verbessern, wie sich jüngst etwa bei Nuclear zeigte. Das Exploit-Kit, das normalerweise unterschiedliche Ransomware-Spielarten ausliefert, übertrug in diesem Fall eine Variante der Software für das anonyme Tor-Netz. Mit dieser Taktik wird versucht, die schädlichen Datenpakete zu anonymisieren und dadurch die Nachverfolgung der Aktivitäten zu erschweren.

Wenn ein Exploit-Kit einen Schadcode ausliefert, kann dieser über den Command-and-Control-Verkehr der Malware aufgespürt werden. In diesem Fall lieferte Nuclear jedoch zunächst eine ausführbare Tor-Datei aus und initiierte erst dann die Kommunikation über Tor. Da Tor ein Routing-Protokoll mit „End-to-Exit"-Verschlüsselung nutzt, ist keine Erkennung der Aktivitäten der Malware innerhalb des Tor-Netzes möglich.

Die Auslieferung von Ransomware über Exploit-Kits gehört mittlerweile zu einer der einträglichsten Strategien von Cyberkriminellen (siehe „Ransomware: Eine kaum abzustellende Geldmaschine" auf **Seite 7**). Daher überrascht es wenig, dass Ransomware-Entwickler daran arbeiten, die Effektivität ihrer Malware zu steigern – und ihren „Marktpreis" gegenüber anderen Exploit-Kits zu erhöhen. Und dafür erweist sich die Nutzung des Tor-Netzes durch Nuclear als cleverer Schachzug.

Weitere Informationen zu diesem Thema finden Sie im **Blog-Beitrag von Cisco Talos**.

ANGREIFER ERWEITERN IHRE KAMPAGNEN AUF DIE SERVERSEITE

Cyberkriminelle versuchen immer, den maximalen Profit aus ihren Kampagnen zu schlagen. So ist die Auslieferung von Malware oder Exploit-Kits an Clients oder Endnutzer für sie zwar eine effektive, in ihrer Durchschlagskraft aber begrenzte Methode, da Client-seitig sowohl die Bandbreite als auch die Ressourcen begrenzt sind, die die Angreifer kapern können.

Mit der Serverseite haben sie nun jedoch eine noch potenzialstärkere Startrampe gefunden, um ihre Kampagnen zu Geld zu machen. So wurde die Ransomware-Variante SamSam jüngst über Netzwerke verbreitet, in die Cyberkriminelle über die Anwendungsplattform JBoss einbrachen (siehe **Seite 7**). Im genannten Fall – der Angriff richtete sich gegen Vertreter des Gesundheitswesens – nutzten sie dazu JexBoss, ein Open-Source-Tool, mit dem Sicherheitslücken in JBoss-Anwendungsservern aufgespürt und ausgenutzt werden können. Nachdem sie sich so Zugang zu den Netzwerken verschafft hatten, schritten sie dann mit SamSam zur Verschlüsselung von Windows-Dateien.

Mit der Verbreitung von Ransomware über Sicherheitslücken in Servern nimmt diese ohnehin schon enorme Bedrohung eine neue Dimension an. So haben unsere Forscher bei einer Untersuchung zahlreiche mit dem Internet verbundene Systeme gefunden, die bereits kompromittiert und für die Auslieferung einer Ransomware-Payload bereit waren. Daneben stellten die Forscher fest, dass ca. 1.600 IP-Adressen bereits mit rund 2.000 passenden Backdoors ausgestattet waren. Betroffen waren hierbei in erster Linie Server, auf denen eine gängige Software für die Verwaltung von Schulbibliotheken im Einsatz war. Cisco informierte den Hersteller der Software über das Problem, der daraufhin umgehend einen entsprechenden Patch veröffentlichte.

Sicherheitslücken auf der Serverseite sind eine riesige Spielwiese für Cyberkriminelle, und die Eingrenzung und Behebung derartiger Kompromittierungen ist mit einem enormen Zeit- und Arbeitsaufwand verbunden. Client-seitige Anwendungen wie Webbrowser werden mittlerweile immer häufiger durch automatische Updates gepatcht und bieten daher weniger Angriffsfläche.

Serverseitige Anwendungen leiden dagegen unter chronischer Überalterung. Dies hängt einerseits damit zusammen, dass IT-Teams oft nur begrenzte Zeit für Patches und Upgrades haben und andererseits, dass Serversysteme in der Regel nur schwer aktualisiert werden können, ohne den laufenden Betrieb zu beeinträchtigen. Hinzu kommt ein durchlässiger Netzwerkperimeter: Angreifer verschaffen sich genau über die Ebene Zugriff auf Server, die eigentlich deren Schutz gewährleisten sollte.

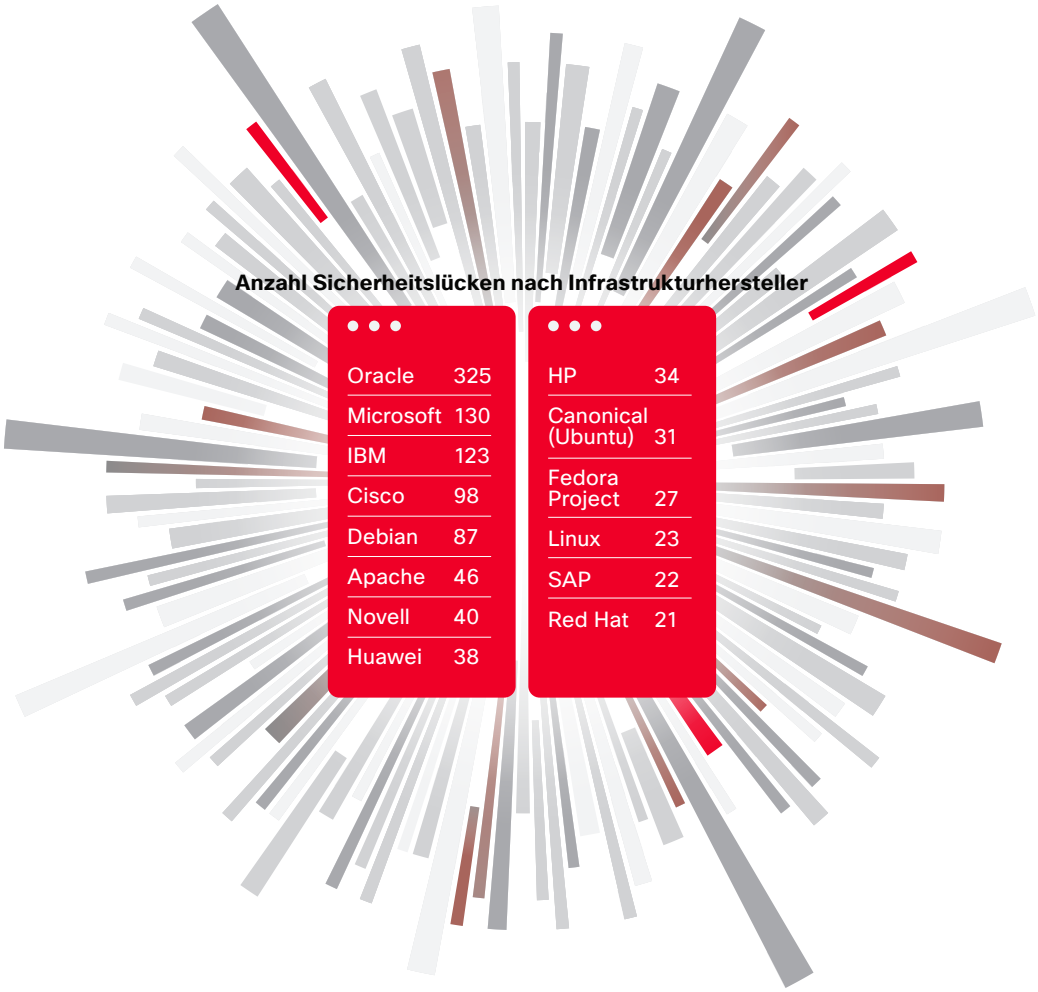
Wie Abbildung 4 zeigt, weisen viele Produkte namhafter Infrastrukturhersteller Sicherheitslücken auf, die sowohl client- als auch serverseitige Anwendungen betreffen.

Weitere Details zu den Gefahren von Sicherheitslücken in Serverlösungen können Sie in den folgenden Blog-Beiträgen von Cisco Talos nachlesen:

„Widespread JBoss Backdoors a Major Threat“

„SamSam: The Doctor Will See You, After He Pays the Ransom“

Abbildung 4: Sicherheitslücken nach Infrastrukturhersteller, 1. Januar bis 30. März 2016



Quelle: Cisco Security Research

JBOSS: ANGREIFBARE INFRASTRUKTUR BRINGT ZEITGEWINN FÜR KRIMINELLE OPERATIONEN

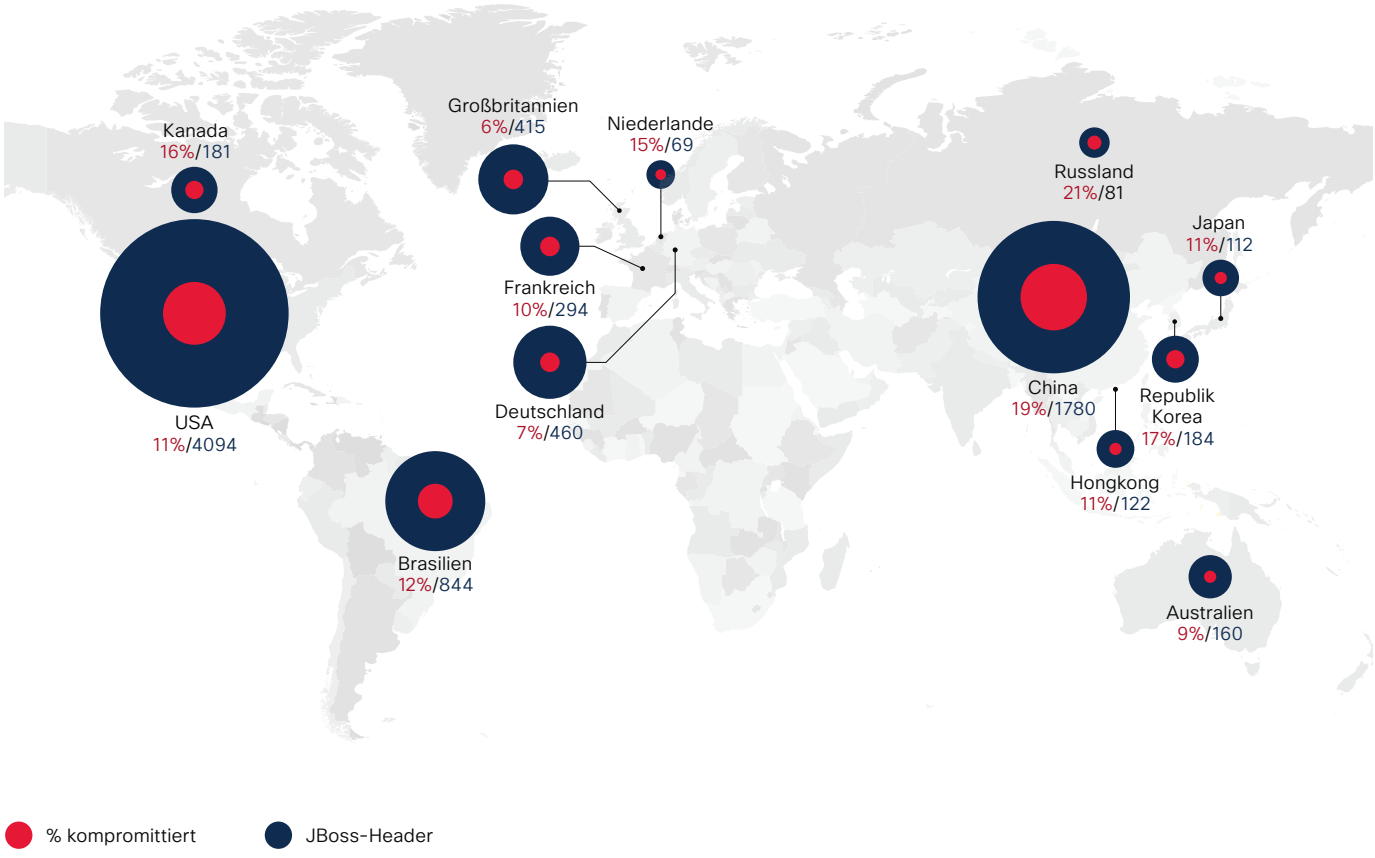
Ransomware-Entwickler haben in der JBoss-Anwendungssoftware ein leistungsfähiges Werkzeug für die Unterstützung ihrer Kampagnen gefunden. So nutzten Cyberkriminelle bei einem Ransomware-Angriff auf Gesundheitsdienstleister (siehe **Seite 7**) Sicherheitslücken in JBoss, um in Netze einzubrechen und von dort aus seelenruhig Daten zu sammeln und Malware zu verbreiten. Mangelhafte Wartung von Netzwerken war auch hier wieder die Ursache für im Grunde leicht vermeidbare Angriffe.

Unsere Forscher fanden heraus, dass durch Kompromittierungen über JBoss-Sicherheitslücken bereits erhebliche Einfallstore auf Servern entstanden sind. Zu dieser Erkenntnis gelangten sie wie folgt:

- Suche nach Internetservern, deren HTTP-Header oder Seiteninhalte eine JBoss-Installation erkennen lassen
- Durchsuchung der Hosts nach verschiedenen Backdoors, Webshells oder anderen Kompromittierungen auf Dateien mit der Endung .jsp

Abbildung 5 zeigt den Anteil der kompromittierten Server im Vergleich zur Gesamtzahl der Server mit JBoss-Installation. So wurden z. B. in den USA bei elf Prozent der untersuchten Webshells Anzeichen einer Kompromittierung festgestellt.

Abbildung 5: Webshells deuten auf JBoss-Kompromittierungen hin



Quelle: Cisco Security Research

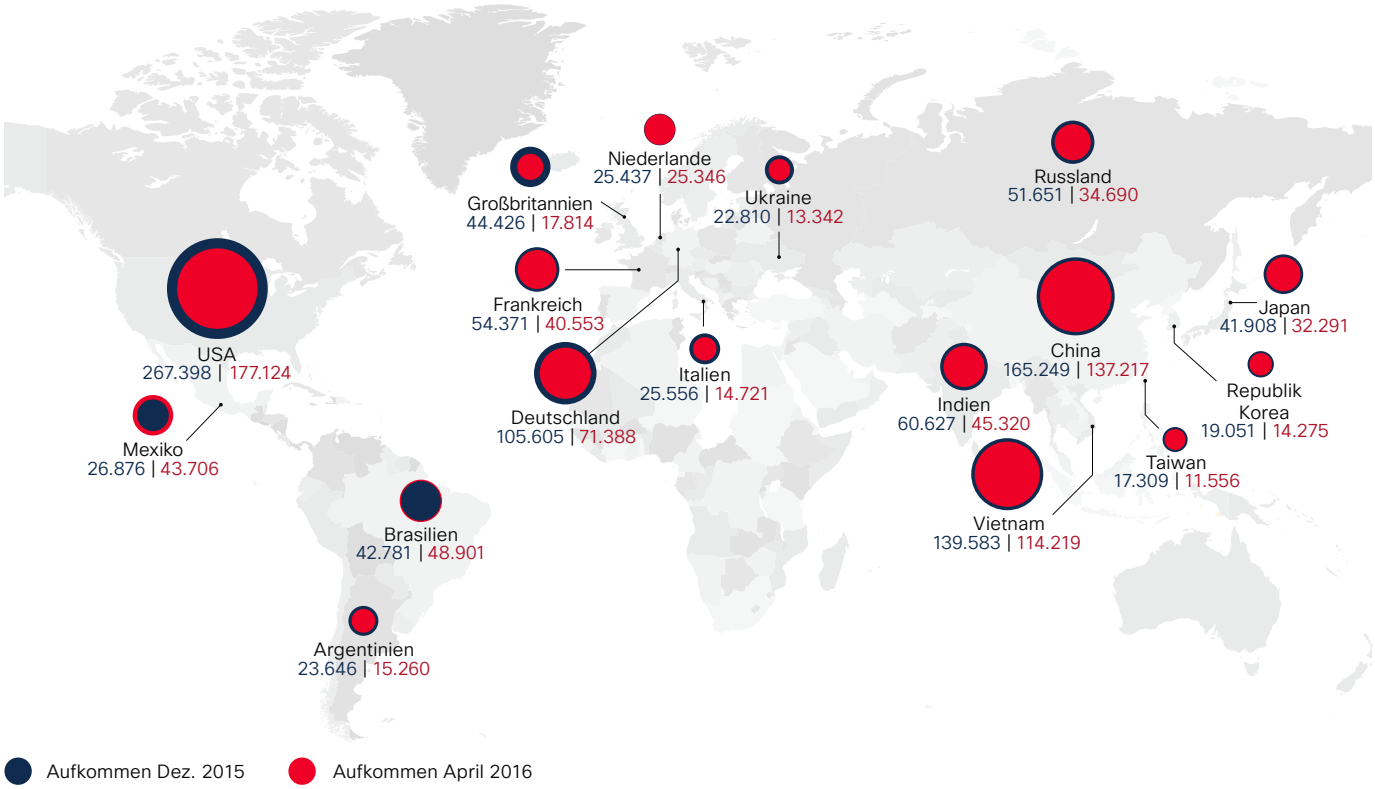
WELTWEITES SPAM-AUFKOMMEN BLEIBT RELATIV KONSTANT

Für die Ermittlung des weltweiten Spam-Traffics erfassen wir Stichproben aus unseren E-Mail-Appliances, die den Effekt von Appliance- und Gateway-Richtlinien z. B. im Hinblick auf blockierte oder als unbekannt markierte Nachrichten anzeigen. Spam-E-Mails dienen häufig als Angriffsvektor, insbesondere für Ransomware.

Unsere Untersuchung des E-Mail-Verkehrs zwischen Dezember 2015 und Mai 2016 zeigt ein relativ konstantes Spam-Aufkommen (Abbildung 6). In Brasilien waren im Januar und März 2016 Ausschläge zu verzeichnen, was vermutlich auf ein in diesen Monaten aktives Spam-Botnet zurückzuführen ist.

Wie auf **Seite 47** (Abschnitt „Blockierung von Web-Angriffen: Regionaler Überblick“) näher ausgeführt, verlagern Angreifer ihre Operationen häufig zwischen verschiedenen Ländern und Hosting-Providern, je nachdem, wo sie die günstigen Bedingungen für ihre Kampagnen vorfinden. Spammer nutzen Botnet-Server, die bei für sie zuverlässigen Hosts untergebracht sind und von diesen verwaltet werden. Wird ein Botnet-Server von einem Erkennungssystem aufgespürt, wechseln sie einfach zum nächsten.

Abbildung 6: Spam-Aufkommen nach Land, Dezember 2015 bis Mai 2016



Quelle: Cisco Security Research

TEILEN

Abbildung 7: Weit verbreitete Social-Engineering-Themen in Spam-Nachrichten

Anzahl Versionen	URL	Nachrichteninhalt	Sprache	Veröffentlichung (GMT)
95	RuleID4626	Rechnung, Zahlung	Englisch, Deutsch	3.18.16
82	RuleID4400KVR	Bestellung	Deutsch	2.1.16
64	RuleID4626(cont)	Rechnung, Zahlung, Versandbestätigung	Deutsch, Englisch, Spanisch	1.28.16
62	RuleID4961KVR	Zahlung, Überweisung, Bestellung, Versand	Deutsch	3.25.16
58	RuleID4961KVR	Angebotsanfrage, Produktbestellung	Deutsch, Englisch, mehrere Sprachen	1.25.16
52	RuleID5118KVR	Produktbestellung, Zahlung	Englisch, Deutsch	3.17.16
49	RuleID858KVR	Versandaufstellung, Zahlung	Deutsch	3.14.16
47	RuleID4961	Überweisung, Versand, Rechnung	Deutsch, Englisch, Spanisch	2.22.16
44	RuleID4627 und RuleID4627KVR	Flugticket	Deutsch	3.29.16
30	RuleID8337KVR	Bestellung, Zahlung, Kostenvoranschlag	Deutsch	1.21.16

Quelle: Cisco Security Research

Spam-Autoren versuchen weiterhin, Nutzer mit geschicktem Social-Engineering dazu zu verleiten, schädliche Anhänge (z. B. mit Malware infizierte PDF-Dateien, siehe **Seite 15**) oder Links in den Nachrichten zu öffnen. Wie Abbildung 7 zeigt, geben die Spam-Nachrichten z. B. vor, wichtige Informationen wie Rechnungen, Reisedokumente oder Angebote zu enthalten. Häufig erstellen sie die Nachrichten zudem in mehreren Sprachen, um mehr Opfer zu erreichen.

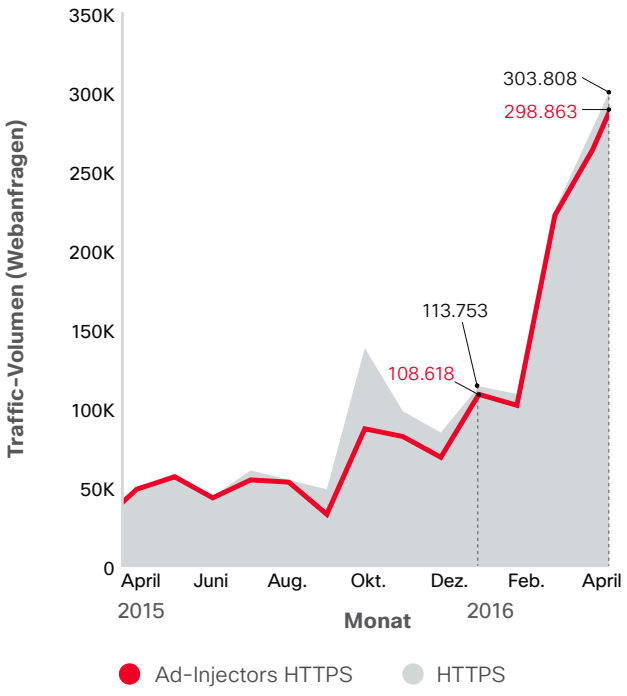
DIE RÜCKKEHR DER BLACKLISTS? UMSTIEG DER ANGREIFER AUF HTTPS MACHT UNTERSUCHUNGEN UNGLEICH SCHWERER

Verschlüsseln Ad-Injectors bösartige Werbung via HTTPS, können Nutzer und Sicherheitsteams nicht mehr anhand der URL-Informationen feststellen, ob es sich um eine potenzielle Bedrohung handelt. Das machen sich mittlerweile deutlich mehr Angreifer zunutze, um ihre Web-Aktivitäten zu verbergen und mehr Zeit für ihre Operationen zu gewinnen.

Zwischen September 2015 und März 2016 wurde ein fünffacher Anstieg von schädlichen Aktivitäten im Zusammenhang mit HTTPS-Datenverkehr registriert, wie unsere 16-monatige Untersuchung von 80 Malware-Kampagnen in acht Bedrohungskategorien ergab. Zurückzuführen ist diese Zunahme des HTTPS-Datenverkehrs in erster Linie auf Ad-Injectors und Adware (Abbildung 8).

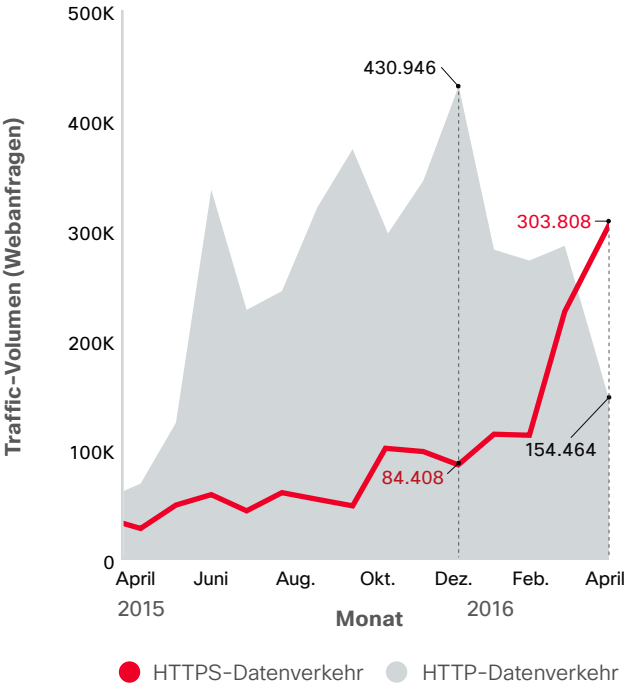
Zwischen Dezember 2015 und April 2016 wurde bei von Ad-Injectors generiertem HTTPS-Verkehr sogar ein Anstieg um 300 Prozent verzeichnet (Abbildung 9).

Abbildung 8: Ad-Injectors sind maßgeblicher Faktor für die Zunahme des HTTPS-Traffics



Quelle: Cisco Security Research

Abbildung 9: Von Ad-Injectors generierter HTTPS-Traffic stieg innerhalb von 4 Monaten um 300 Prozent



Quelle: Cisco Security Research

Bösartige Ad-Injectors gehören zu den Hauptverantwortlichen für Adware-Infektionen (Abbildung 10). Cyberkriminelle vergrößern mit diesen Browsererweiterungen die Reichweite von Ransomware- und andere Malware-Kampagnen. Dies geschieht, indem der Ad-Injector bösartige Werbung auf den vom Nutzer aufgerufenen Webseiten einschleust und ihn mit schädlichen Pop-up-Einblendungen überhäuft. Das Problem dabei: Malvertising und bösartige Ad-Injectors bewegen sich in einem Bereich des Werbe-Ökosystems, in dem sich legitimes und schädliches Verhalten nur schwer unterscheiden lassen.

Infektionen mit Ad-Injectors und Adware sollten auf keinen Fall ignoriert werden. Denn über Adware können auch Schadprogramme ausgeliefert werden, wie dies etwa mit einer neuen Version des Trojaners „DNSChanger“ der Fall ist, die unsere Sicherheitsforscher dieses Jahr entdeckt haben. Diese Entwicklung macht deutlich: Das Gefahrenpotenzial von Ad-Injector- oder Adware-Infektionen wird für Einzelnutzer ebenso wie für Unternehmen immer größer.[3]

Ebenfalls im Kommen: Die Übertragung von Malware über HTTPS. Diese Entwicklung vollzieht sich zwar bislang noch langsamer als bei Ad-Injectors, doch dies hängt vermutlich mit dem Profitgedanken der Angreifer zusammen: Infrastrukturänderungen werden nur dann vorgenommen, wenn dafür eine unbedingte Notwendigkeit besteht.

Cyberkriminelle sind jedoch nicht die einzigen, die Infrastrukturaktualisierungen eher zögerlich angehen. Ironischerweise beobachten wir den gleichen Trend auch in der rechtskonformen Geschäftswelt: Viele Unternehmen haben Patches für bekannte Sicherheitslücken in ihrer Internet-Infrastruktur oft jahrelang vor sich hergeschoben, da sie fürchteten, dass ihnen durch die Upgrade-bedingten Ausfallzeiten ihrer Hard- und Software Gewinne entgehen könnten (siehe „Veraltete Infrastruktur: Ausbreitung von Ransomware macht das Schließen seit Langem bestehender Sicherheitslücken unabdingbar“ auf **Seite 30**). Sicher haben Angreifer ihre bestehenden Technologien aber auch einfach aus dem Grund noch im Einsatz, weil sie wissen, wie aufwändig das Patchen großer Zahlen von infizierten Hosts ist.

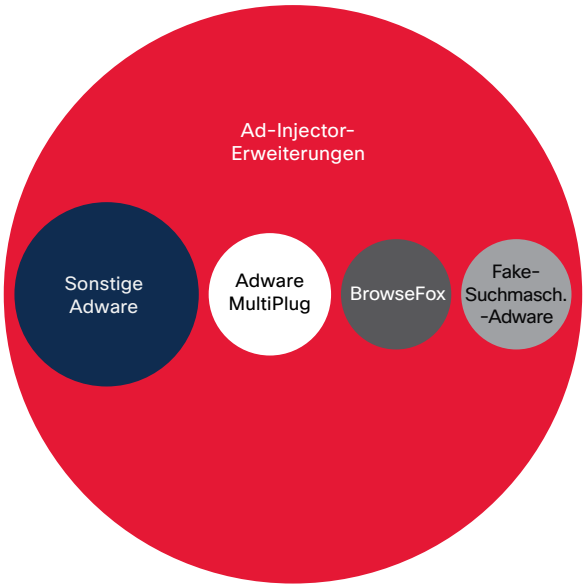
Im Verlauf unserer 16-monatigen Analyse stellten wir einen Anstieg der HTTPS-Nutzung bei folgenden Malware-Familien fest:

- Gamarue/Andromeda – ein Mehrzweck-Botnet
- Necurs – ein für Identitätsdiebstahl genutztes Botnet
- Miuref/Boaxxe – ein für Klickbetrug genutztes Botnet
- Ramdo/Redyms – ein ebenfalls für Klickbetrug genutztes Botnet
- Für die Ausschleusung von Daten konzipierte Trojaner

Die Zunahme des durch schädliche Aktivitäten generierten HTTPS-Datenverkehrs gibt Grund zur Sorge, denn für Sicherheitsforscher gestaltet sich die Verfolgung und Analyse der auf diese Art verschlüsselten Malware-Kampagnen deutlich schwieriger. So können etwa Techniken wie die in IDS für HTTP-Traffic verwendete signaturbasierte Bedrohungserkennung anhand von URL-Mustern nur auf HTTPS angewendet werden, wenn diese durch Funktionen zur SSL-Analyse ergänzt werden. In vielen Fällen haben Sicherheitsforscher zudem lediglich einen Domain-Namen oder eine IP-Adresse als Ausgangspunkt, an dem sie für ihre Untersuchungen ansetzen können.

Die Kategorisierung von Bedrohungen gestaltet sich ebenfalls schwierig, da diese häufig gemeinsam genutzte Infrastrukturen verwenden. Als Ausweichstrategie kämen hier zwar Blacklists (Listen mit sämtlicher bekannter Malware) in Frage, doch diese sind fehleranfällig und ineffektiv, da nicht präzise genug. Hinzu kommt ein hoher Zeitaufwand, denn Analysten müssen Bedrohungen bei dieser Methode manuell untersuchen und kategorisieren.

Abbildung 10: Ad-Injectors sind eines der zentralen Vehikel für Adware-Infektionen



Quelle: Cisco Security Research

[3] „DNSChanger Outbreak Linked to Adware Install Base“, Cisco Security Blog, Februar 2016: **http://blogs.cisco.com/security/dnschanger-outbreak-linked-to-adware-install-base**.

MALVERTISING-AS-A-SERVICE: HOCHGRADIG EFFIZIENTE AUSBREITUNG VON INFEKTIONEN

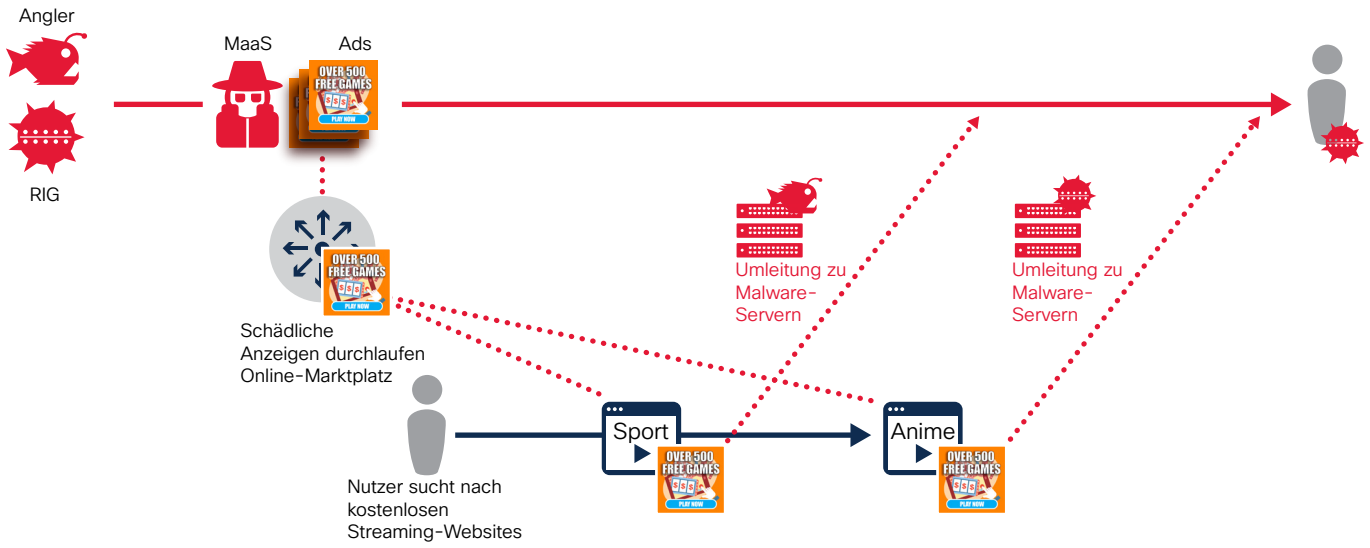
Werbeanbieter dienen, ob wissentlich oder nicht, als Vehikel für die Verbreitung von bösartiger Online-Werbung – und ermöglichen damit ein neues Geschäftsmodell für Cyberkriminelle: „Malvertising-as-a-Service". Dabei kaufen die Kriminellen Werbeplätze auf populären legitimen Webseiten, über die sie die schädlichen Anzeigen einschleusen – ein Umstand, der nicht nur neue Herausforderungen hinsichtlich der Abwehr bedeutet. Er wirft auch die Frage auf, wer für den Schutz der Endnutzer vor Malvertising verantwortlich ist.

Der Kauf von legitimen Werbeplätzen bietet Angreifern eine äußerst einfache Möglichkeit, Bedrohungen auf unterschiedlichste Websites auszubreiten. Und da die Anzeigen immer nur sehr kurz eingeblendet werden, bleibt für Sicherheitsexperten kaum Zeit, überhaupt eine Bedrohung festzustellen. Zudem passen Werbeanbieter die Einblendung von Anzeigen auf Basis von Informationen wie Browsertyp und -version an die jeweilige Zielgruppe an. Das bedeutet, die Kriminellen können bestimmte Nutzergruppen noch gezielter, z. B. in ihrer Sprache, anvisieren.

Malvertising-as-a-Service ist in gewisser Wese vergleichbar mit dem sogenannten Domain-Squatting, bei dem Domain-Namen verkauft oder besetzt werden, die Nutzer normalerweise mit legitimen Unternehmen und bekannten Marken verbinden. Über diese Domains leiten die Akteure die Nutzer an infizierte Websites weiter, an der Auslieferung der Malware selbst sind sie jedoch nicht direkt beteiligt.

Ad-Blocker sind eine logische Abwehrstrategie gegen Malvertising, insbesondere gegen die neuesten Varianten, die Systeme ohne jegliche Interaktion mit dem Nutzer infizieren und ihre Payload ausliefern können. Anbieter von Online-Inhalten finanzieren sich jedoch in erster Linie durch Werbeanzeigen. Einige der führenden Anbieter machen ihre Inhalte daher nur für Nutzer anzeigbar, die den Ad-Blocker für ihre Seite deaktivieren. Für die Nutzer ist dies ein Risiko, für Sicherheitsteams ein Dilemma. Denn nun müssen sie abwägen, ob sie Websites sperren, die Werbeanzeigen aus Online-Marktplätzen ausliefern.

Abbildung 11: Funktionsweise von Malvertising-as-a-Service (MaaS)



Quelle: Cisco Security Research

Weiterleitung auf unterschiedlichsten Ebenen

Wie bereits ausgeführt, kaufen Cyberkriminelle Werbeplätze, auf denen sie schädliche Anzeigen schalten. Die Infektion der Nutzer erfolgt dabei entweder direkt oder durch Weiterleitung an eine andere Website, über die die Malware-Payload ausgeliefert wird. Häufig erfolgt die Weiterleitung über mehrere Ebenen. Zudem wurden Fälle registriert, bei denen die Nutzer noch nicht einmal mit der schädlichen Werbeanzeige interagieren mussten, um sich die Infektion einzufangen. Der gesamte Vorgang erfolgte dabei im Hintergrund, weit abseits des Bildschirms.

Bei einer erstmals im Oktober 2015 beobachteten Malvertising-as-a-Service-Kampagne wurden die Nutzer zu verschiedenen Exploit-Kits weitergeleitet, darunter Angler und RIG. Diese lieferten unterschiedliche Payloads aus, in vielen Fällen Varianten von Ransomware wie TeslaCrypt oder CryptoWall. Infiziert wurden die Nutzer über eine schädliche Anzeige, die sich als die Werbung einer Glücksspiel-Website ausgab. Der Code hinter der Anzeige beinhaltete einen Link zu JavaScript, der den Nutzer auf eine mit Angler infizierte Landing-Page leitete. Der Code enthielt jedoch auch andere Weiterleitungen, z. B. iFrames.

Weitere Informationen zu Malvertising-as-a-Service (MaaS) finden Sie im folgenden Blog-Beitrag von Cisco Talos:

„Threat Spotlight: Spin to Win ... Malware“

Diese neue Methode zur Verbreitung von Malvertising zeigt ein weiteres Mal: Cyberkriminalität nimmt in der Schattenwirtschaft immer mehr die Züge eines „Industriezweigs“ an. Malvertising-as-a-Service wird dabei voraussichtlich in Zukunft eine noch größere Rolle spielen. Denn sicher wollen künftig mehr Cyberkriminelle diese Methode nutzen, um auf effiziente und unauffällige Weise große Nutzerzahlen über legitime Websites zu infizieren. Malvertising ist eines der zentralen Vehikel für die Verbreitung von Ransomware, dem von Cyberkriminellen aufgrund seines für sie enormen Gewinnpotenzials zunehmend bevorzugt eingesetzten Malware-Typ. (siehe „Ransomware: Eine kaum abzustellende Geldmaschine“ auf **Seite 7**).

„Malvertising-as-a-Service wird in Zukunft voraussichtlich eine noch größere Rolle spielen. Denn sicher wollen künftig mehr Cyberkriminelle diese Methode nutzen, um auf effiziente und unauffällige Weise große Nutzerzahlen über legitime Websites zu infizieren.“

WEB-ANGRIFFSMETHODEN: ALLE HEBEL STEHEN AUF RANSOMWARE

Einige Trends bei den Web-Angriffsmethoden stehen in der ersten Jahreshälfte 2016 im Zusammenhang mit der explosionsartigen Zunahme von Ransomware-Angriffen. Verdächtige Windows-Binärdateien etwa stehen in der Liste in Abbildung 12 ganz oben und werden verwendet, um z. B. Spyware oder Adware auszuliefern. Mit diesen Tools nisten sie sich in Netzwerkinfrastrukturen ein und starten von dort aus z. B. Angriffe mit Ransomware.

Facebook-Scams (Social-Engineering), Trojaner und iFrames sind weiterhin beliebte Mittel der Angreifer, um auf die Computer von Webnutzern und in Unternehmensnetzwerke zu gelangen.

Wie in unserem letzten Security Report ausgeführt, waren Facebook-Scams in der zweiten Jahreshälfte 2015 noch die am häufigsten verwendete Web-Angriffsmethode, während Windows-Binärdateien noch auf Platz 4 lagen. JavaScript-Malware hatte damals noch ganze drei Plätze belegt, ist jedoch in der aktuellen Top-10 überhaupt nicht mehr vertreten.

Das bedeutet jedoch keinesfalls, dass dieser Malware-Typ von der Bildfläche verschwunden ist. JavaScript-Malware war im Gegenteil sogar eine maßgebliche Komponente zahlreicher Ransomware-Kampagnen in diesem Jahr.

In Abbildung 13 sind die weniger häufig anzutreffenden Malware-Typen aufgeführt, die aber vermutlich tiefer in der Infektionskette verborgen liegen.

Im langen Ausläufer des Spektrums in Abbildung 13 sind dann auch Typen wie Ransomware-Signaturen, Trojaner und Dropper angesiedelt. Mit der wachsenden Beliebtheit von Ransomware bei Angreifern sind zudem auch die für die Erpresserkampagnen benötigten Infrastrukturkomponenten häufiger anzutreffen als etwa Malware für den Identitätsdiebstahl.

Abbildung 12: Am häufigsten registrierte Malware

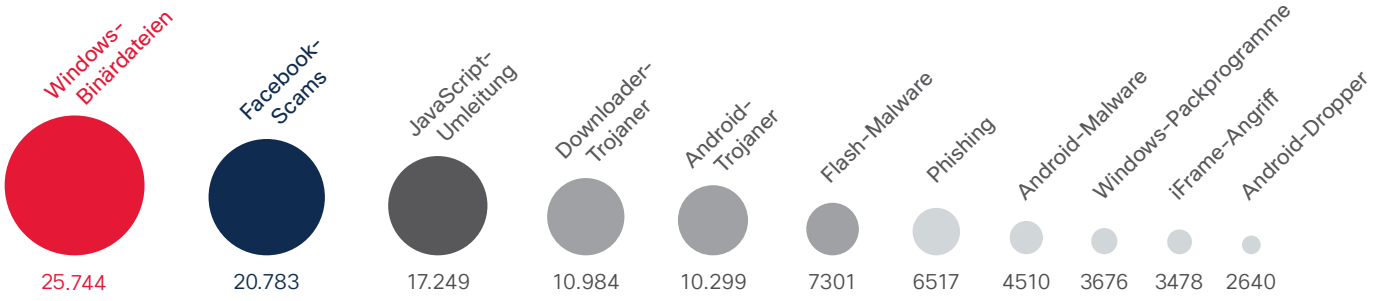
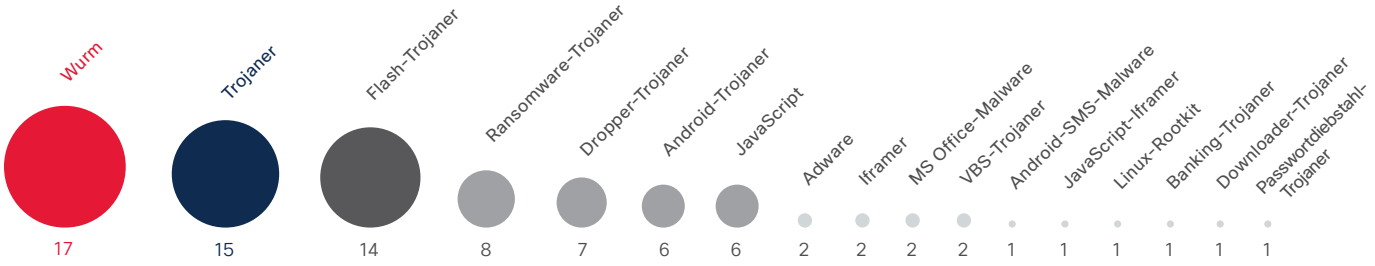


Abbildung 13: Weniger häufig registrierte Malware (Auszug)



Quelle: Cisco Security Research

Zeit zum Absichern

Zeit zum Absichern

Immer neue Innovationen werden im Kampf gegen Cyberkriminelle ins Feld geführt. Die der digitalen Wirtschaft zugrundeliegende Infrastruktur bleibt aber – als Folge unangemessener Sicherheitsverfahren – weiterhin anfällig. Denn die meisten Unternehmen haben ein Sammelsurium aus verschiedensten Webbrowsern, Anwendungen und Infrastrukturelementen im Einsatz, die Angreifern zahlreiche Eintrittswege bieten.

Zumeist nur unzureichend geschützt, eröffnet diese Hard- und Software Räume für kriminelle Operationen. Es gilt, diese Räume bestmöglich zu schließen und die Erkennung von Angreifern zu verbessern. Dies müssen die Top-Prioritäten in der IT-Sicherheit sein.

Sicherheitsrisiko Patching-Lücke: Trotz schneller Verfügbarkeit werden Sicherheitsupdates nicht rechtzeitig installiert

Viele der namhaften Hersteller zeigen sich in den letzten Jahren proaktiver und bringen nach Bekanntwerden von Sicherheitslücken und Exploits schneller entsprechende Patches heraus und arbeiten zudem mit den Sicherheitsforschern zusammen, die diese Lücken entdecken. Tatsächlich betrug die mittlere Zeit von der Veröffentlichung einer Sicherheitslücke bis zur Verfügbarkeit eines Patches, für deren Ermittlung wir Tausende der in den Common Vulnerabilities and Exposures (CVE) dokumentierten Sicherheitslücken untersuchten, bei den großen Softwareherstellern Null Tage. Mit anderen Worten: Ein entsprechender Patch ist bereits zu dem Zeitpunkt verfügbar, an dem die Sicherheitslücke öffentlich bekannt gegeben wird – die Hersteller gehen also auch koordiniert bei der Veröffentlichung vor.

Trotz ihrer schnellen Verfügbarkeit installieren viele Nutzer die Patches jedoch nicht rechtzeitig. Dadurch lassen diese Nutzer das Zeitfenster offen, in dem Angreifer Exploits gegen sie ausführen können – und geben ihnen damit Zeit für Operationen im Netzwerk, die sich bereits durch einen simplen Softwarepatch verhindern ließen. Unter Umständen fahren Angreifer zudem bereits Exploits gegen eine Sicherheitslücke, bevor diese überhaupt öffentlich bekannt gegeben wurde. Für die Abwehr ist es daher unabdingbar, das Zeitfenster zwischen Verfügbarkeit und Installation von Patches zu schließen.

Die Hersteller haben dazu verschiedene Formen von Auto-Update-Funktionalitäten in ihre Produkte integriert, die von periodischen Checks mit Nutzerbenachrichtigung bis hin zu Updates reichen, die nach entsprechender Festlegung im Hintergrund ausgeführt werden und nutzerseitig zunehmend schwer zu deaktivieren sind.

Je nachdem, wie das Verfahren für die automatischen Updates geregelt ist, kann der Nutzer das Update auf einen späteren Zeitpunkt verschieben oder bei manchen Produkten auch komplett überspringen. Eine Untersuchung bezüglich der auf den Endgeräten unserer Kunden installierten Browser-Versionen macht die Vorteile von automatischen Updates deutlich. So hatte bei Google Chrome, bei dem die Deaktivierung der Auto-Updates starken Regelungen unterliegt, die Mehrheit der Nutzer (60 bis 85 Prozent, mit der Stärke der Update-Regelung zunehmend) die neueste Version des Browsers im Einsatz.

Im schlimmsten Fall waren es 75 bis 80 Prozent der Nutzer, die entweder die neueste Version installiert hatten oder eine Version hinterher waren (Abbildung 14). Google macht es zunehmend schwerer, Chrome in einer veralteten Version auf dem System zu halten: Die automatischen Updates lassen sich nur mit Administratorrechten deaktivieren, und der Hersteller bietet auf seiner Website keine älteren Versionen des Browsers zum Download an und untersagt dies auch auf anderen Webseiten.

Die Verfügbarkeit von Auto-Updates allein hat wenig Einfluss darauf, welche Versionen eingesetzt werden. Es kommt darauf an, wie diese geregelt sind. Jede der von uns untersuchten Software beinhaltete ein bestimmtes Auto-Update-System, von Pop-up-Nachrichten zur Update-Verfügbarkeit bis hin zu Updates, die automatisch im Hintergrund ausgeführt und nutzerseitig nur mit großem Aufwand deaktiviert werden können. Je strikter die Update-Regelung, desto stärker tritt das gewünschte Verhalten zutage.

Abbildung 14: Chrome-Installationen nach Version (obere 50% der Nutzer)

Hinweis: Die Time-to-Patch-Diagramme zeigen die Ergebnisse für die oberen 50 Prozent der untersuchten Nutzer. Durch Hervorhebung einer einfachen Mehrheit der Nutzer lässt sich leichter feststellen, ob Updates wie geplant durchgeführt werden oder ob weiterreichende Herausforderungen bestehen.

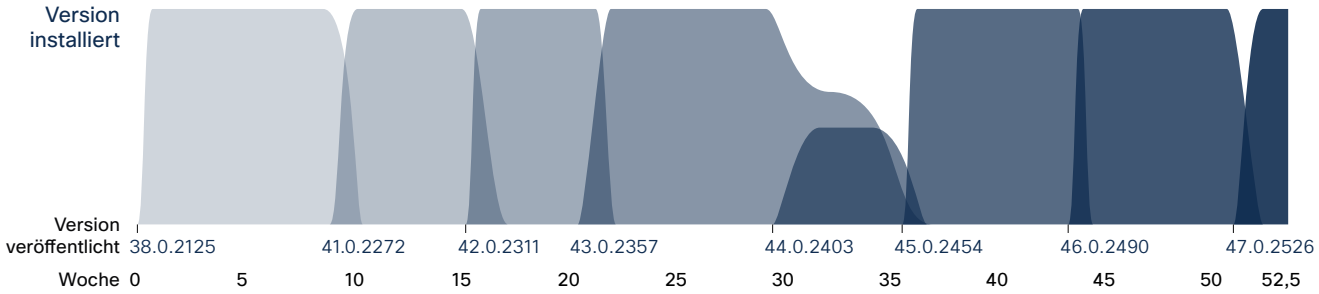


Abbildung 15: Java-Installationen nach Version (obere 50% der Nutzer)

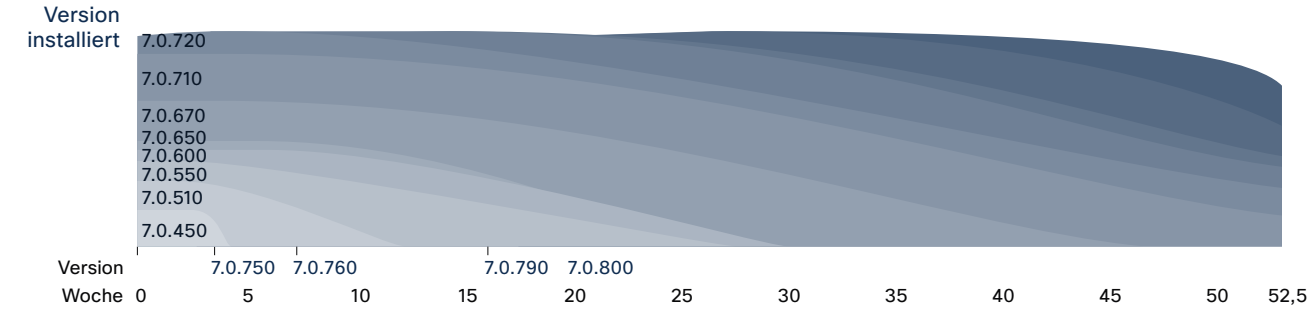
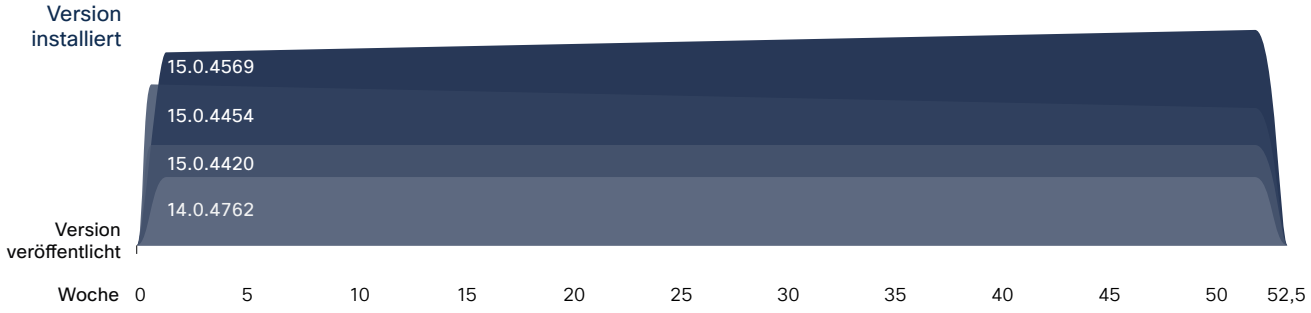


Abbildung 16: Microsoft Office-Installationen nach Version (obere 50% der Nutzer)



Quelle: Cisco Security Research

Betrachtet man andere Software als Browser, so werden die Auswirkungen mangelhafter Regelungen für Auto-Updates deutlich. Bei der Untersuchung der auf den Endgeräten unserer Kunden installierten Java-Software (Abbildung 15 auf der vorherigen Seite) fanden unsere Forscher sogar Indicators-of-Compromise (IOC): Ein Drittel der Systeme hatte noch Java SE 6 am Laufen, eine Version die Oracle derzeit einstellt; die aktuelle Version ist SE 10. (Die genauen Zahlen lagen zu Beginn der 1-jährigen Untersuchung bei 33 Prozent, zum Ende bei 23 Prozent.)

Hinzu kommt, dass bei vielen Nutzern u. U. neben der aktuellen noch alte Java-Versionen laufen, da sie diese entweder für bestimmte Software benötigen oder einfach noch nicht deinstalliert haben. Somit wären also noch immer Versionen mit bekannten Sicherheitslücken vorhanden, über die ihre Systeme angreifbar sind. Andere Abwehrmaßnahmen, z. B. Intrusion-Prevention-Systeme, bieten hier zwar einen gewissen Schutz für die Nutzer, sind jedoch keine Garantie. Fehlt es am Endpunkt zudem an weiteren Schutzmaßnahmen, ist die Gefahr sogar noch größer.

Bei unserer Untersuchung der installierten Versionen von Microsoft Office (Abbildung 16 auf der vorherigen Seite) wurde deutlich, wie schwierig sich die Verwaltung dieser Suite für Unternehmen gestaltet. Auto-Update-Funktionalität ist – zwar in schwacher Ausführung – auch in dieser Suite vorhanden, das Gros der Anwender verwendet aber eine bestimmte Version und bleibt auch bei dieser. Fallen für Upgrades zudem Kosten für Lizenzen oder IT-Support an, oder gibt es vonseiten der Nutzer Vorbehalte, dass zusammen mit den Sicherheitsupdates auch Änderungen ihrer gewohnten Funktionen ausgeliefert werden, gestaltet sich das bei Produktivitätstools ohnehin schon komplizierte Patch-Management zusätzlich schwieriger.

Während des Untersuchungszeitraums waren vier Hauptversionen von Office verfügbar, von denen die neueste Version jedoch in den wenigsten Fällen übernommen wurde. Unter den drei am weitesten verbreiteten Hauptversionen lag die Verteilung der Prozentwerte in etwa bei 28-52-20, mit leichtem Anstieg im Verlauf eines Jahres. Upgrades auf neue Hauptversionen erfordern eine Lizenz, geringfügige Updates einer bestehenden Hauptversion sind jedoch Teil des normalen Software-Wartungszyklus. Nun wäre zu erwarten, dass die Mehrheit der Nutzer einer bestimmten Hauptversion das jeweils neueste Service-Pack installiert hat. Bei der neuesten Version (Office 2013/Version 15.x) waren die drei wichtigsten Sicherheitsupdates, nach denen wir die Unterscheidung vornahmen, jedoch beinahe gleichstark vertreten.

Unter dem Strich lässt sich also festhalten: Viele der namhaften Hersteller zeigen sich engagiert bezüglich der Sicherheit ihrer Produkte, indem sie Warnmeldungen, Korrekturen und Notfallpatches zeitnah herausgeben. Die Endnutzer allerdings schenken dem Patching ihrer Software insgesamt zu wenig Beachtung – und gefährden damit sowohl ihre eigene als auch die Sicherheit ihres Unternehmens.

Für Sicherheitsverantwortliche gilt es daher, nicht nur für eine schnelle Installation veröffentlichter Patches zu sorgen, sondern auch zu prüfen, inwieweit sie mit der Hilfe von Auto-Update-Funktionalitäten ein zeitnahes Patching gewährleisten können. Sicher ist diese Strategie nicht auf alle Systeme gleich gut anwendbar. Browser-Updates etwa lassen sich auf Endgeräten mit minimalen Auswirkungen durchführen. Die Aktualisierung von Unternehmensanwendungen und serverseitigen Infrastrukturelementen gestaltet sich dagegen deutlich schwieriger und kann sich zudem auf die Geschäftskontinuität auswirken. Dementsprechend werden diese häufig seltener aktualisiert. Sicherheitsverantwortliche müssen Updates und Patches daher an den Stellen priorisieren, an denen diese optimal zum Schutz ihrer Netzwerke vor bekannten und offensichtlichen Bedrohungen beitragen.

Problematisch ist zudem, dass Sicherheitsupdates häufig auch funktionale Anpassungen beinhalten. Die Nutzer stehen Updates daher oft skeptisch gegenüber, da sie keine Änderungen an ihren gewohnten Funktionen wünschen. Für die Hersteller wiederum erhöhen sich mit den zahlreichen Versionen im Umlauf der Support-Aufwand und die Komplexität.

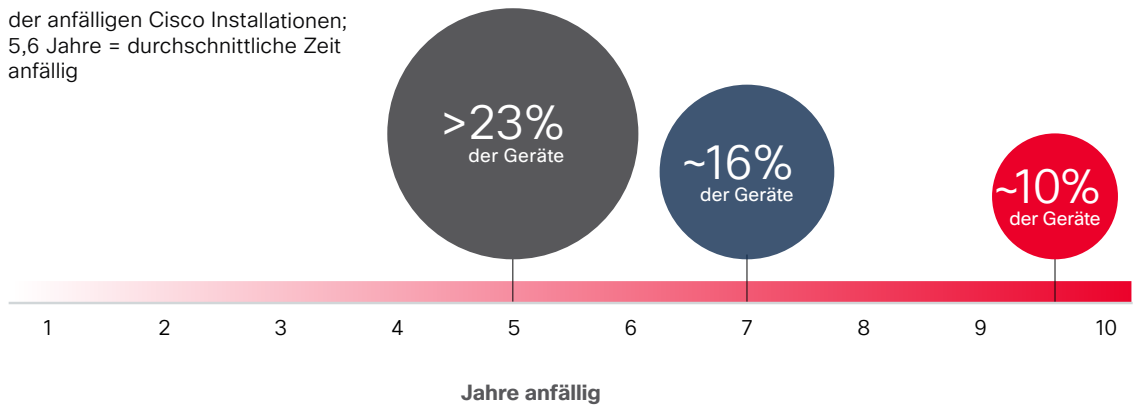
Veraltete Infrastruktur: Ausbreitung von Ransomware macht das Schließen seit Langem bestehender Sicherheitslücken unabdingbar

Vergangenes Jahr haben wir 115.000 Cisco Geräte untersucht, um auf die Risiken von unzureichend gepflegter, veralteter Infrastruktur und nicht behobener Sicherheitslücken in Betriebssystemen aufmerksam zu machen.[4] 106.000 dieser Geräte (92 Prozent) verwendeten Software mit bekannten Sicherheitslücken.

Für den vorliegenden Report haben wir bei einer Stichprobe von Cisco Geräten untersucht, wie weit auf diesen zentralen Infrastrukturelementen (Router und Switches) vorhandene bekannte Sicherheitslücken zurückdatieren. Insgesamt stellten wir bei 103.121 an das Internet angebundenen Geräten bekannte CVEs aus den Jahren 2002 bis 2016 fest. Jedes Gerät wies dabei im Schnitt 28 bekannte Sicherheitslücken auf.

Im Durchschnitt waren bei dieser Stichprobe seit 5,6 Jahren bekannte Sicherheitslücken vorhanden. Bei mehr als 23 Prozent der Geräte datierten die Sicherheitslücken bis ins Jahr 2011 zurück, bei knapp 16 Prozent bis ins Jahr 2009. Und beinahe 10 Prozent wiesen bekannte Sicherheitslücken auf, die bereits vor mehr als 10 Jahren veröffentlicht wurden (Abbildung 17).

Abbildung 17: Geräte mit bekannten Sicherheitslücken nach Alter (in Prozent)

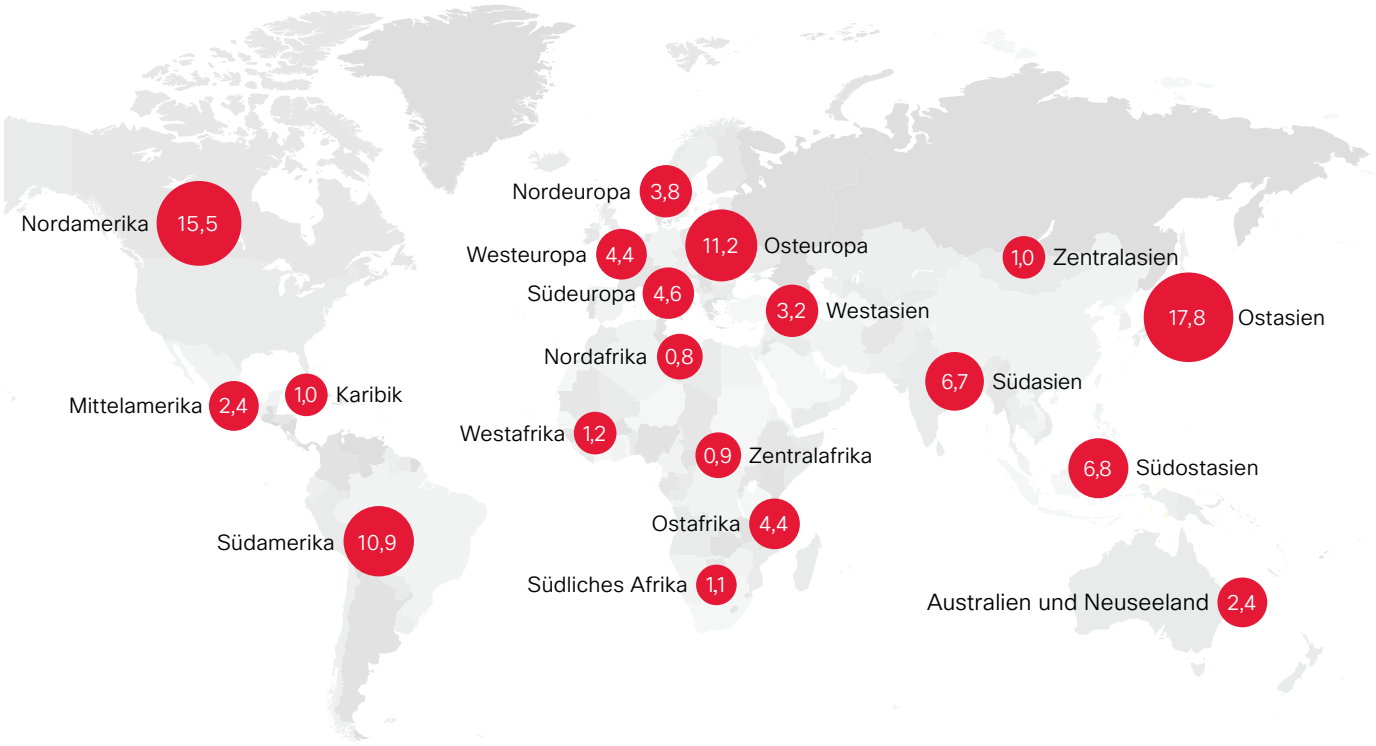


Quelle: Cisco Security Research

TEILEN

[4] Cisco hat die 115.000 Geräte aus dieser eintägigen Stichprobe mittels Internet-Scan identifiziert und mit Blick von „außen nach innen“ (vom Internet aus und in das Unternehmen hinein) untersucht. Weitere Informationen hierzu finden Sie im Cisco Annual Security Report 2016 unter **cisco.com/go/msr2015**.

Abbildung 18: Anfällige Cisco Geräte nach Region (in Prozent)



Quelle: Cisco Security Research

Mit 17,8 bzw. 15,5 Prozent war in Ostasien und Nordamerika der Anteil an angreifbaren Cisco Geräten am größten. (siehe Abbildung 18).

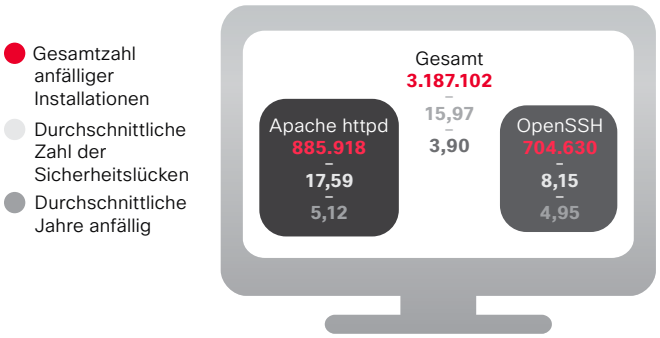
Kaum vergleichbar: Ausmaß der Verbreitung anfälliger Softwareinfrastruktur

Um zu ermitteln, ob Unternehmen beim Patching ihrer Softwareinfrastruktur vielleicht sorgfältiger vorgehen, untersuchten wir weit verbreitete Produkte dieser Art auf bekannte Sicherheitslücken (Abbildung 19). Bei über drei Millionen Installationen wurden Sicherheitslücken festgestellt. Zu finden waren diese bei zahlreichen unterschiedlichen Produkten, größtenteils jedoch bei Apache httpd (885.918) und OpenSSH (704.630). Im Gesamtdurchschnitt ergaben sich pro installiertem Softwareprodukt knapp 16 bekannte Sicherheitslücken.

Im Schnitt war die von den Unternehmen eingesetzte Webserver-Software seit 3,9 Jahren über bekannte Sicherheitslücken angreifbar.

Im regionalen Vergleich wiesen Nordamerika, Westeuropa und Osteuropa die höchsten Zahlen an anfälligen Softwareinstallationen auf (Abbildung 20).

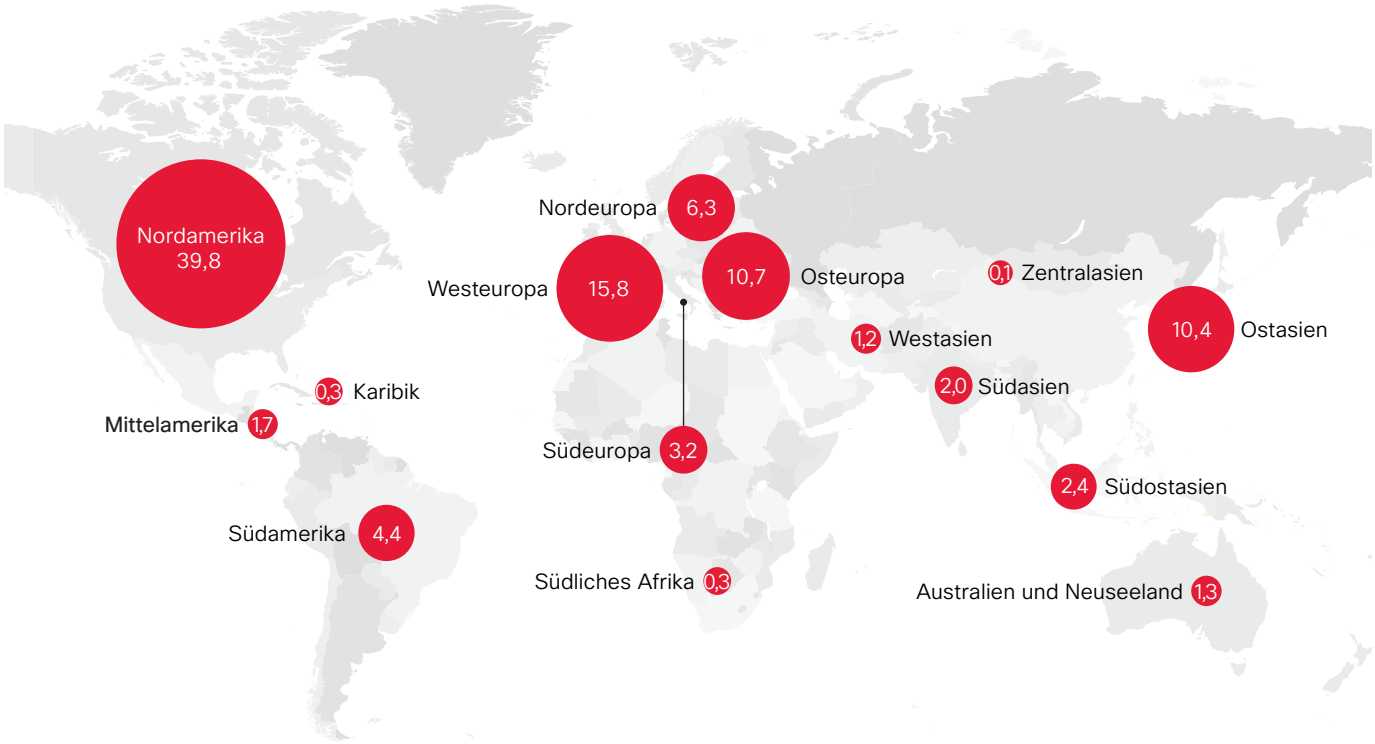
Abbildung 19: Anzahl der anfälligen Software-Installationen nach Produkt



Quelle: Cisco Security Research

TEILEN

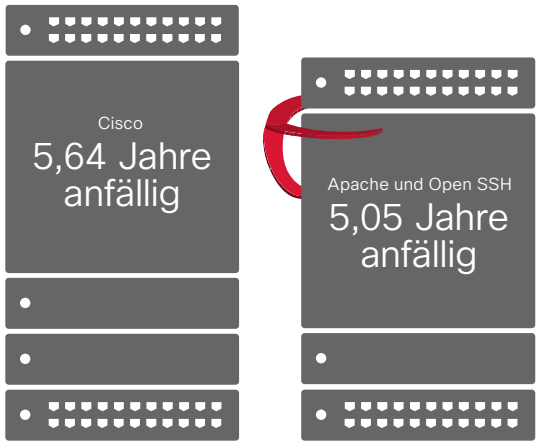
Abbildung 20: Anfällige Software-Installationen nach Region (in Prozent)



Quelle: Cisco Security Research

Vergleicht man die Zahlen für die Produkte von Cisco, Apache und OpenSSH, zeigt sich zudem, dass Unternehmen die Installation von Patches für bekannte Sicherheitslücken bei keiner dieser Produktgruppen sonderlich sorgsam angehen (Abbildung 21). Viele Unternehmen sparen sich lieber die Mühe und warten ab, bis sie ihre Infrastruktur ersetzen. Wieder andere schieben Upgrades zu lange vor sich her und stellen dann fest, dass der Support für ihre Produkte bereits eingestellt wurde und somit auch keine Aktualisierung mehr möglich ist. So ergab unsere Analyse, dass jedes dieser Produkte im Schnitt seit 5 Jahren mit bekannten Sicherheitslücken im Einsatz war.

Abbildung 21: Softwarepflege im Überblick: Cisco im Vergleich zu Apache und OpenSSH



Quelle: Cisco Security Research

Wer jetzt nicht handelt, hat später das Nachsehen

Auch wenn Upgrades der Infrastruktur mitunter zeitaufwändig und teuer sind – wenn Unternehmen es versäumen, die erforderlichen Aktualisierungen vorzunehmen, öffnen sie ihre Pforten für Cyberkriminelle. Denn die jüngste Kampagne mit der Ransomware SamSam (siehe **Seite 7**) belegt: Kriminelle nehmen seit Langem bestehende, bekannte Sicherheitslücken gezielt mit Angriffen ins Visier, die jeden Unvorbereiteten lahmlegen und teuer zu stehen kommen können (siehe „JBoss: Angreifbare Infrastruktur bringt Zeitgewinn für kriminelle Operationen“ auf **Seite 18**).

Unternehmen müssen insbesondere verstehen, dass jeder, der über die passenden Werkzeuge und das nötige Know-how verfügt, sich Einblick in die Produktinstallationen aus der zuvor ausgeführten Untersuchung verschaffen kann. Und dazu gehören selbstverständlich auch Kriminelle.

Unternehmen weltweit müssen der Aktualisierung überalterter Infrastruktur und Systeme daher höchste Priorität einräumen. Und das betrifft nicht nur das Schließen von bekannten Sicherheitslücken, die seit langem vor sich hin gären. Auch und vor allem geht es darum, Infrastruktur und Systeme widerstandsfähiger gegenüber Cyberangriffen zu machen. Daher gilt es, jetzt der Realität ins Auge zu blicken und sich von Produkten zu verabschieden, die herstellerseitig keinen Support mehr erhalten und nicht mehr auf den neuesten Stand der Sicherheit gebracht werden können.

Wie aus den Abbildungen 22 und 23 hervorgeht, scheint hier besonders in wirtschaftlich schwächeren sowie Entwicklungs- und Schwellenländern Nachholbedarf zu bestehen.

Abbildung 22: Regionaler Überblick: So lange waren anfällige Cisco Geräte im Schnitt im Einsatz

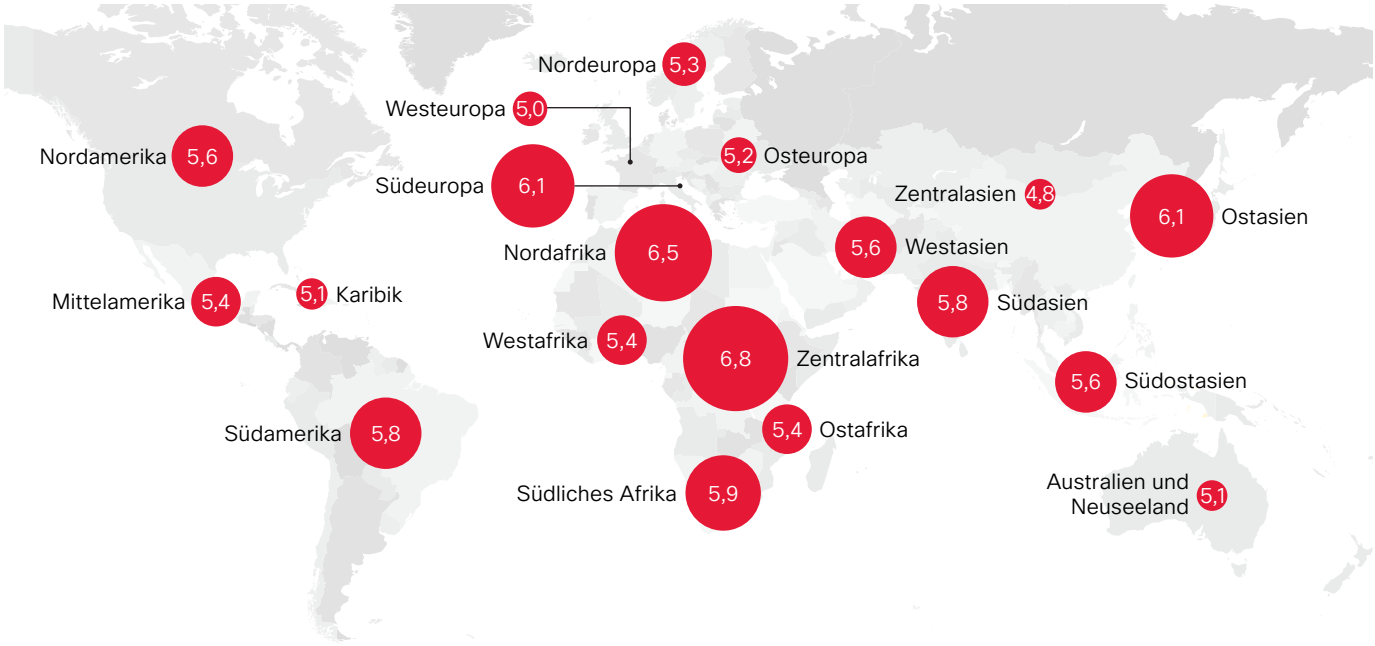
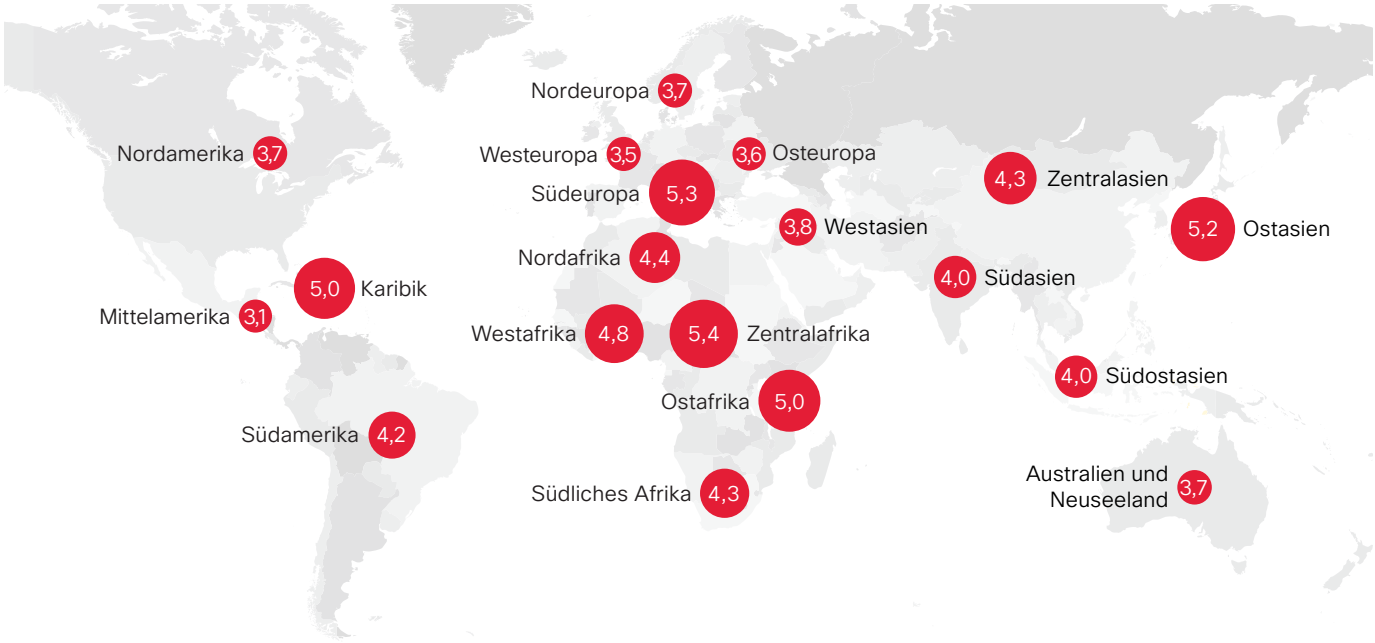


Abbildung 23: Regionaler Überblick: So lange war anfällige Serversoftware verschiedener Hersteller im Schnitt im Einsatz



Quelle: Cisco Security Research

Eine anfällige Infrastruktur kann das sichere Fundament nicht liefern, das ein Unternehmen in der immer umfassender von Digitalisierung und Internet of Things bestimmten Wirtschaft von heute und morgen braucht. Und die Potenziale dieser Trends werden Unternehmen nur dann in vollem Umfang nutzen können, wenn sie die Sicherheitsprobleme der ersten Welle der Digitalisierung in Angriff nehmen.

Zurückzuführen sind diese Probleme zumindest teilweise auf fehlende Weitsicht: Der Aspekt der Sicherheit spielte in den Anfangszeiten des Internets zunächst keine Rolle, da niemand damit gerechnet hatte, dass diese Infrastruktur einmal im Visier von Kriminellen stehen würde. Die überalterten, über bekannte Sicherheitslücken angreifbaren Infrastrukturen von heute sind jedoch ein hausgemachtes, da bewusst verschlepptes Problem. Denn statt ihre kritischen Infrastrukturen für eine Aktualisierung vorübergehend offline zu nehmen und damit ein noch kalkulierbares Risiko einzugehen, spekulieren viele lieber darauf, dass die Angreifer sie verschonen werden – eine in der heutigen Zeit doch allzu blauäugige Einstellung.

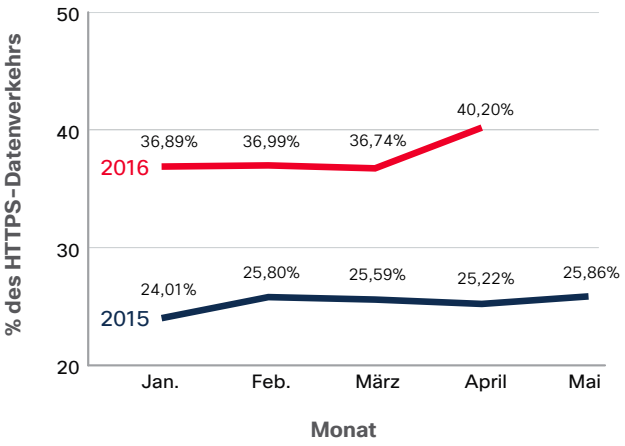
„Eine anfällige Infrastruktur kann das sichere Fundament nicht liefern, das ein Unternehmen in der immer umfassender von Digitalisierung und Internet of Things bestimmten Wirtschaft von heute und morgen braucht. Und die Potenziale dieser Trends werden Unternehmen nur dann in vollem Umfang nutzen können, wenn sie die Sicherheitsprobleme der ersten Welle der Digitalisierung in Angriff nehmen.“

Verschlüsselung: HTTPS-Datenverkehr bleibt 2016 zumindest vorerst konstant

Unternehmen setzen für den Schutz ihrer vertraulichen Daten sowie der Privatsphäre ihrer Kunden zunehmend auf Verschlüsselungsverfahren. Dies ging bereits aus unserem letzten Security Report hervor, in dem wir im Verlauf des Jahres 2015 eine allmähliche, aber signifikante Zunahme der HTTPS-Anforderungen verzeichneten. Zwischen Januar und April 2016 blieb der HTTPS-Verkehr dann aber relativ konstant.

Die bis dato festgehaltenen Zahlen zeigen in diesem Jahr zwar nur einen geringfügigen Anstieg des HTTPS-Verkehrs, in der Security-Branche rechnet man jedoch damit, dass sich der Aufwärtstrend des Vorjahres auch weiterhin fortsetzen wird (Abbildung 24).

Abbildung 24: HTTPS-Datenverkehr bleibt 2016 vorerst konstant

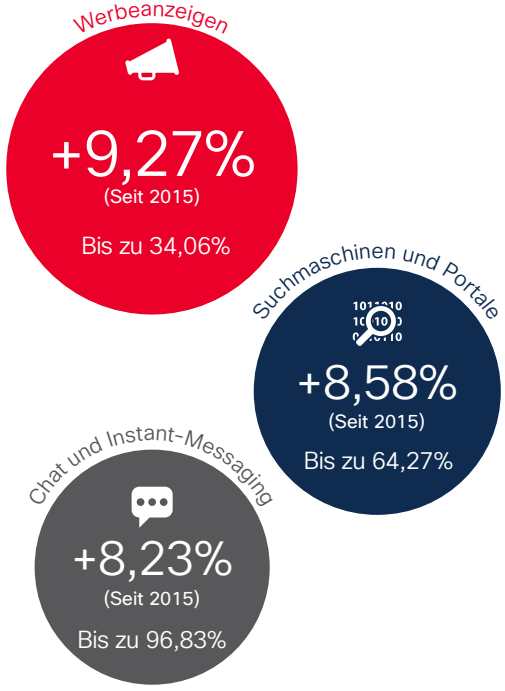


Quelle: Cisco Security Research

Eine Zunahme des HTTPS-Verkehrs war in den ersten vier Monaten dieses Jahres im Bereich der digitalen Werbung zu verzeichnen (siehe Abbildung 25). Zurückzuführen ist dies sehr wahrscheinlich auf verstärkte Anstrengungen der Branche, die Privatsphäre der Nutzer zu schützen und Malvertising zu unterbinden. Möglich ist aber auch, dass gerade Malvertising ein maßgeblicher Faktor für diesen Anstieg ist. Denn Ad-Injectors – das zentrale Vehikel für die Verbreitung von Adware-Infektionen – werden mittlerweile sehr ausgedehnt für via HTTPS verschlüsselte Malvertising-Kampagnen eingesetzt.

Am häufigsten wird HTTPS-Verschlüsselung in den folgenden drei Anwendungsbereichen verwendet: Unternehmens-E-Mail, Chat/Instant-Messaging sowie webbasierte E-Mail-Dienste (siehe Abbildung 26).

Abbildung 25: Zunahme des von Malware generierten HTTPS-Datenverkehrs, Januar 2015 bis April 2016



Quelle: Cisco Security Research

Der zunehmende Einsatz von Verschlüsselungstechniken für legale Zwecke ist für Endnutzer im Allgemeinen positiv zu bewerten. Für Sicherheitsexperten entstehen daraus jedoch neue Herausforderungen: Auch Kriminelle haben erkannt, dass sie über verschlüsselte Verbindungen ihre Aktivitäten verbergen und somit über längere Zeiträume ungestört operieren können (Näheres zum Einsatz von HTTPS durch Malware-Entwickler auf **Seite 22**). Denn Punktlösungen können Indicators-of-Compromise (IOCs) aus verschlüsselten Verbindungen nicht mehr erkennen und somit kaum noch wirksam Unterstützung dabei leisten, schädliche Aktivitäten frühzeitig aufzuspüren.

Abbildung 26: Anwendungen mit höchstem HTTPS-Volumen

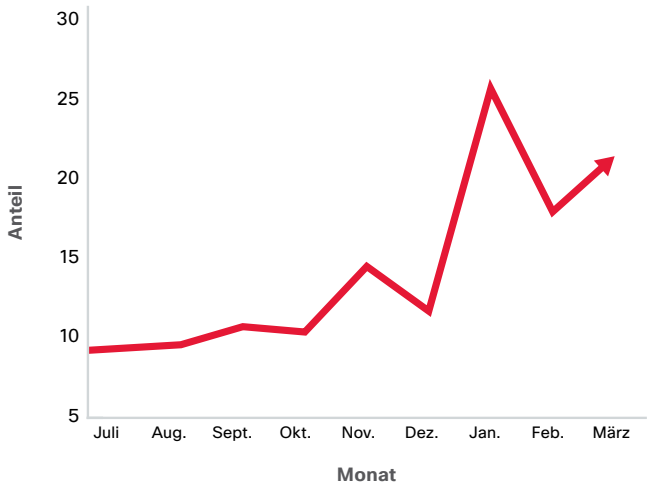
Kategorie Jan-Apr	HTTPS durchschn. in %
Unternehmens-E-Mail	97,88%
Chat und Instant-Messaging	96,83%
Webbasierte E-Mail-Dienste	96,31%
Online-Speicherung und -Backup	95,70%
Internettelefonie	95,07%
Business-Social-Networks	90,78%
Soziale Netzwerke	81,15%
Dateiübertragungsdienste	67,63%
Video-Streaming	64,71%
Suchmaschinen und Portale	64,27%
Fotosuche/Bildmaterial	61,90%
Webseiten-Übersetzung	54,60%
SaaS und B2B	54,36%

Quelle: Cisco Security Research

TLS-Verschlüsselung macht zwar die Payload, nicht aber das Verhalten einer Malware unkenntlich

Technologien, die für legale Zwecke weithin im Einsatz sind, werden oft und gerne auch von Cyberkriminellen genutzt, wenn sie ihre Tarnung damit länger aufrecht erhalten können. Transport Layer Security (TLS), ein gängiges Protokoll zur Verschlüsselung des Netzwerkverkehrs, ist hierfür ein weiteres Beispiel. So konnten unsere Forscher mittels Analyse der bei TLS nicht verschlüsselten Header-Informationen eine geringe, aber dennoch wachsende Zahl von Malware-Stichproben ermitteln, die ihre Kommunikation mithilfe von TLS abschirmte. Dies gibt Grund zur Sorge für Sicherheitsverantwortliche, denn Deep-Packet-Inspection ist als Sicherheitstool in diesem Fall wirkungslos.

Abbildung 27: Malware-Stichproben, die TLS nutzen (in Prozent)



Quelle: Cisco Security Research

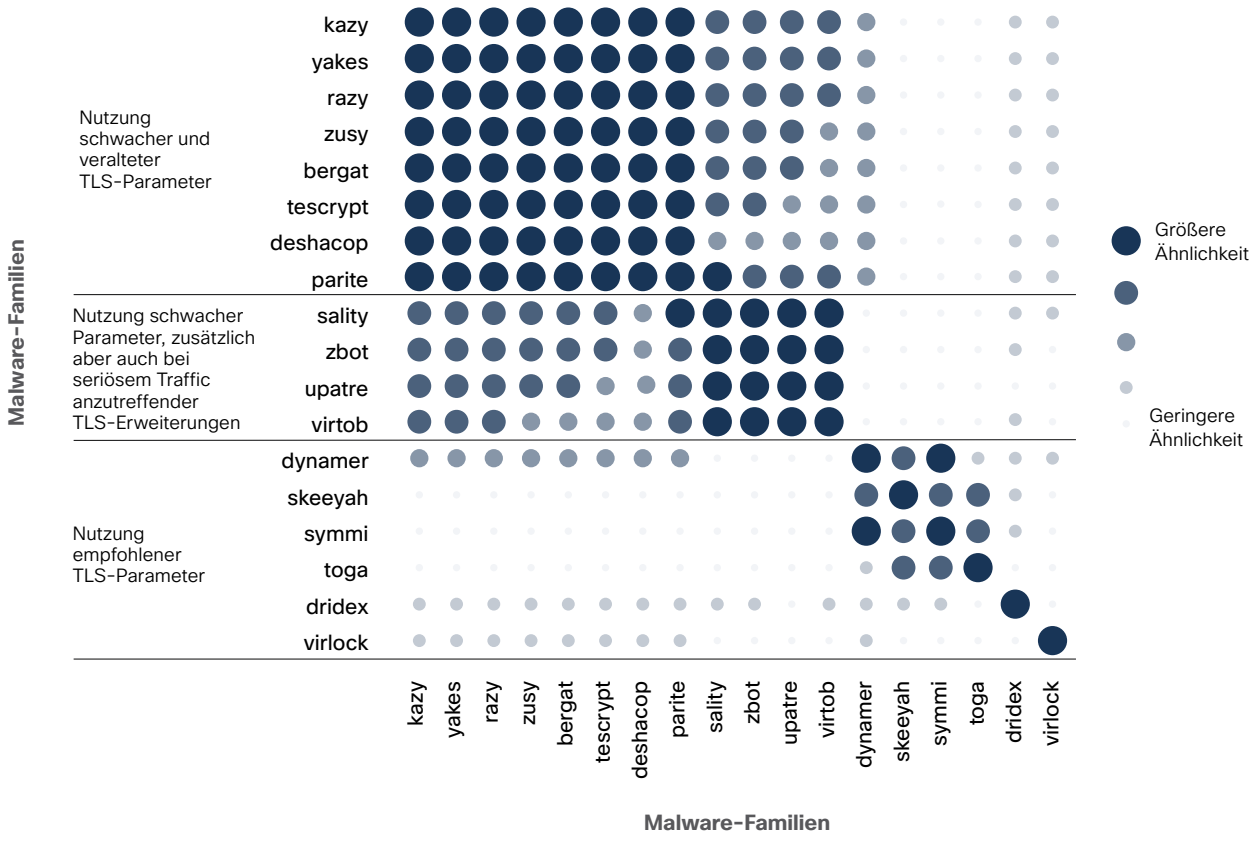
Derzeit werden unseren Forschern zufolge 60 Prozent des Netzwerkdatenverkehrs mittels TLS verschlüsselt. Von den Malware-Stichproben, die unsere Forscher untersuchten, nutzen insgesamt 10 Prozent das Protokoll. Diese Zahl mag gering erscheinen, wird aber mit der großflächigeren Nutzung von verschlüsselten Verbindungen für seriösen Datenverkehr voraussichtlich ebenfalls steigen. So wurde zwischen Juli 2015 und März 2016 bereits eine Zunahme des von Malware generierten, verschlüsselten Datenverkehrs verzeichnet (Abbildung 27).

Wie aber lässt sich Malware erkennen, die ihre Kommunikation mit TLS verschlüsselt? Wie sich zeigte, nutzt Malware TLS auf eine andere Weise als seriöse Anwendungen. Dadurch werden Muster im Datenverkehr erkennbar, die sich bei den meisten Malware-Familien mit hoher Genauigkeit klassifizieren lassen.

So fanden unsere Forscher heraus, dass Malware-Entwickler in der Regel ältere kryptografische Parameter verwenden. Weist der Datenverkehr also die Merkmale einer älteren Chiffrierungsroutine auf, kann dies auf Malware hindeuten, da seröse Anwendungen tendenziell eher die neuesten TLS-Verfahren verwenden. Dies hängt vermutlich damit zusammen, dass die Hersteller durch ein höheres Sicherheitsniveau ihrer Produkte im Wettbewerb punkten wollen.

Cyberkriminelle stützen sich dagegen eher auf ältere Kryptografie-Bibliotheken, damit ihre Schadsoftware in so vielen Umgebungen wie möglich fehlerfrei läuft. Denn ist die von ihnen verwendete Bibliothek auf dem Zielhost nicht vorhanden, kann die Malware darauf nicht ausgeführt werden.

Abbildung 28: Ähnlichkeit von Malware-Familien nach TLS-Parametern



Quelle: Cisco Security Research

Um die Muster zu bestimmen, nach denen Malware TLS einsetzt, untersuchten unsere Forscher 18 Malware-Familien, Tausende Malware-Stichproben und Zehntausende verschlüsselte Netzwerk-Flows. Daraus ergaben sich für die Malware-Familien folgende Kategorien:

- Familien, die die empfohlenen TLS-Parameter nutzen (z. B. die Malware „Skeeyah“)
- Familien, die schwache Parameter, zusätzlich aber TLS-Erweiterungen nutzen, die auch bei seriösem Datenverkehr anzutreffen sind (z. B. die Malware „Sality“)
- Familien, die schwache und veraltete Parameter nutzen (z. B. die Malware „Tescrypt“)

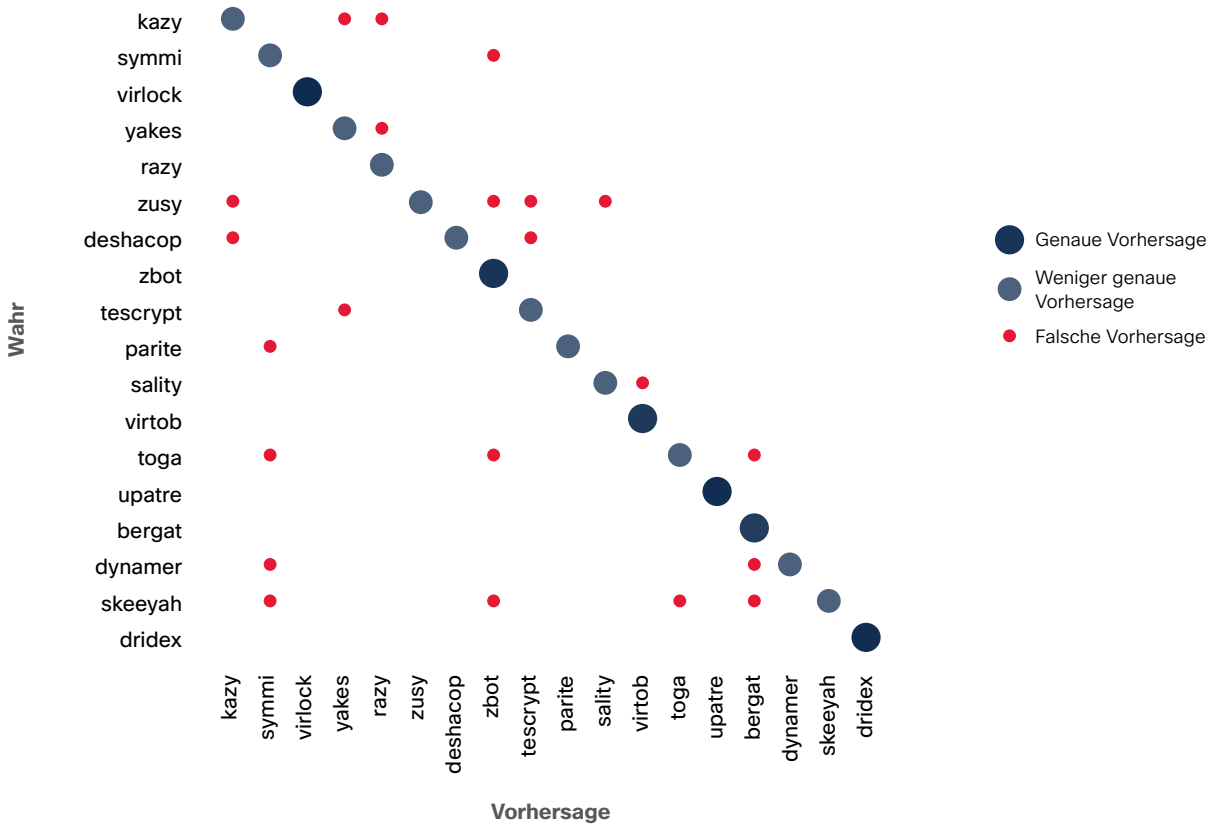
Wie in Abbildung 28 dargestellt, weisen einige Malware-Familien Gemeinsamkeiten in der Art und Weise auf, wie diese die TLS-Verschlüsselung nutzen.

Ein Blick auf die Wahrheitsmatrix in Abbildung 29 macht deutlich, wie einfach eine Unterscheidung zwischen den verschiedenen Malware-Familien möglich ist. Die Familien auf der Skala „Vorhersage“ weisen Ähnlichkeiten mit den Familien auf der Skala „Wahr“ auf (durch einen großen Punkt dargestellt); fehlerhafte Vorhersagen werden durch einen kleinen Punkt dargestellt.

Gehen Malware-Familien zu fortschrittlicheren TLS-Verfahren über, gestaltet sich die Klassifizierung logischerweise schwieriger. Unsere Forscher fanden jedoch heraus, dass die Datenverkehrsmuster durch Hinzuziehen von TLS-spezifischen Attributen (z. B. ob ein Zertifikat selbstsigniert ist) noch präziser bestimmt werden können. So waren sie z. B. in der Lage, Netzwerkkommunikationen selbst dann noch mit einer Genauigkeit von 86,8 Prozent einer spezifischen Malware-Familie zuzuordnen, wenn ihnen für die Analyse gerade einmal ein verschlüsselter Datenfluss zur Verfügung stand. Das macht deutlich: Es braucht eine integrierte Bedrohungsabwehr, die klassische Kategorisierungsverfahren durch maschinelles Lernen ergänzt. Denn erst die Kombination von maschinellem Lernen mit neuartigen Dateninterpretationsverfahren kann Sicherheitsverantwortlichen aussagekräftige Informationen zur Bedrohungslage liefern.

Die Fähigkeit, Malware genau zu einer bekannten Familie zuordnen zu können, ist enorm wertvoll für Incident-Response-Teams. Denn so sind sie in der Lage, den Typ der Bedrohung auch ohne ein Reverse-Engineering der Malware zu bestimmen. Zudem gewinnen sie durch die Überprüfung der verschlüsselten Traffic-Flows wichtige Informationen, anhand derer sie Maßnahmen gegen Malware-Infektionen effektiver nach ihrem Gefahrenpotenzial priorisieren können.

Abbildung 29: Wahrheitsmatrix: Unterscheidung zwischen Malware-Familien



Quelle: Cisco Security Research

Bedrohungs-Erkennungszeit: Ein hitziges Wettrüsten ist im Gange

Cisco definiert die Bedrohungs-Erkennungszeit (auch „Time to Detection", TTD) als die Zeitspanne vom Auftreten einer Kompromittierung bis zu deren Erkennung als Bedrohung Für die Ermittlung der TTD ziehen wir Sicherheitstelemetrie heran, die von Cisco Security-Produkten weltweit erfasst wird. Durch kontinuierliche Analysen dieser Daten können wir dann feststellen, zu welchem Zeitpunkt ein bislang unbekannter Schadcode auf einem Endgerät ausgeführt wurde, und zu welchem Zeitpunkt dieser Code als Bedrohung klassifiziert wurde.

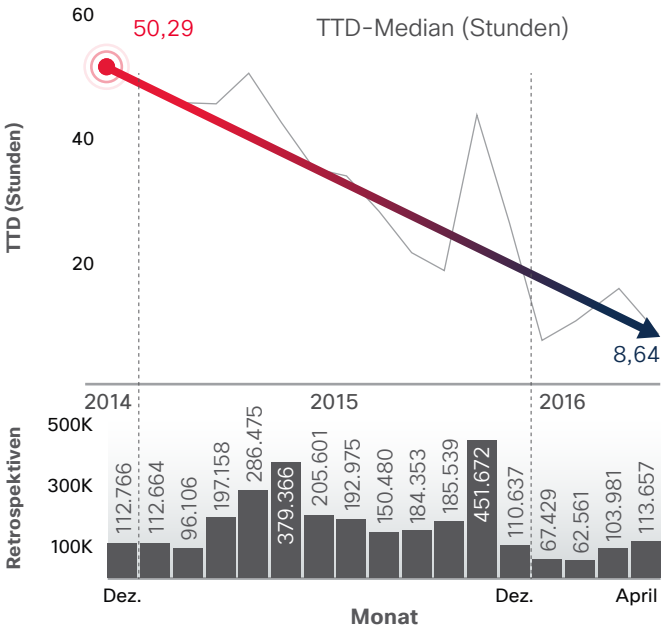
Seit Ende 2014 halten wir unsere Fortschritte bei der Verkürzung der TTD fest. Vor einem Jahr lag unser TTD-Median bei rund zwei Tagen (50 Stunden),[5] den wir aber bis Oktober 2015 bereits auf ca. 17 Stunden reduzieren konnten.

Eine sogar noch niedrigere TTD – ca. 13 Stunden – ergab sich aus dem gewichteten Durchschnitt der fünf zwischen Dezember 2015 und April 2016 gemessenen Median-Werte.

Unser TTD-Median liegt damit deutlich unter dem Branchendurchschnitt von derzeit 100 bis 200 Tagen. Wir werden aber auch weiterhin daran arbeiten, die Erkennungszeit für ein noch breiteres Spektrum an Bedrohungen zu verkürzen. Abbildung 30 zeigt die Gesamtentwicklung unserer TTD von Dezember 2014 bis April 2016.

Insgesamt zeigt die Kurve in Abbildung 30 einen stetigen Abwärtstrend, macht im Verlauf aber auch deutliche Ausschläge nach oben und unten. Daraus lässt sich das „Wettrüsten" zwischen Angreifern und Verteidigern erkennen.

Abbildung 30: TTD-Median nach Monat, Dezember 2014 bis April 2016



Quelle: Cisco Security Research

„Unser TTD-Median liegt deutlich unter dem Branchendurchschnitt von derzeit 100 bis 200 Tagen. Wir werden aber auch weiterhin daran arbeiten, die Erkennungszeit für ein noch breiteres Spektrum an Bedrohungen zu verkürzen."

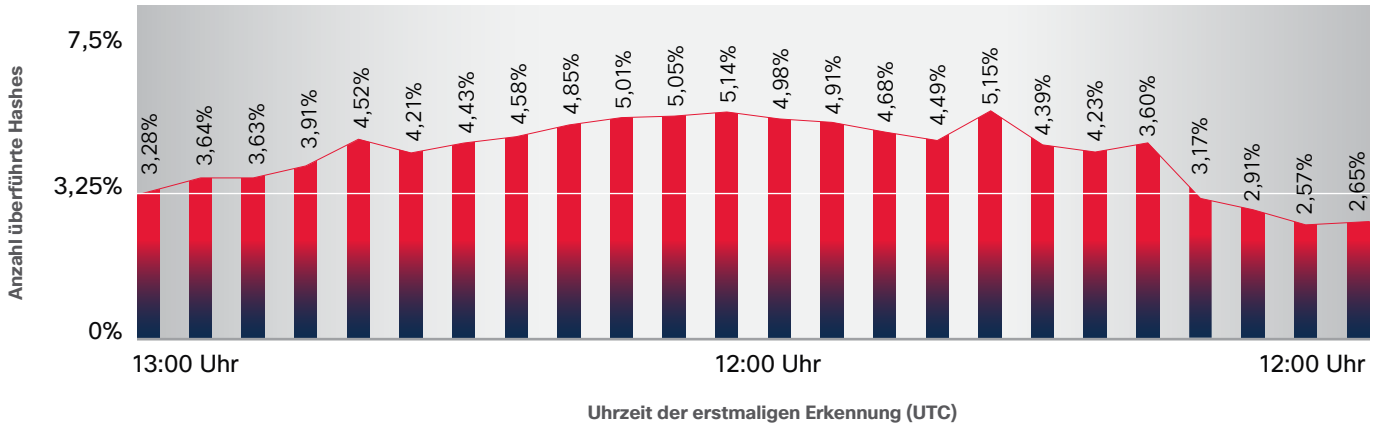
[5] Cisco Annual Security Report 2015, hier zum Download verfügbar: **cisco.com/go/msr2015**.

Angreifer entwickeln laufend neue Techniken, die ihre Tarnung verbessern. Die Security-Branche wiederum hält mit Techniken dagegen, die eine präzisere Identifizierung von IOCs ermöglichen. Diese integrieren sie dann in automatisierte Erkennungstechnologien und bereitet die Daten durch die Ergänzung von Kontext als aussagekräftige Threat-Intelligence für Kunden auf (siehe „Indicators-of-Compromise sind keine Threat-Intelligence“ auf **Seite 53**).

In den Zeiträumen, in denen die TTD deutlich nach unten ging, hatten wir die Nase vorn – wir konnten Bedrohungen schneller erkennen als die Angreifer neue Techniken entwickeln und ins Feld führen konnten. Die Ausschläge nach unten markieren das Gegenteil: In diesen Zeiträumen warteten die Angreifer mit neuen Techniken auf, die erst durch tiefergehende Analysen oder mit der Hilfe von anderen Intelligence-Quellen aufgespürt werden konnten – der TTD-Median stieg somit an.

Dieses Wettrüsten setzt sich auch weiterhin fort – mit einer Flut an neuen Bedrohungen, gegen die die Security-Branche schnell wirksame Gegenmaßnahmen finden muss. Abbildung 31 zeigt die Zahl der Hashes (Dateien), die wir im Untersuchungszeitraum (Dezember 2015 bis April 2016) für gewöhnlich pro Tag als schädlich überführten. Im Tagesverlauf blieb diese Zahl relativ konstant.

Abbildung 31: Überführte Hashes nach Tageszeit



Quelle: Cisco Security Research

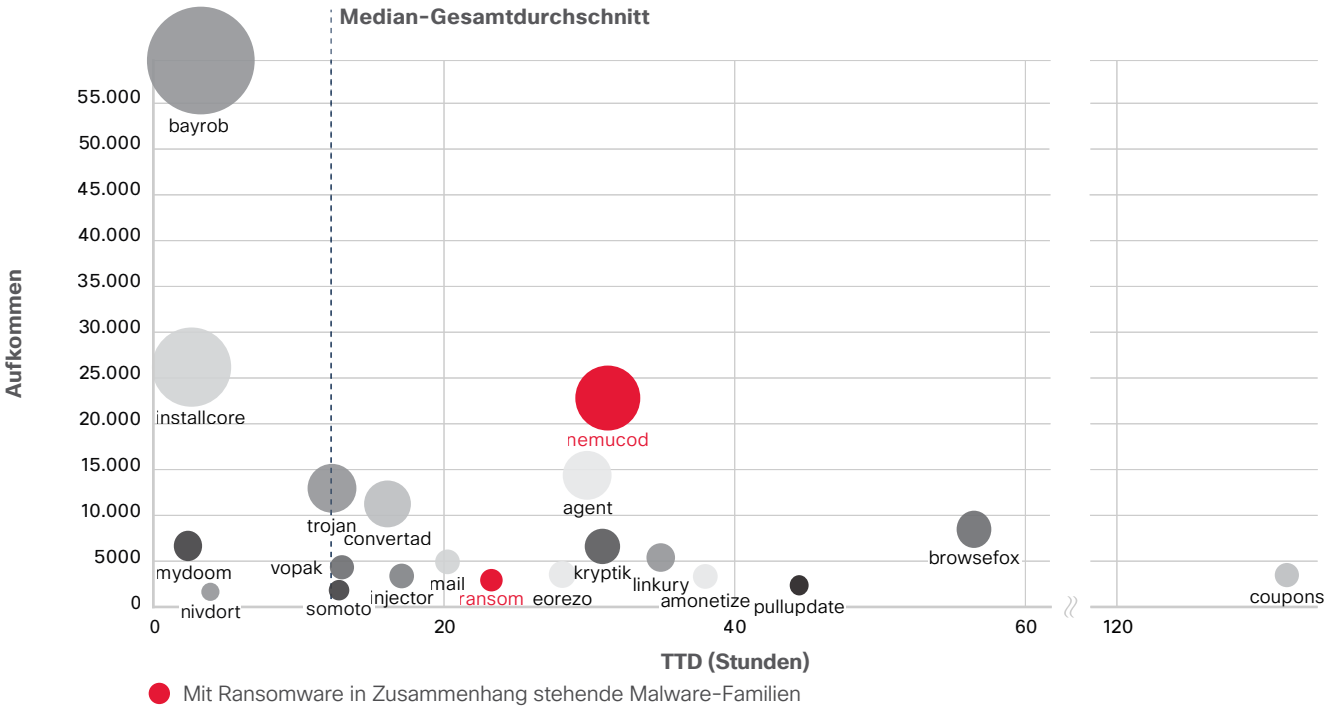
„In den Zeiträumen, in denen die TTD deutlich nach unten ging, hatten wir die Nase vorn – wir konnten Bedrohungen schneller erkennen als die Angreifer neue Techniken entwickeln und ins Feld führen konnten.“

Jüngste Schwankungen des TTD-Medians stehen mit explosionsartiger Zunahme von Ransomware in Zusammenhang

In unserem letzten Security Report haben wir bereits darauf hingewiesen: Unsere Fortschritte bei der Verkürzung der TTD seit Dezember 2014 sind zu einem nicht unerheblichen Teil auf die „Industrialisierung des Hacker-Business", also die großflächige Nutzung von Standard-Malware durch eine große Zahl von Angreifern zurückzuführen, da weiter verbreitete Bedrohungen leichter aufzuspüren sind.

Malware-Familien, die bei denen die TTD in den ersten fünf Monaten 2016 auf oder in der Nähe des Median-Werts von ca. 13 Stunden lag, gehören zu den älteren Generationen, sind aber nach wie vor weit verbreitet. Beispiele hierfür sind u. a. Bayrob, eine Botnet-Malware, die seit 2007 in Umlauf ist und Anfang dieses Jahres wieder verstärkt anzutreffen war, sowie der Computerwurm „Mydoom", der Windows-Systeme befällt und über E-Mail übertragen wird. Gesichtet wurde dieser erstmals im Jahr 2004. Ebenfalls stark vertreten war die Adware „InstallCore"; dies vermutlich aufgrund ihrer Rolle bei der Auslieferung von Ransomware (Abbildung 32).

Abbildung 32: TTD-Medianwerte für die wichtigsten Malware-Familien (obere 20 Familien nach Erkennungsrate)



Quelle: Cisco Security Research

TEILEN

Die stärkere Verbreitung – und somit vermehrte Erkennung – bestimmter Malware-Familien steht im direkten Zusammenhang mit der explosionsartigen Zunahme von Ransomware im vergangenen Jahr.

Bei einigen dieser Malware-Familien lag die TTD über dem Median, da diese nicht mittels automatisierter Techniken wie Heuristik und Sandboxing frühzeitig erkannt werden konnten. Stattdessen waren für die Erkennung zunächst eingehendere Untersuchungen durch unsere Analysten nötig. Der damit verbundene Zeitaufwand schlägt sich in der TTD nieder.

Abbildung 33 zeigt eine Monatsübersicht der am häufigsten von uns erkannten Malware-Familien im Zeitraum von Januar bis April 2016; darin hervorgehoben sind Beispiele für Malware-Familien, die im Zusammenhang mit Ransomware stehen. Die Schwankungen des TTD-Medians gehen auf den verstärkten bzw. geringeren Einsatz bestimmter Malware-Familien seitens der Angreifer zurück. So lag der TTD-Median im Februar 2016 noch bei etwas mehr als 9 Stunden, stieg dann aber im März 2016 auf über 14 Stunden an, da in diesem Monat Bedrohungen auftraten, die erst nach eingehenderen Untersuchungen durch unsere Analysten aufgespürt werden konnten.

Abbildung 34 macht deutlich: Die Verkürzung der TTD ist nach wie vor eine Herausforderung für die Verteidiger. Für Unternehmen ist es daher umso wichtiger, ihren Schutz durch eine integrierte Bedrohungsabwehr zu stärken. Bedrohungen, bei denen die TTD unter dem Median liegt, werden durch automatisierte Techniken wie Sandboxing erkannt. Bei neuen oder komplexeren Bedrohungen müssen dagegen interne oder externe Untersuchungen angestellt und Security-Intelligence hinzugezogen werden; die Erkennung nimmt somit mehr Zeit in Anspruch.

Jede Malware-Kampagne findet irgendwann ihr Ende. Nicht so jedoch der Wettlauf zwischen Angreifern und Verteidigern: Angreifer werden immer wieder neue und noch besser getarnte Bedrohungen ins Feld führen, die ihnen mehr Zeit für ihre Operationen verschaffen. Und auch weiterhin werden die Verteidiger ununterbrochen dagegenhalten. Auch weiterhin werden sie die neuesten Malware-Auswüchse dingfest machen, die dabei identifizierten IOCs in automatisierte Erkennungstechnologien integrieren und die gewonnenen Daten als aussagekräftige Threat-Intelligence aufbereiten.

Auch in den kommenden Monaten werden wir alles daran setzen, Bedrohungen noch schneller aufzuspüren – unter genauer Beobachtung des TTD-Medians, an dem wir unsere Fortschritte messen. Auch andere Unternehmen sollten den TTD-Median für sich ermitteln und auf dieser Grundlage Verbesserungen anstreben. Denn derzeit liegt der Branchendurchschnitt noch bei 100 bis 200 Tagen – ein inakzeptabler Wert.

Erkennungszeiten verkürzen, rechtzeitiges Patchen, Verbindungen verschlüsseln, überalterte Infrastrukturen proaktiv aktualisieren – das alles sind Maßnahmen, die den Spielraum der Angreifer eingrenzen. Die TTD sowie die TTP (Time to Patch – der Zeitraum von der Veröffentlichung bis zur Installation eines Patches) sind dabei besonders wichtige Kennzahlen. Denn diese verraten den Verteidigern, wo und wie sie vorgehen müssen, um Angreifer effektiver aufzuspüren – und damit bestmöglich zu verhindern, dass sie ihre Strategien anpassen und vom Radar verschwinden.

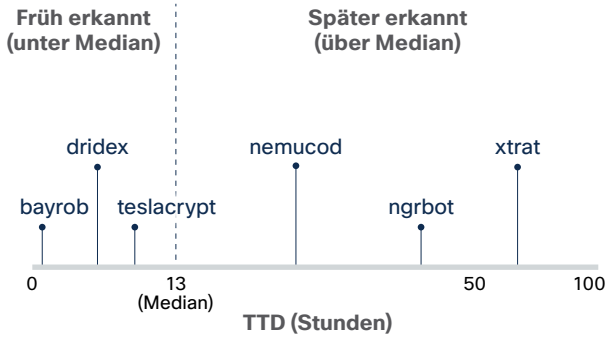
Abbildung 33: Die 10 im Monatsvergleich am häufigsten erkannten Malware-Familien

	Januar	Februar	März	April
1.	bayrob	downloader	downloader	bayrob
2.	downloader	installcore	nemucod	downloader
3.	installcore	convertad	agent	installcore
4.	agent	msil	installcore	nemucod
5.	convertad	browsefox	convertad	agent
6.	ransom	linkury	mydoom	convertad
7.	linkury	nemucod	msil	fareit
8.	kryptik	agent	browsefox	msil
9.	browsefox	kryptik	kryptik	trojan
10.	msil	mydoom	vilsel	heur

● Mit Ransomware in Zusammenhang stehende Malware-Familien

Quelle: Cisco Security Research

Abbildung 34: Beispiele für früher und später erkannte Malware-Familien (auf Grundlage des TTD-Medians von 13 Stunden)



Quelle: Cisco Security Research

Incident-Response: Versäumnisse, die die Sicherheit durchlöchern

Neue Meldungen zu Netzeinbrüchen, Ransomware-Angriffen und Ausbrüchen von hochkomplexer Malware machen in den einschlägigen Medien die Runde – ebenso wie die Tragweite derartiger Ereignisse, z. B. Betriebsschließungen und Rufschädigungen. Dennoch scheinen Angriffe wie diese viele Unternehmen zu überraschen – Unternehmen, die ihre Bedrohungserkennungs- und Incident-Response-Systeme für widerstandsfähig halten, obwohl sie in Wahrheit sehr durchlässig sind.

Häufig stützen sich diese Unternehmen auf Sicherheitstechnologien und -verfahren, die hinter den aktuellen Lösungen um Jahre hinterherhinken. Kommt es dann zum Ernstfall, sind ihre Sicherheitsteams schnell überfordert, insbesondere wenn für eine angemessene Reaktion auf den Angriff spezielles Know-how vonnöten ist.

Wir beraten Unternehmen aller Größen bezüglich ihrer Sicherheitsstrategie und stellt dabei häufig fest, dass es an Best-Practices zur Stärkung der Sicherheit fehlt. Angreifer erkennen diese Mängel ebenfalls – und nutzen sie aus, um sich Eintritt in die Netzwerke zu verschaffen.

So wird z. B. bei Fusionen und Übernahmen das Risikoprofil des jeweils anderen Partners nicht immer hinreichend geprüft. Sicherheitsmängel fallen dann erst auf, wenn die Unternehmen bereits zusammengeschlossen und die Probleme nicht mehr oder nur noch schwer zu beheben sind, da auch die Netzwerke bereits zusammengelegt wurden. Chief Information Security Officer (CISO) sollten daher alle Sicherheitsprozesse und -verfahren bereits im Vorfeld umfassend beurteilen, zumindest aber das jeweils andere Netzwerk nach verdächtigen Aktivitäten absuchen, bevor sie mit dem Gesamtnetzwerk in Produktion gehen.

Unzureichend geprüfte Netzwerke verschaffen Angreifern mehr Zeit für ihre Aktivitäten darin. Gleiches gilt für dürftige Sicherheitsvorkehrungen, z. B. schwache Passwörter oder eine übermäßige Nutzung von Administratorberechtigungen. Vieles deutet darauf hin, dass Unternehmen insgesamt nicht ausreichend auf komplexe Bedrohungen vorbereitet sind. Denn nicht selten wissen sie noch nicht einmal, ob oder inwiefern ihre Netzwerke in der Vergangenheit von Angriffen betroffen waren, und behaupten bisweilen sogar, bei ihnen sei es noch nie zu einem Sicherheitsvorfall gekommen. Doch das zeugt allenfalls von Unkenntnis der Aktivitäten in ihrem Netzwerk – jedes Unternehmen wird im Laufe seines Bestehens zumindest bis zu einem gewissen Grad mit Standard-Malware oder einem versuchten Netzeinbruch konfrontiert.

Ebenfalls verbreitet ist der Glaube, das eigene Unternehmen sei kein attraktives Ziel. Brachen wie etwa der Gesundheitssektor stehen in den letzten Jahren jedoch verstärkt im Fokus von Cyberkriminellen, da sie hier eine optimale Kombination vorfinden: wertvolle Daten und eine über Jahre hinweg schwach gesicherte IT (siehe **Seite 45**). Daneben geraten z. B. auch Schulen zunehmend ins Visier, da die Kriminellen in Institutionen wie diesen ebenfalls mit einer tendenziell eher schwachen Gegenwehr rechnen können. Unternehmen können ihre Incident-Response aber auch deutlich verbessern, wenn sie sich eine Reihe von Best-Practices zu eigen machen (Näheres hierzu auf **Seite 52**.)

„Noch immer behaupten einige Unternehmen, bei ihnen sei es noch nie zu einem Sicherheitsvorfall gekommen. Doch das zeugt allenfalls von Unkenntnis der Aktivitäten in ihrem Netzwerk – jedes Unternehmen wird im Laufe seines Bestehens zumindest bis zu einem gewissen Grad mit Standard-Malware oder einem versuchten Netzeinbruch konfrontiert.“

Unzureichende Netzwerkpflege: Ransomware-Ausbrüche im Gesundheitswesen stehen exemplarisch für ein branchenübergreifendes Problem

Gleich mehrere Ransomware-Angriffe erschütterten in diesem Jahr den Gesundheitssektor, von denen auch einige unserer Kunden betroffen waren. Eine Ursachenanalyse bei diesen Kunden führte einige Schwachstellen zutage, die die Infektion begünstigten, darunter:

- Gemeinsam genutzte Passwörter und Nutzerkonten mit unnötig hohen Zugriffsberechtigungen
- Unzureichende Aufzeichnung von sicherheitsrelevanten Ereignissen und somit keine Möglichkeit, kompromittierte Passwörter aufzudecken
- Webanwendungen, die über die **OWASP**-Top-10 der schwerwiegendsten Schwachstellen angreifbar waren
- Nicht aktualisierte Betriebssysteme und Anwendungen

Unsere Forscher stellten zudem fest, dass Kliniken häufig auf ihrem gesamten PC-Bestand angreifbare Software im Einsatz haben, darunter etwa Windows XP oder veraltete Versionen von Adobe Flash Player oder Java. Und genau hierauf gehen auch die jüngsten Ransomware-Infektionen zurück. Denn wie unsere Untersuchung ergab, handelte es sich bei den betroffenen Systemen um Computer, die das Klinikpersonal zum Surfen im Internet verwendete, dabei aber keine Patches für den Flash Player installiert hatte.

In diesem Zusammenhang fiel bei unseren Kunden aus dem Gesundheitswesen ein generelles Problem auf: Das Fehlen von formellen Prozessen, die eine rechtzeitige Installation von Sicherheitspatches sicherstellen.

Beim Großteil der Betroffenen fehlte es darüber hinaus auch an Incident-Response-Plänen. Eine effektive Reaktion auf die Angriffe war daher kaum möglich.

Gesundheitseinrichtungen haben für den Bereich Security zudem nur selten ein spezialisiertes Team aufgestellt, sondern übertragen die Instandhaltung ihrer IT an eine oder mehrere Personen, die bestenfalls über allgemeine IT-Kenntnisse verfügen.

Sicher stehen aber nicht nur unsere Kunden vor Herausforderungen wie diesen. Die folgenden Maßnahmen können jedem Gesundheitsdienstleister dabei helfen, sein Sicherheitsniveau insgesamt zu erhöhen:[6]

- Schutz vor Malware- und Hacker-Angriffen durch grundlegende Systemhärtung
- Prüfung der vorliegenden IT-Landschaft: Welche und wie viele Gräte sind an das Netzwerk angebunden? Wo befinden sich diese Geräte?
- Aufklärung der Nutzer über Bedrohungen und Best-Practices
- Ausarbeitung eines Incident-Response-Plans
- Aktive Überwachung des Netzwerks auf Anzeichen von Kompromittierungen

Und nicht zuletzt bleibt das Schließen bekannter Sicherheitslücken auch weiterhin unabdingbar, waren es bei jüngsten der SamSam-Kampagne doch seit langem bestehende Sicherheitslücken in JBoss-Servern, über die sich die Drahtzieher lateral durch die Internet-Infrastruktur bewegten und die Netze von Gesundheitsdienstleistern angriffen (siehe **Seite 7**). Und sicher werden Cyberkriminelle die Internet-Infrastruktur künftig noch ausgedehnter als Startrampe für Ransomware-Kampagnen nutzen, betrachtet man die große Zahl der anfälligen Hardware und Software, die internetweit im Einsatz ist (siehe „Ausbreitung von Ransomware macht das Schließen seit Langem bestehender Sicherheitslücken unabdingbar“ auf **Seite 30**).

Unternehmen aller Branchen können ihre Lehren aus den Ransomware-Attacken auf den Gesundheitssektor ziehen. Auch sie sollten prüfen, ob die Tools, Ressourcen und Prozesse ihrer IT-Teams in der Lage sind, Sicherheit effektiv zu gewährleisten.

[6] Hinweis: Alle Vorhaben zur Stärkung der Sicherheit müssen auf ihre Konformität mit gesetzlichen oder branchenspezifischen Bestimmungen geprüft werden, da diese ggf. Auswirkungen darauf haben, wie z. B. Aspekte wie Datensicherheit und Schutz von personenbezogenen Daten gehandhabt werden müssen.

Globale Perspektiven und Sicherheitsempfehlungen

Globale Perspektiven und Sicherheitsempfehlungen

Malware grassiert rund um den Globus. Ihre Ursprungsorte aber variieren, da die Hintermänner ihre Operationsbasen bei Bedarf sehr schnell verlagern. Unabhängig davon ist jedoch klar: Keine Branche ist vor Angriffen gefeit – auch wenn noch immer einige glauben, sie stünden nicht im Visier der Kriminellen. Andere wiederum stützen Bedrohungserkennung und Incident-Response lediglich auf IOCs – starke Sicherheit erreichen sie jedoch nur mit echter Threat-Intelligence

Unterdessen begleiten die zunehmend komplexe Bedrohungslandschaft zusätzliche Unsicherheiten: Widersprüchliche Signale, Gesetze und Forderungen einer durch wachsende Sorgen um Datenkontrolle und -zugriff geprägten Politik, die internationalen Handel, Sicherheit in der Informationstechnik und vertrauensvolle öffentlich-private Partnerschaften auszubremsen und deren Grundsätze zu konterkarieren droht.

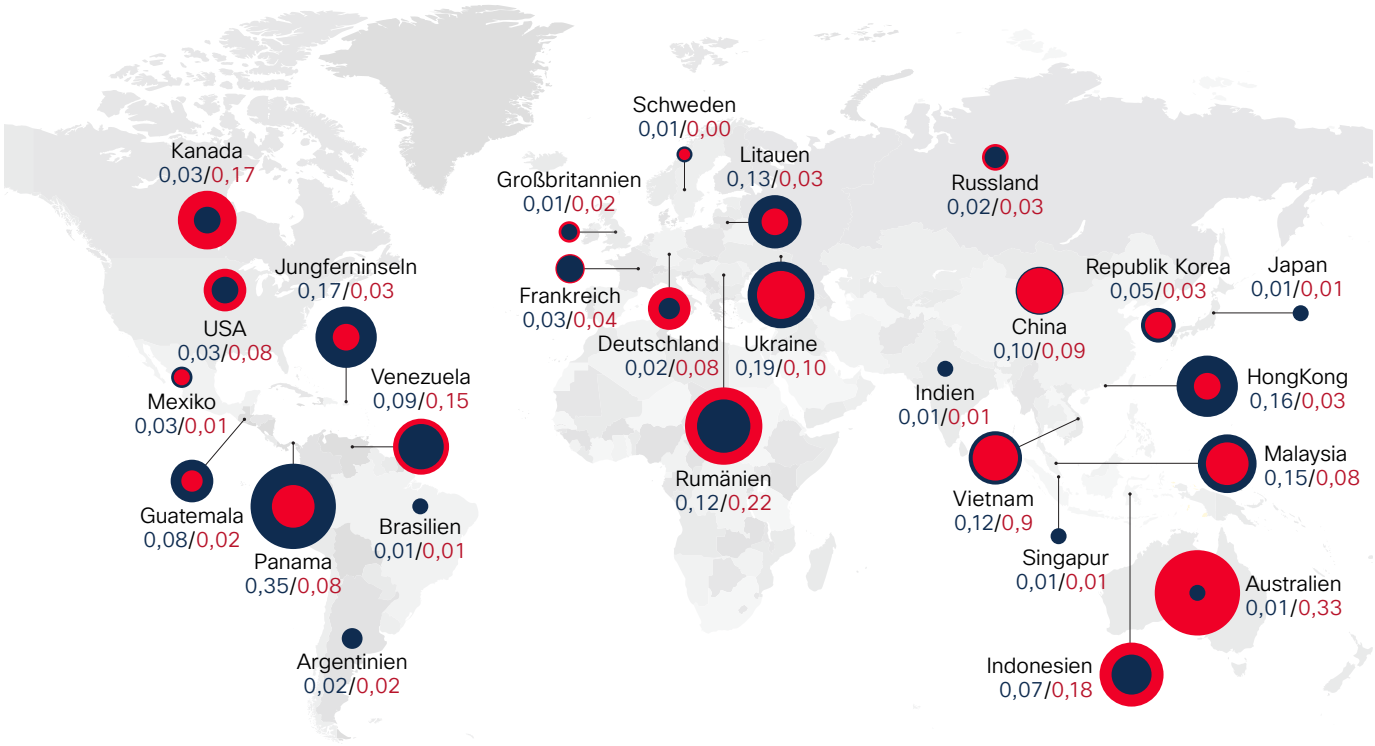
Blockierung von Web-Angriffen: Regionaler Überblick

Der Umfang der Blockierungsaktivitäten im Verhältnis zum gesamten Internetverkehr liefert Hinweise über den Ursprung von Malware. So ging in Nord- und Südamerika der meiste blockierte Datenverkehr auf Kanada zurück.

In Europa, dem Nahen Osten und Afrika wurden – gemessen am Gesamt-Datenverkehr in dieser Region – die meisten Blockierungen in der Ukraine und in Rumänien verzeichnet. Im Asien-Pazifik-Raum stand Australien ganz oben auf der Liste (siehe Abbildung 35 auf der nächsten Seite).

Abhängig von Faktoren wie etwa der Verfügbarkeit von einfach zu kapernden Servern in einer Region, verlagern Angreifer ihre Operationsbasen jedoch auch bei Bedarf.

Abbildung 35: Web-Blockierungen nach Land



Quelle: Cisco Security Research

Unter dem Strich lässt sich aber – wie auch für den Branchenvergleich auf **Seite 49** – für jedes Land und jede Region das Gleiche festhalten: Vor Malware-Traffic ist niemand sicher. Malware ist vielmehr ein globales Problem, auch wenn einige Regionen und Länder verhältnismäßig höhere Blockierungsaktivitäten aufweisen als andere. Hier lag die Ursache in Sicherheitslücken in der Infrastruktur, die von Angreifern ausgenutzt wurden. Indes hatte aber auch ein Ausschlag der Malware-Aktivitäten in Australien im Dezember 2015 und Januar 2016 eine deutliche Verschiebung der Gewichtung der einzelnen Länder und des dort verzeichneten Blockierungsvolumens zur Folge.

Malware-Auftrittsrisiko im Branchenvergleich: Keine Branche ist gefeit

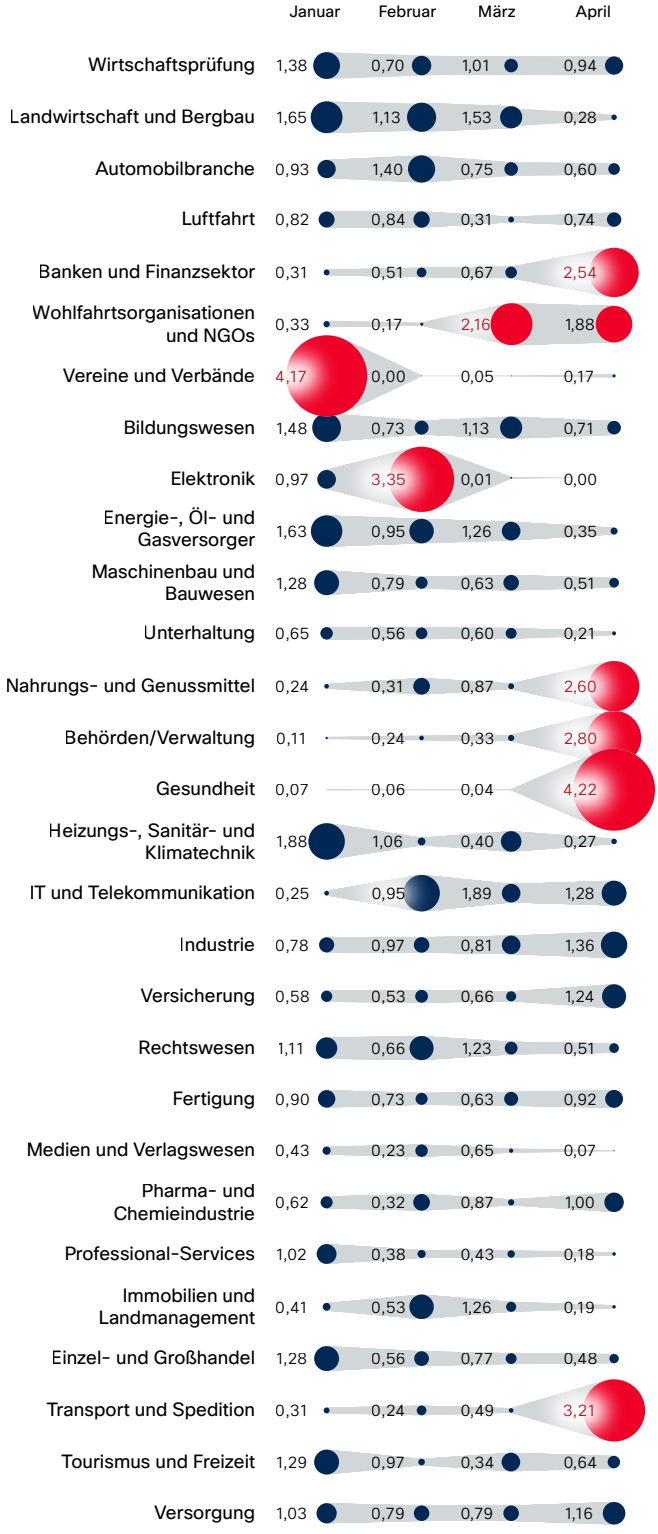
An dieser Stelle muss zunächst festgehalten werden: Die Behauptung, irgendeine Branche sei nicht attraktiv für Angreifer, ist schlicht falsch. Denn das eindeutige Ergebnis unserer periodischen Untersuchung des schädlichen Datenverkehrs („Blockierungsrate“) und des „normalen“ bzw. erwarteten Datenverkehrs einer Branche ist: Malware kann jede Branche treffen. Angreifer wählen ihre Ziele einzig danach aus, wo sie ihre Kampagnen am effektivsten aufziehen und am längsten fahren können.

Der Gesundheitssektor gilt in den Medien zwar derzeit als die am stärksten betroffene Branche (siehe **Seite 7**), doch unsere Daten zeigen in den ersten Monaten 2016 auch in anderen Branchen ein verhältnismäßig hohes Malware-Volumen. So wurden besonders hohe Blockierungsraten etwa auch in Vereinen und Verbänden, Wohlfahrtsorganisationen und Nichtregierungsorganisationen (NGOs) sowie in der Elektroindustrie gemessen.

Unter dem Strich lässt sich aus den Blockierungsraten durch die Bank in jeder Branche ein Risiko ablesen. In einigen Branchen sind zwar mitunter auch Ausschläge nach oben zu verzeichnen, doch das Gesamtbild ist eindeutig: Angreifer konzentrieren ihre Anstrengungen zunächst dort, wo sie Netzwerke am leichtesten kompromittieren können. Ihre Kampagnen fahren sie dann dort, wo es für sie am profitabelsten ist, ganz gleich, welche Branche das letztlich sein mag.

Abbildung 36 zeigt die 29 Branchen mit der im Verhältnis zum normalen Netzwerkverkehr höchsten Blockierungsaktivität. Bei einer Rate von 1,0 verhält sich die Anzahl der Blockierungen proportional zum dokumentierten Netzwerkverkehr. Bei einem Wert über 1,0 ist die Blockierungsrate höher als erwartet. Liegt die Rate unter 1,0, ist sie niedriger als erwartet.

Abbildung 36: Monatliche Blockierungsraten nach Branche, Januar bis April 2016



Quelle: Cisco Security Research

Geopolitisches Update: Politik und Wirtschaft auf der Suche nach Auswegen aus dem Datenschutz-Dilemma

Technologie- und Telekommunikationsanbieter, aber auch andere weltweit aufgestellte Unternehmen, müssen sich auch weiterhin durch ein geopolitisches Umfeld aus komplexen und oft auch einander widersprechenden Cybersecurity-Regularien manövrieren, mit denen versucht wird, im Spannungsfeld zwischen den Anforderungen von Politik und Wirtschaft und der Privatsphäre und Sicherheit des Einzelnen die richtigen Stellschrauben zu setzen.

Auf der Top-Agenda der Netzpolitik steht aktuell die Datensicherheit. So sollen etwa personenbezogene Daten oder die Integrität kritischer Infrastruktur wie der nationalen Strom- und Wasserversorgungsnetze geschützt, gleichzeitig aber auch die rechtlichen Voraussetzungen für eine im Bedarfsfall behördlich angeordnete Überwachung des Telekommunikationsverkehrs geschaffen werden.

Viele sehen diese Ziele jedoch gefährdet, da dem Staat die Kontrolle über Informationstechnik und Datenzugriff entgleite und es daher gelte, die Kontrolle zurückzugewinnen – eine Ansicht, die vor dem Hintergrund einer zunehmenden Terrorgefahr und einer schleppenden Weltkonjunktur zusätzlich bekräftigt wird. Und so ist die politische Stimmung weitgehend geprägt von dem Bestreben, beim Schutz von Bürgern und Unternehmen Stärke zu zeigen:

- Nachdem die Snowden-Enthüllungen grundlegende Fragen über die Rechte des Einzelnen gegenüber den Rechten des Staates aufgeworfen hatten, wurden internationale Abkommen zur Disposition gestellt und schließlich überarbeitet, z. B. Safe Harbor. Sein Nachfolger, der „EU-US-Datenschutzschild“, sieht nun für Unternehmen in den USA strengere Auflagen zum Schutz der personenbezogenen Daten europäischer Bürger vor dem Zugriff durch US-Behörden vor.
- Im Zuge der Flüchtlingskrise in der Europäischen Union sowie den jüngsten Terroranschlägen in Paris, Brüssel, der Türkei, den Vereinigten Staaten und andernorts wurden Rufe laut, Strafverfolgern den Zugriff auf verschlüsselte Verbindungen von Privatnutzern zu ermöglichen. Ihren Höhepunkt erreichte die Debatte im Streit zwischen FBI und Apple Inc., bei dem die US-Behörde von dem Hersteller verlangte, das iPhone eines Terroristen zu entschlüsseln.
- Regierungen und private Sicherheitsfirmen gehen nun auch stärker gegen mutmaßliche Fälle von Cyberspionage und Datendiebstahl durch Nationalstaaten vor. So sollen Angriffe, die über das internationale Finanznetzwerk SWIFT (Society for Worldwide Interbank Financial Telecommunication) gegen Banken gefahren wurden, auf Nordkorea zurückgehen. Beim Cyberangriff auf den deutschen Bundestag sollen die Spuren jüngsten Meldungen deutscher Behörden zufolge nach Moskau führen.

Regierungen weltweit erhoffen sich durch Maßnahmen zur Stärkung ihrer Kontrolle über die Informationstechnik eine bessere Ausgangsposition im Kampf gegen Terror und Cyberkriminalität. Dabei nehmen sie auch das Risiko in Kauf, neue Sicherheitslücken aufzuschlagen, behalten sich in einigen Fällen allerdings auch das Recht vor, diese für ihre Zwecke zu nutzen. Da sich aber auch vorbehalten, ob sie diese Informationen mit den Herstelllern hinter den Technologien teilen, stellt sich unweigerlich die Frage, wer bei der Offenlegung von Sicherheitslücken die Verantwortung trägt. Denn in der Öffentlichkeit sind es die Unternehmen, die in der Schusslinie stehen, wenn der Staat seine Abhörpraktiken ausweitet.

Trotz der rasant voranschreitenden Globalisierung hat es die Weltgemeinschaft noch immer nicht geschafft, in Sachen Cybersicherheit oder damit verbundenen Themen wie Transparenz, Zurechenbarkeit, Datensicherheit und Verschlüsselung eine gemeinsame Linie zu finden. Das Ziel einer allgemeinen „Verkehrsordnung“ für die weltweiten Datenautobahnen bleibt zwar bestehen. Doch solange in dieser Sache gegensätzliche Prioritäten aufeinanderprallen, werden sich Unternehmen auch weiterhin in einem stark politisierten und juristisch riskanten Umfeld zurechtfinden müssen.

„Trotz der rasant voranschreitenden Globalisierung hat es die Weltgemeinschaft noch immer nicht geschafft, in Sachen Cybersicherheit oder damit verbundenen Themen wie Transparenz, Zurechenbarkeit, Datensicherheit und Verschlüsselung eine gemeinsame Linie zu finden.“

Neue Regularien sind im Anmarsch

Internationale Telekommunikations- und Technologieanbieter müssen hinsichtlich der gesetzlichen Bestimmungen der einzelnen Länder immer auf dem Laufenden bleiben. Sie unterliegen im Ausland den Gesetzen souveräner Staaten und müssen gleichzeitig die rechtlichen Rahmenbedingungen und die Erwartungen der Öffentlichkeit im eigenen Land erfüllen. Angesichts der zahlreichen neuen Vorschläge und Pläne der Gesetzgeber verschiedener Länder, ist dies jedoch eine Herausforderung.

So hat etwa Großbritannien mit der Investigatory Powers Bill einen Entwurf für ein Gesetz eingebracht, das sämtliche Überwachungsbefugnisse der britischen Sicherheitsbehörden übergreifend regeln soll. Das Gesetz soll bis Ende des verabschiedet werden, wird derzeit aber noch im britischen Parlament debattiert. Unter Politikern, Unternehmen und Menschenrechtsorganisationen wird der Entwurf kontrovers diskutiert, u. a. auch aufgrund einer Klausel, nach der Technologie- und Telekommunikationsanbieter im Bedarfsfall und nach Anordnung der Sicherheitsbehörden die Verschlüsselung ihrer Produkte aufheben müssten.

Auch in anderen Ländern werden Maßnahmen wie diese vorangetrieben, z. B.:

- Die Europäische Union will noch in diesem Sommer ihre eigene Richtlinie zur Netz- und Informationssicherheit beschließen.
- Frankreich ist dabei, ein Anti-Terror-Gesetz im Eilverfahren durchs Parlament zu bringen, das für Unternehmen hohe Geldstrafen und für Führungskräfte Freiheitsstrafen vorsieht, falls diese sich weigern, bei Ermittlungen gegen Terroristen mit den Behörden zusammenzuarbeiten. Befürworter des Gesetzes hoffen, dass es noch vor Aufhebung des Ausnahmezustandes verabschiedet wird, den das Land seit den Anschlägen in Paris im November verhängt hat.
- In Ungarn wird darüber debattiert, Verschlüsselungssoftware per Gesetz zu verbieten.
- Russland und China wollen in Sorge um zunehmende Terrorgefahren die Kontrolle des Staates über die heimischen Netzwerke ausweiten.

Für Telekommunikations- und Technologieanbieter sind diese Entwicklungen besorgniserregend, denn die strengen Anforderungen dieser Maßnahmen können für sie auch rechtlich zum Problem werden.

Komplexität gefährdet die Sicherheit

Für Unternehmen ist dieses zunehmend komplexe Umfeld aus unterschiedlichen Regularien eine Herausforderung. Doch darüber hinaus gefährdet es vor allem auch die Sicherheit. Denn Angreifer können und werden sich die Uneinigkeit der Staaten zunutze machen.

- Die Vereinigten Staaten befanden sich bislang in der einzigartigen Position, dass in großen Mengen Daten auf US-Servern gespeichert waren, die für Regierungen nützlich sind. Mittlerweile aber bringen Länder wie Deutschland, Russland und China Gesetze und Bestimmungen zur Datenlokalisierung auf den Weg, die die Speicherung von Daten nur noch im eigenen Land vorsehen.
- In den Vereinigten Staaten wird ein Gesetz diskutiert, das sogar weiter reichen würde als die Pläne der britischen Regierung. Danach sollen Hardware- und Software-Hersteller, aber auch jedes andere Unternehmen, das etwa einen App-Store unterhält, Daten für Behörden lesbar zur Verfügung stellen und die Möglichkeit zum Reverse-Engineering ihrer Produkte zu integrieren, sodass auch verschlüsselte Daten sichtbar gemacht werden können.

Da es an einem globalen Maßnahmenpaket mangelt, sind bessere Kommunikation und größeres Verständnis zwischen Regierungen und dem privaten Sektor im Hinblick auf Cybersicherheit dringend vonnöten. Effektivere Systeme für den Austausch von Datenanforderungen sind ein guter Ausgangspunkt für dieses Vorhaben. Der Informationsaustausch zwischen Regierungen und Unternehmen ist ebenfalls unerlässlich, auch wenn hierbei noch Missverständnisse ausgeräumt werden müssen.

Unternehmen halten z. B. dagegen, dass es zwar kurzfristige Sicherheitsvorteile bieten kann, aber das Vertrauen der Verbraucher letzten Endes zerstören könnte, wenn Technologieanbieter gezwungen werden, eine „Hintertür“ für den Einblick in Daten einzubauen. Dies würde seinerseits diejenigen Unternehmen schädigen, die das Rückgrat ihrer jeweiligen Volkswirtschaft bilden.

Sowohl für den öffentlichen als auch den privaten Sektor ist der Datenschutz ein Dilemma. Vereinbarungen wie der EU-US-Datenschutzschild wurden so konzipiert, dass der internationale Datenfluss erleichtert wird, um Analysen anstellen zu können und den Verbrauchern das Vertrauen zu vermitteln, dass der Datenfluss ohne Risiko für sie oder die Daten erfolgt. Ob die Verbraucher derartige Maßnahmen akzeptieren, bleibt jedoch abzuwarten.

„Da es an einem globalen Maßnahmenpaket mangelt, sind bessere Kommunikation und größeres Verständnis zwischen Regierungen und dem privaten Sektor im Hinblick auf Cybersicherheit dringend vonnöten.“

Sicherheitsempfehlungen

Mit dem Aufkommen der nächsten Generation von Ransomware müssen Unternehmen eine „erste Verteidigungslinie“ aufbauen, um die Möglichkeiten der Angreifer zu einzuschränken, sich lateral durch Netze bewegen und über lange Zeiträume hinweg ungestört operieren zu können. Diese erste Verteidigungslinie umfasst neben grundlegenden Best-Practices wie dem Patching anfälliger Internet-Infrastruktur und -Systeme (siehe **Seite 22** und **Seite 29**) und einem optimierten Passwortmanagement (siehe **Seite 44**) die Netzwerksegmentierung.

Unternehmen können die Netzwerksegmentierung nutzen, um die laterale Bewegung von sich selbst ausbreitenden Bedrohungen nicht nur zu stoppen oder zu verlangsamen, sondern auch einzugrenzen. Die Segmentierung des Netzwerks beinhaltet folgende Komponenten:

- VLANs und Subnetze für die logische Trennung des Zugriffs auf Daten auch auf Workstation-Ebene
- Dedizierte Firewall- und Gateway-Segmentierung
- Hostbasierte Firewalls mit Filterkonfiguration für ein- und ausgehenden Datenverkehr
- Blacklists und Whitelists für Anwendungen
- Rollenbasierte Netzwerkfreigabe-Berechtigungen (Prinzip der geringsten Rechte)
- Angemessenes Management von Anmeldeinformationen

DIE LETZTE VERTEIDIGUNGSLINIE: BACKUP-WIEDERHERSTELLUNG

Die Backup-Wiederherstellung ist die letzte Verteidigungslinie für Unternehmen, die – heute und in Zukunft – vermeiden wollen, empfindlich hohe Lösegelder an Angreifer zahlen zu müssen, die ihre Daten mit Ransomware verschlüsselt haben (siehe **Seite 10**). Die Fähigkeit, nach einem Ransomware-Angriff eine Wiederherstellung mit minimalen Datenverlusten und Serviceunterbrechungen durchzuführen, hängt jedoch davon ab, ob System-Backups und Disaster-Recovery-Standorte kompromittiert wurden.

In einem Ransomware-Szenario, in dem lokale Backups von Angreifern gelöscht, entfernt oder anderweitig unzugänglich gemacht werden, sind externe Backups häufig die einzige Hoffnung für Unternehmen, den Betrieb wiederaufzunehmen, ohne das Lösegeld zahlen zu müssen. Wie viele Daten, wenn überhaupt, unzugänglich bleiben oder verloren gehen, ist davon abhängig, wie häufig Backups extern gespeichert werden.

BROWSERINFEKTIONEN SIND EINE ERNSTZUNEHMENDE BEDROHUNG

Wenn Ad-Injectors schädliche Werbung über HTTPS-verschlüsselten Datenverkehr ausliefern, können Sicherheitsteams die Bedrohung nicht sofort feststellen (siehe **Seite 21**). Und da Angreifer immer häufiger HTTPS nutzen, um ihre Aktivitäten zu verschleiern, dürfen Sicherheitsteams Browserinfektionen erst recht nicht mehr nur als geringfügiges Sicherheitsrisiko für Unternehmen und Nutzer ansehen.

Eine scheinbar harmlose Browserinfektion kann sich schnell zu einem größeren Problem entwickeln. Denn Ad-Injectors sind mittlerweile ein zentrales Vehikel für die Vorbereitung von schwerwiegenderen Angriffen geworden.

Daher sollten Unternehmen Browserinfektionen genau im Auge behalten, um Bedrohungen im Ernstfall schnell identifizieren und entschärfen zu können. Tools für die Verhaltensanalyse und aus verschiedenen Quellen zusammengetragene Threat-Intelligence leisten hierbei massive Unterstützung. Enorm wichtig ist zudem, dass Nutzer ihre Sicherheitsteams umgehend benachrichtigen, wenn sie eine Zunahme von Popup-Einblendungen und anderer unerwünschter Werbung feststellen.

PATCHING ZUR ROUTINE MACHEN

Unternehmen aller Größen und Branchen müssen sich angesichts der komplexen Bedrohungen von heute davon verabschieden, in Sachen Sicherheit nur das Nötigste zu tun. Es braucht heute eine integrierte Bedrohungsabwehr – ebenso wie ein dediziertes Budget für Security.

Das Sicherheitsteam muss z. B. mit den Tools, die ihm zur Verfügung steht, regelmäßig eine Überprüfung auf unerwartete System- oder Administratorkonten vornehmen. Daneben muss es außerdem jegliche Netzwerkkommunikation protokollieren, sie auf schädlichen Datenverkehr untersuchen und entsprechenden verdächtigen Datenverkehr auf IOCs überprüfen. Die Unternehmensführung wiederum muss die dazu erforderlichen Tools zur Verfügung stellen.

Darüber hinaus muss sie sicherstellen, dass die Umgebung auf dem neuesten Stand ist. Dazu sollte das Patching formell geregelt werden, damit sichergestellt ist, dass Sicherheitslücken in Betriebssystemen und gängiger Software nicht von Angreifern ausgenutzt werden können.

Indicators-of-Compromise sind keine Threat-Intelligence

Indicators-of-Compromise (IOCs) sind die Sprache der Threat-Intelligence – die Bausteine, aus denen sich die Aktivität von Bedrohungen zusammensetzt. IOCs können für Untersuchungen zwar wertvoll sein, sie sind aber dennoch grundlegend von Threat-Intelligence zu unterscheiden.

Listen von IOCs werden Millionenfach als Threat-Intelligence verkauft. Doch diese Daten müssen dann noch immer von den Sicherheitsteams ausgewertet und für das Unternehmen aufbereitet werden – ein äußerst aufwändiges Unterfangen, das Ressourcen für wichtigere Aufgaben kostet. Das Vertrauen auf IOCs kann sogar zu der falschen Annahme führen, dass das Unternehmen und Netzwerk so sicher ist, dass Angreifer lieber auf leichtere Ziele ausweichen.

Was also ist Threat-Intelligence? Es sind Daten, die durch die Einbeziehung des Kontextes, in dem sie produziert wurden, als aussagekräftige Informationen aufbereitet wurden. Durch diesen Kontext macht Threat-Intelligence erkennbar, wie auf diese Daten gezielt reagiert werden kann. Ohne derartige Informationen sind Daten nicht viel wert – so wie Sand am Meer.

Echte Threat-Intelligence erhalten Unternehmen bei Security-Anbietern, die IOCs, Kontext mit relevanten Informationen zu Gefahrenpotenzialen sowie Empfehlungen zur Reaktion vereinen. Diese Anbieter ergänzen die maschinellen Analysen zudem durch menschliche Intelligenz und integrieren die Erkenntnisse in ihre Sicherheitstools, die die Threat-Intelligence automatisieren.

IOCs sollten nicht mit Threat-Intelligence verwechselt werden. Denn erst Threat-Intelligence ermöglicht es, einen Angriff in seiner Gesamtheit zu verstehen und die Erkennung und Reaktion auf Vorfälle zu verbessern.

„IOCs sollten nicht mit Threat-Intelligence verwechselt werden. Denn erst Threat-Intelligence ermöglicht es, einen Angriff in seiner Gesamtheit zu verstehen und die Erkennung und Reaktion auf Vorfälle zu verbessern.“

Fazit

Die Angriffe von heute entwickeln sich derzeit schneller, als Sicherheitsteams reagieren können. Solange Angreifern unbegrenzt Zeit zugestanden wird, zu operieren und sich anzupassen und weiterzuentwickeln, ist ihr Erfolg nahezu gesichert. Wenn ein Unternehmen aber den Handlungsspielraum und die Zeit eingrenzt, in der Angreifer ihre Operationen durchführen können, müssen diese Entscheidungen unter Druck treffen und laufen daher leichter Gefahr, erkannt zu werden.

Eine Strategie besteht darin, Angreifer mit den eigenen Waffen zu schlagen, indem man die Zeit für ihre Operationen eingrenzt und sie damit zwingt, laufend neue Bedrohungen zu entwickeln. Denn je mehr sie sich anpassen müssen, desto wahrscheinlicher ist es, dass sie eine Spur hinterlassen, die letztlich zu ihrer Identifizierung führt – unabhängig von der Anzahl der Methoden, mit denen sie versuchen, der Erkennung zu entgehen und ihre Spuren zu verwischen.

Verteidiger können ihre Strategien zudem nur verbessern, wenn sie wissen, wie sie in Sachen Bedrohungserkennung aufgestellt sind. Die TTD (Time to Detection) sowie die TTP (Time to Patch) sind dabei besonders wichtige Kennzahlen. Denn an diesen können Sicherheitsteams ablesen, an welchen Stellen sie ihre Abwehrtechniken optimieren und damit Angreifer dazu zwingen können, ihre Strategie zu ändern.

Unternehmen und Endnutzer spielen eine zentrale Rolle dabei, die Zeit von Angreifern für ihre Operationen einzugrenzen. Tatsächlich müssen Unternehmen jetzt handeln und daran arbeiten, ihre Sicherheitsverfahren und -maßnahmen zu verbessern.

Durch die Aktualisierung veralteter Infrastruktur und Systeme und das Patching bekannter Sicherheitslücken können sich Cyberkriminelle dieser Ressourcen nicht mehr für ihre Kampagnen bedienen. Und diese Maßnahmen sind enorm wichtig. Denn die jüngste Kampagne mit der Ransomware SamSam hat sicher in kriminellen Kreisen für Aufsehen gesorgt und gezeigt, wie profitabel Attacken auf seit langem bestehende Sicherheitslücken sein können (siehe „Ransomware: Eine kaum abzustellende Geldmaschine“ auf **Seite 7**).

Viele Unternehmen haben mittlerweile erkannt, dass sie ihre Internet-Infrastruktur neu überdenken müssen. Sie wollen ihre Geräte und Software vereinfachen und aktualisieren, um Kosten zu senken und ihre IT zu einem starken Fundament für Erfolg im digitalen Zeitalter zu machen. In diesem Zuge sollten sie auch die Sicherheit stärken und die nötige Transparenz in ihrem Netzwerk schaffen, um die Operationen von Angreifern frühzeitig zu unterbinden.

„Viele Unternehmen haben mittlerweile erkannt, dass sie ihre Internet-Infrastruktur neu überdenken müssen [...] In diesem Zuge sollten sie auch die Sicherheit stärken und die nötige Transparenz in ihrem Netzwerk schaffen, um die Operationen von Angreifern frühzeitig zu unterbinden.“

Über Cisco

Cisco bietet intelligente Lösungen für die IT-Sicherheit und verfügt über das branchenweit umfangreichste Portfolio an Systemen für eine fortschrittliche Bedrohungsabwehr, die unterschiedlichste Angriffsvektoren abdecken. Durch seinen bedrohungsorientierten und operationalisierten Ansatz verringert Cisco die Komplexität und verhindert die Fragmentierung von Sicherheitstools. Dies ermöglicht ein hohes Maß an Transparenz, konsistente Kontrollen und einen intelligenten Bedrohungsschutz vor, während und nach einem Angriff.

Die Forschungsgruppe des Collective Security Intelligence (CSI) Ecosystem ermittelt Entwicklungen in der Bedrohungslandschaft anhand von Telemetriedaten aus zahllosen Geräten und Sensoren, öffentlichen Feeds sowie der Open-Source-Community von Cisco. Dazu werden jeden Tag mehrere Milliarden Internetanfragen sowie Millionen von E-Mails, Malware-Stichproben und Netzwerk-Zugriffsversuche analysiert.

Eine hochmoderne Infrastruktur, unterstützt durch branchenführende Systeme, wertet die Telemetriedaten aus. Dies ermöglicht maschinelles Lernen, es können Bedrohungen für Netzwerke, Rechenzentren, Endpunkte, Mobilgeräte, virtuelle Systeme, das Internet, den E-Mail-Verkehr und die Cloud nachverfolgt sowie Ursachen ermittelt und Outbreaks analysiert werden. Die so gewonnenen Informationen fließen direkt in den Echtzeitschutz der Produkte und Services ein, die bei Cisco Kunden weltweit im Einsatz sind.

Weitere Informationen zum bedrohungsorientierten Sicherheitsansatz von Cisco finden Sie unter **www.cisco.com/web/DE/products/security/index.html**.

Mitwirkende am Cisco Midyear Cybersecurity Report 2016

TALOS SECURITY INTELLIGENCE AND RESEARCH GROUP

Talos ist die Threat-Intelligence-Organisation von Cisco. Die Talos Forschungsgruppe ermittelt unter Einsatz hochmoderner Systeme wichtige Daten aus der Bedrohungslandschaft, die es den Produkten von Cisco ermöglichen, bekannte und neue Bedrohungen zu erkennen, zu analysieren und abzuwehren. Das Team von Talos aktualisiert die offiziellen Regelsätze von Snort.org, ClamAV, SenderBase.org und SpamCop und liefert seine Forschungsergebnisse an das Cisco CSI Ecosystem.

SECURITY AND TRUST ORGANIZATION

Die Security and Trust Organization zeichnet für den Schutz der Kunden von Cisco aus dem öffentlichen und privaten Sektor verantwortlich. Der Fokus liegt dabei nicht nur auf der konsistenten Anwendung der Grundsätze der Cisco Secure Development Lifecycle and Trustworthy Systems über das gesamte Cisco Produkt- und Serviceportfolio hinweg, sondern auch auf dem Schutz von Cisco vor den komplexen Bedrohungen von heute. Sicherheit und Vertrauen schließen bei Cisco Menschen und Richtlinien ebenso wie Prozesse und Technologien ein. Denn erst auf dieser Basis können Informationssicherheit, vertrauenswürdige Technik, Datenschutz und Privatsphäre, Cloud-Sicherheit, Transparenz und Nachvollziehbarkeit sowie Zuverlässigkeit gegenüber Kunden umfassend sichergestellt werden. Weitere Informationen finden Sie unter **http://trust.cisco.com**.

GLOBAL GOVERNMENT AFFAIRS

Cisco engagiert sich auf verschiedenen Regierungsebenen für die Gestaltung von wachstums- und innovationsfreundlichen Regelwerken, die Wirtschaft, Politik und Zivilgesellschaft voranbringen. Im engen Austausch mit Interessenvertretern und Branchengruppen ist Cisco dabei auf globaler und nationaler ebenso wie auf regionaler Ebene tätig. Das Team von Global Government Affairs vereint die umfangreiche Erfahrung von ehemaligen Mandatsträgern, Parlamentariern, Behördenvorständen, Beamten der US-Regierung und anderen Experten für wirtschafts- und gesellschaftspolitische Belange, die auf ein gemeinsames Ziel hinarbeiten: Die Förderung von Wohlstand durch die sichere Nutzung von Technologie.

COGNITIVE THREAT ANALYTICS

Cisco Cognitive Threat Analytics ist ein Cloud-basierter Dienst, der Sicherheitsverletzungen, Aktivitäten von Malware in geschützten Netzwerken und andere Bedrohungen mittels statistischer Analysen des Netzwerkdatenverkehrs erkennt. Der Dienst identifiziert die Symptome von Malware-Infektionen oder Datenschutzverletzungen anhand von Verhaltensanalysen und Anomalie-Erkennung und schließt so die Lücken von Abwehrsystemen am Perimeter. Neben fortschrittlichen statistischen Modellen bringt Cognitive Threat Analytics maschinelles Lernen zum Einsatz. So können neue Bedrohungen selbständig erkannt und der Schutz laufend optimiert werden.

INTELLISHIELD TEAM

Das IntelliShield Team analysiert das Gefahrenpotenzial von Sicherheitslücken und korreliert seine Ergebnisse mit Daten der Cisco Security Research & Operations und von externen Quellen. Diese Informationen integriert das Team im IntelliShield Security Intelligence Service, der in zahlreichen Produkten und Services von Cisco zum Einsatz kommt.

LANCOPE

Lancope, ein Cisco Unternehmen, bietet führende Netzwerk- und Security-Intelligence zum Schutz vor den komplexen Bedrohungen von heute. Das Lancope StealthWatch® System untersucht NetFlow, IPFIX und andere Arten von Netzwerk-Telemetrie anhand kontextbezogener Sicherheitsanalysen, mit deren Hilfe APTs und DDoS-Angriffe ebenso wie Zero-Day-Malware und Insider-Bedrohungen schnell und zuverlässig erkannt werden können. Durch die Überwachung lateraler Bewegungen von Benutzern, Geräten und Anwendungen ermöglicht Lancope dabei eine schnelle Reaktion auf Vorfälle, liefert präzise Forensik und reduziert die Risiken für Unternehmen.

ACTIVE THREAT ANALYTICS TEAM

Das Team von Cisco Active Threat Analytics (ATA) unterstützt Unternehmen unter Einsatz fortschrittlicher Big-Data-Technologien bei der Abwehr von bekannten Bedrohungen, Zero-Day-Angriffen und Advanced Persistent Threats. Dieser Managed-Komplettservice wird durch unsere Experten sowie unser weltweites Netzwerk von Security Operations Centers bereitgestellt und bietet Netzwerküberwachung und On-Demand-Analysen rund um die Uhr an sieben Tagen die Woche.

SECURITY RESEARCH AND OPERATIONS (SR&O)

Die Security Research & Operations (SR&O) zeichnen für das Bedrohungs-und Schwachstellenmanagement der Produkte und Services von Cisco verantwortlich und koordinieren die Aktivitäten des branchenführenden Product Security Incident Response Team (PSIRT). Auf Veranstaltungen wie Cisco Live und Black Hat bieten die SR&O in Zusammenarbeit mit Cisco Partnern und anderen Branchenvertretern eine Anlaufstelle bei Fragen bezüglich aktueller Entwicklungen in der Bedrohungslandschaft. Daneben sind die SR&O an der Entwicklung und Bereitstellung von innovativen Services wie Cisco Custom Threat Intelligence (CTI) beteiligt, mit der Indicators-of-Compromise erkannt werden können, die anderen Sicherheitsinfrastrukturen entgangen sind.

ADVANCED SECURITY RESEARCH AND GOVERNMENT (ASRG)

Advanced Security Research and Government (ASRG) ist einer der Richtungsgeber für die langfristige Security-Strategie und -Vision von Cisco. In dieser Rolle führt ASRG in zentralen Bereichen der IT-Sicherheit, darunter fortschrittliche Kryptografie und Sicherheitsanalytik, interne Untersuchungen bei Cisco durch. Darüber hinaus unterstützt ASRG Hochschulen und Universitäten sowohl durch finanzielles als auch durch persönliches Engagement dabei, Lösungen für langfristige Herausforderungen zu erarbeiten.

CISCO SECURITY INCIDENT RESPONSE SERVICES (CSIRS)

Das Team der Cisco Security Incident Response Services (CSIRS) unterstützt Cisco Kunden durch umfassendes Know-how, Security-Lösungen der Enterprise-Klasse, hochmoderne Response-Techniken und seit langem bewährte Verfahren zur Abwehr von Cyberangriffen dabei, Angriffe proaktiv zu vereiteln, im Ernstfall schnell zu reagieren und den Geschäftsbetrieb zügig wiederherzustellen.

Grafiken zum Download

Alle Grafiken aus diesem Report können Sie hier herunterladen: **www.cisco.com/go/mcr2016graphics.com**

Aktualisierungen und Korrekturen

Aktualisierungen und Korrekturen zu diesem diesen Report finden Sie hier: **www.cisco.com/go/mcr2016errata.com**

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

Hauptgeschäftsstelle Asien-Pazifik-Raum
Cisco Systems (USA) Pte. Ltd.
Singapur

Hauptgeschäftsstelle Europa
Cisco Systems International BV Amsterdam,
Niederlande

Cisco verfügt über mehr als 200 Niederlassungen weltweit. Die Adressen mit Telefon- und Faxnummern finden Sie auf der Cisco Website unter **www.cisco.com/go/offices**.

Veröffentlicht im Juli 2016