Schutz vor modernen kritischen Bedrohungen

Bedrohungsbericht von Februar 2019

cisco

Inhalt

Zurückschauen und weiterkommen

Wenn es um die Bedrohungslandschaft geht, sollte man gelegentlich einen Blick in den Rückspiegel werfen.

Wie beim Autofahren erfahren Sie dabei nicht nur, was hinter Ihnen liegt; sie sehen oft auch, ob etwas schnell auf Sie zukommt und Sie überholen will.

Und darum geht es in diesem Bedrohungsbericht. Wir haben fünf wichtige Geschichten aus dem letzten Jahr ausgewählt – nicht nur, weil es sich dabei um große Ereignisse handelte, sondern weil wir glauben, dass diese oder ähnliche Bedrohungen in naher Zukunft wieder auftreten könnten.

Nehmen wir modulare Bedrohungen wie Emotet und VPNFilter als Beispiel. Dies sind Bedrohungen, die ein On-Demand-Menü aus Angriffen und Bedrohungen bereitstellen können, je nachdem, welches Gerät infiziert oder das Ziel des Angreifers ist. Wir haben in der jüngeren Geschichte viele dieser modularen Bedrohungen erlebt und wären nicht überrascht, wenn wir in Zukunft noch mehr davon sehen würden.

E-Mails bleiben weiterhin die beliebteste Methode für Hacker, um Krypto-Mining zu betreiben oder Emotet einzuschleusen. Es ist auch sehr wahrscheinlich, dass andere Bedrohungen wie nicht autorisierte MDM-Profile genutzt werden. Dies macht deutlich, dass Sie Ihren Posteingang genau im Auge behalten sollten.

Vorgehensweise

Die Hauptmotivation von Angreifern ist immer noch Geldschneiderei: Malware verfolgt den Weg des Geldes. Krypto-Mining-Bedrohungen haben exakt dieses Ziel. Emotet hat sich mittlerweile zu einem Verteilnetz für Bedrohungen entwickelt, das verschiedene Methoden zum Geldverdienen nutzt.

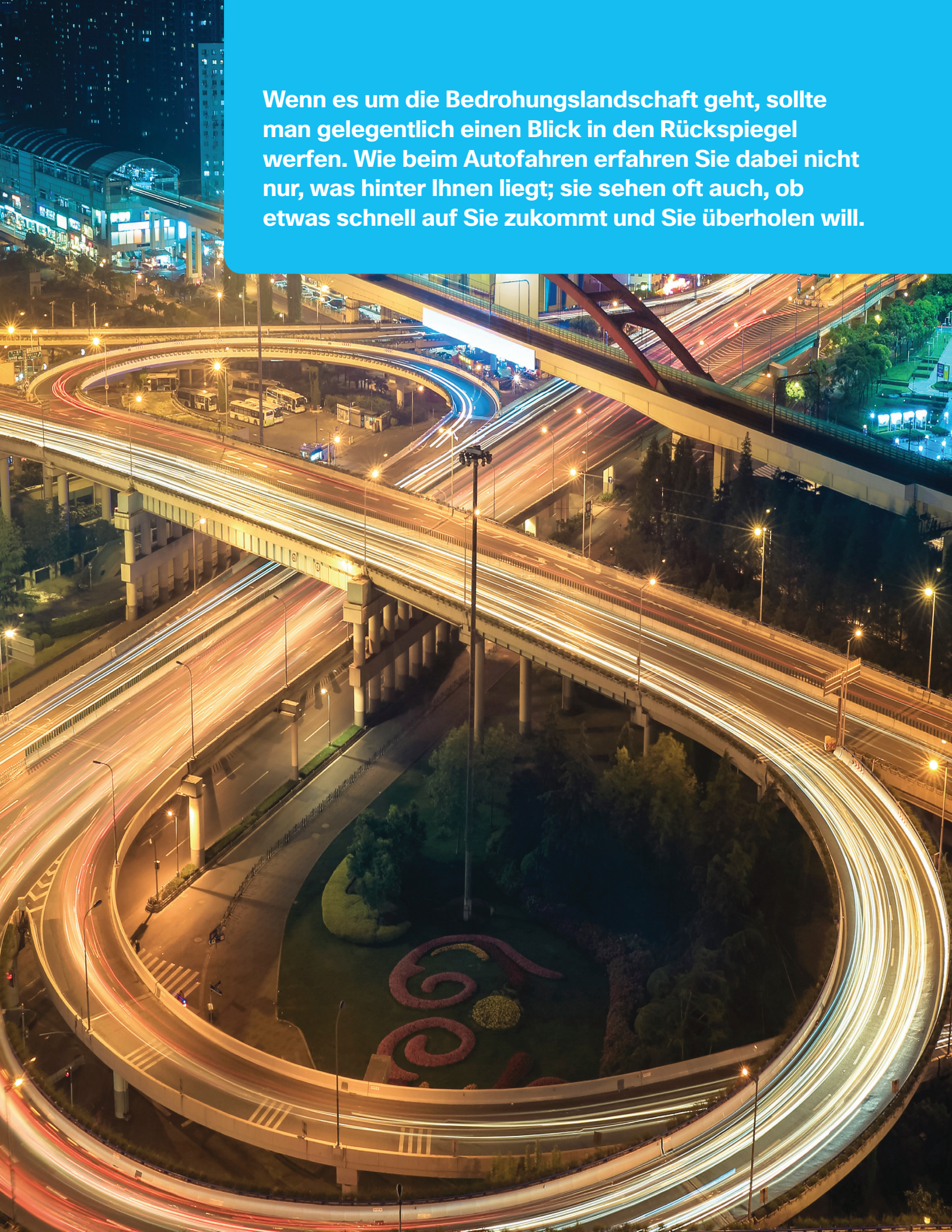
Der Datendiebstahl ist ebenfalls ins Rampenlicht gerückt. Er war das Hauptmotiv für viele aktuelle Bedrohungen wie VPNFilter, die allem Anschein nach für den Diebstahl von Daten konzipiert waren. Der Trojaner Emotet stiehlt nicht nur Anmeldeinformationen für das Netzwerk, sondern unterstützt auch die Verbreitung von Trickbot, einem weiteren notorischen Banking-Trojaner, der Informationen klaut.

Wir haben fünf wichtige Geschichten ausgewählt, weil wir glauben, dass diese oder ähnliche Bedrohungen erneut auftreten könnten.

Abschließend sei bemerkt, dass einige Bedrohungen einfach nur Zerstörung anrichten wollen, wie es der Fall bei Olympic Destroyer ist. Wir haben einige solcher Bedrohungen im letzten Jahr gesehen, aber keine hat die Überschriften so dominiert wie der Angriff, dessen einziger Zweck es offenbar war, die Olympischen Spiele zu stören.

Während wir also auf einige der beeindruckendsten Bedrohungen von 2018 zurückblicken, müssen wir bedenken, was diese Bedrohungen so erfolgreich gemacht hat. Viele dieser Bedrohungen sind womöglich ein Ding der Vergangenheit, aber haben Sie diese wirklich hinter sich gelassen oder schicken sie sich an, Sie und Ihre Sicherheitsstrategie zu überholen?

Wenn es um die Bedrohungslandschaft geht, sollte man gelegentlich einen Blick in den Rückspiegel werfen. Wie beim Autofahren erfahren Sie dabei nicht nur, was hinter Ihnen liegt; sie sehen oft auch, ob etwas schnell auf Sie zukommt und Sie überholen will.



Angriffsarten und Schutz

Ein mehrstufiger Sicherheitsansatz ist immer ratsam. Wir haben am Ende jeder Geschichte Symbole eingesetzt, um auf die wichtigsten (vermutlich) verwendeten Bedrohungsvektoren und die Tools hinzuweisen, die im jeweiligen Fall gegen sie verwendet werden können. Nachstehend erklären wir die Symbole und sprechen über die Vorteile, die eine Bereitstellung diverser Schutzmaßnahmen als Teil einer integrierten Sicherheitsarchitektur mit sich bringt.

Erweiterte Malware-Erkennungs- und Schutztechnologie (wie Cisco Advanced Malware Protection, oder AMP) kann unbekannte Dateien nachverfolgen, bekannte schädliche Dateien blockieren und die Ausführung von Malware auf Endpunkten oder Netzwerkgeräten verhindern.

Netzwerksicherheitslösungen wie die Cisco Next-Generation Firewall (NGFW) und das Next-Generation Intrusion Prevention System (NGIPS) können schädliche Dateien daran hindern, über das Internet ins Netzwerk einzudringen oder sich innerhalb des Netzwerks auszubreiten. Netzwerktransparenz- und Sicherheitsanalyseplattformen wie Cisco Stealthwatch können interne Netzwerkanomalien erkennen, die womöglich auf eine Aktivierung von Malware als Payload hinweisen. Und schließlich kann mit Segmentierung die laterale Bewegung von Bedrohungen innerhalb eines Netzwerks verhindert und eine Ausbreitung des Angriffs eingedämmt werden.

Webscanning an einem Secure Web Gateway (SWG) oder **Secure Internet Gateway (SIG)** wie Cisco Umbrella bedeutet, dass Sie Benutzer (innerhalb oder außerhalb des Unternehmensnetzwerks) daran hindern können, sich mit schädlichen Domänen, IP-Adressen und URLs zu verbinden. Dies verhindert, dass Mitarbeiter Malware unabsichtlich Zugang zum Netzwerk gewähren und dass sich Malware, die es ins Netzwerk geschafft hat, sich mit einem Command-and-Control-Server verbindet.

E-Mail-Sicherheitstechnologie (z. B. Cisco Email Security), die vor Ort oder in der Cloud bereitgestellt wird, blockiert schädliche E-Mails, die von Bedrohungsakteuren im Rahmen ihrer Kampagnen gesendet werden. Dies verringert die Gesamtmenge an Spam-Nachrichten, entfernt schädliche Spam-Nachrichten und scannt alle Komponenten einer E-Mail (z. B. Absender, Betreff, Anhänge und eingebettete URLs), um Nachrichten mit Bedrohungen zu finden. Diese Funktionen sind entscheidend, da E-Mails von Bedrohungsakteuren immer noch gerne als Ausgangspunkt für Angriffe verwendet werden.

Fortschrittliche Malware-Erkennung und Schutztechnologie, wie Cisco AMP für Endpunkte kann die Ausführung von Malware auf dem Endpunkt verhindern. Sie kann außerdem helfen, infizierte Endgeräte zu isolieren, zu untersuchen und zu warten, wenn ein Prozent der Angriffe selbst die stärksten Abwehrmaßnahmen überwinden sollte.

Der Wandel von Emotet: vom Banking zur Distribution

Emotet hielt sich jahrelang im Hintergrund. Diese Taktik hat sich als hilfreich erwiesen.

In der Bedrohungslandschaft sorgen ziemlich häufig Angriffe für Schlagzeilen, die ein Novum darstellen. Es wird beispielsweise eine Sicherheitslücke entdeckt, die sich auf eine große Anzahl an Geräten auswirkt oder es stellt sich heraus, dass ein Angriff gegen eine große Organisation ausgeführt wurde.

Die am weitesten verbreiteten Bedrohungen schaffen es jedoch nie ins Rampenlicht. Sie setzen eher auf bewährte Methoden, anstatt die neuesten und besten Techniken. Und das spielt den Angreifern in die Hände. Was unbemerkt eindringt, kann weiter wachsen, was bei den aufsehenerregenden Angriffen eher nicht der Fall ist.

Emotet ist ein Paradebeispiel dafür. Während Bedrohungen wie WannaCry und NotPetya in den Medien heiß diskutiert wurden, blieb Emotet jahrelang im Hintergrund. Diese Taktik hat sich für den Trojaner als hilfreich erwiesen, der mittlerweile zu den erfolgreichsten Bedrohungsarten gezählt wird.

Der Erfolg des Trojaners Emotet liegt in der Art und Weise, wie er sich entwickelt hat. Nach seinen „bescheidenen“ Anfängen als Banking-Trojaner schwenkten die Bedrohungsakteure bald um und machten aus der Bedrohung eine modulare Plattform, die eine Vielzahl verschiedener Angriffe ausführen kann. Wir kehren schnell in die Gegenwart zurück und erkennen, dass andere Bedrohungsarten, die früher als Gegner betrachtet wurden, den Trojaner jetzt zur Verbreitung ihrer Schadprogramme benutzen. Und während sich die Bedrohungslandschaft wieder wandelt, haben jetzt alle Emotet auf dem Schirm.

Von bescheiden zu modular

Als Emotet zum ersten Mal auf der Bildfläche erschien, war er einer von vielen Banking-Trojanern. Die Bedrohung wurde über Spam-Kampagnen eingeschleppt, üblicherweise mithilfe von Spam-Nachrichten zum Thema Rechnung oder Zahlung. Es wurde häufig als Office-Dokument mit aktivierten Makros, als JavaScript-Datei oder als in den Mailtext eingebetteter Link verschickt. Die Verteilungstechniken variierten, allerdings richteten sich viele der Kampagnen gegen Banken in bestimmten Regionen, insbesondere deutschsprachige Länder in Europa und die USA.

Zunächst war die Bedrohung vor allem darauf ausgelegt, Banking-Informationen zu stehlen, etwa Benutzernamen, Kennwörter, E-Mail-Adressen und andere finanzielle

E-Mail: der häufigste Angriffsvektor

Ein Thema, dem wir bei den meisten großen Bedrohungen von heute immer wieder begegnen, sind E-Mails. Sie bleiben der am weitesten verbreitete Angriffsvektor für Bedrohungsakteure, um ihre Schadprogramme zu verbreiten, und das wird sich in naher Zukunft wahrscheinlich auch nicht ändern.

Sehen wir uns Emotet als Beispiel an. Woche für Woche starten die Angreifer hinter dem Trojaner zahllose neue Phishing-Kampagnen.

Dasselbe gilt für bösartiges Krypto-Mining, bei dem Spam-Kampagnen die Benutzer ständig dazu verleiten, schädliche Mining-Programme auf ihren Computer herunterzuladen.

Und was MDM-Bedrohungen (Mobile Device Management; mobile Geräteverwaltung) angeht, diese Angriffe fingen höchstwahrscheinlich mit gefälschten E-Mails an.

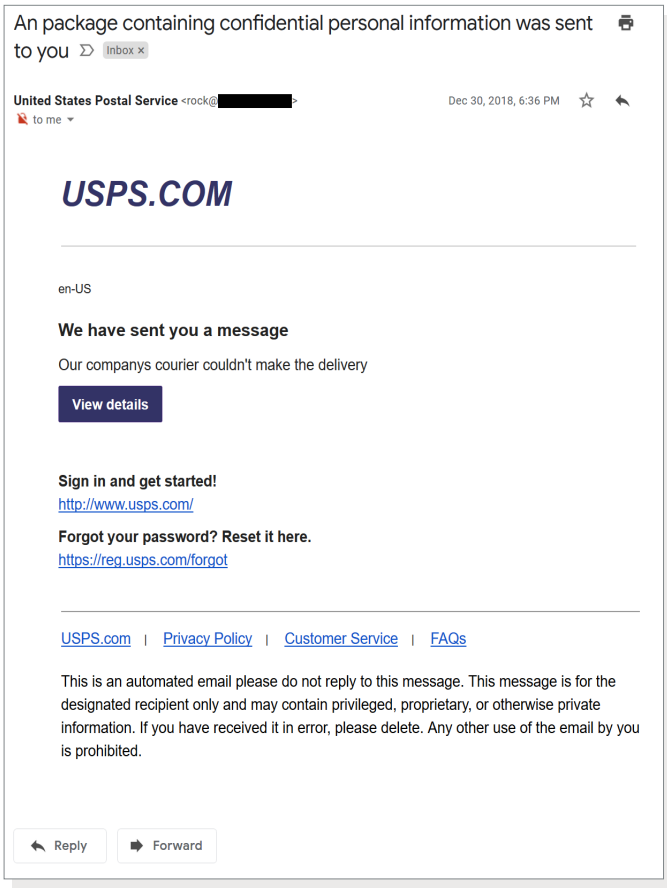
(Forts.)

Informationen. Im Laufe der Zeit begann Emotet, sich auf allgemeinere Zielgruppen zu verbreiten. Eine neue Version der Bedrohung legte den Grundstein für die modulare Konfiguration, die wir heute kennen und verschiedene Tools für verschiedene Funktionen umfasst. Einige Module stehlen E-Mail-Anmeldeinformationen, während andere sich auf die Benutzernamen und Kennwörter konzentrieren, die im Browser gespeichert sind. Andere bieten DDOS-Funktionen (Distributed Denial-of-Service), während wieder andere Ransomware verteilen.

Das überrascht angesichts der überzeugenden Gestaltung vieler Phishing-E-Mails auch nicht, erst recht, wenn sie auf dem Mobiltelefon angezeigt werden. Und vielbeschäftigte Benutzer kann der dringende Ton der E-Mail dazu verleiten, sofortige Maßnahmen zu ergreifen. Die verdächtigen Anzeichen einer anstehenden Bedrohung werden dabei leicht übersehen.

Da ist es kein Wunder, dass sich Angreifer immer wieder der E-Mail bedienen, um ihre Malware zu verbreiten.

Abbildung 1 Beispiel für eine Spam-E-Mail von Emotet



Geld her

Der Hauptzweck von Emotet liegt darin, eine Möglichkeit zu finden, aus einem kompromittierten Rechner Geld herauszuschlagen. Und hier kommen die Module ins Spiel. Anscheinend werden sie auf einem bestimmten Gerät dort installiert, wo am meisten Geld zu holen ist. Spielen Sie folgende Szenarien durch:

- Zeigt die Browserchronik auf dem Rechner häufige Aufrufe von Banking-Webseiten an? Stellen Sie Banking-Module bereit, um Anmeldeinformationen zu stehlen und Geld zu überweisen.
- Handelt es sich bei dem Gerät um einen Spitzenlaptop, der vermuten lässt, dass der Eigentümer verfügbares Einkommen hat? Stellen Sie Module für die Malware-Verteilung bereit und installieren Sie Ransomware oder Krypto-Mining-Software.
- Handelt es sich bei der Maschine um einen Server in einem Netzwerk mit hoher Bandbreite? Installieren Sie Module für die E-Mail- und Netzwerkverteilung, um Emotet weiter zu verbreiten.

Ganovenehre

Was Emotet wirklich von vielen Bedrohungen in der heutigen Bedrohungslandschaft unterscheidet, ist nicht nur seine Reichweite und Modularität, sondern die Tatsache, dass die dahinter stehenden Akteure den Trojaner anderen Angreifergruppen als Distributionskanal zur Verfügung stellen wollen.

Wir haben beispielsweise Situationen beobachtet, in denen Emotet einen Computer nur infiziert, um Trickbot als Payload in das System einzuschleusen. In diesem scheinbar widersprüchlichen Fall schleust der Trojaner Emotet, der als Banking-Trojaner wohlbekannt ist, einen weiteren Banking-Trojaner ein, anstatt seine eigenen Module für Datendiebstahl zu nutzen. Noch interessanter ist die Tatsache, dass der Trojaner Trickbot die Ransomware Ryuk nachlädt, nachdem er selbst eingeschleust wurde.

Es mag seltsam klingen, aber die verschiedenen Gruppen arbeiten wahrscheinlich deshalb zusammen, weil sie gemeinsam das meiste Geld einstreichen können. Wenn Emotet ein Gerät nicht zur weiteren Verbreitung nutzen kann, kann Trickbot die Banking-Informationen stehlen. Werden keine Banking-Informationen gefunden, kann Ryuk das Gerät verschlüsseln und Lösegeld verlangen. Wie lange diese unheilige Allianz anhält, weiß natürlich keiner.

Was die Zukunft bereithält

Natürlich bleibt eine Bedrohung, die größere Ausmaße annimmt, nur selten unbemerkt. Ende 2018 wurde die Security-Branche endlich auf die Auswüchse von Emotet aufmerksam. Grund dafür ist die Tatsache, dass sich Verteiler von Spam-Nachrichten von Krypto-Mining-Payloads abgewandt und stattdessen auf die Verteilung von Emotet und Remote-Zugriffs-Trojaner (RATs) verlegt haben. Und diese Auswirkungen sind spürbar. Tatsächlich hat es laut US-CERT

Die Angreifer, die hinter Emotet stehen, scheinen den Trojaner auch anderen Angreifergruppen als Distributionskanal zur Verfügung stellen zu wollen.

bis zu 1 Millionen USD gekost, um Emotet-Infektionen zu beseitigen.

Es ist eher unwahrscheinlich, dass Emotet allmählich verschwindet; vielmehr wird der Trojaner die Bedrohungslandschaft auf absehbare Zeit dominieren. Und wenn die Vergangenheit irgendwie auf die Zukunft schließen lässt, wird Emotet schließlich verebben und durch einen anderen dominanten Player in der Bedrohungslandschaft ersetzt werden.

Für einen tieferen Einblick in dieses Thema siehe:

https://blog.talosintelligence.com/2019/01/return-of-emotet.html

https://www.us-cert.gov/ncas/alerts/TA18-201A

https://duo.com/decipher/the-unholy-alliance-of-emotet-trickbot-and-the-ryuk-ransomware

https://blog.talosintelligence.com/2018/12/cryptocurrency-future-2018.html

IoT-Umtriebe: der Fall VPNFilter

Bild: Talos

VPNFilter ist ein Vorbote für das, was zwangsläufig noch auf uns zukommen wird.

Im vergangenen Jahrzehnt gab es eine Reihe bemerkenswerter Bedrohungen im Zusammenhang mit dem Internet of Things (IoT). Beispielsweise das Mirai-Botnet, das IP-Kameras und Router infizierte, um DDoS-Angriffe auszuführen. Und wer könnte die Babyphone-Angriffe vergessen, bei denen Eltern ins Kinderzimmer kamen und Hacker mit ihren Kindern sprechen hörten, nachdem sie das Gerät gehackt hatten?

Ob es Ihnen gefällt oder nicht, das IoT hat mit Smart Assistants und Krankenhausgeräten mit Internetanschluss in unserem Heim und am Arbeitsplatz Einzug gehalten. Leider wurde bei diesem Prozess in vielen Fällen die Festlegung geeigneter Sicherheitsmaßnahmen übersehen. Uns wir mussten demzufolge erleben, wie diese Geräte von Cyberkriminellen ins Visier genommen wurden.

Doch nichts war so bösartig wie VPNFilter. Diese Bedrohung richtete sich gegen zahlreiche Router von verschiedenen Herstellern und nutzte wahrscheinlich nicht gepatchte Sicherheitslücken aus, um sie zu kompromittieren. Bei diesen Angriffen sollten anscheinend vertrauliche Daten aus den betroffenen Netzwerken herausgeschleust werden. Doch die Malware enthielt auch ein modulares System, das deutlich mehr anrichten konnte und daher besonders besorgniserregend war.

Insgesamt waren mindestens eine halbe Millionen Geräte in 54 Ländern von der Bedrohung betroffen. Zum Glück bemerkten die Forscher der Cisco Talos-Gruppe diese schon frühzeitig. Als die Anzahl der Infektionen anstieg, konnten sie diese zum Stillstand bringen. Heute geht von VPNFilter dank der Arbeit von Threat Intelligence-Partnern aus dem öffentlichen und privaten Sektor sowie der Gesetzeshüter kaum mehr eine Bedrohung aus. Trotzdem ist VPNFilter ein Vorbote für das, was zwangsläufig noch auf uns zukommen wird.

Die Durchführung

Stufe eins – VPNFilter verfügt über drei Hauptkomponenten, oder „Stufen", die die Bedrohung ausmachen. Das oberste Ziel der ersten Stufe ist, sich dauerhaft auf einem Gerät einzunisten. Vor VPNFilter konnte man sich der Malware, die auf IoT-Geräte abzielte, normalerweise durch einen einfachen Neustart des Geräts entledigen. Wegen der Komponente der Stufe eins in VPNFilter übersteht die Malware einen solchen Versuch. Stufe eins umfasst außerdem mehrere Optionen, um eine Verbindung zum Command-and-Control-Server (C2-Server) herzustellen, welcher der Malware sagt, was sie tun soll.

Stufe zwei – ist die entscheidende Komponente bei der Verfolgung der böswilligen Ziele von VPNFilter; sie ermöglicht beispielsweise Dateisammlung, Befehlsausführung, Datenausschleusung und Gerätemanagement. Einige Varianten der Stufe zwei enthalten sogar einen „Kill-Switch", der das infizierte Gerät dauerhaft unbrauchbar machen kann, wenn er aktiviert wird.

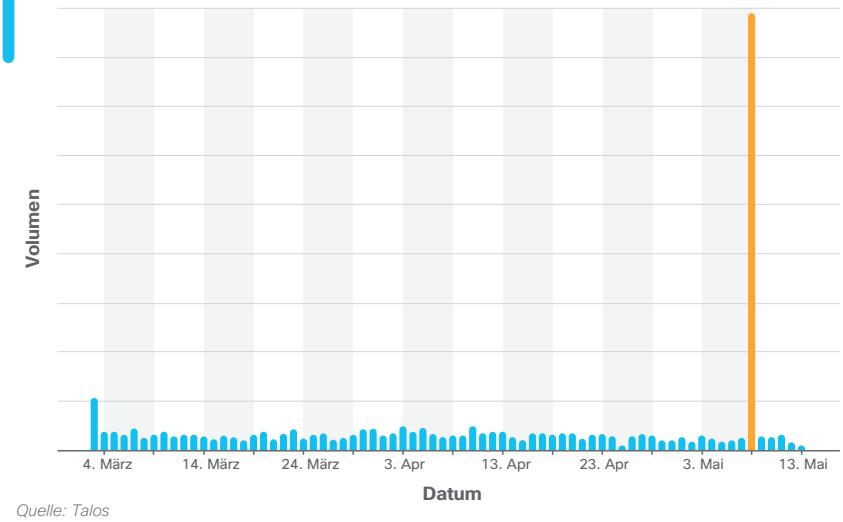
Stufe drei – erweitert die Funktionen von Stufe zwei und stellt Plug-ins bereit, die weitere schädliche Aktionen erleichtern. Einige dieser Plug-ins können Folgendes:

- Den Netzwerkdatenverkehr überwachen
- Verschiedene Anmeldeinformationen stehlen
- Bestimmten Datenverkehr von industriellen IoT-Geräten überwachen
- Die Kommunikation mit dem C2-Server verschlüsseln
- Netzwerke zuweisen
- Endpunktsysteme ausnutzen
- Sich auf andere Netzwerke ausbreiten
- DDoS-Angriffe ausführen
- Ein Proxy-Netzwerk erstellen, das dazu verwendet werden könnte, die Quelle für zukünftige Angriffe zu verbergen

VPNFilter startet (beinahe) durch

Talos hatte VPNFilter mehrere Monate lang untersucht und festgestellt, dass die Infektionsrate relativ konstant war. Das Team hatte infizierte Geräte überwacht und gescannt, um die Bedrohung und die in der Malware enthaltenen Funktionen besser nachvollziehen zu können.

Abbildung 2 Neue VNPFilter-Infektionen pro Tag



Quelle: Talos

Das war zumindest bis zum 8. Mai 2018 so, als plötzlich eine deutliche Zunahme der Infektionsaktivität verzeichnet wurde. Und nicht nur das, die Mehrzahl der Infektionen wurden in der Ukraine festgestellt. Am 17. Mai, etwa ein Jahr nach dem NotPetya-Angriff, kam es in der Ukraine zu einem weiteren Schub an VPNFilter-Infektionen. Angesichts der Tatsache, dass es in der Ukraine mehrere zerstörerische Angriffe gegeben hatte, entschloss sich Talos, möglichst bald gegen diesen Infrastrukturangriff anzugehen, obwohl die Untersuchungen weitergingen.

Talos fuhr mit seinen Ermittlungen fort und veröffentlichte Informationen über das Botnet, bis die Gruppe im September 2018 das Ende der Bedrohung verkünden konnte.

Vorbei, aber nicht vergessen

Bedrohungen wie VPNFilter mögen zwar der Vergangenheit angehören, jedoch werden leider immer noch Sicherheitslücken in IoT-Geräten gefunden. Dass sich in Zukunft weitere Bedrohungen gegen das IoT richten werden, ist fast unausweichlich.

Derartige Bedrohungen abzuwenden ist schwierig. IoT-Geräte wie Router sind in der Regel direkt mit dem Internet verbunden. Und weil viele Benutzer nicht über das technische Know-how verfügen, Patches anzuwenden oder diese Geräte nicht für eine Bedrohung halten, kann die Situation sehr gefährlich werden.

Letztendlich wird das IoT als Teil des Netzwerks immer weiter wachsen. VPNFilter zeigt uns, was passieren kann, wenn wir in Zukunft nicht die richtigen Maßnahmen zum Schutz dieser Geräte ergreifen.

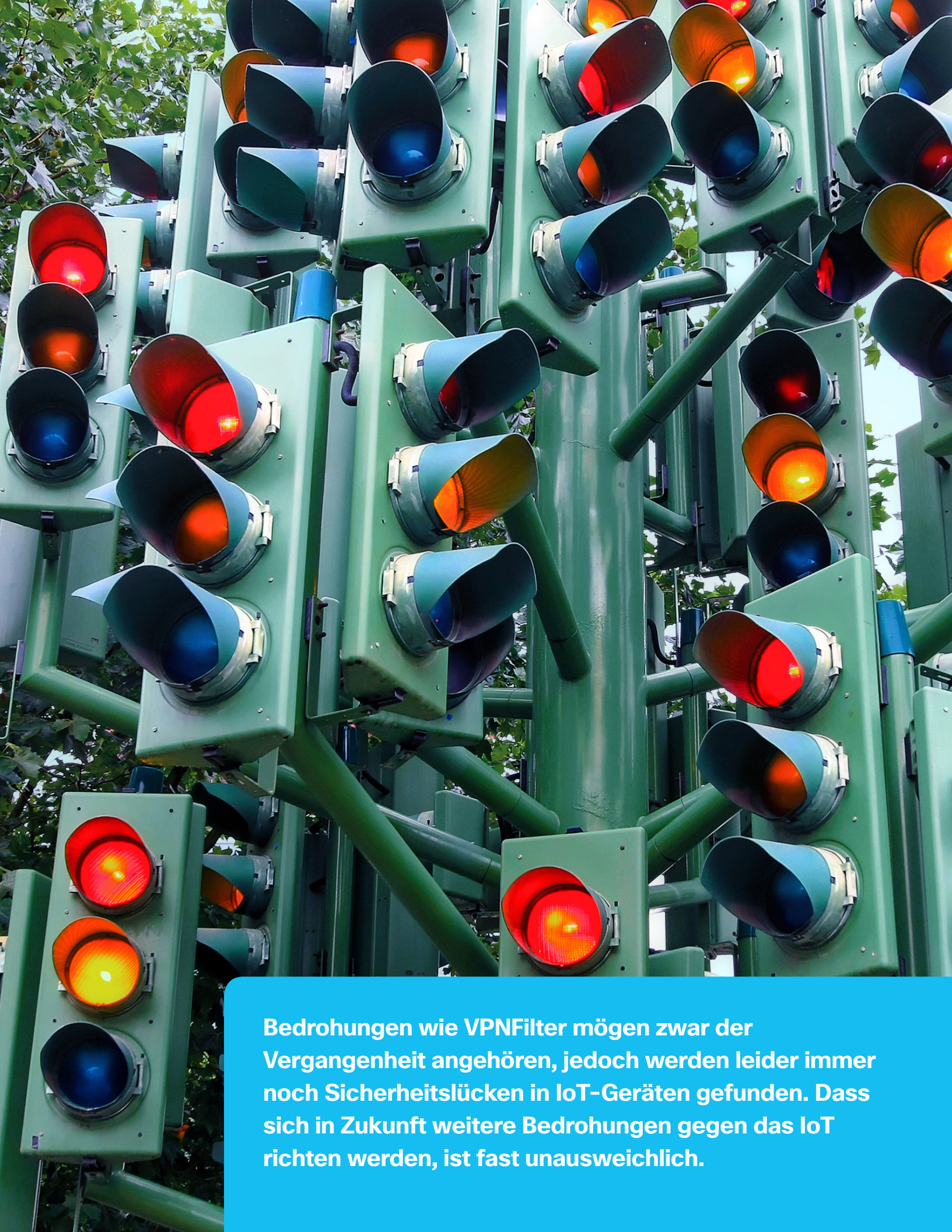
Für einen tieferen Einblick in dieses Thema siehe:

https://blog.talosintelligence.com/2018/05/VPNFilter.html

https://blog.talosintelligence.com/2018/06/vpnfilter-update.html

https://blog.talosintelligence.com/2018/09/vpnfilter-part-3.html

https://blog.talosintelligence.com/2018/12/year-in-malware-2018-most-prominent.html



Bedrohungen wie VPNFilter mögen zwar der Vergangenheit angehören, jedoch werden leider immer noch Sicherheitslücken in IoT-Geräten gefunden. Dass sich in Zukunft weitere Bedrohungen gegen das IoT richten werden, ist fast unausweichlich.

Mobile Geräteverwaltung: Fluch und Segen

Talos entdeckte, dass Cyberkriminelle herausgefunden haben, wie Sie MDM für böswillige Zwecke nutzen können.

Die MDM-Funktionalität (Mobile Device Management; mobile Geräteverwaltung) war für Unternehmen ein wahrer Segen. Organisationen können damit viel mehr Kontrolle über die Geräte in ihrem Netzwerk übernehmen. Wie wir jedoch 2018 feststellen mussten, hat die Funktion kapitalkräftigen Cyberkriminellen Tür und Tor geöffnet.

Was mobile Malware angeht, sind mobile Betriebssysteme nur schwer zu knacken. Das geschlossene System, das um mobile Betriebssysteme herum errichtet wurde, bietet gegen schädliche Apps hinreichenden Schutz.

Das soll aber nicht heißen, dass Cyberkriminelle nicht versucht hätten, Mobiltelefone anzugreifen. Es wurden schädliche Apps in offiziellen App Stores entdeckt, doch in den meisten Fällen beschränkten sich Angreifer auf die Kompromittierung von Geräten, die entsperrt wurden, einem sogenannten „Jailbreak“ (unautorisiertes Entfernen von Nutzungsbeschränkungen) zum Opfer gefallen sind oder Apps von Drittanbietern akzeptieren.

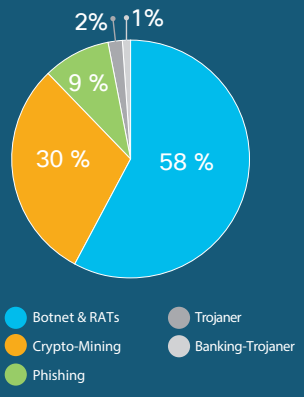
Das geschlossene System ist sicher, kann sich aber auch als Gefängnis erweisen. Der Nachteil dieser Einschränkung und der damit verbundenen Sicherheit ist, dass Sie nur Apps aus einem offiziellen App Store installieren können oder das Gerät für alle Drittanbieter-Apps offen lassen (sofern verfügbar). Dies wird ein Problem für Unternehmen, die proprietäre Anwendungen erstellen, auf die nur ihre Mitarbeiter zugreifen können sollen, und die ihre Geräte gleichzeitig schützen wollen.

Die Einführung der mobilen Geräteverwaltung (MDM)

Um diese Anforderungen zu erfüllen, wurden MDM-Systeme eingeführt. Diese erlauben Unternehmen, ihre eigenen Mobiltelefone herzunehmen und darauf Profile zu erstellen, die bei ihrem Unternehmen registriert sind, und letztlich beliebige Anwendungen darauf zu installieren. MDM bietet häufig auch andere unternehmensfreundliche Funktionen wie die Möglichkeit, Geräteeinstellungen zu kontrollieren, den Zugriff auf unerwünschte Websites zu unterbinden oder verloren gegangene Geräten zu finden.

Eine Momentaufnahme von Sicherheitsvorfällen

Welches sind die häufigsten Sicherheitsvorfälle in Organisationen? Unsere Kollegen der Cisco Cognitive Intelligence Group haben es für uns ausgerechnet. Hier ist eine Momentaufnahme der fünf Hauptkategorien (vom Juli 2018).



Insgesamt führen Botnets und RATs die Liste der Sicherheitsvorfälle an. Zu dieser Kategorie gehören Bedrohungen wie Andromeda und Xtrat.

Die zweitgrößte Bedrohungskategorie ist das Krypto-Mining, in der unter anderem die nicht autorisierten Mining-Programme Monero und Coinhive entdeckt wurden.

Das auffälligste Merkmal dieses Snapshots ist, wie gering der Anteil an Banking-Trojanern ausfällt. Dies wird sich zweifellos ändern, wenn Emotet an Boden gewinnt.

Wir werden auf diese Metrik in zukünftigen Berichten zurückkommen und beobachten, wie sie sich verändert.

Bild: Talos

Es steht außer Frage, dass MDM ein leistungsstarkes Tool ist. Und zwar so leistungsstark, dass Cisco Talos Folgendes erkannte: Cyberkriminelle haben einen Weg gefunden, um es für böswillige Zwecke zu missbrauchen.

Es begann in Indien

Unsere Forscher bei Talos entdeckten Geräte in Indien, die mithilfe eines Open-Source-MDM-Systems kompromittiert wurden. Den Angreifern war es gelungen, schädliche Profile auf die Geräte zu laden und Apps zu installieren, die beispielsweise Daten abfangen, SMS-Nachrichten stehlen, Fotos und Kontakte herunterladen und den Standort der Geräte nachverfolgen sollten.

Die Apps enthielten modifizierte Versionen von gängigen Anwendungen wie WhatsApp und Telegram, die zusätzliche, oder „quergeladene“ Funktionen enthielten, welche den Angreifern das Abhören von Konversationen auf jedem kompromittierten Gerät erlaubten.

Wie diese Geräte diesem Angriff zum Opfer fielen, ist schleierhaft. Es ist möglich, dass die Angreifer physischen Zugriff auf die Geräte hatten und sie so ein Profil installieren konnten, das ihnen Kontrolle darüber gab. Es ist jedoch auch denkbar, dass die Angreifer eine Social-Engineering-Taktik verwendeten, um Benutzer zur Installation des Profils zu verleiten.

Die böswillige Meldung könnte per E-Mail oder SMS versandt worden sein, um den Benutzer glauben zu machen, dass sie das schädliche Profil dringend installieren mussten. Trotzdem würde der Benutzer eine Reihe von Anweisungen befolgen und sich durch diverse Aufforderungen klicken müssen, bevor das Gerät vollständig kompromittiert wurde.

Pflege Ihres geschlossenen Systems

Hierbei handelt es sich zweifelsohne um eine wirksame und besorgniserregende Angriffsmethode. Zum Glück ist sie selten. Die von Talos enthüllte Angriffskampagne ist die einzige öffentlich bekannte Kampagne dieses Typs. Sie ist außerdem schwer durchzuführen, wenn man bedenkt, wie viele

Angesichts des potenziellen Gewinns werden wir in Zukunft wahrscheinlich noch mehr dieser Angriffe erleben, die von kapitalkräftigen Cyberkriminelle durchgeführt werden.

Schritte Benutzer ausführen müssen, bis das Gerät für schädliche Aktivitäten konfiguriert ist. Jedoch ist der potenzielle Gewinn hoch und Talos stellt bereits mehr Angriffe auf Mobilgeräte fest, die von kapitalkräftigen Cyberkriminellen durchgeführt werden.

Paradoxerweise ist der beste Schutz gegen einen MDM-Angriff die mobile Geräteverwaltung.

Organisationen sollten sicherstellen, dass Unternehmensgeräte Profile enthalten, welche die Installation von schädlichen Profilen oder von Apps aus Drittanbieter-App-Stores überwachen und verhindern können.

Auch die Benutzer müssen für den MDM-Installationsvorgang sensibilisiert und zu diesen Angriffen geschult werden. Nur so wird vermieden, dass sie eine schädliche MDM-Software installieren.

Für einen tieferen Einblick in dieses Thema siehe:

https://blog.talosintelligence.com/2018/07/Mobile-Malware-Campaign-uses-Malicious-MDM.html

https://blog.talosintelligence.com/2018/07/Mobile-Malware-Campaign-uses-Malicious-MDM-Part2.html

Was ist aus der Ransomware geworden?

Im Jahr 2017 schien es, als ob Ransomware die Bedrohungslandschaft auf lange Zeit dominieren würde. Bedrohungen wie SamSam und Bad Rabbit beherrschten die Schlagzeilen; sie verlangten nach Zahlungen in Kryptowährung, andernfalls würden die Betroffenen alle ihre Daten verlieren.

Etwas über ein Jahr später sieht die Sache schon ganz anders aus.

Ransomware wurde hauptsächlich durch bösartiges Krypto-Mining von seinem Spitzenplatz verdrängt.

Wie kam es so plötzlich dazu? Bei Ransomware bezahlt nur ein kleiner Prozentsatz der Betroffenen das Lösegeld. Und selbst wenn, wäre dies nur eine einmalige Zahlung und keine wiederkehrende Einnahmequelle.

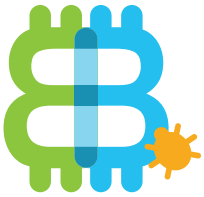
Sie ist außerdem noch riskanter, weil Gesetzeshüter auf der ganzen Welt anfingen, hart gegen Ransomware-Angreifer vorzugehen. Als die Festnahmen in Zusammenhang mit Ransomware anstiegen, wandten sich die Angreifer weniger riskanten Angriffsarten zu.

Das soll nicht heißen, dass Ransomware von der Bildfläche verschwunden ist; wir haben 2018 einige dieser Angriffe festgestellt. GandCrab machte sich weiterhin bemerkbar und Ryuk konnte sich über Infektionen mit Emotet und Trickbot verbreiten. Ohne Ransomware als unangefochtene Superbedrohung müssen wir trotzdem wachsam bleiben, um Infektionen zu vermeiden.

Krypto-Mining: ein Wolf im Schafspelz ist immer noch ein Wolf

Die bei Weitem profitabelste Bedrohung für Angreifer im Jahr 2018 war böswilliges Krypto-Mining. Dies ist ein Thema, das die Threat-Intelligence-Gruppe von Cisco Talos seit einiger Zeit untersucht. Für den Angreifer ist es fast das perfekte Verbrechen: Mining-Programme laufen häufig im Hintergrund und ohne Wissen des Benutzers, sie stehlen deren Rechenleistung und generieren gleichzeitig ein Einkommen für den Angreifer.

Während also Unternehmen Ransomware immer besser in den Griff bekamen und Gesetzeshüter auf der ganzen Welt Ransomware-Angreifer in die Mangel nahmen, wandten sich immer mehr Angreifer der risikoärmeren Beschäftigung zu, bösartige Krypto-Mining-Software zu verbreiten.



Zwischen der vom Benutzer und der von Cyberkriminellen installierten Krypto-Mining-Software gibt es kaum Unterschiede.

Schaf trifft Wolf

Häufig gibt es zwischen der vom Benutzer und der von Cyberkriminellen installierten Krypto-Mining-Software kaum bis gar keine Unterschiede. Die einzige Abweichung besteht in der Zustimmung, denn bösartige Krypto-Mining-Software wird ohne das Wissen des Eigentümers ausgeführt. Diese Tatsache hat für Angreifer einen offensichtlichen Reiz, schließlich können sie sich bereichern, ohne dass das Opfer davon weiß.

Was das Verhältnis aus Risiko und Gewinn angeht, wird Krypto-Mining eher nicht die Aufmerksamkeit der Gesetzeshüter auf sich ziehen. Trotzdem ist jede Software, die ohne Wissen des Eigentümers auf einem Gerät ausgeführt wird, Anlass zur Sorge.

Und Krypto-Mining – ob illegal durchgeführt oder nicht – lohnt sich finanziell. In den letzten paar Jahren und in der ersten Hälfte des Jahres 2018 stieg der Wert von Kryptowährungen enorm an. Wie bei allem, was mit Software zu tun hat und als wertvoll gilt, wurden Cyberkriminelle hellhörig, da ohnehin gerade ein Rückgang von Ransomware zu beobachten war. Und Krypto-Mining bietet wiederkehrende Einnahmen, während das Opfer bei Ransomware in der Regel nur einmal zahlt.

Die Gefahren von bösartigem Krypto-Mining

Aus Sicht der Verteidiger gibt es viele Gründe, sich wegen bösartiger Krypto-Mining-Software Sorgen zu machen. Wie jede andere Software auf einem Computer auch wird sich Krypto-Mining negativ auf die Gesamtleistung des Systems auswirken und mehr Energie verbrauchen. In einem einzigen System mag das noch nicht ins Gewicht fallen, aber wenn sich die Kosten für mehrere Endpunkte in einer Organisation multiplizieren, kann dies zu einem spürbaren Anstieg der Energiekosten führen.

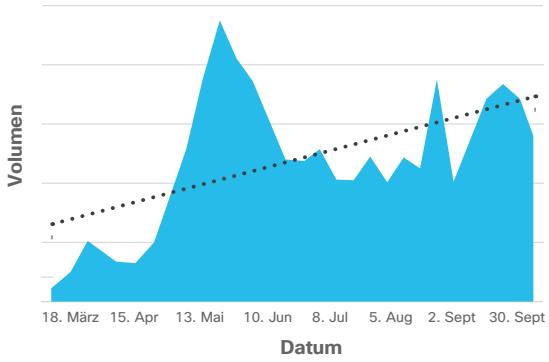
Darüber hinaus kann es Probleme bei der Erfüllung gesetzlicher Auflagen geben, wenn Krypto-Mining-Programme Einnahmen aus Unternehmensnetzwerken generieren. Dies gilt insbesondere für Unternehmen im Finanzsektor, in dem strenge Regeln für aus Unternehmensressourcen generierte Umsätze gelten könnten. Dabei spielt es auch keine Rolle, ob Leute in Führungspositionen darüber Bescheid wissen oder nicht.

Was daran so beunruhigend ist: Das Vorhandensein einer Krypto-Mining-Infektion, die von den Netzwerkbetreuern nicht bemerkt wird, kann auf Sicherheitslücken in der Netzwerkkonfiguration oder den Sicherheitsrichtlinien insgesamt hinweisen. Solche Löcher könnten genau so leicht von Angreifern zu anderen Zwecken genutzt werden. Kurz gesagt: Wenn eine Krypto-Mining-Infektion in einem Netzwerk entdeckt wird, was sollte dann andere Bedrohungen davon abhalten, mittels derselben Sicherheitslücken andere schädliche Aktivitäten auszuführen?

Was passiert jetzt?

Cisco hat im Gesamtvolumen des Krypto-Mining-Datenverkehrs auf DNS-Ebene einige Spitzen und Täler verzeichnet und man geht davon aus, dass der Krypto-Mining-Trend noch einige Zeit anhalten wird.

Abbildung 3 Umfang Krypto-Mining-Datenverkehr in Unternehmens-DNS



Quelle: Cisco Umbrella

Das Interessante dabei ist, dass der Wert vieler gängiger Kryptowährungen während desselben Zeitraums zurückgegangen ist und auf einen nachlassenden Trend verweist. Nehmen Sie zum Beispiel die beliebte Kryptowährung Monero, die für schädliches Krypto-Mining verwendet wird.

Abbildung 4 Monero-Schlusswerte

Quelle: coinmarketcap.com

Cyberkriminelle pushen weiterhin schädliche Krypto-Mining-Software, weil sie sich einfach bereitstellen lässt und das Risiko einer Erkennung gering ist. Wenn diese nämlich einmal auf einem Gerät installiert ist, können Cyberkriminelle damit Geld verdienen, solange sie aktiv bleibt.

Wie kommt schädliche Krypto-Mining-Software in ein System?

Es gibt verschiedene Möglichkeiten, schädliche Krypto-Mining-Software in Ihre Umgebung einzuschleppen, wie:

- Ausnutzung von Sicherheitslücken
- Versenden von E-Mails mit schädlichen Anhängen
- Einsatz von Botnets
- Nutzung von Krypto-Mining im Webbrowser
- Nutzung von Adware-Bedrohungen, die Browser-Plug-ins installieren
- Interne Angreifer

Leider wird schädliches Krypto-Mining für die absehbare Zukunft erhalten bleiben. Und Distributoren von Spam-Nachrichten werden wahrscheinlich weiterhin Krypto-Mining-Bedrohungen versenden.

Wenn Krypto-Mining-Software von Netzwerkadministratoren nicht bemerkt wird, könnte dies auf andere Sicherheitslücken im Netzwerk hinweisen.

Geld ist und wird wahrscheinlich immer eine der Hauptmotivationen für Cyberkriminelle bleiben. In vielerlei Hinsicht kann schädliches Krypto-Mining als eine Möglichkeit für Angreifer betrachtet werden, schnelles Geld mit geringem Aufwand zu verdienen. Das trifft vor allem deshalb zu, weil die Zielpersonen sich weniger Gedanken über die Auswirkungen von Krypto-Mining-Software auf ihren Geräten machen als bei anderen Bedrohungen. Es ist die ideale Gelegenheit für einen Wolf, sich als Schaf zu verkleiden und die Gewinne einzustreichen.

Für einen tieferen Einblick in dieses Thema siehe:

https://blogs.cisco.com/security/cryptomining-a-sheep-or-a-wolf

https://blog.talosintelligence.com/2018/12/cryptocurrency-future-2018.html

https://blog.talosintelligence.com/2018/12/cryptomining-campaigns-2018.html

Auf dem Radar

Für den vorliegenden Bericht haben wir uns eine Vielzahl von Bedrohungen angesehen. Es wurden zwar nicht alle in den Bericht aufgenommen, wir planen aber, in den kommenden Monaten die folgenden Themen in unserer Blog-Reihe Bedrohung des Monats aufzugreifen. Hier ist schon mal ein kleiner Vorgeschmack:

Digitale Erpressung. Eine der hinterhältigeren Phishing-Kampagnen der letzten Zeit nutzte Ängste von Empfängern, um Bitcoin-Zahlungen zu erpressen. Bei einigen Kampagnen wird behauptet, der Empfänger wäre beim Betrachten von pornografischen Websites von einer Kamera gefilmt worden. Andere enthalten falsche Bombendrohungen. Letztendlich handelt es sich dabei allesamt um Lügenmärchen, die möglichst viele Empfänger dazu bringen sollen, die Bitcoin-Wallets der Angreifer zu füllen.

Office 365-Phishing. Eine weitere auffällige Phishing-Kampagne konzentriert sich auf den Diebstahl von Anmeldeinformationen in Microsoft Office 365-Konten. Dafür haben Angreifer verschiedene Methoden verwendet. Wir werden die verschiedenen Kampagnen in unserem nächsten Blog-Beitrag beschreiben und aufzeigen, wie man sie erkennt.

Registrieren Sie sich für unsere Mailingliste und besuchen Sie die Seite „Bedrohung des Monats“ um über unsere Blog-Reihe „Bedrohung des Monats“ auf dem Laufenden zu bleiben.

Anmelden: http://cs.co/9002ERAWM

Bedrohung des Monats: http://cisco.com/go/threatofthemonth

Und es wurde Winter: Olympic Destroyer

Bild: Talos

Der Angriff auf die Olympischen Spiele mag eine einmalige Sache gewesen sein, doch die dahinterstehende Gruppe wird keine Ruhe geben.

Das letzte Jahr begann mit einem großen Knall. Cybersicherheitsexperten hatten noch mit den Auswirkungen des Doppelschlags WannaCry und NotPetya zu kämpfen und hofften auf einen ruhigeren Start ins neue Jahr. Diese Hoffnung wurden schnell zerschlagen, als Talos entdeckte, dass die Störungen bei der Eröffnungsveranstaltung der Olympischen Winterspiele 2018 in Pyeongchang (Südkorea) durch Malware verursacht wurden.

Die Malware war äußerst destruktiv und exakt auf diese Umgebung zugeschnitten. Ihr Name mag mit einem historischen Ereignis zusammenhängen, aber die Bedrohung durch Olympic Destroyer lebt weiter.

Während der Eröffnungsfeier fiel die WLAN-Verbindung im Stadion und in den Medienbereichen der Olympischen Spiele aus und die offizielle Website zu den Spielen verschwand aus dem Netz. Eine groß angelegte Störung wie diese hat unzählige Herausforderungen wie Datenschutzrisiken, eine angeschlagene Markenreputation und nachlassende Kundenzufriedenheit zur Folge.

Schließlich zeigte sich, dass es sich bei der Störung um einen Cyberangriff handelte, und eine längerfristige Untersuchung ergab, dass die Malware zwei Eigenschaften aufwies: Erstens handelte es sich um eine Wiper-Malware, die Ressourcen zerstören (und nicht etwa als Ransomware ausführen) sollte und zweitens, was noch interessanter ist, sollte sie ihren Ursprung verbergen und Forscher hinters Licht führen. **Dies war ein komplexer Angriff, der hochentwickelte Malware-Techniken mit einer hinterhältigen Strategie kombinierte.**

Wie genau geht Olympic Destroyer bei der Zerstörung vor?

Über die Bereitstellungsmethode von Olympic Destroyer wird weithin spekuliert. Klar ist, befindet sich die Bedrohung erst einmal im Zielnetzwerk, bewegt sie sich darin weiter, und zwar schnell.

Unsere beste Annahme nach dem Angriff in Pyeongchang lautet, dass sie sich wie ein Wurm fortbewegt und dabei schnell und äußerst destruktiv vorgeht. Die Datei stiehlt Kennwörter, löscht Backup-Daten und zielt auf Daten ab, die auf dem Server gespeichert sind, wodurch in kürzester Zeit ein maximaler Schaden angerichtet wird.

Olympic Destroyer war hoch destruktiv und darauf ausgelegt, Informationen zu vernichten.

Die Angreifer nutzten legitime Tools für eine laterale Bewegung, in diesem Fall PsExec (ein Windows-Protokoll, mit dem Sie Programme auf Remote-Computern ausführen können). Da der Zeitpunkt des Angriffs genau mit der Eröffnungsveranstaltung der Olympischen Spiele zusammenfiel, wurde der Angriff höchstwahrscheinlich aus der Ferne ausgelöst.

Die Malware Olympic Destroyer sollte wahrscheinlich eine glaubhafte Abstreitbarkeit für seine Autoren bewirken, indem Sie Teile von altem Code nutzte, der mit anderen Angreifern in Verbindung gebracht wurde. Einige Sicherheitsexperten wurden bei einer vorschnellen Schuldzuweisung ebenfalls dadurch getäuscht.

Und der Winter geht weiter ...

Welche Motivation auch immer dahinterstehen mag, Cisco Talos fand in der Malware Olympic Destroyer Hinweise auf einen raffinierten Akteur. Daher wissen wir, dass Olympic Destroyer zwar ein maßgeschneiderter Angriff war, die dahinterstehende Gruppe aber keine Ruhe geben wird. Sie werden diese hochgradig effektive Methode wahrscheinlich erneut verwenden, um weiteres Chaos anzurichten oder um Diebstahl oder andere illegale Aktivitäten auszuüben. Wir müssen daher wachsam sein, wenn wir nach Malware dieser Art suchen.

Und so begann 2018. Hoffen wir, dass 2019 keine derart schädlichen und raffinierten Bedrohungen für ein anderes großes Ereignis bereithält.

Für einen tieferen Einblick in dieses Thema siehe:

https://blog.talosintelligence.com/2018/02/olympic-destroyer.html

https://blog.talosintelligence.com/2018/02/who-wasnt-responsible-for-olympic.html

https://blog.talosintelligence.com/2018/12/year-in-malware-2018-most-prominent.html

Über die Cisco Reihe zur Cybersicherheit

Im vergangenen Jahrzehnt hat Cisco eine Fülle an maßgeblichen Sicherheits- und Bedrohungsinformationen für Sicherheitsexperten veröffentlicht, die sich für den aktuellen Stand der globalen Cybersicherheit interessieren. Diese umfassenden Berichte enthielten detaillierte Beschreibungen von Bedrohungslandschaften und ihren organisatorischen Auswirkungen sowie Best Practices zum Schutz vor den negativen Folgen von Datensicherheitsverletzungen.

In unserem neuen Ansatz für unsere Vordenkerposition veröffentlicht Cisco Security eine Reihe von forschungsbasierten, datengesteuerten Publikationen unter der Überschrift **Cisco Reihe zur Cybersicherheit**. Wir haben die Anzahl der Titel erweitert, sodass sie jetzt auch verschiedene Berichte für Sicherheitsexperten mit anderen Interessen enthalten. Diese Berichtsammlung für 2019 greift auf die tiefgreifenden und umfangreichen Kenntnisse von Bedrohungsforschern und Innovatoren in der Sicherheitsbranche zurück und enthält die Benchmark-Studie zum Datenschutz, den Bedrohungsbericht und die Cisco Benchmark-Studien. Weitere Berichte sollen im Jahresverlauf folgen.

Weitere Informationen finden Sie unter www.cisco.com/go/securityreports.

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 Februar 2019 THRT_01_0219_r2