CROWDSTRIKE

DAUERGEFAHR RANSOMWARE: WIE SICH UNTERNEHMEN UND INSTITUTIONEN GEGEN NEUE TRENDS UND METHODEN SCHÜTZEN KÖNNEN

DAUERGEFAHR RANSOMWARE: WIE SICH UNTERNEHMEN UND INSTITUTIONEN GEGEN NEUE TRENDS UND METHODEN SCHÜTZEN KÖNNEN

Keine Frage: Ransomware und die damit verbundenen erpresserischen Lösegeldforderungen sind eine wachsende Bedrohung. Versierte Angreifer haben 2019 für Schlagzeilen gesorgt, indem sie mehrere US-Städte lahmlegten, darunter Baltimore, Maryland und Park City, Utah. Diese Angriffe beleuchten jedoch nur die sichtbare Seite einer viel größeren kriminellen Branche, die sehr innovativ vorgeht. Ransomware ist die schnellst wachsende Bedrohung für die Cybersicherheit. Die Schäden durch erpresserische Lösegeldforderungen sollen bis 2021 weltweit auf **20 Milliarden Dollar ansteigen – gegenüber „nur" 345 Millionen Dollar im Jahr 2015.**

Dieses Whitepaper erklärt die Hintergründe zur Ransomware-Entwicklung, zeigt neue Trends bei erpresserischen Lösegeldforderungen auf und gibt Empfehlungen dazu, wie Sie Ihre Organisation vor solchen Angriffen schützen können.

ENTWICKLUNG UND AKTUELLE TRENDS DER RANSOMWARE

EIN ALTES SCHEMA

Auch wenn Ransomware in den letzten fünf Jahren immer wieder in die Schlagzeilen gerät: Die Idee, Dateien oder Computer von Benutzern durch Verschlüsseln, Sperren des Systemzugriffs oder andere Methoden zu kapern und Lösegeld für die Freigabe zu verlangen, ist ziemlich alt. Bereits in den späten 1980er Jahren kaperten Kriminelle Computer oder Dateien und gaben sie erst wieder gegen Bargeld heraus, das sie sich per Post schicken ließen. Eines der ersten jemals dokumentierten Ransomware-Viren war der AIDS-Trojaner (PC-Cyborg-Virus), der 1989 per Diskette verbreitet wurde. Die Opfer mussten 189 Dollar an ein Postfach in Panama schicken, damit sie wieder Zugriff auf ihre Systeme erhielten. Dabei handelte es sich um ein recht einfaches Virus, das mit **symmetrischer Kryptographie** arbeitete.

MONETARISIERUNG

Trotz ihrer langen Geschichte waren Ransomware-Angriffe bis weit in die 2000er Jahre hinein nicht weit verbreitet – vermutlich wegen der problematischen Zahlungsabwicklung. Mit dem Aufkommen von Kryptowährungen wie Bitcoin im Jahr 2010 änderte sich all das schlagartig. Jetzt stand eine einfache und nicht nachverfolgbare Methode bereit, Geld von Opfern zu erhalten. So entstand im Fahrwasser der virtuellen Währungen die Möglichkeit, Lösegeld zu einem lukrativen Geschäft zu machen.

EINFACHER, ABER IMMER NOCH UMSTÄNDLICH

Unter „eCrime" werden bösartige Aktivitäten von Cyberkriminellen zusammengefasst, einschließlich Malware, Banking-Trojaner, Ransomware, Mineware (Cryptojacking) und Crimeware. eCrime nutzte sofort die Monetarisierungsmöglichkeiten, die Bitcoin geschaffen hatte. Dies führte ab 2012 zu einer erheblichen Verbreitung von Ransomware. Dieses Geschäftsmodell für Ransomware ist jedoch nach wie vor nicht perfekt. Denn während Bitcoin-Zahlungen für Kriminelle kein Problem darstellen, gilt das nicht für die Opfer, die technisch meist nicht so versiert sind. Einige Kriminelle eröffnen sogar spezielle Call-Center, die technische Unterstützung bieten und den Opfern erklären, wie man sich für Bitcoin anmeldet. Das soll die Zahlung sicherstellen, kostet aber Zeit und Geld.

FALLSTUDIE: MALWARE „ROBBINHOOD" SCHÄDIGT DIE STADT BALTIMORE SCHWER

Im Mai 2019 fügte eine Ransomware namens „RobbinHood" der Stadt Baltimore im US-Staat Maryland einen schweren Schaden zu. Der Stadt entstand ein Verlust von mindestens **18,2 Millionen Dollar** an entgangenen oder verspäteten Einnahmen, zusätzlich zu den direkten Kosten für die Wiederherstellung der Systeme. Der Angriff legte das Kreditkartenzahlungssystem der Stadt lahm und brachte den Immobilienmarkt zum Erliegen, da es die kommunalen Prozesse zur Einziehung von Grundsteuern, Grundbesitzabgaben und Bußgeldern außer Kraft setzte.

RobbinHood ist ein neuer Typ von Ransomware, der im April 2019 auftauchte. Er schaltet die signaturbasierten Antiviren- (AV) und Backup-Dienste des Anwenders ab, die normalerweise eine Verschlüsselung unterbinden würden. Hierzu gibt RobbinHood den Befehl „sc. exe stop" aus: **cmd.exe /c sc.exe stop AVP /y** (AVP steht für AntiVirus Program und ist der generische Name für AV-Software). Auf diese Aktion folgt eine Reihe weiterer invasiver Befehle und Maßnahmen. Nach ihrer Ausführung blockiert die Ransomware 181 Windows-Dienste, die mit AV-Software, Mailservern und anderer Software verbunden sind, die die Dateiverschlüsselung verhindern könnten. Dies ist ein Beispiel für die Vorgehensweise, bereits im System vorhandene Werkzeuge zu nutzen, um bösartige Aufgaben durchzuführen – wie Persistenz, Eskalation der Rechte und Umgehung der Verteidigungsmechanismen. Diese Taktiken schalten die Verteidigung ab und ermöglichen es Angreifern, heimlich Endgeräte zu infiltrieren.

„GROSSWILDJAGD“

Anstatt ihre potenziellen Opfer mit einem ungezielten „Dauerfeuer“ anzugreifen, konzentrieren sich Cyberkriminelle mittlerweile auf Angriffe gegen Ziele, die hohe finanzielle Erträge versprechen – die sogenannte „Großwildjagd“. Hierbei wird Ransomware mit Taktiken, Techniken und Verfahren (TTPs) kombiniert, die bei gezielten Angriffen auf größere Unternehmen und Institutionen üblich sind. Anstatt eine große Anzahl von Lösegeldangriffen gegen kleine Ziele zu führen, konzentrieren sich Cyberkriminelle hierbei auf weniger Opfer, die größere finanzielle Erträge versprechen – also Opfer, bei denen sich der Einsatz und Aufwand wirklich lohnt.

Dieser Wechsel war so deutlich, dass er im **CrowdStrike® 2020 Global Threat Report** als einer der wichtigsten eCrime-Trends erwähnt wird. Jüngste eCrime-Statistiken zeigen, dass das Aufkommen von Ransomware-Angriffen zwar zurückgegangen ist, die Komplexität dieser Angriffe jedoch erheblich zugenommen hat.

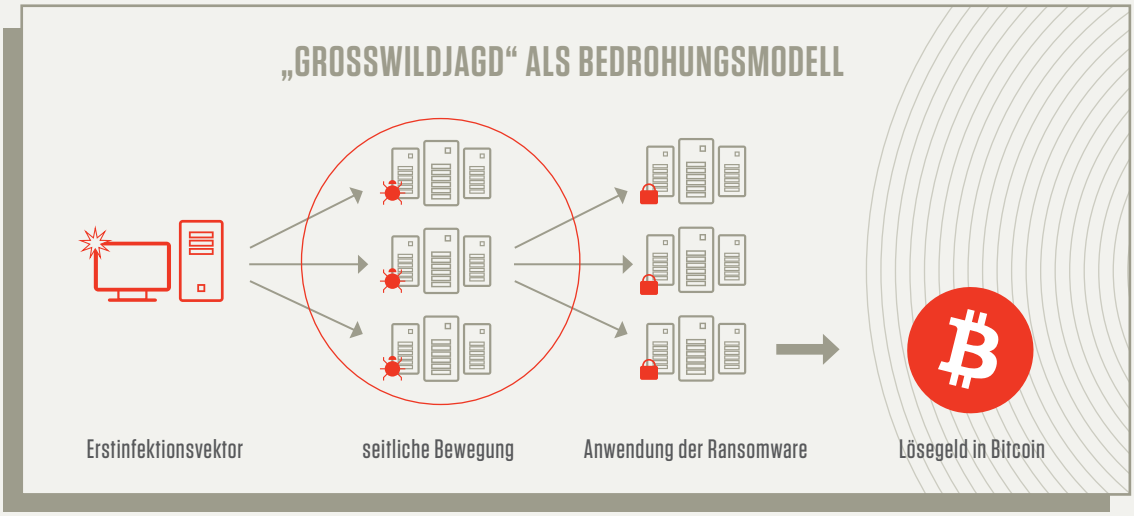


Abb. 1: Die sogenannte „Großwildjagd“ zielt auf größere Unternehmen und Institutionen ab, die höhere Gewinne versprechen..

DIE AKTEURE HINTER DEN RANSOMWARE-ANGRIFFEN

CrowdStrike® Intelligence überwacht das eCrime-Ökosystem, indem es eCrime-Organisationen, unabhängige Bedrohungsakteure und deren Beziehungen verfolgt. So wurde zum Beispiel der Entwickler von Samas (alias Sam Sam) als ein Bedrohungsakteur namens BOSS SPIDER identifiziert; INDRIK SPIDER wurde die Entwicklung von Dridex zugeschrieben; und WIZARD SPIDER, auch bekannt als der in Russland ansässige Betreiber der Banken-Malware TrickBot – die in der Vergangenheit hauptsächlich auf Überweisungsbetrug abzielte – wurde als Gruppe identifiziert, die auch Ryuk entwickelt hat. Diese Gruppen wurden dabei beobachtet, wie sie gezielte Ransomware-Angriffe initiieren, die dem Konzept der „Großwildjagd“ folgen und dabei große Gewinne erwirtschaften. Beispielsweise hat BOSS SPIDER seit dem ersten Erscheinen im Jahr 2016 bis zur letzten bekannten Aktivität gegen Ende 2018 mehr als 6,7 Millionen US-Dollar eingenommen. Seit dem ersten Auftritt von WIZARD SPIDER im August 2018 hat diese Gruppe an Bedrohungsakteuren schätzungsweise über 695,80 Bitcoin in 51 Transaktionen mit einem ungefähren Wert von 3,6 Millionen US-Dollar eingestrichen.

CrowdStrike konnte zudem eine zunehmende Kooperation von Bedrohungsakteuren bei gezielten Angriffen beobachten.

HÖHERE KOMPLEXITÄT UND UNSCHARFE LINIEN

Wie alle Software-Entwickler arbeiten auch eCrime-Gruppen ständig an der Verbesserung ihrer Ransomware und rüsten diese mit neuen Funktionen auf. WIZARD SPIDER zum Beispiel hat Ryuk um viele neue Funktionen erweitert und unnötige und veraltete Funktionen aus dem Code entfernt. Diese Gruppe bedient sich neuer Auszählmodule, die auf die Systeme der Opfer heruntergeladen werden, um Zugangsdaten zu orten und eine seitliche Bewegung in der Umgebung des Opfers durchzuführen – mit dem Ziel, Zugang zum Domain-Controller zu erhalten. Bei erfolgreichem Zugriff auf den Domain-Controller kann WIZARD SPIDER seine Ransomware Ryuk in der gesamten Umgebung des Opfers implementieren.

Erschwerend kommt hinzu, dass sich die Grenzen zwischen nationalstaatlichen und eCrime-Ransomware-Kampagnen verwischen. Dieser Trend ist seit 2018 zu beobachten. Ob der Ransomware-Code gestohlen oder willentlich zwischen nationalstaatlichen Akteuren und Cyberkriminellen geteilt wird, ist nach wie vor unklar. CrowdStrike hat allerdings beobachtet, dass beide Arten von Gegnern ähnliche Malware einsetzen – wie beispielsweise Ryuk. Entweder um sich finanziell zu bereichern oder um den Ursprung eines nationalstaatlichen Angriffs zu verschleiern.

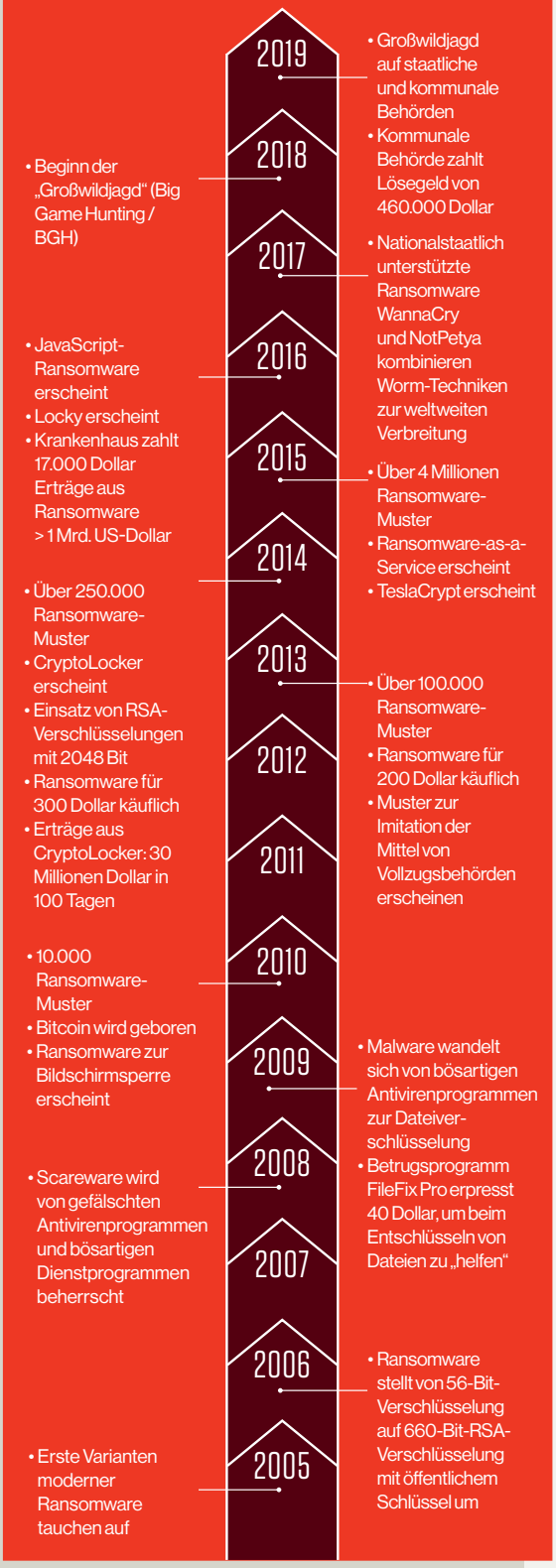
DIE FUNKTIONSWEISE VON RANSOMWARE

Es gibt viele Einstiegsmöglichkeiten für Ransomware, wobei Phishing-E-Mails und Website-Pop-ups zu den häufigsten Vektoren gehören. Ein weiterer Zugang führt über Exploit-Kits, die bestimmte Schwachstellen ausnutzen.

FINSTERE PSYCHOLOGIE: GESCHÄFTSSINN GEPAART MIT SKRUPELLOSEM SOCIAL ENGINEERING

Technologie und menschliche Natur sind zwei Seiten derselben Medaille, wenn es um Ransomware-Angriffe geht. In einem von CrowdStrike beobachteten Fall wurde die E-Mail einer Führungskraft gefälscht. Der Angreifer nutzte Social Engineering, um Mitarbeiter dazu zu bringen, auf einen Link in einer gefälschten E-Mail der Führungskraft zu klicken. Damit dieser Angriff zum Erfolg führte, waren methodische Nachforschungen über die Unternehmensleitung, die Mitarbeiter und die Branche erforderlich. Social Engineering bei Phishing-Angriffen gegen lukrative Opfer wird immer stärker genutzt. Auch soziale Medien spielen eine große Rolle, da sie es Angreifern nicht nur ermöglichen, Informationen über potenzielle Opfer auszuspähen, sondern auch als Mittel für die Verbreitung von Malware dienen.

DIE ENTWICKLUNG DER MODERNEN RANSOMWARE



DAUERGEFAHR RANSOMWARE: WIE SICH UNTERNEHMEN UND INSTITUTIONEN GEGEN NEUE TRENDS UND METHODEN SCHÜTZEN KÖNNEN

WEBSITE-POP-UPS UND EXPLOIT-KITS: EINE GEFÄHRLICHE KOMBINATION

Website-Pop-ups und Exploit-Kits können von Angreifern zusammen verwendet werden, um Ransomware zu verbreiten und „Trojaner-Pop-ups" oder Werbung mit verstecktem bösartigem Code zu erstellen. Wenn Benutzer darauf klicken, werden sie heimlich auf die Zielseite des Exploit-Kits umgeleitet. Dort wird der Rechner von einer Komponente des Exploit-Kits heimlich auf Schwachstellen gescannt, die der Angreifer dann ausnutzen kann. Bei erfolgreicher Suche sendet das Exploit-Kit eine Ransomware, die den Host infiziert. Exploit-Kits sind bei Cyberkriminellen aufgrund der automatisierten Vorgehensweise sehr beliebt. Zudem sind Exploits eine effiziente Technik, die ohne Dateien auskommt. Sie können direkt in den Speicher injiziert werden, ohne dass Daten auf die Festplatte geschrieben werden müssen. Daher können sie von herkömmlicher Antiviren-Software nicht erkannt werden. Exploits-Kits werden auch von weniger versierten Angreifern eingesetzt, da sie kein großes technisches Know-how voraussetzen. Mit einer bescheidenen Investition im Darknet kann praktisch jeder ins Online-Geschäft mit Ransomware einsteigen.

DATEILOSE-ANGRIFFE: RANSOMWARE OHNE RANSOMWARE

Dateilose Ransomware-Techniken sind im Aufwind. Bei diesen Angriffen werden zunächst keine ausführbaren Dateien auf die Festplatte geschrieben. Stattdessen werden vorhandene Betriebssystemwerkzeuge, wie PowerShell oder WMI, benutzt, mit denen der Angreifer Aufgaben ausführen kann, ohne dass eine bösartige Programmdatei auf dem angegriffenen System ausgeführt werden muss. Diese Technik ist beliebt, weil sich die meisten älteren AV-Lösungen mit dateilosen Angriffen umgehen lassen.

Wenn Sie sich detailliert über die Funktionsweise von dateiloser Ransomware informieren möchten, laden Sie die Infografik von **CrowdStrike zur dateilosen Ransomware herunter.**

RANSOMWARE-AS-A-SERVICE (RAAS)

Da Cyberkriminelle immer nach Möglichkeiten suchen, ihre Abläufe zu optimieren und höhere Gewinne zu erzielen, ließen sie sich vom SaaS-Modell (Software-as-a-Service) inspirieren und entwickelten ein RaaS-Modell (Ransomware-as-a-Service). RaaS-Anbieter bieten alle für die Durchführung von Ransomware-Kampagnen erforderlichen Angriffskomponenten an – von bösartigem Code bis hin zu Ergebnis-Dashboards. Einige betreiben sogar eine Serviceabteilung, mit der sie ihre Ransomware auch für technisch nicht so versierte Kriminelle zugänglich machen. Darüber hinaus werden die Subskriptionskosten in der Regel aus dem Erlös der Kampagne gedeckt – ein kostengünstiges Modell, das von Cyberkriminellen genutzt werden kann.

Ein Beispiel ist der bekannte RaaS namens „Hermes", der erstmals 2017 vertrieben und in Darknet-Foren für 300 US-Dollar verkauft wurde. Ein Hermes-Käufer erhielt in der Regel einen Build, der zwei E-Mail-Adressen, einen Entschlüsseler und ein eindeutiges RSA-Schlüsselpaar unterstützt. Sobald sich der Erfolg von Hermes herumgesprochen hatte, tauchten weitere eCrime-Gruppen auf.

Ein weiteres Beispiel ist PINCHY SPIDER, eine RaaS-Organisation und kriminelle Gruppe, die erstmals 2018 beobachtet wurde*. Diese kriminelle Gruppe teilt sich die Profite mit ihren Kunden im Verhältnis 60:40 und stellte alle zwei Wochen aktualisierte Versionen bereit. Dieser beschleunigte Entwicklungszyklus hängt mit der Tatsache zusammen, dass die Gruppe ihren Code häufig modifizieren musste, um eine Blockierung durch Sicherheitsanbieter zu verhindern.

* CrowdStrike 2019 Global Threat Report

NENNENSWERTE RANSOMWARE-DERIVATE

BitPaymer: Zielt auf Anwender ab, die das Dridex-Lademodul verwenden, und dient dazu, ins Netzwerk des Opfers einzudringen.

Dridex: Eine Banking-Malware, die Systeme über Microsoft-Office-Makros infiziert.

Hermes: Eine erstmals 2017 verbreitet RaaS. Mitte August 2018 erschien eine modifizierte Version von Hermes namens Ryuk in einem öffentlichen Malware-Repository.

KeRanger: Die erste Ransomware, die auf Mac OS X abzielte, konnte auch Time-Machine-Sicherungsdateien verschlüsseln.

Petya: Verschlüsselt die Master File Table (MFT), um das gesamte System unzugänglich zu machen.

PowerWare: Verschlüsselt Dateien über eine „fileless"-Infektion.

Ransom32: In Javascript geschriebene Ransomware, die sich für plattformübergreifende Infektionen auf Mac- und Linux-Systemen eignet.

Ryuk: Ähnlich wie Samas und BitPaymer; zielt auf große Institutionen ab und nutzt PowerShell; die Binärdateien werden über PsExec verbreitet.

Samas: Nutzt verwundbare JBOSS-Systeme und verbreitet sich über ein Netzwerk. Greift sogar Backup-Dateien im Netzwerk an. Zielt auf große Institutionen per „Großwildjagd" ab.

WannaCry: Ransomware-Worm, der den Exploit EternalBlue für Microsoft Windows nutzt; verschlüsselt per AES-Chiffre.

DAUERGEFAHR RANSOMWARE: WIE SICH UNTERNEHMEN UND INSTITUTIONEN GEGEN NEUE TRENDS UND METHODEN SCHÜTZEN KÖNNEN

WIE MAN SICH VOR RANSOMWARE SCHÜTZT

KONKRETE SCHRITTE

Backups sind eine gute Verteidigungsmaßnahme, müssen aber auch geschützt werden, da sie oft das erste sind, was Angreifer in einer Umgebung zu sperren oder zu zerstören versuchen. Es gehört daher zur Standardvorkehrung, sicherzustellen, dass Backups auch in einer kompromittierten Umgebung separat zugänglich bleiben und gut geschützt sind.

Im September 2019 veröffentlichte das **US-Heimatschutzministerium** einen Artikel, in dem weitere Maßnahmen skizziert wurden, die Unternehmen und Institutionen im Umgang mit Ransomware ergreifen sollten. Der Artikel enthält Ratschläge dazu, wie man sich vor Ransomware schützt, wie man sich auf einen möglichen Vorfall vorbereitet, wie man Schäden beseitigt und wo man Hilfe findet. Er enthält zudem praktische Empfehlungen – vom Installieren nötiger Updates über die Schulung von Endbenutzern bis hin zur Erstellung und Umsetzung eines Plans für den Umgang mit Sicherheitsvorfällen.

DAS ATT&CK™-FRAMEWORK VON MITRE

Das **MITRE ATT&CK®-Framework** ist eine umfassende Matrix, die die von Gegnern angewandten Techniken und Taktiken inventarisiert und klassifiziert. Unter der Kategorie **„Impact“** führt sie Ransomware-spezifische Techniken auf. Anhand der darin enthaltenen Informationen können Sicherheitsverantwortliche erkennen, wie sie möglicherweise angegriffen werden. Zudem können sie abwägen, über welche Fähigkeiten sie verfügen, um derartige Techniken aufzuspüren und zu stoppen und einen optimalen Schutz planen.

DAS KONZEPT VON CROWDSTRIKE

Da die Entwickler von Ransomware ständig ihre Techniken ändern, nutzt CrowdStrike Falcon® als Lösung für den Endgeräteschutz der nächsten Generation eine ganze Reihe von ergänzenden Verfahren zur Prävention und Erkennung:

- **Maschinelles Lernen** zur Prävention bekannter und bisher unbekannter oder „Zero-Day“-Ransomware, ohne dass Updates erforderlich sind
- **Exploit Blocking,** um die Ausführung und Verbreitung von Ransomware über nicht gepatchte Schwachstellen zu stoppen
- **Angriffsindikatoren (Indicators of Attack / IOAs)** zur Identifizierung und Blockierung krimineller Verhaltensweisen sowie zum Schutz gegen dateilose Angriffe und neuer Ransomware-Kategorien
- **Automatisierte Bedrohungsanalyse** zur detaillierten sofortigen Analyse der gefundenen Ransomware, wie beispielsweise Herkunft, Zuschreibung, Ähnlichkeiten und IOCs (Gefährdungsindikatoren)

CrowdStrike Falcon als Plattform zum Schutz von Endgeräten nutzt das MITRE ATT&CK-Framework für Warnmeldungen. So können Sicherheitsverantwortliche im Falle eines Angriffs schnell und klar erkennen, was an ihren Endgeräten vor sich geht – beispielsweise, in welcher Phase sich der Angriff befindet und welche gegnerischen Gruppen damit in Verbindung stehen.

ANGRIFFSINDIKATOREN: EINE EINZIGARTIGE UND EFFIZIENTE MÖGLICHKEIT ZUR ABWEHR DATEILOSER MALWARE

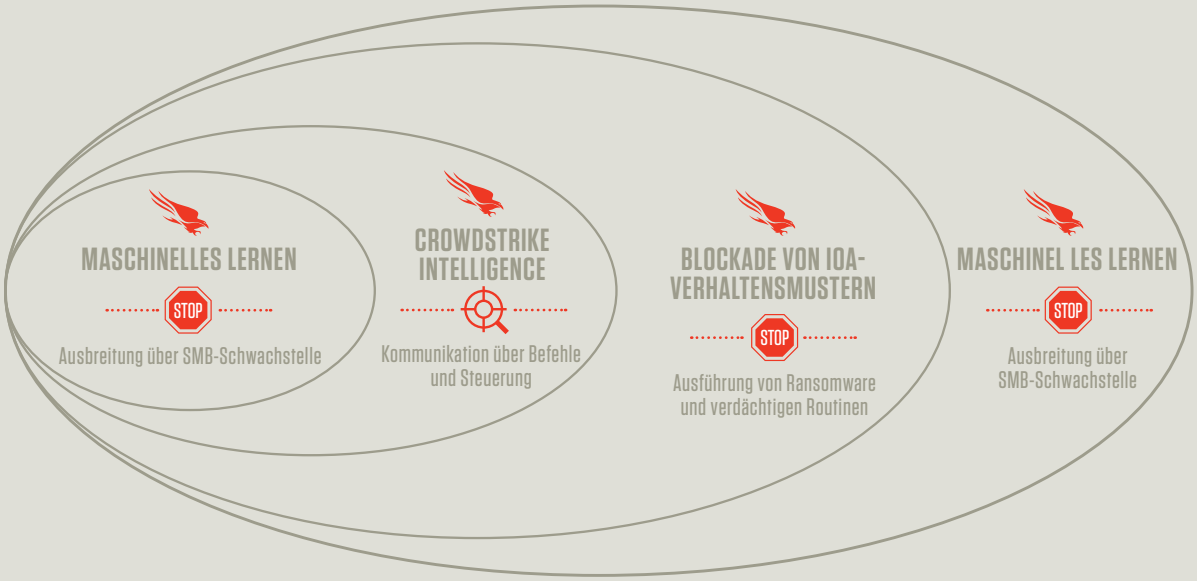
Dateilose Ransomware ist mit signaturbasierten Methoden, Sandboxing oder einer Analyse, die auf maschinellem Lernen basiert, äußerst schwer zu erkennen. CrowdStrike hat einen effektiveren Ansatz entwickelt, bei dem Angriffsindikatoren (Indicators of Attack / IOA) eingesetzt werden, um zusätzliche unbekannte Ransomware und andere Arten von Angriffen zu identifizieren und zu blockieren. IOAs suchen nach Frühwarnzeichen für einen möglichen Angriff. Anzeichen dafür können unter anderem die Ausführung von Code, Versuche zur Tarnung und Seitwärtsbewegungen sein. Durch die Identifizierung der Ausführung dieser Aktivitäten in Echtzeit – einschließlich ihrer Abfolge und Abhängigkeiten – erkennt die IOA-Technologie solche Aktivitäten als Frühindikatoren, die die wahren Absichten und Ziele eines Angreifers offenbaren.

IOAs verhindern außerdem zuverlässig, dass die Ransomware vorhandene Backups löscht. So können Benutzer verschlüsselte Dateien wiederherstellen, selbst wenn die Dateiverschlüsselung bereits begonnen hat, bevor die Ransomware gestoppt wurde. Da IOAs die Ziele der Ransomware überwachen, erkennen und abwehren, können Angriffe gestoppt werden, bevor Schaden entsteht. Das IOA-Konzept ist zudem wirksam und widerstandsfähig gegen Iterationen von Ransomware, da ein einziger IOA zahlreiche Varianten und Versionen mehrerer Ransomware-Familien abdecken kann, auch neue, sobald sie in Umlauf gebracht werden.

FALLSTUDIE: CROWDSTRIKE SCHÜTZT VOR WANNACRY-RANSOMWARE

Die vielschichtigen Präventionsfunktionen der CrowdStrike Falcon-Plattform verhinderten, dass die Ransomware WannaCry Dateien verschlüsseln und sich weiterverbreiten konnte. Weil sich WannaCry selbstständig verbreiten kann, verursachte die Ransomware im Rahmen einer Kampagne, die am 12. Mai 2017 begann, eine beträchtliche Anzahl von Infektionen. Die Geschwindigkeit, mit der sich WannaCry in einer Organisation verbreiten kann, verleiht diesem Typ von Ransomware ein hohes zerstörerisches Potenzial. Sobald sich WannaCry in einem Netzwerk befindet, nutzt es eine Schwachstelle im SMB-Protokoll von Microsoft Windows aus, um sich durch die gesamte Organisation zu bewegen. Nach Ausführung von WannaCry auf einem Zielsystem dauert es nur wenige Sekunden, bis die Dateien auf einem zweiten System verschlüsselt sind. Kurz darauf folgt die Lösegeldforderung. CrowdStrike Falcon schützte nicht nur Systeme vor der Erstinfektion mit WannaCry, sondern verhinderte auch die Verbreitung von WannaCry in geschützten Umgebungen. Darüber hinaus war CrowdStrike Intelligence in der Lage, neue Varianten der Schadsoftware schnell zu identifizieren. Die gewonnenen Erkenntnisse wurden unverzüglich in die Falcon-Plattform integriert, um zusätzliche Schutzebenen zu schaffen.

FALCON-ENDGERÄTESCHUTZ GEGEN **WANNACRY**



VOLLER SCHUTZ VON ANFANG AN

FAZIT

Die Schlagzeilen in den Nachrichten machen es immer wieder deutlich: Ransomware ist und bleibt eine erhebliche Bedrohung. Cyberkriminelle und nationalstaatliche Bedrohungsakteure arbeiten ständig daran, ihre Fähigkeiten zu verbessern. CrowdStrike geht wirksam gegen Ransomware-Angriffe vor. Hierzu entwickeln wir unsere Sicherheitstechnologien laufend innovativ weiter, um auch hochversierten Angreifern immer einen Schritt voraus zu sein.

Wie dieses Whitepaper deutlich macht, bedarf es einer Kombination verschiedener Elemente, um Ihre Organisation angemessen zu schützen. Dazu zählen konkrete Schritte zur Anpassung Ihrer Strategie an solide Sicherheitspraktiken und der Einsatz einer innovativen, cloud-nativen Technologie der nächsten Generation zur Prävention und Erkennung, wie sie mit der CrowdStrike Falcon-Plattform bereitgestellt wird.

ÜBER CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), ein weltweit führendes Unternehmen im Bereich der Cybersicherheit, definiert mit seiner von Grund auf neu konzipierten Endgeräteschutzplattform die Sicherheit im Cloud-Zeitalter neu. Die schlanke Single-Agent-Architektur der CrowdStrike Falcon®- Plattform nutzt Cloud-skalierte Künstliche Intelligenz und sorgt unternehmensweit für Schutz und Transparenz. So werden Angriffe auf Endgeräte sowohl innerhalb als auch außerhalb des Netzwerks verhindert. Mit Hilfe des firmeneigenenCrowdStrike Threat Graph® korreliert CrowdStrike Falcon weltweit und in Echtzeit über 3 Billionen endpunktbezogene Ereignisse pro Woche. Damit ist die CrowdStrike Falcon Plattform eineder weltweit fortschrittlichsten Datenplattformen für Cyber-Sicherheit.

Mit CrowdStrike profitieren Kunden von besserem Schutz, besserer Leistung und sofortiger Time-to-Value – und das alles auf der cloud-nativen Falcon-Plattform.

Sie sollten vor allem eines über CrowdStrike wissen: **Wir stoppen Datendiebstahl.**

Sprechen Sie mit uns, um mehr darüber zu erfahren, was CrowdStrike für den Schutz Ihrer Umgebung tun kann:

Telefon: +49 (0)241 936 88811

Email: germany@crowdstrike.com Web: www.crowdstrike.de

Testen Sie jetzt kostenlos den Virenschutz der nächsten Generation

Erfahren Sie mehr unter **www.crowdstrike.de**