April 2017

Threats-Report

McAfee Labs

Mirai, das IoT-Botnet

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

Angriffsprozess

1 Suche nach IoT-Geräten
Mirai durchsucht einen breiten IP-Adressbereich nach offenen Telnet- oder SSH-Ports, um dahinter liegende IoT-Geräte zu finden.

2 Brute-Force-Angriff
Anschließend startet Mirai einen Brute-Force-Angriff auf diese IoT-Geräte und nutzt dabei ein Wörterbuch mit häufig standardmäßig festgelegten Benutzernamen und Kennwörtern, um schlecht gesicherte Geräte zu identifizieren.

3 Senden von Anmeldedaten
Sobald der Brute-Force-Angriff erfolgreich ist, sendet die Malware die IP-Adresse sowie die Anmeldeinformationen des kompromittierten IoT-Geräts an den Kontroll-Server.

4 Download des Mirai-Bots
Ein Download-Server lädt die Mirai-Bot-Binärdatei auf das IoT-Gerät herunter.

5 Warten auf Angriffs-anweisungen
Nach der Infizierung wartet die IoT-Geräte-Malware auf Anweisungen für einen DDoS-Angriff.

6 Durchführung des DDoS-Angriffs
Mirai kann DDoS-Angriffe auf den Schichten 3, 4 und 7 des OSI-Modells durchführen.

2,5 Millionen
Etwa 2,5 Millionen IoT-Geräte wurden mit Mirai infiziert.

5 pro Minute
Pro Minute werden rund fünf IP-Adressen den Mirai-Botnets hinzugefügt.

1,2 TBit/s Datenverkehr
Auf dem Höhepunkt des Angriffs wurde ein Mirai-Botnet-Ziel mit 1,2 TBit/s an Datenverkehr überflutet, was dem stärksten bisher ermittelten DDoS-Datenverkehr entspricht.

50 bis 7.500 USD pro Tag
Mirai-basierte DDoS-Angriffe werden heute als Service angeboten, der zwischen 50 und 7.500 US-Dollar/Tag kostet.

Zeitschiene der Mirai-Evolution

August | September | Oktober | November

1 *August 2016*
Erste Mirai-Version
Mirai ELF-Binärdateien werden veröffentlicht

2 *20. September 2016*
DDoS-Angriff auf die Webseite „Krebs on Security"
Mirai infiziert DVRs und Überwachungskameras über Telnet-Port

3 *1. Oktober 2016*
Veröffentlichung des Mirai-Quellcodes
Anna-Senpai veröffentlicht Mirai-Quellcode

4 *4. Oktober 2016*
Mirai-Botnet-as-a-Service
Untergrundforum bietet DDoS-as-a-Service an

5 *28. November 2016*
Ausfall bei der Deutschen Telekom
Neue Mirai-Variante gefunden, die Port 7547 angreift

Austausch von Bedrohungsdaten

Transparenz bietet Schutz.

Was sind Bedrohungsdaten?

Strategische Informationen
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.

Taktische Informationen
Von Sicherheitssystemen, Scannern und Sensoren erfasste Informationen. Hierbei handelt es sich häufig um Kompromittierungsindikatoren, die für Forensik- und Behebungsmaßnahmen nützlich sind.

Operative Informationen
Die kritischen Komponenten für die Kontextermittlung. Dazu gehören der Umfang und das Ausmaß eines vermuteten Angriffs sowie die Frage, wie die Reaktionsmaßnahmen am besten koordiniert werden sollten. Zur Stärkung der Mitarbeiterkompetenzen und -entscheidungen können Big Data-Analysen, Machine Learning und weitere automatisierte Techniken zur Entscheidungsfindung herangezogen werden.

Große Herausforderungen beim Austausch von Bedrohungsdaten

Datenvolumen
Sicherheitssensoren, Big Data-Analysen und Machine Learning-Tools haben ein erhebliches Missverhältnis zwischen nützlichen und unwichtigen Informationen (Signal/Rauschen) geschaffen, das die Analyse, Verarbeitung und Nutzung der Bedrohungsdaten erschwert.

Validierung
Wir müssen die Bedrohungsdatenquellen überprüfen, um zu gewährleisten, dass die Daten aus legitimen Quellen stammen – und nicht von Akteuren, die mit falschen Berichten Bedrohungsdaten-Tools verwirren oder unbrauchbar machen.

Korrelation
Unverzichtbar für effektive Maßnahmen sind die Validierung von Daten nahezu in Echtzeit, ihre Korrelation über Betriebssysteme, Geräte und Netzwerke hinweg, die Analyse des Ereignisses sowie die Ermittlung des Umfangs der Gegenmaßnahmen.

Qualität
Legitime Quellen können beliebige Daten senden, von Kompromittierungsindikatoren bis hin zu einem ganzen Ereignis-Feed, was für die Empfänger jedoch irrelevant sein kann. Filter, Tags und Deduplizierung müssen automatisiert sein, damit die Bedrohungsdaten praktisch verwertbar sind.

Geschwindigkeit
Offene und standardisierte Kommunikation, die nahezu in Echtzeit abläuft, ist unverzichtbar, um die Verzögerung zwischen der Erkennung eines Angriffs und dem Empfang von Bedrohungsdaten zu minimieren.

Statistische Bedrohungsdaten

Jede Minute werden 176 neue Bedrohungen erkannt. Das entspricht fast 3 pro Sekunde.

Vorfälle (974)
Im 4. Quartal erfassten wir 197 öffentlich bekannte Zwischenfälle. Im gesamten Jahr 2016 waren es 974 öffentlich bekannte Zwischenfälle.

Malware (24 %)
Die Anzahl neuer Malware-Varianten fiel im 4. Quartal auf 23 Millionen. Das sind 17 % weniger als im 3. Quartal. **Die Gesamtanzahl stieg jedoch im Jahr 2016 um 24 % auf 638 Millionen Varianten.**

Mac OS-Malware (744 %)
Obwohl die Zahlen im Vergleich mit Windows-Bedrohungen weiterhin niedrig sind, stieg die Anzahl neuer Mac OS-Malware-Varianten aufgrund von Adware-Bundles im 4. Quartal um 245 %. **Insgesamt stieg die Zahl neuer Mac OS-Malware 2016 um 744 %.**

Mobilgeräte-Malware (99 %)
Die Anzahl der neuen Mobilgeräte-Malware-Varianten ging im 4. Quartal um 17 % zurück. **Gleichzeitig stieg die Zahl neuer Mobilgeräte-Malware 2016 um 99 %.**

Spam-Botnets (24 %)
Von den 10 größten Botnets versendete Spam-E-Mails gingen im 4. Quartal um 24 % auf 181 Millionen E-Mails zurück. Im Jahr 2016 generierten diese 10 größten Botnets zusammen 934 Millionen Spam-E-Mails.

Ransomware (88 %)
Die Zahl neuer Ransomware-Varianten sank im 4. Quartal um 71 %, vor allem aufgrund eines Rückgangs bei generischen Ransomware-Erkennungen sowie bei Locky und CryptoWall. **Die Gesamtanzahl der Ransomware-Varianten stieg 2016 um 88 %.**

McAfee Global Threat Intelligence

McAfee GTI erhielt täglich durchschnittlich 49,6 Milliarden Anfragen.

McAfee GTI

66 Millionen
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**.

37 Millionen
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**.

71 Millionen
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**.

35 Millionen
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**.

McAfee Labs Threats-Report: April 2017

Den vollständigen Report finden Sie unter www.mcafee.com/April2017ThreatsReport.

2614_0217_info-threat-report-mirai-iot