Threats Report

McAfee Labs

Mirai, the IoT Botnet

The Mirai botnet infected and then exploited poorly secured IoT devices to perform the largest ever distributed denial-of-service attack.

Attack process

1 Scan for IoT devices
Mirai scans a broad range of IP addresses for open Telnet or SSH ports and locates IoT devices behind them.

2 Brute-force attack
Mirai then launches a brute-force attack on those IoT devices, using a dictionary of common default usernames and passwords to identify poorly secured devices.

3 Send credentials
Once the brute-force attack is successful, the malware sends the compromised IoT device's IP address and credentials to the control server.

4 Download the Mirai bot
A loading server downloads the Mirai bot binary to the IoT device.

5 Wait for attack instructions
Once infected, the IoT device malware waits for DDoS attack instructions.

6 Start DDoS attack
Mirai is capable of DDoS attacks on Layers, 3, 4, and 7 of the OSI model.

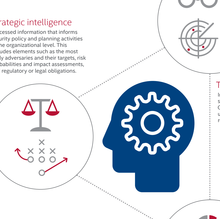
2.5 million
About 2.5 million IoT devices have been infected with Mirai.

5 every minute
Every minute, about five IP addresses are added to Mirai botnets.

1.2Tbps of traffic
At its peak, one Mirai botnet target was attacked by 1.2Tbps of traffic, the largest volume of DDoS traffic ever recorded.

$50 to $7,500 per day
Mirai-based DDoS attacks are now offered as a service that costs from $50 to $7,500 per day.

Mirai evolution timeline



Around August 2016
Initial Mirai release
Mirai ELF binaries start surfacing.

October 1, 2016
Mirai source code release
Anna-Senpai releases source code of Mirai.

November 28, 2016
Deutsche Telekom outage
New variant of Mirai found. Targets port 7547.

September 20, 2016
DDoS on "Krebs on Security" website
Mirai infects DVRs and CCTVs on Telnet port.

October 4, 2016
Mirai botnet-as-a-service
Underground forum offers DDoS-as-a-service.

August | September | October | November

Threat Intelligence Sharing

What you don't know can hurt you.

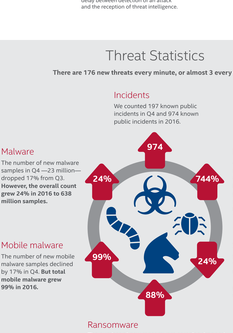
What is threat intelligence?

Strategic intelligence
Processed information that informs security policy and planning activities at the organizational level. It includes insights into the most likely adversaries and their targets, risk probabilities and impact assessments, and regulatory or legal obligations.

Tactical intelligence
Information gathered by security systems, scanners, and sensors. Often indicators of compromise, verified. Informs work and remediation efforts.

Operational intelligence
The critical components for establishing context. Includes the scope and extent of a suspected attack, and how best to respond to specific threats and events. Big data analytics, machine learning, and other automated decision-making techniques can be applied to this problem to augment human capacity and judgment.

Critical challenges in threat intelligence sharing



Volume
Security sensors, big data analytics, and machine-learning tools have created a massive signal-to-noise problem affecting the ability to triage, process, and act on intelligence.

Validation
We must vet shared threat intelligence sources to ensure that data comes from legitimate sources—and not from adversaries filing false reports to mislead or overwhelm threat intelligence tools.

Correlation
Validating data in near real time, correlating it across operating systems, devices, and networks, triaging the event, and scoping the response are critical to effective action.

Quality
Legitimate sources can send anything from indicators of compromise to an entire event feed, which may be irrelevant to the receiver. Filters, tags, and deduplication must be automated to make threat intelligence actionable.

Speed
Open, standardized, near real-time communication is essential to limit the delay between detection of an attack and the reception of threat intelligence.

Threat Statistics

There are 176 new threats every minute, or almost 3 every second.

Incidents
We counted 197 known public incidents in Q4 and 974 known public incidents in 2016.

Malware
The number of new malware samples in Q4—23 million—dropped 13% from Q3. **However, the overall count grew 24% in 2016 to 638 million samples.**

Mac OS malware
Although still small compared with Windows threats, the number of new Mac OS malware samples grew 245% in Q4, due to adware bundling. **Total Mac OS malware grew 744% in 2016.**

Mobile malware
The number of new mobile malware samples declined by 17% in Q4. **But total mobile malware grew 99% in 2016.**

Spam botnets
Spam emails from the top 10 botnets dropped 24% in Q4 to 181 million emails. These top 10 botnets generated 934 million spam email messages in 2016.

Ransomware
The number of new ransomware samples dropped 71% in Q4, mostly due to a drop in generic ransomware detections, as well as a decrease in Locky and CryptoWall. **The number of total ransomware samples grew 88% in 2016.**

McAfee Global Threat Intelligence

McAfee GTI received on average 49.6 billion queries per day.

66 million
McAfee GTI protections against malicious URLs **increased to 66 million per day in Q4** from 57 million per day in Q3.

37 million
McAfee GTI protections against potentially unwanted programs (PUPs) showed an **increase to 37 million per day in Q4** from 32 million per day in Q3.

McAfee GTI

71 million
McAfee GTI protections against malicious files **decreased to 71 million per day in Q4** from 150 million per day in Q3 due to greater download blocking.

35 million
McAfee GTI protections against risky IP addresses showed an **increase to 35 million per day in Q4** from 27 million per day in Q3.

McAfee Labs Threats Report: April 2017

Visit www.mcafee.com/April2017ThreatsReport for the full report.

© 2017 McAfee, Inc.
3414_0217_mfe-threat-report-mini-ed_ENG