

Threats Report

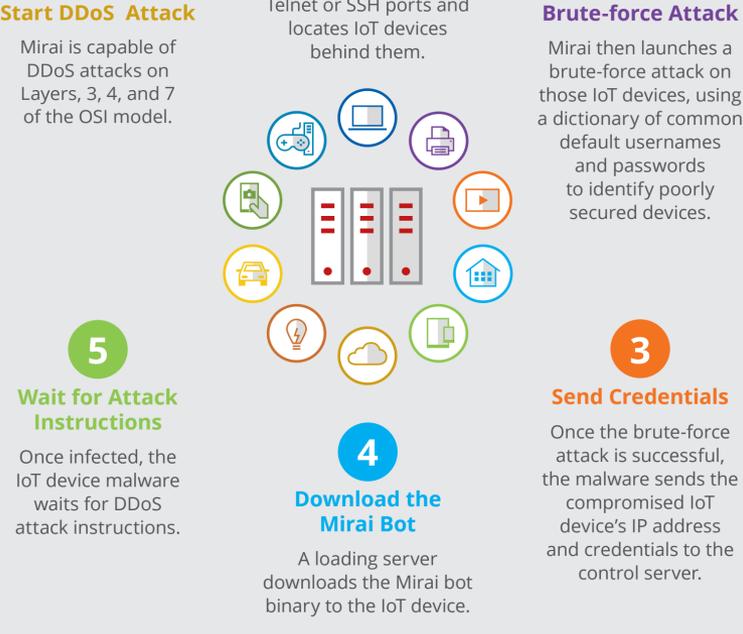
McAfee Labs

April 2017

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.

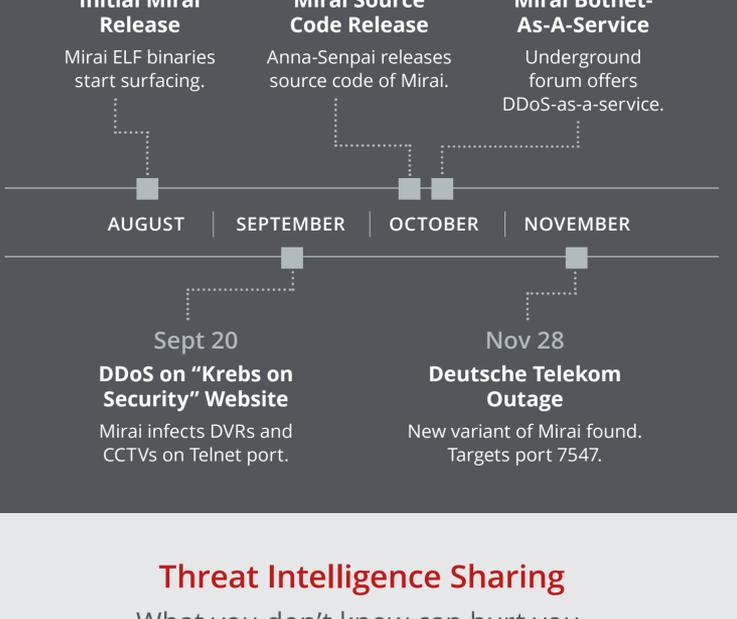
Attack Process



- 2.5 Million Infected**
About 2.5 million IoT devices have been infected with Mirai.
- 1.2 Tbps of Traffic**
At its peak, one Mirai botnet target was flooded by 1.2 Tbps of traffic, the highest volume of DDoS traffic ever recorded.
- 5 IPs Every Minute**
Every minute, about five IP addresses are added to Mirai botnets.
- \$50 - \$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

August - November 2016



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. This includes elements such as 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, useful for forensic 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 coordinate the incident response actions. 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.
- 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.
- 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.
- 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.

- ↑744% 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.
- ↑99% Mobile Malware**
The number of new mobile malware samples declined by 17% in Q4. But total mobile malware grew 99% in 2016.
- ↑88% 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.
- ↑974 Incidents**
We counted 197 known public incidents in Q4 and 974 known public incidents in 2016.
- ↑24% Malware**
The number of new malware samples in Q4—23 million—dropped 17% from Q3. However, the overall count grew 24% in 2016 to 638 million samples.
- ↓24% 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.

"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.
- 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.

Download: [McAfee Labs Threats Report: April 2017](#)
Visit: www.mcafee.com/April2017ThreatsReport for the full report.