

# Threats Report

**McAfee Labs**

December 2016

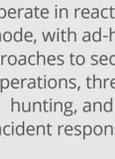
## The Security Operations Center

Current state and future plans for the security operations center.

Almost nine out of 10 companies have a SOC.



receive some type of security operations assistance from managed security services providers.



are progressing toward the goal of a proactive and optimized security operation, but 26% still operate in reactive mode, with ad-hoc approaches to security operations, threat hunting, and incident response.



use a SIEM solution today. 45% of those with a SIEM intend to deploy the functionality within the next 12-18 months.

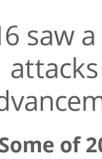


Most organizations are overwhelmed by alerts, and 93% are unable to triage all relevant threats.

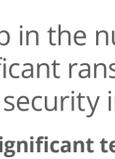


of those with a SOC have formal threat-hunting operations.

Areas for future growth improve the ability to:



to confirmed attacks, including coordination, remediation, eradication, and preventing reoccurrences.



signals of potential attacks, including focusing on relevant events and alerts, triage, and prioritization.



potential attacks, including scoping the full extent and impact of an attack.

## A Year at Ransom

2016 saw a huge jump in the number of ransomware attacks and significant ransomware technical advancements. The security industry fought back.

Some of 2016's most significant technical advancements in ransomware include:



Partial and full disk encryption.



Through the end of Q3, the number of new ransomware samples this year totaled 3.9 million, an increase of 80% since the beginning of the year.



Demands based on the victim's ability to pay.



Attackers pay service providers for the use of infrastructure and ransomware.



Encryption of websites used by legitimate applications.



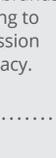
More sophisticated exploit kits for ransomware delivery.



Detecting and evading security sandboxes used to test suspicious code.

The security industry fought back.

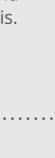
### Collaboration



#### No More Ransom!

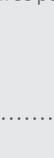
Founded in July, this organization provides prevention advice, investigation assistance, and decryption tools.

### Law Enforcement Actions



#### WildFire

Ransomware takedown.



#### Shade

Ransomware takedown.

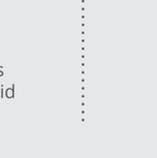
## "Trojanized" Legitimate Software

Trojans infect legitimate code and hide, hoping to go unnoticed as long as possible to maximize payouts.

### Trojan Benefits



Payloads are concealed behind recognizable brands, contributing to the impression of legitimacy.



Legitimate software provides cover during security scans and forensics analysis.

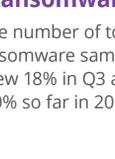


Trojanizing legitimate software provides free persistence.

## Ways to Trojanize legitimate software:



executable as they are downloaded through man-in-the-middle attacks.



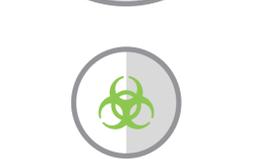
interpreted, open-sourced, or decompiled code.



clean and dirty files together using binders or joiners.



the master source code, especially in redistributed libraries.



using patchers, seamlessly maintaining application use.



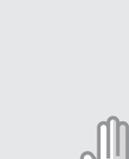
Through Q3, more than 700,000 Trojanized binaries were seen from three Android malware families.



Through Q3, 30,000 Android binaries were Trojanized using two popular backdoor patching kits.

## Threat Statistics

There are 245 new threats every minute, or more than 4 every second.



### Mac OS Malware

Although still small compared with Windows threats, the number of new Mac OS malware samples grew 65% in Q3. Total Mac OS malware has grown 215% in the past year.



### Ransomware

The number of total ransomware samples grew 18% in Q3 and 80% so far in 2016.



### Malware

The number of new malware samples in Q3—32 million—dropped 21% from Q2. However, the overall count has grown 29% in the past year to 644 million samples.



### Mobile Malware

The number of new mobile malware samples—more than 2 million—was the highest ever recorded in Q3. Total mobile malware has grown 138% in the past year.



### Macro Malware

New macro malware continues at a high rate. Total macro malware grew 32% in the past quarter.



### Spam Botnets

Spam emails generated from the Kelihos botnet dropped 97% in Q3 but the Necurs botnet increased 554%. In aggregate, spam emails from botnets dropped 19% in Q3.

## McAfee Global Threat Intelligence

McAfee GTI received on average 44.1 billion queries per day.



McAfee GTI protections against malicious URLs decreased to 57 million per day in Q3 from 100 million per day in Q2.



McAfee GTI protections against malicious files increased to 150 million per day in Q3 from 104 million per day in Q2. Last year for this period, we saw a decrease.



McAfee GTI protections against potentially unwanted programs showed a small increase in Q3 from Q2. However, there was a dramatic drop in Q3 2016 compared with Q3 2015. In Q3 2016, we saw 32 million per day v. 175 million per day in Q3 2015.



McAfee GTI protections against risky IP addresses showed a slight decrease to 27 million per day in Q3 from 29 million per day in Q2. This was a much smaller decrease than the one seen from Q2 to Q3 in 2015.

Download *McAfee Labs Threats Report: December 2016*

Visit: [www.mcafee.com/December2016ThreatsReport](http://www.mcafee.com/December2016ThreatsReport)