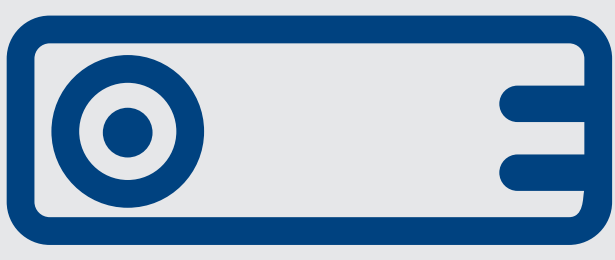
May 2015

Threats Report

McAfee Labs

Hard Drive Firmware Exploits

The Equation Group's malware infects hard disk and solid state drives and cannot be removed or detected.



Phase 1

Web-based exploitation
Victim visits infected website. Target's system is infected by 1st stage malware.

Phase 2

1st stage install/implant DoubleFantasy
Confirms target and delivers 2nd stage malware.

Phase 3

2nd stage install/implant EquationDrug/GrayFish
Manages installation and maintenance of HDD/SSD firmware modules.

Phase 4

HDD/SSD firmware modules
Reprograms firmware, manages hidden storage area.

Equation Group HDD/SSD attack modules:

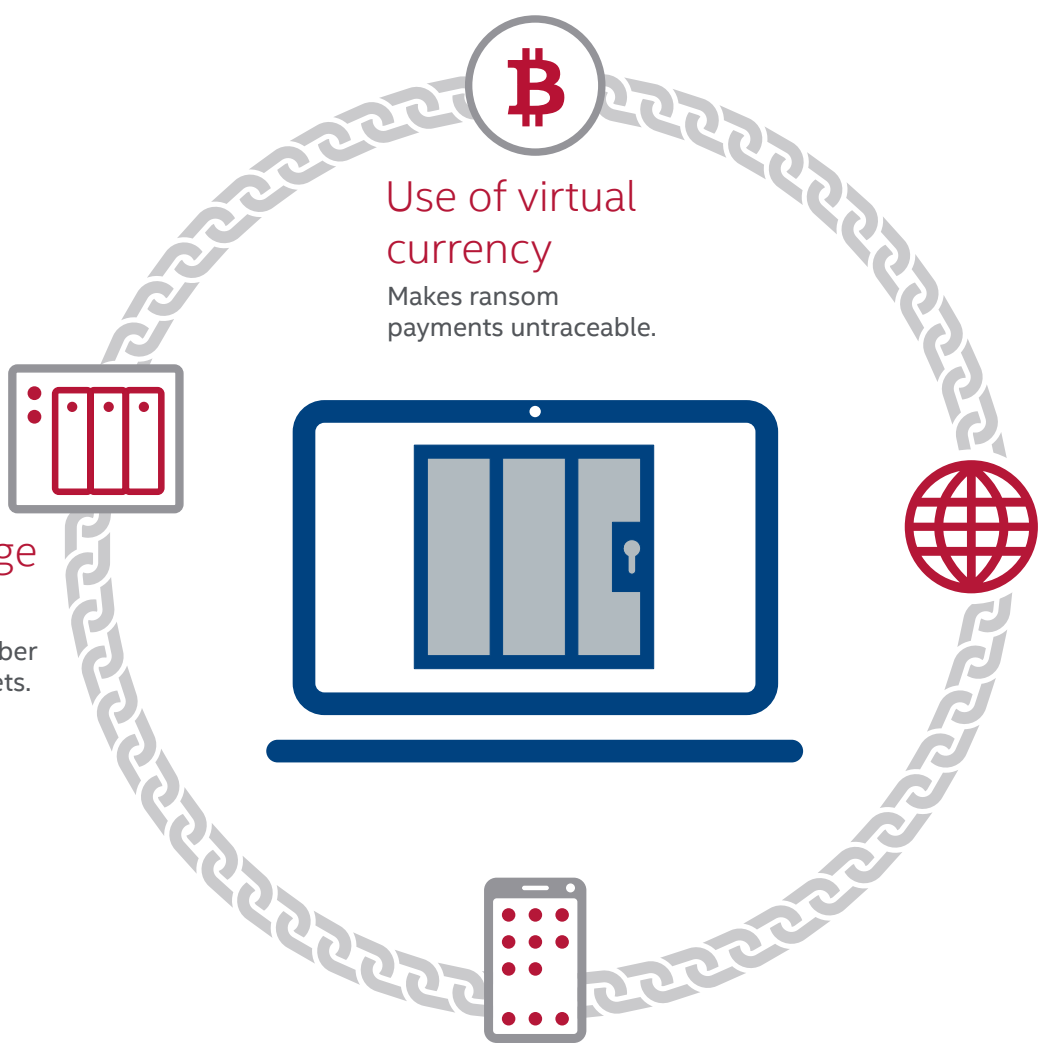
- **Persistent:** Reprogrammed firmware can survive disk reformatting and operating system reinstallation.
- **Invisible:** Hidden storage area is known only to the reprogrammed firmware and it remains intact even if the HDD/SSD is reformatted.
- **Undetectable:** Reprogrammed firmware and hidden malware is undetectable by security software once the drive has been infected.

McAfee Labs considers this one of the most visible and advanced examples of firmware attack ever seen.

Ransomware Returns

Attacks are growing rapidly, led by a new ransomware family.

Ransomware has become more powerful:



Use of virtual currency

Makes ransom payments untraceable.

Use of Tor network

Allows attackers to hide the location of their control servers.

Targeting mass-storage devices

Increases the number of high-value targets.

Moving to mobile

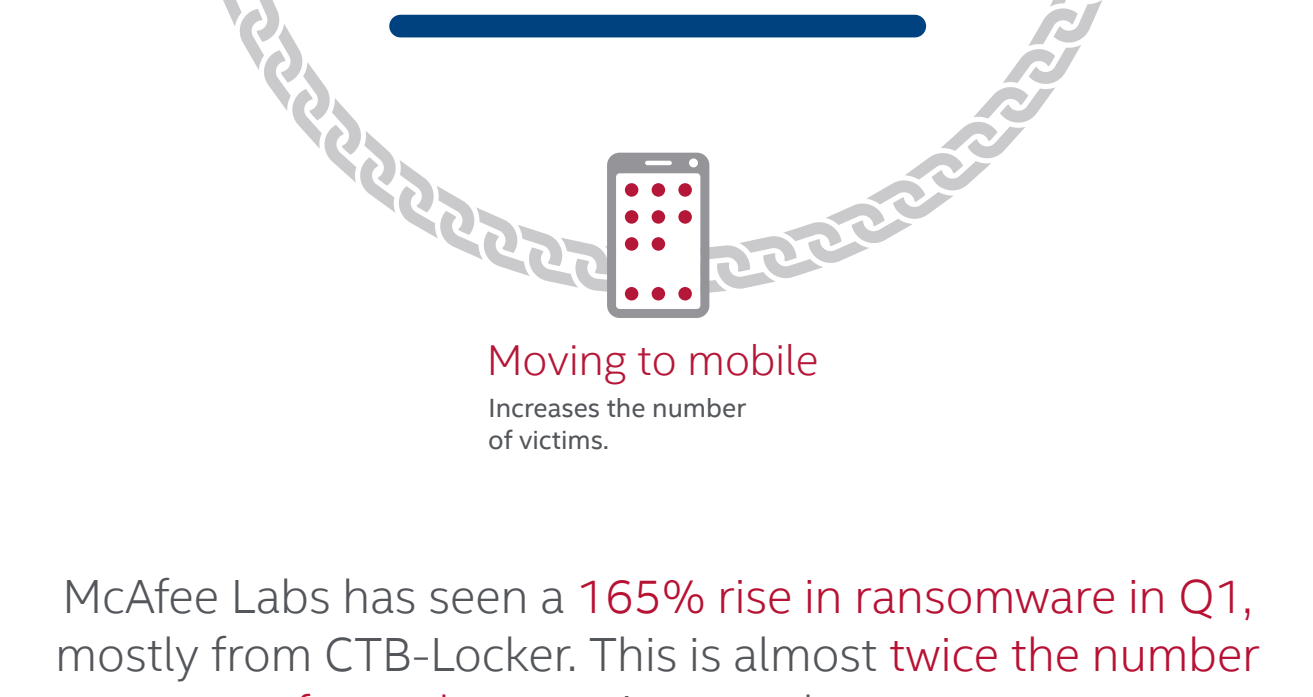
Increases the number of victims.

McAfee Labs has seen a 165% rise in ransomware in Q1, mostly from CTB-Locker. This is almost twice the number of samples seen in any other quarter.

Adobe Flash Vulnerabilities

Vulnerabilities that have not been patched by users lead to rapid increase in attacks.

Number of Flash .swf samples seen by Intel Security:



Why do malware authors target Adobe Flash?

- Flash's popularity has attracted malware authors.
- User delay in applying available software patches that eliminate vulnerabilities.
- Steep increase in the number of mobile devices.
- New methods of Flash exploitation.

The number of new Flash .swf samples increased by 317% in Q1 2015.

42 new Flash CVEs were added in Q1 2015, an increase of 50% from Q4 2014. All 42 have been patched by Adobe.

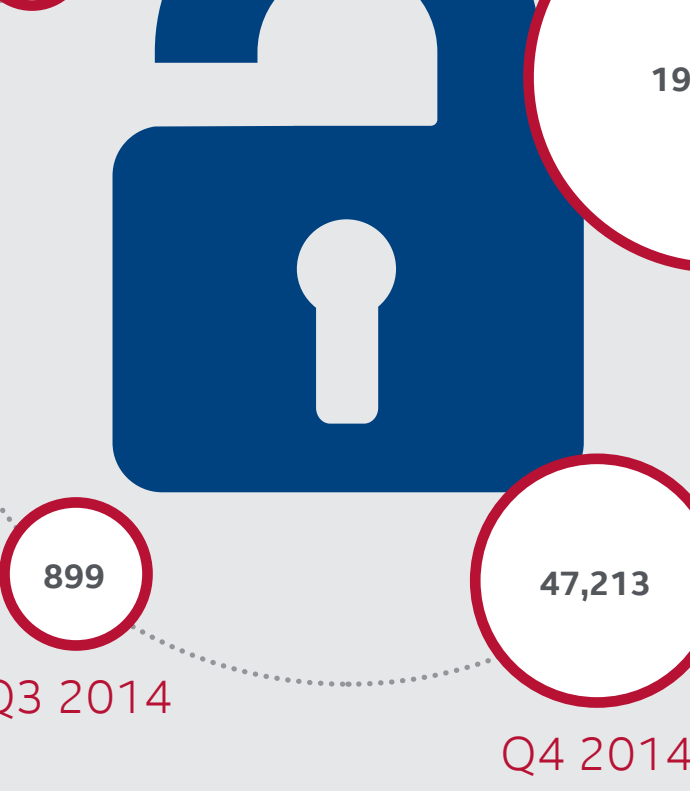
Threat Statistics

May 2015

There are 362 new threats every minute, or more than 6 every second.

The McAfee Labs malware zoo grew 13% from Q4 2014 to Q1 2015. It now contains 400 million samples.

The number of new mobile malware samples jumped by 49% from Q4 2014 to Q1 2015.



Spam held steady with 6 trillion spam messages sent in Q1 2015.

New suspect URLS are growing quickly again, with an 81% jump from Q4 2014 to Q1 2015.

McAfee Labs Threats Report: May 2015

Visit **www.mcafee.com/May2015ThreatsReport** for the full report.

intel Security

61955info_qtr-q1_0615_fnl_PAIR

McAfee is now part of Intel Security.