November 2015

Threats Report

McAfee Labs

Fileless Malware

The newest fileless malware leaves no trace on disk, making detection more difficult.

21,403
Powelike family

47,418
Kovter family

5,650
XswKit family

74,471 samples
In the first three quarters of 2015, McAfee Labs detected 74,471 samples from three prominent fileless malware families.

Types of fileless malware

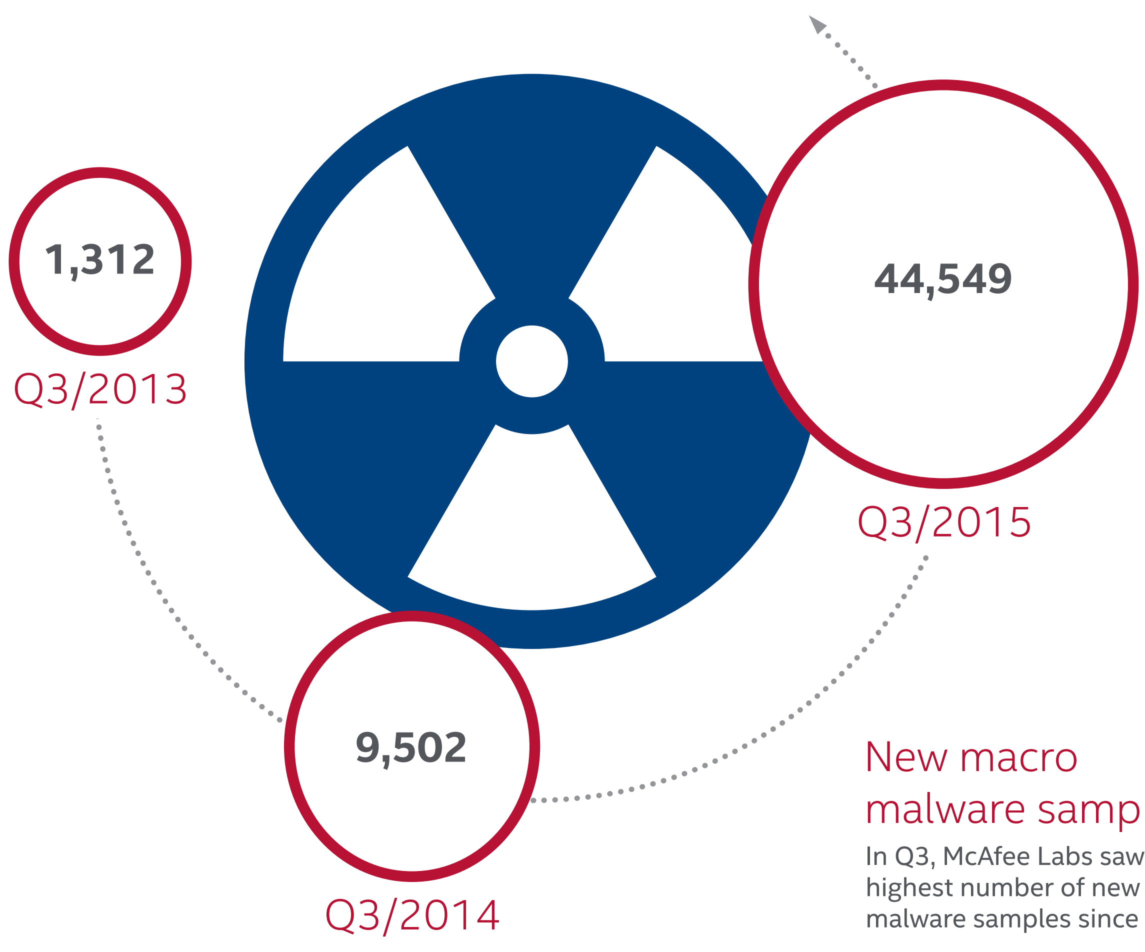
Memory resident
Uses the memory space of a legitimate application.

Rootkits
Hides its presence behind a user- or kernel-level API.

Windows registry
Resides in the registry of the Windows operating system.

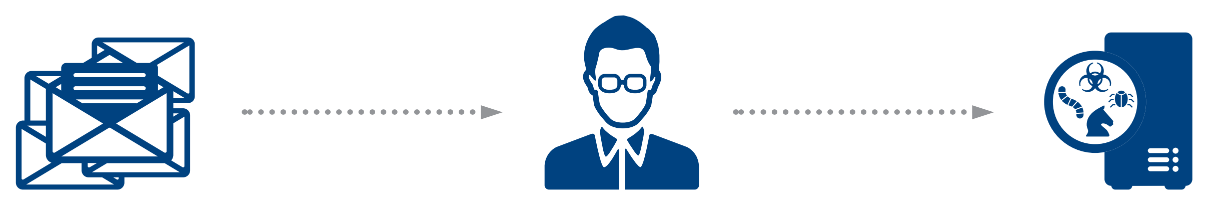
Macro Malware

Macro malware returns to prominence through sophisticated spam campaigns and clever macros that remain hidden even after they have downloaded their payloads.



New macro malware samples
In Q3, McAfee Labs saw the highest number of new macro malware samples since 2009.

Macro malware infection chain



Spam Contains Office Document with Macro

User Enables and Executes the Macro

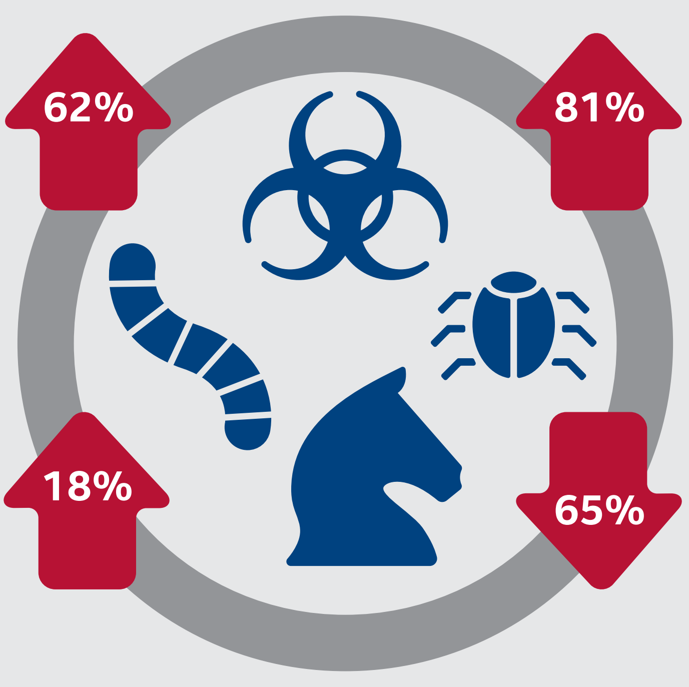
Malware Downloads More Malware from Control Server

Remains hidden
Macro malware-laden files appear to be normal documents, even after performing their malicious acts.

Social engineering techniques
Macro malware developers are using sophisticated social engineering techniques to turn unwitting enterprise users into victims.

Threat Statistics

There are 327 new threats every minute, or more than 5 every second.



The McAfee Labs malware zoo has grown 62% during the past year. It now contains more than 476 million samples.

The total number of mobile malware samples grew 81% during the past year. New mobile malware has risen for five consecutive quarters.

The number of new ransomware samples grew 18% from Q2 to Q3. The total number of ransomware samples grew 155% over the past year.

New rootkit malware dropped 65% from Q2 to Q3. It is the lowest number of new samples since Q4 of 2008.

McAfee Global Threat Intelligence

McAfee GTI received on average 44.5 billion queries per day.

7.4M attempts
More than 7.4 million attempts were made to entice our customers into connecting to risky URLs.

7.4M PUPs
An additional **7.4 million potentially unwanted programs** attempted installation or launch.

McAfee GTI

3.5M files
More than 3.5 million infected files were exposed to our customers' networks.

2.2M attempts
2.2 million attempts were made to connect to or from risky IP addresses.

McAfee Labs Threats Report: November 2015

Visit **www.mcafee.com/November2015ThreatsReport** for the full report.

intel Security

62190info_nov-threats_1215_PAIR

McAfee is now part of Intel Security.