September 2017

McAfee
Together is power.

Threats Report

McAfee Labs

I don't WannaCry no more

The WannaCry attacks infected more than 300,000 computers in over 150 countries in less than 24 hours.

>300,000
The WannaCry attacks infected more than 300,000 computers.

>150
In over 150 countries.

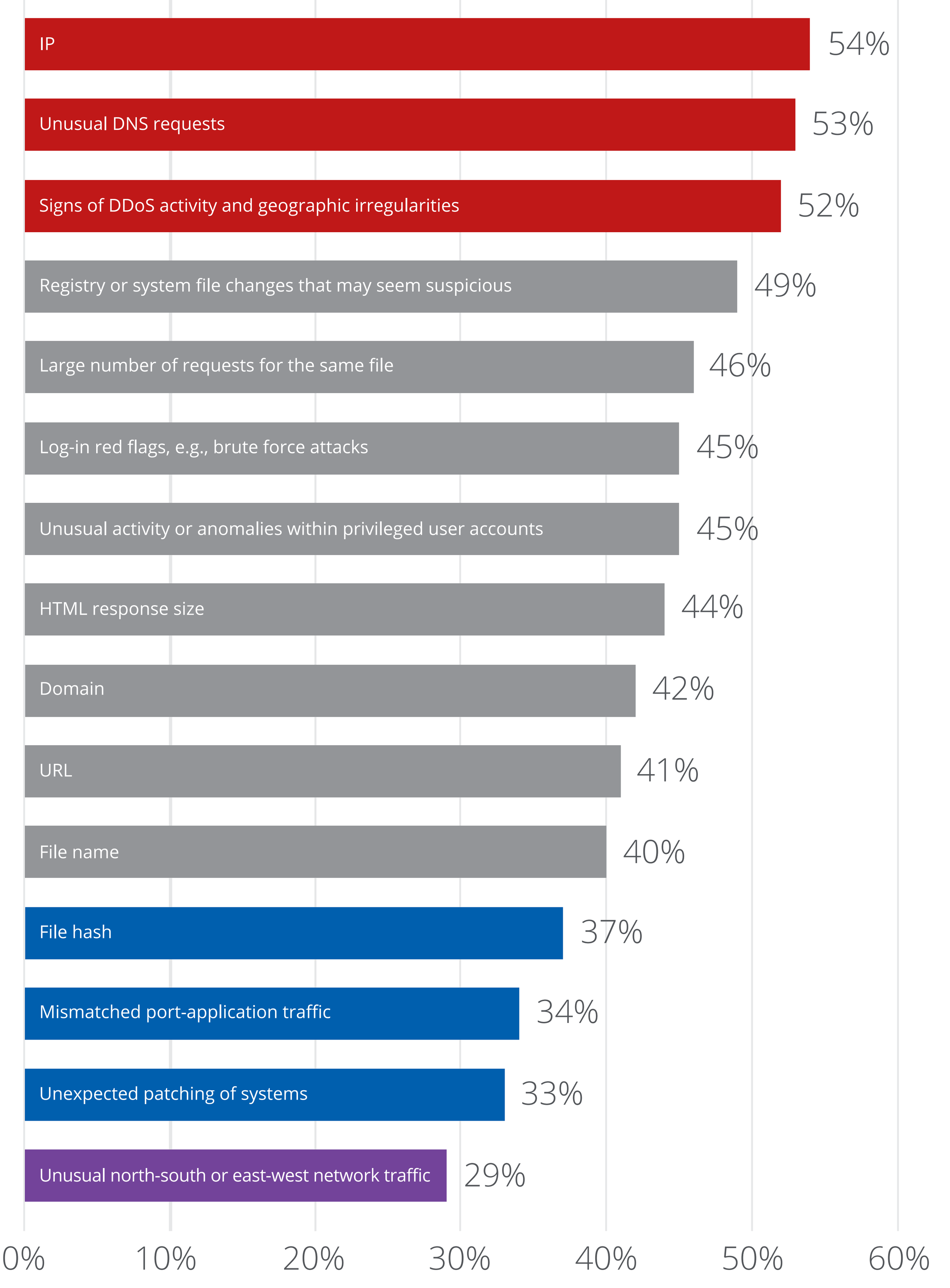
<24
In less than 24 hours.

Threat hunting like a pro

Threat hunting is a proactive approach to finding attacks and compromised machines without waiting for alerts. Threat hunters assume that there is always at least one compromised system on the network, the victim of an attack that has managed to evade the organization's security measures.

Indicators of Compromise

Which of the following IOCs do you typically use for threat hunting?



Source: McAfee Threat Hunting Survey, May 2017.

Examples of Effective Threat Hunting

From McAfee Foundstone Services security consulting team

EXAMPLE 1
Hunting for command and control
Hypothesis: An infected system on the network is generating command and control traffic that has not yet been detected.
How to: Perform least-frequent analysis on both DNS and user agents.

EXAMPLE 2
Hunting for persistence
Hypothesis: At least one system is infected by some malware variant that has established itself to autostart and that has not yet been detected.
How to: Take daily snapshots and run diffs and least-frequent analysis, focusing on the outliers.

EXAMPLE 3
Hunting for privilege escalation
Hypothesis: An attacker already present on a compromised system is trying to elevate privileges by adding a user to a privileged group.
How to: Examine the creation of Event IDs 4728, 4732, and 4756 on enterprise domain controllers (or individual computers in nondomain environments).

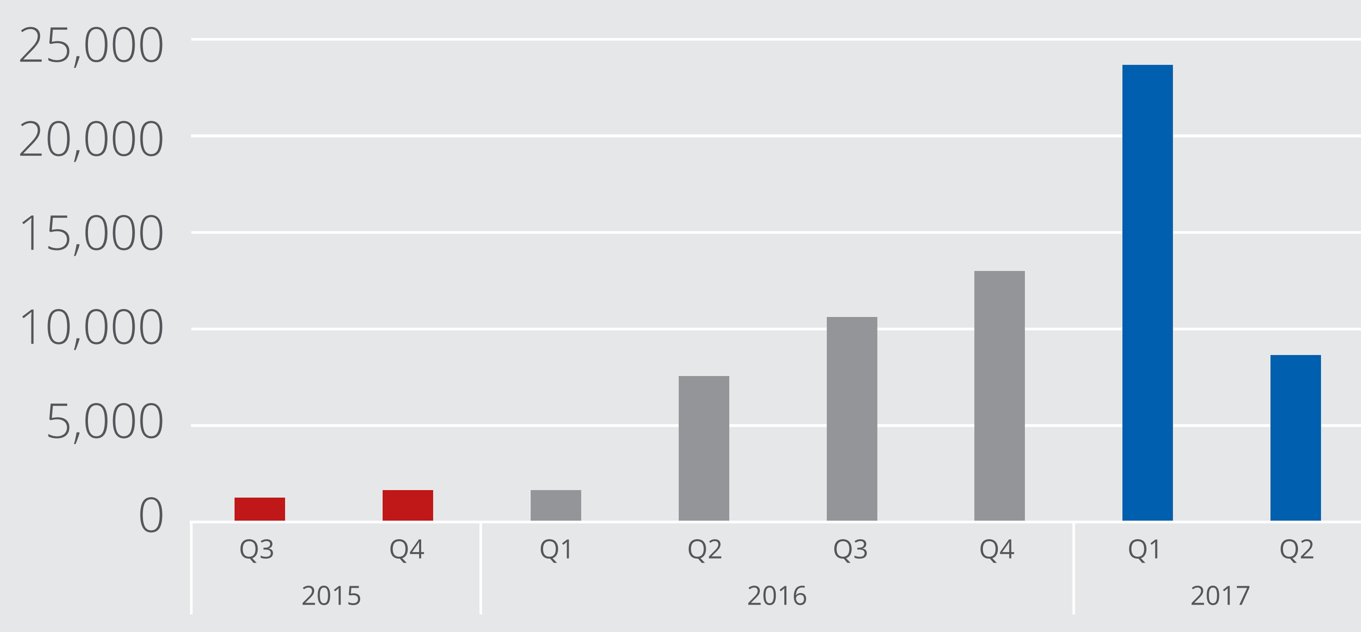
EXAMPLE 4
Hunting for Lateral Movement
Hypothesis: An active attacker on the network is trying to move laterally by employing Microsoft's PsExec admin tool.
How to: Examine the creation of Event ID 7045 for evidence of PsExec execution and ID 7045 in combination with ID 7030 for evidence of Metasploit's PsExec execution.

EXAMPLE 5
Hunting for exfiltration
Hypothesis: An attacker is attempting to exfiltrate a large volume of data to a nonbusiness-related geolocation.
How to: Profile what normal looks like on your network and hunt for connections that remain pinned for a long time, connections to foreign countries, and connections with a high volume of data sent.

The rise of script-based malware

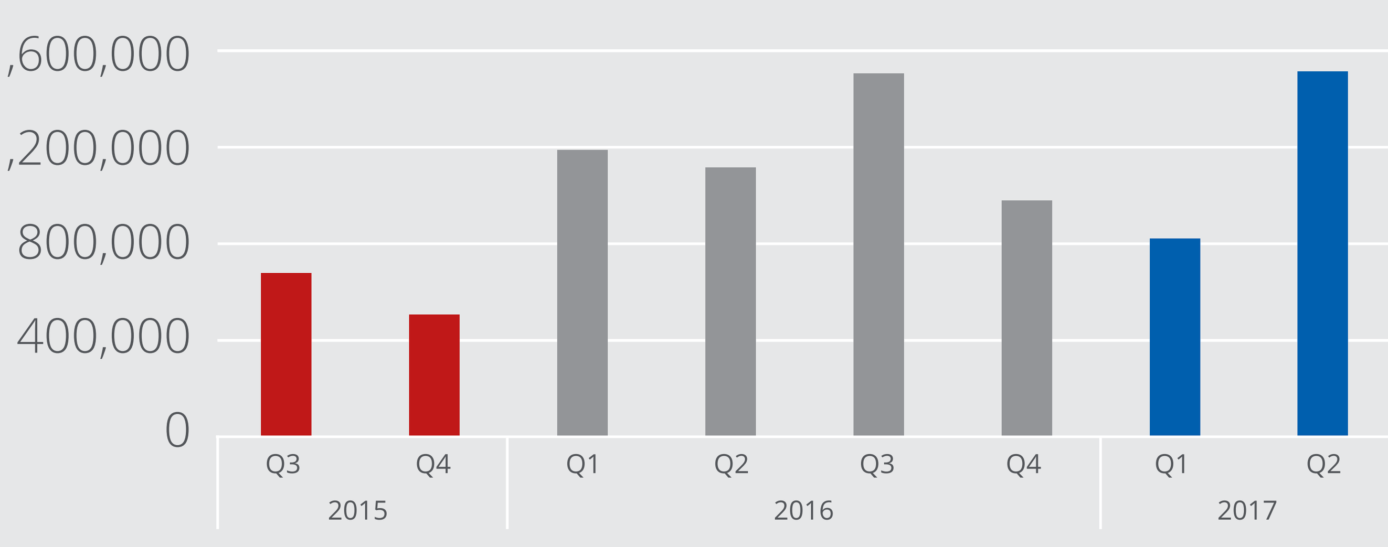
Malware authors use JavaScript, VBScript, PHP, PowerShell, and other scripts to distribute their malware.

PowerShell malware submitted to McAfee Labs



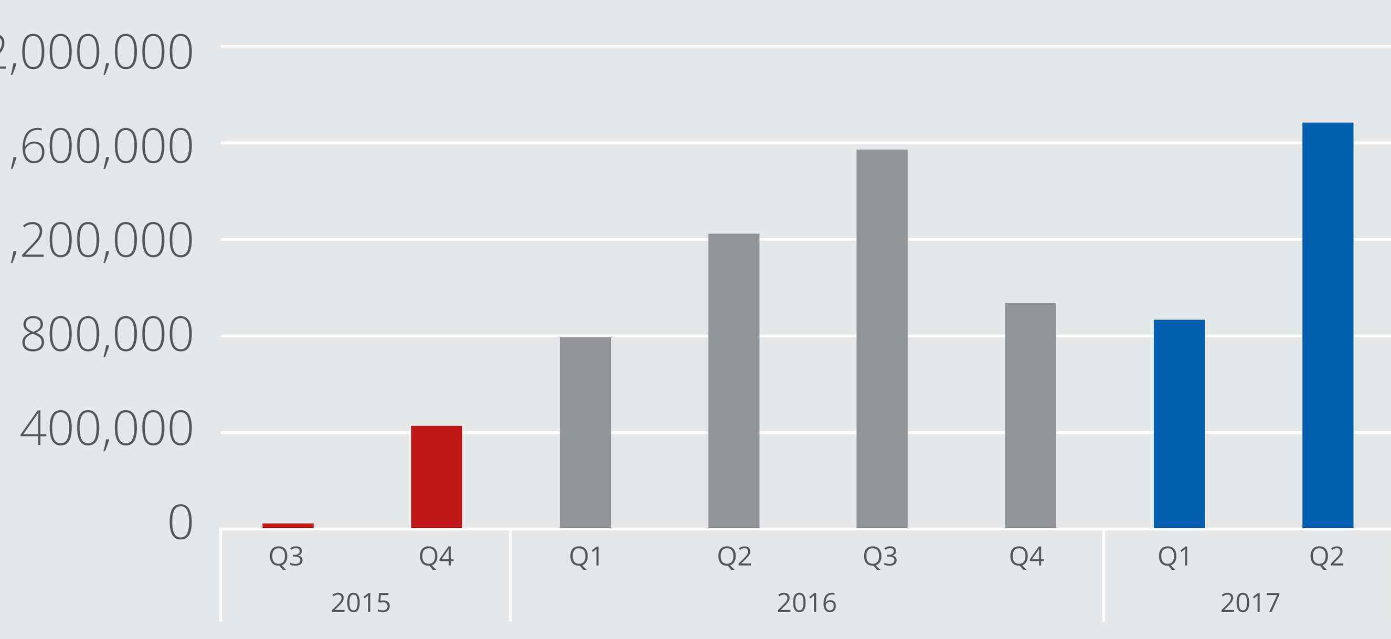
Source: McAfee Labs, September 2017.

Hypertext-application and VBS malware submitted to McAfee Labs



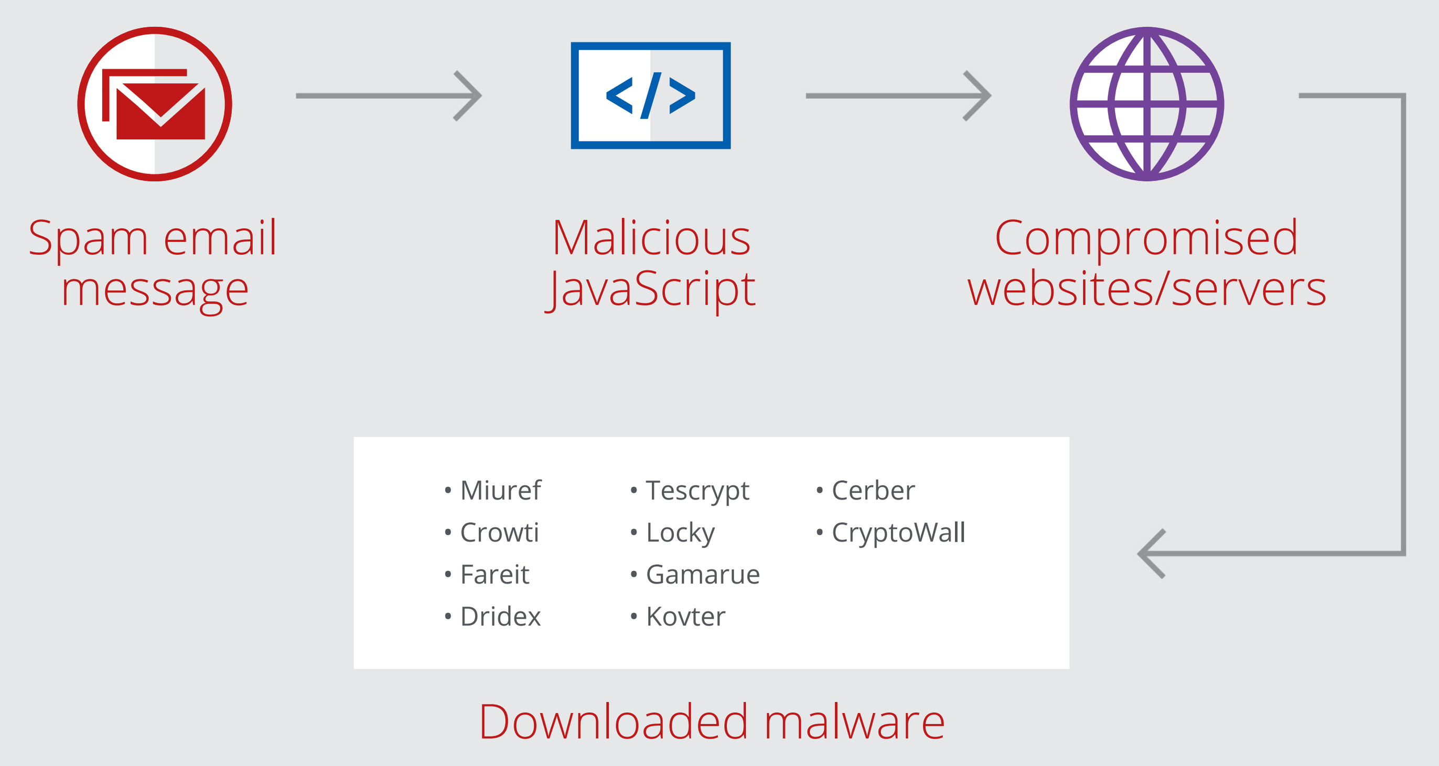
Source: McAfee Labs, September 2017.

Nemucod malware submitted to McAfee Labs



Source: McAfee Labs, September 2017.

The first steps in an infection



Threat Statistics

Incidents
We counted 311 publicly disclosed security incidents in Q2, an increase of 3% over Q1. The health, public, and education sectors comprised more than 50% of the total. 78% of all publicly disclosed security incidents in Q2 took place in the Americas.

Malware
New malware samples leaped up in Q2 to 52 million, a 67% increase. **The total number of malware samples grew 23% in the past four quarters to almost 723 million samples.**

Mobile malware
Global infections of mobile devices rose by 8%, led by Asia with 18%. **Total mobile malware grew 61% in the past four quarters to 18.4 million samples.**

Mac OS malware
With the decline of a glut of adware, Mac OS malware has returned to historical levels, growing by only 27,000 in Q2. Still small compared with Windows threats, **the total number of Mac OS malware samples increased by just 4% in Q2.**

Macro malware
New macro malware rose by 35% in Q2. **91,000 new samples raised the total count to 1.1 million.**

Ransomware
New ransomware samples again increased sharply in Q2, by 54%. **The number of total ransomware samples grew 47% in the past four quarters to 10.7 million samples.**

McAfee Global Threat Intelligence

McAfee GTI received on average 44 billion queries per day in Q2.

42 million
McAfee GTI protections against medium-risk URLs **decreased to 42 million per day in Q2 from 95 million per day in Q1** due to improved accuracy.

77 million
McAfee GTI protections against potentially unwanted programs **rose to 77 million per day in Q2 from 56 million per day in Q1.**

36 million
McAfee GTI protections against malicious files **increased to 36 million per day in Q2 from 34 million per day in Q1** due to earlier malware detection and better local intelligence.

57 million
McAfee GTI protections against risky IP addresses declined to **57 million per day in Q2 from 61 million per day in Q1** due to earlier detection.

McAfee Labs Threats Report: September 2017

Visit www.mcafee.com/September2017ThreatsReport for the full report.

McAfee
Together is power.

3580_0917_info-threats-report-wannacry_PAIR