

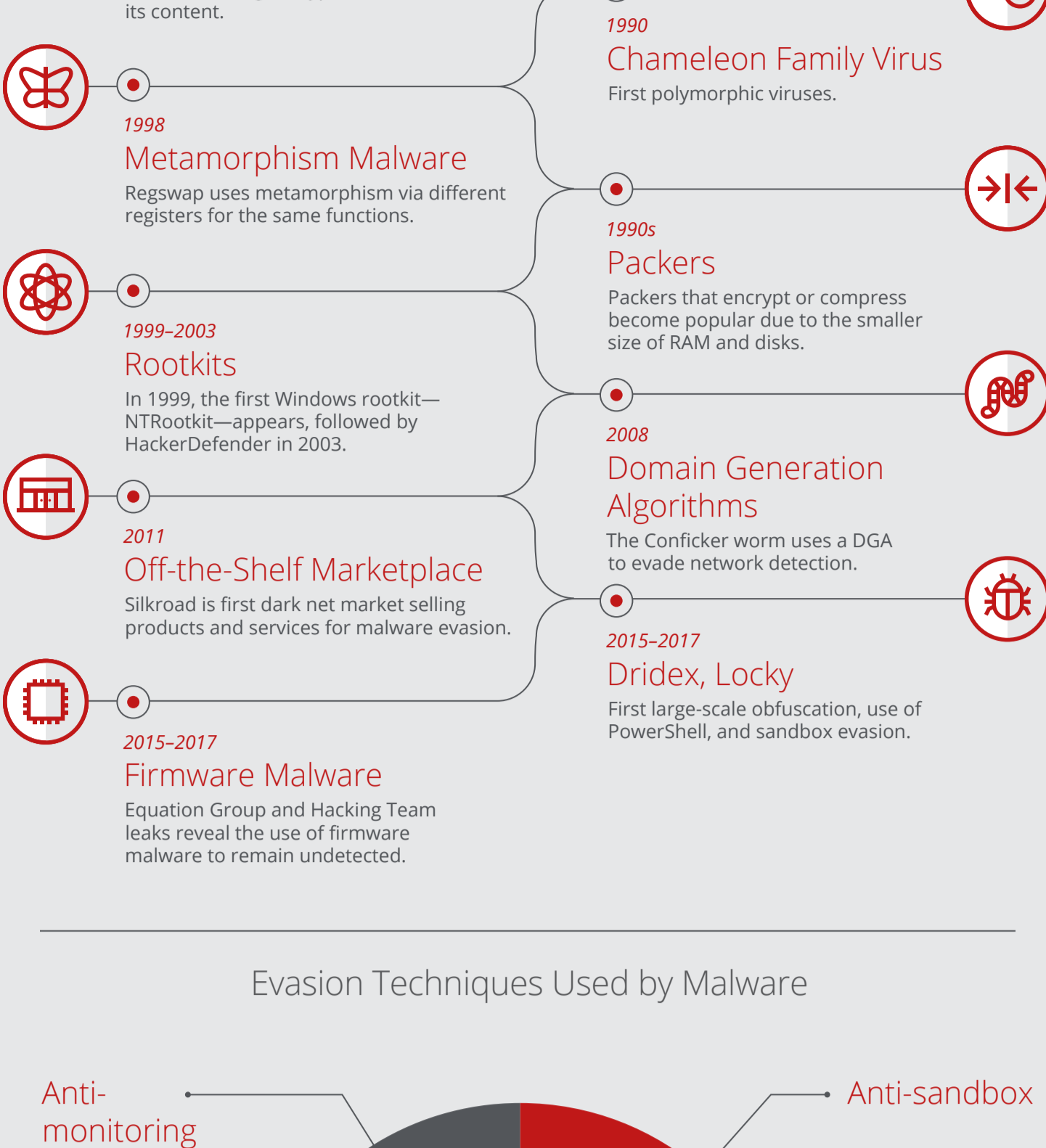
Threats Report

McAfee Labs

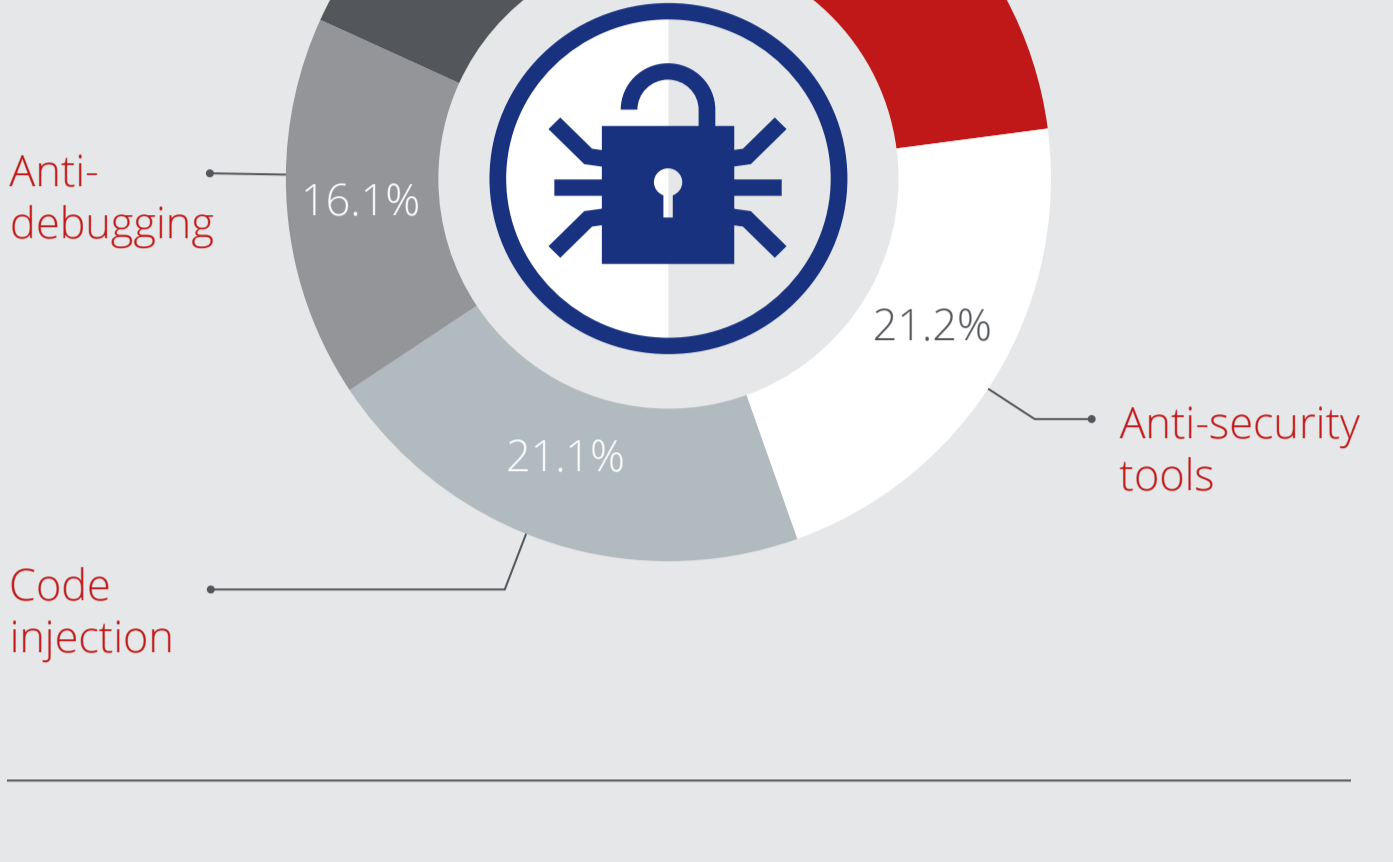
Malware evasion techniques and trends

Malware evasion techniques are widely available and are becoming more powerful.

The History of Evasion Techniques



Evasion Techniques Used by Malware



Evasion

Evasion technique code can be purchased off the shelf, sometimes for free.



Firmware

Firmware infection is a growing method to evade detection.



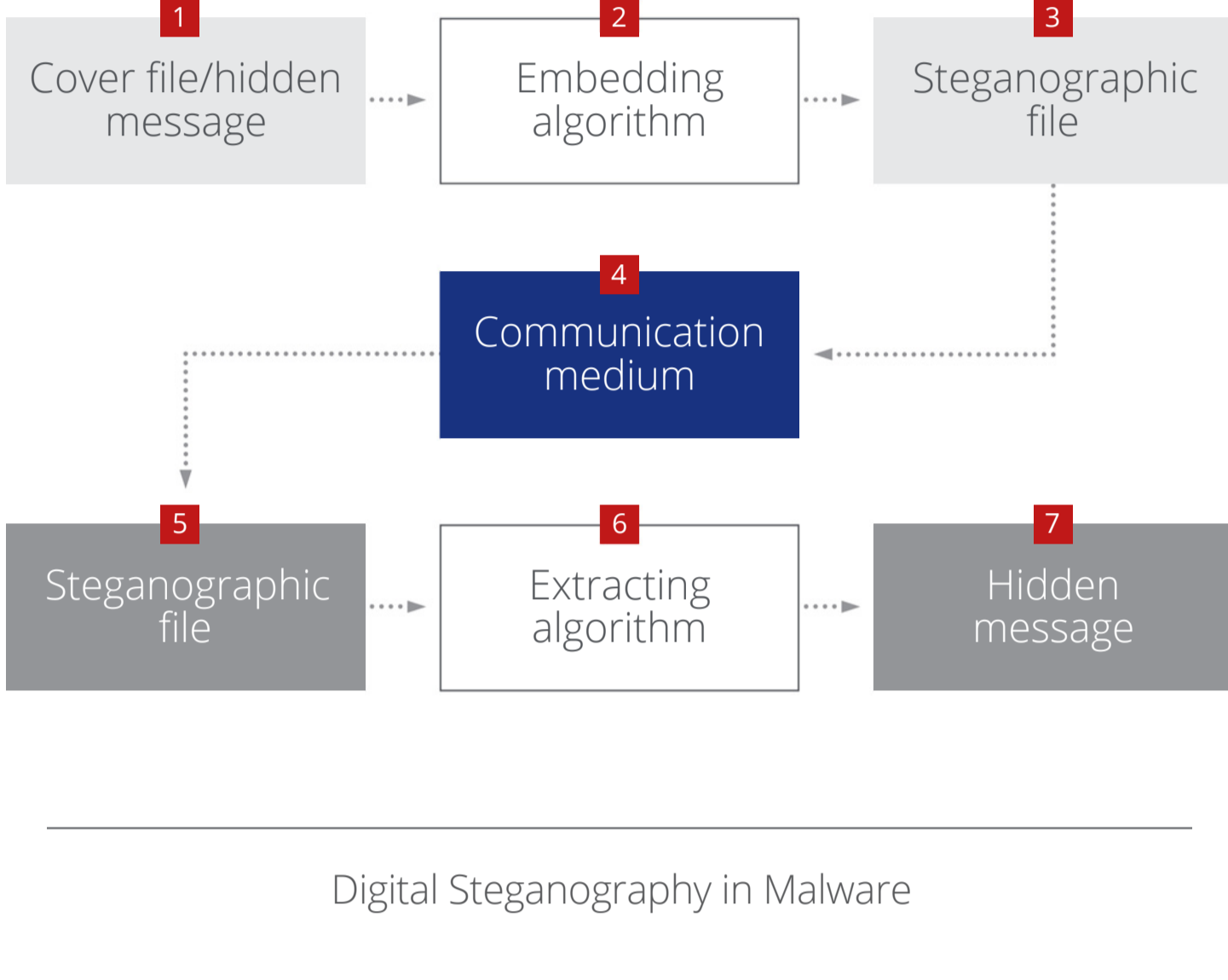
Machine learning

Attackers are developing techniques to evade machine learning security.

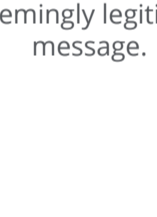
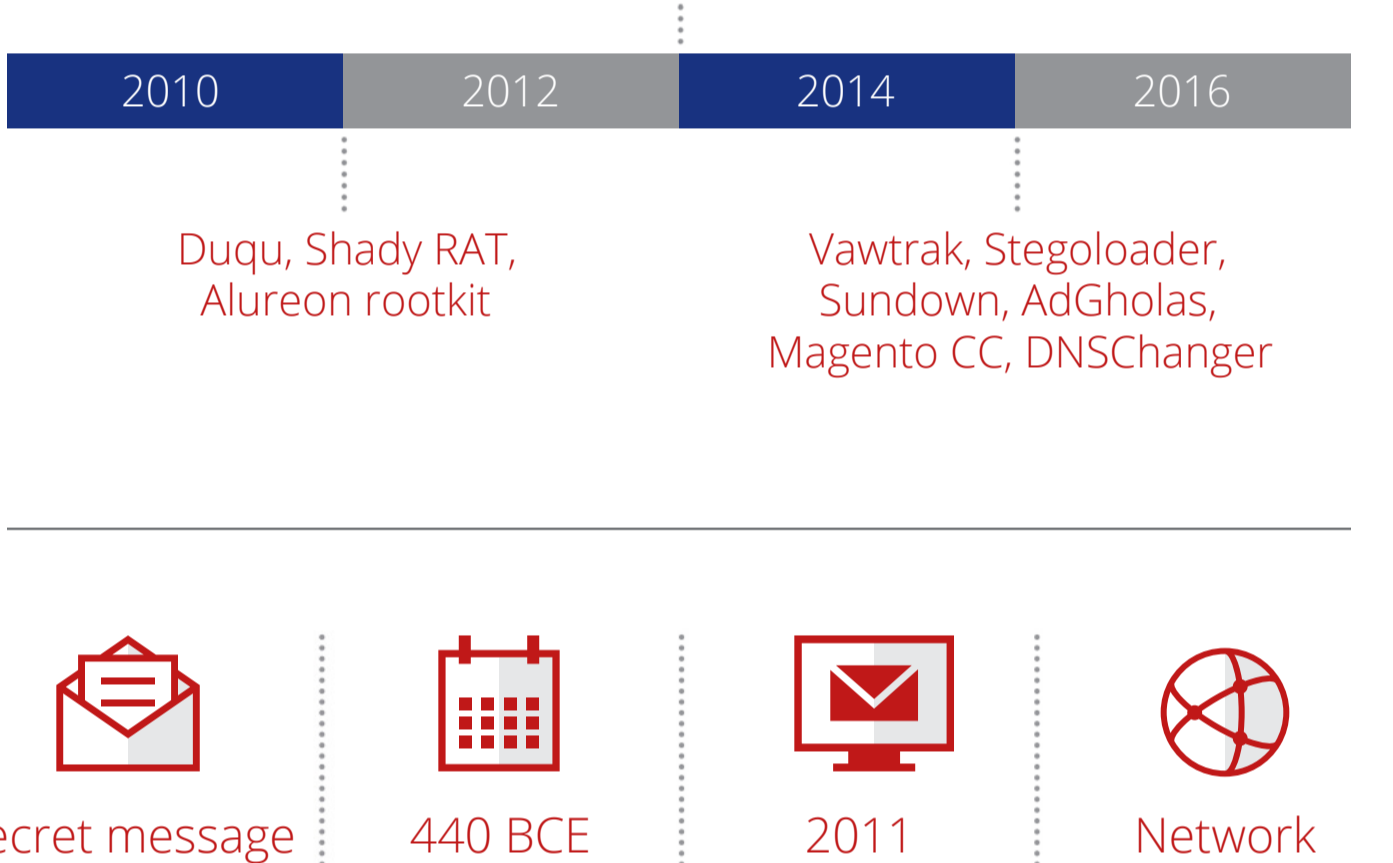
Hiding in plain sight: The concealed threat of steganography

Steganography—the art and science of secret hiding.

The Digital Steganography Process



Digital Steganography in Malware



Secret message

Steganography hides a secret message within a seemingly legitimate message.



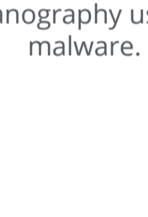
440 BCE

Steganography has been used in various forms since at least 440 BCE.



2011

Digital steganography was first used by Duqu in 2011.



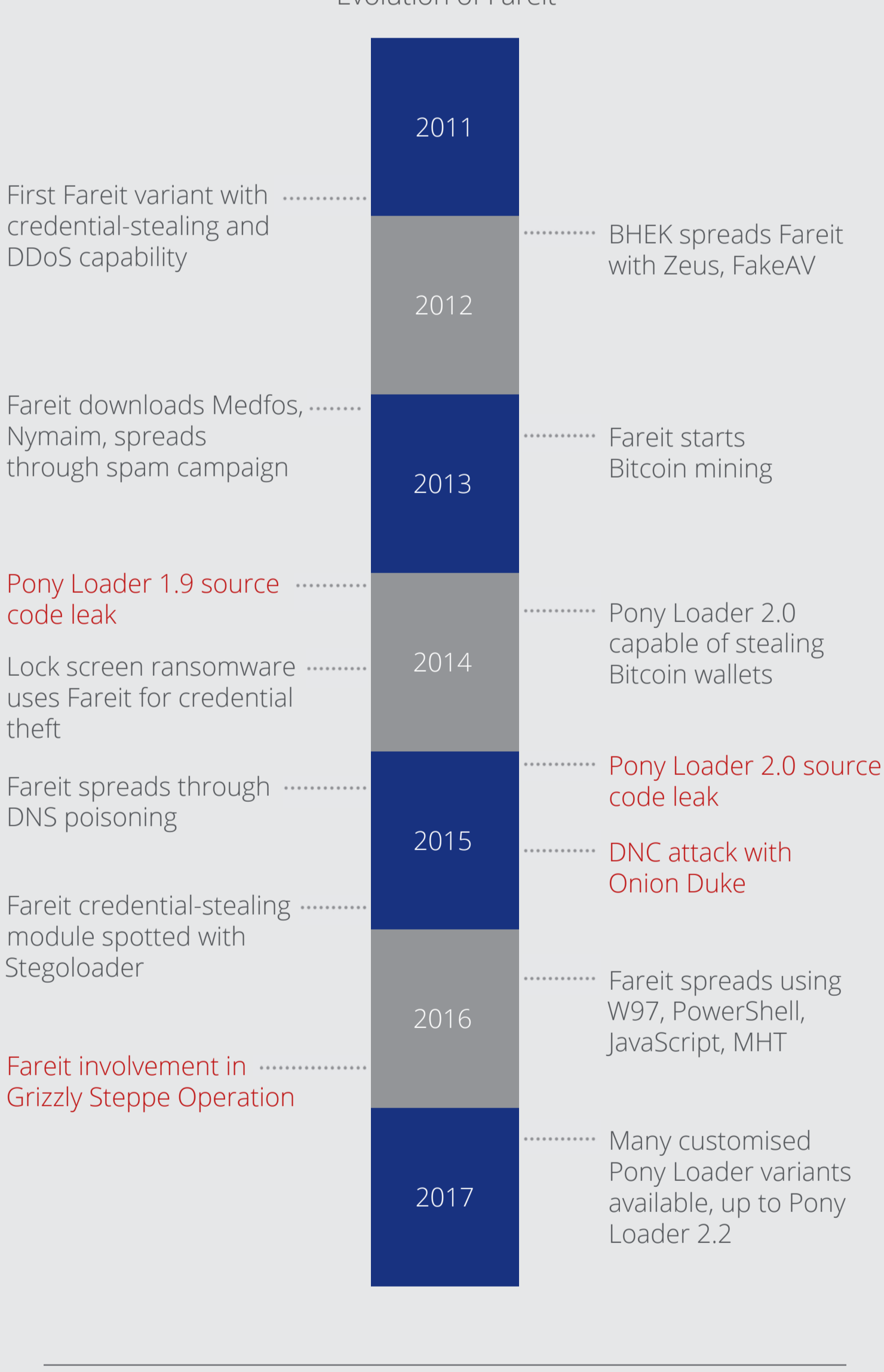
Network

Network steganography is the latest type of digital steganography used by malware.

The growing danger of Fareit, the password stealer

Password stealers are used in the early stages of nearly all major advanced persistent threats. Fareit was likely used in the 2016 breach of the Democratic National Committee.

Evolution of Fareit



5,599

Fareit was first discovered in 2011. There have been 5,599 Fareit customer incidents in the past year.

Fareit has several capabilities:

- Steal passwords
- Download and execute arbitrary malware
- Perform DDoS attacks
- Steal cryptocurrency wallets
- Steal FTP credentials

Threat Statistics

In Q1, there were 244 new threats every minute, or more than 4 every second.

Incidents

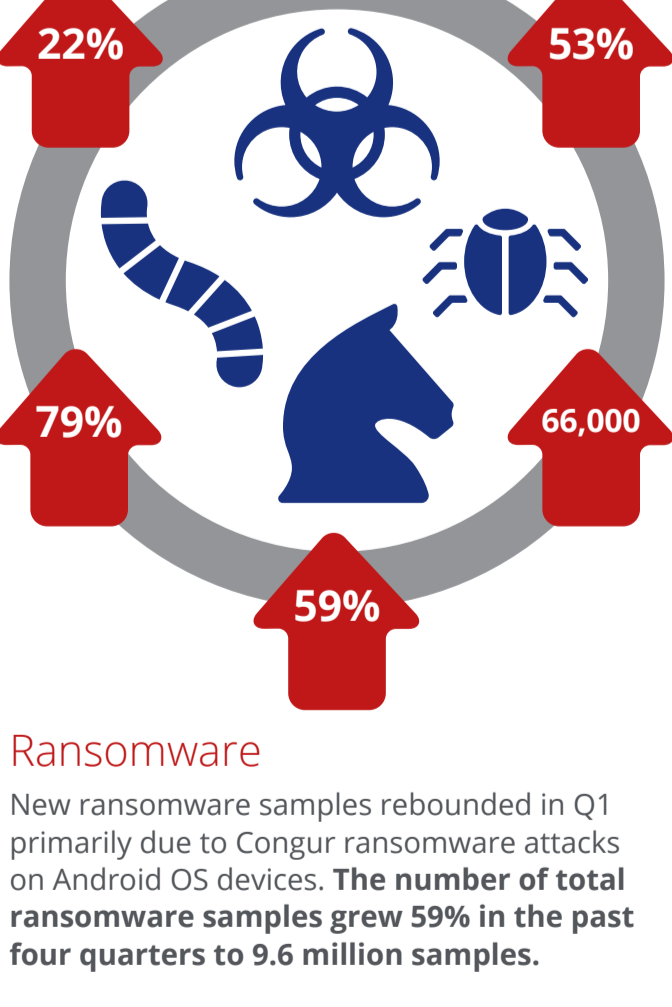
We counted 301 publicly disclosed security incidents in Q1, an increase of 53% over Q4. The health, public, and education sectors comprised more than 50% of the total. 78% of all publicly disclosed security incidents in Q1 took place in the Americas.

Malware

New malware samples rebounded in Q1 to 32 million. The total number of malware samples increased 22% in the past four quarters to 670 million samples.

Mobile malware

Mobile malware reports from Asia doubled in Q1, contributing to a 57% increase in global infection rates. Total mobile malware grew 79% in the past four quarters to 16.7 million samples.



Mac OS malware

During the past three quarters, Mac OS malware has been boosted by a glut of adware. Although still small compared with Windows threats, the total number of Mac OS malware samples grew 53% in Q1.

Macro malware

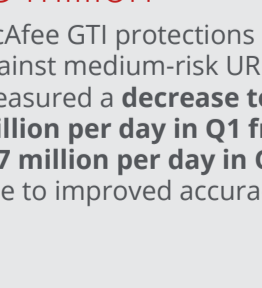
New macro malware subsided to its 3-year average. 66,000 new macro malware samples were seen in Q1.

Ransomware

New ransomware samples rebounded in Q1 primarily due to Congur ransomware attacks on Android OS devices. The number of total ransomware samples grew 59% in the past four quarters to 9.6 million samples.

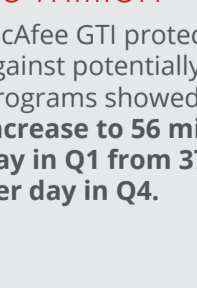
McAfee Global Threat Intelligence

McAfee GTI received on average 55 billion queries per day in Q1.



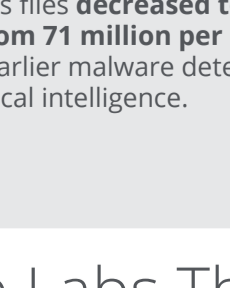
95 million

McAfee GTI protections against medium-risk URLs measured a decrease to 95 million per day in Q1 from 107 million per day in Q4 due to improved accuracy.



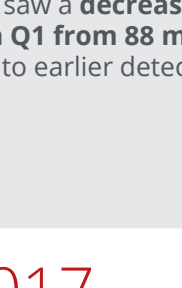
56 million

McAfee GTI protections against potentially unwanted programs showed an increase to 56 million per day in Q1 from 37 million per day in Q4.



34 million

McAfee GTI protections against malicious files decreased to 34 million in Q1 from 71 million per day in Q4 due to earlier malware detection and better local intelligence.



59 million

McAfee GTI protections against risky IP addresses saw a decrease to 59 million per day in Q1 from 88 million per day in Q4 due to earlier detection.

McAfee Labs Threats Report: June 2017

Visit www.mcafee.com/June2017ThreatsReport for the full report.