McAfee
Together is power.

McAfee Labs Threats Report

Cryptocurrency, Cortana und mehr
Track 2C – 11:45 Uhr

Rolf Haas | Enterprise Technology Specialist Data Protection & Cloud
CTO Ambassador EMEA

Speaker

Senior Enterprise Technology Specialist (ETS)
Cloud Security Platform and Data Protection
CTO Ambassador

Dipl.-Inform.(FH), S+, CISSP, CCSP

McAfee Germany GmbH

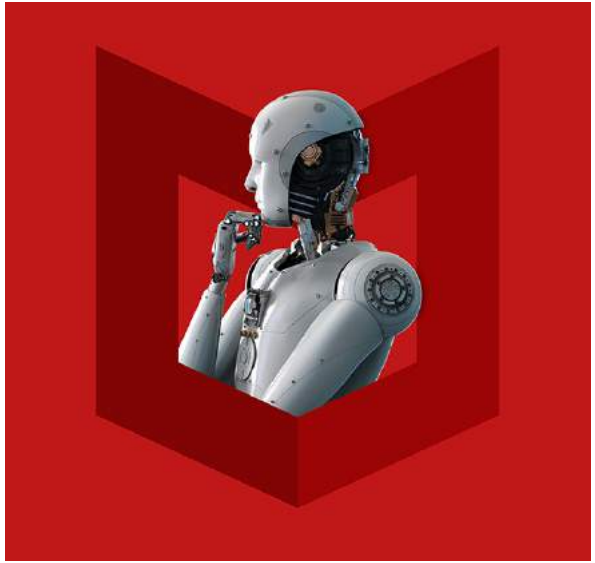
+18 years @McAfee

@rolfhaas

Agenda

Studerus Technology Forum – TEFO18 – Track2C

- Cryptocurrency & Mining Gefahren
- Hey Cortana!
- AsiaHitGroup Sneaks Billing-Fraud Appikationen
- Sicherheitsvorfälle Q2/18
- Statistiken Q2/18
- Fragen & Antworten



Recent Reports

Mining

for cryptocurrencies requires significant computing power and equipment can be expensive.

$5,000+

Cost of a dedicated mining machine.

Cybercriminals

employ malware to use a victim's computing power to mine for coins (without their permission) or to locate and steal the user's cryptocurrency.

$1.5B

Estimated stolen cryptocurrency in the past two years.

Infect and Collect

Extend operations in cryptocurrency mining surge

- Total coin miner malware grew 86% in Q2
  - Now 5.4 Mio, up from 2.9 Mio samples in Q1
- Category includes malware that infects systems to mine cryptocurrencies
  - Hijacking victim's systems or browsers to secretly create cryptocurrency coins, primarily Bitcoin
- Angles
  - Cryptocurrency as a cybercrime enabler
  - Evolution of cybercrime story

Evolution of Cybercrime in Cryptocurrency

Cybercriminals pursue cryptocurrency mining to minimize effort & risk

- Cybercriminals warm to the prospect of simply infecting users' systems and collecting payments without having to rely on third parties to monetize crimes
- First, data theft: theft, fraud schemes, or sale to fraudsters
- Second, ransomware: infects, extorts, cashes out via BTC or other coins
- Now, cryptocurrency mining: infects and collects – no middlemen risks

HaoBao Bitcoin-Stealing Campaign

Lazarus phishing campaigns steal bitcoin from financial sector and users

- Bitcoin-stealing phishing campaign HaoBao targets financial organizations and Bitcoin users
- Recipients open malicious email attachments, implant scans for Bitcoin activity, establishes implant for persistent data gathering and crypto mining
- Closely resembles Lazarus 2017 phishing campaigns, when attackers posed as recruiters
- Primary targets were defense contractors and financial institutions; object of campaigns was theft of sensitive military information or money
- Several attacks delivered documents via Dropbox revealed use of two implants—the first for data gathering and the second to establish persistence
- Typically embedded in older versions of Word docs, launched via Visual Basic macro; then sends data to control server

Blog: https://securingtomorrow.mcafee.com/mcafee-labs/lazarus-resurfaces-targets-global-banks-bitcoin-users/

Blockchain Threat Report

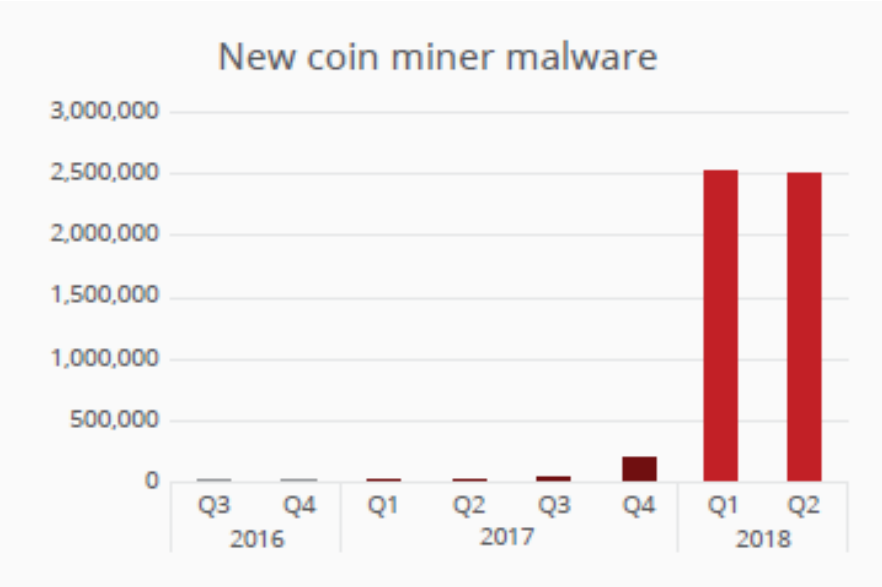
Blockchain, a Revolutionary Basis for Decentralized Online Transactions, Carries Security Risks

- Blockchain records transactions in a decentralized way, changing the way we look at money and offering a path to solve old business problems in new ways
- Blockchain enables cryptocurrencies Bitcoin and others
- Bad actors have already targeted many blockchain implementations using social engineering, malware, and exploits.
- Primary blockchain attack vectors
  - Phishing
  - Malware (examples: ransomware, miners, and cryptojacking)
  - Implementation vulnerabilities
  - Technology

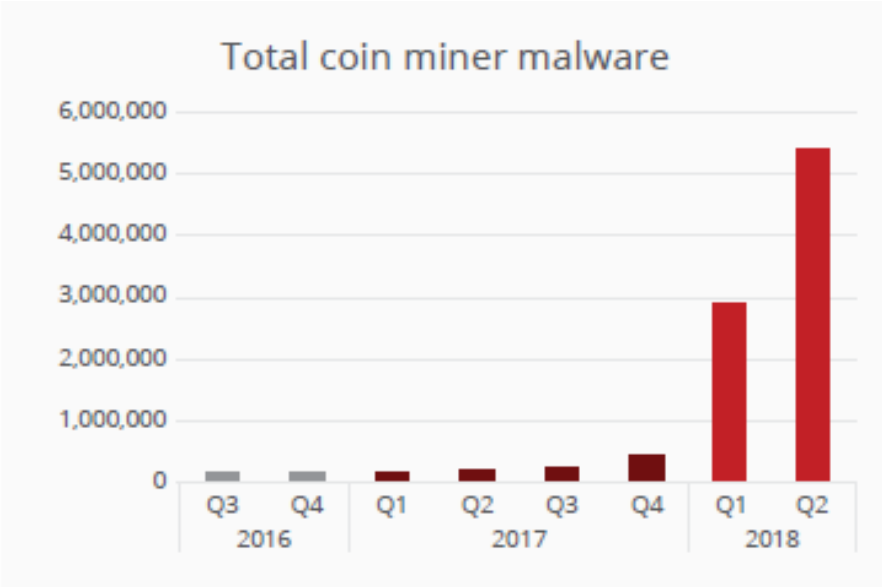
Report: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-blockchain-security-risks.pdf

Coin miner malware

Coin miner malware hijacks systems to create (“mine”) cryptocurrency without victims consent or awareness. Total coin miner threats jumped 86% in Q2.



Source: McAfee Labs, 2018.



Source: McAfee Labs, 2018.

Hey, Cortana!

Windows 10 voice assistant allowed an attacker to talk to a locked system and take control

- Advanced Threat Research team found a vulnerability in Windows 10 R3 and R4 that allowed a local attacker to take over a locked system
- “BadUSB” attacks inspired us to find and report to Microsoft several issues related to Cortana
- Typing while Cortana is listening opens the door
- Microsoft provided a patch in June after we told them of the problem earlier in the year. CVE-2018-8140

Blog: https://securingtomorrow.mcafee.com/mcafee-labs/want-to-break-into-a-locked-windows-10-device-ask-cortana-cve-2018-8140/

AsiaHitGroup Sneaks Billing-Fraud Apps Onto Google Play

Mobile Research team finds campaign of at least 15 apps in 2018

- AsiaHitGroup Gang has been active since at least late 2016 with the distribution of fake-installer applications
- Apps appear to work as advertised with ring tones (including “Despacito”), QR scanners, etc.
- Malware silently subscribes victims to a premium-rate service using WAP billing, which does not require sending SMS messages
- AsiaHitGroup Gang might have earned $60,500–$145,000 since January

- Google removed apps after we told them, but some quickly returned (and were again removed)

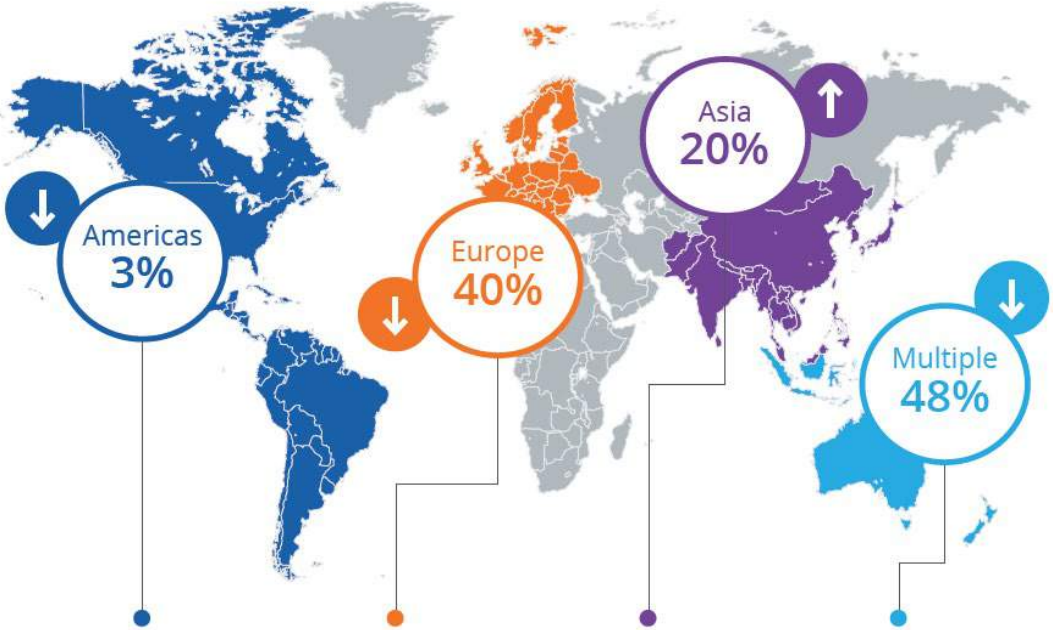
Blog: https://securingtomorrow.mcafee.com/mcafee-labs/asiahitgroup-gang-again-sneaks-billing-fraud-apps-onto-google-play/

Verticals and Vectors

McAfee counted 243 publicly disclosed security incidents in Q2, down from 313 in Q1

By Vertical and Vector

Reported Security Incidents



Americas

Disclosed incidents remained almost the same in Q2, down only .

Europe

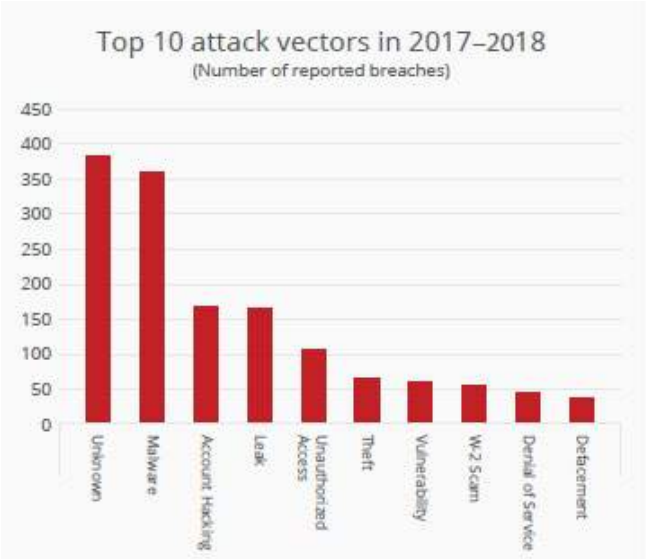
Disclosed incidents dropped significantly in Q2, falling by 40.

Asia

Disclosed incidents increased in Asia in Q2, up by 20%.

Multiple Regions

Disclosed incidents targeting multiple regions saw the biggest decline in Q2, dropping



Source: McAfee Labs, 2018.

Vertical Industry Incidents

Publicly reported security incidents by industry, over time

- **Multiples and Americas** Incidents in multiple sectors (54), targeting primarily the Americas (115) were the leading types of incidents
- **Public sector** 41 disclosed incidents in the public sector, up from 32 in Q1
  - Health Care was second, with 28 incidents
- **Cryptocurrency** Incidents of attacks on this sector rose by a factor of three
  - Complements increase in cryptojacking attacks
- **Finance** Disclosed incidents dropped by half

Threat Statistics

McAfee Labs saw on average five new threat samples every second in Q2 2018

Source: McAfee, 2017.

McAfee GTI received on average 49 billion queries per day in Q2.

86,000

McAfee GTI protections against **malicious files** reported **86,000 (0.1%) of them risky in Q2,** out of 86 million tested files.

268,000

McAfee GTI protections against **malicious IP addresses** reported **268,000 (0.4%) of them risky in Q2,** out of 67 million tested IP addresses.

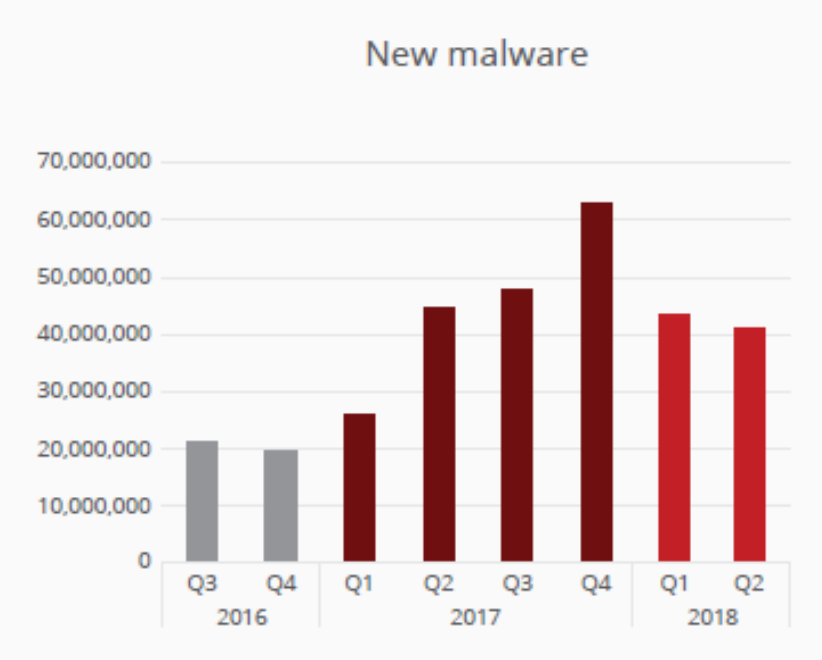
365,000

McAfee GTI protections against **malicious URLs** reported **365,000 (0.5%) of them risky in Q2,** out of 73 million tested URLs.

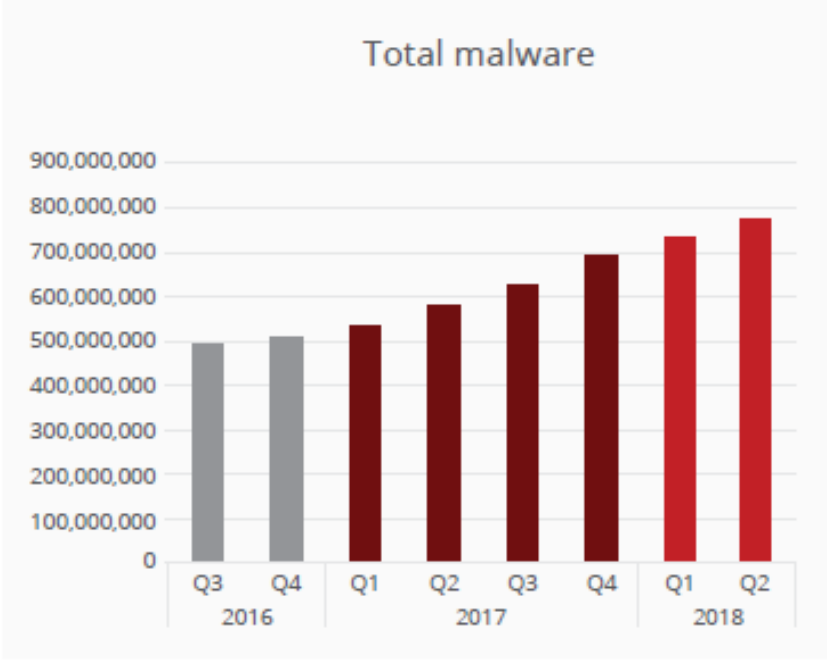
Malware

New malware samples were down in Q2 to about 41 million, a 5% decrease. The total number of malware samples grew 34% in the past four quarters to more than 774 million samples.

.



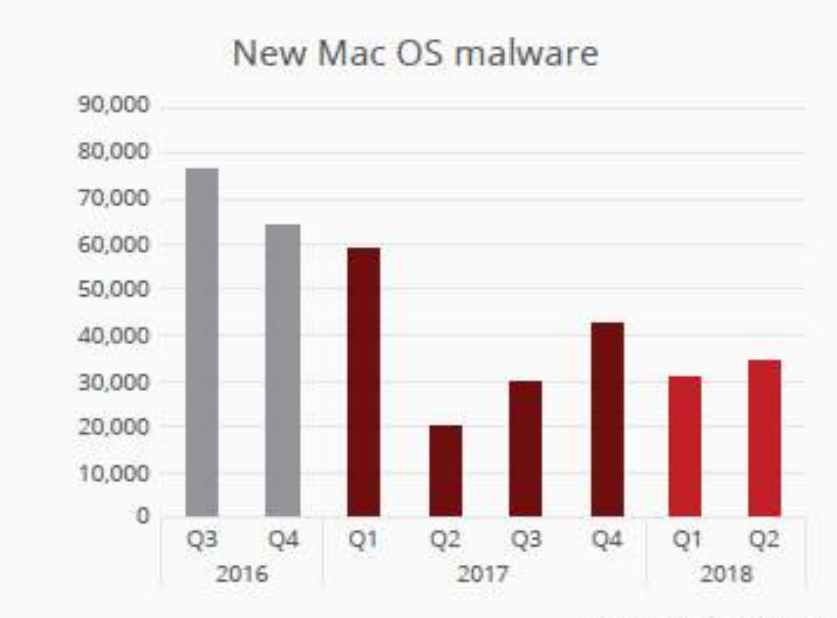
Source: McAfee Labs, 2018.

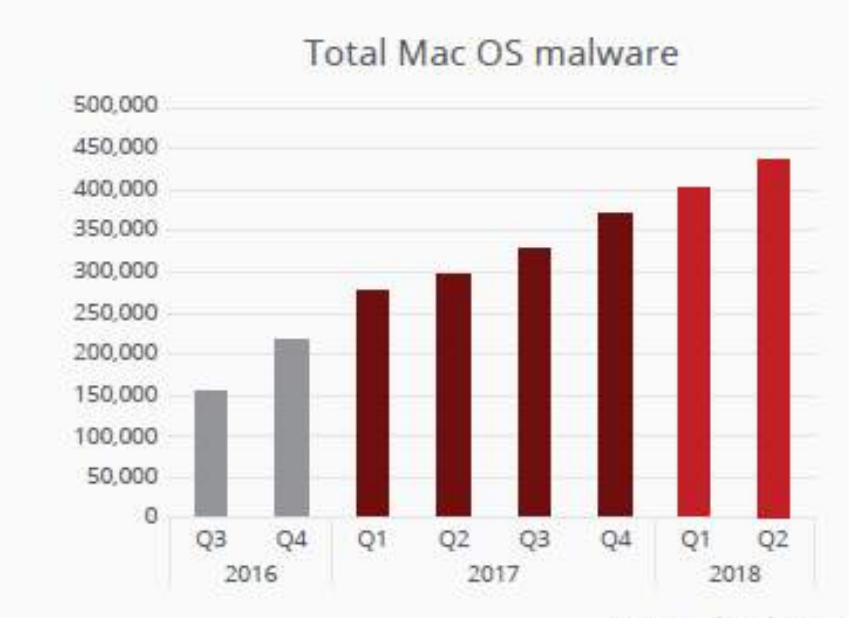


Source: McAfee Labs, 2018.

Mac OS malware

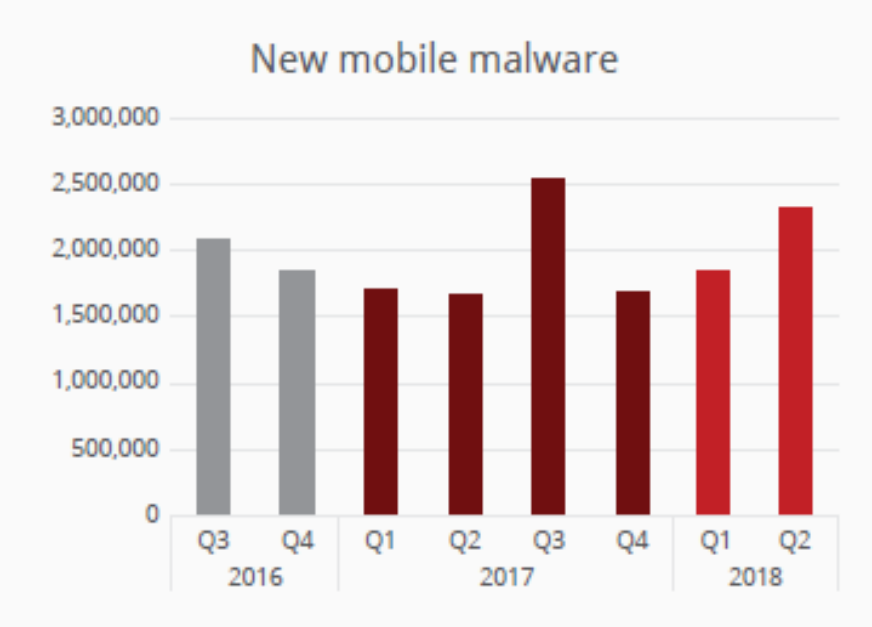
New Mac OS malware rose by 12% in Q2. Still small compared with Windows threats, the total number of Mac OS malware samples increased by 9%, to 435,000, in Q2.



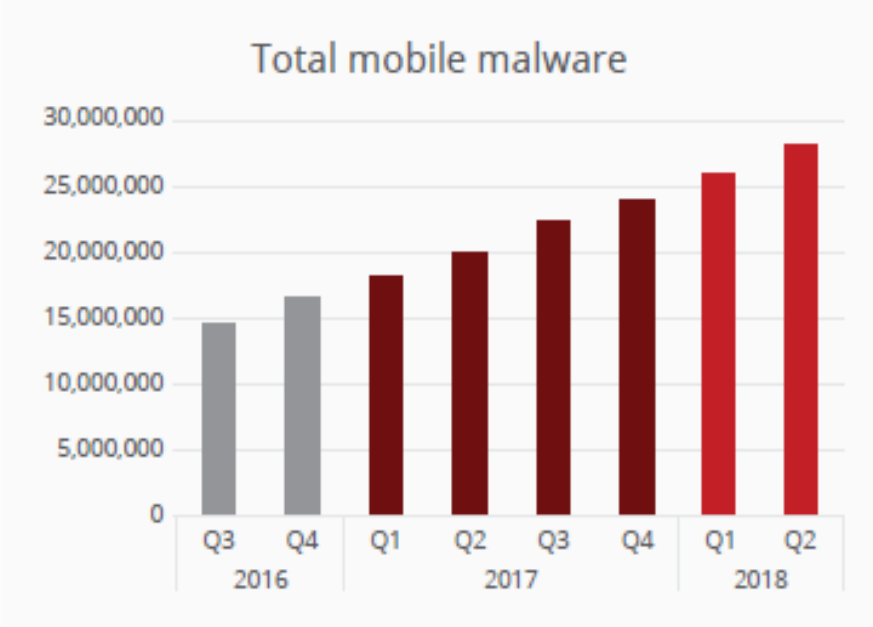


Mobile malware

Total known malware samples grew 42% in the past four quarters.



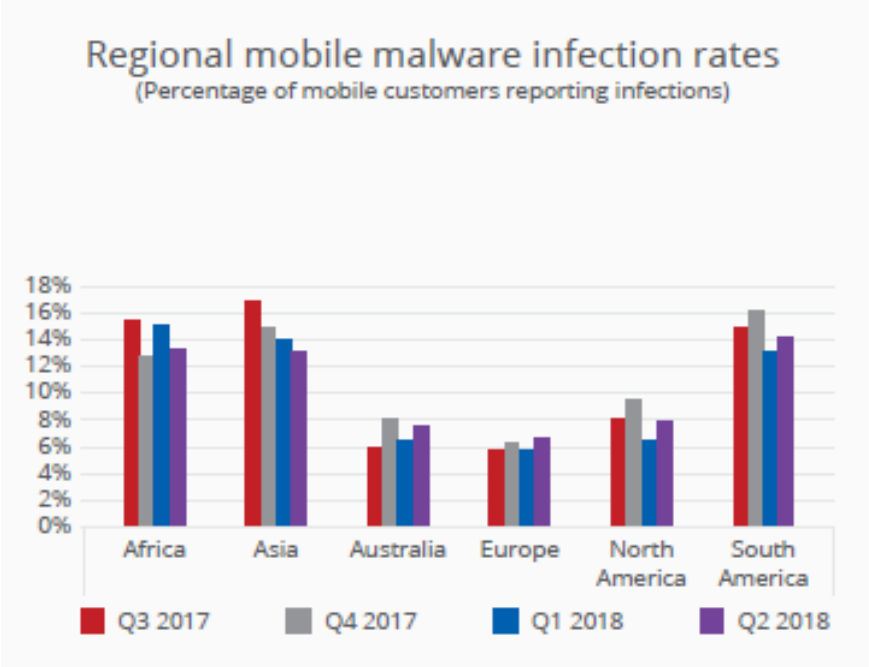
Source: McAfee Labs, 2018.



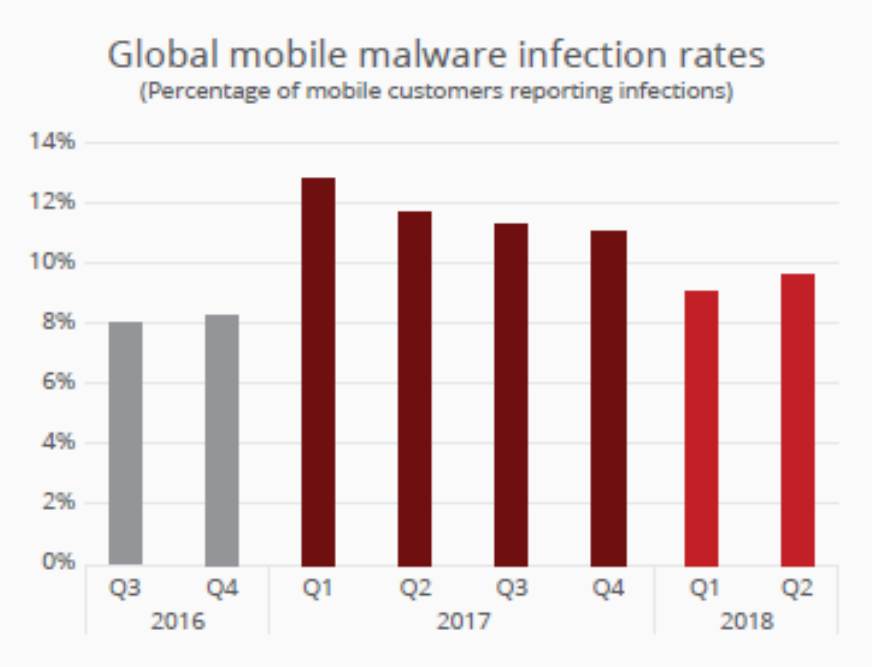
Source: McAfee Labs, 2018.

Mobile malware cont.

Global infections of mobile devices rose by 2%; South America reported the highest rate, at 14%



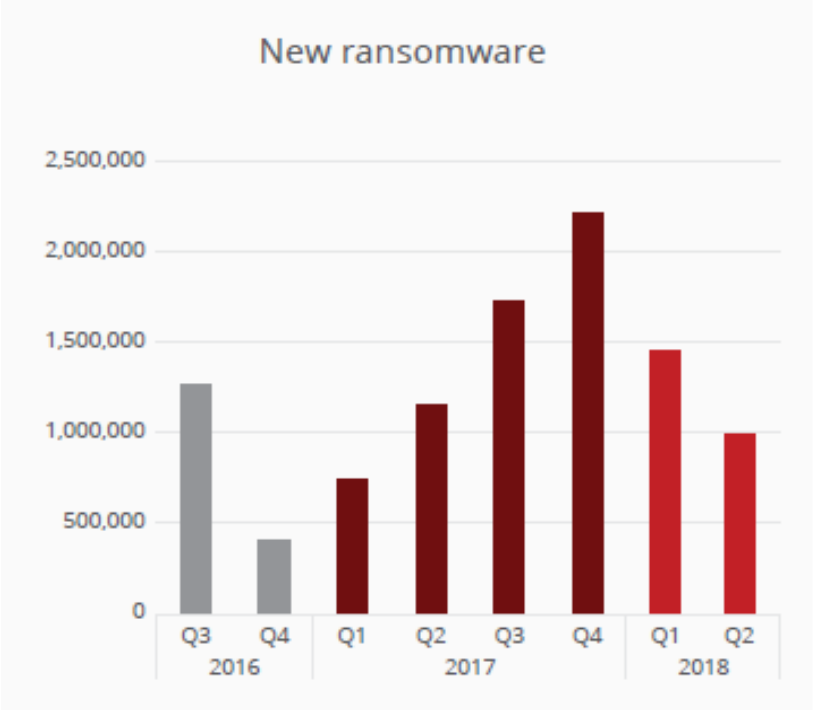
Source: McAfee Labs, 2018.



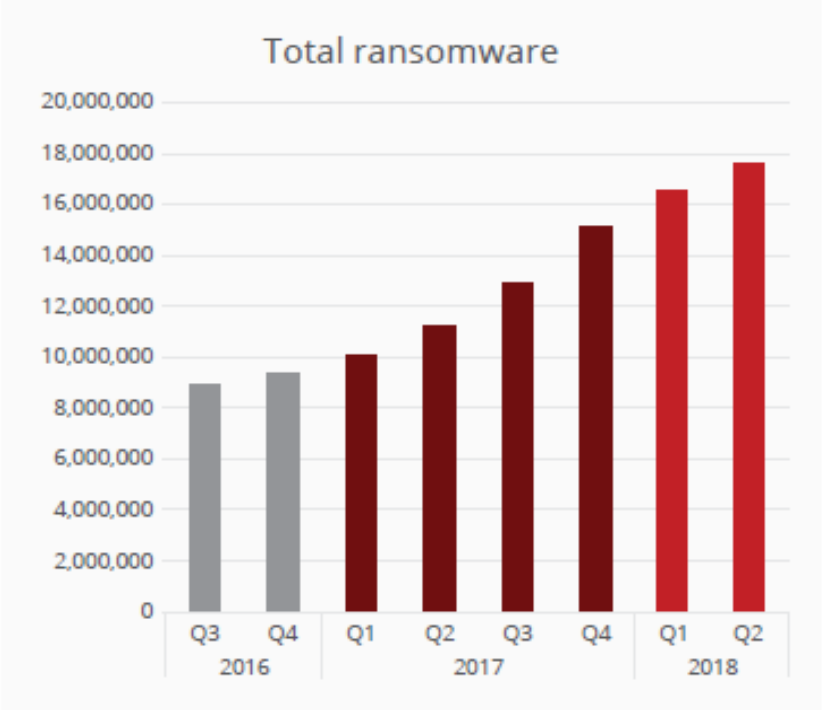
Source: McAfee Labs, 2018.

Ransomware

While growth in new ransomware slowed by 32% in Q2 2018, the total number of ransomware samples continues to grow, increasing 57% in the past four quarters to almost 18 million samples. One family that continued to grow was Scarab, which introduced a dozen variants in Q2, more than 50% of the total Scarab samples.



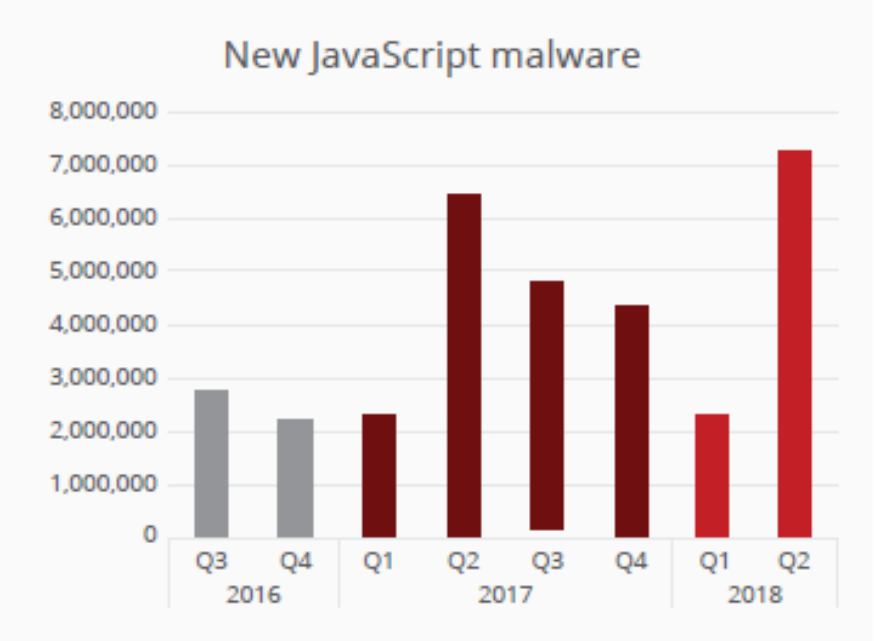
Source: McAfee Labs, 2018.



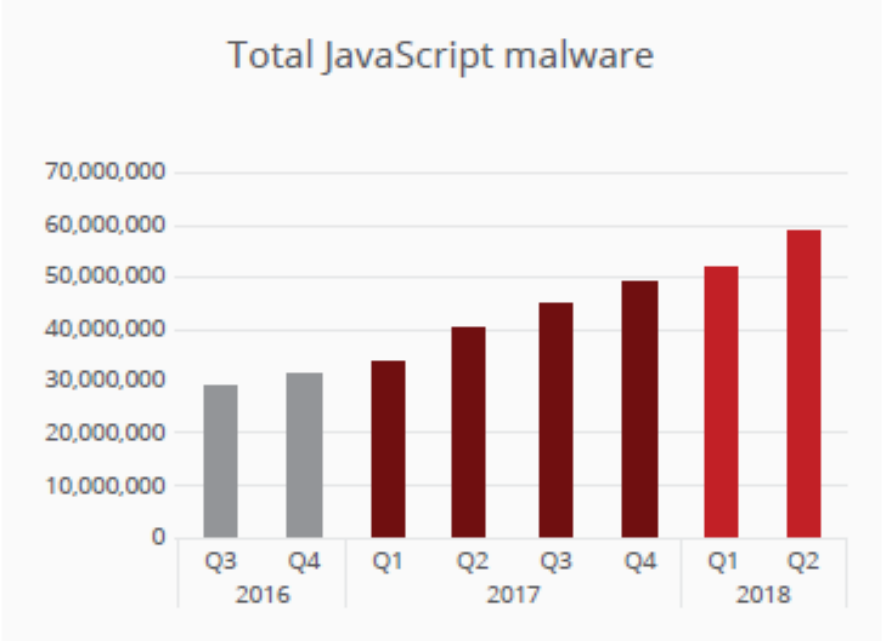
Source: McAfee Labs, 2018.

JavaScript malware

PowerShell malware has fallen to historic levels, but the far more popular JavaScript threats show no signs of slowing, increasing by 200% in Q2.



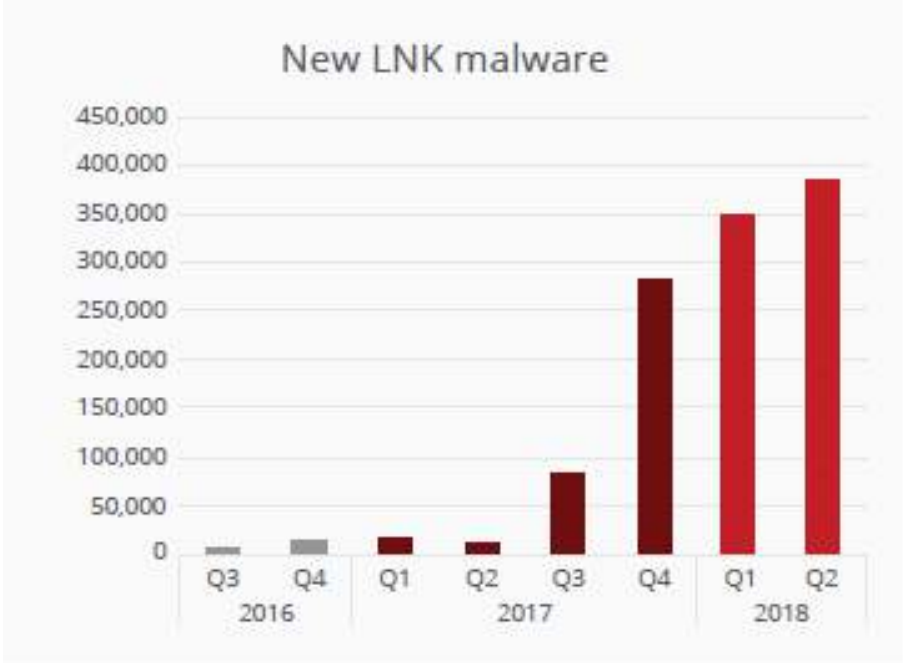
Source: McAfee Labs, 2018.



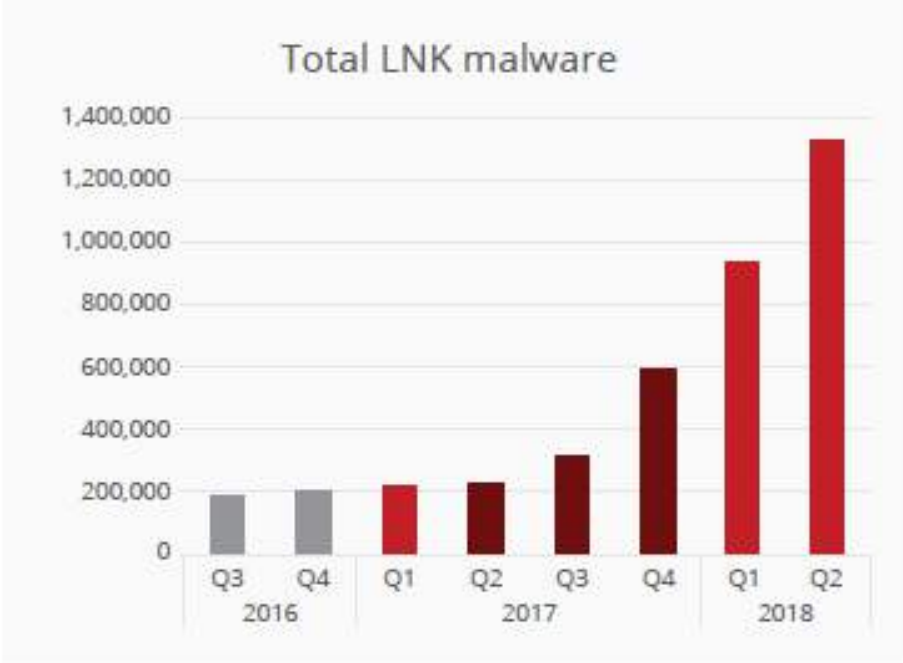
Source: McAfee Labs, 2018.

LNK malware

While PowerShell attacks slowed following their 2017 surge, cybercriminals are increasingly using .lnk shortcuts to surreptitiously deliver malicious PowerShell scripts and other malware. The total count of malware that exploits LNK capabilities rose 41% in Q2.



Source: McAfee Labs, 2018.



Source: McAfee Labs, 2018.

Fragen?