

Threats Report

McAfee Labs

September 2018

Cybercriminals Continue to Follow the Money

Cryptocurrencies remain a target for cybercriminals, with total coin miner malware nearly doubling in Q2.

\$232B↑

Size of Bitcoin Market¹



Mining

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



\$500-\$1,000

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

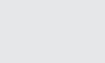
Estimated stolen cryptocurrency in the past two years.²

Check Your Bill on Google Play

The AsiaHitGroup Gang used several hijacked apps on Google Play—including a ringtone of the popular song "Despacito"—to steal money from unsuspecting victims.



User downloads hijacked app from Google Play.



App uses a silent background push notification to trigger a fake update dialog.



When victims start the fake "update," they are instead subscribed to a premium service.

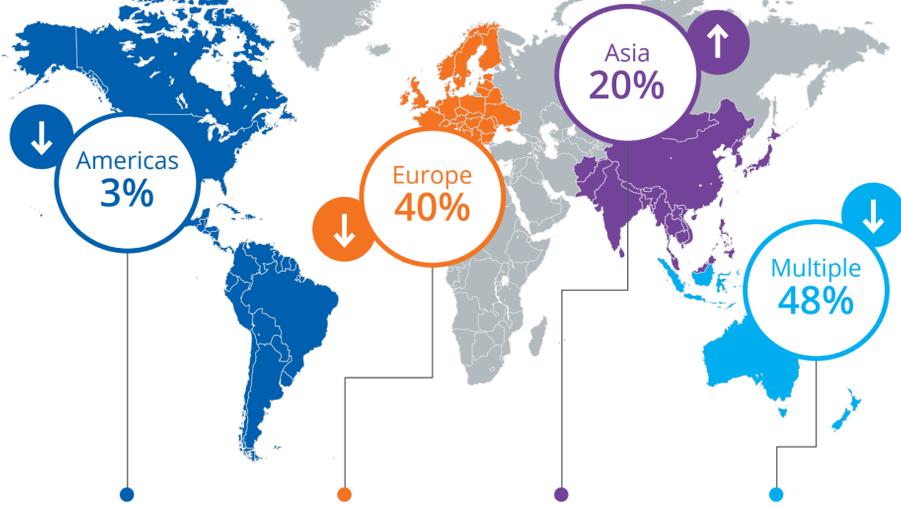


The subscription operates via WAP billing, which does not require sending SMS messages to premium-rate numbers.



Though current victims of this campaign are limited to Asia and Russia, toll fraud is a leading category of potentially harmful apps on Google Play.

Reported Incidents by Region



Americas

Disclosed incidents remained almost the same in Q2, down only 3%.

Europe

Disclosed incidents dropped significantly in Q2, falling by 40%.

Asia

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

Multiple Regions

Disclosed incidents targeting multiple regions saw the biggest decline in Q2, dropping 48%.

Threat Statistics



22% ↓

Incidents

We counted 243 publicly disclosed security incidents in Q2, a 22% decrease from Q1. Incidents involving the Americas (115) and those targeting Multiple Regions (54) were the leading types in Q2.



204% ↑

JavaScript malware

After decreasing significantly over the last 3 quarters, new JavaScript malware surged up 204% in Q2. More than 7 million new samples marks a record high, up from around 2 million in Q1.



5% ↓

Malware

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



27% ↑

Mobile malware

New mobile malware samples rose by 27% in Q2. McAfee customers in South America reported the highest rate of infection, at 14%. Total mobile malware grew 42% in the past four quarters to more than 28 million samples.



11% ↑

LNK malware

Although growth slowed to 11% in Q2, new LNK malware continues to climb. The total number of LNK malware samples has increased 489% over the past four quarters.



32% ↓

Ransomware

New ransomware samples continued to decrease in Q2, falling 32%. The total number of ransomware samples continues to grow, increasing 57% over the past four quarters to more than 17 million samples.

McAfee Global Threat Intelligence

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.

Read the full *McAfee Labs Threats Report: September 2018*. Download now www.mcafee.com/September2018ThreatsReport

1 "Cryptocurrency Market Capitalizations." CoinMarketCap, 2018. www.coinmarketcap.com/.
2 Stanley, Aaron. "U.S. Secret Service: Action Needed To Address Anonymous Cryptocurrencies." Forbes, Forbes Magazine, 20 June 2018. www.forbes.com/.

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2018 McAfee, LLC. 4117_0918 September 2018