Executive Summary

McAfee Threats Report: Second Quarter 2013

By McAfee® Labs

In the second quarter of 2013 the global cybercriminal community pursued four primary strategies to extract currency and confidential information from their victims. Their tactics included:

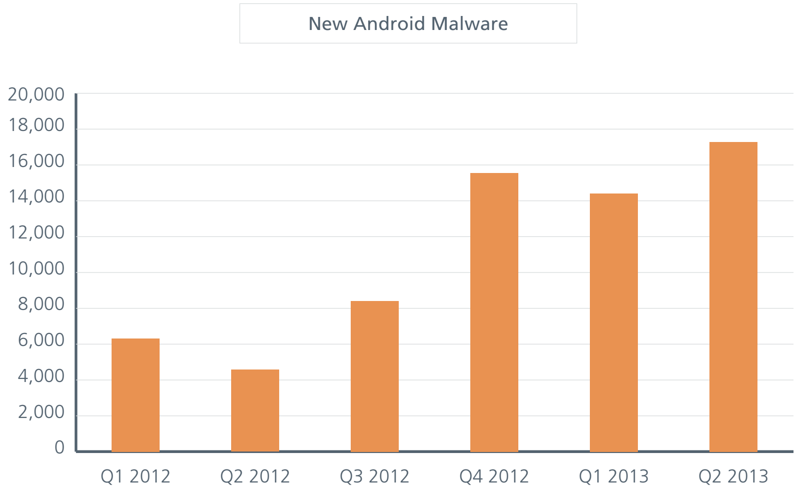
- Aggressive attacks on users of Android-based mobile devices.
- Significant expansion of malicious or infected websites to distribute malware.
- High-volume spam campaigns promoting bogus pharmaceutical drug offers.
- Extensive use of ransomware to extract currency from victims.

Each of these trends targets very different victims with distinct attack tactics, but each carries its own dangers for both individuals and enterprises. In addition to these attacks on consumers and enterprises, the cybercriminal and hacktivist communities also launched significant attacks on the Bitcoin infrastructure and a broad range of targets in the Middle East, reflecting the ongoing conflict in that region.

Mobile Attacks

After a relatively slow first quarter, McAfee Labs discovered that Android-based malware resumed the growth rate seen in 2012. This quarter nearly 18,000 new Android malware samples were cataloged. The newest Android-based threats fall into four broad categories:

- Banking malware that intercepts the SMS message containing the required token to log into one's bank account. In doing so, the cybercriminal gangs can directly access and empty victims' bank accounts. McAfee Labs researchers identified four significant pieces of malware that "forward" the required login token to cybercriminal gangs.
- Adult entertainment and dating apps that dupe users into signing up for paid dating services that, in fact, don't provide any services at all.
- Weaponized versions of legitimate apps that steal user data. A modified version of the KakaoTalk app collects sensitive user information (contacts, call logs, SMS messages, installed applications, and location) and uploads the data to the attacker's server.
- Fake app installers that actually install spyware to collect and deliver user data to cybercriminals.

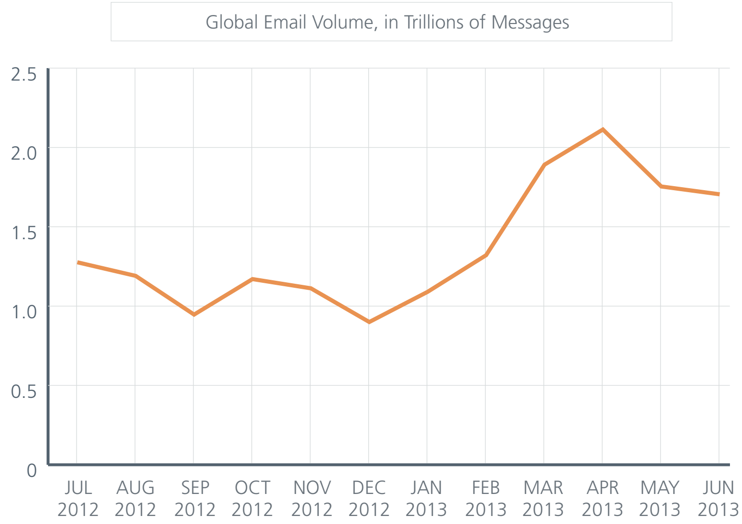


Suspicious Websites

McAfee Labs very carefully tracks suspicious websites on an hourly basis. This quarter Labs researchers observed a 16 percent increase in suspicious URLs, bringing the total to nearly 75 million. This increase shows just how important "infected" sites remain as a distribution mechanism for malware. It may also be indicative of the success the cybercriminal community is having in their attempts to infect and repurpose legitimate websites.

Volume Spam

After three years of declining volume, global spam campaigns appear to have staged a comeback. After a spike in the first quarter, global spammers continued their attacks this quarter, delivering more than 5.5 trillion spam messages representing approximately 70 percent of global email volume. As is common, however, spam volume varied significantly by region. Ukraine and Belarus, for example, each saw an increase of greater than 200 percent this period. Japan grew by 142 percent. Conversely, France fell by 25 percent, and the United States decreased by 16 percent.

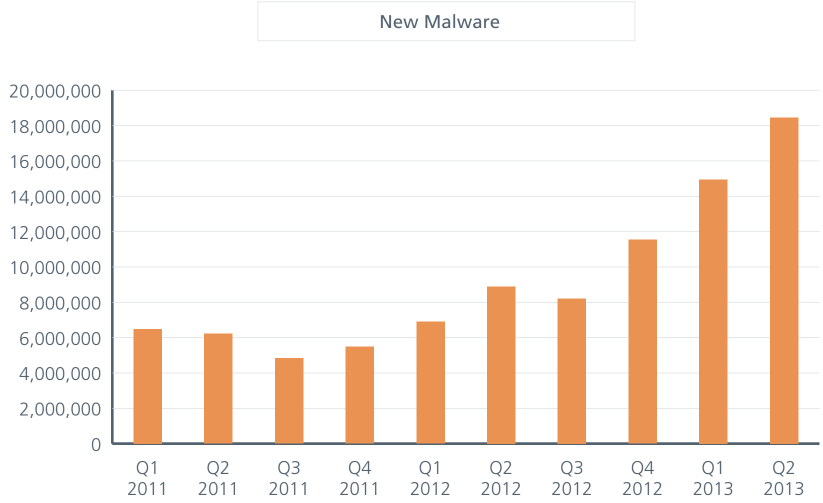


Ransomware

Ransomware is a serious Internet threat that continues to get worse. The number of new, unique samples this quarter is greater than 320,000, more than twice as many as in the first quarter of 2013. During the past two quarters McAfee Labs has catalogued more ransomware samples than in all previous periods combined. The primary reason for ransomware's growth is that it is a very efficient means for criminals to earn money because they use various anonymous payment services.

PC Malware Growth

While the cybercriminal community continues to turn its attention to mobile devices, there's been no reduction in the number of new attacks on traditional PC platforms. This quarter McAfee Labs cataloged 18.5 million new malware samples, bringing the total McAfee "zoo" to more than 147 million unique pieces of malware.



Other Trends

In addition to this quarter's top four trends, mentioned above, a number of other developments are worth noting:

- Continued attacks on financial services and media firms, now known as Operation Troy, in South Korea.
- A very sophisticated trend of attacks on the global Bitcoin infrastructure.
- Digitally "signed" malware samples increased 50 percent, to 1.2 million new samples. This trend will inevitably undermine confidence in the global certificate trust infrastructure.

Perhaps the most interesting of the commercial attacks this quarter was the spike in attacks on Bitcoin exchanges. At the end of February, Bitcoin (BTC) broke its historical peak trading value, at more than US$33 to 1 BTC. Some days later, the BitInstant exchange service was forced to shut down after attackers managed to extract more than US$12,000 in BTC.

In April, Tokyo-based Mt. Gox, the largest Bitcoin exchange service, was targeted by a number of distributed denial of service (DDoS) attacks that disrupted business. The first assault occurred around April 3; at that time the BTC exchange rate exceed US$140. On April 10, the value leaped to US$266 before closing at US$125 the next day. This keen interest resulted in 20,000 new accounts created each day.

The sudden activity in this market attracted the interest of cybercriminals of all kinds. They engaged in further DDoS actions against Mt. Gox. Silk Road, the underground marketplace using Bitcoin as e-money, was taken down several times by DDoS attacks. It's clear that Bitcoin exchanges will continue to be targeted by the cybercriminal community as long as they believe they can extract value directly by hacking them or by holding them hostage to further DDoS attacks.

A copy of the full report can be found here: http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2013.pdf.

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com