MCAFEE LABS SEES NEW THREATS SUBVERTING DIGITAL SIGNATURE VALIDATION

Third Quarter Threats Report Identifies Android Malware That Bypasses App Validation as Signed PC Malware Continues to Surge; Bitcoin Popular in Illicit Trade and Cybercrime

SYDNEY, Australia. – Nov. 21, 2013 – McAfee Labs today released the McAfee Labs Threats Report: Third Quarter 2013, which found new efforts to circumvent digital signature app validation on both PCs and Android-based devices. The McAfee Labs team identified a new family of mobile malware that allows an attacker to bypass the digital signature validation of apps on Android devices, which contributed to a 30 per cent increase in Android-based malware. At the same time, traditional malware signed with digital signatures grew by 50 per cent to more than 1.5 million samples. Less surprising but no less daunting was a 125 per cent increase in spam.

"The efforts to bypass code validation on mobile devices, and commandeer it altogether on PCs, both represent attempts to circumvent trust mechanisms upon which our digital ecosystems rely," said Sean Duca, Enterprise Solutions Architect, McAfee ANZ. "The industry must work harder to ensure the integrity of this digital trust infrastructure given these technologies are becoming even more pervasive in every aspect of our daily lives."

The third quarter also saw notable events in the use of Bitcoin for illicit activities such as the purchase of drugs, weapons, and other illegal goods on websites such as Silk Road. The growing presence of Bitcoin-mining malware reinforced the increasing popularity of the currency.

Duca continued: "As these currencies become further integrated into our global financial system, their safety and stability will require initiatives leveraging both the financial system's monetary controls and oversight and the technical controls and defences our industry provides."

Leveraging data from the McAfee Global Threat Intelligence (GTI) network, the McAfee Labs team identified the following trends in Q3 2013:

· Digitally signed malware. Digitally signed malware samples increased 50 per cent, to more than 1.5 million new samples. McAfee Labs also revealed the top 50 certificates used to sign malicious payloads. This growing threat calls into question the validity of digital certificates as a trust mechanism.

· New mobile malware families. McAfee Labs researchers identified one entirely new family of Android malware, Exploit/MasterKey.A, which allows an attacker to bypass the digital signature validation of apps, a key component of the Android security process. McAfee Labs researchers also found a new class of Android malware that once installed downloads a second-stage payload without the user's knowledge.

· Virtual currencies. Use of new digital currencies by cybercriminals to both execute illegal transactions and launder profits is enabling new and previously unseen levels of criminal activity. These transactions can be executed anonymously, drawing the interest of the cybercriminal community and allowing them to offer illicit goods and services for sale in transactions that would normally be transparent to law enforcement. McAfee Labs also saw cybercriminals develop Bitcoin-mining malware to infect systems, mine their processing power, and produce Bitcoins for commercial transactions. For more information, please read the McAfee Labs report "Virtual Laundry: An Analysis of Online Currencies, and Their Use in Cybercrime."

· Android malware. Nearly 700,000 new Android malware samples appeared during the third quarter, as attacks on the mobile operating system increased by more than 30 per cent. Despite responsible new security measures by Google, McAfee Labs believes the largest mobile platform will continue to draw the most attention from hackers given it possesses the largest base of potential victims.

· Spike in spam. Global spam volume increased 125 per cent in the third quarter of 2013. McAfee Labs researchers believe much of this spike was driven by legitimate "affiliate" marketing firms purchasing and using mailing lists sourced from less than reputable sources.

Each quarter, the McAfee Labs team of 500 multidisciplinary researchers in 30 countries follows the complete range of threats in real time, identifying application vulnerabilities, analysing and correlating risks, and enabling instant remediation to protect enterprises and the public. To read the full McAfee Labs Threats Report: Third Quarter 2013, please visit: http://mcaf.ee/s4xfb.

About McAfee Labs

McAfee Labs is the world's leading source for threat research, threat intelligence, and cyber security thought leadership. The McAfee Labs team of 500 threat researchers correlates real-world data collected from millions of sensors across key threat vectors—file, web, message, and network—and delivers threat intelligence in real-time to increase protection and reduce risk.

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), empowers businesses, the public sector, and home users to safely

experience the benefits of the Internet. The company delivers proactive and proven security solutions and services for systems, networks, and mobile devices around the world. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence network, McAfee is relentlessly focused on keeping its customers safe. http://www.au.mcafee.com

###