McAfee Labs report sees mobile malware target trust in early 2014

Cybercriminals Exploit Flappy Bird Game's Popularity, other Trusted App and Service Vulnerabilities

Sydney, Australia – Tuesday, 24 June, 2014 – McAfee Labs today released the McAfee Labs Threats Report: June 2014, revealing mobile malware tactics that abuse the popularity, features, and vulnerabilities of legitimate apps and services, including malware-infested clones masquerading as the popular mobile game Flappy Birds. The report highlights the need for mobile app developers to be more vigilant about the security of their apps, and encourages users to be mindful when granting permission requests that criminals could exploit for profit.

The manipulation of legitimate mobile apps and services played a key role in the expansion of mobile malware at the beginning of 2014. McAfee Labs found that 79 per cent of sampled clones of the Flappy Birds game contained malware. Through these clones, perpetrators were able to make phone calls without user permission, install additional apps, extract contact list data, track geo-location, and establish root access for uninhibited control over anything on the device, including the recording, sending, and receiving of SMS messages.

Beyond app reputation, McAfee Labs saw notable examples of mobile malware that take advantage of the features of trusted apps and services, including:

· Android/BadInst.A: This malicious mobile app abuses app store account authentication and authorisation to automatically download, install, and launch other apps without user permission

· Android/Waller.A: This Trojan exploits a flaw in a legitimate digital wallet service to commandeer its money-transfer protocol and transfer money to the attacker's servers

· Android/Balloonpopper.A: this Trojan exploits an encryption method weakness in the popular messaging app WhatsApp, allowing attackers to intercept and share conversations and photos without users' permission

"We tend to trust the names we know on the internet and risk compromising our safety if it means gaining what we most desire," said Vincent Weafer, senior vice president for McAfee Labs. "The year 2014 has already given us ample evidence that mobile malware developers are playing on these inclinations, to manipulate the familiar, legitimate features in the mobile apps and services we recognise and trust. Developers must become more vigilant with the controls they build into these apps, and users must be more mindful of what permissions they grant."

Each quarter, the McAfee Labs team of 450 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.

Additional Key Findings

· Mobile on the move: McAfee Labs' "zoo" of mobile malware samples grew by 167 percent between Q1 2013 and Q1 2014

· Suspicious URLs:New suspect URLs set a three-month record with more than 18 million, a 19 percent increase over Q4 2013 and the fourth straight quarterly increase

· Signed malware: New malicious signed binaries remain a popular form of attack, increasing by 46 percent in the first quarter of 2014

· Master boot record malware: New threats attacking the master boot record increased by 49 percent in the first quarter, reaching an all-time high for a single quarter

· Ransomware in repose: Ransomware sample counts have dropped for three straight quarters

· Botnets and currency mining: McAfee Labs saw botnet providers include virtual currency mining capabilities with their services, reflecting the increasing popularity of digital currencies such as Bitcoin

To read the full McAfee Labs Threats Report: June 2014, please visit: http://mcaf.ee/5q3wh

About McAfee Labs

McAfee Labs is the world's leading source for threat research, threat intelligence, and cybersecurity thought leadership. The McAfee Labs team of 450 researchers collects threat data from millions of sensors across key threat vectors—file, web, message, and network. It then performs cross-vector threat correlation analysis and delivers real-time threat intelligence to tightly integrated McAfee endpoint and network security products through its cloud-based McAfee Global Threat Intelligence service. McAfee Labs also develops core threat detection technologies—such as McAfee DeepSAFE technology, application profiling, and graylist management—that are incorporated into the broadest security product portfolio in the industry. http://www.mcafee.com/us/mcafee-labs.aspx

- ENDS -

About McAfee

McAfee, part of Intel Security and 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.mcafee.com

Contacts

Jesse Lewis
02 8303 6464
mailto: jesse@zing.net.au