

McAfee Threats Report Shows Global Expansion of Cybercrime

Wednesday, November 14, 2012 01:00:00 PM (GMT)

Report Reveals Further Details of "Operation High Roller," Explores Evolution of Ransomware, Shows Malware Topping 100 Million Samples, and Finds Database Breaches at All-Time High

McAfee today released the [McAfee Threats Report: Third Quarter 2012](#), which explores techniques in cybercrime as well as the global evolution of cyber exploits. The latest report uncovers new details of "Operation High Roller," tracks that mobile malware almost doubled the previous quarter's total, and reveals an all-time high in database breaches. McAfee Labs also saw jumps in some categories of malware, including ransomware and signed binaries. Rootkits and Mac malware continue to rise, while password-stealing Trojans and AutoRun malware also trended strongly upward.

"Cybercrime exhibits few signs of slowing down," said Vincent Weafer, senior vice president of McAfee Labs. "Though we tend to highlight the numbers, the fact is that we continue to see increased sophistication of attacks. Cybercrime, hacktivism, and cyberwarfare are in a continual state of evolution. Everyone from governments to large enterprises, small business and home users are facing a wider range of digital threats from these forces, as they gain more actionable intelligence on their victims, and leverage the newest attack platforms and exploits tools to launch their campaigns. We all need to equip ourselves with basic situation awareness to our online risks and how best to prevent and combat these threats."

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, analyzing and correlating risks, and enabling instant remediation to protect enterprises and the public. This quarter, McAfee Labs identified the following trends:

- **Financial Fraud Ring Extends Worldwide Reach:** Online financial fraud attacks have spread worldwide in Q3. New research indicates that Operation High Roller, a financial fraud ring identified earlier this year by McAfee Labs and Guardian Analytics, has now spread outside Europe, including to the United States and Colombia. Cybercriminals set up an automated transfer system (ATS) that was used to attack European financial institutions, and set out to target a major U.S. multinational financial institution.
- **Ransomware Continues to Evolve:** In Q3, the number of unique samples of ransomware, which extorts money from its victims, grew by another 43 percent, making it one of the fastest-growing areas of cybercrime. Devices are infected via links in email and social networks, drive-by downloads, and pay-per-install methods. Most malware typically accuses the user of visiting illegal websites, locks the computer, and then demands a payment to unlock the device. Although victims can pay, they are not guaranteed complete system restores.
- **Malware "Zoo" Tops 100 Million:** While growth in malware slowed slightly this quarter, the overall number in the malware "zoo" still topped 100 million samples, as predicted. Mobile malware almost doubled the previous quarter's total, while the Android platform remains the largest target. McAfee Labs now sees an average of 100,000 new malware samples per day. Since January, signed malware has doubled, which has implications for global trust infrastructure.
- **Database Breaches at an All-Time High:** The total number of data breaches in 2012 has already surpassed the figure for the entire 2011 calendar year; this year, close to 100 new database-related vulnerabilities have been disclosed or silently patched by developers.
- **Stealth Malware Shows Steady Growth:** Showing steady growth in Q3, this type of stealth malware is known as one of the "nastiest" classifications because they are designed to evade detection.
- **Web Threats Increase 20 percent:** Among web and messaging threats, we saw a 20 percent increase this quarter in suspicious URLs, with a vast number of these URLs hosting malware. Almost 64 percent of these newly discovered suspect URLs are mainly located in North America.

To learn more about the rise in malware in the full copy of the McAfee Threats Report, Third Quarter 2012, please visit <http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2012.pdf>.

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.mcafee.com>

Note: McAfee is a trademark or registered trademark of McAfee, Inc. in the United States and other countries. Other names and brands may be claimed as the property of others.

--30-- JR/SF

Contact:

McAfee

Ian Bain, 408-346-3877

ian_bain@mcafee.com

or

Zeno Group

Stephanie Chaney, 312-222-1758

Stephanie.chaney@zenogroup.com

Copyright Business Wire 2012

1.2

Industries: Consumer Electronics, Internet, Mobile/Wireless, Networks, Security, Software, Technology

Languages: English

Primary Identifiers: 002WNN-E, INTC-US

Related Identifiers: MFE-US, INTC, US458140100

Source: McAfee

Subjects: Product/Service, Survey