MCAFEE LABS REPORT HIGHLIGHTS SUCCESS OF PHISHING ATTACKS WITH 80 PERCENT OF BUSINESS USERS UNABLE TO DETECT SCAMS

Results Show Finance and HR Departments, Which Hold Sensitive Corporate Data, Performed Worst

Sydney, Australia – Thursday 4th September, 2014 – McAfee Labs today released the McAfee Labs Threats Report: August 2014, revealing that phishing continues to be an effective tactic for infiltrating enterprise networks. Testing business users' ability to detect online scams, the McAfee Phishing Quiz uncovered that 80% of its participants failed to detect at least one of seven phishing emails. Furthermore, results showed that finance and HR departments, those holding some of the most sensitive corporate data, performed the worst at detecting scams, falling behind by a margin of 4% to 9%. In Australia, the most skilled performers in the quiz were executives and IT professionals. Three quarters of Australian business users fell for at least one of the seven phishing emails.

Since last quarter's Threats Report, McAfee Labs has collected more than 250,000 new phishing URLs, leading to a total of nearly one million new sites in the past year. Not only was there an increase in total volume, there was a significant rise in the sophistication of phishing attacks occurring in the wild. Results showed both mass campaign phishing and spear phishing are still rampant in the attack strategies used by cybercriminals around the world. The study revealed Australia as having 1,709 URL domains containing phishing links, the highest in Asia Pacific, ranked ninth globally.

"One of the great challenges we face today is upgrading the Internet's core technologies to better suit the volume and sensitivity of traffic it now bears," said Vincent Weafer, senior vice president for McAfee Labs. "Every aspect of the trust chain has been broken in the last few years—from passwords to OpenSSL public key encryption and most recently USB security. The infrastructure that we so heavily rely on depends on technology that hasn't kept pace with change and no longer meets today's demands."

Findings also revealed new cybercrime opportunities since the public disclosure of the Heartbleed vulnerability, as stolen data from still vulnerable websites is currently being sold on the black market. Lists of unpatched websites have quickly become hit lists for cybercriminals and tools are readily available to mine unpatched sites. With these tools, it is possible to tie together an automated system that targets known vulnerable machines and extracts sensitive information.

Each quarter, the McAfee Labs team of more than 400 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

Operation Tovar: McAfee joined global law enforcement agencies and others to take down Gameover Zeus and CryptoLocker by blocking more than 125,000 CryptoLocker domains and sinkholing in excess of 120,000 Gameover Zeus domains. However, copycats are on the rise, creating new variants of ransomware or financial-targeting malware using the leaked Zeus source code.

Growth in Malware: New malware samples rose by only 1% in the second quarter. However, with more than 31 million new samples, this was still the largest amount recorded in a single quarter. The total count of mobile malware increased by 17% in the second quarter, while the rate of new malware appears to have leveled off at about 700,000 per quarter.

Network Threats: Denial of service attacks rose by 4% in the second quarter and remain the most prevalent type of network threat. To read the full McAfee Labs Threats Report: August 2014 with a complete list of findings, please visit: http://mcaf.ee/uycbt

About McAfee Labs

McAfee Labs is one of the world's leading sources for threat research, threat intelligence, and cybersecurity thought leadership. The McAfee Labs team of more than 400 researchers collects threat data from millions of sensors across key threat vectors—file, web, message, and network. The team then performs cross-vector threat correlation analysis and delivers real-time threat intelligence to tightly integrated McAfee endpoint, content, 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

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

- 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