FORTINET

October 8, 2012

Fortinet Threat Landscape Research Reports a Surge in Android Adware, an Evolution to Zitmo Mobile Banking Trojan and Large Scale Scans for Web Vulnerability

SUNNYVALE, CA -- (Marketwire) -- 10/08/12 -- Fortinet® (NASDAQ: FTNT) -- a world leader in high-performance network security -- today released its threat landscape research. During the period beginning July 1, 2012 and ending September 30, 2012, FortiGuard Labs researchers reported a marked increase in Android adware, new evidence suggesting that Zitmo (Zeus-in-the-Mobile) mobile banking Trojan is evolving into a botnet and the detection of Romanian hackers performing large scale scanning for Web vulnerabilities.

Android Adware on the Rise
In the last three months, FortiGuard Labs reported a surge in Android-based mobile adware with a volume of activity comparable to Netsky.PP, one of the most infamous and prolific spam generators encountered in Internet history. Two adware variants Android/NewyearL and Android/Plankton were detected by close to one percent of all FortiGuard monitoring systems in the APAC and EMEA regions and four percent in the Americas. These two adware variants cover various applications that embed a common toolset for unwanted advertisements displayed on the mobile's status bar, user tracking through their International Mobile Equipment Identity (IMEI) number and dropping of icons on the device's desktop.

"The surge in Android adware can most likely be attributed to users installing on their mobile devices legitimate applications that contain the embedded adware code. It suggests that someone or some group is making money, most likely from rogue advertising affiliate programs," said Guillaume Lovet, senior manager of Fortinet's FortiGuard Labs Threat Response Team.

These types of applications require too many unnecessary rights for a normal application, indicating it has a hidden agenda. Such data request includes permission to access parts of the device that are irrelevant to the application, to get access to the device's browser history, bookmarks contact data, phone logs and identity as well as system log files.

For best practices, FortiGuard Labs recommends paying close attention to the rights asked by the application at the point of installation. More generally, it is also recommended to download mobile applications that have been highly rated and reviewed.

Zitmo Gets More Sophisticated
In the last quarter, FortiGuard researchers discovered that Zitmo (or Zeus-in-the-mobile) has evolved into a more complex threat, with new versions recently released for Android and BlackBerry.

Zitmo is the notorious mobile component of the Zeus banking Trojan that circumvents two-factor authentication by intercepting SMS confirmation codes to access bank accounts. The new versions for Android and BlackBerry have now added botnet-like features, such as enabling cybercriminals to control the Trojan via SMS commands.

"The new version of Zitmo may already be in the wild in Europe and Asia. While we're detecting only a few instances of the malware in those regions, it's leading us to believe the code is currently being tested by its authors or deployed for very specific, targeted attacks," Lovet continued.

As more banks and online merchants roll out two-factor authentication -- usually through the use of an SMS code to bring the second authentication factor and confirm a transaction -- Android and BlackBerry users should be mindful anytime their financial institution asks them to install software onto their computing device, as this is something banks rarely if ever request from their customers. For complete security, FortiGuard Labs recommends conducting online banking from the original operating system CD. If that is not an option, users should install an antivirus client on their phone and desktop PCs and make sure they are updated with the latest patches.

Romanian Hackers Scanning for phpMyAdmin Vulnerability
In the last three months, FortiGuard Labs has detected large scale scans for vulnerability. These scans were performed through a tool developed by Romanian Hackers to seek Web servers running vulnerable versions of the mySQL administration software (phpMyAdmin) in order to take control of those servers.

The tool, called ZmEu, contains code strings in the payload that refers to AntiSec, the global hacking movement initiated by Anonymous and Lulzsec last year. The scans are being performed around the world, and in September, almost 25 percent of FortiGuard monitoring systems were detecting at least one such scan per day.

"The goal behind an attack on this vulnerability is open to speculation," added Lovet. "But if these hackers are indeed related to AntiSec, possible scenarios include exfiltering sensitive data, using the compromised servers as a direct denial of service

(DDoS) launch base or defacing the Websites they've infiltrated."

To secure Web servers against this threat, Fortinet recommends updating to the latest version of PhPMyAdmin.

About FortiGuard Labs
FortiGuard Labs compiled threat statistics and trends for this threat period based on data collected from FortiGate® network security appliances and intelligence systems in production worldwide. Customers who use Fortinet's FortiGuard Services should be protected against the vulnerabilities outlined in this report as long as the appropriate configuration parameters are in place.

FortiGuard Services offer broad security solutions including antivirus, intrusion prevention, Web content filtering and anti-spam capabilities. These services help protect against threats on both application and network layers. FortiGuard Services are updated by FortiGuard Labs, which enables Fortinet to deliver a combination of multi-layered security intelligence and zero-day protection from new and emerging threats. For customers with a subscription to FortiGuard, these updates are delivered to all FortiGate, FortiMail™ and FortiClient ™ products.

Ongoing research can be found in the FortiGuard Center or via FortiGuard Labs' RSS feed. Additional discussion on security technologies and threat analysis can be found at the FortiGuard Blog.

About Fortinet (www.fortinet.com)
Fortinet (NASDAQ: FTNT) is a worldwide provider of network security appliances and a market leader in unified threat management (UTM). Our products and subscription services provide broad, integrated and high-performance protection against dynamic security threats while simplifying the IT security infrastructure. Our customers include enterprises, service providers and government entities worldwide, including the majority of the 2011 Fortune Global 100. Fortinet's flagship FortiGate product delivers ASIC-accelerated performance and integrates multiple layers of security designed to help protect against application and network threats. Fortinet's broad product line goes beyond UTM to help secure the extended enterprise -- from endpoints, to the perimeter and the core, including databases and applications. Fortinet is headquartered in Sunnyvale, Calif., with offices around the world.

Copyright © 2012 Fortinet, Inc. All rights reserved. The symbols ® and ™ denote respectively federally registered trademarks and unregistered trademarks of Fortinet, Inc., its subsidiaries and affiliates. Fortinet's trademarks include, but are not limited to, the following: Fortinet, FortiGate, FortiGuard, FortiManager, FortiMail, FortiClient, FortiCare, FortiAnalyzer, FortiReporter, FortiOS, FortiASIC, FortiWiFi, FortiSwitch, FortiVoIP, FortiBIOS, FortiLog, FortiResponse, FortiCarrier, FortiScan, FortiAP, FortiDB and FortiWeb. Other trademarks belong to their respective owners. Fortinet has not independently verified statements or certifications herein attributed to third parties, and Fortinet does not independently endorse such statements. Notwithstanding anything to the contrary herein, nothing herein constitutes a warranty, guarantee, binding specification or other binding commitment by Fortinet, and performance and other specification information herein may be unique to certain environments. This news release may contain forward-looking statements that involve uncertainties and assumptions. Changes of circumstances, product release delays, or other risks as stated in our filings with the Securities and Exchange Commission, located at www.sec.gov, may cause results to differ materially from those expressed or implied in this press release. If the uncertainties materialize or the assumptions prove incorrect, results may differ materially from those expressed or implied by such forward-looking statements and assumptions. All statements other than statements of historical fact are statements that could be deemed forward-looking statements. Fortinet assumes no obligation to update any forward-looking statements and expressly disclaims any obligation to update these forward-looking statements.

FTNT-O

Add to Digg Bookmark with del.icio.us Add to Newsvine

Media Contacts:

Rick Popko

Fortinet

408-486-7853

rpopko@fortinet.com

Source: Fortinet

News Provided by Acquire Media