Fortinet December Threat Landscape Report Highlights Cyber Criminals Regionalizing Operations to Diversify Fund Distribution

Buzus Trojan Makes a Holiday Appearance in the Guise of an E-Card

SUNNYVALE, CA -- (MARKET WIRE) -- 01/04/11 -- Fortinet® (NASDAQ: FTNT) -- a leading network security provider and the worldwide leader of unified threat management (UTM) solutions -- today announced its December 2010 Threat Landscape report, which identifies a concerning evolutionary step cyber criminal operations are taking to more effectively diversify the distribution of their ill-gotten gains.

"This month we saw a wide variety of money mule recruitment campaigns that -- for the first time -- targeted specific countries in an orchestrated manner," said Derek Manky, project manager, cyber security and threat research at Fortinet. "The campaigns, which were seeded in a number of Asian and European countries, solicited local individuals who already have or had established relationships in the banking industry or were looking for work as 'online sales administrators.'"

To make these "localized" campaigns even more effective, they incorporated regional-sounding domain names, such as cv-eur.com, asia-sitezen.com and australia-resume.com. Upon closer scrutiny, Fortinet's FortiGuard team discovered all three domains were registered to the same Russian contact, and all contact addresses for worldwide recruitment used Google mail hosting. By using localized campaigns, criminals can obtain mule accounts internationally -- each one falling under different banks and governing laws. Thus, if one is taken offline (due to increased enforcement activity), the others will remain online and business will be as usual.

Buzus Trojan in E-Card
December also saw the reemergence of the Buzus Trojan, this time being distributed through mass emails posed as e-cards just in time for the holiday season. Once a compromised attachment is opened, the now infected system sends out similar e-cards to everyone it finds in the system's email address book in an effort to "seed," growing the botnet. Fortinet's FortiGuard team discovered the main payload of Buzus was none other than the nefarious Hiloti botnet.

"Hiloti is particularly innovative, as it uses DNS as a communication channel to watermark its report information to its servers," Manky continued. "This is done to evade detection, since it appears like normal, legitimate DNS traffic. Hiloti, which is distributed through many different botnets, is a preferred piece of malware among cyber criminals today because it incorporates a 'pay-per-install' affiliate program wherein established botnet distributors receive a payment each time Hiloti is injected into a new machine. This type of incentive program allows Hiloti originators to grow their infection base quicker than attempting to grow it organically."

Adobe, Microsoft, Apple Zero-Day Vulnerabilities
In December, FortiGuard labs also disclosed three arbitrary code execution vulnerabilities in Microsoft and Apple products. FGA-2010-65 describes an MS Windows Kernel vulnerability that may allow execution in privileged (Ring0) context. FGA-2010-64 is yet another DLL loading vulnerability that affects multiple products within the Windows 7 operating system. And FGA-2010-62 outlines an integer overflow vulnerability in Apple QuickTime, which can lead to potential infection by simply viewing a specially-crafted QuickTime movie file.

New and old vulnerabilities will continue to be exploited, so it's important to keep all application patches up to date. Additionally, a valid intrusion prevention system (IPS) can help mitigate attacks against both known vulnerabilities and zero-days. With the use of communication through common protocols, application control is becoming more important to identify malicious activity on the application level.

FortiGuard Labs compiled threat statistics and trends for December 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 this vulnerability with the appropriate configuration parameters 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.

The full December Threat Landscape report, which includes the top threat rankings in several categories, is available now. 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 Fortinet Security Blog and Fortinet's monthly Security Minute videocast.

About Fortinet (www.fortinet.com)
Fortinet (NASDAQ: FTNT) is a worldwide provider of network security appliances and the 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 2009 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 © 2010 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, 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. This news release may contain forward-looking statements that involve uncertainties and assumptions. 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, including but not limited to, any statements related to expected trends in cybercriminal activity. These trends are difficult to predict and any stated expectations regarding these trends may not ultimately be correct. Fortinet assumes no obligation to update any forward-looking statements, and does not intend to update these forward-looking statements.

FTNT-O

Video-Link Available: http://www2.marketwire.com/mw/frame_mw?attachid=1466116

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

Media Contact:

Rick Popko

Fortinet, Inc.

+1-408-486-7853

rpopko@fortinet.com

Source: Fortinet

News Provided by Acquire Media