Fortinet January Threat Landscape Report Highlights Jump in Exploitation of New Vulnerabilities

Feebs, Buzus and Virut Trojans Jockey for Top Spot in Malware Detections for Report Period

SUNNYVALE, CA -- (MARKET WIRE) -- 02/02/11 -- Fortinet® (NASDAQ: FTNT) -- a leading network security provider and the worldwide leader of unified threat management (UTM) solutions -- today announced its January 2011 Threat Landscape report, which identifies a 61 percent exploitation rate of new vulnerabilities found this period and tracked by FortiGuard Labs. On a typical month, exploit activity falls between 30 percent and 40 percent. Half of new vulnerabilities rated as "critical" were targeted, opening doorways for an attacker to execute any command(s) on a target machine.

"It is no secret that software vulnerabilities continue to be disclosed in large numbers on an ongoing basis -- especially critically rated ones," said Derek Manky, senior security strategist at Fortinet's FortiGuard Labs. "Hackers are sinking their teeth into unprotected systems, thanks to readily available exploit code and attack frameworks that support these new vulnerabilities. Since they are freshly disclosed, not everyone may have up-to-date signatures or proper patches in place. It is imperative to ensure both are updated in a timely fashion in order to effectively combat this threat. Also, with the use of communication through common protocols, application control is becoming more important in identifying malicious activity on the application level."

Top Three Malware Detections for the Month
The Feebs, Buzus and Virut Trojans remained persistent and active this month. Feebs is a mass mailer that uses Javascript to infect systems. The "mal"-mail typically contains a password protected archive, along with the information in the mail body. Buzus, on the other hand, was more prevalent in the spam scene, sending infected attachments of itself using a variety of spam campaigns.

Two Virut variants surfaced during this report period and, as of this writing, they are still receiving commands from Virut controllers to download and execute malware. Virut.U uses an updated IRC channel and encrypts all traffic to this IRC channel, while Virut.A continues to connect to the IRC server "proxim.ircgalaxy.pl" unencrypted. Both variants are using port 65520 for connection. Virut, which has been around since 2006 and has been in Fortinet's Top 10 and Top 100 lists ever since, is a rigid file infector that contains a bot component, making it very difficult to clean since it spreads to thousands of files on a system once it hits. FortiGuard Labs observed Virut downloading other botnets, meaning an infected system would soon have multiple pieces of malware in place. Virut is one of the most persistent botnets the lab sees today, since it is tough to remove from an infected system, uses a public IRC domain and has hybrid spreading capabilities.

FortiGuard Labs compiled threat statistics and trends for January 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 January 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.

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=1498487

Media Contact:

Rick Popko

Fortinet, Inc.

+1-408-486-7853

rpopko@fortinet.com

Source: Fortinet

News Provided by Acquire Media