Fortinet February Threat Landscape Report Highlights New Zero-Day Vulnerabilities

SpyEye Botnet Enters Top 10 List and Credit Card Phishing Campaign Email Allows Attackers to Easily Intercept Login Credentials

SUNNYVALE, CA -- (MARKET WIRE) -- 03/02/11 -- Fortinet® (NASDAQ: FTNT) -- a leading network security provider and the worldwide leader of unified threat management (UTM) solutions -- today announced its February 2011 Threat Landscape report, which details five zero-day vulnerabilities found in Cisco (FGA-2011-03), Adobe (FGA-2011-06) and Microsoft (FGA-2011-04) products. FortiGuard Labs worked diligently with these companies to address and disclose these vulnerabilities as part of its responsible disclosure program, which includes more than 125 zero-day vulnerability discoveries to date.

Microsoft also issued a zero-day security advisory regarding an information disclosure vulnerability with Internet Explorer and MHTML, making it possible under certain conditions for attackers to inject a client-side script in the response of a Web request run in the context of the victim's Internet Explorer. The script could spoof content, disclose information or take any action that the user could take on the affected Web site on behalf of the targeted user.

SpyEye Botnet Activity Surges
The SpyEye Botnet entered the Threat Landscape Report's Top 10 Malware listing for the first time this month, signaling a possible shift of criminal organizations around the world that had previously employed the Zeus botnet. Historically, Zeus developers have made efforts to avoid detection and analysis on their configuration files by prepending garbage (red herrings) before data structures. Last year, FortiGuard Labs analyzed an emerging mobile component of Zeus, known as Zitmo and recently noted that Zitmo.B has resurfaced with both a Symbian and Windows Mobile version that was actively in the wild.

"We're likely to see similar ongoing activity by the SpyEye group, such as routine obfuscation of their data and command and control transmissions," said Derek Manky, senior security strategist at Fortinet. "SpyEye developers are also working to make their product more efficient in terms of management and automation, which is evidenced by the bot's new Automatic Transfer System."

New Credit Card Phishing Email
This month FortiGuard Labs observed a new credit card phishing email, which employs a scare tactic that says the account has been "in violation of policies." In the example discovered, the highlighted link pointed to a rogue domain that did not belong to the card vendor -- however, streamed authentic content from card vendor's site.

"Always observe these types of traits before clicking on links," Manky said. "In this case, clicking the link would direct the victim to a landing site located at a datacenter in Bangkok. This landing site would then redirect the user to a server in China, which borrowed content from the legitimate credit card site using a proxy. This man-in-the-middle setup allowed the attackers to easily intercept login credentials along the way."

Once these credentials are obtained, it becomes very easy for criminals to launder stolen funds through the likes of anonymous transferring services and money mules.

FortiGuard Labs compiled threat statistics and trends for February 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 February 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.

FTNT-O

Embedded Video Available

Embedded Video Available: http://www2.marketwire.com/mw/frame_mw?attachid=1530398

Media Contact:

Rick Popko

Fortinet, Inc.

+1-408-486-7853

rpopko@fortinet.com

Source: Fortinet

News Provided by Acquire Media