Fortinet Threat Landscape Research Warns of New Apache Server Vulnerability

"Operation Occupy Wall Street" Receives Support From "Anonymous" in the Form of SQL Injection and DoS Attack

SUNNYVALE, CA -- (MARKET WIRE) -- 10/03/11 -- Fortinet® (NASDAQ: FTNT) -- a leading network security provider and the worldwide leader of unified threat management (UTM) solutions -- today released its latest Threat Landscape report, which reveals the new "Apache Killer" tool is currently being used to exploit an Apache Server vulnerability that could be used to launch denial of service (DoS) attacks against Web hosts running older versions of Apache. Apache has fixed the flaw and recommends users immediately upgrade to Apache 2.2.20.

Wall Street Reformers Receive "Anonymous" Help
"Operation Occupy Wall Street," a grass roots protest movement formed in early July to draw attention to what the group perceives as corruption and greed on Wall Street, received assistance in late August from hacktivist group "Anonymous." Anonymous, widely known for rallying behind WikiLeaks director, Julian Assange, by engaging in distributed denial of service attacks (DDos) against PayPal, MasterCard, Visa and others, recently deployed a new DDoS tool called #RefRef, which exploits SQL server vulnerabilities.

"#RefRef is Anonymous' next move from their Apache Killer and Low Orbit Ion Cannon (LOIC)," said Derek Manky, senior security strategist at Fortinet. "Unlike the LOIC which requires multiple users to target a site with a constant bombardment of TCP and UDP packets, #RefRef only requires a single attack. Once in place on a vulnerable target system, the software actually uses the system's processing power against itself until it ultimately crashes due to resource exhaustion."

FortiGuard released the IPS signature 'RefRef.DoS' to help mitigate this threat.

Email Malware Gets Sneakier
In the second half of September, the malware top 10 consisted mainly of malware that was spread through spammed email attachments or malicious links. Most of the poisoned emails under investigation included some form of infected attachment, such as a PDF/Word document, an invoice, a receipt, a PayPal notification or a zipped document. One of the interesting behavioural characteristics these attachments possess is their ability to delete themselves after being executed by a user, which helps to avoid detection.

The trick that these malicious email creators use to get unsuspecting users to click on an infected attachment is to disguise the malware executable icon with a legitimate-looking icon that's associated with the various types of documents in use today. The safest way to avoid this type of infection is to not double-click on attachments, but, instead, right-click over the icon and save the attachment to your desktop and then right-click over the saved document to check the file's properties. If a file properties check fails to reveal the nature of the document, the questionable file can be submitted to FortiGuard's online virus scanner, which can be found here.

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 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 Threat Landscape report, which includes the top threat rankings in several categories, is available now. September's Security Minute video podcast, which features commentary on today's latest threats can be found here. Ongoing research can be found in the FortiGuardCenter or via FortiGuard Labs' RSS feed. Additional discussion on security technologies and threat analysis can be found at the Fortinet Security Blog.

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 © 2011 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. Nothing in the news release constitutes a warranty, guaranty, or contractually binding commitment. 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

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

Media Contacts:

Rick Popko

Fortinet, Inc.

408-486-7853

rpopko@fortinet.com

Source: Fortinet

News Provided by Acquire Media