Malware Variants Mark Record-Breaking Activity Levels in Fortinet August '09 Threatscape Report

Email Scams Remain Aggressive with Classic Campaigns; Critical Vulnerabilities Increasingly Exploited in the Wild

SUNNYVALE, Calif. - Aug 28, 2009 - Fortinet® - a market-leading network security provider and worldwide leader of unified threat management (UTM) solutions - today announced its August 2009 Threatscape Report. Vacations may be wrapping up towards the end of summer, but there was no time-off for the threat landscape as Fortinet reports a flood of malware activity executed through several spam campaigns in this period. In addition, increasing levels of software vulnerabilities were marked by critical in-the-wild exploits. Key highlights of the August Threatscape Report include:

- ZBot Variant Bumps Headline-making Worms of Years Past: Surpassing the single-day run of the Sober worm in 2006, the Storm worm in 2007 and rogue security software in 2008, ZBot variants flooded cyberspace on July 24th with record levels: one through HTML/Agent.E, an attachment in an email which used the ever-popular eCard hook to potentially steal and sell personal consumer information. An additional ZBot variant made it to the top 10 malware list, yet, even with such high activity rates, ZBot still didn't grab up the top position. Instead, the online gaming trojan W32/OnlineGames.BBR maintained its first place position for the third consecutive month.
- Spam Continues to Test the Unsuspecting: While the popular eCard social engineering campaign continued to prey on the innocent, this month's report highlighted a newly rendered - but an old time classic - money mule scheme. Using a fake job advertisement, this plays on a legitimate company name and the desperation of victims to make a quick buck in a money-laundering scheme. Israel entered the top five region list for receiving high spam volume, while the USA, Japan and France accounted for the remaining share of detected spam.
- Cause for Remote Code Execution Concern: Marking a consistent trend of increasing software vulnerabilities, threat rates during the August period jumped up from July. Of 168 new vulnerabilities detected, 62 were reported to be actively exploited in the wild, with a large portion of these attacked vulnerabilities rated as critical. Critical vulnerabilities typically indicate a concern for remote code execution - an easy way for attackers to permeate a system. Two in-the-wild vulnerabilities in Microsoft Office Web Components (MS09-043) and in Adobe Reader/Flash (APSA09-03) were detected to have consistent exploit activity during this period, as well.

"Threat activities for this month involved a few well-known schemes that are up to some new tricks, a good indication that cyber criminals weren't pulling out all the stops, but they certainly weren't taking a break during summer vacation," said Derek Manky, project manager, cyber security and threat research, Fortinet. "With criminals counting on consumers to fall for virtually the same old tricks, it can't be stressed enough that we need to know whom and what to trust - this is an important element to a robust security model."

The FortiGuard research team compiled threat statistics and trends for August based on data collected from FortiGate® network security appliances and intelligence systems in production worldwide. Customers who use Fortinet's FortiGuard Subscription Services should already be protected against the threats outlined in this report.

To read the full August Threatscape report which includes the top threat rankings in each category, please visit: http://www.fortiguard.com/report/roundup_august_2009.html. For ongoing threat research, bookmark the FortiGuard Center (http://www.fortiguardcenter.com/) or add it to your RSS feed by going to http://www.fortinet.com/FortiGuardCenter/rss/index.html. Additional discussion on security technologies and threat analysis can be found at the FortiGuard Blog at http://blog.fortinet.com. To learn more about FortiGuard Subscription Services, visit http://www.fortinet.com/products/fortiguard.html.

FortiGuard Subscription Services offer broad security solutions including antivirus, intrusion prevention, Web content filtering and anti-spam capabilities. These services help enable protection against threats on both application and network layers. FortiGuard Services are updated by the FortiGuard Global Security Research Team, 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.

About Fortinet (www.fortinet.com)
Fortinet is a leading provider of network security appliances and the market leader in Unified Threat Management or UTM. Fortinet solutions were built from the ground up to integrate multiple levels of security protection -- including firewall, antivirus, intrusion prevention, VPN, spyware prevention and antispam -- designed to help customers protect against network and content level threats. Leveraging a custom ASIC and unified interface, Fortinet solutions offer advanced security functionality that scales from remote office to chassis-based solutions with integrated management and reporting. Fortinet solutions have

won multiple awards around the world and are the only security products that are certified in five programs by ICSA Labs: Firewall, Antivirus, IPSec VPN, Network IPS and Antispam. Fortinet is based in Sunnyvale, California.

Copyright © 2009 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.