



Fortinet September 2009 Threatscape Report Shows Scareware Spike

Fortinet - a market-leading network security provider and worldwide leader of unified threat management (UTM) solutions has announced that its September 2009 Threatscape Report uncovered a preponderance of scary tactics, showing continued strength one year after the initial cyberspace explosion of scareware in September 2008.

Cyber criminals are spooking innocent with scams - including email threats, botnet downloads and fraudulent software. Their ultimate goal is to scare Internet users into providing banking or credit card details, then using those details to steal funds or commit fraud.

Additionally, several significant computer vulnerabilities were uncovered in September, and the volume of exploits targeting known vulnerabilities remained high in September 2009.

Key highlights of the September Threatscape Report include:

Bredolab and others spook users for scareware anniversary celebration: Marking the one year anniversary since the initial explosion of scareware across cyberspace, the Bredolab botnet (W32/Bredo.G), a Trojan downloader linked to rogue security software, was highly active this period.

This is another example of the growing trend in broad distribution of fraudulent software payloads. Recent examples in September 2009 include SEO black hat campaigns, the NY Times malicious advertisements, and a variant of Pushbot which downloaded fraudulent software payloads.

Bredolab variants were pushed out through a mass mailing campaign that sends fake DHL invoices. If the invoices are opened, the machines are then recruited into a network of computer zombies.

ZBot was again active this period, with the do-it-yourself botnet spreading through another mass mailing attack disguised as a tax scare.

Spam pushes creative money mule hook: In line with the massive scareware tactics rampant in September 2009, cybercriminals continued to roll out creative money mule hooks, hoping to lure

unsuspecting end-users with too-good-to-be-true offers. A commonly used tactic was for spammers to push out attractive job advertisements through a professional looking email, requesting the users bank account details to process payments.

Zero-day attacks: The remote-code execution vulnerability Microsoft Server Message Block (SMB2, CVE-2009-3103) reported low but steadily increasing exploit activity in September 2009. Microsoft has now released a temporary fix for the vulnerability. Additionally, the Microsoft ISS FTP Service (CVE-2009-3023) and Adobe Reader/Flash (CVE-2009-1862) vulnerabilities are increasingly being used in attack activity.

Were seeing a steady if not rapid growth of scareware which like other high-profile threats will eventually begin to diminish in success and profitability once end-users become wise to them, said Derek Manky, project manager, cyber security and threat research, Fortinet. However, its clear that these get-rich-quick schemes are still proving to be successful today, and cybercriminals will undoubtedly continue to mine them until they are forced to move onto other innovative ways to exploit end-users. End-users should continue to be wary, and proceed online as they would offline with the notion that if its too good to be true, it likely is.

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

To read the full September Threatscape report which includes the top threat rankings in each category, please visit: http://www.fortiguard.com/report/roundup_september_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 antispyware -- 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 Antispyware. 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.