



Fortinet November Threatscape Report Shows Calm Before Holiday Storm

Fortinet - the pioneer and leading provider of unified threat management (UTM) solutions - today announced its November Threatscape report showed a continuing downward trend in online threat activity, from the high point reached in September 2008.

In November 2008, with the exception of an increase in the number of exploits, malware and spam showed significant declines. Fortinet believes this to be temporary, as the large surge in online shopping and social activity during the holiday season provides many opportunities for cybercriminals.

Two key activities suggest that the online threat hiatus is only temporary:

The McColo take-down dropped the percentage of email tagged as spam to a low of 37 percent in mid-November; Three of the top five malware variants were members of the Goldun family of key-loggers, which record keystrokes most often for banking and credit card information theft. Increased key-logging activities suggest criminals are getting ready to target people making online purchases over the holiday season.

We expect both of these activities to quickly escalate as spam botnets find new avenues to proliferate themselves in the wake of McColo, said Derek Manky, project manager, cyber security and threat research, Fortinet. And with the online shopping season now kicking off, key-logging activity is expected to follow in hot pursuit. We are already seeing a steady uptick in threat activity since closing the November report.

Following are key findings from Fortinet's November Threatscape report:

Exploits/Intrusion

25 of the 81 active vulnerabilities were considered high-risk categories. The top two were Trojan.Storm.Worm.Krackin.Detection and Worm.Slammer, which accounted for 60 percent of the months total vulnerabilities;

Malware

Activity declined slightly in October and November, due largely to the decrease in scareware, which still remained No. 1 on the top ten malware variant list with Golduns key-logging activity claiming the 2nd, 3rd and 4th positions.

Japan (39.68%) and the U.S. (39.58 %) were the main battle grounds for malware, with China (30.37%), Taiwan (22.16%) and India (17.59%) also being heavily targeted.

Spam

A sharp drop in activity on November 12 resulted from the McColo take-down, but spam remains an active distribution mechanism for cyber criminals.

Three socially-engineered emails topped the list of spam for the month, all with malicious attachments related to top-ranked malware W32/FakeAlert.D and W32/Goldun.RV. Both of these malware families were observed to be involved in the same email campaign, an indicator that different criminal organizations are utilizing the same spam vehicle.

Web traffic

On the web, malware jumped seven points to 21 percent of categorized web threat activities, due for the most part to a near double-digit decline in pornographic traffic.

The Fortinet

FortiGuard Global Security Research team compiled threat statistics and trends for November 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

November Threatscape report which includes the top threat rankings in each category, please visit: http://www.fortiguardcenter.com/reports/roundup_nov_2008.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 products with a subscription to FortiGuard, these updates are delivered to all FortiGate, FortiMail and FortiClient products.

About Fortinet (www.fortinet.com)

Fortinet is the pioneer and leading provider of ASIC-accelerated unified threat management, or UTM, security systems, which are used by enterprises and service providers to increase their security while reducing total operating costs.

Fortinet solutions were built from the ground up to integrate multiple levels of security protection--including firewall, antivirus, intrusion prevention, VPN, spyware prevention and anti-spam -- 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 six programs by ICSA

Labs: Firewall, Antivirus, IPSec VPN,

SSL VPN, Network IPS, and Anti-spam. Fortinet is privately held and based in Sunnyvale, California.

Copyright 2008 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 and FortiDB. Other trademarks belong to their respective owners.

Media Contact: Sebastian Rice, 02 9959 1991, seb@silverspan.com