

## Fortinet

- the pioneer and leading provider of unified threat management (UTM) solutions
- today announced that its January 2009 Threatscape report revealed a surge in attacks against unpatched computer exploits.

Originally detected in October 2008, a

buffer overflow exploit that is outlined in Microsoft Security

Bulletin MS08-067 was used as the basis of a series of attacks on un-patched machines from the end of December 2008 through January 2009. The exploit affects computers running Windows Vista, XP, 2000, Server 2003, and Server 2008. This series of recent attacks reached a peak level of activity on January 14th.

## Online

gaming malware continued to build momentum in January 2009, with two Trojans increasing in activity. Spy/OnLineGames claimed first place on Fortinet's Top 100 malware variants list, with W32/Dropper.VEM!tr surging enormously, demonstrating that criminals are now focusing on using online gaming malware designed to pilfer passwords, personal details, and credit card information. The countries most targetted were the US, Japan, China, Taiwan and India.

## Fortinet's

FortiGuard Global Security Research team also observed increased levels of spam activity, largely driven by social engineering style campaigns which leveraged concerns about economic problems, and the recent US Presidential Inauguration.

## "While

eavesdropping keyloggers and spam-spewing botnets continued to rise in popularity this month, what's most concerning is the explosion of the now dated MS08-067 vulnerability, said Derek Manky, project manager, cyber security and threat research, Fortinet. Propagating as far back as October 2008, this vulnerability underscores the importance of proper patch management and a layered security approach to avoid epidemic outbreaks of this nature.

## The

Fortinet FortiGuard Global Security Research team compiled threat statistics and trends for January 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.

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.

To read the full January Threatscape report which includes the top threat rankings in each category, please visit: [http://www.fortiguardcenter.com/reports/roundup\\_jan\\_2009.html](http://www.fortiguardcenter.com/reports/roundup_jan_2009.html).

About Fortinet ([www.fortinet.com](http://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 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 six programs by ICSA Labs: Firewall, Antivirus, IPSec VPN, SSL VPN, Network IPS, and Antispam. Fortinet is privately held and 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, including, but not limited to, the following trademarks: 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. Fortinet has not independently verified statements above attributed to other parties, and Fortinet does not endorse any such statements.