



## Fortinet December Threatscape Report Shows High Exploit Activity and Online Shoppers Targeted

Fortinet (NASDAQ: FTNT) a leading network security provider and worldwide leader of unified threat management (UTM) solutions today announced its December 2009 Threatscape report showed that while there was a general slow-down in malware activity as compared to the previous three reporting periods, one malware variant bucked the trend to deliver more than 66 percent of total malware activity for the month.

The Bredolab downloader took advantage of the expected surge in holiday online shopping by loading ZBot variants onto infected machines: ZBot is commonly configured to pilfer online banking credentials.

On the exploit front, MS08-067 showed up as the most actively targeted system vulnerability in this reporting period. December 2009 proved to be a busy time for vulnerabilities and zero-day attacks with 157 new vulnerabilities detected, a third of which were in active attack mode.

Overall malware volume returned to pre-October levels this period after several months of record activity driven by ZBot, Bredolab and Pushdo/Cutwail. Nonetheless, the Bredolab loader returned to the top spot with a vengeance in December 2009, accounting for a whopping 66.5 percent of total detected malware activity. Bredolabs threat only spanned over several days, but completely overtook all other malware activity for the month of December. The seeding engines behind Bredolab have so much horsepower that a single seeding campaign can manipulate Threatscape volume for the entire period.

The top three email threats in-the-wild captured the spirit of the season shopping and money. Going for the easy money, two of the three were bank phishing that try to trick users into clicking on a dangerous link in one case by telling users that fraudulent credit card activity has occurred. The third most popular email threat of the period was a money-mule campaign disguised as a job advertisement for a mystery shopper, which ultimately involves the recipient receiving money orders and transferring funds.

Exploitation of MS08-067 (made infamous by the Conficker worm) remains the most actively attacked in December 2009, with Waledac botnet traffic being second as listed in Fortinets Top 10 attack list.

FortiGuard Labs discovered ten zero-day vulnerabilities that were disclosed in December 2009 and uncovered 157 new vulnerabilities in total. On top of this, hackers continued to find ways to exploit zero-day attacks: CVE-2009-4324 was one observed through Adobe Reader/Acrobat and Javascript - an increasingly common attack vector. Another zero-day was addressed by Microsoft through MS09-072 on December 8th.

The growth in cyber criminal activity we observed in 2009 will continue with force in 2010. With more digital convergence undoubtedly to occur in 2010, there will be a wealth of opportunity for cyber criminals: There is an infinite number of victims to target, the infrastructure is already in place along with development resources, and there are ample new delivery vehicles such as social media networks to help facilitate cyber criminal activities, said Derek Manky, project manager, cyber security and threat research, Fortinet. Digesting all of this, it becomes apparent that we are in for a wild ride in 2010 all elements are positioned for a perfect storm in cyberspace.

FortiGuard Labs compiled threat statistics and trends for December 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 December Threatscape report which includes the top threat rankings in each category, please visit: [http://www.fortiguards.com/report/roundup\\_december\\_2009.html](http://www.fortiguards.com/report/roundup_december_2009.html). For ongoing threat research, bookmark the FortiGuard Center (<http://www.fortiguardscenter.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/fortiguards.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 FortiGuard Labs, which are designed to enable 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](http://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 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 and Fortinet does not independently endorse such statements. This news release contains 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