# Fortinet November Threat Landscape Report Highlights Reduced Spam Levels After Bredolab Takedown

## Koobface Servers Taken Down on November 14 Reconfigured to New Control Servers Five Days Later

SUNNYVALE, CA -- (MARKET WIRE) -- 12/01/10 -- Fortinet® (NASDAQ: FTNT) -- a leading network security provider and the worldwide leader of unified threat management (UTM) solutions -- today announced its November 2010 Threat Landscape report, which highlights a 12 percent reduction in global spam after Dutch authorities dismantled a large Bredolab network by taking more than 140 servers offline.

"Bredolab was often used to load spam engines, which are typically used to sell fraudulent pharmaceuticals," said Derek Manky project manager, cyber security and threat research at Fortinet. "The scale of this Bredolab botnet had a huge impact on spam levels, dropping as much as 26 percent one week after it was dismantled."

*Koobface Takedown*
Koobface, a botnet well known for spamming popular social media sites, was taken offline on November 14 when UK ISP provider Coreix took three MotherShip servers offline. Koobface used intermediary servers (proxies) to communicate with these MotherShip servers through HTTP port 80.

"We confirmed that on November 14, when the primary servers were taken offline, the intermediary servers failed to proxy content, which effectively crippled the botnet," Manky continued. "Unfortunately, we saw communication restored five days later on November 19th. This is likely due to the fact that Koobface contains an FTP harvesting module."

Operators may use stolen FTP credentials to hijack Web servers for intermediary/proxy use. By reconfiguring their intermediary servers to new MotherShip servers, the operators seemingly regained control of their botnet.

*Adobe, Microsoft, Apple Zero-Day Vulnerabilities*
In November, FortiGuard labs also disclosed zero-day vulnerabilities in Adobe Shockwave (FGA-2010-54), Adobe Flash (FGA-2010-56), Microsoft Office PowerPoint (FGA-2010-58), and Apple QuickTime (FGA-2010-61). In addition to the four zero days, 146 additional new vulnerabilities were covered by FortiGuard IPS; 40 percent of which were actively exploited in the wild. As of this writing, a zero-day vulnerability is still being exploited in the wild for Microsoft Internet Explorer (FGA-2010-55). All five vulnerabilities were critical, and had the potential to allow attackers to execute arbitrary code from a remote location.

New and old vulnerabilities will continue to be exploited, so it's important to keep all application patches up to date. Additionally, a valid intrusion prevention system (IPS) can help mitigate attacks against both known vulnerabilities and zero-days. With the use of communication through common protocols, application control is becoming more important to identify malicious activity on the application level.

FortiGuard Labs 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 Services should be protected against this vulnerability with the appropriate configuration parameters in place.

FortiGuard Services offer broad security solutions including antivirus, intrusion prevention, Web content filtering and anti-spam capabilities. These services help protect against threats on both application and network layers. FortiGuard Services are updated by FortiGuard Labs, 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.

The full November Threat Landscape report, which includes the top threat rankings in several categories, is available now. Ongoing research can be found in the FortiGuard Center or via FortiGuard Labs' RSS feed. Additional discussion on security technologies and threat analysis can be found at the Fortinet Security Blog.

*About Fortinet (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 © 2010 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 may contain 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*

Add to Digg Bookmark with del.icio.us Add to Newsvine

**Media Contact:**

Rick Popko

Fortinet, Inc.

+1-408-486-7853

rpopko@fortinet.com

Source: Fortinet

News Provided by Acquire Media