



Fortinet's Latest Threat Report Shows New PDF Exploit Being Widely Circulated Via Spam

Fortinet (NASDAQ: FTNT) - a leading network security provider and worldwide leader of unified threat management (UTM) solutions today announced its May 2010 threat report showed a new PDF exploit being circulated in high volume through an ongoing spam campaign.

The vulnerability, first blogged about by Didier Stevens on March 29, 2010, is CVE-2010-1240, and the malicious documents now exploiting this are detected by Fortinet as PDF/Pidief.BV!exploit. Though no patch exists, Adobe has recommended mitigation strategies on its blog. To further combat the threat, Fortinet recommends implementing an intrusion prevention and antivirus solution. This vulnerability was ranked second for overall malware activity this month, behind only the nefarious Pushdo botnet.

What sets PDF/Pidief.BV apart from other PDF threats we are seeing, is that it requires user interaction, said Derek Manky, project manager, cyber security and threat research, Fortinet. More specifically, a user needs to click on the open button when prompted by a dialog box to initiate the infection. This threat is another reason why it's imperative for users to carefully read messages when they appear.

In the case of PDF/Pidief.BV, clicking open will first execute VBScript and then add a malicious botnet loader binary, which compromises the system. For detailed information on this specific PDF attack, please view our FortiGuard virus encyclopedia entry [here](#).

Botnet Activity on the Rise

Botnet activity remained strong in this report, with Gumbiar and Sasfis present in both the Top 10 Attack and Top 10 Malware lists. Though the main botnets such as Pushdo, Cutwail and Sasfis continue to pose significant threats, newer botnets are emerging.

Fortinet first detected the CMultiLoader botnet in the wild on April 8, 2010. A variant of this botnet, W32/CMultiLoader.A, has landed in the sixth spot in our Top 10 Malware list this report. The Katusha botnet (W32/Katusha.1824!tr) just missed the Top 10 list this report, ranking #11. These are two examples of up and coming botnets that are making waves. Total detected malware volume has remained fairly consistent since the beginning of the year, though distinct detection continues to rise. This indicates more variations of malware are circulating in cyberspace as malware creators continue to pack, encrypt and morph their malicious binaries.

FortiGuard Labs compiled threat statistics and trends for May 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 May threat report which includes the top threat rankings in each category, please visit: http://www.fortiguard.com/report/roundup_may_2010.html. For ongoing threat research, bookmark the FortiGuard Center or add it to your RSS feed. Additional discussion on security technologies and threat analysis can be found at the Fortinet Security Blog. 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 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.

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