Fortinet's January Threatscape Report Rings in Busy New Year, Highest Levels of Malicious Code Ever Detected

Bredolab Maintains Dominance With New Variants and Web Mailing Engine; Brings Japan to Number One for Overall Malware Volume

SUNNYVALE, CA, Feb 02, 2010 (MARKETWIRE via COMTEX News Network) -- Fortinet(R) (NASDAQ: FTNT) -- a leading network security provider and worldwide leader of unified threat management (UTM) solutions -- today announced its January 2010 Threatscape report showed a busy start to the new year with a continuous dominance of botnet malware activity, led by new variants of the ever-popular Bredolab downloader -- which represented more than 40 percent of total malware activity for the month of January. In addition, there was a twofold increase of distinct malware from last period, marking the highest number of malicious code instances ever detected. In-the-wild exploits also created a stir this period, with high-profile vulnerabilities targeting Adobe PDF and Microsoft Internet Explorer incurring peak activity levels. And, not to be left out, Bredolab received some competition this period from Buzus, a bot which functions similar to Bredolab, but seeds through its own mass mailing SMTP engine. Key threat activities for the month of January include:

-- Bredolab Holds onto Top Positions: For the third consecutive month, the Bredolab botnet grabbed top positions in Fortinet's top 10 malware list, with variants in the first and second positions that made up more than 40 percent of total malware activity detected. Another variant in the top 10, related to the Gumblar attacks, drops the Bredolab loader through malicious websites that are hosting obfuscated Javascript code as a way to start an infection. Furthering Bredolab's reach even more, a new Web mailing engine was discovered by the Fortinet threat research team, which will allow Bredolab to seed through accounts such as Hotmail and Gmail, opening the door to more effective spamming services on these platforms. Although overall malware volume returned to calmer pre-October 2009 levels, Bredolab secured most of the threat activity this period, putting Japan at number one in terms of pure detected malware volume.
-- Aurora: Not the Sleeping Beauty -- Active and Ugly: The highly publicized attacks on over 30 corporations, including Google, may share the same name as Sleeping Beauty; however, it's anything but calm and beautiful. Code-named "Aurora" (actual identifier: CVE-2010-0249), the zero-day Internet Explorer vulnerability came out in mid-January and quickly sky-rocketed to fourth spot for malicious network activity this period, making it one of the top six 'critical' flaws identified. Aurora's exploits, combined with botnet propagation and communications activities, made up the majority of top network attacks in January.
-- Spam Welcomes an Oldie, but Goodie: New to Fortinet's Threatscape Report this period, Buzus was represented by two variants and works by spreading spam through its own SMTP engine. Buzus (Circa 2008) made its wave this period through a purported Christmas greeting card from 123greetings.com, which is attached as a zip file. In addition, two new tactics helped to push spam levels this month, including an interesting social engineering hook that lures users into thinking they've discovered a money-making secret: an email conversation with a link that points people to an alleged algorithm for winning cash through online gambling. The other tactic brings spam back to the basics with a simple message, usually with an "it's you" subject, which then seeds a link redirecting browsers to a second domain, often with obfuscated Javascript code.

"There was certainly no shortage of threat activity this month, proving that 2010 will likely be another action-packed year. The amount of malicious code in the wild is increasing to available source and packing/obfuscation techniques, while in-the-wild exploits and emerging zero-day attacks targeting very popular software, like Microsoft IE and Adobe PDF, create a vulnerable

environment for users -- at every point of connectivity," said Derek Manky, project manager, cyber security and threat research, Fortinet. "As the monetary gains of these threats continue to prove value to the criminals creating them, we'll only continue to see new and creative attacks take form. As an example, this month we disclosed a new web mailing engine breaking in the wild that can spew spam more effectively through popular services such as Gmail. It is yet another reminder to keep patches up-to-date and employ a layered security approach that protects users from every direction."

FortiGuard Labs compiled threat statistics and trends for January based on data collected from FortiGate(R) 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 January Threatscape report which includes the top threat rankings in each category, please visit: http://www.fortiguard.com/report/roundup_january_2010.html. For ongoing threat research, bookmark the FortiGuard Center (http://www.fortiguardcenter.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/fortiguard.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 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(TM) and FortiClient(TM) 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 Copyright 2010 Fortinet, Inc. All rights reserved. The symbols (R) and (TM) 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 press release contains forward-looking statements that involve risks and uncertainties. These statements include statements regarding trends in the Threatscape and in malicious code. Such trends are difficult to predict and are based on factors outside of our control and so future circumstances might differ from the assumptions on which such statements are based and results may differ. All forward-looking statements reflect our opinions only as of the date of this release, and we undertake no obligation to revise or publicly release the results of any revision of these forward-looking statements in light of new information or future events.

FTNT-O

Media Contacts:
Kim Nguyen
Fortinet, Inc.
408-486-5458
knguyen@fortinet.com

SOURCE: Fortinet

mailto:knguyen@fortinet.com

Copyright 2010 Marketwire, Inc., All rights reserved.

News Provided by COMTEX