



## Fortinet's February Threatscape Report Shows Rise in Ransomware, Spam Nears Record Numbers

Fortinet (NASDAQ: FTNT) - a leading network security provider and worldwide leader of unified threat management (UTM) solutions today announced its February 2010 Threatscape report showed strong spam activity, with one particular campaign accounting for more than half of the total volume of malware detected this period.

In just a two-day run HTML/Goldun.AXT dominated spam and overall threat levels, nearing record numbers, and contributed to the explosion of ransomware. A number of other varying spam campaigns helped to elevate ransomware in February, distributing a threat variant known as Security Tool.

What we observed this month is that while spamming campaigns may change over time and methods of execution reworked a bit, the tried and true techniques that have proven successful in the past continue to thrive, said Derek Manky, project manager, cyber security and threat research, Fortinet. Spam will continue to come in new flavors, with either old binaries under a different package or a new binary code under a similar guise; and new tools, like crime-as-a-service, will continue to support the growing distribution. This gives us another reason to support a layered security approach as an imperative for getting in front of the next wave.

Key threat activities for the month of February include:

**Ransomwares Reality:** The spread of ransomware became a reality this period with high activity through a variety of spam campaigns. Most notable was the number one chart-topping malware variant HTML/Goldun.AXT, which works by disseminating a binary malware file that downloads the ransomware Security Tool and, once executed, locks up applications until a cleansing tool is purchased to restore the computer.

While this example accounts for the majority of activity detected this period, the Security Tool ransomware was also distributed through SEO attacks as well. The HTML/Goldun campaign brings a new ransomware tactic to the table and ups the ante for monetary gains, but the campaign in and of itself isn't new. The first waves of the campaign were seen in late 2008, alongside the first flood of scareware that hit cyberspace.

Job Vacancies -- Cutwail

Hired: Spam this

period came in different shapes and sizes, but one thing is for sure: it came in record numbers. The culprit behind the mass distribution was Cutwail, a botnet spam engine whose most prevalent campaigns sent scareware and ransomware through social engineering schemes.

In February, additional botnet binaries were linked to Cutwail, indicating Cutwail is being used as a spamming service, which ultimately multiplies the number of cybercriminals pushing out these spam campaigns.

Buzus and Botnets Go

Berserk: While

ransomware took the prize in this period's Threatscape report, the Buzus spam Trojan and various botnets, including the infamous Bredolab, Gumbler and Sasfis, still created a stir across Fortinet's Top 10 Malware list.

One new-comer to the top 10 attack list was the Sun Java vulnerability (CVE-2009-3867), which is triggered through a malicious Java Applet by visiting a malicious website, proving that the platform is, once again, a quick and easy target for such campaigns.

FortiGuard Labs compiled threat statistics and trends for February based on data collected from FortiGate network security appliances

and intelligence systems in production worldwide. Customers who use Fortinet FortiGuard Subscription Services should already be protected against the threats outlined in this report.

To read the full February Threatscape report which includes the top threat rankings in each category, please visit: [http://www.fortiguard.com/report/roundup\\_february\\_2010.html](http://www.fortiguard.com/report/roundup_february_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 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

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 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.