# Fortinet July Threat Landscape Report Shows Sasfis Botnet Variants Multiplying and Focusing on Spam Delivery

## Stuxnet Attack Still Under Investigation While Awaiting Microsoft Patch

SUNNYVALE, CA, Aug 02, 2010 (MARKETWIRE via COMTEX News Network) -- Fortinet(R) (NASDAQ: FTNT) -- a leading network security provider and a worldwide leader of unified threat management (UTM) solutions -- today announced its July 2010 Threat Landscape report, which showed that eight Sasfis botnet variants have landed in the company's top 10 malware listing this period. This is an increasingly common occurrence, as developers continue to roll out updated copies of their creations. Earlier this year, the Sasfis botnet was dedicated to downloading and executing software (primarily fake antivirus) on infected systems. This period, Sasfis was observed downloading updated spamming modules. Typical Sasfis spam examples include fake UPS invoices and Facebook photo links.

"Spam bots continue to diversify, sending a variety of spam themes on a frequent basis," said Derek Manky, project manager, cyber security and threat research, Fortinet. "This month we observed various socially engineered emails that came with HTML attachments. These attachments further contained obfuscated javascript which would redirect users to malicious sites. The diversity of these spam campaigns and their targets shows how botnets continue to evolve to serve the needs of their underground customers."

Stuxnet Attack This month's Stuxnet attack (read our FAQ here), reiterates the importance of quickly patching security holes as fixes become available and having a broad intrusion prevention system (IPS) in place. Even with proper patch management, all it takes is one zero-day vulnerability to be exploited (even in low volume) to potentially cause a significant impact. While the Stuxnet attack is still under investigation, the fact that a trojan associated with the exploit was seemingly developed to target industrial control systems underscores this point. This is also a good example of how little interaction is required by the end user to become infected. The Stuxnet exploit attacked a Windows Shell vulnerability (CVE-2010-2568). To launch its attack, a user simply opened a folder.

"We saw a similar attack method with PDF files through JBIG2 image streams and Windows shell extensions back in February 2009 (CVE-2009-0658), where simply browsing a folder could trigger an infection," Manky continued. "Fortinet detects the vulnerability associated with the Stuxnet attack as 'MS.Windows.Shell.LNK.Code.Execution,' and generically detects the exploited '.LNK' payload with antivirus as 'W32/ShellLink.a!exploit.CVE20102568'. As of writing, there are workarounds but no official patch has been released from Microsoft."

Windows Help Center Vulnerability Exploited On June 5, vulnerability within the Windows Help and Support Center that could allow remote code execution was publicly disclosed. Like Stuxnet, this is yet another example of a zero-day vulnerability successfully attacked before a patch is made available. We witnessed attacks on the vulnerability as early as June 11th before Microsoft issued a patch for CVE-2010-1855 on July 13th. The attacks that occurred through Websites were made more potent because they were launched through the HCP protocol handler, which is used by all browsers. In many cases Websites that serve exploits will try to fingerprint browsers and launch attack code tailored to those browsers.

FortiGuard Labs compiled threat statistics and trends for July 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 July Threat Landscape report which includes the top threat rankings in each category, please visit: http://www.fortiguard.com/report/roundup_july_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 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 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(TM) and FortiClient(TM) products.

About Fortinet (www.fortinet.com) Fortinet (NASDAQ: FTNT) is a worldwide provider of network security appliances and a 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.

FTNT-O

```
Media Contact:
Rick Popko
Fortinet, Inc.
+1-408-486-7853
```
rpopko@fortinet.com


SOURCE: Fortinet

mailto:rpopko@fortinet.com

News Provided by COMTEX