Fortinet June Threat Landscape Report Shows New Variations of Sasfis Botnet, Obfuscated JavaScript Attacks

Operation Aurora Vulnerability Comes Out of Hibernation With Hit-and-Run Attack

SUNNYVALE, CA, Jun 30, 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 June 2010 Threat Landscape report showed that new variations of the Sasfis botnet have entered the malware Top 10 list. Sasfis, which has been competing with the Pushdo botnet in terms of sheer volume, was very active this month.

"We observed Sasfis loading a spambot component, which was heavily used to send out binary copies of itself in an aggressive seeding campaign," said Derek Manky, project manager, cyber security and threat research, Fortinet. "The Sasfis socially-engineered emails typically had two themes; one looked like a fake UPS Invoice attachment, and the other was disguised as a fees statement. Much like the Pushdo and Bredolab botnets, Sasfis is a loader -- the spambot agent is just one of multiple components downloaded."

IE Vulnerabilities Come Out of Retirement This month, FortiGuard Labs saw a hit-and-run attack for the Internet Explorer HTML Object Memory Corruption Vulnerability (known as CVE-2010-0249 within Microsoft and MS.IE.Event.Invalid.Pointer.Memory.Corruption within Fortinet). This attack first surfaced in January 2010 and was used in the infamous Aurora attacks to plant spy trojans within targeted, major corporations. The attack has since subsided, last appearing in FortiGuard's top 10 in February's Threat Landscape report.

Additional threat activities for the month of June:

- 200 Vulnerabilities: FortiGuard Labs covered more than 200 new vulnerabilities this period, nearly double from last report. This suggests that an increase in software vulnerabilities continue to be disclosed, ultimately available to hackers for malicious use.
- Flash and Excel Vulnerabilities: FortiGuard Labs discovered four Flash and Excel vulnerabilities, which were disclosed and patched this period. For more information see FortiGuard's Adobe and Microsoft advisories.
- Malicious JavaScript Code: In terms of malware, the only detection that topped the aforementioned botnet binaries was JS/Redir.BK -- obfuscated JavaScript code, which had a surge of activity on June 12 and June 13. The JavaScript code redirected users to various legitimate domains hosting an injected HTML page named "z.htm." FortiGuard observed JavaScript code was circulated through an HTML attachment in spam emails using various themes. In one attack, the HTML containing the malicious JavaScript code was attached as the file "open.htm" in an e-mail urging the user to update their MS Outlook client. The exact same e-mail also circulated with a FakeAV binary attachment, once again proving that spam templates are often recycled for various attacks. In another example, a "bad news" email socially engineered for the FIFA World Cup, had the same malicious JavaScript attached through a file named "news.html."

"There is no doubt that JavaScript is one of the most popular languages used today for attacks," Manky continued. "It is used in a growing number of poisoned document attacks (PDF), particularly with heap-spray based techniques. It's also used to launch exploits, and it is popular as a browser redirector to malicious sites, since the JavaScript code can be obfuscated and appear to be more complex than traditional IFrame based attacks from the past."

FortiGuard Labs compiled threat statistics and trends for June 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 June Threat Landscape report which includes the top threat rankings in each category, please visit:

http://www.fortiguard.com/report/roundup_june_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 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.

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

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

SOURCE: Fortinet

`mailto:rpopko@fortinet.com`

News Provided by COMTEX