Fortinet September Threat Landscape Report Shows PDF Vulnerability Used to Jailbreak iPhones

"Broken" Phones Then Susceptible to Malware Attacks

SUNNYVALE, CA, Sep 30, 2010 (MARKETWIRE via COMTEX News Network) -- Fortinet(R) (NASDAQ: FTNT) -- a leading network security provider and the worldwide leader of unified threat management (UTM) solutions -- today announced its September 2010 Threat Landscape report, which showed a new vulnerability that is being used to exploit Jailbroken Apple iPhones leveraging the PDF file format. Jailbreaking is typically done to circumvent digital rights management (DRM) in order to make the phone open to a greater number of applications.

"Once an iPhone, or any device, has been 'broken,' the door is open. The device may then execute code or function in a way it was not designed to do," said Derek Manky, project manager, cyber security and threat research, Fortinet. "In the case of malware attacks, the Ikee worm did precisely this last year: it relied on Jailbroken iPhones to gain unauthorized entry via SSH. Jailbroken devices can also run malicious applications, so it is plausible that a two-stage malware attack could occur."

QuickTime, Outlook and Acrobat Vulnerabilities Plugged

- Two vulnerabilities were patched for Apple QuickTime on September 15, one of which was discovered by FortiGuard Labs (FGA-2010-46). The other vulnerability (CVE-2010-1818) was a critical issue that bypassed Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR) protection technologies using QuickTime. Fortinet research has determined that there are in-the-wild flash samples actively trying to exploit this vulnerability. Patches can be downloaded here.
- Microsoft has issued security advisories for the Outlook Web Access Privilege Elevation Vulnerability and ASP.NET, which could allow information disclosure.
- Adobe has issued two zero-day security advisories for Adobe Reader/Acrobat and its Flash player.

Botnets Still Hot on the Malware Scene On September 14, FortiGuard Labs detected a surge in Sasfis activity that was linked to the Asprox spambot. While Asprox has been around for some time, it has been silent for more than a year. The Asprox module that was dissected was intended to be used for an email seeding campaign. The emails contained zipped executable attachments, disguised as fax copies. The attachment was a copy of Sasfis, which would download Asprox in order to send more spam on the freshly infected machine.

In addition to an increase in Sasfis activity, the FortiGuard Center downloaded a sniffer module that scans traffic on TCP ports 21, 25 and 110 (FTP, SMTP and POP3).

"Traffic on these ports would be processed by the module into encrypted data sets and sent via HTTP POST to a command and control server located in Europe," Manky continued. "Stolen FTP credentials can be quite valuable and are often used to hijack Web servers. The variant was also observed downloading the TotalSecurity ransomware suite, which has been high on our malware radar for a number of weeks."

FortiGuard Labs compiled threat statistics and trends for September 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 September Threat Landscape report which includes the top threat rankings in each category, please visit: http://www.fortiguard.com/report/roundup_september_2010.html. To view the monthly Security Minute videocast visit: http://www.youtube.com/watch?v=OjwO6SjXYDo.

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.

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 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