August 5, 2013

Fortinet(R)'s FortiGuard(R) Labs Reports a 30 Percent Increase in Mobile Malware in the Last Six Months; Seeing 1300 New Samples per Day

Team Reveals That Attackers Are Taking Advantage of Old Vulnerabilities, Despite Being Patched, in Ruby on Rails, Java, Acrobat and Apache

SUNNYVALE, CA -- (Marketwired) -- 08/05/13 -- Fortinet® (NASDAQ: FTNT) -- a world leader in high-performance network security -- today announced the findings of its FortiGuard threat landscape research for the period of January 1 - July 31, 2013. The complete report can be downloaded here: http://www.fortinet.com/resource_center/whitepapers/quarterly-threat-landscape-report-q213.html

Mobile Malware on the Rise
FortiGuard® Labs observed a 30 percent increase in mobile malware in the labs over the last six months. The team is now seeing more than 1,300 new samples per day, is currently tracking over 300 unique Android malware families and over 250,000 unique malicious Android samples. ***Figure 1*** shows the increase in mobile malware from January, 2013 through July, 2013.

Bring Your Own Trouble
The Bring Your Own Device (BYOD) phenomenon has many benefits for a business, chief among them are increased employee efficiency and productivity gains. However, the disadvantage of a lenient BYOD policy is the threat of mobile malware infecting the user's device and, subsequently, the business network.

"Three years ago, mobile malware wasn't much of a concern for users or businesses. Most malware at the time targeting smartphones and tablets were nothing more than annoyware such as the Cabir virus or scam software used to commit SMS fraud or replace icons," said Axelle Apvrille, senior mobile anti-virus researcher for Fortinet's FortiGuard Labs. "However, as devices have proliferated, so, too, have cybercriminals eager to capitalize on the growing user base, and our research shows the proliferation of mobile malware will not abate anytime soon."

Symbian Started it All
In 2009, the majority of mobile malware in existence targeted the Symbian OS, as iOS and Android were still relatively new in the marketplace. In addition, a large number of the malware was coded by programmers in Eastern Europe and China, places where Symbian commanded a large share of the user base. ***Figure 2*** shows which countries were distributing the most mobile malware in 2009. ***Figure 3*** shows which mobile operating systems were targeted most frequently in 2009.

2013 Changed the Mobile Threat Landscape
In 2013, the mobile threat landscape changed dramatically. Wide scale manufacturer adoption of Google's Android OS globally has led to an explosion of smartphones in the marketplace. Android devices are available in every market, at price levels from the incredibly inexpensive to feature-rich, cutting edge computing monsters. Coupled with the explosion of available applications to extend device functionality, cybercriminals and other nefarious types have used this platform as a new business opportunity.

Mobile Ransomware Has its Coming Out
In 2012, FortiGuard predicted that the financially lucrative ransomware would make its way onto mobile phones.

"Ransomware has been incredibly successful financially for cybercriminals, it's no surprise they've turned their attention to mobile devices," said Richard Henderson, security strategist for Fortinet's FortiGuard Labs. "The Fake Defender malware for Android follows the same M.O. as PC fake antivirus software -- it pretends to be altruistic, but in reality, it lies in wait to launch its true form. This malware then locks the victim's phone and demands payment before unlocking the device. Once the phone is locked, the victim can either pay the ransom or completely erase their device, losing all their photos and data unless they have a full backup elsewhere."

New Attacks on Old Vulnerabilities
Even though we've seen recent patches for Ruby on Rails, Java, Adobe Acrobat and Apache, FortiGuard Labs is finding attackers are still exploiting those old vulnerabilities.

Ruby on Rails
In January, it was announced that a critical vulnerability in the Ruby on Rails Framework could allow a remote attacker to execute code on the underlying Web server.

Ruby on Rails (RoR) is a Web application framework for the Ruby programming language. Put simply, it allows for rapid, easy and elegant deployment of "Web 2.0" Websites. RoR is a popular framework: hundreds of thousands of Websites online use RoR in some fashion.

Further adding to the problem, a Metasploit module was made available to scan for the vulnerability, making the ability to find a Web server to exploit a trivial matter.

"The exploit involved a flaw in the XML processor deserialization routine, which is used to create Ruby objects on the fly," said Henderson. "RoR was patched to correct the flaw, but four months later it was discovered that an attacker or attackers was searching for and exploiting, unpatched Web servers in order to infect them with software."

Java Remote Code Execution
In January, a zero-day exploit that was able to bypass Java's sandbox and run arbitrary Java code was discovered.

Java is a ubiquitous technology online -- most computers have some form of Java installed and enabled. The vulnerability allowed a malicious applet to run any Java program, bypassing Java's sandbox and granting full access to the vulnerable computer.

Attacks were discovered in the wild and the exploit was quickly integrated into many popular crimeware attack kits, such as BlackHole, Redkit and Nuclear Pack, giving purchasers of these kits the ability to take advantage of the exploit and install malware on computers. A Metasploit module was also created for the vulnerability, making the ability to find victims a simple point and click affair.

"The exploit involved a flaw in a JMX (Java Management Extensions) component that allowed the malicious applet to elevate its privileges and run any Java code it wished," Henderson said.

Oracle was quick to release a patch for the flaw -- but similar to other exploits integrated into crimeware kits, many new victims were found -- and continue to be found -- running unpatched versions of Java, allowing malware to be installed.

Acrobat/Acrobat Reader Zero-Day in the Wild
In February, a PDF pretending to be a travel visa form from Turkey was detected circulating in the wild and took advantage of a previously unseen vulnerability in Adobe's Reader software. The exploit worked with all recent versions of Adobe Reader (9.5.X, 10.1.X, and 11.0.X), and on most versions of Microsoft Windows, including 64-bit Windows 7 and most Mac OS X systems.

The exploit PDF was used by cybercriminals in order to install malware on their target's computers.

Adobe released a patch for the flaws in Reader on February 20th, but cybercriminals continue to use repackaged versions of the exploits online in spear-phishing attacks. These exploits in Adobe's Reader software continue to be actively exploited by cybercriminals as a malware delivery method, taking advantage of users who don't expeditiously patch their computers.

CDorked Attacks Apache
In late April, a new attack on the popular Apache Web server was discovered. Dubbed CDorked, the malware was able to compromise the Web server and redirect visitors of the compromised Web server to other servers that deliver malware using the BlackHole exploit kit. The attack may also have targeted the Lighttpd and Nginx Web server platforms.

CDorked shows many similarities to 2012's DarkLeech attack on Apache servers, but is significantly stealthier and smarter than DarkLeech was: unlike DarkLeech, CDorked didn't load additional malicious modules on the infected server; instead it maliciously modified the existing httpd binary.

CDorked was interesting in that it did not write any information to the Web server's hard drive: everything was kept in memory and was accessed via obfuscated GET requests sent by the attackers to the compromised server. None of those GET requests were logged.

CDorked showed some intelligence in how it operated.

"It had a quota system built in," Henderson said. "In other words, CDorked did not attempt to redirect each and every visitor to a BlackHole site. It also hid from users attempting to access administrative pages on the compromised Web server in an attempt to keep users who may have been more likely to notice a redirect to a crimeware delivery site from discovering the compromise. CDorked isn't alone though: other malicious malware have intelligence built-in to watch for malware analysts and other White Hat hackers."

Follow Fortinet Online: Twitter at: www.twitter.com/fortinet; Facebook at: www.facebook.com/fortinet; YouTube at: http://www.youtube.com/user/SecureNetworks.

About FortiGuard Labs
FortiGuard Labs compiled threat statistics and trends for this threat period based on data collected from FortiGate® network security appliances and intelligence systems in production worldwide. Customers who use Fortinet's FortiGuard Services should be protected against the vulnerabilities outlined in this report as long as the appropriate configuration parameters are in place.

FortiGuard 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™ and FortiClient™ products.

Ongoing research can be found in the FortiGuard Center or via FortiGuard Labs' RSS feed. Additional discussion on security technologies and threat analysis can be found at the FortiGuard Blog.

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 2012 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.
408-486-7853
rpopko@fortinet.com

Investor Contact:
Michelle Spolver
Fortinet, Inc.
408-486-7837
mspolver@fortinet.com

Source: Fortinet

News Provided by Acquire Media