February 4, 2013

Fortinet(R)'s FortiGuard Threat Landscape Research Team Reports Four Samples of Money Making Malware to Watch for in 2013

Team Also Identifies an Increase in Mobile Advertising Malware Toolkits and in Hacktivist Web Server Vulnerability Scanning

SUNNYVALE, CA -- (Marketwire) -- 02/04/13 -- 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 October 1 - December 31, 2012. FortiGuard® Labs has highlighted malware samples that show four typical methods cyber criminals are using today to extract money from their victims. In addition, the report shows increasing activity in mobile malware variants of the Android Plankton ad kit as well as in hacktivist Web server vulnerability scanning.

Four Money Making Malware to Watch for in 2013
In the last three months, FortiGuard Labs has identified four pieces of malware that spiked, showing high levels of activity within a very short period of time (from a day to a week). The following examples reflect four typical methods cyber criminals are using today to monetize their malware:

1. Simda.B: This sophisticated malware poses as a Flash update in order to trick users into granting their full installation rights. Once installed, the malware steals the user's passwords, allowing cybercriminals to infiltrate a victim's email and social networking accounts to spread spam or malware, access Website admin accounts for hosting malicious sites and siphoning money from online payment system accounts.

2. FakeAlert.D: This fake antivirus malware notifies users via a convincing-looking pop-up window that their computer has been infected with viruses, and that, for a fee, the fake antivirus software will remove the viruses from the victim's computer.

3. Ransom.BE78: This is ransomware, a frustrating piece of malware that prevents users from accessing their personal data. Typically the infection either prevents a user's machine from booting or encrypts data on the victim's machine and then demands payment for the key to decrypt it. The main difference between ransomware and fake antivirus is that ransomware does not give the victim a choice regarding installation. Ransomware installs itself on a user's machine automatically and then demands payment to be removed from the system.

4. Zbot.ANQ: This Trojan is the "client-side" component of a version of the infamous Zeus crime-kit. It intercepts a user's online bank login attempts and then uses social engineering to trick them into installing a mobile component of the malware on their smartphones. Once the mobile element is in place, cybercriminals can then intercept bank confirmation SMS messages and subsequently transfer funds to a money mule's account.

"While methods of monetizing malware have evolved over the years, cybercriminals today seem to be more open and confrontational in their demands for money -- for faster returns," said Guillaume Lovet, senior manager of FortiGuard Labs' Threat Response Team. "Now it's not just about silently swiping passwords, it's also about bullying infected users into paying. The basic steps users can take to protect themselves, however, have not changed. They should continue to have security solutions installed on their computers, update their software diligently with the latest versions and patches, run regular scans and exercise common sense."

Android Mobile Advertising Malware
In the last threat landscape report, FortiGuard Labs detected a surge in the distribution of the Android Plankton ad kit. This particular piece of malware embeds a common toolset on a user's android device that serves unwanted advertisements in the user's status bar, tracks the user's International Mobile Equipment Identity (IMEI) number and drops icons on the device's desktop.

In the last three months, the kit's activity plunged. In its place, FortiGuard Labs has detected the rise of ad kits that appear to be directly inspired by Plankton and have approached the same elevated activity level Plankton was operating at three months ago.

"The ad kits we've monitored suggest that Plankton's authors are trying to dodge detection. Either that, or competing ad kit developers are trying to take a piece of the lucrative adware cake. Either way, the level of activity we're seeing with ad kits today suggests that Android users are highly targeted and thus should be especially vigilant when downloading apps to their smartphones," said Lovet.

Users can protect themselves by paying close attention to the rights asked by an application at the point of installation. It is also recommended to download mobile applications that have been highly rated and reviewed.

Hacktivist Scanning Tool Goes Into Overdrive
In the third quarter of 2012, FortiGuard Labs detected high activity levels of ZmEu, a tool that was developed by Romanian hackers to scan Web servers running vulnerable versions of the mySQL administration software (phpMyAdmin) in order to take control of those servers. Since September, the activity level has risen a full nine times before finally levelling off in December.

"This activity spike suggests a heightened interest by hacktivist groups to facilitate various protests and activist movements around the world. We expect such scanning activity to remain high as hacktivists pursue an ever-increasing number of causes and publicise their successes," Lovet continued.

To secure Web servers against this threat, FortiGuard Labs recommends updating to the latest version of PhPMyAdmin.

Visit the Fortinet FortiGuard Researchers at RSA
Fortinet will be participating at the upcoming RSA security conference, which is taking place February 25 - March 1 at San Francisco's Moscone Center. Stop by booth #2025, meet the members of the FortiGuard research team, see a demonstration of the lab's latest threat intelligence services and receive a free USB wristband.

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.

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

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 Contacts:

Rick Popko

Fortinet

408-486-7853

rpopko@fortinet.com

Source: Fortinet