FORTINET

December 10, 2012

Fortinet's FortiGuard Labs Reveals 2013 Threat Predictions

Expected Trends Include Mobile Advanced Persistent Threats, IPv6 Safe Havens and Exploits Through Machine-to-Machine Communications

SUNNYVALE, CA -- (Marketwire) -- 12/10/12 -- Fortinet® (NASDAQ: FTNT) -- a world leader in high-performance network security -- today revealed FortiGuard Labs' 2013 threat predictions, highlighting six threats to watch out for next year.

Top 6 Security Predictions for 2013

1. *APTs Target Individuals through Mobile Platforms*
APTs also known as Advanced Persistent Threats are defined by their ability to use sophisticated technology and multiple methods and vectors to reach specific targets to obtain sensitive or classified information. The most recent examples include Stuxnet, Flame and Gauss. In 2013 we predict we'll see APTs targeted at the civilian population, which includes CEOs, celebrities and political figures. Verifying this prediction will be difficult, however, because after attackers get the information they're looking for, they can quietly remove the malware from a target device before the victim realizes that an attack has even occurred. What's more, individuals who do discover they have been victims of an APT will likely not report the attack to the media. Because these attacks will first affect individuals and not directly critical infrastructure, governments or public companies, some types of information being targeted will be different. Attackers will look for information they can leverage for criminal activities such as blackmail; threatening to leak information unless payment is received.

2. *Two Factor Authentication Replaces Single Password Sign on Security Model*
The password-only security model is dead. Easily downloadable tools today can crack a simple four or five character password in only a few minutes. Using new cloud-based password cracking tools, attackers can attempt 300 million different passwords in only 20 minutes at a cost of less than $20 USD. Criminals can now easily compromise even a strong alpha-numeric password with special characters during a typical lunch hour. Stored credentials encrypted in databases (often breached through Web portals and SQL injection), along with wireless security (WPA2) will be popular cracking targets using such cloud services. We predict next year we'll see an increase in businesses implementing some form of two-factor authentication for their employees and customers. This will consist of a Web-based login that will require a user password along with a secondary password that will either arrive through a user's mobile device or a standalone security token. While it's true that we've seen the botnet Zitmo recently crack two-factor authentication on Android devices and RSA's SecurID security token (hacked in 2011), this type of one-two punch is still the most effective method for securing online activities.

3. Exploits to Target Machine-to-Machine (M2M) Communications
Machine-to-machine (M2M) communication refers to technologies that allow both wireless and wired systems to communicate with other devices of the same ability. It could be a refrigerator that communicates with a home server to notify a resident that it's time to buy milk and eggs, it could be an airport camera that takes a photo of a person's face and cross references the image with a database of known terrorists, or it could be a medical device that regulates oxygen to an accident victim and then alerts hospital staff when that person's heart rate drops below a certain threshold. While the practical technological possibilities of M2M are inspiring as it has the potential to remove human error from so many situations, there are still too many questions surrounding how to best secure it. We predict next year we will see the first instance of M2M hacking that has not been exploited historically, most likely in a platform related to national security such as a weapons development facility. This will likely happen by poisoning information streams that transverse the M2M channel -- making one machine mishandle the poisoned information, creating a vulnerability and thus allowing an attacker access at this vulnerable point.

4. Exploits Circumvent the Sandbox
Sandboxing is a practice often employed by security technology to separate running programs and applications so that malicious code cannot transfer from one process (i.e. a document reader) to another (i.e. the operating system). Several vendors including Adobe and Apple have taken this approach and more are likely to follow. As this technology gets put in place, attackers are naturally going to try to circumvent it. FortiGuard Labs has already seen a few exploits that can break out of virtual machine (VM) and sandboxed environments, such as the Adobe Reader X vulnerability. The most recent sandboxing exploits have either remained in stealth mode (suggesting that the malware code is still currently under development and test) or have actively attempted to circumvent both technologies. Next year we expect to see innovative exploit code that is designed to circumvent sandbox environments specifically used by security appliances and mobile devices.

5. Cross Platform Botnets
In 2012, FortiGuard Labs analyzed mobile botnets such as Zitmo and found they have many of the same features and functionality of traditional PC botnets. In 2013, the team predicts that thanks to this feature parity between platforms, we'll begin

to see new forms of Direct Denial of Service (DDoS) attacks that will leverage both PC and mobile devices simultaneously. For example, an infected mobile device and PC will share the same command and control (C&C) server and attack protocol, and act on command at the same time, thus enhancing a botnet empire. What would once be two separate botnets running on the PC and a mobile operating system such as Android will now become one monolithic botnet operating over multiple types of endpoints.

6. Mobile Malware Growth Closes in on Laptop and Desktop PCs
Malware is being written today for both mobile devices and notebook/laptop PCs. Historically, however, the majority of development efforts have been directed at PCs simply for the fact that there are so many of them in circulation, and PCs have been around a much longer time. For perspective, FortiGuard Labs researchers currently monitor approximately 50,000 mobile malware samples, as opposed to the millions they are monitoring for the PC. The researchers have already observed a significant increase in mobile malware volume and believe that this skewing is about to change even more dramatically starting next year. This is due to the fact that there are currently more mobile phones on the market than laptop or desktop PCs, and users are abandoning these traditional platforms in favor of newer, smaller tablet devices. While FortiGuard Labs researchers believe it will still take several more years before the number of malware samples equals what they see on PCs, the team believes we are going to see accelerated malware growth on mobile devices because malware creators know that securing mobile devices today is currently more complicated than securing traditional PCs.

2013 Threat Predictions Webcast
FortiGuard Labs' senior security strategist, Derek Manky and Fortinet product manager, Kevin Flynn, will host a free 2013 Threat Predictions WebEx presentation at 11:00 a.m. on December 12. In this Webcast, participants are expected to gain a better understanding of what they can expect in the world of cyber security over the next twelve months. Participants will have the opportunity to ask questions and learn what steps they can take to safeguard their information.
Login details can be found here: https://fortinet.webex.com/fortinet/onstage/g.php?t=a&d=572900199
Event Number: 572 900 199

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.

Last year's threat predictions can be found here. Ongoing research can be found in the FortiGuardCenter or via FortiGuard Labs' RSS feed. Additional discussion on security technologies and threat analysis can be found at the Fortinet Security Blog.

Follow Fortinet Online: Subscribe to threat landscape reports: http://blog.fortinet.com/feed/; 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 2011 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.

other binding commitment by Fortinet, and performance and other specification information herein may be unique to certain environments. This news release may contain forward-looking statements that involve uncertainties and assumptions. Changes of circumstances, uncertainties inherent in predictions, product release delays or other risks as stated in our filings with the Securities and Exchange Commission, located at www.sec.gov, may cause results to differ materially from those expressed or implied in this press release and the predictions herein may not come to pass. 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. Fortinet assumes no obligation to update any forward-looking statements, and expressly disclaims any obligation to update these forward-looking statements.

FTNT-O

Add to Digg Bookmark with del.icio.us Add to Newsvine

Media Contacts:

Rick Popko

Fortinet, Inc.

408-486-7853

rpopko@fortinet.com

Source: Fortinet

News Provided by Acquire Media