November 25, 2013

Fortinet's FortiGuard Labs Reveals Top 10 Threat Predictions for 2014

Expected Trends Include Android Malware Migrating to Industrial Control Systems, Cybercriminals Battling It Out in the Deep Web and New Exploits Targeting Home Devices

SUNNYVALE, CA -- (Marketwired) -- 11/25/13 -- Fortinet® (NASDAQ: FTNT) -- a global leader in high-performance network security -- today revealed FortiGuard Labs' 2014 threat predictions, highlighting 10 threats to watch out for next year.

Top 10 Threat Predictions for 2014

1. Android Malware Expands to Industrial Control Systems and Internet of Things
As sales of mobile phones likely plateau in the coming years, Android developers are being tasked to find untapped markets for the Google operating system. A few of these emerging markets include tablets, portable game consoles, wearable devices, home automation equipment and industrial control systems (ICS/SCADA). Next year, we predict we'll see the first instances of malware on these new device types, specifically around embedded ICS/SCADA systems. While we don't believe we'll see a "mobile-Stuxnet" in 2014, we think cybercriminals will be attracted to platforms that go beyond common SMS fraud. This includes new home automation devices that have control over our electrical consumption, the temperature of our fridges, etc. and feature software with remote login control panels to show/confirm who may be at home at a given time. This is bound to give cybercriminals new and nefarious ideas around how and when to rob someone's home.

2. Encryption Won't Change, but Use of Encryption Will Increase
Despite the hype around super computers or quantum computers, encryption algorithms and cryptography is unlikely to change next year. However, while the general population will fail to use any form of encryption in their daily lives, we predict for 2014 an uptick in use of encryption based on fears that critical data and intellectual property could be easily compromised or stolen through strategically-placed malware or governmental eavesdropping programs such as PRISM or XKeyScore.

3. FBI in Conjunction with Global Cyber Security Agencies to Shut Down Botnet Operators
This year we saw the FBI take down Silk Road and, in conjunction with the NSA, basically declare war on the Tor dark net. The FBI in partnership with other global cyber security agencies have been felt from Dublin, when earlier this year when the agency cracked the world's largest facilitator of child pornography to Denmark, where they may have helped the Dutch crack a banking malware gang that swindled $1.4 million from unsuspecting consumers. Next year, we predict the FBI along with agencies such as the Dutch National High Tech Crime Unit, national CERTs such as KISA, along with frameworks such as FIRST and ITU-IMPACT will continue to wield their influence on a global scale. We expect to see these agencies broaden their scope beyond the dark net to go after a broader set of global cyber targets, such as botnet operators and individuals selling cybercrime services.

4. The Battle for the Deep Web
While the FBI will broaden its scope of targets in the coming year, we believe the agency will also continue to make inroads into the Tor dark net and questionable file sharing services such as Mega Upload. Knowing the cat and mouse games black and white hats have been playing since the dawn of the first computer viruses, we predict the increased scrutiny of these "anonymous" services will lead to new and, dare we say, improved versions that will be even harder to infiltrate, compromise and/or take down. We've already seen the MegaUpload takedown birth Mega, a fundamentally more robust platform. Expect to see similar renewed development vigor around Silk Road in the coming year.

5. New Exploits Target Off-Net Devices to Penetrate Corporate Resources
The increased maturity of desktop exploit and advanced mitigation tools in the enterprise, such as malware sandboxing and next-generation antivirus, makes penetrating corporate networks a substantive challenge. The increased difficulty hackers are having penetrating today's enterprise firewalls, will force them to take more creative approaches into networks or devices that are traditionally not hardened compared to the corporate network. These soft targets can include home routers, smart televisions, home automation and/or set top box connections. Taking a page from the NSA, an agency that generally targets infrastructure over desktops, we predict we'll see the first generic exploitation frameworks and mass malware agents for these types of home devices later next year.

6. Network Security Vendors Forced to Become More Transparent
In September, the Federal Trade Commission severely penalized a company that marketed video monitoring technology to consumers for suggesting in its literature that their product was "secure" when evidence clearly showed it was not. This was the agency's first action against a marketer of an everyday product with interconnectivity to the Internet and other mobile devices, and the company was required to make a number of conciliatory measures. Next year, we predict we'll see this level of

increased scrutiny and accountability at the network security vendor level. Customers are no longer going to accept the "proprietary security-hardened OS" marketing spin. They will demand proof, and when they are subject to undue risk, they will demand accountability. This will be in the form of greater transparency around supply chain management, patch management and Secure Development Lifecycle (SDL) practices.

7. More Botnets Will Migrate From Traditional Command and Control (CnC) Servers to Peer-to-Peer (P2P) Networks
Traditional botnets use client-server (CS) mode to communicate with a CnC server. When a server is detected and taken down, the whole network collapses, making it difficult for bot herders to re-ignite compromised machines. P2P mode takes the servers out of the equation. Each PC in a P2P network could play a server or client role, thus making the botnet harder to dismantle. Major botnets that have migrated to this new model include ZeroAccess, Kelihos, Bublik and Zeus v3. Next year we predict that number to rise significantly.

8. More Botnets Will Cross Breed with Other Botnets
Historically, botnets worked alone. In rare instances, when a botnet such as TDSL infected a computer, the first thing it did was to look for traces of other botnets running on the same PC and remove them, thus preventing the compromised computer from becoming too unstable. In time, botnet creators became better at hiding their malware on machines, which made competing botnet detection and removal increasingly more difficult. Rather than compete against other botnets, the trend we're seeing is botnets actually joining forces with other botnets in order to better grow their bases of infected users. We saw the first instance of this back in 2009 with Virut. This year we're seeing an uptick in this type of activity, with the Andromeda, Bublik, Dorkbot, Fareit, and ZeroAccess botnets doing just that. Next year, we predict we'll see even more botnets sharing their infected user base for cross infection purposes.

9. Increase in attacks targeting Windows XP
Microsoft will end support for Windows XP on April 8, 2014. This means that newly discovered vulnerabilities will not be patched, leaving systems around the world vulnerable to attacks. According to NetMarketShare, as of September 2013, Windows XP is still used on 31.42% of PCs in the world. According to Gartner, by the time April 8 rolls around, it is estimated that more than 15% of mid- to large-sized enterprises will still have Windows XP running on at least 10 percent of their PCs. Next year, we predict hackers, already in possession of zero day exploits, will wait until the 8*th* in order to sell them to the highest bidder. Because of their expected high price tag, these zero days will likely be used to launch targeted attacks against high-value businesses and individuals rather than deployed by common cybercriminals in order to propagate mass infections.

10. Biometrics for authentication will increase
This year Apple made a bold move when it announced its new iPhone 5s would integrate fingerprint authentication into the device. Never mind that it was hacked a few days after the phone shipped. It got people talking about the importance two-factor authentication in a world where the single factor password login is growing increasingly archaic. As a result of this renewed interest, we predict next year we'll see additional mobile companies including a second factor of authentication into their devices. We'll also see an increase in additional forms of authentication, such as tattoos and pills, iris scanning and facial recognition.

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.

Last year's threat predictions can be found here. 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
LinkedIn at: http://www.linkedin.com/company/fortinet
G+ at: https://plus.google.com/+fortinet

About Fortinet
Fortinet (NASDAQ: FTNT) helps protect networks, users and data from continually evolving threats. As a global leader in high-

performance network security, we enable businesses and governments to consolidate and integrate stand-alone technologies without suffering performance penalties. Unlike costly, inflexible and low-performance alternatives, Fortinet solutions empower customers to embrace new technologies and business opportunities while protecting essential systems and content. Learn more at www.fortinet.com.

Copyright © 2013 Fortinet, Inc. All rights reserved. The symbols ® and ™ 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, FortiAP, FortiDB, FortiVoice 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. Notwithstanding anything to the contrary herein, nothing herein constitutes a warranty, guarantee, binding specification or other binding commitment by Fortinet, and performance and other specification information herein may be unique to certain environments. This news release contains forward-looking statements that involve uncertainties and assumptions. Changes of circumstances, 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. 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

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