December 3, 2014

Cyber Threats to Increase in Scope and Complexity in the New Year as Black Hat Hackers Become More Sophisticated, According to Fortinet 2015 Threat Predictions

FortiGuard Labs Researchers Anticipate Increase of Vulnerabilities, IoT Attacks, Denial of Revenue and Counter Threat Intelligence Exploits that Could Impact Multiple Industries and Governments Globally

SUNNYVALE, CA -- (Marketwired) -- 12/03/14 -- As the 2015 New Year looms, Fortinet® (NASDAQ: FTNT), a global leader in high-performance network security, and its threat research division FortiGuard Labs, have taken a look ahead to determine the most significant cyber security threats of the upcoming New Year -- both from the perspective of a Black Hat hacker, as well as a Threat Intelligence solutions vendor. As the number of devices connected to the network increases, cyber criminals will continue to hone their prowess when it comes to IoT attacks and advanced evasion techniques, while also continuing to exploit large-scale server side vulnerabilities for financial gains and other nefarious purposes. Businesses and government organizations globally are at risk, as are consumers' important personal information.

Significant trends and cyber security threats from the perspective of a black hat hacker in 2015 include:

- ***Blastware to Destroy Systems, Erase Data and Cover Hacker Tracks***
  This destructive new trend of malware, following Scareware and Ransomware could lead to the ability for hackers to infiltrate systems, gather data and then wipe out the information on systems and hard drives to cover tracks and thwart forensics. FortiGuard Labs observed the first indications of Blastware in 2014, Dorkbot/NGRbot, where the hackers had code routines built in, that if altered, would self-destruct and wipe out all information on the hard drive. This is a direct counter response to the rise of incident response services. FortiGuard predicts that APT (advanced persistent threat) developers will build in sophisticated self-destruct mechanisms in seek-and-destroy fashion that could hamper law enforcement and forensics efforts as these resources increase to fight cyber crime. Hackers may also seek to use these tactics for ransom -- i.e. to destroy data if ransom isn't paid in a certain timeframe.

- ***Hackers Look to Evade Law Enforcement, Frame the Innocent***
  As cyber crime increases, law enforcement practices to catch and penalize perpetrators increase with it. Thus, hackers must be more careful and calculated to evade arrest. In 2015, advanced evasion techniques will evolve in order for attackers to cover their tracks. To date, evasion has been currently focused on counter antivirus and intrusion prevention/antibotnet. Fortinet predicts this will evolve with a focus on Sandbox evasion. In addition, similar to counter intelligence, it is possible that attackers will frame the innocent by throwing more red herrings into their attacks to thwart investigators and intentionally planting evidence that point to an unassociated attacker.

- ***Internet of Things Becomes Internet of Threats (IoT)***
  In 2014, we saw an interesting shift -- namely Heartbleed and Shellshock -- focused on server side vulnerability and exploitation. Looking forward to 2015, we fully expect this trend to continue in an alarming way as black hat hackers pry open the Internet of Things. Hackers will continue to follow the path of least resistance as more and more devices are connected to the network. Vulnerabilities that Black Hat hackers will look to exploit will include Consumer home automation and security systems, as well as webcams, which we are already beginning to see. On the Enterprise side, Network Attached Storage and Routers will continue to be targets, as will critical infrastructure such as Human Machine Interfaces (HMI) and Supply Chain systems, which will create significant problems with third-party components and patch management. Common malware distributed and sold will include SCADA functionality, such as Havex's OPC routine that would fingerprint devices used in industrial networks, and report this back to users.

- ***Denial of Revenue/Data Breaches Continue and Expand***
  2014 is becoming known as the "year of the data breach," with significant thefts from stores like Target, Michaels, P.F. Changs and Home Depot. FortiGuard predicts this trend will continue in 2015 as hackers become more sophisticated and find new loopholes for infiltrating retail and financial systems. In the New Year, damages will also extend to denial of service on assembly line, factory, industrial control systems, ERP/SAP systems, as well as healthcare and building management, creating even more challenges in the way of critical consumer data compromises, revenue losses and reputation damages for organizations globally.

- ***Rise in Counter Threat Intelligence***
  Crime services and solutions have already supported QA for malware, including sample scanning. FortiGuard predicts this to extend to support QA for threat intelligence and undetected coverage for indicator of compromise (IOC) in 2015. As crime services extend their research and coverage, hackers will utilize the same type of processes for determining the best ways to bypass security systems. For example, current crime services scan malware against vendors' capabilities to stop it, and give them a score result. As vendors expand from malware detection to threat intelligence correlation,

criminals will work to counter this movement with the same type of approaches to find out if their botnet infrastructure is flagged in other intelligence systems as well, and work to hide their tracks.

Actions Threat Intelligence and Network Security vendors must take in order to protect against new threats:

- ***Actionable Threat Intelligence***
  Security vendors are overloaded with threat intelligence, but technology must integrate to automate protection against that intelligence and not rely on administrative decision. In 2015, cyber security vendors and managed security solutions will make an even greater push toward actionable threat intelligence, with proactive services that filter data that matters and alerts clients to their potential vulnerabilities and protection measures, prior to an attack. A vendor's ability to ensure interoperability between different security products as well as networking, computer, storage and end devices on the network will be a key to success, by helping to create a "self-healing" network.

- ***Proactive Incident Response***
  Incident response to date has generally been reactive. Moving forward, proactive response will significantly reduce damages that organizations will face in the future. The selection of third-party vendors that provide more secure development through Product Security Incident Response teams (PSIRT), as well as deep threat research, will limit breach scenarios before they happen. Two-factor strong authentication will increase in 2015 as one simple and cost effective proactive measure, while vendor incident response services will grow to help clients when they are under attack.

"FortiGuard Labs has been monitoring and detecting cyber threats for over a decade, to ensure Fortinet customers are protected and the industry at large is more aware of looming dangers," said Derek Manky, global security strategist at Fortinet. "Our white hat threat researchers step into the black hat world on a daily basis and think in tandem with the enemy, to help protect against the enemy. In 2014, we saw an interesting shift focused on server side vulnerability and exploitation with the likes of Heartbleed, Shellshock. Looking forward to 2015, we fully expect this trend to continue in an alarming way as black hat hackers pry open the Internet of Things. As threats continue to evolve, organizations are at even greater risk. It is imperative they choose not just a security solution, but a proactive and intelligent solution, to protect them from the breadth and depth of growing attacks that firewall solutions alone will not stop."

About FortiGuard Labs
The FortiGuard Labs global research team continuously monitors the evolving threat landscape and distributes on a daily basis to Fortinet customers worldwide preventative measures to protect those customers from newly introduced, sophisticated cyber-threats. More than 200 researchers and automated detection and prevention technology provide around-the-clock coverage to ensure your network stays protected, despite a sophisticated and ever-changing threat landscape. FortiGuard Labs delivers rapid updates and detailed security knowledge, providing protection from the latest threats.

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 broad, high functioning security to prevent cyber-attacks, 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, or follow Fortinet at the Fortinet Blog, Google+, Linkedin or Twitter.

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 may contain 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

Stefanie Hoffman
Fortinet, Inc.
408-486-5416
shoffman@fortinet.com

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

Source: Fortinet

News Provided by Acquire Media