November 21, 2016

Fortinet Predicts Tipping Point For Cybersecurity as Threats Become More Intelligent, Autonomous, and Difficult to Detect Than Ever Before in 2017

Evolution of Threat Landscape Creates Urgency for Increased Security Accountability at Multiple Levels to Avoid Impact to Global Digital Economy

SUNNYVALE, CA -- (Marketwired) -- 11/21/16 -- ***Derek Manky, global security strategist, Fortinet***
"The expanding attack surface enabled by technology innovations such as cloud computing and IoT devices, a global shortage of cybersecurity talent, and regulatory pressures continue to be significant drivers of cyber threats. The pace of these changes is unprecedented, resulting in a critical tipping point as the impact of cyber attacks are felt well beyond their intended victims in personal, political, and business consequences. Going forward, the need for accountability at multiple levels is urgent and real affecting vendors, governments, and consumers alike. Without swift action, there is a real risk of disrupting the progress of the global digital economy."

News Summary
Fortinet® (NASDAQ: FTNT), the global leader in high-performance cybersecurity solutions, today unveiled six predictions from the FortiGuard Labs threat research team about the threat landscape for 2017. These predictions reveal the methods and strategies that Fortinet researchers anticipate cyber criminals will employ in the near future and demonstrate the potential impact of cyber attacks to the global digital economy. For a detailed view of the 2017 predictions visit our blog. Highlights of the predictions follow:

1. From smart to smarter: automated and human-like attacks will demand more intelligent defense
Threats are getting smarter and are increasingly able to operate autonomously. In the coming year we expect to see malware designed "human-like" with adaptive, success-based learning to improve the impact and efficacy of attacks.

2. IoT manufacturers will be accountable for security breaches
If IoT manufacturers fail to better secure their devices, the impact on the digital economy could be devastating should consumers begin to hesitate to buy them out of cybersecurity fears. We will see an increase in the call to action from consumers, vendors and other interest groups for the creation and enforcement of security standards so that device manufacturers are held accountable for their device's behaviors out in the wild.

3. 20 billion IoT devices are the weakest link for attacking the cloud
The weakest link in cloud security is not in its architecture. It lies in the millions of remote devices accessing cloud resources. We expect to see attacks designed to exploit endpoint devices, resulting in client side attacks that can effectively target and breach cloud providers. Organizations will increasingly adopt fabric-based security and segmentation strategies that enable them to create, orchestrate, and enforce seamless security policies between their physical, virtual, and private cloud environments from IoT to the cloud.

4. Attackers will begin to turn up the heat in smart cities
As building automation and management systems continue to grow over the next year they will be targeted by hackers. The potential for massive civil disruption should any of these integrated systems be compromised is severe, and are likely to be a high-value target for cybercriminals.

5. Ransomware was just the gateway malware
We expect to see very focused attacks against high-profile targets, such as celebrities, political figures, and large organizations. Automated attacks will introduce an economy of scale to ransomware that will allow hackers to cost-effectively extort small amounts of money from large numbers of victims simultaneously, especially by targeting IoT devices.

6. Technology will have to close the gap on the critical cyber skills shortage
The current shortage of skilled cybersecurity professionals means that many organizations or countries looking to participate in the digital economy globally will do so at great risk. They simply do not have the experience or training necessary to develop a security policy, protect critical assets that now move freely between network environments, or identify and respond to today's more sophisticated attacks.

Threat Predictions Trends and Take-Aways
The Internet of Things (IoT) and cloud continue to play heavily in the predictions but a few trends have become apparent. The digital footprint of both businesses and individuals has expanded dramatically, increasing the potential attack surface.

Additionally, everything has become a target and anything can be a weapon. Threats are becoming more intelligent, operate autonomously, and are increasingly difficult to detect. Lastly, old threats keep returning, but enhanced with new technologies that push the boundaries of detection and forensic investigation.

Additional Resources

- Read a complete overview of the 2017 predictions on the Fortinet blog.
- Visit our website for more details about how Fortinet's Security Fabric can deliver integrated, high-performance security across the IT infrastructure from IoT to the cloud in 2017.
- Follow Fortinet on Twitter, LinkedIn, and Facebook.

About FortiGuard Labs

FortiGuard Labs consists of more than 200 expert researchers and analysts around the world. The researchers work with world class, in-house developed tools and technology to study, discover, and protect against breaking threats. The team has dedicated experts studying every critical area including malware, botnets, IoT, and zero-day vulnerabilities. Service analysts study breaking code and develop mitigation signatures while technology developers continually create new defense engines to combat continually evolving threats. FortiGuard Labs uses data collected from more than two million sensors around the globe to protect more than 290,000 customers every day.

About Fortinet

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network -- today and into the future. Only the Fortinet Security Fabric architecture can deliver security without compromise to address the most critical security challenges, whether in networked, application, cloud or mobile environments. Fortinet ranks #1 in the most security appliances shipped worldwide and more than 290,000 customers trust Fortinet to protect their businesses. Learn more at http://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.

FTNT-O

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, such as statements regarding technology releases. 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.

Media Contact
John Welton
Fortinet, Inc.
408-235-7700
Email contact

Investor Contact
Michelle Spolver
Fortinet, Inc.
408-486-7837
Email contact

Analyst Contact
Ron Davis
Fortinet, Inc.

415-806-9892
Email contact

Source: Fortinet

News Provided by Acquire Media