FORTINET

August 2, 2016

Fortinet FortiGuard Labs Cites Increased Cyber Threat Activity in Brazil Deserving Special Attention in Coming Weeks

Global Cybersecurity Threat Report Provides Research on Advanced Threat Techniques and Data on Cyber Threats in the Wild With Overall Volume Remaining High

LAS VEGAS, NV -- (Marketwired) -- 08/02/16 -- ***Black Hat USA 2016 -***

Ladi Adefala, Senior Security Strategist, Fortinet

"The expanding attack surface enabled by technology innovation, new IoT devices, regulatory pressures, and a global shortage of cybersecurity talent continue to drive cyber threats. All of these elements combined with global political events add more complexity to the situation and complexity is the enemy of security. Simply deploying security point solutions end-to-end is not enough. Organizations need to adopt a Security Fabric that will enable direct communication between solutions for a unified and rapid response to advanced threats."

News Summary:

Fortinet® (NASDAQ: FTNT) -- the global leader in high-performance cyber security solutions -- today announced the findings of its FortiGuard Labs cyber threat landscape global report.

Report Overview and Highlights:

- The report cites increased threat activity in Brazil and explains why it deserves special attention ahead of the Rio Olympics.
- Identifies the top phishing countries, as well as top malware, botnets, and exploit kits found around the globe.
- Ilustrates the trending of a sophisticated method to help attackers persist inside systems they have breached called "behavior blending."
- The threat data used in the analysis is based on a subset of telemetry data for the months of April, May and June 2016.
- The risk and threat implications contained in the report are illustrated using FortiGuard's industry-leading threat data, research and analysis. FortiGuard Labs uses data collected from more than two million sensors around the globe to protect more than 280,000 customers every day.

Increased Threat Activity in Brazil

- The volume of malicious and phishing artifacts (i.e. domain names and URLs) in Brazil is on the rise. In June, Brazil's percentage increase was higher in three of four categories in Fortinet's report when compared with the global percentage increase. The highest percentage growth was in the malicious URL category at 83% compared to 16% for the rest of the world.
- As the 2016 Rio Olympics approaches, the history of these increased attacks will undoubtedly continue and FortiGuard Labs is already seeing indicators of repeat techniques such as domain lookalikes for payment fraud and malicious websites or URLs targeting event and government officials.
- Cyberattacks during the Olympic games are not new. Fortinet FortiGuard Labs research has found a spike of attacks focused on the Olympics beginning as far back as the 2004 Summer Olympics in Greece.

Threatscape: Old is New Again and Volume Remains High

Fortinet FortiGuard Labs research is seeing a return of old threats and attack vectors, and the continued persistence of classic attacks, such as Conficker and ransomware, through updated variants. Fortinet's telemetry data and research indicates that the two most common delivery methods are phishing emails and malicious websites.

- ***Advanced Threat Technique - "Behavior Blending":*** Over the past three months a sophisticated method to help attackers persist inside systems they have breached is on the rise. Behavior blending is a technique used by criminals that allows them to blend in on a compromised network. For example, on a corporate network, the attacker may take on the behavior of an employee to avoid detection. Given this evasion technique has a lot of potential for thwarting detection, Fortinet expects to see more of it as it is refined and new tools are developed to better mimic the behavior of a credentialed target.

- ***Phishing:*** The volume of global phishing activity remains high with a 76% increase from April to June based on FortiGuard Labs' phishing domains and URLs threat data. The percentage growth from May to June was 11%. Additional email phishing takeaways include increased activity from Tokelau with the top four country code domains in Q2 2016 being Brazil, Columbia, Russia and India. Additionally, domain lookalikes are still very active (e.g. nefflix vs netflix). Lastly, FortiGuard also observed a number of large financial institutions' names included as part of the phishing domains and URLs.
- ***Exploit Kits:*** There's an uptick in the use of JavaScript-based Exploit Kits (EKs) with malicious URLs to deliver ransomware mostly as first-stage downloader payloads. A shift is in play currently from Angler to Fiesta and Neutrino which both show up consistently in FortiGuard's top 10 exploit kits globally.
- ***Advanced Malware:*** The JS/Nemucod family has been the dominant malware family globally in the last three months. This family is currently the most active ransomware downloader, with overall ransomware attacks significantly on the rise.
- ***Data Exfiltration - Botnet Indicators:*** FortiGuard's threat telemetry shows botnet activity and chatter on the rise, with ransomware botnet activity from Locky and Cryptowall as the notable names in the top 10.

Additional Resources:

- Learn more about the Fortinet Security Fabric.
- Download or read more about the report on our blog.
- 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, mobile, 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 280,000 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. More than 280,000 customers worldwide trust Fortinet to protect their businesses. Learn more at http://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.

* 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, plans regarding new products and services, and others. Changes of circumstances, product release delays and changes in product plans, execution risks, and 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.
415-215-8348
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