June 6, 2017

Fortinet Threat Landscape Report Reveals Visibility and Control of Distributed Infrastructures Have Diminished as Number of Potential Attack Vectors Continues to Grow

Research Demonstrates Highly Automated Cyber Defenses are Critical to Mitigate Pervasive "Cybercrime-as-a-Service" Attacks

SUNNYVALE, Calif., June 06, 2017 (GLOBE NEWSWIRE) --

Phil Quade, chief information security officer, Fortinet
"In the past year, highly-publicized cybersecurity incidents have raised public awareness of how our TVs and phones can be manipulated to deny others' Internet availability, and have shown, that demanding ransom is being used to disrupt vital patient care services. Yet, awareness alone isn't enough. Unfortunately, as organizations increasingly adopt convenience and cost-saving IT techniques, such as cloud services, or add a variety of smart devices to their network, visibility and control of their security is at risk. Meanwhile, attackers are buying or re-using tools of their own. Cybersecurity strategies need to increasingly adopt trustworthy network segmentation and high degrees of automation to prevent and detect adversaries' efforts to target the newly-exposed flanks of our businesses and governments."

News Summary:

Fortinet® (NASDAQ:FTNT), the global leader in high-performance cybersecurity solutions, today announced the findings of its latest Global Threat Landscape Report. The data spans the cybersecurity kill chain focusing on three central aspects of the landscape, including application exploits, malicious software, and botnets against the backdrop of important enterprise technology and industry sector trends. The research reveals that while more high profile attacks have dominated the headlines, the reality is that the majority of threats faced by most organizations are opportunistic in nature fueled by a pervasive Crime-as-a-Service infrastructure. For a detailed view of the findings and some important take-aways for CISOs read our blog. Three important research highlights follow:

1) Attack Tools Never Forget and Are Always Ready for Service, Anywhere and Anytime
Modern tools and Crime-as-a-Service infrastructures enable adversaries to operate on a global scale at light speed. As a result, the Internet seems not interested in geographic distances or boundaries because most threat trends appear more global than regional. Adversaries are always on the attack, looking for the element of surprise whenever possible on an international scale.

Understanding exploit trends or how ransomware works and spreads, the better we can avoid the impact caused by the next WannaCry. The malicious ransomware and its variants achieved great scale with hundreds of organizations affected across the world at once.

- **Ransomware:** Just under 10% of organizations detected activity associated with ransomware. On any given day, an average of 1.2% dealt with ransomware botnets running somewhere in their environment. The peak days of activity fell on weekends, with the hope of slipping traffic past weekend security operations staff. As the average traffic volume of various ransomware botnets increased, the average number of firms impacted by them rose as well.

- **Exploit Trends:** 80% of organizations reported high or critical-severity exploits against their systems. The majority of these targeted vulnerabilities were released in the last five years, but no shortage of attempts was made against premillennial CVEs. Exploit distribution was pretty consistent across geographical regions, likely because a huge proportion of exploit activity is fully automated via tools that methodically scan wide swaths of the Internet probing for opportunistic openings.

2) Hyperconvergence and IoT Are Accelerating the Spread of Malware
As networks and users increasingly share information and resources, attacks are spreading rapidly across distributed geographic areas and a wide variety of industries. Studying malware can help provide views into the preparation and intrusion stages of these attacks. Although protecting against mobile malware is particularly challenging because devices are not shielded on the internal network, are frequently joining public networks, and often are not under corporate ownership or control.

- **Mobile Malware:** The prevalence of mobile malware remained steady from Q4 2016 to Q1 2017, with about 20% of

organizations detecting it. More Android malware families made the top 10 list by volume or prevalence this quarter. The overall ratio among all types of malware was 8.7% for Q1 comparing to Q4's 1.7%.

- **Regional Prevalence:** Mobile malware prevalence rose in every region except the Middle East. The rate of growth was statistically significant in all cases rather than simply random variation. Compared to some other regional threat comparisons, Android malware appeared to have stronger geographic tendencies.

3) Visibility of Distributed and Elastic Infrastructure is Diminishing

Threat trends reflect the environment in which they occur, therefore, understanding how information technologies, services, controls, and behaviors change over time is important. It can act as a window into broader security policies and governance models and is valuable to monitoring the evolution of exploits, malware, and botnets as networks become increasingly complex and distributed.

Visibility and control over today's infrastructures are diminishing as the number of potential attack vectors across the expanded network landscape continues to grow. The rush to adopt private and public cloud solutions, the growth of IoT, the variety and volume of smart devices connecting to the network, and out-of-band threat vectors like shadow IT have stretched security professionals past their limits.

- **Encrypted Traffic:** The median ratio of HTTPS to HTTP traffic hit a high mark of nearly 55%. While helpful for maintaining privacy, this trend presents challenges to threat monitoring and detection. Many defensive tools have poor visibility into encrypted communications. Organizations—especially those with higher HTTPS ratios—could face threats lurking within encrypted communications.

- **Applications:** The median number of cloud applications used per organization was 62, which is roughly a third of all applications detected, with IaaS applications hitting a new high point. For many of these organizations, the challenge is that data visibility can drop significantly once it moves into the cloud. In addition, data stored in these applications and services continues to grow, instead of shrink, making it a problematic trend.

- **Industry Sectors:** Cluster analysis by vertical industry shows that the attack surface across most industries was the same with a few exceptions such as the Education and Telco sectors. This means that adversaries can easily exploit similar attack surfaces across industries more easily, especially with automated tools.

Report Methodology
The Fortinet Global Threat Landscape report is a quarterly view that represents the collective intelligence of FortiGuard Labs drawn from Fortinet's vast array of network devices and sensors within production environments during Q1 2017. Research data covers global, regional, industry sector, and organizational perspectives. It also focuses on three central and complementary aspects of the threat landscape: application exploits, malicious software, and botnets. In addition, Fortinet publishes a free, subscription-based Threat Intelligence Brief that reviews the top malware, virus, and web-based threats discovered every week, along with links to that week's most valuable Fortinet research.

Additional Resources

- Download the full Threat Landscape Report.
- Read our blog for more in depth information about the research.
- View our video and infographic summarizing valuable take-aways from the report.
- Sign up for our weekly FortiGuard intel briefs.
- Learn more about the Fortinet Security Fabric.
- Follow Fortinet on Twitter, LinkedIn, and Facebook.

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 310,000 customers trust Fortinet to protect their businesses. Learn more at http://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.

FTNT-O

are not limited to, the following: Fortinet, FortiGate, FortiGuard, FortiManager, FortiMail, FortiClient, FortiCloud, FortiCare, FortiAnalyzer, FortiReporter, FortiOS, FortiASIC, FortiWiFi, FortiSwitch, FortiVoIP, FortiBIOS, FortiLog, FortiResponse, FortiCarrier, FortiScan, FortiAP, FortiDB, FortiVoice, FortiWeb and FortiCASB. 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, 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

pr@fortinet.com

Investor Contact:

Kelly Blough

Fortinet, Inc.

408-235-7700 x 81612

kblough@fortinet.com

Analyst Contact:

Ron Davis

Fortinet, Inc.

415-806-9892

rdavis@fortinet.com

Primary Logo

Source: Fortinet, Inc.