March 28, 2017

# Fortinet Threat Landscape Report Examines How Cybercriminals Are Building an Army of Things Creating a Tipping Point for Cybersecurity

## Research Reveals Constantly Changing and Sophisticated Avenues of Attack Targeting Evolving Technology Infrastructure Enabled by a Fast-growing Underground Cybercrime Economy

SUNNYVALE, Calif., March 28, 2017 (GLOBE NEWSWIRE) -- **Phil Quade, chief information security officer at Fortinet**

"The cybersecurity challenges facing organizations today are complex with a threat landscape that is rapidly evolving. Threats are intelligent, autonomous, and increasingly difficult to detect, with new ones emerging and old ones returning with enhanced capabilities. In addition, the accessibilty of threat creation tools and services combined with the reward potential is driving the growth of the global cybercrime market into tens of billions of US dollars. To protect themselves, CISOs need to ensure that the data and security elements across all of their environments and devices are integrated, automated, and able to share intelligence, across an organization, from IoT to the cloud."

**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 research reveals the methods and strategies cybercriminals employed in detail and demonstrates the potential future impact to the digital economy. The question, "What's my biggest threat?" remains difficult to pinpoint as old threats resurface, but new, automated and high-volume attacks arise. For a detailed view of the research visit our blog. Highlights follow:

**Infrastructure Trends and How They Relate to Threats**

- Considering infrastructure trends and how they relate to the threat landscape is important. Exploits, malware, and botnets do not happen in a vacuum and finding or preventing threats gets increasingly complicated as network infrastructure evolves.
- Data shows encrypted traffic using SSL stayed steady at about 50% and accounted for roughly half of overall web traffic traversing within an organization. HTTPS traffic usage is an important trend to monitor, because while it is good for privacy, it presents challenges to detecting threats that are able to hide in encrypted communications. Often SSL traffic goes uninspected because of the huge processing overhead required to open, inspect, and re-encrypt traffic, forcing teams to choose between protection and performance.
- In terms of total applications detected per organization, the number of cloud applications trended up at 63, which is roughly a third of all applications detected. This trend has significant implications for security since IT teams have less visibility into the data residing in cloud applications, how that data is being used, and who has access to it. Social media, streaming audio and video, and P2P applications did not trend up sharply.

**An Army of Things Powered by the Digital Underground**

- IoT devices are sought-after commodities for cybercriminals around the world. Adversaries are building their own armies of "things" and the ability to cheaply replicate attacks at incredible speed and scale is a core pillar of the modern cybercrime ecosystem.
- In Q4 2016, the industry was reeling from the Yahoo! data breach and Dyn DDoS attack. Before the quarter was halfway done, the records set by both events were not only broken, but doubled.
- Internet of Things (IoT) devices compromised by the Mirai botnet initiated multiple record-setting DDoS attacks. The release of Mirai's source code increased botnet activity by 25 times within a week, with activity increasing by 125 times by year's end.
- IoT-related exploit activity for several device categories showed scans for vulnerable home routers and printers topped the list, but DVRs/NVRs briefly eclipsed routers as the thing of choice with a massive jump spanning 6+ orders of magnitude.
- Mobile malware become a larger problem than before. Though it accounted for only 1.7 percent of the total malware volume, one in five organizations reporting malware encountered a mobile variant, nearly all was on Android. Substantial regional differences were found in mobile malware attacks, with 36 percent coming from African organizations, 23 percent from Asia, 16 percent from North America, compared to only 8 percent in Europe. This data has implications for the trusted devices on corporate networks today.

**Automated and High-Volume Attacks Are Prevalent**

- The correlation between exploit volume and prevalence implies growing attack automation and lowering costs for malware and distribution tools available on the dark web. This is making it cheaper and easier than ever for cybercriminals to initiate attacks.
- SQL Slammer ranked at the top of the exploit detection list with a high or critical severity ranking, mainly affecting educational institutions.
- An exploit indicating attempted brute force attacks on Microsoft Remote Desktop Protocol (RDP) ranked second in prevalence. It launched RDP requests at a rate of 200 times every 10 seconds, explaining the high volume detected across global enterprises.
- Ranking third in prevalence is a signature tied to a Memory Corruption vulnerability in Windows File Manager that allows a remote attacker to execute arbitrary code within vulnerable applications with a jpg file.
- H-Worm and ZeroAccess had the highest prevalence and volume for botnet families. Both give cybercriminals control of affected systems to siphon data or perform click fraud and bitcoin mining. The technology and government sectors faced the highest numbers of attempted attacks by these two families of botnets.

**Ransomware Isn't Going Anywhere**

- Ransomware warrants attention regardless of industry and this high-value attack method will likely continue with the growth of ransomware-as-a-service (RaaS), where potential criminals with no training or skills can simply download tools and point them at a victim.
- 36% of organizations detected botnet activity related to ransomware. TorrentLocker was the winner and Locky placed third.
- Two malware families, Nemucod and Agent, went on a crime spree. 81.4 percent of all malware samples captured belonged to just these two families. The Nemucod family is infamously affiliated with ransomware.
- Ransomware was present in all regions and sectors, but particularly widespread in healthcare institutions. This remains significant because when patient data is compromised the ramifications can be much more severe, as it has greater longevity and personal value than other types of data.

**Daring Exploits, But Old is New**

- Adversaries took a "leave no vuln behind" policy. Unfortunately, attention focused on security patches and flaws in old devices or software, means less time and attention to focus on the growing attack surface accelerated by the digital devices of today.
- A full 86% of firms registered attacks attempting to exploit vulnerabilities that were over a decade old. Almost 40% of them saw exploits against even older CVEs.
- An average of 10.7 unique application exploits were tracked per organization. About 9 in 10 firms detected critical or high-severity exploits.
- Overall, Africa, Middle East, and Latin America exhibited a higher number and variety of encounters for each threat category when comparing the average number of unique exploit, malware, and botnet families detected by organizations in each world region. These differences appeared most pronounced for botnets.

**Report Methodology**
The Fortinet Global Threat Landscape report represents the collective intelligence of FortiGuard Labs during Q4 2016 with research data covering global, regional, sector, and organizational perspectives. It focuses on three central and complementary aspects of the threat landscape: application exploits, malicious software (malware) and botnets.

**Additional Resources**

- Learn more about the Fortinet Security Fabric.
- Read more details about the report on our blog and view the video or infographic.
- Access the full report online.
- 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 through FortiGuard services. FortiGuard Labs uses data collected from around the globe to protect more than 300,000 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 300,000 customers trust Fortinet to protect their businesses. Learn more at http://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.

***FTNT-O***



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



Source: Fortinet, Inc.

News Provided by Acquire Media