February 20, 2018

# Fortinet Threat Landscape Report Reveals Attacks Per Firm Increased by 82%

## Swarm Cyberattacks Target the Internet of Things (IoT) with Growing Intensity

SUNNYVALE, Calif., Feb. 20, 2018 (GLOBE NEWSWIRE) --

**Phil Quade, chief information security officer, Fortinet**
"The volume, sophistication, and variety of cyber threats continue to accelerate with the digital transformation of our global economy. Cybercriminals have become emboldened in their attack methods as they undergo a similar transformation, and their tools are now in the hands of many. The stark reality is that traditional security strategies and architectures simply are no longer sufficient for a digital-dependent organization. There is incredible urgency to counter today's attacks with a security transformation that mirrors digital transformation efforts. Yesterday's solutions, working individually, are not adequate. Point products and static defenses must give way to integrated and automated solutions that operate at speed and scale."

**News Summary:**
Fortinet® (NASDAQ:FTNT), a global leader in broad, automated, and integrated cybersecurity solutions, today announced the findings of its latest Global Threat Landscape Report. The research reveals that attacks per firm increased over the previous quarter. In addition, automated and sophisticated swarm attacks are accelerating making it increasingly difficult for organizations to protect users, applications, and devices. For a detailed view of the findings and some important takeaways for CISOs read the blog. Highlights of the report follow:

**Swarm Cyberattacks Increase in Volume, Variety, and Velocity**
The sophistication of attacks targeting organizations is accelerating at an unprecedented rate. Digital transformation isn't just reshaping business, cybercriminals are leveraging the expanding attack surface it creates for new disruptive opportunities to attack. They are implementing newer swarm-like capabilities while simultaneously targeting multiple vulnerabilities, devices, and access points. The combination of rapid threat development combined with the increased propagation of new variants is increasingly difficult for many organizations to combat.

- ***Unprecedented Volume:*** An average of 274 exploit detections per firm were detected, which is a significant increase of 82% over the previous quarter. The number of malware families also increased by 25% and unique variants grew by 19%. The data not only indicates growth in volume, but also an evolution of the malware as well. In addition, encrypted traffic using HTTPS and SSL grew as a percentage of total network traffic to a high of nearly 60% on average. While encryption can certainly help protect data in motion as it moves between core, cloud, and endpoint environments, it also represents a challenge for traditional security solutions.
- ***IoT Attack Intensity:*** Three of the top twenty attacks identified targeted IoT devices and exploit activity quadrupled against devices like Wi-Fi cameras. None of these detections were associated with a known or named CVE, which is one of the troubling aspects of vulnerable IoT devices. In addition, unlike previous attacks, which focused on exploiting a single vulnerability, new IoT botnets such as Reaper and Hajime can target multiple vulnerabilities simultaneously. This multi-vector approach is much harder to combat. Reaper's flexible framework means that, rather than the static, pre-programmed attacks of previous IoT exploits, Reaper's code is easily updated to swarm faster by running new and more malicious attacks as they become available. Demonstrating its swarm abilities, exploit volume associated with Reaper exhibited a jump from 50,000 to 2.7 million over a few days before dropping back to normal.
- ***Ransomware Still Prevalent:*** Several strains of ransomware topped the list of malware variants. Locky was the most widespread malware variant and GlobeImposter followed as the second. A new strain of Locky emerged, tricking recipients with spam before requesting a ransom. In addition, there was a shift on the darknet from only accepting Bitcoin for payment to other forms of digital currency such as Monero.
- ***Cryptocurrency Mining on the Rise:*** Cryptomining malware increased, which seems to be intertwined with the changing price of Bitcoin. Cybercriminals recognize the growth in digital currencies and are using a trick called cryptojacking to mine cryptocurrencies on computers using CPU resources in the background without a user knowing. Cryptojacking involves loading a script into a web browser, nothing is installed or stored on the computer.
- ***Sophisticated Industrial Malware:*** An uptick in exploit activity against industrial control systems (ICS) and safety instrumental systems (SIS) suggests these under-the-radar attacks might be climbing higher on attackers' radar. An example is an attack codenamed Triton. It is sophisticated in nature and has the ability to cover its tracks by overwriting the malware itself with garbage data to thwart forensic analysis. Because these platforms affect vital critical infrastructures, they are enticing for threat actors. Successful attacks can cause significant damage with far-reaching impact.
- ***Attack Variety:*** Steganography is an attack that embeds malicious code in images. It's an attack vector that has not

had much visibility over the past several years, but it appears to be on the resurgence. The Sundown exploit kit uses steganography to steal information, and while it has been around for some time, it was reported by more organizations than any other exploit kit. It was found dropping multiple ransomware variants.

**Fighting Swarm Attacks Requires Integrated Security**
The threat data in this quarter's report reinforces many of the predictions unveiled by the Fortinet FortiGuard Labs global research team for 2018, which predicted the rise of self-learning hivenets and swarmbots on the horizon. Over the next couple of years, the attack surface will continue to expand while visibility and control over today's infrastructures diminish. To address the problems of speed and scale by adversaries, organizations need to adopt strategies based on automation and integration. Security should operate at digital speeds by automating responses as well as applying intelligence and self-learning so that networks can make effective and autonomous decisions.

**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 sensors during Q4 2017.  Research data covers global, regional, industry sector, and organizational perspectives. It focuses on three central and complementary aspects of that landscape, namely application exploits, malicious software, and botnets. It also examines important zero-day vulnerabilities and infrastructure trends to add context about the trajectory of cyberattacks affecting organizations over time. To complement the report, 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**

- Read our blog for more information about the research or to access the full report.
- View our video and infographic summarizing valuable take-aways from the report.
- *Share your ideas, discuss the future of cybersecurity, and learn from the best in industry, at #Accelerate18.*
- Sign up for our weekly FortiGuard Threat Intelligence Briefs or participate in the open beta for our FortiGuard Threat Intelligence Service.
- Learn more about the Fortinet Security Fabric.
- Follow Fortinet on Twitter, LinkedIn, Facebook, Instagram, and YouTube.

**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 330,000 customers trust Fortinet to protect their businesses. Learn more at http://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.

***FTNT-O***

*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, contract, binding specification or other binding commitment by Fortinet or any indication of intent related to a binding commitment, 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, such as statements regarding technology releases among others. 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:**

Peter Salkowski
Fortinet, Inc.
408-331-4595
psalkowski@fortinet.com

**Analyst Contact:**

Ron Davis
Fortinet, Inc.
415-806-9892
rdavis@fortinet.com

Source: Fortinet, Inc.

News Provided by Acquire Media