November 14, 2017

Fortinet Predicts Highly Destructive and Self-learning "Swarm" Cyberattacks in 2018

Cybercrime Economy Adopting Advances in Artificial Intelligence and Automation to Ransom Commercial Services, Weoponize Swarms of IoT Devices and Attack Critical Infrastructures

SUNNYVALE, Calif. , Nov. 14, 2017 (GLOBE NEWSWIRE) --

Derek Manky, Global Security Strategist, Fortinet
"Our digital economy is powered by technology innovation that creates opportunity for good and bad in cybersecurity. The proliferation of online devices and the hyperconnectivity of today has created a criminal playground that is increasingly difficult to secure. At the same time, adversaries are leveraging automation and artificial intelligence at an unfathomable pace and scale across the ever-expanding attack surface. Attacks like WannaCry and NotPetya foreshadow the massive disruptions and economic impacts possible in our near future, resulting from the ransom and disruption of commercial services or intellectual property. Fabric-based security approaches that leverage the power of automation, integration, and strategic segmentation are critical to combat the highly intelligent attacks of tomorrow."

News Summary:
Fortinet® (NASDAQ:FTNT), the global leader in high-performance cybersecurity solutions, today unveiled predictions from the Fortinet FortiGuard Labs global research team about the threat landscape for 2018. The trends reveal the methods and strategies that cybercriminals will employ in the near future and demonstrate the potential impact of cyberattacks to the global economy. For a detailed view of the 2018 predictions visit our blog. Highlights of the predictions follow:

Digital Transformation Being Used for Good and Bad
Over the next couple of years, we will see the attack surface continue to expand while broad visibility and control over today's infrastructures diminish. The proliferation of online devices accessing personal and financial information, and the growing connection of everything - from armies of IoT devices and critical infrastructure in cars, homes, and offices, to the rise of smart cities - have created new opportunities for cybercriminals and other threat actors. The cybercriminal marketplace is adept at adopting the latest advances in areas such as artificial intelligence to create more effective attacks. We anticipate this trend to accelerate into 2018, enabling the destructive trends mentioned below.

- **The Rise of Self-learning Hivenets and Swarmbots:** Building on sophisticated attacks like Hajime and Devil's Ivy or Reaper, we predict that cybercriminals will replace botnets with intelligent clusters of compromised devices called hivenets to create more effective attack vectors. Hivenets will leverage self-learning to effectively target vulnerable systems at an unprecedented scale. They will be capable of talking to each other and taking action based off of local intelligence that is shared. In addition, zombies will become smart, acting on commands without the botnet herder instructing them to do so. As a result, hivenets will be able to grow exponentially as swarms, widening their ability to simultaneously attack multiple victims and significantly impede mitigation and response. Although these attacks are not using swarm technology yet, because they have the footprint in their code, adversaries could convert it to act with more self-learning behavior. Adversaries will use swarms of compromised devices, or swarmbots, to identify and target different attack vectors all at once enabling enormous speed and scale, but where the speed of development removes predictability needed to combat attack. FortiGuard Labs recorded 2.9 billion botnet communications attempts all in one quarter earlier this year, adding some context to the severity of what hivenets and swarmbots could cause.

- **Ransom of Commercial Services is Big Business:** Although the threat magnitude of ransomware has already grown 35X over the last year with ransomworms and other types of attacks, there is more to come. The next big target for ransomware is likely to be cloud service providers and other commercial services with a goal of creating revenue streams. The complex, hyperconnected networks cloud providers have developed can produce a single point of failure for hundreds of businesses, government entities, critical infrastructures, and healthcare organizations. We predict that cybercriminals will begin to combine AI technologies with multi-vector attack methods to scan for, detect, and exploit weaknesses in a cloud provider's environment. The impact of such attacks could create a massive payday for a criminal organization and disrupt service for potentially hundreds or thousands of businesses and tens of thousands or even millions of their customers.

- **Next-gen Morphic Malware:** If not next year, soon we will begin to see malware completely created by machines based on automated vulnerability detection and complex data analysis. Polymorphic malware is not new, but it is about to take on a new face by leveraging AI to create sophisticated new code that can learn to evade detection through machine written routines. With the natural evolution of tools that already exist, adversaries will be able to

develop the best possible exploit based on the characteristics of each unique weakness. Malware is already able to use learning models to evade security, and can produce more than a million virus variations in a day. But so far, this is all just based on an algorithm, and there is very little sophistication or control over the output. FortiGuard Labs recorded 62 million malware detections in one quarter in 2017. Out of the millions of malware detections we recorded, we saw 16,582 variants derived from 2,534 malware families. One in five organizations also reported malware targeting mobile devices. The increased automation of malware will only make this situation more urgent in the coming year.

- **Critical Infrastructure to the Forefront**: Recently, critical infrastructure providers continue to be at the top of the list in terms of the highest concern due to both strategic and economic threats. These organizations run high-value networks that protect vital services and information. However, most critical infrastructure and operational technology networks are notoriously fragile as they were originally designed to be air-gapped and isolated. The expectation to respond at digital speeds to employee and consumer demands has begun to change the requirements of these networks, driving the need for advanced security on networks that were originally designed to operate in isolation. Given the importance of these networks, and the potential for devastating results if they are compromised or knocked offline, critical infrastructure providers are now finding themselves in an arms race with nation-state, criminal, and terrorist organizations. The boldness of adversaries and the convergence of operational and information technology, makes critical infrastructure security a priority in 2018 and beyond.

- **The Dark Web and Cybercrime Economy Offer New Services Using Automation:** As the world of cybercrime evolves, so does the dark web. We expect to see new service offerings from the dark web as Crime-as-a-Service organizations use new automation technology for their offerings. We are already seeing advanced services being offered on dark web marketplaces that leverage machine learning. For example, a service known as FUD (Fully Undetectable) is already part of several offerings. This service allows criminal developers to upload attack code and malware to an analysis service for a fee. Afterwards, they receive a report as to whether security tools from different vendors are able to detect it. To shorten this cycle, we will see more machine learning used to modify code on the fly based on how and what has been detected in the lab in order to make these cybercrime and penetration tools more undetectable. Sandbox tools bolstered with machine learning, allow us to quickly identify previously unseen threats and dynamically create protections. There is no reason why this same approach couldn't be automated and used in the other direction for mapping networks, finding attack targets, determining where those attack targets are weak, or blueprinting a target to conduct a virtual penetration test and then building and launching a custom attack.

Staying Ahead of the Threats: Trends and Takeaways

There is an opportunity for enterprising cybercriminals enabled by advances in automation and artificial intelligence to use the right tools to severely compromise our digital economy. Security solutions need to be built around integrated security technologies, actionable threat intelligence, and dynamically configurable security fabrics. 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. This will not only expand visibility and centralize control, but also enable strategic segmentation in order to drive security deep into the network infrastructure to quickly identify, isolate, and remediate compromised devices and thwart attacks, even across different network ecosystems, from endpoint devices and local network resources to the cloud. In addition, basic security hygiene needs to become part of fundamental security protocols. It is something often overlooked, but crucial to limit the bad consequences we want to avoid.

Additional Resources

- Learn more about the Fortinet Security Fabric.
- Read our blog for more details about our Predictions for 2018.
- View our videos summarizing valuable takeaways from the report: Hivenets, Critical Infrastructure, and Automation.
- Sign up for our weekly FortiGuard Labs intel briefs or to be a part of our open beta of Fortinet's FortiGuard Threat Intelligence Service.
- Follow Fortinet on Twitter, LinkedIn, Facebook 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

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