August 21, 2017

Fortinet Threat Landscape Report Reveals Poor Security Hygiene and Risky Applications Enable Destructive Cyberattacks to Spread Infection at Record Pace

Cybercriminals Are Exploiting Known Vulnerabilities and Maximizing Impact With a Hybrid Threat Known as Ransomworms

SUNNYVALE, Calif., Aug. 21, 2017 (GLOBE NEWSWIRE) --

Phil Quade, chief information security officer, Fortinet
"The technology innovation that powers our digital economy creates opportunity for good and bad in cybersecurity. Yet, something we don't talk about often enough is the opportunity everyone has to limit bad consequences by employing consistent and effective cybersecurity hygiene. Cybercriminals aren't breaking into systems using new zero day attacks, they are primarily exploiting already discovered vulnerabilities. This means they can spend more of their resources on technical innovations making their exploits difficult to detect. Newer worm-like capabilities spread infections at a rapid pace and can scale more easily across platforms or vectors. Intent-based security approaches that leverage the power of automation and integration are critical to combat this new ‘normal'."

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 that poor cybersecurity hygiene and risky application usage enables destructive worm-like attacks to take advantage of hot exploits at record speed. Adversaries are spending less time developing ways to break in, and instead are focusing on leveraging automated and intent-based tools to infiltrate with more impact to business continuity. For a detailed view of the findings and some important takeaways for CISOs read our blog. Research highlights are as follows:

Effective Cyber Hygiene is Critical to Fight Worm-like Attacks
Crime-as-a-Service infrastructure and autonomous attack tools enable adversaries to easily operate on a global scale. Threats like WannaCry were remarkable for how fast they spread and for their ability to target a wide range of industries. Yet, they could have been largely prevented if more organizations practiced consistent cyber hygiene. Unfortunately, adversaries are still seeing a lot of success in using hot exploits for their attacks that have not been patched or updated. To complicate matters more, once a particular threat is automated, attackers are no longer limited to targeting specific industries, therefore, their impact and leverage only increases over time.

- **Ransomworms on the Rise:** Both WannaCry and NotPetya targeted a vulnerability that only had a patch available for a couple of months. Organizations who were spared from these attacks tended to have one of two things in common. They had either deployed security tools that had been updated to detect attacks targeting this vulnerability, and/or they applied the patch when it became available. Prior to WannaCry and NotPetya, network worms had taken a hiatus over the last decade.

- **Critical-severity of Attacks**: More than two-thirds of firms experienced high or critical exploits in Q2 2017. 90% of organizations recorded exploits for vulnerabilities that were three or more years old. Even ten or more years after a flaw's release, 60% of firms still experienced related attacks. Q2 data overall quantified 184 billion total exploit detections, 62 million malware detections, and 2.9 billion botnet communications attempts.

- **Active During Downtime:** Automated threats do not take weekends or nights off. Nearly 44% of all exploit attempts occurred on either Saturday or Sunday. The average daily volume on weekends was twice that of weekdays.

Technology Use Foreshadows Threat Risk
Speed and efficiency are business critical in the digital economy, which means that there is zero tolerance for any device or system downtime. As usage and configuration of technology such as applications, networks, and devices evolves, so do the exploit, malware, and botnet tactics of cybercriminals. They are ready and able to exploit weakness or opportunities in new technologies or services. In particular, business-questionable software usage and the vulnerable IoT devices of hyperconnected networks represent potential risk because they are not being consistently managed, updated, or replaced. In addition, while good for Internet privacy and security, encrypted Web traffic also presents a challenge to many defensive tools that have poor visibility into encrypted communications.

- **Application Usage:** Risky applications create risk vectors, which open the door for threats. Organizations allowing a large amount of peer-to-peer (P2P) applications report seven times as many botnets and malware as those that don't allow P2P applications. Similarly, organizations allowing a lot of proxy applications report almost nine times as many botnets and malware as those that don't allow proxy applications. Surprisingly, there was no evidence that higher usage of cloud-based or social media applications leads to increased numbers of malware and botnet infections.

- **Sector Analysis:** The education sector led in nearly every measure of infrastructure and application usage when grouped by element type and industry. The energy sector exhibited the most conservative approach with all others falling in between.

- **IoT Devices:** Almost one in five organizations reported malware targeting mobile devices. IoT devices continue to present a challenge because they don't have the level of control, visibility, and protection that traditional systems receive.

- **Encrypted Web Traffic:** Data shows the second straight record high this quarter for encrypted communications on the web. The percentage of HTTPS traffic increased over HTTP to 57%. This continues to be an important trend because threats are known to use encrypted communications for cover.

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 Q2 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

- Learn more about the Fortinet Security Fabric.
- Read our blog for more in-depth information about the research.
- View our video and infographic summarizing valuable takeaways from the report.
- Sign up for our weekly FortiGuard 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 320,000 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