FORTINET

November 28, 2017

Fortinet Threat Landscape Report Reveals Cybercriminals Successfully Using Common Exploits and "Swarm" Technology to Attack at Speed and Scale

High Rates of Botnet Reoccurrence and Automated Malware Demonstrate Importance of Intelligent and Automated Security Controls Combined with Incident-response Strategies

SUNNYVALE, CA -- (Marketwired) -- 11/28/17 -- ***Phil Quade, chief information security officer, Fortinet***
"Whether it's WannaCry in May or Apache Struts in September, long-known and yet still-unpatched vulnerabilities serve as the gateway for attacks time and time again. Remaining vigilant of new threats and vulnerabilities in the wild is critical, but organizations also need to keep sight of what is happening within their own environment. There is an incredible urgency to prioritize security hygiene and embrace fabric-based security approaches that leverage automation, integration, and strategic segmentation. Our adversaries are adopting automated and scripted techniques, so we need to raise their price of attacking to combat today's 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 high botnet reoccurrence rates and an increase of automated malware demonstrate that cybercriminals are leveraging common exploits combined with automated attack methods at unprecedented speed and scale. For a detailed view of the findings and some important takeaways for CISOs read our blog.

Highly Automated Attacks and Swarm Technology Becoming the Norm
Keeping up with swarm attacks, botnet reoccurrences, or the latest ransomware attack is daunting for the most strategic or staffed security team. If caught off guard, any organization can fall victim to the enormous amount of attacks at play today. To facilitate learning from what is happening in the wild, the intelligence included in the latest report offers views of the cyberthreat landscape from many 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 of the corresponding attack surface to add context about the trajectory of cyberattacks affecting organizations over time.

- ***Severity of Attacks Creates Urgency:*** 79% of firms saw severe attacks in Q3 2017. Research data overall during the quarter quantified 5,973 unique exploit detections, 14,904 unique malware variants from 2,646 different malware families, and 245 unique botnets detected. In addition, Fortinet identified 185 zero-day vulnerabilities to date this year.

- ***Botnet Reoccurrence*** *:* Many organizations experienced the same botnet infections multiple times. This is an alarming data point. Either the organizations did not thoroughly understand the total scope of the breach and the botnet went dormant only to return again after business operations went back to normal, or the root cause was never found and the organization was re-infected with the same malware.

- ***Swarming Vulnerabilities***: The exact application exploit used by attackers to breach Equifax was the most prevalent among 6,000+ unique detections recorded last quarter, and it is once again the most prevalent this quarter. In fact, three exploits against the Apache Struts framework made the top 10 list of most prevalent. This is an example of how attackers swarm when they catch scent of widespread, vulnerable targets.

- ***Mobile Threats:*** One in four firms detected mobile malware. Four mobile malware specific families stood out for the first time because of their prevalence. This is an indication that mobile is increasingly becoming a target and that the threats themselves are becoming automated and polymorphic. With holiday shopping season in full swing this trend is concerning as purchases from mobile devices will be frequent and IoT devices will be popular gifts to be purchased.

- ***Pervasive and Evasive Malware :*** The most common functionality among top malware families was downloading, uploading, and dropping malware onto infected systems. This behavior helps slip malicious payloads through legacy defenses by wrapping them in dynamic packaging. In addition, malware strains that establish remote access connections, capture user input, and gather system information were common as well. These advanced techniques are becoming the norm recently and both data points demonstrate the increased intelligent and automated nature of malware today.

- ***Ransomware is Always There***: After a hiatus during the first half of the year, the Locky ransomware ramped up in a big way with three new campaigns. Roughly 10% of firms reported it. In addition, at least 22% of organizations detected some type of ransomware during the quarter.

- ***Cybercriminals Target All Sizes:*** Midsize firms saw higher rates of botnet infections, demonstrating that they deal with more than their fair share of security problems. Cybercriminals potentially view midsize organizations as a "sweet spot" because often they do not have the same level of security resources and technologies as large enterprises but are seen as having valuable data assets. At the same time, the attack surface for midsize firms is growing at a fast pace because of their cloud adoption rates.

- ***SCADA is Critical:*** In addition to high-volume attacks like those against Apache Struts, some threats fly below the radar or have severe consequences that spillover beyond the organization in which they occur. Among the exploits tracked that target various types of supervisory control and data access (SCADA) systems, only one crossed the 1/1,000 threshold of prevalence and none were observed by more than 1% of reporting firms. Unfortunately, enterprise network intrusions and outages are bad, but breaches into SCADA environments put the physical infrastructure on which many lives depend at risk, demonstrating the importance of this statistic.

Fight Automated Attacks with Actionable Intelligence and Automated Security
The findings this quarter reinforce many of the predictions unveiled recently by the Fortinet FortiGuard Labs global research team for 2018. Both the trends and the threat data potentially foreshadow a wave of new types of attacks coming in the near future. The cybercrime community is already adept at leveraging advances in automation to create attacks exploiting vulnerabilities with increasingly malicious payloads capable of spreading at speed and scale.

Only a security framework that utilizes advanced threat intelligence sharing and an open architecture to tie security and networking components into a single, automated, and proactive defense and response system can protect for the future. The ever-evolving attack surface requires the flexibility to quickly implement the latest security strategies and solutions with the ability to seamlessly add advanced techniques and technologies as they emerge, without throwing out the existing infrastructure.

As the volume, velocity, and automation of attacks increase, it becomes important to align patching prioritization to what is happening in the wild to focus more on the most critical. In addition, organizations need to ensure that a strategic threat detection and incident-response strategy is in place that complements technology and intelligence to speed up the process.

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 Q3 2017. Research data covers global, regional, industry sector, and organizational perspectives. 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

- Learn more about the Fortinet Security Fabric.
- Read our blog for more information about the research or to access the full report.
- 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 330,000 customers trust Fortinet to protect their businesses. Learn more at http://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.

FTNT-O

FortiMail, FortiClient, FortiSIEM, FortiSandbox, FortiWiFi, FortiAP, FortiSwitch, FortiWeb, FortiADC, FortiWAN, and FortiCloud.

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:
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

News Provided by Acquire Media