FORTINET

February 24, 2016

Fortinet Uncovers Most Prevalent Undetected Cyber Threats Traversing Enterprise Networks

Fortinet Global Cyber Threat Assessment Program Provides Unparalleled Visibility Into Security Threats, User Productivity and Network Performance

SUNNYVALE, CA -- (Marketwired) -- 02/24/16 -- ***John Maddison, senior vice president of products and solutions, Fortinet***
"Businesses are constantly under cyber attack. With the attack surface dramatically increased and a mature attackers ecosystem, companies have to be ever more vigilant across all their IT assets. Fortinet's Cyber Threat Assessment Program has been designed to look deep into a company's network traffic and look for Indicators of Compromise. It provides customers a blueprint on how to reduce risk and at the same time make their network more efficient."

News Summary:
Fortinet (NASDAQ: FTNT), the global leader in high-performance cyber security solutions, today unveiled the most prominent, undetected cyber threats and bottlenecks impacting enterprise network security and performance, based on data analysis from the Fortinet Cyber Threat Assessment Program (CTAP).

- Fortinet CTAP issues its first end-user report with data collected from hundreds of U.S. Fortinet users and prospective customers across industries over a few months' time span; analyzed millions of incidents to gain unmatched insight into the largest, unknown security threats traversing their networks.
- Results indicate that enterprises of every size and vertical continue to face a constant and consistently hostile threat landscape, with more than 32.14 million attempted attacks on these networks.
- Top threat types include malware, botnets and application exploits with 357,420 attempts to compromise networks within the top 10 application vulnerabilities alone, and 71 different malware and botnet variants detected across the networks.
- Key verticals analyzed include healthcare, financial services, education and technology companies, with banking being targeted by nearly 45% of all malicious activity, followed by education, which experienced 27.4% of all attack events.

Global Program Uncovers Unknown Risks, Provides Immediate Mitigation Strategies
Fortinet's CTAP has expanded to global organizations, providing a free-of-charge program that enables companies to take a detailed look at their network's current security accuracy, application usage, user productivity and performance through expert guidance from Fortinet. By installing a FortiGate high-performance enterprise firewall within the network, a user can instantly monitor the application traffic traversing the network for intrusions, malware and malicious applications that could cause massive risk to the network. Additionally, FortiAnalyzer provides a Risk Assessment Report with actionable mitigation recommendations at the end of the data collection period.

Key Findings Across Industries: Largest Network Threats and Usage Trends
The data highlighted in Fortinet's initial end-user CTAP report demonstrates that organizations of all types constantly face threats from various angles and need to ensure that they have the right end-to-end security solution in place to mitigate the risks. With hundreds of organizations in North America already benefiting from the global threat intelligence of CTAP, some of the largest cross-industry vulnerabilities and network usage trends include the following:

- ***Automated Attack Systems, Botnets and Malware take Center Stage***
  - With 32.14 million attempted attack events in a 4-month span, it's evident that attackers rapidly build automated systems and tools to probe networks for exploitable vulnerabilities.
  - Headline-generating Malware such as Conficker, Nemucod and ZeroAccess have made significant efforts to rebuild and infect machines, as the financial incentives for these owners are massive. With 5,230 instances of Conficker, followed by 4,220 instances of Nemucod and 3,210 instances of ZeroAccess traversing these networks, it's evident that this threat type will only continue to grow.
  - In just the top 10 incidents analyzed, 357,420 attempts were made to exploit application vulnerabilities, as hackers continue to cast a wide net to try and compromise corporate data.

- ***Social Media, Video Streaming and Advertising Drain Corporate Networks***
  - Social media and multimedia streaming activities account for 25.65% of all network traffic, exposing corporate systems and sensitive data to risks of infection from drive-by downloads, social engineering and malvertising.

Facebook is the most dominant social media site representing 47.27% of all social media traffic, with YouTube contributing to 42.29% of streamed content.
    - Advertising content accounts for 19.1% of network traffic and has been shown to be a potential source of malware as third party advertising networks are subverted or tricked into delivering malicious ads.
    - Application control appears to be a continual challenge for administrators. A significant amount of Peer-to-Peer traffic, primarily Bittorrent and gaming activity opens the network to malicious content that piggybacks on top of applications and files downloaded through these popular sites. Enterprises should exercise caution when building application control policies on their networks.

- ***Financial Services, Education and Healthcare Rank Most Vulnerable Industries***
    - Due to the lucrative financial data obtained when these networks are successfully infiltrated, banking and finance organizations are disproportionately targeted with 44.6% of all malicious activity. Hackers rely on high-velocity attacks and target financial institutions with sophisticated trojans and land-and-expand attack strategies to infiltrate and persist within the network.
    - Education organizations represent 27.4% of all attack events in this report and are the second largest at-risk vertical industry. Botnets are the dominant threat for educational institutions, with 7 out of top 10 infections, while XcodeGhost, the widely publicized iOS malware breaks into the top 10 vulnerabilities list in education.
    - Healthcare ranked third in overall malicious activity with 10.6% of attack events. The healthcare industry is unique in the appearance of automated exploit kits, notably targeting numerous vulnerabilities in Flash, Silverlight and Internet Explorer to compromise a system via a drive-by-download or infected website.

Takeaways and Actionable Insights to Protect Your Network
Attackers are targeting companies of every size in the hopes of gaining access to the valuable assets inside the corporate network. Vertical industries need to know what hackers are after and understand the unique strategies they employ.

- Banking and Finance organizations should bolster their networks against land-and-expand strategies and the predominant use of trojans. Deploying security platforms like Fortinet's Advanced Threat Protection framework can combat sophisticated new variants of malware at the network edge, while implementing internal network segmentation can help contain insider threats and minimize risks to the most valuable data.
- Education security professionals should be mindful of the various devices that can access their network resources, utilizing threat intelligence like FortiGuard Mobile Malware services to detect threats that target student smartphones and tablets as vectors for an attack.
- Healthcare industry protections closely mirror those of banking organizations. Understanding that hackers may be looking to encrypt their data and hold the information hostage, instead of silently exporting data to sell on the dark web makes it even more imperative for healthcare to consider internal segmentation strategies to contain threats.
- Technology businesses are varied and hackers respond with diverse strategies and malware to cast the largest net. Security professionals in these organizations need to understand their devices, applications and platforms that connect to the web using analysis tools like FortiAnalyzer. Understanding their network utilization will help businesses tailor a security posture that matches their individual attack surface.

CTAP is part of a broader effort by Fortinet and its FortiGuard Labs threat research team to integrate risk and advisory capabilities with its end-to-end security platform to provide customers greater insight into dynamically changing cyber risks that threaten their businesses.

Supporting Quote
"As attacks against corporate data resources become increasingly pervasive, TierPoint is committed to providing a clear line of defense to secure our customers. As such, it's critical that we know exactly what is going on inside their networks. Fortinet's Cyber Threat Assessment Program has opened the door to many new business opportunities for TierPoint. CTAP offers deep analysis of existing or possible threats running on customer or prospect networks, helping us ensure that we can recommend the right Fortinet security solutions to mitigate the dynamically changing cyber risks that threaten their businesses.
- Scott Fuhriman, vice president and general manager, TierPoint, #1 CTAP US Partner

Additional Resources

- Report: 2016 CTAP Threat Landscape Report
- Whitepaper: Cyber Threat Assessment - Threat Landscape Report Executive Summary
- Infographic: A Look Behind the Firewall
- Follow Fortinet on Twitter and LinkedIn
- Join the conversation on the Fortinet blog

About Fortinet
Fortinet (NASDAQ: FTNT) protects the most valuable assets of some of the largest enterprise, service provider and government organizations across the globe. The company's fast, secure and global cyber security solutions provide broad,

high-performance protection against dynamic security threats while simplifying the IT infrastructure. They are strengthened by the industry's highest level of threat research, intelligence and analytics. Unlike pure-play network security providers, Fortinet can solve organizations' most important security challenges, whether in networked, application or mobile environments -- be it virtualized/cloud or physical. More than 200,000 customers worldwide, including some of the largest and most complex organizations, trust Fortinet to protect their brands. Learn more at http://www.fortinet.com, the Fortinet Blog or FortiGuard Labs.

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, binding specification or other binding commitment by Fortinet, and performance and other specification information herein may be unique to certain environments. This news release contains forward- looking statements that involve uncertainties and assumptions, such as statements regarding product releases. 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
Darlene Gannon
Fortinet, Inc.
408-235-7700
Email contact

Investor Contact
Michelle Spolver
Fortinet, Inc.
408-486-7837
Email contact

Analyst Contact
Ron Davis
Fortinet, Inc.
415-806-9892
Email contact

Source: Fortinet

News Provided by Acquire Media