Media Contact
Amber Dale
amber@chatterboxpre.com.
+97150 7952652

Fortinet Launches Cyber Threat Assessment Program Internationally to Uncover Critical Security Risks

Analysis of enterprises piloting the program shows that social media and application control demand great vigilance, while banks are favorite targets

Dubai, UAE – February 25, 2016 – Fortinet (NASDAQ: FTNT), the global leader in high-performance cyber security solutions, today unveiled its new Cyber Threat Assessment Program (CTAP) designed to provide organizations a detailed look into the type and amount of cyber threats posing risks to their networks, yet are going undetected by their existing security solutions. This new offering 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.

Program Uncovers Unknown Risks, Provides Immediate Mitigation Strategies

Fortinet, in collaboration with a number of key partners, is offering its threat assessment program to organizations free-of-charge. Through the assessment process, the FortiGate high-performance next generation firewall will be installed within the customer or prospect network, where it monitors the application traffic traversing the network for intrusions, malware and malicious applications that could collectively cause massive risk to the network, giving attackers access to a company's most sensitive files and database information. At the end of the data collection period, a detailed risk assessment report will be generated, using FortiAnalyzer, that provides an analysis of the application traffic, user productivity, network utilization, the overall security risk, and the related business risk, as well as detailed, actionable mitigation recommendations.

"In the past, it was much easier for firewalls to detect significant threats to the network, because traffic could be classified based on specific protocols, and hackers' approaches were not as sophisticated," said John Maddison, Senior Vice President of Products & Solutions for Fortinet. "A growing number of network threats today are designed to avoid detection by bypassing traditional firewalls with ease. Our new CTAP program is specifically designed to quickly detect the threats other solutions are not intercepting to help customers significantly increase protection, while decreasing business risks."

Fortinet's CTAP provides an important opportunity for organizations to ensure that they are not relying on legacy systems that aren't effective against today's dynamic cyber attacks that occur across multiple vectors and stages. By offering a deeper analysis of existing or possible threats, customers are given a clear assessment of the risks to their environments, while Fortinet and its partners help prioritize actions to mitigate those risks, providing customers the peace of mind knowing their critical assets are protected.

Social Media and Application Control are Weak Points; Financial Services Institutions Most Highly Targeted

Hundreds of Fortinet enterprise customers and prospects in the US have tried out CTAP in the last four months and key findings from an analysis report unveiled today reveal that:

1. 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. Headline-generating malware such as Conficker, Nemucod and ZeroAccess have made significant efforts to rebuild and infect machines − 5,230 instances of Conficker, followed by 4,220 instances of Nemucod and 3,210 instances of ZeroAccess were found.

2. 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.

3. 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.

4. 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.

“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," said Maddison. "Fortinet’s Cyber Threat Assessment Program has been designed to look deep into a company’s network traffic and hunt for indicators of compromise. It provides customer a blueprint on how to reduce risk and at the same time make their network more efficient.”

For more information about Fortinet’s Cyber Threat Assessment, please visit: http://www.fortinet.com/how_to_buy/request-cyber-threat-assessment.html

#######