April 15, 2014

Fortinet Leads Industry in Zero-Day Discoveries

Since 2006, Company's FortiGuard Labs Has Uncovered 143 Zero-Day Vulnerabilities, 18 in 2013 Alone

SUNNYVALE, CA -- (Marketwired) -- 04/15/14 -- Fortinet® (NASDAQ: FTNT) -- a world leader in high-performance network security -- today announced that FortiGuard™ Labs, the global threat research arm of Fortinet, discovered 18 critical zero-day vulnerabilities in 2013 -- more than any other network security vendor in the industry. This adds to the 140+ zero-day vulnerabilities identified since 2006. Of these, 128 vulnerabilities have been fixed by the appropriate vendors. For the list of outstanding zero-day vulnerabilities visit: http://www.fortiguard.com/advisory/UpcomingAdvisories.html.

"FortiGuard Labs has been quietly doing great threat research work behind the scenes for Fortinet for more than a decade. It's time to acknowledge the more than 200 unsung heroes who toil behind the scenes around the world," said Derek Manky, global security strategist for Fortinet's FortiGuard Labs. "FortiGuard Labs is the collaborative team that uncovers new threats, liaises with enforcement and emergency response and discovers evasion techniques while developing cutting edge mitigation technology. We have a tactical security research team tasked with breaking the applications most of us take for granted on a daily basis, who then forward their findings to vendors so they can update their software to better protect their customers. Every hole they find is one less vulnerability for the hackers to exploit. In the end, affected products are hardened and clients are protected before and after holes are closed."

A zero-day vulnerability is a previously unknown threat that does not yet have a patch or update available from the vendor to close a security hole, thus leaving it open to attack. Once a zero-day vulnerability is identified, FortiGuard Labs analyzes and verifies it before vendors are notified. Upon verification, FortiGuard Labs develops an advanced zero-day IPS signature(s) that is pushed out to Fortinet customers well in advance of a vendor's patch release, which helps protect against the open security hole(s). These signatures are unique to Fortinet and play an important role in the fight against advanced persistent threats (APTs).

"Zero-day vulnerabilities can be developed into dangerous weapons by cyber criminals or nation states and can be used to effectively subvert targeted systems. Our mission is to take the fuel out of their fire, protecting targets before they are under attack," Manky continued. "Zero-day protection is a tough task, and our approach offers unique and effective protection against APTs."

Responsible Disclosure
FortiGuard Labs' responsible disclosure dictates a discovered vulnerability be patched before public disclosure. Even without a working patch, a signature for the vulnerability can be generated to prevent intrusions. Once a signature is created, it is put through FortiGuard Labs' zero-day signature process and assigned a generic name. The goal is to provide protection while disclosing as few details as possible. From there, FortiGuard works together with vendors to create a patch for the vulnerability. After a patch is released, FortiGuard continues to work with the vendor to analyze the source of the vulnerability and to help prevent similar zero-days from being exploited in the future.

Beyond Signatures
As malware numbers have increased exponentially in recent years, network security vendors have had to find alternate methods for malware detection and mitigation. Fortinet, for example, incorporates several new protective features and functionalities into its FortiOS operating system. FortiOS 5 includes more than 150 new security features that help protect against today's Advanced Persistent Threats (APTs) and Advanced Targeted Attacks (ATAs). These enhancements include advanced malware detection, exploit discovery and protection, cloud-based reputation systems and a multi-vector policy engine, which offers the ability to apply policy based on the user and device identity; an important attribute for distributed, virtual and cloud networks.

In addition to analyzing the threat landscape, FortiGuard Labs researchers write and present papers at global security conferences, including EICAR, Blackhat, Virus Bulletin, Insomni'Hack and Hashdays. Published papers and presentations from these shows can be downloaded from here: http://www.fortiguard.com/resources/ResearchPapers.html

About FortiGuard Labs
FortiGuard Labs has identified the most recent threats based on data collected from FortiGate® network security appliances and intelligence systems in production worldwide. Customers who use Fortinet's FortiGuard Services should be protected against the vulnerabilities outlined in this report as long as the appropriate configuration parameters are in place.

FortiGuard Services offer broad security solutions including antivirus, intrusion prevention, Web content filtering and anti-spam

capabilities. These services help protect against threats on both application and network layers. FortiGuard Services are updated by FortiGuard Labs, which enables Fortinet to deliver a combination of multi-layered security intelligence and zero-day protection from new and emerging threats. For customers with a subscription to FortiGuard, these updates are delivered to all FortiGate, FortiMail™ and FortiClient™ products.

Ongoing research can be found in the FortiGuard Center or via FortiGuard Labs' RSS feed. Additional discussion on security technologies and threat analysis can be found at the FortiGuard Blog.

About Fortinet

Fortinet (NASDAQ: FTNT) helps protect networks, users and data from continually evolving threats. As a global leader in high-performance network security, we enable businesses and governments to consolidate and integrate stand-alone technologies without suffering performance penalties. Unlike costly, inflexible and low-performance alternatives, Fortinet solutions empower customers to embrace new technologies and business opportunities while protecting essential systems and content. Learn more at www.fortinet.com.

FTNT-O

Media Contact:
Rick Popko
Fortinet, Inc.
408-486-7853
rpopko@fortinet.com

Investor Contact:
Michelle Spolver
Fortinet, Inc.
408-486-7837
mspolver@fortinet.com

Source: Fortinet

News Provided by Acquire Media