February 25, 2013

Fortinet(R)'s FortiGuard Labs Launches New Cloud-Based Sandboxing and IP Reputation Services to Help Stop Advanced Persistent Threats (APTs)

FortiGuard(TM) Labs Unique Threat Intelligence Technology Provides Enhanced Protection Capability for FortiGate, FortiCloud, FortiWeb, FortiDDoS and FortiDNS Platforms

SUNNYVALE, CA -- (Marketwire) -- 02/25/13 -- Fortinet® (NASDAQ: FTNT) -- a world leader in high-performance network security -- today announced that the company's FortiGuard Labs has launched new cloud-based sandboxing and IP reputation services that are designed to help protect against advanced persistent threats (APTs). The new FortiGuard Labs services provide additional protection capabilities for the company's FortiGate, FortiCloud, FortiWeb, FortiDDoS and FortiDNS network and application security platforms.

About Advanced Persistent Threats (APTs)

APTs are usually operated by highly-skilled teams or governments and use advanced technology and multiple methods and vectors to reach specific targets and obtain sensitive or classified information. Also known as targeted attacks, reconnaissance is carried out on each target to determine best method of entry. Social engineering or zero day vulnerabilities are the most common infection vectors.

About FortiGuard Cloud-Based Sandboxing Service

The FortiGuard cloud-based sandboxing service uses behavioral attributes to detect malware by executing them within a virtual environment. This serves as an additional protection layer that complements FortiGate's existing, award-winning antivirus engine and its unique inline lightweight sandbox. Suspicious files can be submitted automatically to the new hosted service for further scanning without significantly impacting a FortiGate's performance. In addition, FortiCloud has added a new feature that serves as the online sandboxing portal, which provides detailed status and visibility into the scanned results.

FortiGuard IP Reputation Service

FortiGuard Labs continually investigates and monitors IPs that are compromised or behaving abnormally. The service uses a number of different techniques, including historical analysis, honeypots and botnet analysis to provide immediate protection for FortiGate, FortiWeb and FortiDDoS platforms against wide scale automated attacks. The service also continuously learns from a global footprint of threat sensors, tracking malicious events to IP addresses in real time.

"Today's advanced persistent threats are challenging both IT personnel and network security vendors. While the signature approach to malware abatement is not going away overnight, additional dynamic safeguards need to be implemented now in order to effectively combat these threats at all layers in rapid fashion," said Derek Manky, global security strategist for Fortinet. "The new services announced today offer a strategic approach to detect and respond to breaking threats from numerous attack vectors. Modern threats strike and shift quickly and so should detection."

About FortiGate

The FortiGate consolidated security platform delivers unmatched performance and protection while simplifying networks. Fortinet offers models to satisfy any deployment requirement from the FortiGate-20 series for small offices and distributed enterprises to the FortiGate-5000 series for very large enterprises, service providers and carriers. FortiGate platforms integrate FortiASIC™ processors and the latest generation CPUs and the new FortiOS™ 5 operating system to provide comprehensive, high-performance security. Key security features included in the operating system include:

- *More Security* to fight advanced threats. A client reputation feature gives enterprises a cumulative security ranking of each device based on a range of behaviors and provides specific, actionable information that helps organizations to identity compromised systems and potential zero day attacks in real time. The new advanced anti-malware detection system adds an on-device behavior-based heuristic engine and cloud-based AV services that include an operating system sandbox and botnet IP reputation database. Together with superior industry-validated AV signatures, FortiOS 5 delivers unbeatable multi-layered protection against today's sophisticated malware

- *More Control* to secure mobile devices and BYOD environments by identifying devices and applying specific access policies as well as security profiles, according to the device type or device group, location and usage

- *More Intelligence* with automatic adjustment of role-based policies for users and guests based on location, data and application profile. Enhanced reporting and analysis also provides administrators with more intelligence on the behavior of their network, users, devices, applications and threats

About FortiCloud

FortiCloud is a cloud-based management, reporting and log retention service for all FortiGate and FortiWiFi security appliances. This is a free service that includes 1 GB of log storage. Further, the malware sandboxing results for a specific FortiGate appliance can be viewed in the FortiCloud portal. A subscription version of the service includes 200 GB of log storage and some additional reporting and logging features.

About FortiWeb

FortiWeb Web application firewalls protect, balance and accelerate Web applications, databases and any information exchanged between them. FortiWeb (release 4.4.6) includes the capability to license FortiGuard's IP Reputation Service to stop attacks based by malicious IPs and proxies. FortiWeb has passed ICSA Web Application Firewall Certification, demonstrating FortiWeb's commitment to uphold the industry's highest security standards.

About FortiDDoS

The FortiDDoS platform consists of dedicated appliances that are designed to detect and help protect against today's most damaging and sophisticated DDoS attacks. The appliances feature custom ASICs that are capable of mitigating DDoS attacks while maintaining incredibly-low latency (less than 26 microseconds), preventing loss of availability to critical systems, servers and applications. The upcoming FortiDDoS (release 3.2) includes the capability to license the FortiGuard IP Reputation Service.

About FortiDNS

FortiDNS (release 1.3) can be used as a DNS firewall to enhance or replace existing DNS caching. A licensable Domain Query Protection service helps protect against malicious domains or can detect Botnet communication activity. In addition, FortiGuard's IP Reputation service provides timely updates of malicious domains and IPs. The product family features a high-performance recursive DNS caching engine that supports IPv6 and Domain Name System Security Extensions (DNSSEC). DHCP functionality is also included.

Visit the Fortinet FortiGuard Researchers at RSA

Fortinet will be participating at the RSA security conference, which is taking place February 25 - March 1 at San Francisco's Moscone Center. Stop by booth #2025, meet the members of the FortiGuard research team, see a demonstration of the lab's latest threat intelligence services and receive a free USB wristband.

Anatomy of a Botnet (Free Report)

One of the biggest challenges in Internet security is how to deal with today's ever evolving botnets. In the following free report, FortiGuard Labs researchers explain what a botnet is, how they're used, the people behind them and how cybercrime has evolved into a complex and well-organized hierarchy, and what users can do to fight back. The Anatomy of a Botnet report can be downloaded here: http://www.fortinet.com/resource_center/whitepapers/anatomy-of-a-botnet.html

About FortiGuard Services

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™ FortiClient™, FortiWeb and FortiDDoS 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.

Follow Fortinet Online: Twitter at: www.twitter.com/fortinet; Facebook at: www.facebook.com/fortinet; YouTube at: http://www.youtube.com/user/SecureNetworks.

About Fortinet (www.fortinet.com)

Fortinet (NASDAQ: FTNT) is a worldwide provider of network security appliances and a market leader in unified threat management (UTM). Our products and subscription services provide broad, integrated and high-performance protection against dynamic security threats while simplifying the IT security infrastructure. Our customers include enterprises, service providers and government entities worldwide, including the majority of the 2012 Fortune Global 100. Fortinet's flagship FortiGate product delivers ASIC-accelerated performance and integrates multiple layers of security designed to help protect against application and network threats. Fortinet's broad product line goes beyond UTM to help secure the extended enterprise -- from endpoints, to the perimeter and the core, including databases and applications. Fortinet is headquartered in Sunnyvale, Calif., with offices around the world.

FTNT-O

Media Contact:

Rick Popko

Fortinet, Inc.

408-486-7853

rpopko@fortinet.com

Source: Fortinet

News Provided by Acquire Media