



Barracuda Networks Enhances Virus and Malware Threat Prevention Techniques; Renames Flagship Barracuda Spam Firewall

Barracuda Spam & Virus Firewall Emphasizes Speed of Response and Low False Positives

Campbell, Calif., April 6, 2009 – Barracuda Networks Inc. today announced enhancements to its email virus and malware threat prevention techniques, enabling its newly renamed Barracuda Spam & Virus Firewall to identify viruses and other email-borne malware threats faster than well known competing anti-virus products. The decision to rename its flagship Barracuda Spam Firewall to Barracuda Spam & Virus Firewall reflects Barracuda Networks ongoing commitment to providing best-of-breed malware protection for threats sent over email in real-time.

“What differentiates Barracuda Networks from the competition is that our products are purpose-built to solve the unique needs of email and Web security appliances,” said Stephen Pao, vice president of product management for Barracuda Networks. “Unlike desktop anti-virus engines retrofitted for email server usage, the Barracuda Spam & Virus Firewall features anti-virus technology specifically designed for rapid response to viruses that propagate and mutate quickly over botnets and other bulk delivery techniques.”

Demonstrating the efficacy of Barracuda Central's response to email-borne malware, Barracuda Networks is posting malware classification benchmarks against leading anti-virus vendors, including Symantec (NASDAQ: SYMC), McAfee (NYSE: MFE), and Trend Micro.

Combating malware propagation techniques over email requires dedicated focus on the unique properties of the virus and other malware attack types including: the attack sources, referenced URLs, the social engineering techniques used to entice recipients to launch them, and the rate of attack proliferation. Through advanced technologies, such as Barracuda Real-Time Protection and Predictive Sender Profiling developed specifically for spam and email-borne malware, Barracuda Spam & Virus Firewalls provide industry-leading response times to email-borne threats.

Barracuda Central Rapid Response

Barracuda Real-Time Protection provides industry-leading protection through the rapid identification of threats and the immediate, real-time, dissemination of protection measures to all Barracuda Spam & Virus Firewalls in the field once a virus or other malware has been identified.

To identify these threats as they emerge, Barracuda Central, a 24x7 operations center operated by Barracuda Networks, monitors statistics from both captive virus traps and anonymous data collected in aggregate from over 70,000 customer systems worldwide. Once Barracuda Central engineers identify a potential virus or malware outbreak based on this trend analysis, Barracuda Central validates the hypothesis by collecting samples of suspect emails from Barracuda Spam & Virus Firewalls around the world that elect to participate in data collection. Through efficient evidence collection, Barracuda Central can quickly classify the viruses or malware.

Immediately upon virus or malware classification, Barracuda Spam & Virus Firewalls running Barracuda Real-Time Protection perform live queries for unknown fingerprints against the Barracuda Central virus and spam fingerprint databases, avoiding any need to wait for the next virus definition download for protection. Once categorized, new fingerprints are automatically included in subsequent spam and virus

definitions downloaded by Barracuda Spam & Virus Firewalls through Energize Updates, avoiding the need to perform real-time queries.

To address rapidly mutating threats, Barracuda Networks employs a set of technologies called Predictive Sender Profiling that goes beyond traditional reputation techniques and can identify suspicious behaviors associated with the campaign itself. Examples include hacking of legitimate Web sites or newly infected bots on otherwise legitimate computers or data centers. Predictive Sender Profiling enables immediate blocking of the entire malware campaign, even before more general anti-virus signatures can be developed.

Low false positive ratings critical to complete gateway protection

“Email security solutions must be designed to avoid blocking legitimate email,” said Pao. “As such, Barracuda Central has prioritized low false positive rates in its analysis in not just spam traffic but also impending malware threats over email.”

In order to maintain low false positives for malware threats over email, Barracuda Central works to restrict individual binary signatures as much as possible to specific instances, utilizing other campaign details to provide corroborating evidence to further generalize the mitigation techniques, avoiding false positive problems caused by overly broad signature definitions.

“Barracuda Networks offers the best of both worlds; industry-leading rapid response and protection from the threats that propagate most aggressively without impacting legitimate work,” said Pao.

Augmented by open source protection

Barracuda Networks recognizes that not all email-borne viruses propagate rapidly, including infected attachments sent from one user to another rather than through bulk email delivery techniques. The Barracuda Spam & Virus Firewall completes its coverage of proprietary rapid-response threat data with the world's largest open source collection of common malware vulnerability data. ClamAV excels in identifying viruses which are not well covered by rapid-response techniques, including those that are well-known but that do not propagate quickly. The Barracuda Spam & Virus Firewall – as well as other network security appliances in the Barracuda Networks product portfolio – includes the ClamAV engine, and Barracuda Central leverages the ongoing updates contributed by the open source security research community. With three layers of anti-virus protection – open source signatures, proprietary signatures, and Barracuda Real-Time Protection – the Barracuda Spam & Virus Firewall provides the most comprehensive, purpose-built anti-virus engine for email-borne threats.

About the Barracuda Spam & Virus Firewall

The Barracuda Spam & Virus Firewall is available in eight models and supports up to 100,000 active users with no per user licensing fees. Its architecture leverages 12 defense layers: denial of service and security protection, rate control, IP analysis, sender authentication, recipient verification, virus protection, policy (user-specified rules), Fingerprint Analysis, Intent Analysis, Image Analysis, Bayesian Analysis, and a Spam Rules Scoring engine. In addition, the entire Barracuda Spam & Virus Firewall line features simultaneous inbound and outbound email filtering with the inclusion of sophisticated outbound email filtering techniques, such as rate controls, domain restrictions, user authentication (SASL), keyword and attachment blocking, triple-layer virus blocking, and remote user support for outbound email filtering. The Barracuda Spam & Virus Firewall's layered approach minimizes the processing of each email, which yields the performance required to process millions of messages per day.

About GEOBRIDGE

Since 1997, GEOBRIDGE (www.GEOBRIDGE.net) has been providing information security solutions to global clients. Today our client list includes Fortune 500 companies, financial institutions, health care, government agencies and defense clients across North America and internationally. GEOBRIDGE helps

clients mitigate risk and realize significant value from their IT investments while allowing clients to focus on the growth and profitability of their company. Our team provides solutions, integration services and consultancy in the areas of encryption, network security, identity management, transaction security, and compliance. Due to the increased needs for compliance with internal governance, and external legal and regulatory requirements, we have expanded our compliance and security best-practices offerings to address information assurance. GEOBRIDGE is a Qualified Security Assessor company (QSAC) certified by the Payment Card Industry (PCI) and a TG-3 Assessor recognized by the Electronic Funds Transfer (EFT) networks.