Media Contact:
Tony Welz
Principal
Welz & Weisel Communications
703.218.3555 x226
tony@w2comm.com

Investor Contact:
Tania Almond
Investor Relations Officer
Sourcefire, Inc.
410.423.1919
tania.almond@sourcefire.com

SOURCEFIRE LAUNCHES RAZORBACK, DELIVERING CROSS-SOLUTION THREAT DETECTION AND PROTECTION

Latest Open Source Innovation Enables Users to Tie Together Various Threat Collection and Detection Technologies for Faster, Coordinated Protection

Columbia, Md. – August 2, 2010 – Sourcefire, Inc. (Nasdaq:FIRE), the creator of Snort® and a leader in intelligent cybersecurity solutions, today announced Razorback™, an open source framework designed to deliver deep inspection capabilities for combating today's most complex threats. In addition, Razorback has the ability to link an organization's detection investments and maximize their effectiveness -- providing greater visibility and intelligence into the threats detected by the various security solutions. Developed to help coordinate the response against Advanced Persistent Threats, Razorback enables users to easily collect, analyze and store threat data from disparate technologies, so that they can implement customized enterprise- and threat-specific detection and remediation.

Razorback's goal is to act as an overlay solution and deliver centralized correlation, analysis and action by coordinating Intelligence Driven Response (IDR) processes using custom built and existing security tools (anti-virus, IDS, gateways, email, etc.). IDR goes beyond traditional incident response . It allows users to drive the information learned about specific attackers back into their security infrastructure for a truly customized response to human adversaries. Razorback provides deep analysis and reporting by, storing, in full, every piece of data identified that could indicate a compromise or attack and specifically highlights the components of that data which caused the system to trigger an alert. Additionally, Razorback provides targeted forensics information on common attack vectors.

"Open source is at the core of everything Sourcefire does, and Razorback is the latest innovation providing users with the ability to protect themselves from today's sophisticated threats," said Martin Roesch, Founder and CTO of Sourcefire and Creator of Snort. "The Sourcefire Vulnerability Research Team (VRT) is one of the only groups in the industry that truly understands customer pain points and security limitations. We leveraged this knowledge to deliver a solution that can easily tie together disparate security technologies and convert intelligence gathered on attacker methodology into detection and remediation capabilities."

The innovative Razorback framework performs detection in near-real time (in terms of seconds), allowing for in-line blocking on "store and forward" services, such as email services or web proxies, and providing timely alerts in the event of an attack. It also provides enterprises with the ability to convert intelligence gathered on attacker methodology into detection capabilities,

enabling them to rapidly develop and protect against targeted threats or Zero-Day vulnerabilities.

"Razorback was designed to address the current challenges of today's threat landscape where attackers are specifically creating attacks to avoid off the shelf tools and technologies," said Matt Watchinski, Senior Director of the Sourcefire Vulnerability Research Team. "The power is in combining the intelligence of an organization's security infrastructure with fast and detailed analysis. By providing advanced detection capabilities for uncovering highly obfuscated, difficult-to-detect attacks along with detailed output, Razorback gives response teams a head start on analyzing attacks."

A simple interface allows enterprises to integrate and extend functionality quickly and easily. Sourcefire will continue to develop additional capabilities and publish data collectors, detection engines, analysis software and output handlers to maximize the value of Razorback and encourage innovation from the open source community. Like other open source technologies, Razorback is available at no charge. To learn more about Razorback or download a copy, go to: http://labs.snort.org/razorback.

About the Sourcefire Vulnerability Research Team™ (VRT)

The Sourcefire Vulnerability Research Team™ (VRT) is a group of leading intrusion prevention experts working to discover, assess and respond to the latest trends in hacking activity, intrusion attempts and vulnerabilities. The VRT includes some of the most renowned security professionals in the industry, including the authors of several standard security reference books. This team is also supported by the vast resources of the open source Snort and ClamAV communities, making it the largest group dedicated to advances in the network security industry. To keep up to date with the VRT's research and insights into network security visit http://vrt-sourcefire.blogspot.com/.

About Sourcefire

Sourcefire, Inc. (Nasdaq:FIRE) is a world leader in intelligent Cybersecurity solutions. Sourcefire is transforming the way Global 2000 organizations and government agencies manage and minimize network security risks. Sourcefire's IPS and Real-time Adaptive Security solution equips customers with an efficient and effective layered security defense – protecting network assets before, during and after an attack. Through the years, Sourcefire has been consistently recognized for its innovation and industry leadership by customers, media and industry analysts alike – with more than 50 awards and accolades. Today, the names Sourcefire and founder Martin Roesch have grown synonymous with innovation and network security intelligence. For more information about Sourcefire, please visit http://www.sourcefire.com.

States and other countries. Other company, product and service names may be trademarks or service marks of others.