SOURCEFIRE VRT™:
FOCUSED ON PROTECTING "YOUR" NETWORK

SOURCEFIRE® VULNERABILITY RESEARCH TEAM™ (VRT)

The Sourcefire Vulnerability Research Team (VRT) is a group of elite cybersecurity experts dedicated to serving both Sourcefire commercial customers and open source users. The Sourcefire VRT was founded on one core objective: "Protecting 'Your' Network." While this may sound simplistic, in reality it is quite complex. Every network is different—from the applications running on it, to the users who work on it, to the policies that govern it. This is why the Sourcefire VRT believes that in order to be effective in helping you protect "your" network, we have to be more than just a traditional response organization; we have to be a proactive member of your security ecosystem. This requires that we go beyond simply tracking and detecting today's latest threats; it requires that we push the boundaries of today's security technologies, making them effective against tomorrow's threats.

In order to achieve our core mission objective, the VRT has built comprehensive defensive technologies and techniques that help customers quickly protect assets that span from the cloud to the core. These technologies are open, verifiable, agile, and easy to customize to meet the needs of any environment. This approach allows our customers to take control of their security destiny with technology that automatically fine-tunes and enforces security policies and that can be adapted in real time to the current threat situation.

Key VRT Technology Capabilities

- Open
- Verifiable
- Customizable
- Core Objective of "Protecting Your Network"

We don't believe in the magic black box or silver bullet security solution. Proprietary and closed, these static solutions are blind to the network and inflexible in the face of today's rapidly changing environments. We believe in the cold hard facts that security is difficult and that we need a new approach, one that empowers our customers to address these security challenges.

The VRT is committed to helping every organization quickly gain competencies in the core tenets of effective security: Superior Protection, Comprehensive Intelligence, Innovative Detection Technologies, and Trusted Community. The VRT provides all of this and more, working with our customers and partners on a daily basis to make sure we are effectively "Protecting 'Your' Network."

SUPERIOR PROTECTION

Breadth and Depth of Security Coverage

Protecting your network requires both breadth and depth of coverage. New types of network devices, communication methods, vulnerabilities, malware, and embedded systems are coming online at a rapid pace, and each of these potential attack vectors must be monitored and secured. While some research teams limit their focus to a few areas, the VRT is dedicated to helping provide protection in all areas, and has extensive expertise protecting against different types of threats. The VRT uses open detection content to support a wide range of security solutions including Next-Generation IPS (with and without integrated application control), Next-Generation Firewall and FireAMP™ advanced malware analysis and protection, as well as numerous open source and commercial threat protection systems. This allows the VRT intelligence and threat research to be deployed in any type of environment to protect any type of asset.

"The VRT protects millions of hosts and its intelligence is deployed in hundreds of thousands of locations around the world."

Proven Vulnerability-based Protection

The VRT is well known in the industry for its excellence in detecting the myriad vulnerabilities and exploits that emerge daily. Using high quality, rapid releases on a biweekly basis, the VRT keeps all of our customers up-to-date with vulnerability-based protections for the latest threats. While other vendors claim similar coverage, only the VRT has proven time and time again in third-party validation that our detection content is top notch. For the last two years the

SOURCEfire®

Sourcefire VRT has led the NSS Labs Network IPS test in detection rate with close to 100% detection. Additionally, ICSA Labs has certified the VRT's vulnerability protections for the last five years with 100% detection rates in vulnerability tests.

"This is the second year in a row that (when tuned) Sourcefire blocked the most attacks of all products."

– Network Intrusion Prevention Systems Individual Product Test Results, NSS Labs, April 2011

Advanced Malware Protection

While there is no such thing as a security panacea, the leading-edge malware coverage and post-compromise detection offered by the Sourcefire VRT give our customers a fighting chance in today's threat landscape.

"Sourcefire research suggests as much as 75% of new malware is unique and only seen once."

Keeping our customers safe against the onslaught of malware requires innovative and rapidly advancing detection technologies and detection content. Additionally, it requires massive amounts of intelligence gathering, reverse engineering, and analytics to wade through this mountain of big data and turn it into actionable information used to create protections. For anti-malware protection, Sourcefire offers protection with ClamAV® and advanced malware protection with FireAMP, an enterprise-class solution developed as a result of the Immunet acquisition. FireAMP leverages more than two million endpoint installations to drive its big data analysis. The VRT taps into this analysis to further protect customers from dynamic threats.

The VRT utilizes all of this information to develop malware protections, post-compromise protections, reputation services, and analyzers to locate threats as they appear in the wild. These capabilities are driven back into all Sourcefire products for protecting hosts, mail gateways, and network assets.

Customized Policies and Granular Control

Today's traditional firewall is quickly becoming antiquated for anything other than basic network segmentation, switching and routing. With the world moving to Software as a Service (SaaS), cloud-based applications, and tunneling of just about everything over HTTP, total network visibility, including deep packet inspection for application and policy control, has become extremely critical. Fine-grained control over applications, users, and network assets is essential for a strong security policy.

The Sourcefire VRT provides numerous application and policy controls through our NGIPS, NGIPS with application control, NGFW, and FireAMP solutions. These allow customers to restrict, modify, or create detailed policies governing what users and applications are allowed to do on your networks. Additionally, the VRT publishes extensive reputation data to help our customers determine which sites network users should be allowed to access. Our customers can not only quickly identify and analyze the activities of applications and users on their networks, but can also create access control points for limiting the use of applications and the scope of user activities.

COMPREHENSIVE INTELLIGENCE

Actionable Community-Driven Threat Data

The core component of any holistic security strategy is solid, actionable intelligence. Over the last 10 years the Sourcefire VRT has built one of the most comprehensive intelligence gathering and analytic platforms in the industry. Through the ClamAV, Snort®, Immunet™, and Sourcefire user communities, the VRT receives valuable intelligence that no other security research team can match. In addition, through collaboration with open source users around the globe the VRT is able to detect regionalized and language-specific threats as they emerge. This information is driven back into our processes and protections for everyone's benefit.

Access to Vulnerability Information

The VRT also analyzes numerous public vulnerability feeds every day, looking for new threats, and acting on that information in real-time to develop new detection content. In addition, industry partnerships like Microsoft Active Protection Program (MAPP) allow the VRT to quickly and effectively handle new Microsoft and Adobe targeted threats, releasing our detection on the same day as Microsoft patches. This allows our customers to protect their critical assets with network and host-based protection, while they test and deploy these new patches. Recently, Microsoft itself was a target of a denial-of-service (DOS) attack affecting its own ASP.NET. The Sourcefire VRT responded immediately, creating a protection to help our customers but also to help Microsoft protect is own properties and those of its vendor partners and customers. By responding swiftly and thoroughly the Sourcefire VRT is committed to closing the exposure gap.

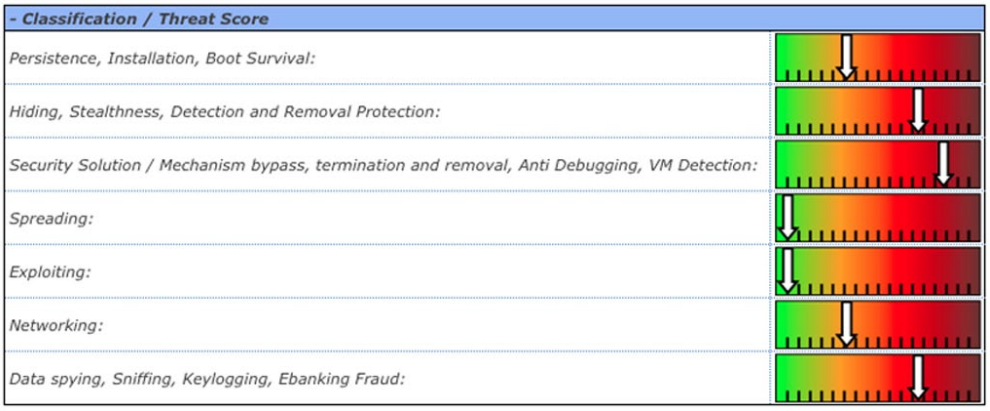
"The VRT covers 100% of Microsoft network-based threats on Microsoft Tuesday."

Real-Time Malware Intelligence

Through data acquired through the millions of users worldwide, along with honeypots, sandnets, and extensive industry partnerships in the malware community, the VRT collects more than 100,000 malicious software samples a day. Through our advanced analysis infrastructure and our team of security experts, the VRT automatically analyzes these samples and rapidly generates detection content to mitigate these threats on a daily basis.

Detailed Threat Reports

VRT Threat Reports contain comprehensive information about what the threat does and where the threat communicates for command and control. A separate report on the functionality of the threat includes information on the registry keys and files that were modified, deleted, or added, where the sample potentially came from, and a detailed list of functional internal components. These reports can be utilized by customers to understand the impact and risk of the threat that entered their environment, and can also help them track the threat back to "patient zero." For example, FireAMP advanced malware protection customers receive threat reports for any threat detected in their environment. The VRT is constantly updating and enhancing these reports to give customers the information they need about new and sophisticated threats.



INNOVATIVE DETECTION TECHNOLOGIES

Flexible Defensive Technologies for Dynamic Environments

The threat landscape has evolved from simple buffer overflows in network services, to complex client side attacks targeting browsers and file formats. As attacks change so must the defensive technologies utilized to detect them. Depth and breadth of protection coverage and comprehensive intelligence simply aren't enough. To be effective security strategies have to become smarter, faster, and must contain more advanced detection methods in order to stay on top of increasingly sophisticated threats. The VRT is constantly working on new detection technologies that push the envelope of today's detection mechanisms, while keeping them agile enough to be quickly adapted to tomorrow's threats.

Additionally, security strategies must stay on top of emerging threat targets such as Critical Infrastructure/ SCADA (Supervisory Control and Data Acquisition) systems, mobile systems, and embedded device security. The VRT's experience in all of these fields combined with the breadth of detection content already provided in these sectors, continuously protects our customers against these new and specialized types of threats.

"Protections for the vulnerabilities used by Stuxnet were already in place before Stuxnet was released."

Whether dealing with new threats or protecting potential new targets, the VRT continuously releases new detection technologies through numerous open source tools that allow security professionals to better defend their networks.

More than Signatures

Basic pattern matching, regular expressions, and protocol parsing are no longer sufficient for detecting file- and browser-based exploits. The VRT utilizes the Shared Object rules language that leverages the full power of the "C" programming language for faster, more accurate detection. With this type of power it is easy to dig deep into complex Javascript, PDF, and other file format based threats. Additionally, the Shared Object rules language allows for quick development, preservation of performance under demanding conditions, and is completely open for rapid adaptation and modification by end users.

The same rules apply to malware. It is just not possible to detect some of today's threats with complex pattern matching; you need a fully featured detection language. For these types of malware threats the Sourcefire VRT utilizes the ByteCode engine that allows for rapid development of complex detections. ByteCode detection can quickly unpack new obfuscation methods, parse complex file formats, and rapidly prototype new detection mechanisms. This allows the VRT to rapidly respond to the most sophisticated malware threats.

The Shared Object rules and ByteCode signatures bring an enormous amount of power and sophistication to the Snort and ClamAV detection engines. The VRT utilizes these innovative technologies to continuously protect our customers. This approach is one of the many reasons why Sourcefire has dominated the NSS Labs Network IPS test two years in a row.

Complex Threat Detection

The Sourcefire VRT invented the Razorback™ detection platform to push the envelope in complex threat detection, and to help security analysts identify Advanced Persistent Threat (APT) indicators. Razorback was designed from the ground up to allow security analysts and researchers to quickly add new detection content and deep analytic modules to the platform to identify and analyze the vast amounts of security data in today's large networks. Any security team can use this open source project to help investigate unknown files, network traffic, or any type of data that might be suspicious, and, if malicious, gain insight into what the threat does and how it works. Razorback allows security analysts everywhere to remain agile in their network defenses, and rapidly close the gap between compromise and detection.

Anticipating Threats

It is one thing to respond to new threats, it is another to protect against new ones. The Sourcefire VRT is constantly searching for new vulnerabilities and threats that could affect our customers. When these new vulnerabilities are discovered the VRT releases rules to protect against these Zero-Day threats, while the affected vendors develop and test their patches. With these VRT protections Sourcefire customers can control the threat while waiting for protections from their vendors.

The VRT is also actively engaged in locating new malicious websites, botnet command-and-control servers, and other malicious sites on the Internet. Once located, this information is cataloged and consolidated into comprehensive IP blacklists and URL filtering feeds which are distributed to our customers.

Examples of VRT Zero-Day Threat Protection:

- MS11-015 – Critical – Windows Media Player
- MS10-062 – Critical – Windows Media Player
- APSB09-07 – Critical – Adobe Reader
- ORACLE08 – Critical – Oracle BEA WebLogic

Controlling Outbreaks

We recognize that security will never be 100% effective in blocking attacks. This is one of the reasons why the VRT believes there is limited security effectiveness in focusing solely on offensive research, and channels more focus on intelligent proactive solutions. That's also why the VRT is constantly developing new technologies and protection content to close the gap between compromise and detection. The VRT spends significant amounts of resources reverse-engineering new malware to help locate and uncover command-and-control activity and other post-compromise behaviors. This information is then utilized to develop extensive post-compromise detection content for containment and control of infections.

TRUSTED COMMUNITY

Extending Your Team

Having a trusted place to turn when the going gets tough is essential to effective security. Without strong communication channels between trusted partners, other security teams, and the response teams of your security vendors it is impossible to stay up to date on the latest threats, and solve your unique security problems. The VRT believes we should be an extension of your security team. We don't just push information at you, we want to have constructive conversations about your goals and how we can help you reach them. The VRT has created several programs to help facilitate this task.

"The VRT should be viewed as an extension of your team, helping you reach your security goals."

Streamlining Communication

The Awareness, Education, Guidance, and Intelligence Sharing (AEGIS) program was created specifically to interact with our customer and partners to help solve custom detection challenges in your specialized environments. AEGIS puts our customers in direct contact with VRT Analysts and Engineers to help build custom detection content, improve security practices, gather feedback on our products and services, and implement customer improvements to our products.

The AEGIS program is utilized by numerous Sourcefire customers daily, and is provided at no cost as part of Sourcefire Diamond and Platinum support packages. It's just one more way we help protect 'your' network.

Interactive Information

The Sourcefire VRT keeps in constant contact with our customers through numerous interactive channels. The VRT and ClamAV blogs are continually updated with information about the latest threats, how to create custom detection content, and in-depth analysis of the latest malware families. For a complete list of content and ways to interact with the VRT see the table on the next page.

Content	Description	Location
VRT Blog	Articles, technical information, exploit detection notes and information on the latest threats.	http://VRT-blog.snort.org/
VRT Advisories	Continuous, ad-hoc releases of rule additions and modifications in the bad-traffic, blacklist, botnet-cnc, chat, dns, dos, exploit, file-identify, misc, oracle, policy, smtp, specific-threats, web-activex and web-misc rule sets to provide coverage for emerging threats from these technologies.	http://www.sourcefire.com/security-technologies/snort/vulnerability-research-team/advisories
VRT Labs	White papers, technical presentations, speaking schedule, tools, exploit research and other research. Also contains VRT contact information using various methods and houses the VRT PGP/GPG public key for encrypted communication.	http://labs.snort.org/
VRT Twitter	Includes regular updates from the VRT as well as links to newly published content on the various VRT web resources.	http://www.twitter.com/VRT_sourcefire
VRT Videos	Includes the "Monthly Vulnerability Report." The Vulnerability Report, which is also available via the iTunes store.	http://vimeo.com/VRT
Razorback	The Razorback project hosted on Sourceforge. Contains links to project files, presentations and the bug-tracking site.	http://razorbacktm.sourceforge.net/
IRC	VRT members can be found online using IRC on irc.freenode.net in these channels: #snort, #razorback and #sfsnort.	
ClamAV Blog	Articles that specifically relate to malware research and information.	http://blog.clamav.net/
ClamAV Website	All the information that relates to the ClamAV project, its development, installation and updating for the most widely used AV engine available.	http://www.clamav.net/lang/en/
Snort VRT Website	Information on the latest VRT rule releases, links to blog content, false positive submission, and many other VRT resources.	http://www.snort.org/VRT
Exploit Development Class	Course outline and schedule for the "Fundamentals of Exploit Development" training class, developed and taught by the VRT.	http://www.sourcefire.com/services/courses/fundamentals

Keeping up to Date

The Sourcefire VRT is responsible for the entire chain of Sourcefire detection and prevention, from intelligence gathering, analysis, content creation, packaging and quality assurance, to end user delivery. Controlling this entire process allows the VRT to rapidly deliver industry-leading detection content in the time frames necessary for defending against today's latest threats. Below is a list of detection content offerings the Sourcefire VRT provides customers.

Package	Description
Security Enhancement Update (SEU) (4.X) Sourcefire Rules Update (SRU) (5.X)	Update package for all detection content for Sourcefire next-generation network security platforms. Contains detection and prevention rules, Shared Object detection, and policy updates. Released every Tuesday and Thursday.
Vulnerability Database (VDB) Updates	Updated content for the VDB. Contains new FireSIGHT™ decoders and detectors, additionally updates the device with new vulnerabilities for R3. Released every two weeks.
Open Source Certified Rules	Contains detection and prevention rules, Shared Object detection, and policy updates for open source Snort users.
Open Source ClamAV Signatures	Contains all malware and AV content for ClamAV.
Sourcefire Advanced Malware Protection Updates	Contains malware signatures and AV content for Sourcefire FireAMP customers.
Open Source Blacklists	IP, DNS, and URL blacklists that can be utilized by customer and end users for blocking malicious sites, botnet servers, and other policy violating content. Updated twice a day.

CONCLUSION

The Sourcefire Vulnerability Research Team provides a uniquely comprehensive and proactive approach to protecting 'your' network. With an enviable track record for success and leadership in the security industry, team members are focused on providing high-quality, customer-driven security research that sets the bar for accuracy and relevance. In addition, the VRT's commitment to helping every organization gain competencies in the core tenets of effective security—Superior Protection, Comprehensive Intelligence, Innovative Detection Technologies, and Trusted Community—furthers the VRT's ability to deliver on its core objective: "Protecting 'Your' Network."

For Sourcefire customers, these skills and research translate directly into award-winning products and services. But even if you're not a Sourcefire customer, you still reap the benefits provided by the VRT's research efforts. With a unique and enduring commitment to an open source model, and a continuing stream of research papers, presentations, blog posts and more, the Sourcefire VRT makes high impact, effective knowledge and tools available to the entire community.

It's a record, and a legacy, that's unmatched in the industry.