DATA SHEET

RedSplice Network Traffic Examiner

NEXT GENERATION NETWORK SNIFFER

RedSplice Network Traffic Examiner is designed to combine process and technology into a **single system for network forensics**

RedSplice Network Traffic Analyzer is a network monitoring tool (packet sniffer, packet analyzer) that brings traffic monitoring and analysis to a whole new level. While providing granular data monitoring and precise packet and session reconstruction it also includes advanced technology for extracting high level content data as images, videos, and scripts, making the network forensics process much easier.

RedSplice's advanced implementation supports the investigation into security and performance issues, decreasing the amount of detective work while enhancing the overall productivity of your security and monitoring systems.

Modern software applications often involve using Web APIs over HTTP/HTTPS which increase interconnectivity and productivity for users. RedSplice has the ability to analyze web traffic and create a structured view of the information, so that the debugging and monitoring activities become much easier for software developers.

RedSplice is a tool that increases productivity for IT specialists like network administrators, software developers, information security analysts and makes network forensics activities accessible even for those with limited technical knowledge

SESSION RECONSTRUCTION

Most packet capture solutions and network sniffers only display raw packets and leave it to the user to decode the content and determine the potential problem they represent. RedSplice collects network traffic and reassembles it and by putting the traffic data in a more human readable format, it is allowing the user to visualize the content and take better and faster decisions

FAST FACTS

SSL / TLS TRAFFIC DECODING
for indepth visibility over the security threats

RECORDS AND REPLAYS
traffic for a complete audit trail of suspicious network activity

HELPS IDENTIFY PERFORMANCE
problems before they result in network downtime

COMPATIBLE WITH GIGABIT
network adapters.

ADVANCED SEARCHING
and filtering for quick identification of desired datum

IDENTIFIES THE SENDER PROCESS
to aid with malware research and local system forensics

CONTENT EXTRACTION
allows quick examination of videos, scripts, images and other files contained in network traffic

CONTENT EXTRACTION

Starting from session reconstruction, RedSplice is capable of extracting the information available in network packets and put it into a form that is easy to visualize and understand. Content extraction is available for HTTP(S) based traffic and it will allow the user to directly view content like images, videos, flash files and javascript content even if they are compressed with gzip and even if the traffic is SSL encrypted.

DATA CAPTURE

The RedSplice Traffic Capture Engine is designed as a service oriented architecture, allowing security professionals to gather forensics information while performing other tasks in parallel. RedSplice is designed to capture data specified via filters based on a myriad of traffic metrics. This approach ensures that all traffic is captured regardless of whether the solution runs interactively or as a background service.

STATISTICAL ANALYSIS

RedSplice provides a variety of statistical measurements, with information on protocol distribution, top hosts, packet-size distribution and bandwidth usage. By regularly analyzing how systems and applications are being used, administrators can proactively identify and eliminate issues before they can result in downtime.

- **Protocol Distribution Statistics:** reports network usage based on MAC and IP layer protocols
- **Top Hosts Statistics:** provides a summary analytics chart in real time, organized based on the amount of traffic generated criteria
- **Size Distribution Statistics:** displays the charts with the number of packets with sizes in six different ranges
- **Bandwidth Usage:** allows monitoring the number of packets per second and the number of bytes per second, flowing across the network, in real time
- **Host Traffic Report:** provides functionality required to create complex reports regarding the network traffic across a specific host.

SSL / TLS DECODING

Nowadays, more and more Internet and Intranet traffic is using encryption, making analysis of malicious traffic as well as troubleshooting a lot more difficult. Decoding of SSL traffic can be done offline, using a saved packet capture of the traffic and SSL private keys or in real-time via RedSplice's built-in SSL proxy. **RedSplice is the only network analyzer on the market that does both passive and active SSL traffic decryption.**

SYSTEM REQUIREMENTS

WINDOWS 7, WINDOWS 2008 R2
WINDOWS 8, WINDOWS 2012
WINDOWS 10, WINDOWS 2012 R2 MICROSOFT INTERNET EXPLORER 9.0+

Windows XP and Vista supported with limited functionality

INTEL PENTIUM IV 2.0 GHz or COMPATIBLE
1GB RAM, 20 GB FREE HDD STORAGE
NETWORK INTERFACE CARD WITH TCP/IP ENABLED

CONTACT INFORMATION

EMAIL
sales@redsplice.com

ADDRESS
25251 Paseo de Alicia, Suite 200,
Laguna Hills, CA, USA