StegAlyzerRTS

BENEFITS

- Detect leakage of sensitive information and intellectual property outside the enterprise network through insider use of steganography
- Detect insider use of steganography to conceal evidence of criminal activity
- Real-time detection of files associated with over 1,150 steganography applications
- Real-time detection of signatures of over 55 steganography applications
- Real-time alerts to network security administrators
- Enforce organizational policy prohibiting insiders from having or using steganography or other data-hiding applications on the enterprise network

Steganography Analyzer Real-Time Scanner

Sensitive data leakage is of utmost concern to corporate management. Data Loss Prevention (DLP) solution providers offer products with a wide range of functionality and capability. However, none of these products detect insider use of steganography.

StegAlyzerRTS is the world's first commercially available network security appliance capable of detecting digital steganography applications and the use of those applications in real-time. StegAlyzerRTS offers a "drop-in, turn-key" capability that will not affect network throughput.

StegAlyzerRTS detects insiders downloading steganography applications by comparing the file fingerprints, or hash values, to a database of known file, or artifact, hash values associated with over 1,150 steganography applications.

StegAlyzerRTS also detects insider use of steganography applications by scanning files entering and leaving the network for known signatures of over 55 steganography applications. StegAlyzerRTS detects insider theft of sensitive information hidden inside other seemingly innocuous files which are sent to an external recipient as an e-mail attachment or posted on a publicly accessible web site.

StegAlyzerRTS was found to be effective for identifying files associated with steganography applications and files that contain hidden steganographic data by the Defense Cyber Crime Institute (DCCI)[1].

Product highlights in StegAlyzerRTS:

- Detect fingerprints of over 1,150 steganography applications
- Detect signatures of over 55 steganography applications
- Exclusive Automated Extraction Algorithm functionality for selected steganography applications gives examiners a "point-click-and-extract" interface to easily extract hidden information from suspect files
- Send real-time alerts to network security administrators
- Retain copies of suspect files for further analysis
- Does not impact network performance
- Available in 100 Mbps and 1 Gbps aggregated throughput models

StegAlyzerRTS licenses include all product updates and hardware maintenance for one year from date of purchase. Operating Lease options for 12, 24, and 36 months are available with and without purchase at fair market value at the end of the lease. Volume license, government, and educational discounts are available.

[1] http://www.dc3.mil/dcci
[2] http://www.cybersciencelab.com

Steganography Analysis and Research Center
Backbone Security

STEGANOGRAPHY ANALYSIS AND RESEARCH CENTER
SARC
RAISING THE THRESHOLD OF PERCEPTION

42 Mountain Park Drive
Fairmont, WV 26554
877-560-SARC
Fax 304-366-9163
www.sarc-wv.com

811 Ann Street
Stroudsburg, PA 18360
888-805-4331
Fax 570-234-0636
www.backbonesecurity.com

BACK BONE SECURITY