

Backbone's Digital Steganography Database Exceeds 900 Applications

FAIRMONT, W.Va., Feb. 1 (SEND2PRESS NEWSWIRE) – Backbone Security is pleased to announce the release of Version 3.8 of the Steganography Application Fingerprint Database (SAFDB) which now contains more than 900 steganography applications.

Developed in Backbone's Steganography Analysis and Research Center (SARC), SAFDB is the world's largest commercially available hash set exclusive to digital steganography applications.

The database is widely used by US and international government and law enforcement agencies, the intelligence community, and private sector digital forensic examiners and network security professionals to detect digital steganography applications on seized digital media or within inbound and outbound network traffic streams.

Discovery of a steganography application during a digital forensics examination is a strong indication the application has been, or will be, used to conceal evidence of criminal activity. Detecting a steganography application in the inbound network traffic stream is a strong indication an insider will use the application to steal sensitive information.



Send2Press® Newswire

SAFDB is an integral part of the Steganography Analyzer Artifact Scanner (StegAlyzerAS), a digital forensics application, and the Steganography Analyzer Real-Time Scanner (StegAlyzerRTS), a network security appliance that detects the presence or use of steganography in the inbound and outbound network traffic stream in real-time.

Existing customers may download updated versions of StegAlyzerAS and StegAlyzerRTS that contains SAFDB v3.8 by logging into their account on the SARC website at <http://www.sarc-wv.com> .

For additional information about Backbone's steganalysis tools, please visit the SARC web site or send email to sarc@backbonesecurity.com .

About the SARC:

The SARC was established to create and maintain a national repository of digital steganography applications, fingerprints, and signatures that can be used during forensic examination of seized digital storage media or when

monitoring network traffic for malicious insider behavior. The Steganography Application Fingerprint Database (SAFDB) is the world's largest database exclusive to digital steganography applications.

About Backbone Security:

In addition to being the leading provider of digital steganalysis tools, Backbone is a Payment Card Industry Data Security Standard (PCI-DSS) Approved Scanning Vendor (ASV) that conducts automated PCI-DSS compliance assessments with their industry leading One-Stop PCI Scan service. Backbone also provides real-time intrusion monitoring, vulnerability assessment, penetration testing, and business continuity and disaster recovery planning services. More information: www.backbonesecurity.com .

– News RSS feed for Backbone Security:

<https://send2pressnewswire.com/author/backbone-security/feed> .

News issued by: Backbone Security



Send2Press® Newswire

Original Image: https://send2pressnewswire.com/image/11-1101-backbone_72dpi.jpg

#

Original Story ID: (6653) :: 2011-02-0201-004

Original Keywords: digital forensics, steganalysis tools, StegAlyzerAS and

StegAlyzerRTS, Steganography Analysis and Research Center, SARC, Backbone Security, networks, private sector digital forensic examiners and network security professionals to detect digital steganography applications on seized digital media Backbone Security Fairmont West Virginia FAIRMONT, W.Va.

Alternate Headline: Version 3.8 of the Steganography Application Fingerprint Database (SAFDB) which now contains more than 900 steganography applications

NEWS ARCHIVE NOTE: this archival news content, issued by the news source via Send2Press Newswire, was originally located in the Send2Press® 2004-2015 2.0 news platform and has been permanently converted/moved (and redirected) into our 3.0 platform. Also note the story "reads" counter (bottom of page) does not include any data prior to Oct. 30, 2016. This press release was originally published/issued: Tue, 01 Feb 2011 19:56:17 +0000