


STEGANOGRAPHIC CONTENT SCREENING OF EXTERNAL DATA FEEDS

A WETSTONE TECHNOLOGIES
STEGOCOMMAND™ WHITE PAPER

THE RISK POSED BY THIRD-PARTY DATA FEEDS

Data feeds from external sources provide many government, financial, education, and research organizations with information essential to the execution of their missions. “These organizations are increasingly seeking insights by tapping into third-party data. This data can include almost anything, from historical demographic and weather data to satellite imagery and private company information.”¹

Data flows from multiple external providers may be significant in volume and the value of the data may be time-dependent. It is, therefore, critical that the processing of these data feeds be able to scale on-demand to accommodate the addition of new external data providers and the growth in quantity of ingested data. Furthermore, data feeds from external sources should be viewed as untrusted and securely screened before the data is allowed inside the network boundaries of the receiving organization.



To ensure the data does not pose a risk to the receiver, it is essential to validate it for format and type conformity and inspect it for the presence of malware and steganographic content. This inspection must be capable of being performed in near real-time in order to make the data available for analytics, data enrichment, research, or other mission needs in a timely manner. The tool used for inspecting data feeds must also integrate easily into existing workflows.

MITIGATING RISK USING STEGANOGRAPHY SCREENING

StegoCommand from WetStone Technologies was developed for organizations who need to inspect and safely ingest data from external providers before making that data available to downstream consumers. These organizations often process common file types, but also have specialized data requirements, unique to their own business needs or their industry. Thus, the provider of the data screening technology must be able to quickly support new file types or changes to the structure or format of a unique data feed.

Secure consumption of external data feeds also demands a resilient infrastructure and, thus, any solution for ingesting and inspecting data feeds must be capable of performing in a highly scalable, portable, stable, and secure cloud-native environment.

StegoCommand builds upon the capabilities of WetStone's industry-leading steganography detection and steganalysis software tool for digital investigators, StegoHunt™. Like StegoHunt, StegoCommand uses a collection of detection algorithms to quickly identify the presence of steganography in suspect carrier files. As an integral step in steganographic screening performed on external data feeds, StegoCommand also validates the type and format conformity of the files passed to it for scanning.

“StegoCommand builds upon the capabilities of WetStone's industry-leading steganography detection and steganalysis software tool for digital investigators, StegoHunt™.”

StegoCommand can be invoked from the Linux command line or from PowerShell. It is easily deployed in most Linux environments, either on-premise or in the cloud, and can scale to support high-volume data feeds, the analysis of very large files and data repositories. By simply provisioning additional compute cores and memory, StegoCommand can scale its processing capability to meet increases in data volume. StegoCommand's signatures and its structural and statistical steganography detection algorithms permit rapid processing of both common and industry-specific file types in near real-time, while also minimizing false-positives and false-negatives.

StegoCommand provides extensive reporting, ranking detections on a severity scale. StegoCommand can integrate into an organization's workflow to ensure that files identified as meeting a certain threat level and probability are quarantined. Once these files are quarantined, WetStone's StegoAnalyst™ provides a comprehensive steganalysis workbench, enabling the examiner to perform a deep investigation of suspect files.

In addition to the tool itself, WetStone's steganography and steganalysis subject matter experts and software developers are available to provide on-going support and services. Professional services include developing algorithms to support steganography detection in additional file types, steganalysis services to provide expert review of detections, and reviewing workflows to meet ever-demanding performance requirements.

STEGOCOMMAND - STEGANOGRAPHY DETECTION FOR STANDARD & INDUSTRY-SPECIFIC FILE TYPES

StegoCommand examines files for structural and statistical indicators of steganographic content and generates a comprehensive report for each scanned file. It detects and reports on the following data hiding techniques:

- // Statistical Anomalies
- // Structural Anomalies
- // The presence of misplaced binary or UTF-8 Data
- // Data Appending
- // Data Prepending
- // File Name Obfuscation
- // The presence of unusual Unicode

StegoCommand can be initiated at the command line or by PowerShell to scan a specific file or to process entire directories. It will traverse an unlimited number of nested archive files. With StegoCommand, users can be assured that all files in an archive will be analyzed, as nested archives are often used in an attempt to conceal the presence of data hiding.

StegoCommand supports several “out-of-the-box” file types for scanning for the presence of steganography. In addition to the standard file types offered, the WetStone Technologies research and development team can work directly with a customer to expand the capabilities to scan for steganography in unique, custom, proprietary, or industry-specific file types.

STANDARD FILE TYPES

- // JPEG
- // BMP
- // GIF
- // PNG
- // WAV
- // MP3
- // ICO
- // JPEG 2000
- // TIFF
- // PCX
- // M4A
- // 3GP
- // M4V
- // MOV
- // MP4
- // AVI
- // FLV
- // MPG
- // ASF
- // OLE (doc, ppt, etc.)
- // Office Files (docx, pptx, etc.)
- // PDF
- // Archive Files (zip, tar, jar, apk, bz2, 7z)
- // ASCII (txt, csv, xml, html)

METEOROLOGICAL AND GEOSPATIAL

- // HDF5
- // NetCDF4
- // BUFR
- // NEXRAD
- // HDF4
- // HSD (Himawari)
- // Rinex
- // OpenGNS

SUMMARY

StegoCommand from WetStone Technologies is currently being used in large cloud-based environments to support data screening operations; specifically verifying whether data received from external sources contains malicious steganographic payloads as embedded content. StegoCommand has a proven ability to identify the presence of steganography in high-volume production data streams in near real-time, while meeting stringent false-positive and false negative requirements.

**For more information, contact
sales@wetstonetech.com**

REFERENCES

¹D. Schatsky, J. Camhi, C. Muraskin, Deloitte Insights, “How third-party information can enhance data analytics”, February 28, 2019, <https://www2.deloitte.com/us/en/insights/focus/signals-for-strategists/smart-analytics-with-external-data.html>