clearswift
by HelpSystems

DATASHEET *(Cybersecurity)*

Anti-Steganography: Combating External Threats and Data Loss in Images

As cyber threats become more evasive, technology that protects organizations must have the capability to look deeper into the content flowing in and out of the network to ensure that the information being shared between users and recipients does not carry a harmful or sensitive payload. Increasingly, attackers are using seemingly innocuous image files to sneak ransomware and spyware into, or sensitive data out of the organization.

Background

"Steganography" is a term used to describe the means of covert communications and comes from the Greek Steganos, or "covered" and the Latin graphia, or 'writing'. Examples of its use go back to 5BC where tyrant, Histiaeus, shaved the head of a servant and tattooed a message on the man's scalp. When the hair had grown back, the servant was sent by Histiaeus to deliver his message - a warning of impending attack by the Persian army - which was revealed when the servant's head was shaved.

In todays digital society, this approach of hiding data amongst innocent files, usually innocuous looking images, has been used by:

- Terror groups such as ISIS and Al-Qaeda to communicate with their followers by hiding messages in images and posting them on pubic websites,
- Malware to contain execution code for infected machines to retrieve and subsequently execute
- People wishing to exfiltrate data from a company by embedding secrets within "normal" files.

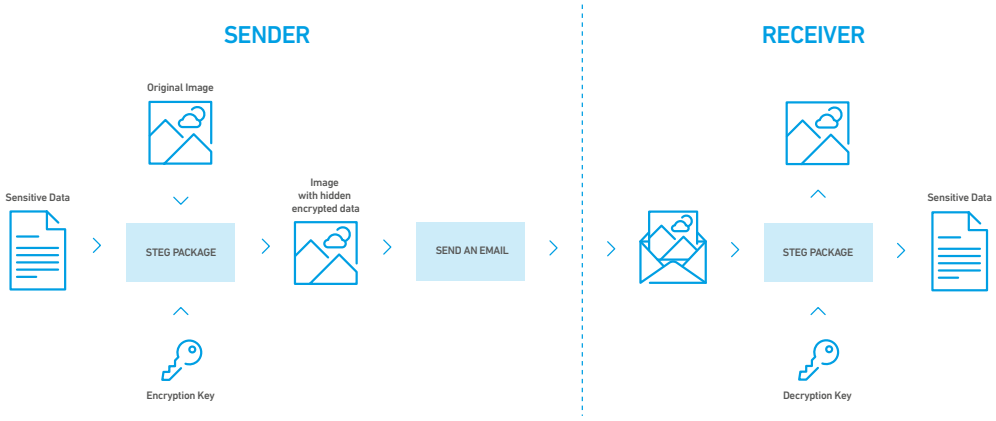
The Problem

Steganography can exploit a number of common file formats in such a way that injecting additional content doesn't change the appearance of the file, so to the naked eye you would never know if the file has been compromised. Compare the two images below. One is a standard, safe image. The other one has 2000 sets of customer details hidden inside of it.

The main file types used to hide data are JPEG, BMP and GIF as these are easily distributed via email and are also used heavily on websites.

To make matters worse, there is no set algorithm for how to embed data into these files which means corresponding applications must be used to encode and decode data hidden in the files. Unless the encoding/decoding package leaves a digital fingerprint, its extremely difficult to detect what package was used to hide the data in the file.

If that doesn't make the task of detecting hidden data hard enough, the encode/decode process can also make use of a password/key to encrypt the payload to make it impossible to identify what secrets were hidden in the carrier file.



The Solution

Given that it's computationally expensive to try and identify if a file contains hidden data and nigh-on impossible to determine what the original data was, the best practice approach is to automatically clean, or sanitize, all images that pass in and out of the network. Sanitization is carried out at the Gateway by disrupting the image, which while not noticeable to the human eye, makes it impossible for a recipient to recover the hidden information.

While this means that some image files may be sanitized unnecessarily, it does mitigate any risk of data being compromised or malware entering the business through a compromised image.

The Clearswift solution cleans the image in milliseconds, so communication flow is not affected. With Clearswift, all images flowing in and out of the network are detected and cleaned, including image files attached to emails or embedded in Office documents such as Word and PDFs shared via the web.

Deployment

The Clearswift Secure Email and Web Gateways can be deployed on premise or in the cloud (either hosted or as a managed service). The anti-steganography feature is part of the Document Sanitization option which offers additional benefits, including the removal of document properties, revision history and other hidden metadata. Due to its high performance implementation, there is no requirement to upgrade hardware or virtual machine sizes. It is fully enabled by license key with no additional software to be installed.

For more information visit **www.clearswift.com**

clearswift
by HelpSystems

www.clearswift.com

About HelpSystems

HelpSystems is a people-first software company focused on helping exceptional organizations Build a Better IT™. Our holistic suite of security and automation solutions create a simpler, smarter, and more powerful IT. With customers in over 100 countries and across all industries, organizations everywhere trust HelpSystems to provide peace of mind. Learn more at www.helpsystems.com.