Solution Brief

Protecting Against Steganographic Threats

Steganography—the art and science of secret hiding—can also be used to hide information in the digital world. A message can be hidden inside an image, audio track, video clip, or text file. It can be used for legitimate purposes, but more often stenography is used by malware.

To avoid detection, some malware uses digital steganography to hide its malicious content within a seemingly innocent "cover" file. This evasion technique takes advantage of the fact that most antimalware signatures detect malicious content in the malware's configuration file. With steganography, the configuration file is embedded in the cover file. In addition, the resulting steganographic file may decrypt into main memory, further reducing the chance of detection. Finally, it is extremely difficult to detect the presence of hidden information such as a configuration file, binary update, or bot command inside a steganographic file. Unfortunately, the use of steganography in cyberattacks is easy to implement and hard to detect.

Policies and procedures for protecting against steganographic attacks

McAfee recommends that organizations take the following steps to protect against steganographic threats.

- **Tighten software delivery and distribution mechanisms to protect against insider threats.** It is always a good idea to have a central repository of trusted corporate applications from which users can download approved software—avoiding the risky practice of letting users download software from unknown sources that may contain stenographic code.
- **Look closely at images.** With the help of image editing software, look for steganography markers such as slight color differences in images. A large number of duplicate colors in an image could be an indicator of a steganographic attack.

McAfee™
Together is power.

- **Control the use of steganography software.** The presence of steganography software on any corporate system should be prohibited unless specifically required for business purposes. Deploy this software only in a contained network segment.
- **Allow only trusted signatures.** Install applications only with trusted signatures from trusted vendors.
- **Configure antimalware to detect binders.** Antimalware software should be configured to identify the presence of binders, which could contain steganographic images.
- **Segment the network.** In the undesirable case of a successful steganographic attack, trusted virtualization architectures combined with proper network segmentation would be helpful to contain an outbreak because the secure and verifiable boot process they use and the continuous traffic monitoring will help to keep applications isolated.
- **Monitor outbound traffic.** Identify the presence of successful steganographic attacks by monitoring outbound traffic.

How McAfee products can protect against steganographic code in malware attacks

McAfee Endpoint Security

Threat Prevention

Ensure McAfee Endpoint Security (ENS) is configured to prevent any known threats from malware that may contain steganographic code:

- Keep McAfee ENS fully up to date with the latest patch, DAT version, and scanning engine.
- Ensure that all systems in your environment are protected and updated.
- Set Real Time Scanning (On Access) to scan all files On Read and On Write. Never turn off scanning On Read, except when configuring low-risk processes.
- Scan exclusion rules should be minimized and used only when necessary. If malware is suspected, ensure that any scan exclusions are temporarily disabled. Learn how to set up exclusions with Knowledge Base article KB88595.
- Understand the performance implications for using High-Risk/Default/Low-Risk Process configurations to limit exposure to steganographic threats in heavily used environments or those in which hardware security is minimal. Learn more about how to improve performance with Endpoint Security KB88205.
- Configure McAfee ENS to use the McAfee Global Threat Intelligence (GTI) file reputation feature. This technology helps bridge the gap between zero-day threats and signature-based detections. Learn about recommended McAfee GTI file reputation settings in KB74983, with more information in KB53735.
- Configure McAfee ENS Access Protection rules to prevent the creation of autorun.inf files.
- Use Access Protection rules to prevent unknown threats from being installed.

Web Control

McAfee ENS Web Control is based on McAfee GTI web reputation and web categorization services. Steganographic-infected software is often located under malware distribution websites.

McAfee ENS Web Control identifies sites—before you visit—that are hosting or are infected by malware, or include inappropriate content.

McAfee Web Control:

- Indicates the relative safety of websites using a color scheme:
  - Green = Safe (very low or no risk)
  - Yellow = Caution (minor risk)
  - Red = Warning (serious risk)
  - Gray = Unknown (not yet rated, use caution)
  - McAfee Secure = tested daily for hacker vulnerabilities
- Is very easily deployed and configured through McAfee ePolicy Orchestrator.
- Provides another layer of endpoint protection. It can be used with Internet Explorer, Firefox, and Chrome.
- Uses effective antispam protection to prevent malicious emails from entering networks.

Read more: McAfee Endpoint Product Guide - Using ENS Web Control

Adaptive Threat Protection

- Enable McAfee Real Protect to apply machine learning techniques to identify advanced threats based on both what they look like and what they might do (pre-execution analysis) and what they do (dynamic behavioral analysis)—all without signatures. Learn more: Adaptive Threat Protection—Real Protect
- Implement McAfee Dynamic Application Containment and follow the recommended best practices. Read more: KB87843.

McAfee VirusScan Enterprise

Customers who have not deployed the latest McAfee ENS should ensure McAfee VirusScan Enterprise (VSE) is configured to prevent any known threats from malware that may contain steganographic code:

- Keep McAfee VSE fully up to date with the latest patch, DAT version, and scanning engine.
- Ensure that all systems in your environment are protected and updated.
- Set Real Time Scanning (On Access) to scan all files On Read and On Write. Never turn off scanning On Read, except when configuring low-risk processes.
- Scan exclusion rules should be minimized and used only when necessary. If malware is suspected, ensure that any scan exclusions are temporarily disabled. Learn how to set up exclusions with Knowledge Base article KB50998.
- In heavily used environments or those in which hardware security is minimal, use High-Risk/Default/Low-Risk Process configurations to limit exposure to steganographic threats. Understand this feature in KB55139 and learn how to configure it in KB58692.
- Configure McAfee VSE to use the McAfee Global Threat Intelligence (GTI) file reputation feature. This technology helps bridge the gap between zero-day threats and signature-based detections. Learn about recommended McAfee GTI file reputation settings in KB74983, with more information in KB53735.
- Configure McAfee VSE Access Protection rules to prevent the creation of autorun.inf files.
- Use Access Protection rules to prevent unknown threats from being installed.

McAfee Application Control

McAfee Application Control is an effective way to block unauthorized applications and code on servers, corporate desktops, and fixed-function devices resulting from steganographic attacks. McAfee Application Control prevents files from being compromised and stops file infectors from spreading across the network.

McAfee Application Control helps secure two major areas:

- **File-based protection:** Defend against file-based attacks, which is typical for steganographic threats. These attacks may attempt to execute new applications or modify current applications.
- **Memory protection:** Defend against memory-based attacks, which can occur from the Internet, across the network, or locally as a result of file execution.

File-based protection

Applications that are not part of the whitelist are neither authorized nor protected. Conversely, whitelisted items are both authorized and protected. If an unauthorized item is introduced to an endpoint (for example, through a download, access over the network, or locally via flash drive or CD), it may be copied to the endpoint, or changed and moved from folder to folder on the endpoint, but at no time can it be executed. Examples of these types of events follow.

Execution Denied	An application that does not appear on the whitelist attempts execution, but is prevented from doing so by McAfee Application Control.
ActiveX Installation Prevented	McAfee Application Control prevents attempts to install unauthorized ActiveX controls.

If an unauthorized process (for example, originating from a malicious file executing on a remote endpoint) or an unauthorized user attempts to modify, rename, move, or delete a whitelisted and hence protected file, McAfee Application Control will block this change. Examples of these types of events follow.

File Write Denied	McAfee Application Control prevents an attempt to modify a whitelisted application by an unauthorized process.
Package Modification Prevented	McAfee Application Control prevents an application using an MSI-based installer package from installation, modification, or removal using an unauthorized mechanism.

Read more: McAfee Application Control Best Practices

McAfee Advanced Threat Defense

McAfee Advanced Threat Defense (ATD) detects stealthy, highly sophisticated packers, encrypted payloads, and zero-day malware with an innovative, layered approach. It combines low-touch antimalware signatures, reputation, and real-time emulation defenses with in-depth static code and dynamic malware analysis (sandboxing) to analyze the behavior of malware.

Read more: FAQs for McAfee Advanced Threat Defense

For Further Reading

McAfee Security Advice Center: Phishing protection

Threat Landscape Dashboard: Sundown exploit kit was updated in late 2016 and discovered to be using steganography to hide exploit code

McAfee
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com