Technical Brief

How to Protect Against Ransomware

Prevent today's ransomware threats with Intel® Security products.

Ransomware is malware that employs asymmetric encryption to hold a victim's information at ransom. Asymmetric (public-private) encryption is cryptography that uses a pair of keys to encrypt and decrypt a file. The public-private pair of keys is uniquely generated by the attacker for the victim, with the private key to decrypt the files stored on the attacker's server. The attacker makes the private key available to the victim only after the ransom is paid, though that is not always the case—as seen in recent ransomware campaigns. Without access to the private key, it is nearly impossible to decrypt the files that are being held for ransom.

Many variations of ransomware exist. Often the ransomware (and other malware) is distributed using email spam campaigns, or through targeted attacks. Intel® Security products leverage a number of technologies that help prevent ransomware. The following McAfee® products and associated configurations are designed to stop many types of ransomware.

McAfee VirusScan® Enterprise 8.8 or McAfee Endpoint Security 10

- Keep DAT files up to date.
- Ensure that McAfee Global Threat Intelligence (McAfee GTI) is in use; it contains more than 8 million unique ransomware signatures.
- Develop Access Protection rules to stop installation of ransomware payloads: Refer to Access Protection Rules Knowledge Base Articles: KB81095 and KB54812.

McAfee Host Intrusion Prevention

- View video on how to configure Host Intrusion Prevention to prevent CryptoLocker payload.
- Enable Host Intrusion Prevention Signature 3894, Access Protection—Prevent svchost.exe executing non-Windows executables.
- Enable Host Intrusion Prevention signatures 6010 and 6011 to block injections immediately.

intel Security

McAfee Host Intrusion Prevention Rules

McAfee Host Intrusion Prevention supports the monitoring of file create, read, write, execute, delete, rename, attribute modification, and hard-link creation. Define which file path/type you want or don't want to alert on and any executables you want to include (known bad sources) or exclude (known creators of false positives). This rule has the potential of being intrusive, so consider using the rule in informational/log mode for a trial period. Note that file protection rules require establishing your trusted applications database.

Rule: Cryptolocker—block EXE in AppData

Rule type: files

Operations: create, execute, write

Parameters:

- Include: Files: **\AppData*.exe
- Include: Files: **\AppData\Local*.exe
- Include: Files: **\AppData\Roaming*.exe

Executables: Include *.*

Note that the following example has omitted many file extensions due to space constraints. Be sure to check all applicable file extensions for your applications.

Rule {

tag "Blocking a Non-Trusted program attempt to write to protected data file extensions"

Class Files

Id 4001

level 4

files {Include "**.3DS" "**.7Z" "**.AB4" "**.AC2" "**.ACCDB" "**.ACCDE" "**.ACCDR" "***.ACCDT" "**.ACR" "**.ADB" "**.AI" "**.AIT" "**.al" "**.APJ" "**.ARW" "**.ASM" "**.ASP" "**.BACKUP" "**.BAK" "**.BDB" "**.BGT" "**.BIK" "**.BKP" "**.BLEND" "**.BPW" "**.C" "**.CDF" "**. CDR" "**.CDX" "**.CE1" "**.CE2" "**.CER" "**.CFP" "**.SRF" "**.SRW" "**.ST4" "**.ST5" "**.ST6" "**.ST7" "**.ST8" "**.STC" "**.STD" "**. STI" "**.STW" "**.STX" "**.SXC" "**.SXD" "**.SXG" "**.SXI" "**.SXM" "**.SXW" "**.TXT" "**.WB2" "**.X3F" "**.XLA" "**.XLAM" "**.XLL" "**. XLM" "**.XLS" "**.XLSB" "**.XLSM" "**.XLSX" "**.XLT" "**.XLTM" "**. XLTX" "**.XLW" "**.XML" "**.ZIP"}

Executable {Include "*"}

user_name{Include "*"}

directives files:writefiles:renamefiles:delete

}

- Access Protection rules: You can also use Access Protection rules to reinforce the Host Intrusion Prevention rule using the flexible wildcard usage: **\Users**\AppData***.exe

Note: With newer versions of SYSCore supplied by updated versions of McAfee VirusScan Enterprise, McAfee Agent, Host Intrusion Prevention, and Data Loss Prevention, the ** no longer functions at the beginning of the "File or folder name to block" field. With newer versions, you need to use the following format:

```
C:\**\AppData\**.exe
```

This is designed to block any random .exe at the root and any subdirectory of a folder named AppData anywhere on the C: drive.

The possible iterations of a rule of this type are almost unlimited, so please carefully consider all aspects of the rule. You may want to consider all aspects of the rule, all possible entries for its intended function, and also how to configure the rules as a whole (example follows):

Process to include: *

Process to exclude: Leave blank

File or folder name to block: <path or directory>

File actions to prevent: Whatever actions you want (recommend that you start with less aggressive actions to minimize possible damage to endpoint)

McAfee SiteAdvisor® Enterprise or Endpoint Security Web Protection

- Use website reputations to prevent or warn users of websites where ransomware is distributed.

McAfee Threat Intelligence Exchange and Advanced Threat Defense

- Threat Intelligence Exchange policy configuration:
  - Start with observation mode—As endpoints are discovered with suspected processes, use system tags to apply Threat Intelligence Exchange enforcement policies.
  - Clean at: known malicious.
  - Block at: most likely malicious (blocking at unknown would provide better protection but may also add initial administrative workload).
  - Submit files to McAfee Advanced Threat Defense at unknown and below.
  - Threat Intelligence Exchange Server policy: Accept Advanced Threat Defense reputations for files not yet seen by Threat Intelligence Exchange.
- Threat Intelligence Exchange Manual Intervention:
  - File reputation enforcement (subject to operation mode)—Most likely malicious—Clean/delete.
  - Might be malicious—Block.
- Enterprise (organizational) reputation can override McAfee GTI:

  - You can choose to block an undesired process, for example, an unsupported or vulnerable application.
  - Mark file as might be malicious.
- Or you can choose to allow an undesired process for testing:
  - Mark file as might be trusted.

McAfee Advanced Threat Protection

- In-box detection capabilities:
  - Signature-based detection—Signatures maintained by McAfee Labs include more than 8 million ransomware signatures including CTB-Locker, CryptoWall, and its variants.
  - Reputation-based detection—McAfee GTI.
  - Real-time static analysis and emulation—Used for signature-less detection.
  - Custom YARA rules.
  - Full static-code analysis—Reverse engineers file code to assess attributes and function sets and fully analyze source code without execution.
  - Dynamic sandbox analysis.
- Create analyzer profiles where ransomware is likely to run:
  - Common OS, Windows 7, 8, XP.
  - Install Windows applications (Word, Excel) and enable macros.
- Provide analyzer profile Internet access:
  - Many samples run a script from a Microsoft document that makes an outbound connection and activates the malware. Providing an analyzer profiles Internet connection and increases detection rates.

McAfee Network Security Platform

- Network Security Platform has signatures in its default policies to detect the following:
  - Verify you have signature id=0x4880f900 (specific to ransomware).
  - Network Security Platform also has signatures to identify TOR, which may be used to transfer files associated with malware.
- Integration with Advanced Threat Defense for new variants of attacks:
  - Configure Advanced Threat Defense integration in advanced malware policy.
  - Configure Network Security Platform to send .exe, Microsoft Office files, Java Archive, and PDF files to Advanced Threat Protection for inspection.
  - Verify Advanced Threat Protection configuration is applied at the sensor level.
- Update callback detection rules (botnet).

McAfee Web Gateway

- Enable McAfee Gateway Anti-Malware inspection.
- Enable McAfee GTI for URL and File reputation:
- Integration with Advanced Threat Defense for sandboxing and zero-day detection.

VirusTotal Convicter: Automated Intervention

- Convicter is a Python script triggered by the McAfee ePolicy Orchestrator® (McAfee ePO™) automated response system to cross-reference a file generating a McAfee Threat Intelligence Exchange threat event with VirusTotal.
- Note that you could alter the script to reference other threat intelligence exchanges, such as GetSusp.
- If the threshold for trusting the community is met, the script will automatically set the enterprise reputation.
- Suggested conviction threshold: 30% of vendors and two majors must agree.
- Filter: Target File Name Does Not Contain: McAfeeTestSample.exe.
- This is a free, community supported tool (not supported by McAfee/Intel Security).

McAfee Active Response

Active Response finds and responds to advanced threats. When used in association with threat feeds such as McAfee GTI, Dell SecureWorks, or ThreatConnect, new threats—including ransomware—can be searched for and eliminated before they have a chance to spread.

- Custom collectors allow you to build specific tools to find and identify indicators of compromise associated with ransomware.
- Triggers and reactions are built by the user to define actions when specific conditions are met. For example, when hashes or file names are found, a delete action can be automatically taken.

For Further Reading

Protecting Against Ransomware

This Knowledgebase article provides customers with the latest detailed information for protecting against ransomware in an Intel Security environment.

For in-depth information about the different CryptoLocker ransomware variants, symptoms, attacked vectors, and prevention techniques, review the following videos:

- CrytpoLocker Malware Session
- CryptoLocker Update

McAfee Labs Threat Advisory: X97M/Downloader

This article provides customers with a detail analysis of a latest version of ransomware.

Defeat Ransomware: Ensure Your Data Is Not Taken Hostage

Four-page solution brief outlines what ransomware is and how some of (but not all) Intel Security solutions help protect against it.

Advice for Unfastening CryptoLocker Ransomware

Detailed blog article on what a customer should do after a ransomware attack.

Ransomware Returns: New Families Emerge with a Vengeance

McAfee Labs Threat Report article (page 14) highlighting new and evolving ransomware.

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