Intel Security Group
Combating Ransomware

Protecting against Ransomware

How to provide another layer of defense

Crypto based ransomware keeps on reinventing itself in order to get through security defenses. New variants are tested against security vendors in order to avoid detection. While some become less active at times such as Cryptolocker or CTB-Locker, others gain ground like Teslacrypt or CryptoWall. Vigilance is needed to prevail as new variants are seen to reemerge with similar behaviors.

This document aims at providing another layer of defense against a highly professionalized, for-profit malware industry that is constantly innovating and trying to either circumvent known security measures or exploit unsecure or outdated systems. By identifying similar patterns of behavior within different variants we have come up with some proactive rules for endpoint products: VirusScan Enterprise (VSE) and Host Intrusion Prevention (HIP). These rules aim at effectively preventing the installation and / or the payload of historical, current, and evolving new variants of all these threats.

Please note the rules suggested in this document for a particular variant do not provide protection for prior/other variants unless otherwise stated and are meant to be implemented in a cumulative manner.

The encryption technique used in the payload makes the recovery of the encrypted files impossible as once executed the private key required is only available to the author.

The use of HIP rules as detailed in the hands-on videos and section below have been proven to be very effective at stopping all current and new variants of these threats. We recommend these to be reviewed, tested, and implemented.

Prior to implementing the recommendations below, it is essential that the rules are tested thoroughly to ensure their integrity and also that no legitimate application, in-house developed or otherwise, is deemed malicious and prevented from functioning in your production environment.

For an in-depth coverage of the different Cryptolocker variants, symptoms, attack vectors, and prevention techniques please review the following videos:

1. Cryptolocker Malware Session **here**
2. Cryptolocker Update **here**

The Q&A document corresponding to the Cyptolocker Malware Session can be found **here**.

VSE Access Protection

The rules suggested in this section can be set in “report-only” mode for testing purposes in order to check if they cause any conflict in your environment. Once it is determined that they will not block any activity from legitimate applications, you can set them to block and apply these settings to all relevant systems.

The paths in suggested Access Protection Rules will need to be adjusted when the language of the operating system is different from English to the corresponding locations in that language.

Disclaimer:
Usage of *.* in an Access Protection rule would prevent all types of files from running and being accessed from that specific location. If specifying a process path under “Processes to Include”, the use of wildcards for Folder Names may lead to unexpected behavior. Users are requested to make this rule as specific as possible.

For reference purposes please review the following KB articles to configure Access Protection Rules in VirusScan Enterprise:

KB81095 - How to create a user-defined Access Protection Rule from a VSE 8.x or ePO 5.x console
KB54812 - How to use wildcards when creating exclusions in VirusScan Enterprise 8.x

Cryptolocker v.I

These are the Access Protection Rules that can be setup in VSE to stop the installation and payload of this variant in your environment.

Rule #	Action	Windows 7	File Actions to Prevent
1	File/Folder Blocking Rule		New files being created Files being executed
	Processes to include	*	
	File or Folder Name to Block	*\Users*\AppData*.exe [1]	
2	File/Folder Blocking Rule		New files being created
	Processes to include	*\Users*\AppData\Roaming*.exe [1]	
	File or Folder Name to Block	*.tmp.*	
3	Registry Blocking Rule		Create Key or Value
	Processes to include	*	
	Value to Block (HKCU)	Software/CryptoLocker*	

[1] **Windows XP use: *\Documents and Settings*\Application Data*.exe**

Cryptolocker v.II

VSE Access Protection Rules cannot influence the payload of this variant.

Cryptolocker v.III

Rule #	Action	Windows 7	File Actions to Prevent
1	File/Folder Blocking Rule		New files being created
	Processes to include	*\Users*\AppData\Roaming*.exe [1]	
	File or Folder Name to Block	*.*.cry	

[1] **Windows XP use: *\Documents and Settings*\Application Data*.exe**

Cryptolocker v.IV

The following Access Protection Rules can be setup to prevent installation and encryption phases.

Rule #	Action	Windows 7	File Actions to Prevent
1	File/Folder Blocking Rule		New Files being created Files being executed
	Processes to include	*	
	File or Folder Name to Block	*decrypt_instructions.*	
2	File/Folder Blocking Rule		New files being created
	Processes to include	*\Users*\AppData\Roaming*.exe [1]	
	File or Folder Name to Block	*.*.encrypted	
3	File/Folder Blocking Rule		Write access to files
	Processes to include	*	
	File or Folder Name to Block	*\Users*\AppData\Roaming*.exe [1]	

[1] **Windows XP use: *\Documents and Settings*\Application Data*.exe**

CryptoWall

The infection causes explorer.exe to be injected from the payload, which in turn enumerates and injects svchost.exe. Then the routine to call home and initiate the encryption routine is invoked. This rule will help disrupt this routine:

Rule #	Action	Windows	File Actions to Prevent
1	File/Folder Blocking Rule		Files being executed
	Processes to include	explorer.exe	
	File or Folder Name to Block	svchost.exe	

In order to stop the re-start mechanism:

Rule #	Action	Windows	File Actions to Prevent
2	Registry Blocking Rule		Write to Key or Value
	Processes to include	explorer.exe	
	Value to Block (HKALL)	Software/Microsoft/Windows/CurrentVersion/Run	

Teslacrypt v.I / v.II

This threat writes to the user's application data directory. By preventing the payload from writing to this directory it stays in an infinite loop attempting to write the file. The restart mechanism is not introduced preventing the threat from surviving a reboot.
Suggested rule to accomplish this:

Rule #	Action	Windows 7	File Actions to Prevent
1	File/Folder Blocking Rule		New files being created Files being executed
	Processes to include	*	
	or more granular	*\Users*\AppData\Local\temp* [1]	
	File or Folder Name to Block	*\Users*\AppData\Roaming*.exe [2]	

[1] **Windows XP use: *\Documents and Settings*\Local Settings\Temp***

[2] **Windows XP use: *\Documents and Settings*\Application Data*.exe**

Teslacrypt v.III

VSE Access Protection Rules cannot influence the payload of this variant.

Teslacrypt v.IV

This threat writes to the user's document directory. By preventing the executable from writing to or creating anything on the system, the malware will not be able to encrypt the user's files.
Suggested rule to accomplish this:

Rule #	Action	Windows 7	File Actions to Prevent
1	File/Folder Blocking Rule		Write access to files New files being created
	Processes to include	*\Users*\Documents*.exe [1]	
	File or Folder Name to Block	*	

[3] **Windows XP use: *\Documents and Settings*\My Documents*.exe**

Locky v.I

This attempts to create a registry key in HKCU. By preventing the payload from creating the key, the malware will execute cmd.exe /C del /Q /F <payload>. The restart mechanism is not introduced preventing the threat from surviving a reboot.
Suggested rule to accomplish this:

Rule #	Action	Windows	File Actions to Prevent
1	Registry Blocking Rule		Create key or value
	Processes to include	*	
	Key to Block	[HKCU] /Software/Locky	

Locky v.II

VSE Access Protection Rules cannot directly influence the payload of this variant as the key is randomly generated, however, you can leverage the Generic mildly aggressive rule #4 to help protect against JS/Nemucod Downloaders.

NanoLocker

This attempts to store the full path of all the encrypted documents in a text file named lansrv.ini located in "%USERPROFILE%\AppData\Local". If it fails to create this file, it aborts execution without encrypting any file and without replicating.
Suggested rule to accomplish this:

Rule #	Action	Windows 7	File Actions to Prevent
1	File/Folder Blocking Rule		New files being created
	Processes to include	*	
	File or Folder Name to Block	*\Users*\AppData\Local\lansrv.ini [1]	

[1] **Windows XP use: *\Documents and Settings*\Local Settings\Application Data\lansrv.ini**

Petya

VSE Access Protection Rules cannot influence the payload of this variant.

Generic mildly aggressive Access Protection Rules

The following rules can be used to prevent some additional variants. Careful testing is advised to ensure exceptions are incorporated prior to deploying to a production environment. Although they can be very effective at blocking these threats, if not configured correctly, they can have an impact to business by blocking legitimate application behaviors.

Rule #	Action	Windows 7	File Actions to Prevent
1	File/Folder Blocking Rule		New files being created Files being executed
	Processes to include	*	
	File or Folder Name to Block	*\Users*\AppData**.exe [1]	
2	File/Folder Blocking Rule		Files being executed
	Processes to include	*	
	File or Folder Name to Block	*\Users*\AppData**.scr [2]	
3	File/Folder Blocking Rule		New files being created
	Processes to include	iexplore.exe	
	File or Folder Name to Block	*\Users*\AppData\Local\Temp*.tmp [3]	
4	File/Folder Blocking Rule		New files being created
	Processes to include	?SCRIPT.EXE	
	File or Folder Name to Block	*\Users*\AppData\Local\temp*.exe [4]	

[1] **Windows XP use: *\Documents and Settings*\Application Data**.exe**

[2] **Windows XP use: *\Documents and Settings*\Application Data**.scr**

[3] **Windows XP use: *\Documents and Settings*\Local Settings\Temp*.tmp**

[4] **Windows XP use: *\Documents and Settings*\Local Settings\Temp*.exe**

Rules to help track systems that have been affected by these threats

Some rules can also be put in place to help identify systems affected by this threats. These rules are for information / tracking purposes and will not prevent the infection or encryption from taking place.

Rule #	Action	Windows	File Actions to Prevent
1	File/Folder Blocking Rule		New files being created
	Processes to Include	*	
	File or Folder Name to Block	*HELP_DECRYPT.HTML	
		*HELP_DECRYPT.TXT	
2	File/Folder Blocking Rule		New files being created
	Processes to Include	*	
	File or Folder Name to Block	*Howto_RESTORE_FILES.BMP	
		*Howto_RESTORE_FILES.HTML	
3	File/Folder Blocking Rule		New files being created
	Processes to Include	*	
	File or Folder Name to Block	*HELP_YOUR_FILES.HTML	
		*HELP_YOUR_FILES.TXT	
		*HELP_YOUR_FILES.PNG	

Host Intrusion Prevention Signatures

Please ensure you plan and configure your Trusted Applications or exclusion list to prevent false detections in your environment. We have created a video that demonstrates how to setup the rules described below in HIP. We recommend you view this and use the updated TXT file in the following link with the HIP rule.

Please ensure that these HIP rules are tested in a non-business impacting representative subset of your production environment prior to a wider distribution in your network.

You can view it in here: **https://community.mcafee.com/videos/1859**

A text file with HIP rule updated to cover all current Cryptolocker versions and CryptoWall can be downloaded from the community **https://community.mcafee.com/docs/DOC-6553**

Enable Signature 3894, Access Protection—Prevent svchost executing non-Windows executables.
***NOTE:** The signature is disabled by default so will need to be enabled.

CryptoWall
HIP signatures 6010 and 6011 block the injection immediately. Ensure they are enabled.

Target extensions:
3DM, 3DS, 3G2, 3GP, 7Z, AB4, ACCDB, ACCDE, ACCDR, ACCDT, ACH, ACR, ACT, ADB, ADS, AI, AIT, AL, APJ, ARW, ASF, ASM, ASP, ASX, AVI, BACK, BACKUP, BAK, BANK, BAY, BDB, BGT, BIK, BKF, BKP, BLEND, BPW, C, CDB, CDF, CDR, CDX, CE1, CE2, CER, CFP, CGM, CLASS, CLS, CMT, CNV, CPI, CPP, CR2, CRAW, CRT, CRW, CS, CSH, CSL, CSV, DAC, DB, DB3, DBF, DBR, DBS, DC2, DCR, DCS, DCX, DDD, DDOC, DDS, DER, DES, DESIGN, DGC, DJVU, DNG, DOC, DOCM, DOCX, DOT, DOTM, DOTX, DRF, DRW, DTD, DWG, DXB, DXF, DXG, EBD, EDB, EML, EPS, ERF, EXF, FDB, FFD, FFF, FH, FHD, FLA, FLAC, FLV, FM, FP7, FPX, FXG, GDB, GRAY, GREY, GRW, GRY, H, HBK, HPP, IBD, IDX, IIF, INDD, JAVA, JPE, JPEG, JPG, KDBX, KDC, KEY, LACCDB, LUA, M, M4V, MAF, MAM, MAQ, MAR, MAW, MAX, MDB, MDC, MDE, MDF, MDT, MEF, MFW, MMW, MOS, MOV, MP3, MP4, MPG, MPP, MRW, MSO, MYD, NDD, NEF, NK2, NRW, NS2, NS3, NS4, NSD, NSF, NSG, NSH, NWB, NX1, NX2, NYF, OBJ, ODB, ODC, ODF, ODG, ODM, ODP, ODS, ODT, OIL, ONE, ORF, OTG, OTH, OTP, OTS, OTT, P12, P7B, P7C, PAGES, PAS, PAT, PBO, PCD, PCT, PDB, PDD, PDF, PEF, PEM, PFX, PHP, PIP, PL, PLC, POT, POTM, POTX, PPAM, PPS, PPSM, PPSX, PPT, PPTM, PPTX, PRF, PS, PSAFE3, PSD, PSPIMAGE, PTX, PUB, PUZ, PY, QBA, QBB, QBM, QBW, QBX, R3D, RAF, RAR, RAT, RAW, RDB, RM, RTF, RWZ, SAS7BDAT, SAY, SD0, SDA, SDF, SNP, SQL, SR2, SRF, SRT, SRW, ST4, ST5, ST6, ST7, ST8, STC, STD, STI, STW, STX, SVG, SWF, SXC, SXD, SXG, SXI, SXM, SXW, TEX, TGA, THM, TLG, TXT, VOB, VSD, VSX, VTX, WAV, WB2, WBK, WDB, WLL, WMV, WPD, WPS, X11, X3F, XLA, XLAM, XLB, XLC, XLK, XLL, XLM, XLR, XLS, XLSB, XLSM, XLSX, XLT, XLTM, XLTX, XLW, XPP, XSN, YUV, ZIP

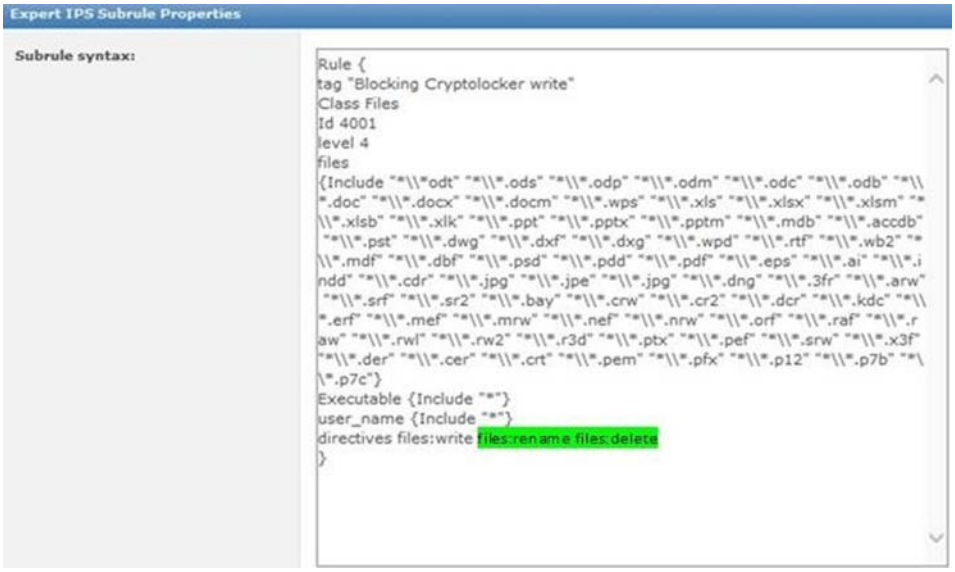
Cryptolocker v.I, v.II, v.IV, Teslacrypt, and Locky

They use their own process to perform the encryption.
In order to provide protection for these variants you need to setup a rule to prevent non-trusted processes to write, rename & delete the list of protected extensions. Please use the rule available at:
https://community.mcafee.com/docs/DOC-6553 as a template and update the actions and file types.

Cryptolocker Target Extensions:
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, CGM, CLS, CMT, CPI, CPP, CR2, CRAW, CRT, CRW, CSH, CSL, CSS, CSV, DAC, DB, DB3, DBF, DC2, DCR, DCS, DDD, DDOC, DER, DESIGN, DGC, DJVU, DNAXML, DNG, DOC, DOCM, DOCX, DOT, DOTM, DOTX, DRF, DRW, DWG, DXB, , ERF, EXF, FDB, FFD, FFF, FH, FHD, FPX, FXG, GRAY, GREY, GRY, H, HBK, HPP, IBD, IDX, JPEG, JPG, JS, KDBX, KDC, LUA, MDB, MDC, MEF, MFW, MMW, MOS, MPG, MRW, MYD, NDD, NEF, NRW, NS2, NS3, NS4, NSD, NSF, NSG, NSH, NWB, NX1, NX2, NYF, ODB, ODF, ODG, ODM, ODP, ODS, ODT, ORF, OTG, OTH, OTP, OTS, OTT, P12, P7B, P7C, PAT, PCD, PDF, PEF, PEM, PFX, PHP, PL, POT, POTM, POTX, PPAM, PPS, PPSM, PPSX, PPT, PPTM, PPTX, PS, PSAFE3, PSD, PTX, PY, RAF, RAR, RAW, RDB, RTF, RWZ, SAS7BDAT, SAV, SD0, SD1, SDA, SDF, SQL, SR2, 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

Teslacrypt Target Extensions:
7Z, ACCDB, AI, APK, ARCH00, ARW, AVI, BAR, BAY, BIG, BIK, BKF, BKP, BLOB, BSA, CAS, CDR, CER, CFR, CR2, CRT, CRW, CSS, CSV, DAS, DB0, DBA, DBF, DCR, DER, DESC, DMP, DNG, DOC, DOCM, DOCX, DWG, DXG, EPS, ERF, ESM, FF, FLV, FORGE, FOS, FPK, FSH, GDB, GHO, INDD, ITL, ITM, IWD, IWI, JPE, JPEG, JPG, JS, KDB, KDC, LAYOUT, LRF, LTX, LVL, M2, M3U, M4A, MAP, MDB, MDBACKUP, MDF, MEF, MENU, MOV, MP4, NCF, NRW, ODB, ODC, ODM, ODP, ODS, ODT, ORF, P12, P7B, P7C, PAK, PDD, PDF, PEF, PEM, PFX, PNG, PPT, PPTM, PPTX, PSD, PSK, PST, PTX, PY, QDF, QIC, R3D, RAF, RAR, RAW, RB, RTF, SAV, SB, SID, SIS, SLM, SNX, SQL, SR2, SRF, SRW, SUM, SVG, TAX, TOR, TXT, UPK, VCF, VDF, VPK, VTF, W3X, WB2, WMA, WMO, WMV, WPD, WPS, X3F, XLK, XLS, XLSB, XLSM, XLSX, XXX, ZIP, ZTMP

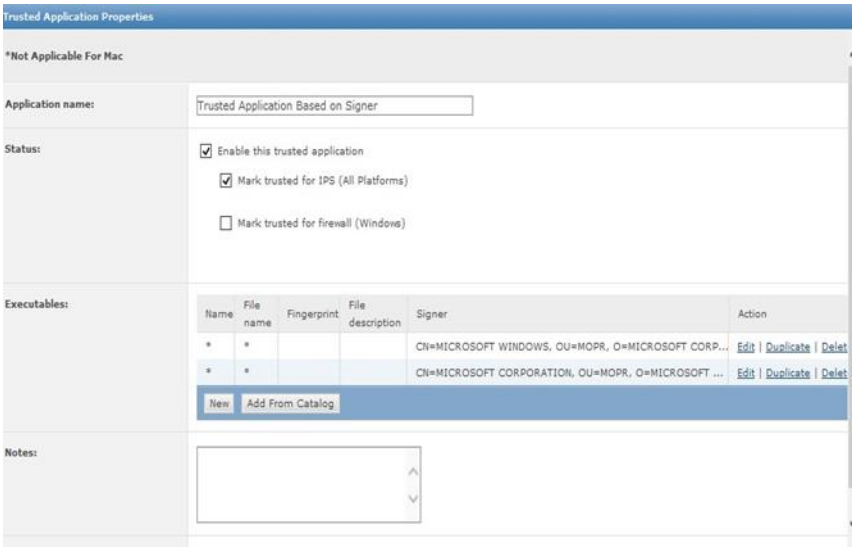
The rule should look like this in the user interface:

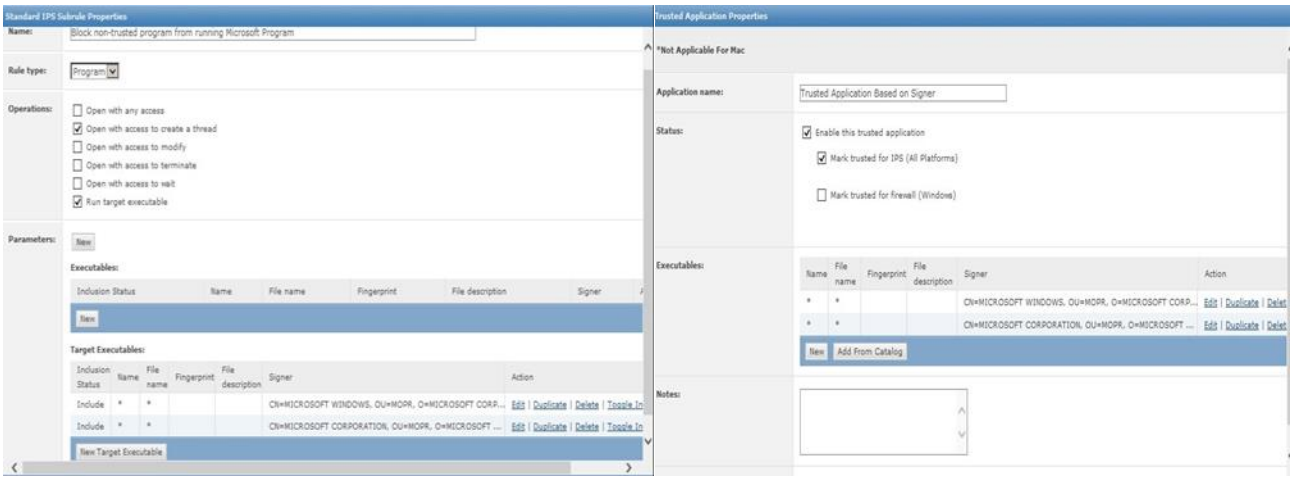


***NOTE: File directives rename/delete have been added to include Cryptolocker v.IV & CryptoWall since the video in the community was created. This is reflected in the updated HIP rule TXT file.

Cryptolocker v.III
To fight this variant you need to setup a rule to prevent non-trusted processes calling trusted processes

The rule should look like this:





For reference purposes please review the following KB articles to configure HIP:

- To blacklist applications using a Host Intrusion Prevention custom signature refer to **KB71329**
- To create an application blocking rules policies to prevent the binary from running refer to **KB71794**
- To create an application blocking rules policies that prevents a specific executable from hooking any other executable refer to **KB71794**
- To block attacks from a specific IP address through McAfee Nitrosecurity IPS refer to **KB74650**

Propagation Prevention

A common vector to introduce these threats into corporate environments is via spam emails with attachments. They appear from legitimate sources and encourage users to click on them. The following configurations can help provide another layer of defense:

Block double extension attachments

VirusScan On-Delivery Email you can configure to “Find attachments with multiple extensions” under the Heuristics section.

HIP signature 413 “Suspicious Double File Extension Execution” is able to prevent double extension attachments from running. This signature is enabled by default on severity level High.

File Filtering

McAfee gateway products like McAfee Email Gateway and McAfee Security for Microsoft Exchange can implement file filtering policies by file name or file format that can stop .SCR, .EXE and .CAB files reaching user’s desktops. Implementing these policies can help reduce new variants using this propagation vector.