

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industry that is constantly innovating and trying to either circumvent known security measures or exploit unsecure or outdated systems.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), Endpoint Security (ENS) 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 Cryptolocker Malware Session can be found [here](#).

VirusScan Enterprise and Endpoint Security 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 and Endpoint Security:

[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

[KB86577](#) - How to create a user-defined Access Protection Rule for a file or folder registry

Cryptolocker v.IV

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

VirusScan Enterprise

Rule #	Action	Windows 6.x	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_instruction*.*	
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

Endpoint Security

Rule #	Action	Windows 6.x	Operations
1	SubRule Type: Files		Create Execute
	Executables [Include]	*	
	SubRule [Include]	*decrypt_instruction*.*	
2	SubRule Type: Files		Create
	Executables [Include]	*\Users*\AppData\Roaming*.exe ¹	
	SubRule [Include]	*.*.encrypted	
3	SubRule Type: Files		Write
	Executables [Include]	*	
	SubRule [Include]	*\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:

VirusScan Enterprise

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	

Endpoint Security

Rule #	Action	Windows	Operations
1	SubRule Type: Files		Execute
	Executables [Include]	explorer.exe	
	SubRule [Include]	svchost.exe	

In order to stop the re-start mechanism:

VirusScan Enterprise

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	

Endpoint Security

Rule #	Action	Windows	Operations
2	SubRule Type: Registry Value		Write
	Executables [Include]	explorer.exe	
	SubRule Value [Include]	*/Software/Microsoft/Windows/CurrentVersion/Run	

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:

VirusScan Enterprise

Rule #	Action	Windows 6.x	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	*	

¹ Windows XP use: *\Documents and Settings*\My Documents*.exe

Endpoint Security

Rule #	Action	Windows 6.x	Operations
1	SubRule Type: Files		Create
	Executables [Include]	*\Users*\Documents*.exe ¹	
	SubRule [Include]	*	

¹ Windows XP use: *\Documents and Settings*\My Documents*.exe

Locky v.II

This threat will create an encrypted version of the original documents, with a .locky extension appended to them. By preventing the creation of these, the original file will not be encrypted. Additionally you can leverage the Generic mildly aggressive rule #4 to help protect against JS/Nemucod Downloaders.

VirusScan Enterprise

Rule #	Action	Windows 6.x	File Actions to Prevent
1	File/Folder Blocking Rule		New files being created
	Processes to include	*	
	File or Folder Name to Block	*.locky	

Endpoint Security

Rule #	Action	Windows 6.x	Operations
1	SubRule Type: Files		Create
	Executables [Include]	*	
	SubRule [Include]	*.locky	

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:

VirusScan Enterprise

Rule #	Action	Windows 6.x	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

Endpoint Security

Rule #	Action	Windows 6.x	Operations
1	SubRule Type: Files		Create
	Executables [Include]	*	
	SubRule [Include]	*\Users*\AppData\Local\lansrv.ini ¹	

² 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.

VirusScan Enterprise

Rule #	Action	Windows 6.x	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	
5	File/Folder Blocking Rule		New files being created Files being executed
	Processes to include	*	
	File or Folder Name to Block	*\Users*\AppData*.exe ¹	
6	File/Folder Blocking Rule		New files being created
	Processes to include	*\Users*\AppData\Roaming*.exe ¹	
	File or Folder Name to Block	*.tmp.*	
7	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

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

Endpoint Security

Rule #	Action	Windows 6.x	Operations
1	SubRule Type: Files		Create Execute
	Executables [Include]	*	
	SubRule [Include]	*\Users*\AppData**.exe ¹	
2	SubRule Type: Files		Execute
	Executables [Include]	*	
	SubRule [Include]	*\Users*\AppData**.scr ²	
3	SubRule Type: Files		Create
	Executables [Include]	iexplore.exe	
	SubRule [Include]	*\Users*\AppData\Local\Temp*.tmp ³	
4	SubRule Type: Files		Create
	Executables [Include]	?SCRIPT.EXE	
	SubRule [Include]	*\Users*\AppData\Local\temp*.exe ⁴	
5	SubRule Type: Files		Create Execute
	Executables [Include]	*	
	SubRule [Include]	*\Users*\AppData*.exe ¹	
6	SubRule Type: Files		Create
	Executables [Include]	*\Users*\AppData\Roaming*.exe ¹	
	SubRule [Include]	*.tmp.*	
7	SubRule Type: Files		Write
	Executables [Include]	*	
	SubRule [Include]	*\Users*\AppData\Roaming*.exe ¹	

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.

VirusScan Enterprise

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	
4		*HELP_YOUR_FILES.PNG	New Files being created Files being executed
	File/Folder Blocking Rule		
	Processes to include	*	
	File or Folder Name to Block	*decrypt_instruction.*	

Endpoint Security

Rule #	Action	Windows	Operations
1	SubRule Type: Files		Create
	Executables [Include]	*	
	SubRule [Include]	*HELP_DECRYPT.HTML	
		*HELP_DECRYPT.TXT	
2	SubRule Type: Files		Create
	Executables [Include]	*	
	SubRule [Include]	*Howto_RESTORE_FILES.BMP	
		*Howto_RESTORE_FILES.HTML	
3	SubRule Type: Files		Create
	Executables [Include]	*	
	SubRule [Include]	*HELP_YOUR_FILES.HTML	
		*HELP_YOUR_FILES.TXT	
		*HELP_YOUR_FILES.PNG	
4	SubRule Type: Files		Create
	Executables [Include]	*	
	SubRule [Include]	*decrypt_instruction*.*	

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.

***NOTE: These signatures will be triggered whether or not an application is Trusted for IPS. In order to suppress legitimate signature violations, exceptions must be added to the enforced IPS Rules policy.

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, LACCD, 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, SDO, 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 from modifying the list of protected extensions with the following attributes: **write, rename & delete**

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, SDO, SD1, SDA, SDF, SQL, SR2, SRF, SRW, ST4, ST5, ST6, ST7, ST8, STC, STD, STI, STW, STX, SXC, XSD, 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, GH0, 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:

Trusted Application Properties

*Not Applicable For Mac

Application name: Trusted Application Based on Signer

Status:

- ☒ Enable this trusted application
- ☒ Mark trusted for IPS (All Platforms)
- ☐ Mark trusted for firewall (Windows)

Executables:

Name	File name	Fingerprint	File description	Signer	Action
*	*			CN=MICROSOFT WINDOWS, OU=MOPR, O=MICROSOFT CORP...	Edit Duplicate Delete
*	*			CN=MICROSOFT CORPORATION, OU=MOPR, O=MICROSOFT ...	Edit Duplicate Delete

New Add From Catalog

Notes:

Standard IPS Inhibit Properties

Name: Block non-trusted program from running Microsoft Program

Rule type: Program

Operations:

- ☐ Open with any access
- ☒ Open with access to create a thread
- ☐ Open with access to modify
- ☐ Open with access to terminate
- ☐ Open with access to wait
- ☒ Run target executable

Parameters:

Executables:

Inclusion Status	Name	File name	Fingerprint	File description	Signer

Target Executables:

Inclusion Status	Name	File name	Fingerprint	File description	Signer	Action
Include	*	*			CN=MICROSOFT WINDOWS, OU=MOPR, O=MICROSOFT CORP...	Edit Duplicate Delete Toggle In
Include	*	*			CN=MICROSOFT CORPORATION, OU=MOPR, O=MICROSOFT ...	Edit Duplicate Delete Toggle In

New Target Executable

Trusted Application Properties

*Not Applicable For Mac

Application name: Trusted Application Based on Signer

Status:

- ☒ Enable this trusted application
- ☒ Mark trusted for IPS (All Platforms)
- ☐ Mark trusted for firewall (Windows)

Executables:

Name	File name	Fingerprint	File description	Signer	Action
*	*			CN=MICROSOFT WINDOWS, OU=MOPR, O=MICROSOFT CORP...	Edit Duplicate Delete
*	*			CN=MICROSOFT CORPORATION, OU=MOPR, O=MICROSOFT ...	Edit Duplicate Delete

New Add From Catalog

Notes:

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.