# Intel Security Group

## Combating Cryptolocker, Cryptowall & Teslacrypt

## Protecting against Cryptolocker, CryptoWall & Teslacrypt

### How to provide another layer of defence

Crypto based ransomware keeps on reinventing itself in order to get through security defences. New variants are tested against security vendors in order to avoid detection. Whilst some become less active at times such as Cryptolocker or CTB-Locker others gain ground like Teslacrypt or CryptoWall. However vigilance needs to prevail as new variants are seen to re-emerge with similar behaviours.

This document aims at providing another layer of defence against a highly professionalised, 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industry that is constantly innovating and trying to either circumvent known security measures or exploit unsecure or outdated systems.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 behaviour 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 prevent the installation and / or the payload of historical, current as well as 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 an accumulative manner.

The encryption technique used in the payload make 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 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 mode only for testing purposes in order to check if they cause any conflict in your environment. Once it is established 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.

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 or Folder Name to block | **\Users*\AppData**.exe [1] | New Files being created. |
| | Processes to include | * | Files being executed. |
| 2 | File or Folder Name to block<br>Processes to include | **.tmp.tmp<br>* | New Files being created. |
| 3 | Registry Blocking | [HKCU] \Software\CryptoLocker* | Create Key or Value |
| | Processes to include | * | |

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

[2] **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

| | Action | Windows 7 | File Actions to Prevent |
|---|---|---|---|
| 4 | File or Folder Name to block | **.*cry | New Files being created. |
| | Processess to include | * | |

## Cryptolocker v.IV

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

| | Action | Windows 7 | File Actions to Prevent |
|---|---|---|---|
| 5 | File or Folder Name to block | **\decrypt_instruction.* | New Files being created. |
| | Process to include | * | Files being executed. |
| 6 | File or Folder Name to block<br>Process to include | **.*.encrypted<br>* | New Files being created. |
| 7 | File or Folder Name to block | **\Users*\AppData\Roaming*.exe [1] | New Files being created. |
| | Processes to include | * | Write access to files. |
| 8 | File or Folder Name to block | ***.scr | New Files being created. |
| | Process to include | * | |
| | Process to exclude | rundll32.exe, winlogon.exe, FrameworkService.exe, McShield.exe, Scan*.exe | Files being executed. |

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

Add only known legitimate programs under the “Application Data” folder to “Processes to exclude”.

## 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, but please ensure the process include is listed as explorer.exe. Failure to do this can cause the system to stop functioning and manual intervention be required.

| | Action | Windows | Action to Block |
|---|---|---|---|
| 9 | File or Folder Name to block | Svchost.exe | Execute |
| ** | Process to include | explorer.exe | |

In order to stop the re-start mechanism:

| | Action | Windows 7 | Registry Action to Block |
|---|---|---|---|
| 10 | Registry Blocking Rule | | Write to Key or Value |
| | Value to Block | [HKALL] \Software\Microsoft\Windows\CurrentVesion | |
| | Processes to include | explorer.exe | |

### Teslacrypt

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

| | Action | Windows 7 | File Actions to Prevent |
|---|---|---|---|
| 11 | File or Folder Name to block | **\Users*\AppData\Roaming*.exe | Execute |
| | Process to include | * | Creation |

*** **Disclaimer**:
Usage of *.* in 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 c behaviour. Users are requested to make this rule as specific as possible.

### Generic mildly aggressive access protection rules

The following rules can be used to prevent some additional variants but require careful testing 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 blocking correct operation of legitimate applications.

| | Action | Windows 7 | File Actions to Prevent |
|---|---|---|---|
| 12 | File or Folder Name to block | **\Users***.exe | Execute |
| | Process to include | * | Creation |

| | Action | Windows 7 | File Actions to Prevent |
|---|---|---|---|
| 13 | File or Folder Name to block | **\Users***.scr | Execute |
| | Process to include | * | Creation |

| | Action | Windows 7 | File Actions to Prevent |
|---|---|---|---|
| 14 | File or Folder Name to block | **\Users*\appdata\local\temp*.tmp | Creation |
| | Process to include | iexplore.exe | |

**Note:** When implemented **rule #12** supersedes rules #1, #7 and #11 & **rule #13** supersedes rule #8

### Rules to help track systems that have been affected by these threat families

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

| | Action | Monitor for CryptoWall | File Actions to Prevent |
|---|---|---|---|
| 15 | File or Folder Name to block | **\HELP_DECRYPT.HTML | Creation |
| | | **\HELP_DECRYPT.TXT | |
| | Process to include | * | |

| | Action | Monitor for Teslacrypt | File Actions to Prevent |
|---|---|---|---|
| 16 | File or Folder Name to block | **\Howto_RESTORE_FILES.bmp | Creation |
| | | **\Howto_RESTORE_FILES.html | |
| | Process to include | * | |

| | Action | Monitor for CryptoWall (ii) | File Actions to Prevent |
|---|---|---|---|
| 17 | File or Folder Name to block | **\HELP_YOUR_FILES.HTML | Creation |
| | | **\HELP_YOUR_FILES.TXT | |
| | | **\HELP_YOUR_FILES.PNG | |
| | Process to include | * | |

## 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 HIPs. 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**

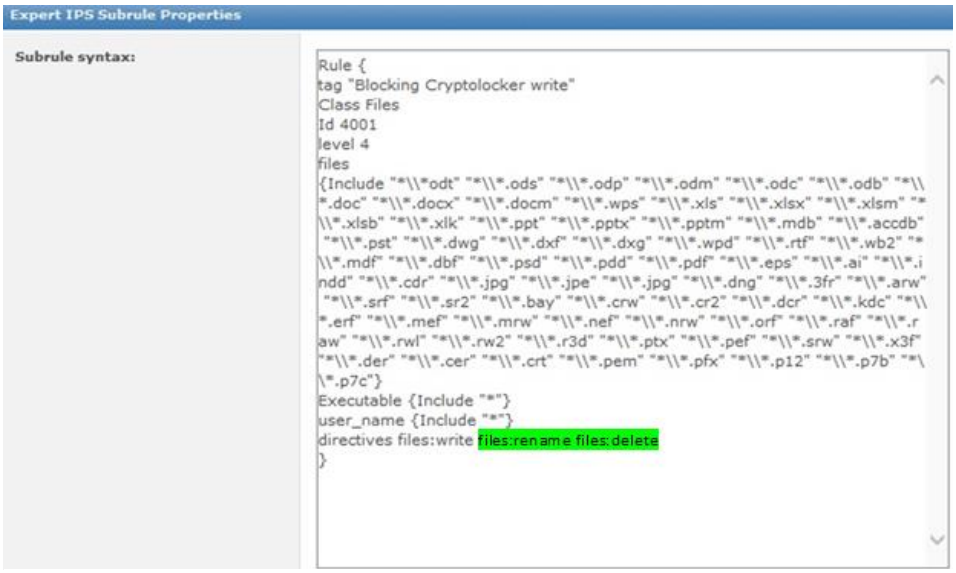
They use their own process to perform the encryption.
In order to provide protection for these variants you need to setup a rule to prevent non-trusted processes to write, rename & delete the list of protected extensions. Please use the rule available at:
**https://community.mcafee.com/docs/DOC-6553**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

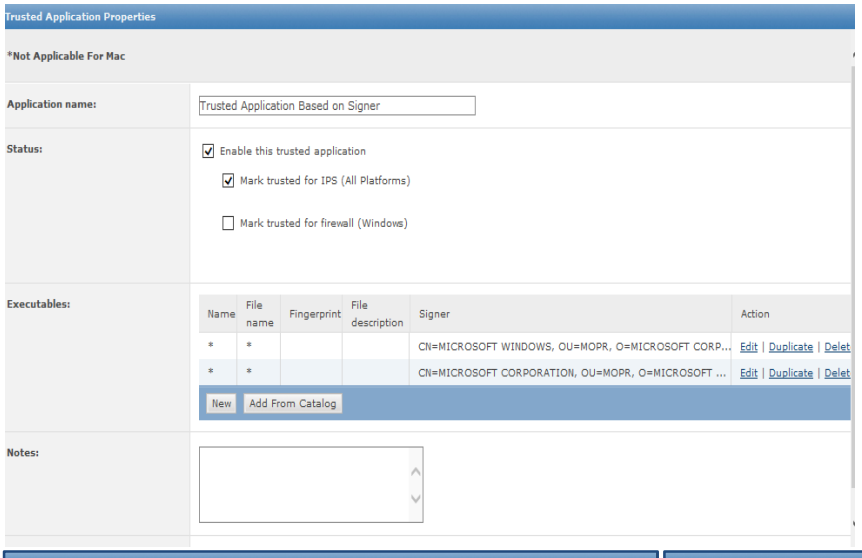
The rule should look like this in the user interface:

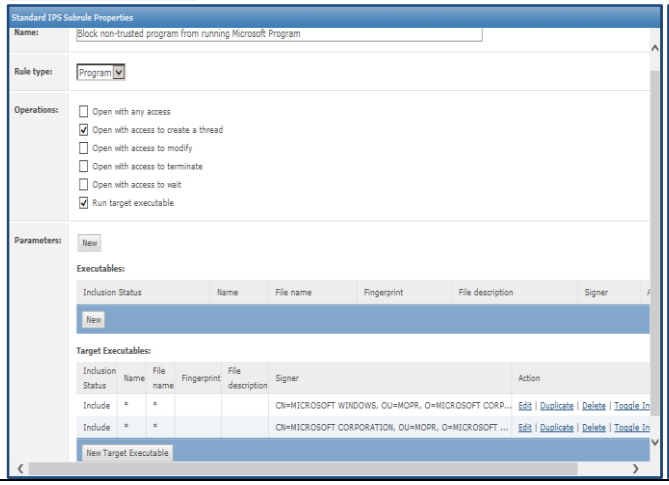


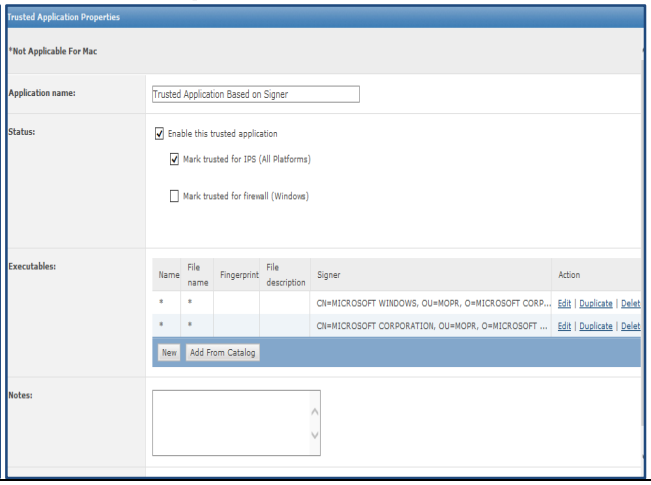

***NOTE:** File directives rename/delete have been added to include Cryptolocker v.IV & CryptoWall since the video in the community was created. This is reflected in the updated HIP rule TXT file.

**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 HIPs:

- 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 defence:

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

HIPS 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 users’ desktops. Implementing these policies can help reduce new variant using this propagation vector.