ESET Tech Center

Best practices to protect against Filecoder (ransomware) malware

Anish | ESET Nederland - 2020-08-13 - Reacties (0) - Endpoint Solutions

Issue

- This article includes best practices to help you configure your system to protect against ransomware

Details

Ransomware is malware that can lock a device or encrypt its contents in order to extort money from the owner in return for restoring access to those resources. This kind of malware can also have a built-in timer with a payment deadline that must be met, otherwise the price for unlocking the data and hardware will grow – or the information and the device will ultimately be rendered permanently inaccessible.

Filecoders/Ransomware are infections that encrypt personal and data files. Typically a workstation is infected and then the Filecoder/Ransomware will attempt to encrypt any mapped shared drives. This can make this infection seem as though it is spreading through your network when it is not.

While your files may be encrypted, your system may not be infected. This is possible when a shared drive on a file server is encrypted but the server itself does not contain the malware infection (unless it is a Terminal server).

Other filecoder threats are also known as the following:

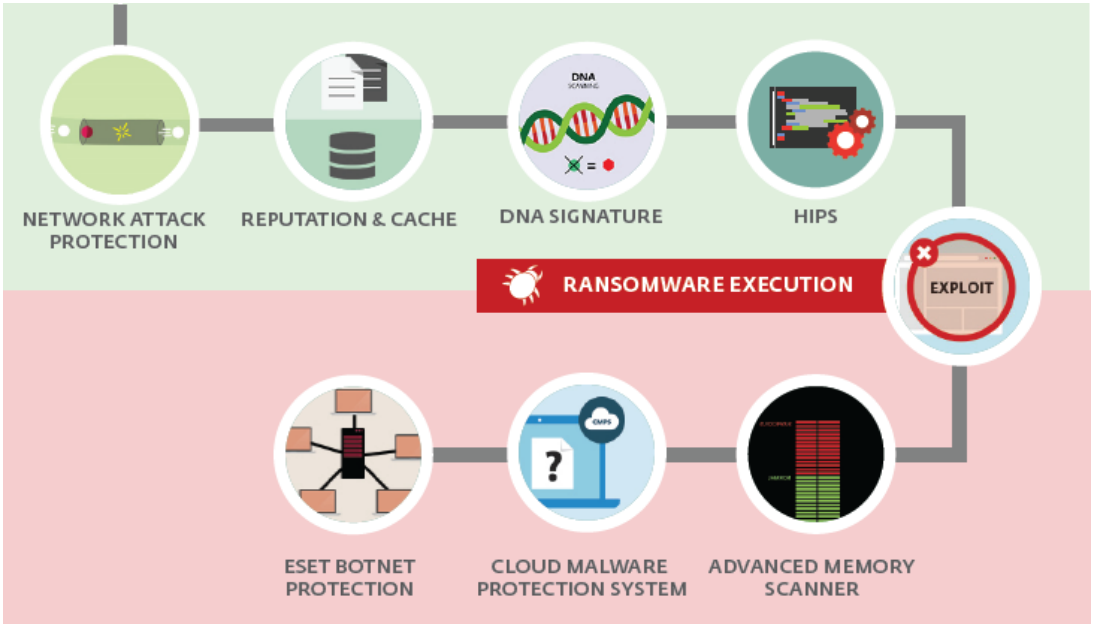
- Win32/Filecoder
- Filecoder.WannaCryptor
- Win32/Filecoder.TeslaCrypt.A (TeslaCrypt) or Win32/Filecoder.Locky.A infection after opening an email from an unfamiliar source or ZIP files from such an email
- "CryptoLocker", "Cryptowall", "Dirty decrypt", and "CTB locker"
- Win32/TrojanDownload.Elenoocka.A
- Win32/Gpcode

Solution

The current versions of ESET products use multiple layers of technologies to protect computers from ransomware.

Examples of these technologies include **Advanced Memory Scanner**, **ESET LiveGrid® Reputation System** and **Exploit Blocker**.

Additionally, the latest ESET products provide an enhanced **Botnet Protection** module that blocks communication between ransomware and Command and Control (C&C) servers.



General ESET product anti-ransomware best practices | General anti-ransomware practices | Recovering encrypted files | ESET Support Services

General ESET product anti-ransomware best practices

- **Keep Advanced Memory Scanner and Exploit Blocker enabled**

These two features are enabled by default in ESET products version 5 and later. These newly designed ESET algorithms strengthen protection against malware that has been designed to evade detection by anti-malware products through the use of obfuscation and/or encryption.

Advanced Memory Scanner looks for suspicious behavior after malware decloaks in the memory and **Exploit Blocker** strengthens protection against targeted attacks and previously unseen vulnerabilities, also known as zero-day vulnerabilities.

We recommend that you upgrade to the latest version if you are running ESET Smart

Security or ESET NOD32 Antivirus (including Business Editions) version 4.x or earlier:

Home users: Which ESET product do I have and is it the latest version? (Home Users)

Business users: Do I have the latest version of ESET business products?

- **Keep ESET LiveGrid enabled**

The ESET Cloud Malware Protection System is based on **ESET LiveGrid**. It monitors for unknown and potentially malicious applications and subjects samples to automatic sandboxing and behavioral analysis.

Make sure that ESET LiveGrid is enabled and working in your ESET product.

- **Ensure that "Network drives" is selected in Real-time file system protection**

  With Network drive protection enabled, the ESET Real-time scanner will be able to trigger detection on an infected workstation, preventing the ransomware process from encrypting the drive. See Real-time file system protection for more information.

- **Keep ESET updated**

  New variants of existing ransomware are released frequently, so it is important that you are receiving regular virus database updates (your ESET product will check for updates every hour provided that you have a valid license and a working internet connection).
  Home users: How do I know ESET Smart Security/ESET NOD32 Antivirus is updating correctly?

  Business users: How do I know if my ESET business product is updating correctly?

- **For Virtual Machine users**

  For best protection against Filecoder malware, we recommend the use of ESET Endpoint Security in virtual environments.

- **Make sure you have Ransomware Shield enabled**

Ransomware Shield as a part of a Self-Defense technology is another layer of protection, that works as a part of HIPS feature. For more information, see Ransomware Shield in ESET Glossary and how to configure it in ESET products.

- **Notifications**

Detected threats

Configure automatic threat notifications in ESET Security Management Center Web Console

(7.x)

General anti-ransomware best practices—Minimize your risk from encryption-based malware (ransomware)

- **Keep backups of your system**

  Plan to take backups of your system on regular intervals, and keep at least one such backup in offline storage, to protect your most recent work from an attack.
- **User permissions and restriction of rights**

  There are many types of restrictions, such as the restriction from accessing application data, and even some that are prebuilt as a Group Policy Object (GPO).
  1. Disable files running from the AppData and LocalAppData folders.

  2. Block execution from the Temp subdirectory (part of the AppData tree by default).

  3. Block executable files running from the working directories of various decompression utilities (for example, WinZip or 7-Zip).

     Additionally, in ESET Endpoint Security/Antivirus, ESET Mail Security and ESET File Security, you can create HIPS rules to allow only certain applications to run on the computer and block all others by default: [KB7257] Create a HIPS rule and enforce it on a client workstation using ESET Security Management Center (7.x)

- **Do not disable User Account Control (UAC)**

Do not open attachments claiming to be a fax, invoice or receipt if they have a suspicious name or you did not expect to receive them.

What can I do to minimize the risk of a malware attack?

- **ESMC/ERA/ECA to apply configuration settings via a policy to protect against ransomware**

1.
   1. Configure HIPS rules for ESET business products

   2. Configure Firewall rules for ESET Endpoint Security

   3. Configure ESET Mail Security

- **Use two-factor authentication (2FA)**

  We recommend ESET Secure Authentication.

- **Threat Defense**

We recommend ESET Dynamic Threat Defense

- **Disable Macros in Microsoft Office via Group Policy**

  Office 2013/2016 (the following link is for 2013 but are the same settings for 2016): Plan security settings for VBA macros for Office
- **Keep your system up-to-date**

To ensure you have the best protection available, keep your operating system and applications updated. Install the latest high priority updates offered in Windows Update tool, and check regularly or enable the Automatic Updates feature. New security updates patch the system vulnerabilities and reduces the risk of malware attack.

Microsoft has released patches for current Windows operating systems as well as Windows XP to mitigate a critical vulnerability. See Microsoft Security Bulletin MS17-010 - Critical for instructions to apply these updates.

- If you are using Windows XP, disable SMBv1.

- **Potential ports/service that could be exploited if left open**

To prevent an unknown IP address from performing successful Brute Force attacks, we strongly recommend locking down SMB, SQL and RDP.

1.
    1. SMB

-
    -
        - Close file sharing ports 135-139 and 445. SMB ports should not be exposed to the internet.
-
    1. SQL
-
    -
        - Whitelist trusted IP addresses that are allowed to connect to SQL
-
    1. RDP
-

- Stop outside RDP Brute Force attacks by closing RDP to external connections. Use a VPN with Two Factor Authentication to connect to the internal network.
- Set automatic account lockouts after a certain number of failed attempts. Include a waiting period for automatic unlock, after an account is locked out.
- Enforce strong passwords
- Disable common unused and default accounts, for example, administrator, admin or root
- Whitelist specific users and groups to allow login using RDP
- Whitelist specific IP addresses to allow an RDP connection

- **Remote Desktop Protocol best practices against attacks**

Encryption-based malware often accesses target machines using the Remote Desktop Protocol (RDP) tool integrated in Windows. RDP allows others to connect to your system remotely, so the attacker can misuse RDP to remove the protection and then deploy the malware.

a) Disable or change Remote Desktop Protocol

If you do not require the use of RDP, you can change the default port (3389) or disable RDP to protect your machine from Filecoder and other RDP exploits. For instructions on how to disable RDP, visit the appropriate Microsoft Knowledge Base article below:

o Windows XP

o Windows 7

o Windows 8

o Windows 10

For more information about RDP, see the following We Live Security article: Remote Desktop (RDP) Hacking 101: I can see your desktop from here!

b) Password-protect your ESET product settings

If you need to keep RDP running and cannot disable or change the RDP settings, you can use a password to protect the ESET product from being altered by an attacker. This prevents from unauthenticated settings modification, disabling the protection or even uninstalling the ESET product. We recommend using a different password from the one used for the RDP login credentials.

Can encrypted files be recovered?

Modern Filecoders/Ransomware encrypt data using asymmetric methods and multiple types of encryption cyphers. In short, files are encrypted with a public key and are not able to be

decrypted without the associated private key. With current ransomware, the private key is never located on the affected workstation or environment. This means that data will need to be restored from a good backup made prior to the infection.

If no backups are available, you can attempt to recover files from Shadow Copies. You can use Shadow Explorer, which you can download from the following web page: http://www.shadowexplorer.com/downloads.html

However, it is not uncommon for ransomware infections to delete Shadow Copies to prevent recovery of files.

What steps should you take if infected with ransomware?

1. Disconnect the computer from the network.

2. Locate the TXT or HTML file with the payment instructions, for example "How to decrypt" shared folders / drives encrypted. This may be used by our malware researchers for further analysis.

3. Run ESET SysRescue on the infected computer. Only restore from a backup once the threat has been identified and removed (see the above section Keep backups of your system).

4. Contact ESET by following the instructions in the **ESET Support Services** section below.

ESET Support Services

- **ESET North American customers**—You can start a live chat session with a technical support agent at the following web page: ESET Live Chat.

- **ESET Customers worldwide**—Contact your local ESET partner for support.

Need Assistance in North America?

If you are a North American ESET customer and need assistance, visit helpus.eset.com to chat with a live technician, view product documentation or schedule a consultation with an ESET Home Advisor.
