ESET®

ENJOY SAFER TECHNOLOGY®

CRYPTOLOCKERS AND OTHER FILECODERS

Cryptolockers and other Filecoders (file-encrypting ransomware)

Ransomware is any malware (malicious software) used by cyber criminals to hold digital files on smartphones, computers and other connected devices for ransom, demanding payment in order to regain access. Ransomware has become a popular way for malware authors to extort money from companies and consumers alike. They plant the malware using tactics such as phishing or exploiting software flaws.

ESET® classifies most forms of malware that use ransomware tactics under the name “Filecoder,” but it is by combining the functions of a cryptolocker and a Filecoder that malware authors create a piece of ransomware. It encrypts certain files, then prompts the victim to pay a ransom for the decryption key. Sometimes, ransomware has a built-in timer with a payment deadline that must be met. Once the payment is sent and verified, the program decrypts the files. If the payment is not made, the victim may lose their files and their hardware.

Ransomware is a type of malicious software that can lock your device and take hostage files that might have some personal or professional value to you.

Malware is often spread via email or by drive-by downloads from compromised websites. After it’s done its malicious job, the ransomware generates a pop-up message telling you to pay.

1. How cryptolockers spread

Cryptolockers have been actively spreading in large attack waves in various regions of the world. The typical infection vector used in these campaigns is an email with a malicious attachment—a tactic known as phishing. The message may be localized to the victim. For example, if a victim is believed to be in the U.S., fake package tracking information will be sent in an email spoofed to appear as if it comes from FedEx or UPS. The location of the potential victim can be determined by the top level domain used in the email address of the target, or the ISP that hosts the domain. If the recipient falls victim to this social engineering scheme and opens the attachment, a trojan executes on the computer, unless blocked by antivirus. In recent cases, the trojan was a downloader that retrieved and then executed the cryptolocker. The cryptolocker then hunts for a wide range of file types to encrypt—and once its dirty work has been done, it displays a message demanding the user electronically transfer the cash to have the files decrypted.

2. ESET detection

Before spreading their malware, the writers typically test to verify that their samples are undetected by the static methods employed by most antivirus software. Therefore, end-user protection must take a multi-layered approach, with technologies focused on proactive behavioral detection and cloud-based solutions.

ESET antimalware solutions provide several protective layers, including proactive heuristics and reactive detections. In all cases, the antivirus must be up-to-date with the latest detection signatures and LiveGrid®, ESET's file reputation service in the cloud, must be enabled for best reaction times and maximum protection. We also strongly recommend using the latest versions of the software to take advantage of the protection provided by Exploit Blocker, Advanced Memory Scanner and other technologies capable of detecting threats at different execution stages.

Of course, antimalware software does not completely cover all possibilities, nor does it replace the other crucial layers of protection. These include keeping other applications up to date, maintaining backups, implementing best-security practices and continuing user education about vigiliance against social engineering attacks.

To ensure your ESET Security products are configured correctly, please do the following.

A. Update your ESET security product

New versions of this malware are released frequently, so it is important that computers receive regular virus database updates, among other precautions, to ensure that they are not vulnerable to this infection. ESET products check for updates every hour provided there is a valid license and a working Internet connection.

B. Enable Advanced Memory Scanner and Exploit Blocker

These newly designed ESET algorithms strengthen protection against malware that uses obfuscation and/or encryption to evade detection by antimalware products. Advanced Memory Scanner looks for suspicious behavior once malware decloaks in memory, while Exploit Blocker monitors processes looking for behavior typical of exploits.

C. Enable LiveGrid

In some cases, ESET products with ESET LiveGrid enabled may respond faster to new threats than signature-based detection, even with regular database updates.

3. Prevention and protection

The encrypted files can essentially be considered damaged beyond repair. We recommend using the following steps to minimize the impact of cryptolockers on the system and stored data. If the system has been properly prepared and secured, risk of data loss is significantly lower than in the case of an unprotected system.

A. Back up your data

The single, best measure that will defeat ransomware is having a regularly updated backup. Remember that a cryptolocker will also encrypt files on drives that are mapped and have been assigned a drive letter, and sometimes on drives that are unmapped as well. This includes any external drives such as a USB thumb drive, as well as any network or cloud file stores. A regular backup regimen is essential when there is an external drive or backup service that is regularly disconnected unless it is actively doing a backup.

B. Show hidden file-extensions

A cryptolocker frequently arrives in a file that is named with the extension ".PDF.EXE". This counts on Window's default behavior of hiding known file extensions. Re-enabling the ability to see the full file extension can make it easier to spot suspicious files.

HOW TO PROTECT YOURSELF

BEFORE YOU GET INFECTED

1. ***Back up*** your data
2. ***Show*** file-extensions hidden by default in Windows
3. ***Filter*** executable (*.exe) files in your e-mail
4. Use a reputable ***security software suite***
5. ***Patch*** or ***update*** your software
6. ***Disable*** remote desktop protocol

IF YOU ARE SUSPICIOUS...

1. ***Disconnect*** from the Internet if you think you've been infected
2. Use ***System Restore***
3. Set the ***BIOS*** clock back
4. And—in particular—***don't pay***

C. Filter EXEs in email

If your gateway mail scanner has the ability to filter files by extension, you may wish to deny emails sent with ".EXE" file attachments, or those with attachments that have two file extensions ending with an executable ("*.*.EXE" files, in filter-speak). If your users legitimately need to exchange executable files within your environment and you are denying emails with ".EXE" extensions, they can exchange those .EXE files within .ZIP files (password-protected, of course) or via cloud services.

D. Don't open attachments or click on links in unsolicited emails or messages

A typical method of infection is a user opening an unsolicited email attachment or clicking on a link in an email claiming to come from a bank or a delivery company. Users should be trained not to open any unknown or suspicious email attachments, links or files.

E. Disable files running from AppData/LocalAppData folders

A particular, notable behavior of a cryptolocker is that it runs its executable from the AppData or Local AppData folder. You can create rules within Windows or with Intrusion Prevention Software to disallow this behavior. If for some reason legitimate software is set to run from the AppData rather than the usual Program Files area, you will need to exclude it from this rule.

F. Disable RDP

Cryptolocker/Filecoder malware often accesses target machines using Remote Desktop Protocol (RDP), a Windows utility that allows others to access desktops remotely. Cyber-criminals have also been known to log in via an RDP session and disable the security software. ESET security software has built-in self-protection tools to protect the security software, but it is a best practice to disable RDP unless you need it in your environment. For instructions to do so, visit the appropriate Microsoft Knowledge Base articles below:

Windows XP RDP disable

Windows 7 RDP disable

Windows 8 RDP disable

G. Patch or update your software

Malware authors frequently rely on people running outdated software with known vulnerabilities, which they can exploit to silently get onto systems. You can significantly decrease the potential for ransomware pain if you make a practice of updating software often. Some vendors release security updates on a regular basis (Microsoft and Adobe both use the second Tuesday of the month), but there are often "out-of-band" or unscheduled updates in case of emergency. Enable automatic updates if you can, or go directly to software vendor websites.

H. Use a reputable security suite

Malware authors frequently send out new variants to avoid detection, so this is why it is important to have multiple layers of protection. Even after it burrows into the system, most malware then relies on remote instructions to carry out its misdeeds. If you run across a ransomware variant that is so new that it gets past antimalware software, it may still be caught when it attempts to connect with its Command and Control (C&C) server to receive instructions for encrypting files. ESET's latest software suite provides a Botnet Protection module that blocks malicious traffic trying to signal a C&C server.

I. Use System Restore to get back to a known-clean state

If System Restore is enabled on the infected Windows machine, it might be possible to take the system back to a known-clean state and restore some of the encrypted files from "Shadow" files. But you have to outsmart the malware and move quickly. That is because newer cryptolockers have the ability to delete the "Shadow" files from

System Restore. Such cryptolockers will start to delete the "Shadow" files whenever the executable file is run, and you might not even know that is happening since executable files can run without the operator knowing, as a normal part of Windows system operation.

J. Use a standard account instead of one with the administrator privileges

Using an account with system administrator privileges is always a security risk, because then malware is allowed to run with elevated rights and may infect the system easily. Be sure that users always use a limited user account for regular daily tasks and use the system administrator account only when it is absolutely necessary. Do not disable User Access Control.

K. Pay attention to the security education of employees

One of the most common infection vectors is social engineering—methods based on fooling users and trying to convince them to run the executable file.

For over 25 years, ESET® has been developing industry-leading security software for businesses and consumers worldwide. With security solutions ranging from endpoint and mobile defense to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give users and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running uninterrupted. For more information, visit www.eset.com.

ENJOY SAFER TECHNOLOGY®