Ransomware identification for the judicious analyst TechBlog

By Karsten Hahn

Published: 2021-02-25 · Archived: 2026-04-05 15:34:23 UTC

When facing a ransomware infection, it helps to be familiar with some tools as well as key points to identify ransomware correctly.

Most ransomware is fire-and-forget malware. The majority of ransomware families do not remain on the system after they have done their deed, and delete the malicious binaries. The system's owner is left with encrypted data and the ransom message. Web services for ransomware identification like id-ransomware might not be an option if customer data is of a confidential nature. Even though the files are encrypted, they can contain information about the customer's system or might be recoverable by third parties.

Identification vs detection

Malware detection is a simple yes- or no-answer to the question: Is this file malicious?
Or in case of ransomware detection: Is this file ransomware? Identification on the other hand will provide an aswer to the question: Which malware or ransomware family is this?

For antivirus software it is usually enough to detect malware in order to prevent infections. But as soon as there was an infection, identification helps to determine the next steps for cleaning the system, reversing the damage (if possible) and preventing infections that use the same infection vector.

Once the ransomware family is identified, you are able to answer the following questions:

- Does the ransomware encrypt data (files or HDD)?
- Is the encrypted data decryptable for free (by third-party decrypters)?
- Are the threat actors able to decrypt the files after payment?
- If the data cannot be decrypted, can it be recovered by other means like file recovery software?
- How did the ransomware get onto the system and how can we prevent this from happening again?
- Does the ransomware typically arrive in combination with other malware that may have done additional damage (like stealing credentials)?

Types of ransomware

The first interesting question to answer is what type of ransomware attacked the system. Most commonly people associate file encrypters with the term ransomware but there are more ways for malware to hold something for ransom. Ransomware is every malware that prevents access to the whole system, part of the system or data, or pretends to do so, and asks for some kind of payment from the system's user to revert the changes.

1. File encrypter

The file encrypter typically searches for files on the system based on their file extensions, encrypts each file one by one and renames it, e.g., by adding an extension.
The file encrypter will often use persistence mechanisms for the duration of the encryption process. In case the user turns off the system midst of encrypting, the file encrypter will continue the process after restart.

Some file encrypters use password protected archives to encrypt and store files, e.g., CryptoHost.

2. Disk encrypter

This kind of ransomware will usually infect the master boot record, thus rendering the operating system unbootable. In addition they encrypt the data on disk or the master file table. There aren't many families out there that do this. Some known ones are Petya, Mamba (aka HDDCryptor) and some very old ones from the DOS era like the AIDS virus. Since there are only a few of them, identification should be comparably easy.

3. Wiper

Sometimes ransomware developers create bugs in the encrypting portion or key storing functions that make it impossible for them or anyone else to decrypt the data. They may damage data instead of encrypting it or make the retrieval of the key(s) impossible, e.g., Ordinypt.
Creating a wiper that poses as file or disc encrypter may also be done on purpose if the actual goal is to damage a business and threat actors want to hide their intent. Some believe Petna aka NonPetya to be one of those wipers.

Identifying this type of ransomware is of particular interest, since paying the ransom in these cases (should this option be considered viable) would be pointless as there are no files to decrypt or recover..

4. Fake encrypter

The fake encrypter will pretend to encrypt files without actually doing it. One common way is to just rename files, e.g. by adding ransomware-typical extensions to them, so that users are fooled into believing that their files are encrypted. As Windows decides based on file extensions which program it uses to open a file, changing the extension will make it seem like the files are "not working anymore". Restoring the file extension will also restore the functionality of the file. Others, like RansomPrank, just tell the user that the files were encrypted, without doing anything to the files.

Ransomware simulators, which are used to demonstrate an infection and to train staff, mostly fall into this category but those shouldn't actually infect systems in the wild.

5. Screenlocker

Screenlockers are often overlooked in discussions about ransomware. They seem less dangerous, less interesting, and less damaging. From a technical standpoint they are indeed less damaging because the locking mechanism can be reversed whereas decryption of data or recovery of wiped data is not always possible. For non tech-savvy users, however, screenlockers still pose a substantial threat. This is especially evident and tragic in those cases where people committed suicide due to a screenlocker infection (e.g., case1, case2).

Very common is the screenlocker combined with tech support scam, where the screenlocker may look like a fake blue screen and show a tech support number that is supposedly from Microsoft. The scammers who pose as Microsoft technicians will then proceed to show the user that their system is damaged and ask for payment in order to repair it (as demonstrated in this example).

Some ransomware families are screenlocker and file encrypter hybrids, that means they lock the screen and also encrypt files on the system. If they are pure screenlockers, it is usually all you need to know to reverse the damage.

Ransomware identification checklist

There are a few key points that you can use for ransomware identification.

Ransom messages

Typical ways to deliver a ransom message are:

- graphical user interface (e.g. Jigsaw), may lock the screen
- text or html file, sometimes opened automatically after encryption
- image file, often put as wallpaper
- contact email in encrypted file extensions
- pop-up after trying to open an encrypted file (e.g. CrypVault)
- voice message (e.g. Cerber)

Ransomware may use several of these ways to deliver the ransom message. However in some cases, systems infected with ransomware do not display a ransom note. The ransomware may have been stopped before it could place the notes. Some antivirus programs detect ransom note files as malicious and clean them from the system. Last but not least, certain buggy ransomware families encrypt their own ransom note files, thus leaving no way to contact the criminals for payment.

The following ransom note contents are interesting for identification:

- ransomware name
- language, structure, typical phrases, artwork
- contact email
- format of the user id (if it exists)
- ransom demand, e.g., digital currency, gift cards
- payment address in case of digital currency
- support chat or support page

If the ransom message contains the name of the ransomware or has a well recognizable look (e.g. due to artwork), it might seem like an easy case for identification. However, if a certain strain of ransomware is successful and well known, other threat actors also want a piece of that pie and copycat the successful families. Cryptolocker, Locky and WannaCry have an uncountable number of copycats. GlobeImposter even got its name from starting out as a copycat of Globe ransomware. TorrentLocker started as a copycat of CryptoLocker and had imitators of its own (e.g. CryptoFortress) after becoming successful. Such copycats are almost never perfect imitators: for instance, one way to distinguish Globe and GlobeImposter ransom notes is the different format of the user ID.

The typical ransom payment is done via Bitcoin. Unusual payment methods like Amazon giftcards (TrueCrypter) or unusual currency like Ethereum (HC7) may reduce the set of possible ransomware families substantially.

Certain contact emails are typical for specific ransomware strains, but some ransomware families may have numerous possible contact emails because they are created with builders.

A sophisticated support page or even chat system is only available for a handful of ransomware families. PadCrypt was the first ransomware to offer chat support. Spora is also known for its elaborate support system which includes a chat (an interesting report of Spora's chat messages was published here).

Affected files

A few years ago, around 2014-2015 it was possible to identify file encrypting ransomware strains solely on the file extension that they used to mark encrypted files. There were almost no overlaps with other families, only occasional copycats like PClock.

In November 2015 CryptoWall 4.0 was released and scrambled file names of encrypted files instead of just adding an extension. Other ransomware families started doing the same, e.g., Locky and CryptXXX. That and the increasing number of ransomware families which use the same extensions (e.g. ".lock" and ".locky" are very common), and the custom extensions created by Ransomware-as-a-Service (RaaS) and ransomware based on open source projects (e.g. HiddenTear), makes identification solely based on file extensions a wild guess. Other factors should be taken into account.

Ransomware decrypters have to determine which files have been encrypted before they can apply decryption. If they cannot or don't want to rely on the extension, they use file markers instead. E.g., Hermes ransomware encrypted files have the string "HERMES" in them. Others append or prepend whole data structures to encrypted files, and may save a file specific encrypted key in there. The ransomware marker may serve to denote the beginning of the file structure. Some ransomware families create a separate text file with a list of all encrypted files on the system. An example is the LST file of older Spora variants.

```
000026C8  43 85 D2 17 E9 9C 49 B4 53 E9 CD 3E 5E 90 4F B9 FF  C…Ò.éœI´SéÍ>^.O¹ÿ
000026D9  56 1E 26 C6 F0 23 D5 48 45 52 4D 45 53 01 02 00 00  V.&Æð#ÕHERMES....
000026EA  10 66 00 00 00 A4 00 00 F1 9D C0 9A 33 CA 3C 3D 71  .f...¤..ñ.À3Ê<=q
000026FB  0B 2E 41 1D 39 B3 72 F3 0A F2 12 17 70 76 54 D4 AE  ..A.9³ró.ò..pvTÔ®
0000270C  93 51 D7 01 E5 E4 81 26 60 CA DC 7C 67 DC 2A D2 07  "Q×.åä.&`ÊÜ|gÜ*Ò.
0000271D  A9 46 F5 F8 0F BB F2 DC 05 46 2C A1 16 E3 35 C4 44  ©Fõø.»òÜ.F,¡.ã5ÄD
0000272E  E0 EF E4 82 53 4A B6 35 CD 5E DC 52 32 F6 09 E6 78  àïä‚SJ¶5Í^ÜR2ö.æx
0000273F  C0 50 AC E8 DB CD C5 F7 C5 DC C8 FA 26 7E 17 74 39  ÀP¬èÛÍÅ÷ÅÜÈú&~.t9
00002750  EA 85 9A 80 20 5E 1B 1C B2 BB 93 19 86 B6 C1 F2 C1  ê…š€ ^..²»".†¶ÁòÁ
00002761  4F 85 25 9A 03 78 43 19 EE 99 67 31 C7 5B 50 1C A7  O…%š.xC.î™g1Ç[P.§
00002772  F4 2C C3 AC 44 11 8D 9E 85 0A F3 44 81 F6 8E 8A A0  ô,Ã¬D..ž….óD.öŽŠ
00002783  D4 CD 03 63 F7 BF 25 B0 AD 38 B0 DC 99 26 BB 92 37  ÔÍ.c÷¿%°.8°Ü™&»'7
00002794  FE 8A 84 4D 57 98 8E D5 E3 BA 34 4F 63 F4 0E CD BA  þŠ„MW˜ŽÕã°4Ocô.Í°
000027A5  2B A0 D5 2A 4D 78 59 84 8B 8B 16 9D 61 81 FF D3 FC  + Õ*MxY„‹‹..a.ÿÓü
000027B6  DD BA 1A 05 ED F6 E7 F6 68 70 E5 67 81 AB 9C B3 7C  Ý°..íöçöhpåg.«œ³|
000027C7  34 E7 B5 D5 55 13 E3 01 5A 4C E6 CD 6D 31 26 ED 3D  4çµÕU.ã.ZLæÍm1&í=
000027D8  9D FB EB 23 4A 59 43 97 CB 2D 9F B7 53 EA 15 C4 9B  .ûë#JYC—Ë-Ÿ·Sê.Ä›
000027E9  6A 4F C8 ED 9E 23 B9 09 CE                          jOÈíž#¹.Î
```

Most file encrypters target files based on their file extension and location. Usually they keep a whitelist for locations they won't encrypt and a blacklist of targeted file extensions. Typically they will include document, picture, video, database, archive, backup and text file extensions. It is notable if ransomware also encrypts executable and library files, even more so if encrypted files are turned into executables as it is the case with VirLock and ACCFISA. VirLock is not only a file encrypter, but also a screenlocker and a polymorphic virus. ACCFISA puts files into self-extracting SFX RAR archives which are password protected.

In some cases ransomware applies their own icon for encrypted files. CrypVault did this using the image of a lock for their icon.

To summarize the key points for ransomware identification based on affected files:

- file renaming scheme of encrypted files: including extension and base name
- file corruption vs encryption
- which files are targeted for encryption?
- do encrypted files have their own icon?
- file markers
- existence of file listings, key files or other data files used by ransomware

Time of Infection

The time of infection should be compared to the time frame when certain ransomware was actually active in the wild. E.g. CryptoLocker is dead since OperationTovar in May 2014. Any self-proclaimed CryptoLocker infection after that date is a copycat.

Entropy and byteplot visualization

File visualization is especially useful when it comes to potentially encrypted contents. Secure encryption algorithms strive to make encrypted data look like randomly generated data in order to not expose any patterns of the key or the plain text. One way to express this randomness is entropy. The meaning of entropy, in particular Shannon's entropy, is described by Billouin as "a measure of the lack of detailed information [. . .]. The greater is the information, the smaller will be the entropy" [Bri04, p. 193] Compressed data, encrypted data and randomly generated data have high entropy, whereas data with patterns and repetition have a low entropy.

Using entropy visualization, we are able to distinguish encrypted from non-encrypted areas as well as potentially appended or prepended data in ransomware encrypted files. PortexAnalyzer creates this visualization by assigning the brightness value of a pixel based on the local entropy of that area. A high entropy area will have a bright pixel and a low entropy area a dark pixel.

The byteplot assigns the actual byte value to the brigthness value of a pixel. Using HSL (hue, saturation, lightness) as color model, the byte value is assigned to the L (lightness) portion of the pixel. Additionally, certain ranges of byte values are colored in certain way using the H (hue) portion of the pixel. PortexAnalyzer colors characters in visible ASCII range in blue, invisible characters in ASCII range are colored green, and byte values outside of ASCII range are yellow. Areas full of zero bytes are simply black in the byteplot. In combination with the entropy image, we can, e.g., distinguish if a zero entropy area is full of zero bytes or another repeated byte value. The latter may happen to zero byte areas if a monoalphabetic substitution cipher was applied.

PortexAnalyzer is able to create a PNG image of the byteplot and the local entropy in a file using the -p or --picture switch.

Although PortexAnalyzer is a PE analysis tool, it will happily create the visualizations for non-PE files that can be applied to them.

In regards to supposedly ransomware encrypted files, the entropy and byteplot visualization may tell us:

- if the file was fully encrypted
- if the file has a header or appended information
- if there are readable strings in the file
- if the file was wiped
- if the encryption is weak (e.g. XOR with a short key, ECB mode)

To do so successfully, I recommend that the files used for analysis had (previous to encryption) a file format that doesn't use too much compression. Otherwise you won't be able to distinguish between high entropy areas due to encryption or due to the compressed areas in the file. JPEG and ZIP files are unfit for that reason whereas most office document formats have low entropy areas, string areas and overall a recognizable structure to them, making them supreme candidates for analysis via visualization.

Additionally it is recommended to have at least one small and one large file for analysis. Appended or prepended structures by the ransomware may be too small in large files to be visible in the image. On the other hand, some ransomware families don't encrypt the whole file if it is too large so they can be faster in encrypting all targeted files.

Infection vector

Given the nature of how a lot of ransomware infections unfold, it might be difficult to identify the initial infection vector. If this information is available, though, it can be valuable for identification. Below are typical infection vectors and examples for well-known ransomware families that use them. Depending on the infection vector, it might be possible to obtain the actual ransomware sample which makes identification easier.

- email attachment: GlobeImposter 2 using Blank Slate malspam campaign, GandCrab
- insecure remote desktop protocol (RDP): GlobeImposter, Dharma, GandCrab
- software downloads and cracks: GandCrab, STOPRansomware, GarrantyDecrypt
- network propagation (worm): WannaCry, Petna via EternalBlue
- self-propagation (virus): Virlock
- infection via removable drives (worm): Spora uses LNK files to spread from and to removable drives
- comorbid infection: Trickbot delivering Ryuk, njRAT backdoor delivering Lime ransomware

Email attachments, RDP and software downloads are quite common ways to deliver ransomware. But there has been an uptick in using exploits since WannaCry. Ransomware that infects files on the other hand is rare.

Worm functionality to spread via removable drives like USB thumb drives is mostly an additional way to infect other systems but not the main one.

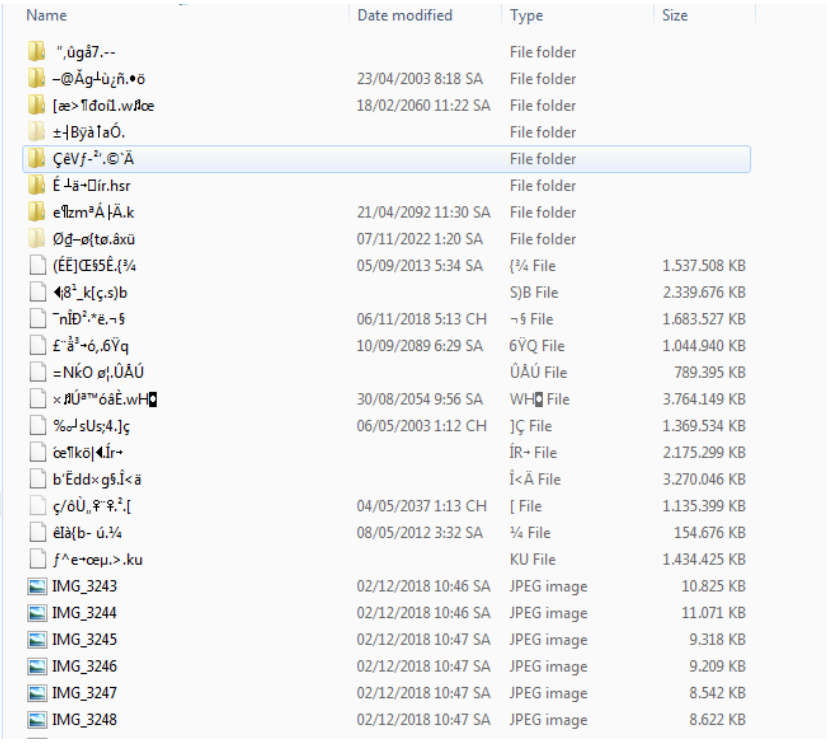
Comorbid infections are different malware families that appear together, e.g., because one malware family will download the other after infection as it is done by Trickbot. The actual infection vector is thus the one for the malware that infected the system first. Ransomware is often the last malware in the food chain because it shows itself to the user and makes it likely that the system will be cleaned afterwards.

Odd cases

Some cases might seem very odd at first but after you heard about them once, you should be able to recognize them.

File corruption

File corruption may look like the result of a file encrypter at first. There is no known ransomware so far that creates file names which look similar to corrupted files. See the picture below to get an idea how file corruption looks like. The section about entropy and byteplot visualization may also help to distinguish encrypted files from non-encrypted corrupted files.



Name	Date modified	Type	Size
",ûgå7.--		File folder	
–@ÄgꞱù¿ñ.•ö	23/04/2003 8:18 SA	File folder	
[æ>¶ðoï1.wß©e	18/02/2060 11:22 SA	File folder	
±┤Bÿà†aÓ.		File folder	
ÇëVƒ-²'.©`Ä		File folder	
É ⊥ä→□ír.hsr		File folder	
e¶lzm³Á├Ä.k	21/04/2092 11:30 SA	File folder	
Ø₫–ø{tø.åxü	07/11/2022 1:20 SA	File folder	
(ÉË]Œ§5Ê.{¾	05/09/2013 5:34 SA	{¾ File	1.537.508 KB
◀¡8¹_k[ç.s)b		S)B File	2.339.676 KB
¯nÎÐ².*ë.¬§	06/11/2018 5:13 CH	¬§ File	1.683.527 KB
£¨⅛³→ó,.6Ÿq	10/09/2089 6:29 SA	6ŸQ File	1.044.940 KB
=NǩO ø¦.ÚÅÚ		ÚÅÚ File	789.395 KB
×ßÚª™óâÊ.wH◘	30/08/2054 9:56 SA	WH◘ File	3.764.149 KB
%ↂ┘sUs;4.]ç	06/05/2003 1:12 CH	]Ç File	1.369.534 KB
©e¶k©|◀.Îr→		ÎR→ File	2.175.299 KB
b'Ëdd×g§.Î<ä		Î<Ä File	3.270.046 KB
ç/öÙ„₹¯₹.².[	04/05/2037 1:13 CH	[File	1.135.399 KB
ëÏà{b- ú.¼	08/05/2012 3:32 SA	¼ File	154.676 KB
ƒ^e→œµ.>.ku		KU File	1.434.425 KB
IMG_3243	02/12/2018 10:46 SA	JPEG image	10.825 KB
IMG_3244	02/12/2018 10:46 SA	JPEG image	11.071 KB
IMG_3245	02/12/2018 10:47 SA	JPEG image	9.318 KB
IMG_3246	02/12/2018 10:47 SA	JPEG image	9.209 KB
IMG_3247	02/12/2018 10:47 SA	JPEG image	8.542 KB
IMG_3248	02/12/2018 10:47 SA	JPEG image	8.622 KB

These files have not been encrypted by ransomware. They are corrupted. Source: https://www.reddit.com/r/antivirus/comments/a3pqmy/anyone_knows_which_type_of_these_virus_are_and/

Superinfection

When coming across a system affected by ransomware, you may even face a superinfection. In those cases, the system was initially infected by one ransomware and subsequently by other ransomwares, too. It may be superinfected by the same ransomware, and sometimes by different ransomware families. In other words: files that were already encrypted by one ransomware are encrypted again by another ransomware. File decryption for these cases is complicated and may not be possible at all, given the potential for misidentification. The signs of ransomware superinfection are:

- multiple ransomware file extensions for encrypted files
- different ransom notes with different naming schemes
- some ransom notes are encrypted, some are not

Here are some file name examples for actual superinfections that we have seen in the wild (we altered the user ids):

Ransomware	File Names
Amnesia and Dharma	HOW TO RECOVER ENCRYPTED FILES.TXT.id_2478862464_fgb15ft4pqanyji7.onion 9g0000000009U8WGvoaZXhE0l7BF59iYLh61kswFEDis7+Grf8ZuT0mIYpsyLztp8fNSDZiOBLE.22222@protonmail.ch.22222.id_
Dharma and BTCamant	AR_letter.doc.id-E5CE84C2.[mk.kitana@aol.com].wallet.BTC
CrySis and ACCDFISA v2.0	assert.dmp.id-6C618ADD.{radxlove7@india.com}.xtbl(!!-to-get-password-email-id-1819340399-to-lathelp16@gmail.com-!!).exe

In the first example, Amnesia encrypted the files first, then Dharma. Decryption of these files has to be done in reverse order of the infection. So for this example Dharma decryption must be applied before the Amnesia decryption.

Infection markers applied by anti-ransomware products

Sometimes systems may show typical markers of a ransomware infection without actually being infected. This may happen if anti-ransomware products apply vaccines for systems. Vaccines are markers that cause a malware to abort infecting the system. Usually these markers indicate for the malware that the system is already infected. So the malware terminates because it tries to avoid a superinfection. Especially if several antivirus products are used, one may identify the vaccine of the other product as an infection.

An example of such a case is in this beepingcomputer thread. The user is afraid of having a Locky infection because the registry key HKCU\Software\Locky is on their system and re-appears after deletion. It turns out that this registry entry was actually a vaccine which was applied by Bitdefender's Crypto-Ransomware Vaccine.

Useful tools and sites

At a time were the amount of ransomware families was still manageable, a group of ransomware researchers (started by Mosh) made a collective effort to note down ransomware families, their extensions, file names and other useful information. The result is this Ransomware Overview in a Google sheet. The sheer amount of new ransomware families made it impossible to keep up the work. For that reason the sheet is out of date by now but it might still be useful for older infections.

Amigo-A has a large collection of ransomware IOCs on id-ransomware.blogspot.com. The site is in Russian, very thorough and up-to-date.

A great source for ransomware information is Bleepingcomputer. They not only have a weekly report on new ransomware discoveries, but also support to identify ransomware infections and provide help with decryption or recovery if possible. If you have no database with collected ransomware information on your own, searching on Google via "inurl:Bleepingcomputer" might be very useful to you.

Michael Gillespie has published some tools to deal with ransomware infections. There is CryptoSearch which allows to find, move or copy ransomware encrypted files to a backup location and may also be used to clean the system from ransom notes and encrypted files. CryptoTester helps to analyze encrypted files.

Ransomware identification services are ID-Ransomware by MalwareHunterTeam and NoMoreRansom.org.

PortexAnalyzer was used in this article to create entropy and byteplot visualizations of files.

Book references

[Bri04] Léon Brillouin. Science and Information Theory. Courier Dover Publications, 2004.
