PROFiT

Prevention of Fraud in Travel
www.profit.uk.com
INDUSTRY BRIEFING NOTE **no. 6**

PRINT OUT THIS DOCUMENT AND KEEP IT IN A SAFE PLACE FOR USE IN AN EMERGENCY

RANSOMWARE DECRYPT COMPENDIUM

Part 2 of 2

USE THE FOLLOWING LIST IN CONJUNCTION WITH INDUSTRY BRIEFING NOTE No.6 - Part 1 of 2

DISCLAIMER

PROFiT has put together this information in good faith using information from partners and internet sources in order to help organisations suffering a ransomware attack. We have not checked any links or websites that are mentioned and cannot verify the credentials of any organisation or website mentioned nor guarantee that any of the decrypt tools will work. Accordingly you should always proceed with caution.

Any materials, opinions and advice given in this publication are for information only based on data available to the authors and are correct at the time of publication. The authors do not accept liability for any mistakes, errors, or omissions that subsequently come to light. The contents of this publication may not reflect the views of some of the organisations listed.

WHAT TO DO IF YOU BECOME THE VICTIM OF A RANSOMWARE ATTACK

1. **Contact Action Fraud**
   Use the hotline **0300 123 2040** for 24/7 assistance. ***Do not use the online reporting tool***.
2. **Isolate any infected devices from the network.**
   If it is possible to do so, switch it off and disconnect it in order to protect other devices which may still be unaffected.
3. **Identify the Ransomware which has infected your computer.**

For this, you may use a free online service called Crypto-Sheriff https://www.nomoreransom.org/crypto-sheriff.php or ID Ransomware's https://id-ransomware.malwarehunterteam.com/ or Bit Defender's service https://labs.bitdefender.com/2017/09/btcware-decryption-tool-now-available-for-free/ which identifies the ransomware and recommends the best decrypt key.

4. **Check if a ransomware decrypt tool is available.**
   If you have some IT expertise or are an IT professional look up the type of ransomware infection to identify the type of ransomware that has been used.
5. **Use any good anti-virus software or anti-ransomware removal tool you already have to remove the ransomware.**
6. **Only if your anti-virus or anti-ransomware software does not work should you consider using a ransomware file decrypt tool.** However, if you have moved your encrypted files to another isolated secure system, you can directly use these tools.

7. Most of these decryption tools are easy to use. The ones by Emsisoft, for instance, require that ransomware victims drag and drop an arbitrary encrypted file and its original version onto the decryptor's window. With some utilities, however, more advanced tech skills are necessary, such as the use of command prompt and the like. Furthermore, ransomware authors tend to tweak their code once in a while in order to defeat previously released decryptors. In any case, the list above should come in handy.

8. An additional recommendation is to look up the name of the ransomware on search engines, browse dedicated forums such as Bleeping Computer, and use the above-mentioned ID Ransomware and No More Ransom services. The best prevention tips are as follows: maintain regular data backups, do not open fishy email attachments, and use reliable security software that goes equipped with an anti-ransomware module.

   Many of the landing pages for the decrypt keys feature more detailed descriptions of the ransomware along with technical information and descriptions of how to use the key.

The Decrypt Key Compendium (as of 01/08/18)

	RANSOMWARE INFECTION	DECRYPT KEY LOCATION	FILE RENAMED	KEY SOURCE	DESCRIPTION
1	7ev3N	https://github.com/hasherezade/malware_analysis/tree/master/7ev3n	.R5A	Git Hub	**7ev3n** encrypts your data and demands 13 bitcoins to decrypt your files. this is the largest demand seen to date for this type of infection. In addition to the large ransom demand, the 7ev3n Ransomware also trashes the Windows system that it was installed on. It does this by modifying a variety of system settings and boot options so that keyboard keys and system recovery options are disabled on the computer. Selected types of files have are renamed to sequential numbered .R5A. This .1R5A, .2R5A, .3R5A etc.
2	7even-HONE$T	https://github.com/hasherezade/malware_analysis/tree/master/7ev3n	.R5A	Git Hub	**7ev3n-HONE$T** ransomware encrypts your data and then ransoms your files for approximately $400 USD in bitcoins. It is currently unknown how it is being distributed or what encryption type it uses. When 7ev3n-HONE$T encrypts your data it renames selected files to sequential numbers using the **.R5A** extension. For example, a folder's files would be renamed to 1.R5A, 2.R5A, 3.R5A, etc. 7ev3n-HONE$T will then add the name of the encrypted file to the **C:\Users\Public\files** file. When it has finished encrypting your data it will connect to the Command & Control server and upload a variety of information and statistics.
3	.777	https://decrypter.emsisoft.com/777	.777	Emsisoft Decrypter	Use this decrypter if your files have been encrypted and renamed to *.777. It may be necessary to select the correct version of the malware in the options tab for the decrypter to work properly.
		https://www.thewindowsclub.com/trend-micro-ransomware-file-decryptor or https://success.trendmicro.com/solution/1114221		Trend Micro	**Trend Micro Ransomware File Decryptor** is a free Ransomware Decryptor Tool that will help you unlock files that have been locked by select ransomware. The second link is via the 'No More Ranomware' website
4	.8Lock8	https://www.bleepingcomputer.com/forums/t/614025/8lock8-help-support-topic-8lock8-read-ittxt/	.8Lock8	Bleeping Computer	A ransomware threat that uses the AES-256 encryption to encrypt its victims' files and then demand the payment of a ransom in bitcoins.
5	AES_NI	https://files.avast.com/files/decryptor/avast_decryptor_aes_ni.exe	.aes_ni .aes256 .aes_ni_0day	Avast	The ransomware adds one of the following extensions to encrypted files: **.aes_ni** **.aes256** **.aes_ni_0day** In each folder with at least one encrypted file, the file "!!! READ THIS - IMPORTANT !!!.txt" can be found. Additionally, the ransomware creates a key file with name similar to: [PC_NAME]#9C43A95AC27D3A131D3E8A95F2163088-Bravo NEW-20175267812-78.key.aes_ni_0day in C:\ProgramData folder. This link is also listed on the 'No More Ranomware' website
		http://media.kaspersky.com/utilities/VirusUtilities/EN/rakhnidecryptor.zip		Kaspersky	This link is the Rakhni Decrypt key said to be capable of unlocking AES_NI via the 'No More Ranomware' website
6	Agent.iih	http://media.kaspersky.com/utilities/VirusUtilities/EN/rakhnidecryptor.zip	.agent.iih	Kaspersky	This link is the Rakhni Decrypt key said to be capable of unlocking Agent.iih via the 'No More Ranomware' website
7	Alcatraz Locker	https://files.avast.com/files/decryptor/avast_decryptor_alcatrazlocker.exe	.alcatraz	Avast	Alcatraz Locker uses AES 256 encryption combined with Base64 encoding. Encrypted files have the "**.Alcatraz**" extension.

8	**Al-Namrood**	https://decrypter.emsisoft.com/al-namrood	**.unavailable .disappeared**	**Emsisoft Decrypter**	The Al-Namrood ransomware is a fork of the Apocalypse ransomware. The group behind it primarily attacks servers that have remote desktop services enabled. Encrypted files are renamed to *.unavailable or *.disappeared and for each file a ransom note is created with the name *.Read_Me.Txt. The ransomware asks the victim to contact "decryptioncompany@inbox.ru" or "fabianwosar@inbox.ru". To decrypt your files the decrypter requires your ID. The ID can be set within the "Options" tab. By default the decrypter will set the ID to the ID that corresponds to the system the decrypter runs on. However, if that is not the same system the malware infection and encryption took place on, make sure to put in the ID as specified in the ransom note.
9	**Alma Locker**	http://info.phishlabs.com/hubfs/Decrypter_Blog_Images_8.24/ALDecrypter_1.cs?__hstc=61627571.34612af1cd87864cf7162095872571d1.1472135921345.1472135921345.1472140656779.2&__hssc=61627571.1.1472593507113&__hsfp=1114323283&hsCtaTracking=22f2fe97-c748-4d6a-9e1e-ba3fb1060abe%7Cd4173312-989b-4721-ad00-8308fff353b3	**6 random hexadecimal characters**	**Phishlabs**	Alma Locker is high-risk ransomware that encrypts files using AES-128 cryptography. This virus appends six random characters to the name of each encrypted file (for example, "sample.jpg" might be renamed to "sample.jpg.tqadgm"). Therefore, it is straightforward to determine which files are encrypted. Following successful encryption, Alma Locker creates two ransom-demand files - "**Unlock_files_(6 random characters).html**" and "**Unlock_files_(6 random characters).txt**" and then places them on the desktop and in each folder containing the encrypted files.
10	**Alpha**	https://www.bleepingcomputer.com/download/alphadecrypter/	**.bin**	**Bleeping Computer**	Appends the **.bin** extension to mutilated entries and leaves **README HOW TO DECRYPT YOUR FILES.html/txt** ransom manuals
11	**Amnesia**	https://decrypter.emsisoft.com/amnesia	**.amnesia**	**Emsisoft Decrypter**	Amnesia is a ransomware written in the Delphi programming language that encrypts your files using the AES-256 encryption algorithm. Encrypted files get renamed to *.amnesia and a ransom note is called "HOW TO RECOVER ENCRYPTED FILES.TXT" and asks you to contact "s1an1er111@protonmail.com". It can be found on your Desktop.
12	**Amnesia2**	https://decrypter.emsisoft.com/amnesia2	**.amnesia**	**Emsisoft Decrypter**	Amnesia2 is a ransomware written in the Delphi programming language that encrypts your files using the AES-128 encryption algorithm. Encrypted files get renamed to *.amnesia and a ransom note is called "HOW TO RECOVER ENCRYPTED FILES.TXT" and asks you to contact "s1an1er111@protonmail.com". It can be found on your Desktop.
13	**Angry Duck**	https://www.barkly.com/ransomware-recovery-decryption-tools-search	**.adk**	**Barkly**	ANGRY DUCK is a ransomware-type virus that encrypts files using AES-512 cryptography. During encryption, ANGRY DUCK appends the names of encrypted files with a "**.adk**" extension. For example, "**sample.jpg**" is renamed to "**sample.jpg.adk**". Following successful encryption, ANGRY DUCK also changes the desktop wallpaper.
14	**Annabelle**	http://download.bitdefender.com/am/malware_removal/BDAnnabelleDecryptTool.exe	**.annabelle**	**BitDefender**	The Annabelle ransomware page can be identified as its reveal message is based around the horror film franchise 'Annabelle'. In addition to ransoming the files it has a number of other features including: terminating numerous security programs, disabling Windows Defender, turning off the firewall, encrypting your files, trying to spread through USB drives, making it so you can't run a variety of programs, and then to sweeten the pot, it overwrites the master boot record of the infected computer with a silly boot loader.

15	**Apocalypse**	https://decrypter.emsisoft.com/apocalypse	**.encrypted .locked .FuckYourData, .Encryptedfile .SecureCrypted**	**Emsisoft Decrypter**	Use this decrypter if your files have been encrypted and renamed to *.encrypted, *.FuckYourData, *.Encryptedfile or *.SecureCrypted with ransom notes named *.How_To_Decrypt.txt, *.Where_my_files.txt, *.How_to_Recover_Data.txt or *.Contact_Here_To_Recover_Your_Files.txt created for each encrypted file. The ransom note asks you to contact "decryptionservice@mail.ru", "ransomware.attack@list.ru", "getdataback@bk.ru" or "recoveryhelp@bk.ru".
		https://www.avg.com/en-us/ransomware-decryption-tools#apocalypse		**AVG**	Apocalypse adds **.encrypted**, **.FuckYourData**, **.locked**, **.Encryptedfile**, or **.SecureCrypted** to the end of filenames. (e.g., Thesis.doc = **Thesis.doc.locked**)
		https://files.avast.com/files/decryptor/avast_decryptor_apocalypse.exe		**Avast**	Apocalypse adds **.encrypted**, **.FuckYourData**, **.locked**, **.Encryptedfile**, or **.SecureCrypted** to the end of filenames. (e.g., Thesis.doc = **Thesis.doc.locked**)
		http://14.141.38.197:8765/QH/Ransom_Decryptor_v1.0.0.2.zip		**Quick Heal**	
16	**ApocalypseVM**	https://decrypter.emsisoft.com/apocalypsevm	**.encrypted .locked**	**Emsisoft Decrypter**	Use this decrypter if your files have been encrypted and renamed to *.encrypted or *.locked with ransom notes named *.How To Decrypt.txt, *.README.txt, *.How_to_Decrypt_Your_Files.txt or *.How_To_Get_Back.txt created for each encrypted file. The ransom note asks you to contact "fabiansomware@mail.ru", "decryptionservice@inbox.ru" or "decryptdata@inbox.ru" and contains a personal ID. To use the decrypter you will require an encrypted file of at least 4096 bytes in size as well as its unencrypted version. To start the decrypter select both the encrypted and unencrypted file and drag and drop them onto the decrypter executable.
17	**Aura**	http://media.kaspersky.com/utilities/VirusUtilities/EN/rakhnidecryptor.zip	**id-_decrypt@india .id-_decode@india .id-_help@antivirusebola.com**	**Kaspersky Labs**	Aura is a ransomware that on execution encrypts certain files present in the user system. The compromised user has to pay the attacker with ransom to get the files decrypted. The malware is usually propagated via spam emails but can also be downloaded by other pieces of malware. It usually displays a well-known icon like a Microsoft Office document to entice users to run it.
18	**AutoLocky**	https://decrypter.emsisoft.com/autolocky	**.locky**	**Emsisoft Decrypter**	AutoLocky is a new ransomware that tries to imitate the sophisticated Locky ransomware but is nowhere near as complex, which makes decryption feasible. Victims of AutoLocky will find their files encrypted and renamed to *.locky.
		https://www.thewindowsclub.com/trend-micro-ransomware-file-decryptor		**Trend Micro**	**Trend Micro Ransomware File Decryptor** is a free Ransomware Decryptor Tool that will help you unlock files that have been locked by select ransomware.
19	**AutoIt**	http://media.kaspersky.com/utilities/VirusUtilities/EN/rakhnidecryptor.zip or http://media.kaspersky.com/utilities/VirusUtilities/EN/rannohdecryptor.zip	**Trojan-Ransom.Win32.Polyglot Trojan-Ransom.Win32.RannohTrojan-Ransom.Win32.AutoIt Trojan-Ransom.Win32.Fury Trojan-Ransom.Win32.CrybolaTrojan-Ransom.Win32.CryakI Trojan-Ransom.Win32.CryptXXX**	**Kaspersky**	RannohDecryptor tool is designed to decrypt files encrypted by **Trojan-Ransom.Win32.Polyglot**, **Trojan-Ransom.Win32.Rannoh**, **Trojan-Ransom.Win32.AutoIt**, **Trojan-Ransom.Win32.Fury**, **Trojan-Ransom.Win32.Crybola**, **Trojan-Ransom.Win32.CryakI** or **Trojan-Ransom.Win32.CryptXXX** versions **1** and **2** and **3**.
20	**Aw3s0m3Sc0t7**	https://www.barkly.com/ransomware-recovery-decryption-tools-search	**.enc**	**Barkly**	Having scrambled one's files, the infection concatenates the .enc extension to each one.

21	**Badblock**	https://decrypter.emsisoft.com/badblock	**This encryption software does not rename files**	**Emsisoft Decrypter**	Use this decrypter if your files have been encrypted but not renamed. The malware identifies itself as BadBlock both in the red ransomware screen as well as in the ransomnote "Help Decrypt.html" that can be found on the Desktop.
		https://www.avg.com/en-us/ransomware-decryption-tools#badblock		**AVG**	BadBlock does not rename your files. After encrypting your files, BadBlock displays one of a range of specific message screens (from a file named **Help Decrypt.html**):
		https://www.thewindowsclub.com/trend-micro-ransomware-file-decryptor		**Trend Micro**	**Trend Micro Ransomware File Decryptor** is a free Ransomware Decryptor Tool that will help you unlock files that have been locked by select ransomware.
		https://files.avast.com/files/decryptor/avast_decryptor_badblock.exe (32 bit Windows) or https://files.avast.com/files/decryptor/avast_decryptor_badblock64.exe (64 bit Windows)		**Avast**	After encrypting your files, BadBlock displays one of these messages (from a file named **Help Decrypt.html)**
22	**Bart**	https://www.avg.com/en-us/ransomware-decryption-tools#bart	**.bart.zip**	**AVG**	Bart adds **.bart.zip** to the end of filenames. (e.g., Thesis.doc = **Thesis.docx.bart.zip**) These are encrypted ZIP archives containing the original files. **Ransom message:** After encrypting your files, Bart changes your desktop wallpaper to an image informing you that all files are locked and can only be unlocked with a private key held on a secret server. The text on the image can also be used to help identify Bart, and is stored on the desktop in files named **recover.bmp** and **recover.txt**.
		http://download.bitdefender.com/am/malware_removal/BDBartDecryptor.exe		**BitDefender**	**Bart ransomware** is distributed by the Russian Cyber Mafia behind Locky via phishing emails with fake photo attachments.
		https://files.avast.com/files/decryptor/avast_decryptor_bart.exe		**Avast**	Bart adds **.bart.zip** to the end of filenames. (These are encrypted ZIP archives containing the original files.
23	**BarRax**	http://blog.checkpoint.com/wp-content/uploads/2017/03/BarRaxDecryptor.zip	**.barrax**	**Check Point**	**Barrax** ransomware is also a cryptovirus. The extension **.BarRax** will get appended to all files that become locked after the encryption process completes. Reported to be a variant of **HiddenTear**, the encryption algorithm is highly likely to be **AES**.
24	**Bitcryptor**	https://aransomware.wpengine.com/static/CoinVaultDecryptor.zip	**.clf**	**Kaspersky**	**BitCryptor** is a ransomware virus that infiltrates operating systems via infected email messages, exploit kits, and fake downloads (for example, rogue video players and fake Flash updates). After successful infiltration, this malicious program encrypts files stored on computers within 66 hours.
25	**BitStak**	https://www.nomoreransom.org/uploads/CoinVaultDecryptor.zip	**.bitstak**	**No More Ransom**	The BitStak Ransomware will encrypt your files, scramble their filenames, and then add the .bitstak extension to encrypted files. For **example**, the file "Penguins.**jpg**" may be renamed "xfZdSbZU.aXd.bitstak". This tool will allow you to decrypt your files and **rename** them back to their original names.
26	**Black Shades Crypter**	https://www.barkly.com/ransomware-recovery-decryption-tools-search	**.silent**	**Barkly**	encrypts your data and ransoms it for the low price of $30 paid in bitcoins or Paypal. This ransom targets both English and Russian speaking victim's and appends the **.silent** extension to encrypted files. Unusually, this ransomware includes strings in the executable that contain taunting messages to security researchers who may be analyzing the ransomware.
27	**BTCWare**	https://labs.bitdefender.com/2017/09/btcware-decryption-tool-now-available-for-free/	**btcware .cryptobyte .onyon .xfile .cryptowin .theva .master .aleta .blocking**	**BitDefender**	The BTCWare ransomware family targets Windows machines and is primarily distributed by brute-forcing weak passwords of the Remote Desktop Protocol (RDP) and manually installing the malware
		https://files.avast.com/files/decryptor/avast_decryptor_btcware.exe		**Avast**	With at least five variants that can be distinguished by encrypted file extension this ransomware uses two different encryption methods – RC4 and AES 192.
		https://www.bleepingcomputer.com/download/btcwaredecrypter/		**Bleeping Computer**	

28	**CBT Locker** **AKA** **Critroni**	https://www.bleepingcomputer.com/forums/t/565020/new-cryptotorlocker2015-ransomware-discovered-and-easily-decrypted/	**.CTBL** **.CTB2** **Random extensions**	**Bleeping Computer**	When you become infected with CTB Locker (Curve-Tor-Bitcoin Locker) or Critroni, the infection will encrypt your files and then rename them to a new extension. Older versions of CTB-Locker would change the file extension to **.CTBL** or **.CTB2**, while newer ones are using a random extension such as **.ftelhdd** or **.ztswgmc**.
29	**Cerber v1**	https://www.thewindowsclub.com/trend-micro-ransomware-file-decryptor	**.cerber**	**Trend Micro**	**Trend Micro Ransomware File Decryptor** is a free Ransomware Decryptor Tool that will help you unlock files that have been locked by select ransomware.
30	**Chimera**	https://www.thewindowsclub.com/trend-micro-ransomware-file-decryptor	**.crypt**	**Trend Micro**	**Trend Micro Ransomware File Decryptor** is a free Ransomware Decryptor Tool that will help you unlock files that have been locked by select ransomware.
31	**CoinVault**	https://support.kaspersky.com/13331		**Kaspersky**	The CoinVault executable file hides in a fake pdf email attachment. If an unsuspecting person clicks on the supposed pdf, the ransomware starts to infect the computer. CoinVault then begins creating copies of the victim's files, encrypting them, and deleting the originals.
32	**Cry9**	https://decrypter.emsisoft.com/cry9	**.-juccy[a]protonmail.ch** **.id-** **.id-_[nemesis_decryptor@aol.com].xj5v2** **.id-_r9oj** **.id-_x3m** **.id-_[x3m-pro@protonmail.com]_[x3m@usa.com].x3m** **.** **.-sofia_lobster[a]protonmail.ch** **._[wqfhdgpdelcgww4g.onion.to].r2vy6**	**Emsisoft Decrypter**	Cry9 is the successor of the CryptON ransomware family that is mostly used for targeted attacks via RDP. Files are encrypted using a customized version of AES, RSA and SHA-512. We have seen the following extensions being used by Cry9: ".-juccy[a]protonmail.ch", ".id-", ".id-_[nemesis_decryptor@aol.com].xj5v2", ".id-_r9oj", ".id-_x3m", ".id-_[x3m-pro@protonmail.com]_[x3m@usa.com].x3m", ".", ".-sofia_lobster[a]protonmail.ch" and "._[wqfhdgpdelcgww4g.onion.to].r2vy6".
33	**Cry128**	https://decrypter.emsisoft.com/cry128	**.fgb45ft3pqamyji7.onion.to._.id__gebdp3k7bolaind4.onion._** **.id__2irbar3mjvbap6gt.onion.to._** **.id-_[qg6m5wo7h3id55ym.onion.to].63vc4**	**Emsisoft Decrypter**	Cry128 belongs to the CryptON/Nemesis ransomware family that is mostly used for targetted attacks via RDP. Files are encrypted using a customized version of AES and RSA. We have seen the following extensions being used by Cry128: ".fgb45ft3pqamyji7.onion.to._", ".id__gebdp3k7bolalnd4.onion._", ".id__2irbar3mjvbap6gt.onion.to._" and ".id-_[qg6m5wo7h3id55ym.onion.to].63vc4".
34	**Cryakl**	https://support.kaspersky.com/8547#block1	**{CRYPTENDBLACKDC}**	**Kaspersky**	The Trojan ransomware Cryakl (Trojan-Ransom.Win32.Cryakl) is distributed through attached archives in e-mails. More recently it has been found on hacked websites containing a script that detects and harnesses vulnerabilities in software installed on the computer. When inside your PC, the Trojan runs in offline mode, which significantly tangles decryption beyond ransom. When encrypting files on a victim's computer, Cryakl creates a long key that it sends to a command-and-control C&C server. Without this key, it is nearly impossible to recover files impacted by the malware. After that, Cryakl replaces the desktop wallpaper with contact details for its creators together with a ransom demand. Cryakl also displays an image of the mask of the 1964 French movie villain Fantomas.
35	**Crypboss**	https://decrypter.emsisoft.com/crypboss	**.crypt** **.R16M01D05**	**Emsisoft Decrypter**	Use this decrypter is your files have been encrypted and renamed to either *.crypt or *.R16M01D05. In addition the ransom note will ask you to contact a @dr.com email address.

36	**Crybola**	https://support.kaspersky.com/8547#block1	**filenames replaced with long gibberish strings**	**Kaspersky**	RannohDecryptor tool is designed to decrypt files dectypted by **Trojan-Ransom.Win32.Polyglot**, **Trojan-Ransom.Win32.Rannoh**, **Trojan-Ransom.Win32.AutoIt**, **Trojan-Ransom.Win32.Fury**, **Trojan-Ransom.Win32.Crybola**, **Trojan-Ransom.Win32.CryakI** or **Trojan-Ransom.Win32.CryptXXX** versions **1** and **2** and **3**.
37	**CrypBoss**	https://decrypter.emsisoft.com/crypboss	**.crypt .R16M01D05**	**Emsisoft Decrypter**	**CrypBoss** is a ransomware family targetting Windows. Encrypted files are renamed to either *.crypt or *.R16M01D05. The malware drops ransom notes named HELP_DECRYPT.jpg or HELP_DECRYPT.txt into various locations on the system.
38	**Crypren**	https://github.com/pekeinfo/DecryptCrypren	**.encrypted**	**GitHub**	The **Crypren Ransomware** is a ransomware infection that replaces the victim's files' extension with the extension '.ENCRYPTED' after encrypting them using the RSA-2048 encryption.
39	**Crypt38**	https://www.bleepingcomputer.com/forums/t/617607/crypt38-ransomware-help-support-topic-crypt38-regist3030yandexru/	**.crypt38**	**Bleeping Computer**	**Crypt38** is a ransomware-type virus distributed via Russian drive-by download websites. After infiltrating the system, Cryp38 encrypts various stored files (for example, .docx, .pdf, .html, etc.). During encryption, this virus adds a .crypt38 extension to the name of each encrypted file. Following successful encryption, Crypt38 opens a window containing a ransom demand message.
40	**Crypt888 AKA Micop**	https://www.avg.com/en-us/ransomware-decryption-tools#crypt888	**Lock.**	**AVG**	Crypt888 adds **Lock.** to the beginning of filenames. (e.g., Thesis.doc = **Lock.Thesis.doc**) **Ransom message:** After encrypting your files, Crypt888 changes your desktop wallpaper to one of several designs.
		https://files.avast.com/files/decryptor/avast_decryptor_crypt888.exe		**Avast**	Crypt888 adds **Lock.** to the beginning of filenames. (e.g., Thesis.doc = **Lock.Thesis.doc**) **Ransom message:** After encrypting your files, Crypt888 changes your desktop wallpaper to one of several designs.
41	**CryptConsole**	https://www.bleepingcomputer.com/forums/t/638344/cryptconsole-uncrypteoutlookcom-support-topic-how-decrypt-fileshta/	**No file extension added**	**Bleeping Computer**	Uses the following email addresses for communication: **unCrypte@outlook.com**, **decipher_ne@outlook.com**, or **decipher_ne@india.com**. Ransom note is called **How decrypt files.hta**
42	**CryptInfinite AKA DecryptorMax**	https://decrypter.emsisoft.com/cryptinfinite	**.CRINF**	**Emsisoft Decrypter**	Use this decrypter if your files have been encrypted and renamed to *.CRINF.
		https://www.bleepingcomputer.com/news/security/cryptinfinite-or-decryptormax-ransomware-decrypted/		**Bleeping Computer**	**CryptInfinite** or **DecryptorMax** is a ransomware family targeting Windows. It creates ransom notes called ReadDecryptFilesHere.txt on your system and encrypts the many file types.
43	**CryptoDefense**	https://decrypter.emsisoft.com/cryptodefense	**No file extension added**	**Emsisoft Decrypter**	Use this decrypter if the malware identifies itself as CryptoDefense and leaves ransom notes named HOW_DECRYPT.txt behind.
44	**CryptoHost AKA Manamecrypt**	https://www.bleepingcomputer.com/news/security/cryptohost-decrypted-locks-files-in-a-password-protected-rar-file/	**No file extension added**	**Bleeping Computer**	CryptoHost is ransomware, but it doesn't encrypt users' files (although it claims it does). It simply takes a variety of files – images, movies, sound files, Office documents, archive files – found on the victims' computer and places them into an RAR archive located in the *C:\Users\[username]\AppData\Roaming* folder, and protects it with a password. The password required to open the file consists of the name of the RAR file + the user name of the logged in user.
45	**Cryptokluchen**	https://www.nomoreransom.org/decryption-tools.html	**No file extension added**	**Kaspersky**	**Cryptokluchen** is a Trojan ransomware that allegedly encrypts files on an affected system and demands ransom for recovering the data back.

46	**Cryptolocker**	https://www.thewindowsclub.com/cryptolocker-decryption-tool	**No file extension added**	**Fire Eye & Fox It**	Cryptolocker is a Trojan horse that infects your computer and then searches for files to encrypt. This includes anything on your hard drives and all connected media — for example, USB memory sticks or any shared network drives. In addition, the malware seeks out files and folders you store in the cloud. Only computers running a version of Windows are susceptible to Cryptolocker; the Trojan does not target Macs. Once your desktop or laptop is infected, files are "locked" using what's known as asymmetric encryption.
47	**CryptoMix AKA CryptoShield**	https://nomoreransom.cert.pl/static/cryptomix_decryptor.exe	**.CRYPTOSHIELD .rdmk .lesli .scl .code .rmd .rscl .MOLE**	**CERT-PL**	Ransom.**Cryptomix** is a ransomware application that will encrypt files on a victims machine and demand payment to retrieve the information.
		https://files.avast.com/files/decryptor/avast_decryptor_cryptomix.exe (only use Offline)		**Avast**	Two variants are known to exist; CryptoMix, and CryptoShield. Both variants encrypt files by using AES256 encryption with a unique encryption key downloaded from a remote server. However, if the server is not available or if the user is not connected to the internet, the ransomware will encrypt files with a fixed key ("offline key"). Encrypted files will have one of the following extensions: **.CRYPTOSHIELD**, **.rdmk**, **.lesli**, **.scl**, **.code**, **.rmd**, **.rscl** or **.MOLE**
48	**CryptON**	https://decrypter.emsisoft.com/crypton	**.id-_locked .id-_locked_by_krec .id-_locked_by_perfect .id-_x3m .id-_r9oj .id-_garryweber@protonmail.ch .id-_steaveiwalker@india.com_ .id-_julia.crown@india.com_", ".id-_tom.cruz@india.com_", ".id-_CarlosBoltehero@india.com_" and ".id-_maria.lopez1@india.com_".**	**Emsisoft Decrypter**	CryptON aka Nemesis aka X3M is a ransomware family that is mostly used for targetted attacks via RDP. Files are encrypted using a mix of RSA, AES-256 and SHA-256. We have seen the following extensions being used by CryptON: ".id-_locked", ".id-_locked_by_krec", ".id-_locked_by_perfect", ".id-_x3m", ".id-_r9oj", ".id-_garryweber@protonmail.ch", ".id-_steaveiwalker@india.com_", ".id-_julia.crown@india.com_", ".id-_tom.cruz@india.com_", ".id-_CarlosBoltehero@india.com_" and ".id-_maria.lopez1@india.com_".
49	**CryptoTorLocker**	http://www.bleepingcomputer.com/forums/t/565020/new-cryptotorlocker2015-ransomware-discovered-and-easily-decrypted/	**.CryptoTorLocker2015!**	**Bleeping Computers**	It is unclear how CryptoTorLocker 2015 is installed on a system, but once installed it will scan your computer and infect any data files and shortcuts that it finds. As it encrypts each file, it will append **.CryptoTorLocker2015!** to the end of each filename. So a file called invoice.doc would become invoice.doc.CryptoTorLocker2015!. It will also create a ransom note called **HOW TO DECRYPT FILES.txt** in each directory it encounters. The text of the ransom note is below. Please note that this ransom note was actually written this way.
50	**Crypt XXX version 1, 2, & 3**	https://support.kaspersky.com/8547#block1	**.crypt .cryp1 .crypz Or 5 hexadecimal characters**	**Kaspersky**	Once executed, this virus scans all drives and looks for targeted files. When found, CryptXXX encrypts these files using a strong encryption method called RSA4096. It appends infected files with **.crypt** extension. **CryptXXX version 2** ransomware was able to defeat Kaspersky's initial decrypt key, lock the screen and display alarming message on the desktop. **CryptXXX version 3** was released. This version appends the file with **.crypz** extension.
		https://www.thewindowsclub.com/trend-micro-ransomware-file-decryptor		**Trend Micro**	**Trend Micro Ransomware File Decryptor** is a free Ransomware Decryptor Tool that will help you unlock files that have been locked by select ransomware.
		https://www.bleepingcomputer.com/virus-removal/cryptxxx-ransomware-help-information		**Bleeping Computer**	
		http://14.141.38.197:8765/QH/Ransom_Decryptor_v1.0.0.2.zip		**Quick Heal**	

51	**Crypt XXX version 4, & 5**	https://www.thewindowsclub.com/trend-micro-ransomware-file-decryptor	**5 hexadecimal characters**	**Trend Micro**	Any files that are encrypted with **CryptXXX 4.x/5.x** will have a random 32 hexadecimal characters (MD5 Hash).**random 5 hexadecimal character** pattern (i.e. 0412C29576C708CF0155E8DE242169B1.**6B3FE**) appended to the end of the encrypted data filename.
52	**Crysis**	https://www.thewindowsclub.com/trend-micro-ransomware-file-decryptor	**.CrySIS .xtbl .crypt**	**Trend Micro**	**Trend Micro Ransomware File Decryptor** is a free Ransomware Decryptor Tool that will help you unlock files that have been locked by select ransomware.
		https://files.avast.com/files/decryptor/avast_decryptor_crysis.exe		**Avast**	CrySiS (JohnyCryptor, Virus-Encode, Aura, Dharma) is a ransomware strain that has been observed since September 2015. It uses AES-256 combined with RSA-1024 asymmetric encryption.
		https://download.eset.com/com/eset/tools/decryptors/crysis/latest/esetcrysisdecryptor.exe		**Eset**	
		http://14.141.38.197:8765/QH/Ransom_Decryptor_v1.0.0.2.zip		**Quick Heal**	
53	**CuteRansomware**	https://github.com/aaaddress1/my-Little-Ransomware/tree/master/decryptoTool	**.加密**	**Git Hub**	**CuteRansomware** uses Google Docs to deliver malicious files to victims and as a C2 server, storing encryption keys and data exfiltrated from victims' machines. This distribution method bypasses network firewalls and intrusion prevention systems as data is transmitted over SSL due to Google Docs use of HTTPS. CuteRansomware is also difficult to block because the only way to avoid it is to block the specific instance of the app containing the malware.
54	**Damage**	https://decrypter.emsisoft.com/damage	**.damage**	**Emsisoft Decrypter**	Damage is a ransomware written in Delphi. It uses a combination of SHA-1 and Blowfish to encrypt the first and last 8 kb of a file. Encrypted files have the extension ".damage" and the ransom note, which is named "damage@india.com[COMPUTERNAME].txt", asks to contact "damage@india.com".
55	**Decrypt Protect**	http://tmp.emsisoft.com/fw/decrypt_mblblock.exe	**.html**	**Emsisoft Decrypter**	The **Decrypt Protect Virus MBLPCBlock.In** (also known as MBL Advisory Virus) is one of the latest computer locked viruses in the long line of moneypak ransomware attacks. All files are changed to .html extensions and redirected. Your system and all your files have been blocked and encrypted. html virus mblblock from http://mblblock.in or http://mblpcblock.in/index.php?
56	**Democry**	http://media.kaspersky.com/utilities/VirusUtilities/EN/rakhnidecryptor.zip	**._[timestamp_$email_address$].777 ._[timestamp_$email_address$].legion**	**Kaspersky**	Concatenates one of the following strings to encoded files: **._[timestamp_$email_address$].777** or **._[timestamp_$email_address$].legion**; the ransom note is called **read_this_file.txt**
57	**DerailLock**	https://www.nomoreransom.org/uploads/deria.pdf	**.deria**	**Quick Heal**	
58	**Dharma**	https://support.kaspersky.com/8547#block1	**.bip**	**Kaspersky**	RannohDecryptor tool is designed to decrypt files dectypted by **Trojan-Ransom.Win32.Polyglot**, **Trojan-Ransom.Win32.Rannoh**, **Trojan-Ransom.Win32.Autolt**, **Trojan-Ransom.Win32.Fury**, **Trojan-Ransom.Win32.Crybola**, **Trojan-Ransom.Win32.Cryakl** or **Trojan-Ransom.Win32.CryptXXX** versions **1** and **2** and **3**.
59	**DMALocker**	https://decrypter.emsisoft.com/dmalocker	**No file extension added**	**Emsisoft Decrypter**	Use this decrypter if your files have been encrypted but not renamed. The malware identifies itself as DMA Locker and the ID is "DMALOCK 41:55:16:13:51:76:67:99".
60	**DMALocker2**	https://decrypter.emsisoft.com/dmalocker2	**No file extension added**	**Emsisoft Decrypter**	Use this decrypter if your files have been encrypted but not renamed. The malware identifies itself as DMA Locker and the ID is "DMALOCK 43:41:90:35:25:13:61:92".
61	**DXXD**	https://www.thewindowsclub.com/trend-micro-ransomware-file-decryptor	**.DXXD**	**Trend Micro**	**Trend Micro Ransomware File Decryptor** is a free Ransomware Decryptor Tool that will help you unlock files that have been locked by select ransomware.

62	**Encryptile**	https://files.avast.com/files/decryptor/avast_decryptor_encryptile.exe	**encrypTile**	**Avast**	EncrypTile uses AES-128 encryption, using a key that is constant for a given PC and user. The ransomware adds the word "encrypTile" into a file name. While running, the ransomware actively prevents the user from running any tools that might potentially remove it.
63	**Everbe**	https://www.bleepingcomputer.com/news/security/decryptor-released-for-the-everbe-ransomware/	**.everbe** **.embrace** **.pain**	**Bleeping Computers**	When victims are infected, their files will be encrypted and will have the **.[everbe@airmail.cc].everbe, .embrace,** or **.pain** extensions appended to the encrypted file's name.
64	**Fabiansomware**	http=s://decrypter.emsisoft.com/fabiansomware	**.encrypted**	**Emsisoft Decrypter**	Use this decrypter if your files have been encrypted and renamed to *.encrypted with ransom notes named *.How_To_Decrypt_Your_Files.txt. The ransom note asks you to contact "decryptioncompany@inbox.ru", "fwosar@mail.ru" or "fabianwosar@mail.ru". To use the decrypter you will require a file pair containing both an encrypted file and its non-encrypted original version. It is important to use a file pair that is as large as possible, as it determines the maximum file size up to which the decrypter will be able to decrypt your files. Select both the encrypted and unencrypted file and drag and drop both of them onto the decrypter file in your download directory.
65	**FenixLocker**	https://decrypter.emsisoft.com/fenixlocker	**.centrumfr@india.com!!**	**Emsisoft Decrypter**	Use this decrypter if your files have been encrypted by the FenixLocker ransomware. FenixLocker encrypts files and renames them by appending the ".centrumfr@india.com!!" extension. It leaves behind a ransom note named "CryptoLocker.txt" or "Help to decrypt.txt" on your Desktop, instructing you to contact "centrumfr@india.com". To start the decrypter simply drag and drop one of your encrypted files onto the decrypter executable.
66	**FindZip**	https://files.avast.com/files/decryptor/avast_decryptor_findzip.exe	**.crypt**	**Avast**	FindZip is a ransomware strain that spreads on Mac OS X (version 10.11 or newer). The encryption is based on creating ZIP files - each encrypted file is a ZIP archive, containing the original document. Encrypted files will have the **.crypt** extension.
67	**Fury**	https://support.kaspersky.com/8547#block1	**No file extension added**	**Kaspersky**	Does not affect the names of encrypted files, displays a desktop wallpaper with recovery steps
68	**GandCrab**	https://labs.bitdefender.com/wp-content/uploads/downloads/grandcrab-removal-tool/	**.GDCB** **.KRAB**	**BitDefender**	**GandCrab ransomware** is the most serious cryptovirus of the time that keeps evolving. GandCrab relies on a .doc file which is downloaded to the system once the victim clicks on the malicious attachment. The .doc file subsequently runs a PowerShell script and creates an exploit file (sct5.txt), which currently affects a 64-bit system. As pointed out by various crypto-malware researchers, the sct5.txt file does not run the ultimate payload of the virus, but executes an exploit and runs as a medium for malware to get inside.
		https://www.thewindowsclub.com/360-ransomware-decryption-tool		**The Windows Club**	
69	**GhostCrypt**	https://download.bleepingcomputer.com/demonslay335/GhostCryptDecrypter.zip	**.Z81928819**	**Bleeping Computers**	Appends files with the **.Z81928819** extension and drops **READ_THIS_FILE.txt** ransom note

70	**Globe** **AKA** **Purge**	https://decrypter.emsisoft.com/globe	**.ACRYPT .GSupport[0-9] .blackblock .dll555 .duhust .exploit .frozen .globe .purge .gsupport .kyra .purge .raid[0-9] .siri-down@india.com .xtbl .zendrz .zendr[0-9] .hnyear**	**Emsisoft Decrypter**	Globe is a ransomware kit that was first discovered at the end of August. Files are encrypted using Blowfish. Since the extension of encrypted files is configurable, several different file extensions are possible. The most commonly used extensions are .purge, .globe and .okean-1955@india.com.!dsvgdfvdDVGR3SsdvfEF75sddf#xbkNY45fg6}P{cg.xtbl. To use the decrypter you will require a file pair containing both an encrypted file and its non-encrypted original version. It is important to use a file pair that is as large as possible, as it determines the maximum file size up to which the decrypter will be able to decrypt your files. Select both the encrypted and unencrypted file and drag and drop both of them onto the decrypter file in your download directory.
		https://www.thewindowsclub.com/trend-micro-ransomware-file-decryptor		**Trend Micro**	**Trend Micro Ransomware File Decryptor** is a free Ransomware Decryptor Tool that will help you unlock files that have been locked by select ransomware.
		https://files.avast.com/files/decryptor/avast_decryptor_globe.exe		**Avast**	Globe adds one of the following extensions to the file name: "**.ACRYPT**", "**.GSupport[0-9]**", "**.blackblock**", "**.dll555**", "**.duhust**", "**.exploit**", "**.frozen**", "**.globe**", "**.gsupport**", "**.kyra**", "**.purged**", "**.raid[0-9]**", "**.siri-down@india.com**", "**.xtbl**", "**.zendrz**", "**.zendr[0-9]**", or "**.hnyear**". Furthermore, some of its versions encrypt the file name as well.
		http://14.141.38.197:8765/QH/Ransom_Decryptor_v1.0.0.2.zip		**Quick Heal**	[.hnyear]
71	**Globe2**	https://decrypter.emsisoft.com/globe2	**.blt**	**Emsisoft Decrypter**	Globe2 encrypts files and optionally file names using RC4. Since the extension of encrypted files is configurable, several different file extensions are possible. The most commonly used extensions are .raid10, .blt, .globe, .encrypted and .[mia.kokers@aol.com]. To use the decrypter you will require a file pair containing both an encrypted file and its non-encrypted original version. Select both the encrypted and unencrypted file and drag and drop both of them onto the decrypter file in your download directory. If file names are encrypted, please use the file size to determine the correct file. Encrypted and original file will have exactly the same size.
		http://14.141.38.197:8765/QH/Ransom_Decryptor_v1.0.0.2.zip		**Quick Heal**	
72	**Globe3**	https://decrypter.emsisoft.com/globe3	**.decrypt2017 .globe .hnumkhotep .happydayzz**	**Emsisoft Decrypter**	Globe3 is a ransomware kit that we first discovered at the beginning of 2017. Globe3 encrypts files and optionally filenames using AES-256. Since the extension of encrypted files is configurable, several different file extensions are possible. The most commonly used extensions are .decrypt2017 and .hnumkhotep. To use the decrypter, you will require a file pair containing both an encrypted file and its non-encrypted original version. Select both the encrypted and unencrypted file and drag and drop both of them onto the decrypter file in your download directory. If file names are encrypted, please use the file size to determine the correct file. The encrypted and the original file will have the same size for files greater than 64 kb.
		http://14.141.38.197:8765/QH/Ransom_Decryptor_v1.0.0.2.zip		**Quick Heal**	[.decrypt2017] [.globe & .happydayzz]
73	**GlobeImposter**	https://decrypter.emsisoft.com/globeimposter	**.crypt**	**Emsisoft Decrypter**	GlobeImposter is a Globe copycat that imitates the ransom notes and file extension found in the Globe ransomware kit. Encrypted files have the extension *.crypt and the base name of the file is unchanged. The ransom note is named "HOW_OPEN_FILES.hta" and can be found in all folders that contain encrypted files.

74	**GoldenEye**	https://www.thewindowsclub.com/360-ransomware-decryption-tool	**No file extension added**	**The Windows Club**	**GoldenEye** the destroyer. Researchers from both Comae Technologies and Kaspersky Lab found that **GoldenEye was** a wiper, designed to destroy data. It used as its base a form of **ransomware** called Petya (hence the NotPetya name) to encrypt crucial files, steal login credentials and seize your hard drive, too.
75	**Gomasom**	https://decrypter.emsisoft.com/gomasom	**.crypt**	**Emsisoft Decrypter**	Use this decrypter if files have been encrypted, renamed to *.crypt and the file name contains an email address to contact.
76	**Gryphon**	https://www.thewindowsclub.com/360-ransomware-decryption-tool	**.[chines34@protonmail.ch].gryphon**	**The Windows Club**	**Gryphon is** a file-encrypting **ransomware**, which **will** encrypt the personal documents found on victim's, appending the .[chines34@protonmail.ch].**gryphon** extension to encrypted files. The **Gryphon ransomware** then displays a message which offers to decrypt the data if a payment between $500 and $1500 in Bitcoins**is** made.
77	**Harasom**	https://decrypter.emsisoft.com/harasom	**.html**	**Emsisoft Decrypter**	Use this decrypter if your files have been converted into *.html files and the ransom note pretends to originate either from Spamhaus or the US Department of Justice.
78	**HiddenTear**	https://files.avast.com/files/decryptor/avast_decryptor_hiddentear.exe	**.locked .34xxx .bloccato .BUGSECCCC .Hollycrypt .lock .saeid .unlockit .razy .mecpt .monstro .lok .암 호 화 됨 .8lock8 .fucked .flyper .kratos .krypted .CAZZO .doomed**	**Avast**	HiddenTear is one of the first open-sourced ransomware codes hosted on GitHub and with hundreds of HiddenTear variants produced by crooks using the original source code. HiddenTear uses AES encryption. Encrypted files will have one of the following extensions (but not limited to): **.locked**, **34xxx**, **.bloccato**, **.BUGSECCCC**, **.Hollycrypt**, **.lock**, **.saeid**, **.unlockit**, **.razy**, **.mecpt**, **.monstro**, **.lok**, **.암 호 화 됨** , **.8lock8**, **.fucked**, **.flyper**, **.kratos**, **.krypted**, **.CAZZO**, **.doomed**.
79	**HydraCrypt and UmbreCrypt**	https://decrypter.emsisoft.com/hydracrypt	**.hydracrypt .umbrecrypt**	**Emsisoft Decrypter**	HydraCrypt and UmbreCrypt are the two new Ransomware variants from the CrypBoss Ransomware family. Once successful in breaching your PC security, HydraCrypt and UmbreCrypt can lock your computer and deny access to your own files. Use this decrypter if your files have been encrypted and renamed to either *.hydracrypt* or *.umbrecrypt*.
80	**ICE Cyber Centre Ransomware**	http://forum.thewindowsclub.com/windows-security/35546-trend-micro-antiransomware-tool-remove-ransomware.html	**No file extension added**	**The Windows Club**	The **ICE Cyber Crime Center Ransomware** is part of the **Troj/Reveton-Ransomware** family and displays a lock screen that requires you to pay a ransom before you will be allowed to access your Windows desktop, applications, or files. This ransomware infection pretends to be from the Department of Homeland Security's ICE Cyber Crime Center and states that it has detected that your computer has been involved in illegal cyber activity. This ransomware will also attempt to take a picture of you via your Webcam to further scare you into sending in the ransom. Last, but not least, this ransomware infection will also delete your Windows Automatic Update service so that you are unable to automatically update Windows.

81	**Jaff** **AKA** **Encryptile**	http://media.kaspersky.com/utilities/VirusUtilities/EN/rakhnidecryptor.zip	**.jaff** **.wlu** **.sVn**	**Kaspersky**	The ransomware is being distributed via "multiple high volume spam campaigns" by the Necurs botnet, which had formerly distributed Locky ransomware. The spam emails have a PDF attachment "with an embedded Microsoft Word document functioning as the initial downloader for the Jaff ransomware. Jaff ransomware successfully encrypts a PC, it demands from 0.5 to 2 bitcoins - from $1,500 to $5,000 at current market rates
82	**Jigsaw** **AKA** **CryptoHit**	https://www.thewindowsclub.com/trend-micro-ransomware-file-decryptor	**Randomly adds one of the following file extensions:** **.kkk** **.btc** **.gws** **.J** **.encrypted** **.porno** **.payransom** **.pornoransom** **.epic** **.xyz** **.versiegelt** **.encrypted,** **.payb** **.pays** **.payms** **.paymds** **.paymts** **.paymst** **.payrms** **.payrmts** **.paymrts** **.paybtcs** **.fun** **.hush** **.uk-dealer@sigaint.org** **.gefickt.**	**Trend Micro**	**Trend Micro Ransomware File Decryptor** is a free Ransomware Decryptor Tool that will help you unlock files that have been locked by select ransomware.
		https://files.avast.com/files/decryptor/avast_decryptor_jigsaw.exe		**Avast**	Jigsaw is named after the movie character "The Jigsaw Killer". Several variants of this ransomware use the Jigsaw Killer's picture in the ransom screen. Encrypted files will have one of the following extensions: **.kkk**, **.btc**, **.gws**, **.J**, **.encrypted**, **.porno**, **.payransom**, **.pornoransom**, **.epic**, **.xyz**, **.versiegelt**, **.encrypted**, **.payb**, **.pays**, **.payms**, **.paymds**, **.paymts**, **.paymst**, **.payrms**, **.payrmts**, **.paymrts**, **.paybtcs**, **.fun**, **.hush**, **.uk-dealer@sigaint.org**, or **.gefickt**.
		https://download.bleepingcomputer.com/demonslay335/JigSawDecrypter.zip		**Bleeping Computer**	Jigsaw ransomware deletes your files if you don't pay up.
83	**KeRanger**	https://news.drweb.com/show/?i=9877&lng=en&c=5	**.encrypted** **README_FOR_DECRYPT.txt** **.kernel_pid** **.kernel_time** **.kernel_complete**	**Dr Web** *(Caution: this is a software company based in Moscow)*	Once **Mac.Trojan.KeRanger.2** is installed on the infected computer, it waits for three days before connecting to the C&C server over the TOR network. Then it starts the encryption procedure. First, the Trojan encrypts all files that it can access with the help of either user or root privileges. **Mac.Trojan.KeRanger.2** then tries to encrypt the contents of the /Volumes logical partition—that is, files stored on a hard drive and on mounted logical partitions. In that case, files are encrypted according to the Trojan's certain list that contains 313 different file types including text files and images. The Trojan downloads an encryption key and a file with cybercriminals' demands from the server.

84	**KeyBTC**	https://decrypter.emsisoft.com/keybtc	**.theva .cryptobyte .cryptowin .btcware .onyon**	**Emsisoft Decrypter**	This ransomware encrypts the system and adds an extension to files (the extension will depend upon the version of the ransomware). After execution, the ransomware generates a random password (one per machine), which is then used to create of the encryption key. The password is then encrypted with a public key (hardcoded in the binary) and presented as a User ID in the ransom files. Use this decrypter if you find a ransom note called DECRYPT_YOUR_FILES.txt on your system that asks you to contact keybtc@inbox.com for decryption.
		https://blog.avast.com/avast-releases-decryptor-tool-for-btcware-ransomware		**Avast**	
85	**KimicilWare**	https://www.fortinet.com/blog/threat-research/kimcilware-ransomware-how-to-decrypt-encrypted-files-and-who-is-behind-it.html	**.kimicilware .locked**	**Fortinet**	Once it infects a web server, one version of the ransomware encrypts files and appends the *.kimcilware* extension to them. In this case, victims are instructed via an "index.html" file added to the infected website to pay $140 to recover their data. Another variant, which appends the *.locked* extension to encrypted files, demands the payment of 1 Bitcoin (roughly $415) in return for a "decryption package."
86	**Lambda Locker**	https://files.avast.com/files/decryptor/avast_decryptor_lambdalocker.exe	**.MyChemicalRomance4EVER**	**Avast**	LambdaLocker is a ransomware strain that we first observed in May 2017. It is written in Python programming language and the currently prevalent variant is decryptable. The ransomware adds the **".MyChemicalRomance4EVER"** extension after a file name: **foobar.doc -> foobar.doc.MyChemicalRomance4EVER** **document.dat -> document.dat.MyChemicalRomance4EVER**
87	**Lamer**	http://media.kaspersky.com/utilities/VirusUtilities/EN/rakhnidecryptor.zip	**.kraken .darkness .locked**	**Kaspersky**	Lamer infects the computer encrypts the files and renames them by adding '.kraken', .darkness' or '.locked'.
88	**LeChiffre**	https://decrypter.emsisoft.com/lechiffre	**.LeChiffre**	**Emsisoft Decrypter**	Use this decrypter if your files have been encrypted and renamed to *.LeChiffre and the ransom note asks you to contact decrypt.my.files@gmail.com via email.
		https://www.thewindowsclub.com/trend-micro-ransomware-file-decryptor		**Trend Micro**	**Trend Micro Ransomware File Decryptor** is a free Ransomware Decryptor Tool that will help you unlock files that have been locked by select ransomware.
		http://14.141.38.197:8765/QH/Ransom_Decryptor_v1.0.0.2.zip		**Quick Heal**	
89	**Legion**	https://www.avg.com/en-us/ransomware-decryption-tools#legion	**._23-06-2016-20-27-23_$f_tactics@aol.com$.legion .$centurion_legion@aol.com$.cb**	**AVG**	Legion adds a variant of ._23-06-2016-20-27-23_$f_tactics@aol.com$.legion or .$centurion_legion@aol.com$.cbf to the end of filenames. (e.g., Thesis.doc = Thesis.doc._23-06-2016-20-27-23_$f_tactics@aol.com$.legion). After encrypting your files, Legion changes your desktop wallpaper and displays a popup which says: 'Your data is encrypted!!! The latest encryption algorithm. To return the file to an email email f-tactics@aol.com
		https://files.avast.com/files/decryptor/avast_decryptor_legion.exe		**Avast**	Legion adds a variant of ._23-06-2016-20-27-23_$f_tactics@aol.com$.legion or .$centurion_legion@aol.com$.cbf to the end of filenames. (e.g., Thesis.doc = Thesis.doc._23-06-2016-20-27-23_$f_tactics@aol.com$.legion).
90	**Linux.Encoder 1 & 3**	https://labs.bitdefender.com/wp-content/plugins/download-monitor/download.php?id=encoder_3_decrypter.zip	**.encrypted**	**BitDefender**	**Linux.Encoder** targets Linux servers and Linux-based websites as it encrypts MySQL, Apache, and root folders. It exploits a flaw in Magento, an open-source content management system application designed for e-commerce sites. Files locked by Linux.Encoder display .encrypted as the file name extension. There are currently three versions of this ransomware.

91	**Locker**	https://www.bleepingcomputer.com/virus-removal/locker-ransomware-information	**No file extension added**	**Bleeping Computer**	**Locker ransomware** is a virus that infects PCs and locks the users files, preventing access to data and files located on the PC until a ransom or fines are paid.
92	**Lock Screen**	https://esupport.trendmicro.com/en-us/home/pages/technical-support/1105975.aspx	**No file extension added**	**Trend Micro**	This ransomware infects your computer through a visit to an infected website. It blocks access to operating system, displays a lock screen. The ransomware says Homeland Security knows you've browsed an illegal site and now you have to pay. Your operating system is completely locked out by the ransomware and you feel you have no options but to pay.
93	**Locky**	https://www.bleepingcomputer.com/virus-removal/locky-ransomware-information-help	**.locky**	**Bleeping Computer**	The **ransomware** uses RSA-2048 + AES-128 cipher with ECB mode to encrypt files. Keys are generated on the server side, making manual decryption impossible, and **Locky ransomware** can encrypt files on all fixed drives, removable drives, network and RAM disk drives.
94	**Lortok**	http://media.kaspersky.com/utilities/VirusUtilities/EN/rakhnidecryptor.zip	**.crime**	**Kaspersky**	Appends files with the **.crime** extension or string of random hexadecimal characters; ransom notes are in Russian
95	**MacRansom**	https://esupport.trendmicro.com/media/13801530/Trend%20Micro%20Ransomware%20Decryptor_V1.0.1.zip	**No file extension added**	**Trend Micro**	**Mac ransomware is** simply **ransomware** that targets Apple desktops and laptops. Once it infects the Apple machine it is completely invisible until it scheduled execution time. it encrypts the whole of the victims home directory within a minute and encrypts with 128-bit encryption before displaying the ransom screen.
96	**Magician**	http://www.free-uninstall.org/how-to-remove-magician-ransomware-and-decrypt-magic-files/	**.magic**	**Uninstall IT**	Magician Ransomware is a virus that encrypts user files. The list of victim files is huge, for example, it affects media files, such as photos, images, video files, PDF and so on. It uses a sophisticated encryption algorithm AES, thereby restore the files by yourself is practically impossible. Magician Ransomware changes the file extensions to **.MAGIC** and completely disables them. After encrypting, it completely blocks the system, the launch of Task Manager and other system tools. In addition, Magician Ransomware excludes the possibility of restoring the previous system restore points.
97	**Maktub**	https://www.securitystronghold.com/gates/remove-maktub-virus.html	**.Norv**	**Security Stronghold**	Maktub is ransomware virus distributed in zipped documents attached to spam e-mails. During opening document runs macros that downloads Maktub executable, enters the system and encrypts files stored on the victim's computer. Maktub adds .NORV extension to affected files. Virus allows ransom ($200 - $600) to be paid during 12 hours frame or decryption would be impossible. As Maktub may encrypt important documents and images, this is very dangerous virus. There is currently no decryption tool for .NORD files.
98	**Marlboro**	https://decrypter.emsisoft.com/marlboro	**.oops**	**Emsisoft Decrypter**	The Marlboro ransomware was first seen on January 11th, 2017. It is written in C++ and uses a simple XOR based encryption algorithm. Encrypted files are renamed to ".oops". The ransom note is stored inside a file named "_HELP_Recover_Files_.html" and includes no further point of contact. Due to a bug in the malware's code, the malware will truncate up to the last 7 bytes from files it encrypts. It is, unfortunately, impossible for the decrypter to reconstruct these bytes.
99	**MarsJoke**	https://support.kaspersky.com/8547#block1	**.oops**	**Kaspersky**	Concatenates the **.oops** string to encrypted files and leaves **_HELP_Recover_Files.html**ransom how-to
100	**Merry X-Mas or MRCR**	https://decrypter.emsisoft.com/mrcr	**.pegs1 .mrcr1 .rare1 .merry .rmcm1**	**Emsisoft Decrypter**	Merry X-Mas is a ransomware family is written in Delphi and uses a custom encryption algorithm. Encrypted files will have either ".PEGS1", ".MRCR1", ".RARE1", ".MERRY", or ".RMCM1" as an extension. The ransom note is named "YOUR_FILES_ARE_DEAD.HTA" or "MERRY_I_LOVE_YOU_BRUCE.HTA" and asks victims to contact either "comodosec@yandex.ru" or "comodosecurity" via the secure mobile messenger Telegram.
101	**MirCop**	https://www.thewindowsclub.com/trend-micro-ransomware-file-decryptor	**This ransomware does not change the file extension**	**Trend Micro**	**Trend Micro Ransomware File Decryptor** is a free Ransomware Decryptor Tool that will help you unlock files that have been locked by select ransomware.

102	**Mole**	https://nomoreransom.cert.pl/static/mole_decryptor.exe	**.mole**	**Cert-PL**	Mole is distributed through SPAM emails that pretend to be shipping notifications. These emails state that a package could not be delivered and then displays a link to a site where additional information. When a user clicks on the enclosed link, it will redirect to a fake Microsoft Word Online site that displays a supposedly unreadable document. This page then states that the document cannot be read in the browser and that the victim needs to download and install a plugin. If the user clicks on the download button, it will download a file named **plugin-office.exe**or **pluginoffice.exe**. If these files are executed, the Mole Ransomware will be installed. Once the ransomware executable is downloaded and executed on the victim's computer, it will display a fake alert that states: This fake alert is designed to coerce a victim into clicking Yes at a UAC prompt so the ransomware runs with administrative privileges. Once you press OK button in the above prompt, you will be presented with a User Account Control prompt, which asks if you wish to allow the command **"C:\Windows\SysWOW64\wbem\WMIC.exe" process call create "%UserProfile%\pluginoffice.exe"** to execute.
103	**Moneropay**	https://link.safecart.com/22hacu/aHR0cDovL2Rvd25sb2FkLmVuaWdtYXNvZnR3YXJlLmNvbS9zcHlodW50ZXItZnJlZS1kb3dubG9hZC9yZXZlbnVld2lyZS9TcHlldW50ZXItSW5zdGFsbGVyLmV4ZQ?rza	**.encrypted**	**Safecart**	MoneroPay tries to take advantage of the cryptocurrency craze by spreading itself as a wallet for a fake coin called SpriteCoin. While users were installing what they thought was a new cryptocoin, MoneroPay was silently encrypting the files on the computer. Once a user downloaded and ran the wallet, it would load up and go through what appeared to be a normal setup for a new cryptocoin wallet. When you install a cryptocoin wallet for the first time, the wallet first needs to connect to the coin's network and synchronize itself with the blockchain. Depending on how many coins have already been mined and the speed of the network, this process can take a long time. Knowing this, the ransomware developer encrypted the computer while the SpriteCoin wallet pretended to download and synchronize the blockchain. As this normally takes a long time and could cause a lot of hard drive activity, it was the perfect cover for the MoneroPay ransomware.
104	**NanoLocker**	https://github.com/Cyberclues/nanolocker-decryptor	**No file extension added**	**GitHub**	Does not add any extension to encrypted filenames; creates the **ATTENTION.rtf** ransom note on the desktop
105	**Nemucod**	https://decrypter.emsisoft.com/nemucod	**.crypted**	**Emsisoft Decrypter**	Use this decrypter if your files have been renamed to *.crypted and you find a ransomnote named DECRYPT.txt on your desktop. To use the decrypter you will require an encrypted file of at least 4096 bytes in size as well as its unencrypted version. To start the decrypter select both the encrypted and unencrypted file and drag and drop them onto the decrypter executable.
		https://www.thewindowsclub.com/trend-micro-ransomware-file-decryptor		**Trend Micro**	**Trend Micro Ransomware File Decryptor** is a free Ransomware Decryptor Tool that will help you unlock files that have been locked by select ransomware.
		http://14.141.38.197:8765/QH/Ransom_Decryptor_v1.0.0.2.zip		**Quick Heal**	
106	**NemucodAES**	https://decrypter.emsisoft.com/nemucodaes	**.crypted**	**Emsisoft Decrypter**	NemucodAES is a new variant of the Nemucod ransomware family. Written in a combination of JavaScript and PHP it uses AES and RSA in order to encrypt your files. Encrypted files will keep their original file names and a ransom note named "DECRYPT.hta" can be found on your Desktop.
107	**Ninja**	http://14.141.38.197:8765/QH/Ransom_Decryptor_v1.0.0.2.zip	**.@aol.com$777**	**Quick Heal**	**Ninja Ransomware** [@aol.com$.777] is a Russian Trojan horse malware infection that it sneaks silently onto your Windows operating system, once it activates itself and displays its ransom note on your desktop, you will definitely know about its presence. When this Trojan hits you, it hits you hard. It encrypts main file types on your hard drive, which you can only decrypt by paying a certain amount to the cyber criminals behind this intrusive Trojan. This Trojan might arrive as a simple spam e-mail to your Inbox, and disguise itself as a “must see” picture or video, but it can also be a .pdf file sometimes. Once you click on the attachment, it downloads and activates in the background right away.

108	**NMoreira**	https://decrypter.emsisoft.com/nmoreira	**.maktub .__AiraCropEncrypted!**	**Emsisoft Decrypter**	Use this decrypter if your files have been renamed to either *.maktub or *.__AiraCropEncrypted! and you find a ransom note named either "Recupere seus arquivos. Leia-me!.txt" or "How to decrypt your files.txt" on your system.
109	**NoobCrypt**	https://twitter.com/JakubKroustek/status/775040000278818817		**Jakub Kroustek**	
		https://files.avast.com/files/decryptor/avast_decryptor_noobcrypt.exe	**No file extension added**	**Avast**	NoobCrypt doesn't change file name. Files that are encrypted are unable to be open with their associated application, however. For encrypting user's files, this ransomware uses AES 256 encryption method.
110	**ODCODC**	http://14.141.38.197:8765/QH/Ransom_Decryptor_v1.0.0.2.zip	**.odcodc**	**Quick Heal**	**[.ODCODC] Ransomware** is a dangerous ransom virus which was made to lock your computer and deny access to your own files. Just like other ransomware, this new threat will encrypt certain files on the computer. It also changes file extensions to **.odcodc** and demand payment before you can regain access and reverse these changes. It demands user to pay certain amount using specified payment websites.
111	**Opentoyou**	http://14.141.38.197:8765/QH/Ransom_Decryptor_v1.0.0.2.zip	**.-opentoyou@india.com**	**Quick Heal**	When it first infects a computer, the **OpenToYou ransomware** will create a password string, use SHA-1 to derive an encryption key from the password, which it then uses to encrypt the victim's files with the RC4 algorithm. As a side note, **OpenToYou** also encrypts files without a file extension. [.-opentoyou@india.com]
		https://decrypter.emsisoft.com/opentoyou		**Emsisoft Decrypter**	When it first infects a computer, the **OpenToYou ransomware** will create a password string, use SHA-1 to derive an encryption key from the password, which it then uses to encrypt the victim's files with the RC4 algorithm. As a side note, **OpenToYou** also encrypts files without a file extension. [.-opentoyou@india.com] The ransomware will lock files on all drives with a number of exceptions. However due to an error in the programming this leaves the victim's computer in the unfortunate situation of not being able to boot the next time they restart their PC.
112	**Operation Global III**	https://news.thewindowsclub.com/operation-global-iii-ransomware-decryption-tool-released-70341/	**.exe**	**The Windows Club**	This ransomware attacks your system and then displays leaving the user with no choice but to pay the ransom amount. All your encrypted file extensions are changed to .EXE and are infected with the malicious codes.
113	**OpenToYou**	https://decrypter.emsisoft.com/opentoyou	**.-opentoyou@india.com**	**Emsisoft Decrypter**	OpenToDecrypt is a ransomware written in the Delphi programming language that encrypts your files using the RC4 encryption algorithm. Encrypted files get renamed to *.-opentoyou@india.com and a ransom note named "!!!.txt" can be found on your Desktop.
114	**Ozozalocker**	https://decrypter.emsisoft.com/ozozalocker	**.locked**	**Emsisoft Decrypter**	Use this decrypter if your files have been renamed to *.locked and you find a ransom note named "HOW TO DECRYPT YOU FILES.txt" on your desktop. Double clicking an encrypted file will also display a message box instructing you to contact "santa_helper@protonmail.com". To use the decrypter you will require an encrypted file of at least 510 bytes in size as well as its unencrypted version. To start the decrypter select both the encrypted and unencrypted file and drag and drop them onto the decrypter executable.
115	**PClock**	https://decrypter.emsisoft.com/pclock	**No file extension added**	**Emsisoft Decrypter**	Does not change filenames, stores the list of scrambled data inside **enc_files.txt** document
116	**PETYA**	https://www.thewindowsclub.com/petya-ransomware-decrypt-tool-password-generator	**No file extension added**	**The Windows Club**	PETYA ransomware is one of the most recent online threats for PC users. It is a malware which overwrites the MBR (Master Boot Record) of your PC and leaves it unbootable and also disallows restarting the PC in Safe Mode.
		https://www.thewindowsclub.com/360-ransomware-decryption-tool		**The Windows Club**	Ransomware is not necessarily a one-time attack. It is very likely that your PC might get attacked once again even after it is patched, in fact, the chances of this happening is pretty high. The 360 Decryption Tool offers you a chance of getting files back without having to pay the ransom.

117	**Philadelphia**	https://decrypter.emsisoft.com/philadelphia	**.locked**	**Emsisoft Decrypter**	Philadelphia is a ransomware kit offered within various hacking communities. Written in AutoIt, it encrypts files using AES-256 encryption, file names using RC4 encryption and uses the *.locked file extension. It is based on a similar ransomware kit called "Stampado" that is written by the same author. To use the decrypter you will require a file pair containing both an encrypted file and its non-encrypted original version. Due to the file name encryption this can be a bit tricky. The best way is to simply compare file sizes. Encrypted files will have the size of the original file rounded up to the next 16 byte boundary. So if a the original file was 1020 bytes large, the encrypted file will be 1024. Select both the encrypted and non-encrypted file and drag and drop both of them onto the decrypter file in your download directory.
118	**PHP Ransomware**	http://blog.checkpoint.com/wp-content/uploads/2016/12/PHP-ransomware-decryptor.zip	**.crypted**	**Checkpoint**	This ransomware is more of a PHP script and not a piece of ransomware per se, as it doesn't ask for a ransom to decrypt files. It only encrypts files, without displaying a ransom note and without attempting to communicate with a command and control (C&C) server. The script checks folders recursively and, when it finds files with specific extensions, changes the access permissions for reading, writing and executing them. Next, the script encrypts the first 2048 bytes of each file (or the entire file if it's smaller than 2048 bytes), and appends the **.crypted** extension to them.
119	**PizzaCrypts** **AKA** **JuicyLemon**	http://download.bleepingcomputer.com/BloodDolly/JuicyLemonDecoder.zip	**. id-[victim_ID]_maestro@pizzacrypts.info**	**Bleeping computers**	Appends the **.id-[victim_ID]_maestro@pizzacrypts.info** extension to files and creates "**Pizzacrypts Info.txt**" ransom note.
120	**Pletor**	https://support.kaspersky.com/us/10556#block1	**No file extension added**	**Kaspersky**	Mostly affects Android devices, locking the screen and demanding a fine for alleged law violations.
121	**Polyglot**	https://support.kaspersky.com/8547#block1	**.oops**	**Kaspersky**	Concatenates the **.oops** string to encrypted files and leaves **_HELP_Recover_Files.html**ransom how-to
122	**Pompous**	http://www.bleepingcomputer.com/news/security/pompous-ransomware-dev-gets-defeated-by-backdoor/	**.locked**	**Bleeping Computer**	This ransomware encrypts your data using AES encryption, appends the Locked extension, and then demand .5 bitcoins to get the decryption key. There have been quite a few EDA2 ransomware variants, but what makes this story different is how this ransomware developer is such a pompous ass and that we were able to get the victim's keys back. Instead, this developer acts like a pompous jackass by bragging about how the police will never find them, what the victim did wrong, and basically going on a power trip.
123	**Powerware**	https://www.pcrisk.com/removal-guides/9922-files-encrypted-read-me-html-ransomware	**No file extension added**	**PC Risk**	PowerWare is a ransomware-type malware that encrypts various files. This ransomware is distributed via emails that contains a malicious Word document with an embedded macro. When users opens this document, the aforementioned macro runs automatically. Malicious files are then downloaded and automatically execute to encrypt stored data. Once the data is encrypted, a ransom is demanded from the victims.
124	**Popcorn Time**	https://www.elevenpaths.com/downloads/RecoverPopCorn.zip	**No file extension added**	**Eleven Paths**	"Popcorn Time" gives the victim the option of paying the ransom or infecting two other individuals and getting them to pay. The ransom note gives the victim seven days to choose either option or the files will be lost forever.
125	**Radamant**	https://decrypter.emsisoft.com/radamant	**.rdm** **.rrk**	**Emsisoft Decrypter**	Use this decrypter if your files have been encrypted and renamed to either *.rdm or *.rrk.
126	**Rakhini**	https://support.kaspersky.com/10556	**.locked** **.kraken**	**Kaspersky**	Use the special utility **RakhniDecryptor** to unlock files with the .locked and .kraken extensions. These files are encrypted by **Trojan-Ransom.Win32.Rakhni**.

127	**Rannoh**	https://support.kaspersky.com/8547#block1	**.locked-[original_filename].[random_4_chars]**	**Kaspersky**	Uses the **.locked-[original_filename].[random_4_chars]** extension and sets a desktop wallpaper containing recovery steps
128	**Rector**	https://support.kaspersky.com/4264	**No file extension added**	**Kaspersky**	Cybercriminals use **Trojan-Ransom.Win32.Rector** for disrupting normal performance of computers and for unauthorized modification of data making it unusable. Once the data has been "taken hostage" (blocked), its owner (user) receives a ransom demand. The victim is supposed to deliver the ransom in exchange for pirate's promise to send a utility that would restore the data or repair the PC. The **Trojan-Ransom.Win32.Rector** malware encrypts files with the following extensions: **.jpg, .doc, .pdf, .rar**. Then a cybercriminal nicknamed "††**KOPPEKTOP**††" offers to unblock the files and prompts to contact him.
129	**Rotor**	http://media.kaspersky.com/utilities/VirusUtilities/EN/rakhnidecryptor.zip	**!____cocoslim98@gmail.com____.tar !____glok9200@gmail.com____.tar !__recoverynow@india.com__.v8**	**Kaspersky**	Appends filenames with one of the following extensions: "**!____cocoslim98@gmail.com____.tar**", "**!____glok9200@gmail.com____.tar**", or "**!__recoverynow@india.com__.v8**", encouraging victims to negotiate the terms of decryption over email
130	**Samas** **AKA** **Kazi**	https://www.2-spyware.com/download/ReimageRepair	**.iloveworld .helpmeencedfile .whereisyourfiles .weareyourfriends .theworldisyours .encryptedyourfiles .whereisyourfiles .weencedufiles**	**www.2-spyware**	Samas locks files by applying the RSA-2048 military-grade encryption and then appends **encrypted.RSA** extension to the endings of the filenames. Later virus versions which also use some other extensions including **.iloveworld; .helpmeencedfile; .whereisyourfiles; weareyourfriends, .theworldisyours, .encryptedyourfiles** and **.whereisyourfiles** to render the victim's personal data useless. The newest, Samas 2017, version relies on **.weencedufiles** file extension. Once the files are encrypted, the malicious payload drops a ransom note called **PLEASE_READ_FOR_DECRYPT_FILES_{victim's ID}, 001-READ-FOR-DECRYPT-FILES.html** or **READ-READ-READ.html** on the victim's computer, demanding to pay the ransom in exchange for the decryption key.
131	**SamSam**	https://sensorstechforum.com/samsam-ransomware-samas-remove-decrypt-files/	**.weapologize**	**Sensor Tech Forum**	Files are encrypted with RSA encryption and become inaccessible with an added *.weapologize* file extension to them. A ransom note with instructions for paying the ransom shows as **000-SORRY-FOR-FILES.html** file.
132	**Scatter**	https://support.kaspersky.com/11333	**.pzdc .crypt .good**	**Kaspersky**	The malicious program **Trojan-Ransom.BAT.Scatter** is used by cyber criminals for unauthorised modifying the data on the victim computer so that the information becomes inaccessible.
133	**Scraper**	https://support.kaspersky.com/11718	**No file extension added**	**Kaspersky**	The malicious program **Trojan-Ransom.Win32.Scraper** encrypts user files to block access to them. After the data has been blocked, the user is required to pay a ransom.
134	**Shade**	http://www.mcafee.com/us/downloads/free-tools/shadedecrypt.aspx	**.7h9r .no_more_ransom .windows10 .xtbl .ytbl .better_call_saul .heisenberg .breaking_bad .da_vinci_code**	**Mcafee Intel**	Shade Ransomware Decryption Tool will help decrypt files with the following extensions: .xtbl, .ytbl, .breaking_bad, .heisenberg.
		https://support.kaspersky.com/13059		**Kaspersky**	Appends **.7h9r**, **.no_more_ransom**, **.windows10**, **.xtbl**,**.ytbl**, **.better_call_saul**, **.heisenberg**, **.breaking_bad**, or **.da_vinci_code** extension to encrypted files; sprinkles multiple copies of **README.txt** ransom note across the system
135	**SNSLocker**	https://www.thewindowsclub.com/trend-micro-ransomware-file-decryptor	**.RSNSLocked**	**Trend Micro**	**Trend Micro Ransomware File Decryptor** is a free Ransomware Decryptor Tool that will help you unlock files that have been locked by select ransomware.

136	**Stampado**	https://decrypter.emsisoft.com/stampado	**.locked**	**Emsisoft Decrypter**	Stampado is a ransomware kit offered within various hacking communities. Written in AutoIt, it encrypts files using AES-256 encryption and renames them to *.locked. Known variants of this ransomware ask victims to contact paytodecrypt@sigaint.org, getfiles@tutanota.com, successl@qip.ru, clesline 212@openmailbox.org or ransom64@sigaint.org to facilitate payment. In order for the decrypter to work you will require both the email you are asked to contact as well as your ID. Please keep in mind that both are case sensitive, so proper capitalization does matter. Please put both information into the appropriate fields in the options tab. Since version 1.17.0 each Stampado infection also has a unique "salt" that is specific to the ransomware buyer. The salt can either be specified manually or detected automatically. In order to determine the salt automatically the ransomware has to be running on the system. Fill in the ID and email address and click the "Detect ..." button next to the salt input field. If the malware has already been removed, please don't attempt to reinfect yourself. Instead submit the malware file via email to fw@emsisoft.com so I can extract the correct salt for you. You can also try the pre-configured salts that have been used by known Stampado campaigns in the wild so far.
		https://www.thewindowsclub.com/trend-micro-ransomware-file-decryptor		**Trend Micro**	**Trend Micro Ransomware File Decryptor** is a free Ransomware Decryptor Tool that will help you unlock files that have been locked by select ransomware.
		https://files.avast.com/files/decryptor/avast_decryptor_stampado.exe		**Avast**	Stampado is a ransomware strain written using the AutoIt script tool. It is being sold on the dark web, and new variants keep appearing. One of its versions is also called Philadelphia. Stampado adds the .locked extension to the encrypted files. Some variants also encrypt the filename itself, so the encrypted file name may look either as **document.docx.locked** or **85451F3CCCE348256B549378804965CD8564065FC3F8.locked**.
137	**Surprise**	https://sensorstechforum.com/remove-surprise-ransomware-and-restore-surprise-encrypted-files/	**No file extension added**	**Sensors Tech Forum**	Infects the user via a downloader Trojan and encrypts his/her files asking for ransom payment in Bitcoin for the decryption of the data. The user may witness his files being encrypted with the .surpise file extension plus **DECRYPTION_HOWTO.Notepad** file created on the Desktop.
138	**SZF Locker**	https://www.avg.com/en-us/ransomware-decryption-tools#szflocker	**.szf**	**AVG**	SZFLocker adds **.szf** to the end of filenames. (e.g., Thesis.doc = **Thesis.doc.szf**). When you try to open an encrypted file, SZFLocker displays the following message (in Polish): 'Plik zaszyfrowany. Usluga odzyfrowania dostepna pod adresem deszyfr@yandex.ru'
		https://files.avast.com/files/decryptor/avast_decryptor_szflocker.exe		**Avast**	SZFLocker adds **.szf** to the end of filenames. (e.g., Thesis.doc = **Thesis.doc.szf**)
139	**Teamxrat/Xpan**	https://www.thewindowsclub.com/trend-micro-ransomware-file-decryptor	**.__xratteamLucked**	**Trend Micro**	**Trend Micro Ransomware File Decryptor** is a free Ransomware Decryptor Tool that will help you unlock files that have been locked by select ransomware.
140	**Telecrypt**	https://malwarebytes.app.box.com/s/kkxwgzbpwe7oh59xqfwcz97uk0q05kp3	**.Xcri**	**Malwarebytes**	Targets Windows users, appends **.Xcri** to files or no extension at all, and displays a ransom note called "**Informer**" spelled out in Russian

141	**TeslaCrypt (v.1**, v.2**, v.3, and v.4)**	https://blogs.cisco.com/security/talos/teslacrypt	**.EEC .VVV .ABC .CCC .XYZ .ZZZ .mp3 .micro .xxx .ttt** **v.4 does NOT rename files**	**Cisco**	Cisco offers a free Decryption Tool for TeslaCrypt Ransomware Victims. This TeslaCrypt Decryption Tool is an open source command line utility for decrypting TeslaCrypt ransomware encrypted files so users' files can be returned to their original state.
		https://github.com/Googulator/TeslaCrack		**GitHub**	TeslaCrack is available on GitHub. It will help you decrypt files that were encrypted with the latest version of the TeslaCrypt ransomware.
		https://www.avg.com/en-us/ransomware-decryption-tools#teslacrypt		**AVG**	After encrypting your files, TeslaCrypt displays a variant of the following message: 'your documents, photos, databases and other important files have been encrypted! To decrypt your files follow the instructions….'
		https://www.thewindowsclub.com/trend-micro-ransomware-file-decryptor		**Trend Micro**	**Trend Micro Ransomware File Decryptor** is a free Ransomware Decryptor Tool that will help you unlock files that have been locked by select ransomware.
		http://news.thewindowsclub.com/teslacrypt-ransomware-developers-release-new-decryptor-key-84151/		**The Windows Club**	**TeslaCrypt** encrypted files can be decrypted if they have the following extensions: .mp3, .micro, .xxx, and .ttt.
142	**Thanatos**	https://github.com/Cisco-Talos/ThanatosDecryptor	**.thanatos**	**Git Hub**	ThanatosDecryptor is an executable program that attempts to decrypt certain files encrypted by the Thanatos malware
143	**TorrentLocker**	http://www.bleepingcomputer.com/forums/t/547708/torrentlocker-ransomware-cracked-and-decrypter-has-been-made/	**No file extension added**	**Bleeping Computer**	**TorrentLocker** (Trojan-Ransom.Win32.Rack in Kaspersky Lab classification) is a type of cryptographic ransomware, which is gaining increasing popularity nowadays. Trojan-Ransom.Win32.Rack uses a symmetric block cipher AES to encrypt the victim's files and an asymmetric cipher RSA to encrypt the AES key. Versions 1-3 contain a flaw which makes it possible to decrypt the victim's files. Unfortunately, starting from version four, the malware authors have identified and fixed this flaw, rendering this decryption method impossible. Current versions of this malware demand ransom payments through the Bitcoin system and host its payment webpages in the Tor network.
144	**Troldesh**	http://14.141.38.197:8765/QH/Ransom_Decryptor_v1.0.0.2.zip	**.xtbl .dharma .wallet .onion**	**Quick Heal**	The Troldesh Ransomware is a ransomware infection that was created in Russia. The Troldesh Ransomware is a new threat released in 2015. The Troldesh Ransomware is also known as Encoder.858 and Shade and has been responsible for threat attacks all around the world. The Troldesh Ransomware carries out a similar attack to most encryption threats; the Troldesh Ransomware encrypts the victim's files and then demands payment of a ransom in order to decrypt the files (hence the term 'ransomware'). The Troldesh Ransomware appends the .xtbl, .dharma, .wallet, or.onion extension to the end of all the encrypted files. The most common distribution method for the Troldesh Ransomware is through spam email messages containing infected attachments or links.
145	**Vindows**	https://malwarebytes.account.box.com/login?redirect_url	**.vindows**	**Malwarebytes**	Vindows is a worm capable of infecting legacy systems, such as **Windows** XP and 2003.
146	**Wannacry**	https://github.com/gentilkiwi/wanakiwi/releases	**No file extension added**	**Git Hub**	**WannaCry is a ransomware** cryptoworm, which targets computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency. Once infected the ransomware locks the hard drive and displays a ranom note.
147	**Wannacrypt**	https://www.thewindowsclub.com/wannacrypt-wannacry-ransomware-decryptor	**No file extension added**	**The Windows Club**	Under favorable conditions, WannaKey and WanaKiwi, two WannaCrypt decryption tools can help decrypt WannaCrypt or WannaCry Ransomware encrypted files by retrieving the encryption key used by the ransomware.
148	**Wildfire Locker**	https://support.kaspersky.com/13107	**.wflx**	**Kaspersky**	Use the WildfireDecryptor tool to decrypt .wflx files encrypted with Wildfire Locker.
		http://www.mcafee.com/us/downloads/free-tools/wildfiredecrypt.aspx		**McAfee Intel**	

149	**XData**	https://files.avast.com/files/decryptor/avast_decryptor_xdata.exe	**.~xdata~**	**Avast**	XData is a ransomware strain that was derived from AES_NI and like WannaCry, it uses the Eternal Blue exploit to spread to other machines. The ransomware adds the ".~xdata~" extension to the encrypted files. In each folder with at least one encrypted file, the file "HOW_CAN_I_DECRYPT_MY_FILES.txt" can be found. Additionally, the ransomware creates a key file with name similar to: [PC_NAME]#9C43A95AC27D3A131D3E8A95F2163088-Bravo NEW-20175267812-78.key.~xdata~
150	**XORBAT**	https://www.thewindowsclub.com/trend-micro-ransomware-file-decryptor	**.crypted**	**Trend Micro**	**Trend Micro Ransomware File Decryptor** is a free Ransomware Decryptor Tool that will help you unlock files that have been locked by select ransomware.
151	**XORIST**	https://decrypter.emsisoft.com/xorist	**.xorist random extension**	**Emsisoft Decrypter**	Use this decrypter if your files have been encrypted by the Xorist ransomware. Typical extensions used by Xorist include *.EnCiPhErEd, *.0JELvV, *.p5tkjw, *.6FKR8d, *.UslJ6m, *.n1wLp0, *.5vypSa and *.YNhlv1. The ransomnote can usually be found on the Desktop with the name "HOW TO DECRYPT FILES.txt". To use the decrypter you will require an encrypted file of at least 144 bytes in size as well as its unencrypted version. To start the decrypter select both the encrypted and unencrypted file and drag and drop them onto the decrypter executable.
		https://support.kaspersky.com/2911		**Kaspersky**	Malware of the family **Trojan-Ransom.Win32.Xorist** is designed for unauthorized modification of data on a victim computer. It makes computers uncontrollable or blocks its normal performance.
		https://www.thewindowsclub.com/trend-micro-ransomware-file-decryptor		**Trend Micro**	**Trend Micro Ransomware File Decryptor** is a free Ransomware Decryptor Tool that will help you unlock files that have been locked by select ransomware.