Lost all your files to some nasty ransomware?

We're here to fix that.

Associate Partner

Download one of our free decrypter tools to recover your files without paying the ransom

I NEED REMOVAL HELP

[Jul, 13, 2017] - Version: 1.0.0.80

Emsisoft Decrypter for NemucodAES

DOWNLOAD

32304 downloads

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. The ransom note reads as follows:

> *ATTENTION!*
> *All your documents, photos, databases and other important personal files were encrypted*
> *using a combination of strong RSA-2048 and AES-128 algorithms.*
>
> *The only way to restore your files is to buy decryptor. Please, follow these steps:*
>
> *Create your Bitcoin wallet here:*
> *https://blockchain.info/wallet/new*
> *Buy 0.13066 bitcoins here:*
> *https://localbitcoins.com/buy_bitcoins*
> *Send 0.13066 bitcoins to this address:*
> *1FeZr4bvMpCf1QTS49VjsdhtnP6zPvMjbP*
> *Open one of the following links in your browser:*
> *http://luxe-limo.ru/counter/?*
> *1FeZr4bvMpCf1QTS49VjsdhtnP6zPvMjbP*
> *http://musaler.ru/counter/?*
> *1FeZr4bvMpCf1QTS49VjsdhtnP6zPvMjbP*
> *http://vinoteka28.ru/counter/?*
> *1FeZr4bvMpCf1QTS49VjsdhtnP6zPvMjbP*
> *http://www.agrimixxshop.com/counter/?*
> *1FeZr4bvMpCf1QTS49VjsdhtnP6zPvMjbP*
> *http://sharedocsrl.it/counter/?*
> *1FeZr4bvMpCf1QTS49VjsdhtnP6zPvMjbP*
> *Download and run decryptor to restore your files.*

> *You can find this instruction in "DECRYPT" file on your desktop.*

To decrypt your files, please run the decrypter on the encrypted system. The decrypter requires various files from your %TEMP% directory of the user that spawned the infection. Therefore it is important not to reformat the system or run any cleanup tools before attempting the decryption.

→ More technical information → Detailed usage guide

[May, 30, 2017] - Version: 1.0.0.54

Emsisoft Decrypter for Amnesia2

DOWNLOAD

17336 downloads

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.

→ More technical information → Detailed usage guide

[May, 6, 2017] - Version: 1.0.0.33

DOWNLOAD

Emsisoft Decrypter for Amnesia

18490 downloads

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.

→ More technical information → Detailed usage guide

[May, 2, 2017] - Version: 1.0.0.54

Emsisoft Decrypter for Cry128

DOWNLOAD

25437 downloads

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".

→ More technical information → Detailed usage guide

[Apr, 6, 2017] - Version: 1.0.0.41

Emsisoft Decrypter for Cry9

DOWNLOAD

23672 downloads

Cry9 is the successor of the CryptON ransomware family that is mostly used for targetted 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".

→ More technical information → Detailed usage guide

[Mar, 11, 2017] - Version: 1.0.0.12

Emsisoft Decrypter for Damage

DOWNLOAD

16233 downloads

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".

[Mar, 7, 2017] - Version: 1.0.0.41

Emsisoft Decrypter for CryptON

DOWNLOAD

28718 downloads

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_".

→ More technical information → Detailed usage guide

[Jan, 12, 2017] - Version: 1.0.0.61

Emsisoft Decrypter for MRCR

DOWNLOAD

23282 downloads

MRCR or Merry X-Mas is a ransomware family that first appeared in December last year. It 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.

→ More technical information → Detailed usage guide

[Jan, 12, 2017] - Version: 1.0.0.116

Emsisoft Decrypter for Marlboro

DOWNLOAD

11919 downloads

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.

→ Detailed usage guide

[Jan, 4, 2017] - Version: 1.0.0.22

Emsisoft Decrypter for Globe3

DOWNLOAD

26872 downloads

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.

→ More technical information → Detailed usage guide

[Dec, 30, 2016] - Version: 1.0.0.34

Emsisoft Decrypter for OpenToYou

DOWNLOAD

8833 downloads

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.

→ More technical information

[Dec, 23, 2016] - Version: 1.0.0.35

Emsisoft Decrypter for GlobeImposter

DOWNLOAD

23675 downloads

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.

→ Detailed usage guide

[Nov, 29, 2016] - Version: 1.0.0.15

Emsisoft Decrypter for NMoreira

DOWNLOAD

48266 downloads

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.

→ Detailed usage guide

[Nov, 23, 2016] - Version: 1.0.0.30

Emsisoft Decrypter for OzozaLocker

DOWNLOAD

14725 downloads

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.

→ Detailed usage guide

[Oct, 8, 2016] - Version: 1.0.0.18

Emsisoft Decrypter for Globe2

DOWNLOAD

35185 downloads

Globe2 is a ransomware kit that was first discovered at the beginning of October. 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.

→ Detailed usage guide

[Oct, 1, 2016] - Version: 1.0.0.11

Emsisoft Decrypter for Globe

DOWNLOAD

29816 downloads

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.

→ More technical information → Detailed usage guide

[Sep, 28, 2016] - Version: 1.0.0.51

Emsisoft Decrypter for Al-Namrood

DOWNLOAD

13456 downloads

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.

[Sep, 18, 2016] - Version: 1.0.0.13

Emsisoft Decrypter for FenixLocker

DOWNLOAD

56376 downloads

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.

→ Detailed usage guide

[Sep, 16, 2016] - Version: 1.0.0.31

Emsisoft Decrypter for Fabiansomware

DOWNLOAD

12442 downloads

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.

→ More technical information

[Sep, 10, 2016] - Version: 1.0.0.17

Emsisoft Decrypter for Philadelphia

DOWNLOAD

17930 downloads

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.

→ Detailed usage guide

[Jul, 22, 2016] - Version: 1.0.0.205

Emsisoft Decrypter for Stampado

DOWNLOAD

24309 downloads

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, clesline212@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.

→ More technical information → Detailed usage guide

[Jun, 18, 2016] - Version: 1.0.0.34

Emsisoft Decrypter for ApocalypseVM

DOWNLOAD

21401 downloads

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.

[Jun, 12, 2016] - Version: 1.0.0.24

Emsisoft Decrypter for Apocalypse

DOWNLOAD

23664 downloads

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".

→ More technical information → Detailed usage guide

[May, 28, 2016] - Version: 1.0.0.174

Emsisoft Decrypter for BadBlock

DOWNLOAD

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.

→ More technical information

16466 downloads

[May, 17, 2016] - Version: 1.0.0.33

Emsisoft Decrypter for Xorist

DOWNLOAD

35008 downloads

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.

→ More technical information → Detailed usage guide

[May, 17, 2016] - Version: 1.0.0.29

Emsisoft Decrypter for 777

DOWNLOAD

17866 downloads

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.

[Apr, 16, 2016] - Version: 1.0.0.11

Emsisoft Decrypter for AutoLocky

DOWNLOAD

123967 downloads

Use this decrypter if your files have been encrypted and renamed to *.locky, but the file base name is still unchanged, and you find a ransom note named info.txt or info.html on your Desktop.

[Mar, 22, 2016] - Version: 1.0.0.26

Emsisoft Decrypter for Nemucod

DOWNLOAD

59581 downloads

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.

→ Detailed usage guide

[Feb, 18, 2016] - Version: 1.0.0.187

Emsisoft Decrypter for DMALocker2

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".

DOWNLOAD

13912 downloads

[Feb, 12, 2016] - Version: 1.0.0.175

Emsisoft Decrypter for HydraCrypt

Use this decrypter if your files have been encrypted and renamed to either *.hydracrypt* or *.umbrecrypt*.

→ More technical information → Detailed usage guide

DOWNLOAD

10187 downloads

[Feb, 6, 2016] - Version: 1.0.0.115

Emsisoft Decrypter for DMALocker

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".

DOWNLOAD

10281 downloads

→ More technical information → Detailed usage guide

[Jan, 30, 2016] - Version: 1.0.0.164

Emsisoft Decrypter for CrypBoss

DOWNLOAD

11986 downloads

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.

→ More technical information → Detailed usage guide

[Jan, 25, 2016] - Version: 1.0.0.172

Emsisoft Decrypter for Gomasom

DOWNLOAD

17525 downloads

Use this decrypter if files have been encrypted, renamed to *.crypt and the file name contains an email address to contact.

→ Detailed usage guide

[Jan, 25, 2016] - Version: 1.0.0.173

Emsisoft Decrypter for LeChiffre

DOWNLOAD

10889 downloads

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.

→ More technical information → Detailed usage guide

[Jan, 24, 2016] - Version: 1.0.0.112

Emsisoft Decrypter for KeyBTC

DOWNLOAD

10053 downloads

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.

→ More technical information → Detailed usage guide

[Jan, 2, 2016] - Version: 1.0.0.167

Emsisoft Decrypter for Radamant

DOWNLOAD

8750 downloads

Use this decrypter if your files have been encrypted and renamed to either *.rdm or *.rrk.

→ More technical information → Detailed usage guide

[Nov, 22, 2015] - Version: 1.0.0.149

Emsisoft Decrypter for CryptInfinite

DOWNLOAD

9033 downloads

Use this decrypter if your files have been encrypted and renamed to *.CRINF.

→ More technical information → Detailed usage guide

[Apr, 29, 2015] - Version: 1.0.0.109

Emsisoft Decrypter for PClock

DOWNLOAD

16042 downloads

Use this decrypter if your files have been encrypted without a change in file extension, the malware identifies itself as "CryptoLocker" and you find a "enc_files.txt" in your user profile directory.

→ More technical information → Detailed usage guide

[Apr, 2, 2014] - Version: 1.0.0.97

Emsisoft Decrypter for CryptoDefense

DOWNLOAD

12038 downloads

Use this decrypter if the malware identifies itself as CryptoDefense and leaves ransom notes named HOW_DECRYPT.txt behind.

→ More technical information → Detailed usage guide

[Aug, 18, 2013] - Version: 2.1.0.72

Emsisoft Decrypter for Harasom

DOWNLOAD

9610 downloads

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.

→ More technical information → Detailed usage guide

EMSISOFT

COMPANY CAREERS MEDIA RESOURCES BECOME A RESELLER AFFILIATES