Smrss32 (.encrypted) Ransomware Help & Support - _HOW_TO_Decrypt.bmp - Ransomware Help & Tech Support

By Demonslay335

Archived: 2026-04-10 02:12:51 UTC

#1 Smrss32 (.encrypted) Ransomware Help & Support - _HOW_TO_Decrypt.bmp: post #1

Demonslay335

Ransomware Hunter

- Avatar image
- Security Colleague
- 4,770 posts
- OFFLINE

- Gender:Male
- Location:USA
- Local time:08:12 PM

Posted 11 August 2016 - 07:52 PM

A new ransomware has been floating around for the past few weeks, and only now have we been able to find information on it.

Dubbed Smrss32 based on internal project settings of the malware, this ransomware encrypts files with AES and appends the extension ".encrypted" (which is also used by several other ransomwares). The ransom note "_HOW_TO_Decrypt.bmp" is dropped in every folder that is hit, and will look like the following image, asking the victim to contact the criminals at helprecover@ghostmail.com, among other email addresses.

INTRODUCTION

Data encryption involves converting and transforming data into scrambled, unreadable, cipher-text using non-readable mathematical calculations and algorithms. Restoring requires a corresponding decryption algorithm in form of software and the decryption key.

Data encryption is the process of transforming information by using some algorithm to make it unreadable to anyone except those possessing a key. In addition to the private key you need the decryption software with which you can decrypt your files and return everything to the same level as it was in the first place. **Any attempts to try restore you files with the third-party tools will be fatal for your encrypted content.**

I almost understood but what do I have to do?

The first thing you should do is to read the instructions to the end. Your files have been encrypted with the "CryptoWall" Software. The instructions, along with encrypted files are not viruses, they are you helpers. After reading this text, 99% of people turn to a search engine with the word "CryptoWall" where you'll find a lot of thoughts, advices and instructions.

Unfortunately, antivirus companies are not and will not be able to restore your files. Moreover, they make things worse by removing instructions to restore encrypted content. Antivirus companies will not be able to help decrypt your encrypted data, unless the correct software and unique decryption key is used.

Fortunately, our team is ready to help to provide instructions to decrypt your encrypted content. Keep in mind that the worse has already happened and the further life of your files directly depends on determination and speed of your actions. Therefore, we advice not to delay and follow **"HOW TO DECRYPT"** instructions.

After purchasing a software package with the unique decryption key you'll be able to:

1. **Decrypt all your files**
2. **Work with your documents**
3. **View your photos and other media content**
4. **Continue habitual and comfortable work at your computer**

If you are aware of the whole importance and criticality of the situation, then we suggest to go directly to the below **"HOW TO DECRYPT"** instructions where you will be given final simple steps, as well as guarantees to restore your files.

HOW TO DECRYPT

1. **In case if you don't already have, Register/Create a BitCoin Wallet.**
2. **Send 1.00 BTC to the following BitCoin Address:** 1Fn97Gida4ryJtPQhA8zPPMKHdedyK2cNP
3. **Register a New E-mail Account at:** www.ghostmail.com
4. **Using your New E-mail Address (From Step #3) send confirmation to the following E-mail address:** helprecover@ghostmail.com
   Mail Subject - Ref#_b4eb96984b26
   Mail Content - *"4 lines of text" Only:*
   Line 1: Ref#_b4eb96984b26
   Your Reference Number - Must match with "Mail Subject"
   Line 2: "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
   Sender/Sent from - Your BitCoin Address
   Line 3: 1Fn97Gida4ryJtPQhA8zPPMKHdedyK2cNP
   Receiver/Sent to - Our BitCoin Address
   Line 4: "1.00 BTC" - 1 Bitcoin - Service Charge
5. **After verification process (Confirmed, as Paid by our 3rd party provider) is completed, decryption software and unique key will be E-mailed to you without delays.**

* Mail Subject, other than "Ref#_xxxxxxxxxx" (Your Reference Number) will be automatically ignored by the system and will result in no reply.

* Mail Content, other than "Ref#_xxxxxxxxxx", "Sent from" (Your BitCoin Address), "Sent to" (Our BitCoin Address) and "Amount (1.00 BTC) will be automatically ignored by the system and will result in no reply.

* Any Additional/Irrelevant Subject or Additional/Irrelevant Mail Content will be automatically ignored by the system and will result in no reply.

* **DO NOT USE** any other Email Service Provider except "ghostmail.com", as explained in "Step #3". Using any other than "ghostmail.com" Email Provider will result in no reply.

Among the large wall of text, it does try to call itself "CryptoWall Software", but it is in no way nearly as sophisticated as the real thing.

Based on the way this ransomware behaves, and the project file associated with it, it is assumed this variant is spread via manual RDP hacks into a system.

I do not recommend paying the ransom at this time.

If you have been hit by this ransomware, please post 2-3 different well-known encrypted files here (e.g. .png, .doc, .docx, .xls, .xlsx, .pdf, or .zip), and we will contact you via PM with a key and decrypter.

Edited by Demonslay335, 22 August 2016 - 02:36 PM.

- Back to top

BC AdBot (Login to Remove)

- 
- BleepingComputer.com

#2 Smrss32 (.encrypted) Ransomware Help & Support - _HOW_TO_Decrypt.bmp: post #2

Amigo-A

Amigo-A

Security specialist and Ransomware expert. Volunteer Helper

- Avatar image
- Members
- 3,203 posts
- OFFLINE

- Gender:Male
- Location:Bering Strait
- Local time:07:12 AM

Posted 12 August 2016 - 04:34 AM

Smrss32 skipped files with the extension **.bmp.**

The listed of targeted extensions:

.18113 .3gp2 .3gpp .8pbs .acs2 .acsm .aifc .aiff .albm .amff .ascx .asmx .aspx .azw3 .back .backup .backupdb .bank .bdmv .blob .bndl .book .bsdl .cache .calb .cals .cctor .cdda .cdr3 .cdr4 .cdr5 .cdr6 .cdrw .ciff .class .clipflair .clpi .conf .config .contact .craw .crtr .crtx .ctor .ctuxa .d3dbsp .data .dazip .ddat .ddoc .ddrw .desc .divx .djvu .dmsk .dnax .docb .docm .docx .dotm .dotx .dsp2 .dump .encrypted .epfs .epub .exif .fh10 .flac .fmpp .forge .fsproj .gray .grey .group .gtif .gzip .h264 .hkdb .hplg .html .hvpl .ibank .icns .icxs .ilbm .im30 .incpas .indd .indt .ipsw .itc2 .itdb .ithmb .iw44 .java .jfif .jhtml .jnlp .jpeg .json .kdbx .kext .keychain .keychain .kpdx .lang .latex .lay6 .layout .ldif .litemod .log1 .log2 .log3 .log4 .log5 .log6 .log7 .log8 .log9 .m2ts .m3url .macp .maff .mcmeta .mdbackup .mddata .mdmp .menu .midi .mobi .moneywell .mp2v .mpeg .mpga .mpls .mpnt .mpqge .mpv2 .mrwref .ms11 .msmessagestore .mspx .mswmm .oeaccount .opus .otpsc .pack .pages .paint .phtml .pict .pj64 .pkpass .pntg .potm .potx .ppam .ppsm .ppsx .pptm .pptx .ppxps .psafe3 .psmdoc .pspimage .qcow2 .qdat .qzip .rels .rgss3a .rmvb .rofl .rppm .rtsp .s3db .sas7bcat .sas7bdat .sas7bndx .sas7bpgm .sas7bvew .sidd .sidn .sitx .skin .sldm .sldx .smil .sqlitedb .svg2 .svgz .targa .temp .test .text .tiff .tmpl .torrent .trace .tt10 .uns2 .urls .user .vcmf .vfs0 .view .vmdk .wallet .wbmp .webm .webp .wlmp .wotreplay .wrml .xbel .xfdl .xhtml .xlam .xlsb .xlsm .xlsx .xltm .xltx .xspf .xvid .ycbcra .ychat .yenc .zdct .zhtml .zipx .ztmp

Total: 233 extensions, the list is cleaned from duplicates is type .BACKUPDB and .backupdb and others.

If i something do not see - fix.

- Back to top

#3 Smrss32 (.encrypted) Ransomware Help & Support - _HOW_TO_Decrypt.bmp: post #3

loopbackbr

loopbackbr

- Avatar image
- Members
- 1 posts
- OFFLINE

- Local time:11:12 PM

Posted 12 August 2016 - 12:23 PM

If anybody want's additional info, the infected machine stills untouched.

- Back to top

#4 Smrss32 (.encrypted) Ransomware Help & Support - _HOW_TO_Decrypt.bmp: post #4

Grinler

Grinler

Lawrence Abrams

- Avatar image
- Admin
- 45,400 posts
- ONLINE

- Gender:Male
- Location:USA
- Local time:10:12 PM

Posted 12 August 2016 - 05:22 PM

Thanks...we are still trying to figure out a solution. Hang tight. You may want to image the drive if you need to get it up and running again.

- Back to top

#5 Smrss32 (.encrypted) Ransomware Help & Support - _HOW_TO_Decrypt.bmp: post #5

trixiebix

trixiebix

- Avatar image
- Members
- 2 posts
- OFFLINE

- Local time:10:12 PM

Posted 16 August 2016 - 09:26 AM

We had a customer get hit with this last week. Found that their local profiles still had "previous versions" (shadow copies) accessible. So we were able to recover their profiles and documents that way. Found some of the computers had smrss32.exe in the c:\encryptor folder. Some were empty. Also found a few computers that were not affected had their profiles wiped out, which was strange. They rdp'd into the servers and to any desktops they could hit.

Edited by trixiebix, 16 August 2016 - 09:47 AM.

- Back to top

#6 Smrss32 (.encrypted) Ransomware Help & Support - _HOW_TO_Decrypt.bmp: post #6

Demonslay335

Demonslay335

Ransomware Hunter

- Topic Starter

- Avatar image
- Security Colleague
- 4,770 posts

- OFFLINE

- Gender:Male
- Location:USA
- Local time:08:12 PM

Posted 16 August 2016 - 10:02 AM

If anyone has paid for a key, I would love to see it via PM please.

@trixiebix

Can you submit the smrss32.exe here so I can verify there are no modifications? http://www.bleepingcomputer.com/submit-malware.php?channel=168

Also if any files are left along with smrss32.exe in the same folder as it.

- Back to top

#7 Smrss32 (.encrypted) Ransomware Help & Support - _HOW_TO_Decrypt.bmp: post #7

0E800

0E800

- Avatar image
- Members
- 1 posts
- OFFLINE

- Gender:Male
- Local time:07:12 PM

Posted 16 August 2016 - 02:22 PM

Once on the systems, the attacker launches a web page and visits the following site to download the ransomware payload:

$USER/AppData/Roaming/Microsoft/Windows/Recent/**uyy.lnk** (was unable to get remote address)

A zip file with a random three letter filename is then dropped onto the system. The ransomware payload (smrs32.exe) is then unpacked and launched.

Note that it appears the malware is not compatible with WS2003 as only Windows 7 and WS2008 machines were encrypted with the ransomeware.

It was confirmed that the attackers did access our older servers but none of those systems were tampered with.

Best thing to do is to turn off computers when not in use, and make sure to have a password lockout policy in place.

Change the RDP port to something other than default. Do not use easy to guess passwords.

- Back to top

#8 Smrss32 (.encrypted) Ransomware Help & Support - _HOW_TO_Decrypt.bmp: post #8

Praetorians

Praetorians

- Avatar image
- Members
- 19 posts
- OFFLINE

- Local time:03:12 AM

Posted 17 August 2016 - 04:07 AM

Hello all. Since this is my first post in this forum, initially I would like to thank all the members for their invaluable input and help.

Yesterday one of our computers, a Win7 machine was infected with a ransomware resulting in all files being encrypted with ".encrypted" extension. Many of the files were backed up on an external hdd 4TB, which unfortunately was also left connected to the PC overnight. UAC was disabled on the machine and Sophos apparently wasn't able to do much. The PC had also RDP enabled default ports and weak pass... yep I know :(Thankfully when the user woke up his PC in the morning, the first thing he did was disconnecting the external hdd so not all the files were encrypted in there (too many files and many large ones like videos etc. I presume).

I'm not a very tech savvy person, so after bypassing dhe "lockscreen" through Safe Mode, I tried to identify the ransomeware through HitmanPro and Malwarebytes with not much luck. All I could find were some WinIo32.sys, winlogon.exe and conhost.exe files apparently malicious identified as Trojan.backdoors.

After that I tried to identify the threat online through ID Ransomware by uploading the text file and one encrypted file.
I got 2 results: potentially Apocalypse or Smrss32.

I tried both Emsisoft and AVG Apocalypse decryptors on the files with no success. Emsisot says "apparently the files are not encrypted", while AVG returns 0 decryptions. The text files appears to be more like the one of Apocalyspse than the Smrss32 one I see here. However I think I'm left with with Smrss32 as the only remaining option

Can anyone suggest another identification method to be certain if it is or not Smrss32? There was no c:\encrypted folder on my PC from what I see here.
Thanks in advance guys.

P.S. - At least around 7.500 files were also encrypted on the external backup HDD.

Edited by Praetorians, 17 August 2016 - 04:19 AM.

- Back to top

#9 Smrss32 (.encrypted) Ransomware Help & Support - _HOW_TO_Decrypt.bmp: post #9

quietman7

quietman7

Bleepin' Gumshoe

- Avatar image
- Global Moderator
- 65,779 posts
- OFFLINE

- Gender:Male
- Location:Virginia, USA
- Local time:10:12 PM

Posted 17 August 2016 - 05:50 AM

Praetorians, on 17 Aug 2016 - 09:07 AM, said: Quote snapback image

> ...Can anyone suggest another identification method to be certain if it is or not Smrss32? There was no c:\encrypted folder on my ...

TorrentLocker (Crypt0L0cker), Apocalypse, Crypren, Smrss32, and KeRanger OS X Ransomware all add an .encrypted extension to the end of filenames.

Smrss32 Ransomware will leave files (ransom notes) named _HOW_TO_Decrypt.bmp which advises your files have been encrypted with "CryptoWall" Software.

Apocalypse Ransomware will leave files (ransom notes) named filename.extension.encrypted.How_To_Decrypt.txt, filename.extension.encrypted.How_To_Get_Back.txt (i.e. family.jpg.encrypted.How_To_Decrypt.txt) for each file encrypted. The ransom note asks you to contact "decryptionservice@inbox.ru" or "decryptdata@inbox.ru" and contains a personal ID.

Crypren Ransomware will leave files (ransom notes) named READ_THIS_TO_DECRYPT.html.

Crypt0L0cker (TorrentLocker) will leave files (ransom notes) with names like DECRYPT_INSTRUCTIONS.TXT, DECRYPT_INSTRUCTIONS.HTML, INSTRUCCIONES_DESCIFRADO.HTML, How_To_Recover_Files.txt, How_To_Restore_Files.txt and HOW_TO_RESTORE_FILES.HTML.

KeRanger OS X Ransomware will leave files (ransom notes) named README_FOR_DECRYPT.txt.

- Back to top

#10 Smrss32 (.encrypted) Ransomware Help & Support - _HOW_TO_Decrypt.bmp: post #10

Praetorians

Praetorians

- Avatar image
- Members
- 19 posts
- OFFLINE

- Local time:03:12 AM

Posted 17 August 2016 - 05:52 AM

quietman7, on 17 Aug 2016 - 10:50 AM, said: Quote snapback image

> **Smrss32 Ransomware** leaves files (ransom notes) named _HOW_TO_Decrypt.bmp which advises your files have been encrypted with "CryptoWall" Software.
>
> **Apocalypse Ransomware** leaves files (ransom notes) named filename.extension.encrypted.How_To_Decrypt.txt, filename.extension.encrypted.How_To_Get_Back.txt (i.e. family.jpg.encrypted.How_To_Decrypt.txt) for each file encrypted. The ransom note asks you to contact "decryptionservice@inbox.ru" or "decryptdata@inbox.ru" and contains a personal ID.

Thank you very much quietman7. Than definitely it is not Smrss32 since also my bitmaps were encrypted.
I will have to move my problem to the appropriate apocalypse thread then.

Below is what the ransom note consistent with Apocalypse says:

THIS COMPUTER HAS BEEN LOCKED AND ALL THE FILES HAVE BEEN CRYPTED.

(images, videos, documents, backups, etc).

Contact by Email for data recovery.

Then, we'll provide Unlock-Password and Data Decryption Software to you.

Email: fabiansomware@mail.ru

WARNING: If you don't contact in 48 hours, then all DATA will be damaged unrecoverably!!!

Edited by Praetorians, 17 August 2016 - 05:57 AM.

- Back to top

#11 Smrss32 (.encrypted) Ransomware Help & Support - _HOW_TO_Decrypt.bmp: post #11
Demonslay335

Demonslay335

Ransomware Hunter

- Topic Starter

- Avatar image
- Security Colleague
- 4,770 posts
- OFFLINE

- Gender:Male
- Location:USA
- Local time:08:12 PM

Posted 17 August 2016 - 08:26 AM

@Praetorians

See my reply in the Apocalypse topic. You definitely have the newest Apocalypse we uncovered yesterday, which ID Ransomware will pickup on by the extension, ransom note name, and email address in the ransom note. You'll need to use the ApocalypseVM decrypter for that particular variant.

http://www.bleepingcomputer.com/forums/t/617212/apocalypse-encrypted-ransomware-help-topic-filenamehow-to-decrypttxt/?p=4065585

- Back to top

#12 Smrss32 (.encrypted) Ransomware Help & Support - _HOW_TO_Decrypt.bmp: post #12

Demonslay335

Demonslay335

Ransomware Hunter

- Topic Starter

- Avatar image
- Security Colleague
- 4,770 posts
- OFFLINE

- Gender:Male
- Location:USA
- Local time:08:12 PM

Posted 17 August 2016 - 10:10 AM

@All

If anyone has been hit by this ransomware and has not paid, please share an encrypted image or Office file (e.g., *.png.encrypted, *.jpg.encrypted, *.doc.encrypted, etc.). We will be able to provide a key and decrypter via PM. :)

- Back to top

#13 Smrss32 (.encrypted) Ransomware Help & Support - _HOW_TO_Decrypt.bmp: post #13

R2D2015

R2D2015

- Avatar image
- Members

- 6 posts
- OFFLINE

- Local time:09:12 PM

Posted 17 August 2016 - 12:51 PM

Demonslay335, on 17 Aug 2016 - 3:10 PM, said:Quote snapback image

> @All
>
> If anyone has been hit by this ransomware and has not paid, please share an encrypted image or Office file (e.g., *.png.encrypted, *.jpg.encrypted, *.doc.encrypted, etc.). We will be able to provide a key and decrypter via PM. :)

Did you get my .PNG.Encrypted files?

- Back to top

#14 Smrss32 (.encrypted) Ransomware Help & Support - _HOW_TO_Decrypt.bmp: post #14

Frakkle

Frakkle

- Avatar image
- Members
- 1 posts
- OFFLINE

- Local time:10:12 PM

Posted 17 August 2016 - 01:15 PM

Demonslay335, on 12 Aug 2016 - 12:52 AM, said:Quote snapback image

> A new ransomware has been floating around for the past few weeks, and only now have we been able to find information on it.
>
> Dubbed Smrss32 based on internal project settings of the malware, this ransomware encrypts files with AES and appends the extension ".encrypted" (which is also used by several other ransomwares). The ransom note "_HOW_TO_Decrypt.bmp" is dropped in every folder that is hit, and will look like the

> following image, asking the victim to contact the criminals at helprecover@ghostmail.com, among other email addresses.
>
> Among the large wall of text, it does try to call itself "CryptoWall Software", but it is in no way nearly as sophisticated as the real thing.
>
> Based on the way this ransomware behaves, and the project file associated with it, it is assumed this variant is spread via manual RDP hacks into a system.
>
> If you or someone you know has been hit by this ransomware, please post in this topic. We are looking to gather more information if possible, including whether files still exist in the directory "C:\encryptor" or another suspicious folder on the root of the drive.
>
> I do not recommend paying the ransom at this time.
>
> **If you have been hit by this ransomware, please post an encrypted file here, and we will contact you via PM with a key and decrypter.**

Encrypted and unencrypted version of file:

https://www.dropbox.com/sh/9erahtg50g2ak47/AACyL1dzQjnSSxxAyKFOTbtfa?dl=0

I hope you can help.

Follow-up: Machine is fully restored now. Thanks again so much, you guys are amazing.

Edited by Frakkle, 17 August 2016 - 08:30 PM.

- Back to top

#15 Smrss32 (.encrypted) Ransomware Help & Support - _HOW_TO_Decrypt.bmp: post #15

Demonslay335

Demonslay335

Ransomware Hunter

- Topic Starter

- Avatar image
- Security Colleague
- 4,770 posts
- OFFLINE

- Gender:Male

- Location:USA
- Local time:08:12 PM

Posted 17 August 2016 - 01:52 PM

@R2D2015

Thanks for the reminder, I have your files and will contact you when we have a key.

@Frakkle

I will contact you when we have a key as well.

-  Back to top

---