

Forum:[Hack Forums](#)

Thread: [Ransomware - Need help Decrypting](#)

Antec - January 29, 2017, 8:31 pm

Hey guys,

Recently I got infected with some ransomware and I need help decrypting the files that the malware has encrypted.

The file end in a .crypt

I cant seen to decrypt it using the anti-malware provided stuff they have..

I have a super important excel sheet that I need for work and it's encrypted :(

I've tried to recover using disk recovering software and still failed..

Any help is appreciated... thanks!

EDIT: It is identified as "GlobelImposter"

The thing is I don't have the original undecrypted file, i only have the encrypted one.

I've only ever saved my documents on a USB and there is only one copy of it which is on the usb.

Null - January 29, 2017, 8:32 pm

Do you know what the ransomware is called? There are some public decrypters for specific ones.

Antec - January 29, 2017, 8:39 pm

It's CryptXXX, I've tried the free programs but they're just not working :(

Lante - January 29, 2017, 8:42 pm

Can you tell exactly what free programs you tried without success?

Null - January 29, 2017, 8:45 pm

Here ya go, ->

<https://support.kaspersky.com/viruses/disinfection/8547#block1>

Follow that and let me know how it goes, then we can work from there.

Also, how did you get it in the first place?

Antec - January 29, 2017, 8:59 pm

(Jan 29, 2017 09:42 PM)Lante Wrote: [\[CITE\]](#) Can you tell exactly what free programs you tried without success?

I've tried RannohDecryptor and a few free other ones from AVG.

(Jan 29, 2017 09:45 PM)AltoSaxaphone Wrote: [\[CITE\]](#) Here ya go, ->

<https://support.kaspersky.com/viruses/disinfection/8547#block1>

Follow that and let me know how it goes, then we can work from there.

Also, how did you get it in the first place?

with Rannoh is asks me for the original file which I don't have because I save all my files directly to USB...

This is such a pain in the ass, I am tempted to pay the ransom but I don't know if it'll work or not!

*****W0lf***** - January 29, 2017, 10:17 pm

Try with this programs bro:

<https://www.bleepingcomputer.com/download/windows/ransomware-decryptors/>

Antec - January 29, 2017, 10:39 pm

(Jan 29, 2017 11:17 PM)++W0lf++ Wrote: [\[CITE\]](#) Try with this programs bro:

<https://www.bleepingcomputer.com/download/windows/ransomware-decryptors/>

Thanks man!! but none of them work :(

Apparently this is my ID:

```
C6 91 72 28 1D A8 86 15 AB 53 ED 80 28 9F 03 7A
2C 26 DD 73 44 31 39 CF 51 D0 9D 53 AF 14 37 4E
09 71 3B 05 2B 3B 78 06 FA 8F BE 7F BE 84 2E 32
DD 1A 9F EA D0 2F C3 79 1A 0F 8A BC 34 48 3E 77
E1 96 AA DB 27 59 8C BF 65 E3 68 E9 94 A3 36 EE
7A D1 92 44 F1 FA 24 21 30 43 B3 FC 89 97 EB BB
4E 48 39 2D 12 09 BE 03 91 9E C2 22 5F FE E5 E7
67 80 40 3F F3 68 CE F7 F3 76 36 3A 37 DB 7D B0
```

anyone know if this could lead anywhere??

Thanks :)

ven0m - January 29, 2017, 10:45 pm

Have you tried the tools listed in [this](#) post? Try [ID Ransomware](#) for a better identification.

Antec - January 29, 2017, 11:10 pm

(Jan 29, 2017 11:45 PM)ven0m Wrote: [\[CITE\]](#) Have you tried the tools listed in [this](#) post? Try [ID Ransomware](#) for a better identification.

Thanks for your input Ven0m!

Okay its identified as "GlobeImposter"

The thing is I don't have the unencrypted version of this excel file...

I've only ever saved it to my USB and they've encrypted that file on the USB!!

I hope there is solutions! I am willing to pay anyone to help me decrypt this file!

licker98 - January 29, 2017, 11:21 pm

Just to add variety to the thread, if the document cannot be replicated fast enough, it may be better to pay. I read that most of the cybercriminals give you the files back, but paying the ransome is pretty disheartening and the police certainly wouldn't pay Ransome over a human hostage. Now if only there was a way to send the SAS into your computer...

Reusable - January 29, 2017, 11:23 pm

<https://decrypter.emsisoft.com/globeimposter> says they can decrypt it

ven0m - January 29, 2017, 11:24 pm

(Jan 30, 2017 12:10 AM)Antec Wrote: [\[CITE\]](#) Thanks for your input Ven0m!

Okay its identified as "GlobeImposter"

The thing is I don't have the unencrypted version of this excel file...

I've only ever saved it to my USB and they've encrypted that file on the USB!!

I hope there is solutions! I am willing to pay anyone to help me decrypt this file!

Can you send me the encrypted version of the Excel file via PM? I wish to check.

GenericSkid - January 29, 2017, 11:26 pm

(Jan 29, 2017 09:42 PM)Lante Wrote: [\[CITE\]](#) Can you tell exactly what free programs you tried without success?

Could have also been jerkin it on internet explorer.

Antec - January 29, 2017, 11:38 pm

(Jan 30, 2017 12:23 AM)Reusable Wrote: [\[CITE\]](#) <https://decrypter.emsisoft.com/globeimposter> says they can decrypt it

The thing is I don't have the original. I've only ever saved it on my USB..

It states that you need the original file along with the decrypted file?

(Jan 30, 2017 12:26 AM)Lord Pankake Wrote: [\[CITE\]](#) Could have also been jerkin it on internet explorer.

I've tried so many.. but now things have changed and it's known as "GlobeImposter" when I thought it was "CryptXXX"

(Jan 30, 2017 12:24 AM)ven0m Wrote: [\[CITE\]](#) Can you send me the encrypted version of the Excel file via PM? I wish to check.

Sending it now. Thank you!

Reusable - January 30, 2017, 2:21 am

it states that you need AN original file and a crypted one not the exact one meaning any of the encrypted files and any original file doesnt have to be that exact crypted file. pick another you have a backup of....

they just need to break the encryption.

Anubis - January 30, 2017, 2:27 am

<https://www.nomoreransom.org>

See if they can help you.

If not, you're fucked.

And there is no chance you can decrypt that by yourself.

Such encryptions tend to be really st•rong.

Also I've found these as well....

<https://decrypter.emsisoft.com/globeimposter>

https://decrypter.emsisoft.com/howtos/emsisoft_howto_globeimposter.pdf

And you've got a plenty of tools here..

<https://www.nomoreransom.org/decryption-tools.html>

WeedLover94 - January 30, 2017, 2:43 am

If you don't mind me asking op, what was the message they left? If you search on google for the exact message, or just parts of the message:

Example -

Gib us 100btc pls sir i reall need it to pay for brazzers subscripton send to
s8df09s8df0we'regay9809s8df09s8df address

Type in "Gib us 100btc pls sir" or their BTC address- with the quotes for a specific search term - into google and find other people with your same problem; if you're lucky, someone may have resolved the problem with the same variant. Also you don't need to give them a specific file, just the backup of ANY file that has been encrypted. Another chance you could have if the malware is just a Hidden-Tear variant (it was backdoored, and there is a public decrypter)

Antec - January 30, 2017, 3:20 am

(Jan 30, 2017 03:21 AM)Reusable Wrote: [\[CITE\]](#) it states that you need AN original file and a crypted one not the exact one meaning any of the encrypted files and any original file doesnt have to be that exact crypted file. pick another you have a backup of....

they just need to break the encryption.
Thank you, I will have a look tomorrow.

Thank you all for your help and suggestions!

Wafflemonger - January 30, 2017, 3:31 am

Not sure if this was said as I didn't read all the posts, but it requires an original and an encrypted file. It doesn't matter whether it's the Excel file that you're looking for or a random file that you have backed up.

Anyways, I've heard of a lot of people doing that recently. They don't have any way to perform an off-drive backup, so they keep a PDF or something of that nature backed up on a USB as well as the original on the C drive in the root directory. If they ever get hit by ransomware, the odds of them recovering without paying increase greatly. Not sure if it makes any sense to do so or not, I personally don't. But then again, I'm a firm believer of, "if you care about it enough, you have backups."

EDIT: Looked at the tools pretty sure they try to do collision attacks on it. If that's the case and you have a slow computer ... that will take a while.

Kisame? - January 30, 2017, 12:12 pm

Sucks that it happened to you man.

I might be repeating others, considering I haven't had the time to read the entire thread and all its comments.

The chance of successfully decrypting your files depends on the encryption method and whether there is a decryption tool available for the specific ransomware.

The only things you can do is finding out the kind of ransom that hit you (you said CryptXXX, but keep in mind many ransoms have a lot of modified versions as well, so a tool which decrypted the original ransom encryption might not work depending on which one hit you).

Like the guy above me said as well, you can maybe learn the key if you have a back-up of some original files before they were encrypted. Check your dropbox, google account (google drive), sent email-attachments, your work/school computers, etc. etc.

If it's a good coded ransomware, the chances of just cracking the algorithm and decrypting your files are very low as far as I know, considering there are very strong and almost uncrackable encryption methods nowadays. In the worst case, you might want to pay them and just be done with it, if it is worth your files of course. If you are thinking about doing that, make sure to find out first whether they actually give you the decryption code after payment (by researching other cases). Some ransoms don't even give the decryption key after you've paid them, and that'd be really, really sad.

I hope you can decrypt it, and otherwise I hope you'll not have a lot of trouble with it anymore. The software is kind of retarded to be honest, it's so simple but yet so effective if it is just a decently programmed one...

At least you now know the risks when downloading files, I guess.

Good luck!

s?hane - January 30, 2017, 12:15 pm

How did you even get infected?

Saint - January 30, 2017, 12:27 pm

(Jan 30, 2017 01:15 PM) Shane Wrote: [\[CITE\]](#) How did you even get infected?

Would also like to know,

And maybe a simple idea but have you tried setting your pc back a few days?

Worked for others i've heard with that FBI ransomware.

Might work for you.

Antec - January 30, 2017, 1:38 pm

(Jan 30, 2017 04:31 AM) Wafflemonger Wrote: [\[CITE\]](#) Not sure if this was said as I didn't read all the posts, but it requires an original and an encrypted file. It doesn't matter whether it's the Excel file that you're looking for or a random file that you have backed up.

Anyways, I've heard of a lot of people doing that recently. They don't have any way to perform an off-drive backup, so they keep a PDF or something of that nature backed up on a USB as well as the original on the C drive in the root directory. If they ever get hit by ransomware, the odds of them recovering without paying increase greatly. Not sure if it makes any sense to do so or not, I personally don't. But then again, I'm a firm believer of, "if you care about it enough, you have backups."

EDIT: Looked at the tools pretty sure they try to do collision attacks on it. If that's the case and

you have a slow computer ... that will take a while.

Thank you, I will have a look at other original files I might have on the computer. I know it was silly of me, I always thought it was safe to store it on my USB. oh well, lesson learnt!

(Jan 30, 2017 01:12 PM)David? ?Gilmour Wrote: [\[CITE\]](#) Sucks that it happened to you man. I might be repeating others, considering I haven't had the time to read the entire thread and all its comments.

The chance of successfully decrypting your files depends on the encryption method and whether there is a decryption tool available for the specific ransomware.

The only things you can do is finding out the kind of ransom that hit you (you said CryptXXX, but keep in mind many ransoms have a lot of modified versions as well, so a tool which decrypted the original ransom encryption might not work depending on which one hit you).

Like the guy above me said as well, you can maybe learn the key if you have a back-up of some original files before they were encrypted. Check your dropbox, google account (google drive), sent email-attachments, your work/school computers, etc. etc.

If it's a good coded ransomware, the chances of just cracking the algorithm and decrypting your files are very low as far as I know, considering there are very strong and almost uncrackable encryption methods nowadays. In the worst case, you might want to pay them and just be done with it, if it is worth your files of course. If you are thinking about doing that, make sure to find out first whether they actually give you the decryption code after payment (by researching other cases). Some ransoms don't even give the decryption key after you've paid them, and that'd be really, really sad.

I hope you can decrypt it, and otherwise I hope you'll not have a lot of trouble with it anymore. The software is kind of retarded to be honest, it's so simple but yet so effective if it is just a decently programmed one...

At least you now know the risks when downloading files, I guess.

Good luck!

Going to see if I can find originals today :) I will update everyone on this thread!

(Jan 30, 2017 01:27 PM).Saint Wrote: [\[CITE\]](#) Would also like to know,

And maybe a simple idea but have you tried setting your pc back a few days?

Worked for others i've heard with that FBI ransomware.

Might work for you.

PRETTTTTTY sure I got infected through email. I must have accidentally clicked something in spam, but the last time I remember was a customer sending in a complaint, could be that but I am unsure.

I use a server and one day came in and everything looked basic, figured something was wrong.

Managed to restore everything the way it was back a couple of days ago.

Have 3 hard drives for backups and now they're all encrypted -.-

My mistake, and I've learnt a cold hard lesson from this.

Saint - January 30, 2017, 3:22 pm

(Jan 30, 2017 02:38 PM)Antec Wrote: [CITE](#) Thank you, I will have a look at other original files I might have on the computer. I know it was silly of me, I always thought it was safe to store it on my USB. oh well, lesson learnt!

Going to see if I can find originals today :) I will update everyone on this thread!

PRETTTTTTY sure I got infected through email. I must have accidentally clicked something in spam, but the last time I remember was a customer sending in a complaint, could be that but I am unsure.

I use a server and one day came in and everything looked basic, figured something was wrong.

Managed to restore everything the way it was back a couple of days ago.

Have 3 hard drives for backups and now they're all encrypted -.-

My mistake, and I've learnt a cold hard lesson from this.
Well damn, replying so hopefully someone can come with a solution.

sv1cdr - February 15, 2017, 11:54 am

pay the ransom? :) sorry i have no other ideas seemed this guy knows what hes doing

Tankian - February 15, 2017, 1:08 pm

wow , sorry for ya bro , good luck