

Forum:[Hack Forums](#)

Thread: [Success with removing ransomware?](#)

OneHalf - August 27, 2018, 5:28 pm

So I have a client I'm going to see tomorrow, I do free lancing work in my town for just a few people. He owns a chiropractic office, and got hit with ransomware.

Here's what they're getting

Spoiler [\(Click to View\)](#)

Spoiler [\(Click to View\)](#)

Now I know there are services now through sites like bitdefender, Mccafe, kasperky, etc. But my question is, it looks like everything on the computer is useless, so I don't think I'll be able to test anything on the PC.

I know if the PC is <=windows 7 I can do an autorun file from a USB, and try that way. But, if I can't get a program to run to test the ransomware or open any files to test them, do I have any other options? Kind of stumped here.

Neverwill - August 27, 2018, 5:54 pm

(Aug 27, 2018 05:28 PM)OneHalf Wrote: [\[CITE\]](#) So I have a client I'm going to see tomorrow, I do free lancing work in my town for just a few people. He owns a chiropractic office, and got hit with ransomware.

Now I know there are services now through sites like bitdefender, Mccafe, kasperky, etc. But my question is, it looks like everything on the computer is useless, so I don't think I'll be able to test anything on the PC.

I know if the PC is <=windows 7 I can do an autorun file from a USB, and try that way. But, if I can't get a program to run to test the ransomware or open any files to test them, do I have any other options? Kind of stumped here.

Do you still get the ransomware popup in Safemode?

From my experience, first step is trying to get into Safemode, secondly, if you can't remove the infection via Safemode, System Restore and then try.

OneHalf - August 27, 2018, 5:56 pm

(Aug 27, 2018 05:54 PM)Neverwill Wrote: [\[CITE\]](#) Do you still get the ransomware popup in Safemode?

From my experience, first step is trying to get into Safemode, secondly, if you can't remove the infection via Safemode, System Restore and then try.

I haven't actually been in the office yet, I'm going in tomorrow, this just happened a couple hours

ago. The problem is, it's a chiropractic office, so all the patient files will be lost. Their external HDD was affected as well, and they don't use cloud backup (going to recommend this tomorrow). Also, I'm sure it's spread to their network, so I had them disconnect all internet in hopes of stopping spreading /:

Tr1Ck_ - August 27, 2018, 5:57 pm

Unless you can boot into safe mode with command prompt and perform a system restore, I am afraid that there is not a lot that you can do once your files have been encrypted.

OneHalf - August 27, 2018, 5:58 pm

(Aug 27, 2018 05:57 PM)Tr1Ck_ Wrote: [\[CITE\]](#) Unless you can boot into safe mode with command prompt and perform a system restore, I am afraid that there is not a lot that you can do once your files have been encrypted.

So do you think the programs for decryption made by McAfee and Kaspersky don't work if I can verify the type of Ransomware?

Zexture - August 27, 2018, 5:59 pm

This ransomware is called Ransom.Crysis try googling for a removal

OneHalf - August 27, 2018, 6:00 pm

(Aug 27, 2018 05:59 PM)Zexture Wrote: [\[CITE\]](#) This ransomware is called Ransom.Crysis try googling for a removal

Thank you for figuring that out for me! Did you know just from the picture, or did you do a reverse image search? I did one, and saw that as well, but wanted to take it with a grain of salt until I saw it.

Tr1Ck_ - August 27, 2018, 6:03 pm

Thanks to Zexture and an unknown developer on a forum, removal is apparently possible:

2-spyware.com/remove-crysis-ransomware-virus.html Wrote: Please, do not try to remove CrySiS ransomware manually. It's a complex cyber threat that makes numerous changes to the system and might inject malicious code into legit system processes. Therefore, you should rely on reputable security software and let it remove this cyber threat without causing more damage to the system.

For CrySiS removal we recommend using Reimage or Plumbytes Anti-Malware. However, there might appear obstacles which hinder successful elimination. But our team of experts has prepared instructions which should help you tame the virus and initiate the full system scan. Please check them below.

But before you do run the scan, make sure that your antivirus and malware removal utilities are updated to their latest version. Otherwise, the software may not be able to detect and delete CrySiS from your system, so the virus will continue rampaging on your computer.

Please update us with results, my friend.

Good luck!

Neverwill - August 27, 2018, 6:04 pm

(Aug 27, 2018 06:00 PM)OneHalf Wrote: [\[CITE\]](#) Thank you for figuring that out for me! Did you know just from the picture, or did you do a reverse image search? I did one, and saw that as well, but wanted to take it with a grain of salt until I saw it.

There is a good article on Bleeping Computer regarding this ransomware... There is a slight chance of recovery, otherwise they're gonna lose everything.

Google Search: New Arena Crysis Ransomware Variant Released

It's the BleepingComputer link.

Zexture - August 27, 2018, 6:06 pm

(Aug 27, 2018 06:00 PM)OneHalf Wrote: [\[CITE\]](#) Thank you for figuring that out for me! Did you know just from the picture, or did you do a reverse image search? I did one, and saw that as well, but wanted to take it with a grain of salt until I saw it.

I have reverse searched the image but I believe to a high degree that this is crysis since many google search on the name gave a similar image to yours

OneHalf - August 27, 2018, 6:10 pm

Thank you all so much! I will return tomorrow afternoon with my results! I think I'm going to try the antimalware scan and then followed with the decryptor from Zexture!

Aura - August 27, 2018, 6:12 pm

Upload an encrypted file or ransom note to ID-Ransomware to get an accurate ID of the variant.

<https://id-ransomware.malwarehunterteam.com/>

OneHalf - August 27, 2018, 6:17 pm

Seriously thank you all so much! I will def. update this thread tomorrow after my visit!

gei123 - September 2, 2018, 5:44 pm

PreInstall your pc lol :D

ACCOUNT - September 3, 2018, 6:45 am

(Aug 27, 2018 06:12 PM)Aur? Wrote: [\[CITE\]](#) Upload an encrypted file or ransom note to ID-Ransomware to get an accurate ID of the variant.

<https://id-ransomware.malwarehunterteam.com/>

This was really helpful, thank you. Saved to later.