

Forum:[Hack Forums](#)

Thread: [Infected with Cryptolocker 3](#)

Forezza - June 28, 2015, 9:32 pm

Hey guys,

Nope, I wasn't the smart cookie who got infected, but this is a thread asking for a second option about it. My friend works for a small organisation who was recently infected as one of their staff decided to open resume.exe and it cryptolocked their network drives. They do have backups, however they only backup once every 3 days and the backup was due tonight (they got infected like 4 hours before the backup). They have important files that are worth in excess of the \$500 that it asks for 10 fold.

They're considering paying for it as they cant really lose these important files. What do you think they should do? I understand the cryptography behind Cryptolockers and how they work.

Niko - June 28, 2015, 9:54 pm

Depending on the version, or if it isn't necessarily the original cryptolocker, There may be a few options, I wouldn't recommend removing it yet.

- 1) Shadow Copies. If there are any, that may work.
- 2) Flaw In the malware. If there is a flaw in the malware, it may be able to be reverse engineered.
- 3) Decryption. You may not have any luck here, but depending on the encryption used, it may be decrypted.

Try Number 1, if that is not an option, do they still have the original executable?

Forezza - June 28, 2015, 10:00 pm

They've apparently already looked into #1 and #2 is unlikely as it looks like it's the original cryptolocker 3.0. Decryption isn't going to happen as the files are encrypted with an RSA 2048-bit key. That's not going to be decrypted in the next 10,000 years.

Null Byte - June 28, 2015, 10:04 pm

There is no way to bypass CL3, it's completely rocksolid. Your only two options are restoring from backup or paying the ransom. It's up to you.

How many computer are infected and how much \$ is it asking for?

Armada - June 28, 2015, 10:07 pm

(Jun 28, 2015 10:04 PM)Null Byte Wrote: [\[CITE\]](#) There is no way to bypass CL3, it's completely rocksolid. Your only two options are restoring from backup or paying the ransom. It's up to you.

How many computer are infected and how much \$ is it asking for?

Sadly, if it is in fact the original Crypto Locker 3, you are out of luck. There is no known flaw in the system. ?

ProtectNull™ - June 28, 2015, 10:11 pm

How many computers are infected bro?

Forezza - June 28, 2015, 10:14 pm

There is the option of compromising the VPS in which the decryption site resides on (the muppets are on some random VPS host connected to a hotmail account), however it's not really my place to do this. I will probably just suggest they pay the ransom.

It was a single computer that was infected, however the computers are all connected to the companies network drives. The cryptolocker software has encrypted every file on the company servers where all of the important stuff resides. Sadly it bypassed all of the virus protection that was in place as well. It's asking for \$500, but there is no guarantee that the key will even be given.

Null Byte - June 28, 2015, 10:21 pm

(Jun 28, 2015 10:14 PM)Forezza Wrote: [\[CITE\]](#) There is the option of compromising the VPS in which the decryption site resides on (the muppets are on some random VPS host connected to a hotmail account), however it's not really my place to do this. I will probably just suggest they pay the ransom.

It was a single computer that was infected, however the computers are all connected to the companies network drives. The cryptolocker software has encrypted every file on the company servers where all of the important stuff resides. Sadly it bypassed all of the virus protection that was in place as well. It's asking for \$500, but there is no guarantee that the key will even be given.

If your company will lose more than they spend to unlock those files, I advise against it.

That being said CL has a very good reputation of unlocking encrypted files. You'll probably get them back if you pay.

ProtectNull™ - June 28, 2015, 10:22 pm

(Jun 28, 2015 10:14 PM)Forezza Wrote: [\[CITE\]](#) There is the option of compromising the VPS in which the decryption site resides on (the muppets are on some random VPS host connected to a hotmail account), however it's not really my place to do this. I will probably just suggest they pay the ransom.

It was a single computer that was infected, however the computers are all connected to the companies network drives. The cryptolocker software has encrypted every file on the company servers where all of the important stuff resides. Sadly it bypassed all of the virus protection that was in place as well. It's asking for \$500, but there is no guarantee that the key will even be given.

That is correct, there is no guarantee that the key will be given.

If I were you, just goto the old backup OR

Make a backup with the ransom with CAUTION. And when there is a fix for it, then you can remove the ransom.

Paul Wilson - June 29, 2015, 12:26 am

What exactly was on these files?

If it's important client info, it might be possible to cover up the accident and ask for another copy of the information due to "HD failure"

The problem with all ransomware is that by making the payment, you are giving money to organized criminal gangs, who use said money for things like sex trafficking, drugs, extortion, etc...

Forezza - June 29, 2015, 2:50 am

(Jun 29, 2015 12:26 AM)MishaTheHoovy Wrote: [\[CITE\]](#) What exactly was on these files?

If it's important client info, it might be possible to cover up the accident and ask for another copy of

the information due to "HD failure"

The problem with all ransomware is that by making the payment, you are giving money to organized criminal gangs, who use said money for things like sex trafficking, drugs, extortion, etc...

As far as I know, the data in question is 25 hours of 6 different employees work. Restarting that would put them back way over \$500 USD. Some data may not even be recoverable.

I was looking through the chain of bitcoin addresses these guys have and they are making thousands a day.

LogoiLab - June 29, 2015, 2:28 pm

<http://www.makeuseof.com/tag/cryptolocker-dead-heres-can-get-files-back/>

5chn4pp - June 29, 2015, 2:38 pm

(Jun 29, 2015 02:28 PM)PentestingForever Wrote: [\[CITE\]](#)

<http://www.makeuseof.com/tag/cryptolocker-dead-heres-can-get-files-back/>

and are you sure this works for cryptolocker 3? I dont think so.

LogoiLab - June 29, 2015, 2:57 pm

The versioning is an issue as it's actually different authors stealing each other's ideas but my hopes is that the security companies with this tool have updated their key databases recently

Knautschtabak - June 30, 2015, 5:23 am

(Jun 28, 2015 09:32 PM)Forezza Wrote: [\[CITE\]](#) Hey guys,

Nope, I wasn't the smart cookie who got infected, but this is a thread asking for a second option about it. My friend works for a small organisation who was recently infected as one of their staff decided to open resume.exe and it cryptolocked their network drives. They do have backups, however they only backup once every 3 days and the backup was due tonight (they got infected like 4 hours before the backup). They have important files that are worth in excess of the \$500 that it asks for 10 fold.

They're considering paying for it as they cant really lose these important files. What do you think they should do? I understand the cryptography behind Cryptolockers and how they work.

Cryptolocker is dead. The infection on this system must be a different one. And the very first thing to do to is to identify the actual infection.

Some ransoms are known to claim they are cryptolocker. These are e.g. Torrentlocker and PClock.

But often people just say cryptolocker when they mean any file encrypting ransomware.

Get some more information like ransomnotes, extensions of encrypted files etc. Then we can go from that to identification and possibilities of decryption.