

Forum:[Hack Forums](#)

Thread: [Decrypting a file \(ransomware\)](#)

cryptzoo - June 23, 2016, 9:21 pm

Hey there (noob here),

So recently my work place got attacked by a ransomware called CERBER. After trying out all the options (using all the free available decryptors), I bought the decryptor from the ransomware attacker. However, it is unable to find the private key to decrypt the encrypted files.

So here is my question, I have an encrypted file and its original file. I also have the public key. Is there any way I can crack the encryption? I need the private key to open other encrypted file who's original files are missing with no backups.

Note: I tried panda decryption tool, which was able to decrypt few files, but apparently, the encryption file changes its private key after a while. So I could not decrypt all my files.

Any help is appreciated :)
Cheers!

TouchMyMalware - June 24, 2016, 1:12 am

I doubt there is any way you can crack it. Either they used block level RSA or AES. I know some ransoms use the Win32 Crypto API to generate the keypair. And they forget to set the flag which only stores the key in memory but not in file. So chances are, the private key under those specific conditions is on your machine in your crypto folders. You will just need to import it to the CSP. Then call CryptDecrypt.

iLogic™ - June 24, 2016, 1:13 am

Hello.

It is possible to decrypt but it will take a lot of time (depending on hardware). Can you tell me what kind of encryption algorithm is it?

cryptzoo - June 24, 2016, 1:59 am

(Jun 24, 2016 01:13 AM)iLogic™ Wrote: [\[CITE\]](#) Hello.

It is possible to decrypt but it will take a lot of time (depending on hardware). Can you tell me what kind of encryption algorithm is it?

Hey, from my research, Cerber uses RSA 1024 public key using RC4 algorithm.

Silly Putty - June 24, 2016, 2:10 am

I've sent you a pm regarding

cryptzoo - June 24, 2016, 5:21 am

(Jun 24, 2016 02:10 AM)Silly Putty Wrote: [\[CITE\]](#) I've sent you a pm regarding

^^this guy just stole my money

Bandors Jr. - June 24, 2016, 5:46 am

There is no way you are going to decrypt the files, your best bet is to go to the link they tell you to when you are infected and use your one free decrypt wisely on your most important file and then go ahead and try and restore your system

CyberGuard - June 24, 2016, 9:18 am

(Jun 24, 2016 05:21 AM)cryptzoo Wrote: [\[CITE\]](#) ^^this guy just stole my money
create a scam report about it with proof

BEKFEST - June 24, 2016, 9:56 am

(Jun 24, 2016 05:21 AM)cryptzoo Wrote: [\[CITE\]](#) ^^this guy just stole my money
I really hope he didn't that'd be a scumbag thing to do to someone in your situation, make a scam
report as CyberGuard said.

gabkwong2 - June 24, 2016, 9:49 pm

You are pulling up a dick move by doing that.