nakedsecurity
Award-winning news, opinion, advice and research from SOPHOS

CryptoLocker Ransomware - See how it works and learn about prevention, cleanup and recovery

October 2013 - This article explains how the CryptoLocker ransomware works, including a short video showing it in action. The article tells you about prevention, cleanup, and recovery. It also explains how to improve your security against this sort of threat in future.

CRYPTOLOCKER - WHAT IS IT?

CryptoLocker, detected by Sophos as **Troj/Ransom-ACP**, is a malicious program known as ransomware.

Some ransomware just freezes your computer and asks you to pay a fee. (These threats can usually be unlocked without paying up, using a decent anti-virus program as a recovery tool.)

CryptoLocker is different: your computer and software keep on working, but your personal files, such as documents, spreadsheets and images, are encrypted.

The criminals retain the only copy of the decryption key on their server - it is not saved on your computer, so you cannot unlock your files without their assistance.

They then give you a short time (e.g. 72 hours, or three days) to pay them for the key.

The decryption key is unique to your computer, so you can't just take someone else's key to unscramble your files.

The fee is $300 or EUR300, paid by MoneyPak; or BTC2 (two Bitcoins, currently about $280).

To understand how CryptoLocker goes about its dirty work, please see our step-by-step description.

WHAT DOES CRYPTOLOCKER LOOK LIKE?

CryptoLocker reveals itself only after it has scrambled your files, which it does only if it is online and has already identified you and your computer to the encryption server run by the criminals.

We therefore recommend that you don't try the malware out yourself, even if you have a sample and a computer you don't care about, because you can't easily test it without letting your computer converse with the crooks.

However, we know you would love to see what it does and how it works, so here is a video made by our friend and colleague Mark Rickus, of Sophos Support.

We recommend this video because Mark has pitched it perfectly: he doesn't rush; he doesn't talk down to you; he lets the facts speak for themselves; and he brings an air of calm authority with just a touch of wry humour to what is a rather serious subject:

VIDEO DEMONSTRATION: https://www.youtube.com/watch?v=Gz2kmmsMpMI

HOW DO I DETECT AND REMOVE IT?

You can use the free Sophos Virus Removal Tool (VRT). This program isn't a replacement for your existing security software, because it doesn't provide active protection (also known as on-access or real-time scanning), but that means it can co-exist with any active software you already have installed. The Virus Removal Tool will load, update itself, and scan memory, in case you have malware that is already active.
Once it has checked for running malware, and got rid of it, then it scans your hard disk.

If it finds any malicious files, you can click a button to clean them up.

If CryptoLocker is running and has already popped up its payment demand page, you can still remove it and clean up, but the Virus Removal Tool cannot decrypt your scrambled files - the contents are unrecoverable without the key, so you may as well delete them.

Even if you don't have CryptoLocker, it is well worth scanning your computer for malware.

The criminals are known to be using existing malware infections as "backdoors" to copy CryptoLocker onto victims' computers.

We assume their reasoning is that if you have existing, older malware that you haven't spotted yet, you probably won't spot CryptoLocker either, and you probably won't have backup - and that means they're more likely to be able to squeeze you for money later on.

CAN CRYPTOLOCKER SPREAD ON MY NETWORK?

Fortunately, CryptoLocker is not a virus (self-replicating malware), so it doesn't spread across your network by itself.

But it can affect your network, because it searches extensively for files to encrypt.

Remember that malware generally runs with the same permissions and powers as any program you choose to launch deliberately.

So, any file, on any drive letter or network share, that you can locate and access with a program such as Windows Explorer can be located and accessed by CryptoLocker.

That includes USB drives, network file shares, and even cloud storage folders that are made to appear as a drive letters by special software drivers.

A Naked Security reader just commented that from a single infected computer, he was "faced with 14,786 encrypted files over local and mapped network drives."

So, if you haven't reviewed the security settings on your network shares lately, this would be a good time to do so.

If you don't need write access, make files and folders read only.

SHOULD I PAY UP?

We'll follow the police's advice here, and recommend that you do not pay up. This sort of extortion - Demanding Money with Menaces, as a court would call it - is a serious crime.
Even though CryptoLocker uses payment methods (MoneyPak, Bitcoin) that keep you and the crooks at arm's length, you are dealing with outright criminals here.

Of course, since we don't have 14,786 encrypted files, like the reader we mentioned above, we acknowledge that it may be easier for us to say, "Don't pay" than it is for you to give up on your data.

Obviously, we can't advise you on how likely it is that you will get your data back if you do decide to pay.

IS IT THE WORST VIRUS EVER?

We don't think so, although that is cold comfort to those who have lost data this time round.

Losing files completely is a terrible blow, but you can lose data in lots of other ways: a dropped hard disk, a stolen laptop or just plain old electronic failure.

The silver lining with CryptoLocker is that the criminals don't actually take your data - they just leave it locked up where it was before, and offer to sell you the key.

In many ways, malware that isn't so obvious and aggressive, but which steals your files, or monitors your keyboard while you login to your bank, or takes snapshots of your screen while you're filling out your tax return, can be much worse.

In those cases, the crooks end up with their own duplicate copies of your data, passwords and digital identity.

If you have a recent backup, you can recover from CryptoLocker with almost no consequences except the time lost restoring your files.

Identity theft, however, can be a lot harder to recover from - not least because you have to realise that it's even happened before you can react.

Even if all you have on your computer is zombie malware of the sort that crooks use to send spam, doing nothing about it hurts everyone around you, and imposes a collective cost on all of us.

That's why we are urging you to DO THESE 3 security steps, and TRY THESE 4 free tools, even if you haven't been hit by CryptoLocker.

HOW DO I ENSURE THERE'S NO "NEXT TIME?"

Here are five "top tips" for keeping safe against malware in general and cyberblackmailers in particular:

- **Keep regular backups of your important files**. If you can, store your backups offline, for example in a safe-deposit box, where they can't be affected in the event of an attack on your active files. Your backups will be rendered useless if they are scrambled by CryptoLocker along with the primary copies of the files.
- **Use an anti-virus, and keep it up to date.** As far as we can see, many of the current victims of CryptoLocker were already infected with malware that they could have removed some time ago, thus preventing not only the CryptoLocker attack, but also any of the damage done by that earlier malware.
- **Keep your operating system and software up to date with patches.** This lessens the chance of malware sneaking onto your computer unnoticed through security holes. The CryptoLocker authors didn't need to use fancy intrusion techniques in their malware because they used other malware that had already broken in to open the door for them.
- **Review the access control settings on any network shares you have**, whether at home or at work. Don't grant yourself or anyone else write access to files that you only need to read. Don't grant yourself any access at all to files that you don't need to see - that stops malware seeing and stealing them, too.
- **Don't give administrative privileges to your user accounts.** Privileged accounts can "reach out" much further and more destructively both on your own hard disk and across the network. Malware that runs as administrator can do much more damage, and be much harder to get rid of, than malware running as a regular user.

Article posted at: http://nakedsecurity.sophos.com/2013/10/18/CryptoLocker-ransomware-see-how-it-works-learn-about-prevention-cleanup-and-recovery/