How to fight CryptoLocker and evade its Ransomware demands

Don't feel like paying $300 for access to your own files? Here's how to ward off one of the nastiest viruses in recent memory.

Lauren Orsini Author - November 08, 2013

So you're happily working on your Windows computer, getting stuff done. Little do you know, your personal files are rapidly being encrypted so that you can't access them. Suddenly, an alert appears on the screen—you have 96 hours (or four days) to pay $300 or lose all your encrypted personal files forever. A countdown is already ticking on your screen.

This is CryptoLocker, the latest and most damaging Windows virus in a series of recent ransomware Trojans. The relatively large amount of money it demands, combined with the tight deadline, make it far more aggressive than other similar viruses. And unfortunately for us, it's spreading more rapidly than any of its contemporaries.

You'd think it would be simple to track down the perpetrators given that they're taking a ransom, but it's not that simple. Since CryptoLocker demands payment through MoneyPak or Bitcoin, both of which harness private, decentralized fund-exchange networks, it's much more difficult to follow the money.

Until the good guys are able to track down the bad, the best thing you can do is stay informed. I spoke to Corey Nachreiner, director of security strategy at Watchguard Security, about what you need to know.

Preventing an Infection

Nachreiner said that CryptoLocker is especially dangerous because of its infection rate. "I can tell you anecdotally, we've seen many client and customer queries for it," he said. "I haven't seen this amount of customer based questions in quite a long time."

According to the US Computer Emergency Readiness Team, it spreads through an email that appears to be a tracking notification from UPS or FedEx, though some victims said they got infected on the tail end of wiping out a previous botnet infection. And in case it wasn't clear, you don't need to be in the US to become infected.

Nachreiner said that it's more than opening the email that spreads the virus. You need to open the email and actually download the zip file inside it. Hiding inside that zip file is a double-extension file such as *.pdf.exe. The .exe file lets CryptoLocker run on your computer, while the innocuous .pdf extension hides the file's true function.

While it's hard to imagine savvy computer users falling for such a ploy, Nachreiner said this time of year makes us all more fallible. There's a reason CryptoLocker first surfaced in September 2013, and not earlier in the year.

"This lure is far more common for the holiday shopping season," he said. "As people are doing more shopping online, they'll be more likely not to suspect emails about packages. My guess is we'll also see CryptoLocker mimicking emails from Amazon and other shopping sites, too."

So far the virus has been infecting PCs running Windows 7, Vista, or XP, but Nachreiner said that doesn't mean it won't eventually infect PCs running Windows 8, or even Macs.

So what should you do? Run your antivirus software, though Nachreiner warns that it's "not a silver bullet." Make sure you keep regular and recent backups of all your files. This goes double if you're a business that shares a drive or folder across multiple computers, since CryptoLocker is known to target shared files for encryption first.

Eradicating an Infection

It's all well and good to prepare, but what if you already are infected? Despite the virus's warning not to "disconnect from the Internet or turn off the computer," this is exactly the first order of damage control.

"You've got to realize these guys are criminals and they lie," said Nachreiner. "The only thing turning off your computer does is keep the virus from continuing to infect."

In fact, unplugging your computer may save some of your files, if the virus is still in the process of infecting them.

Next, you need to figure out what damage has been done. Which files have you lost? Do you have backups of these files? If you don't have backups, have you checked Windows' System Restore files, which sometimes automatically back up the computer for you?

If you can help it, Nachreiner highly recommends not giving in to extortion.

"You should never pay these guys ransom," he said. "It's just going to encourage malware authors to create similar viruses."

If you do have a backup, it's time to wipe your computer of the virus. Fortunately for you, said Nachreiner, just about every antivirus vendor has a CryptoLocker cleanup tool. Work with your regular antivirus software, or follow a tutorial. Nachreiner suggests the FAQ at Bleeping Computer, which he links in his own blog post.

Restore your backup, and you should be set. Just don't click on any more dodgy emails.

Does Paying Ransom Work?

Say that for whatever reason you don't have a backup and do want to pay the ransom. The criminals behind CryptoLocker make it very easy to do.

"Even if you haven't made your payment before the deadline, they'll still let you pay. Only this time, instead of 2 BTC ($300), it'll be 20 BTC," Nachreiner said.

Since victims have reported that paying the ransom does work, this is your best hope for getting the encrypted files back. There's no way to track the criminals through the decentralized currency they're accepting payment through, and their encryption methods are simply too strong to unlock without a decryption key.

"Whether these guys will be caught is not a sure deal," said Nachreiner. "And whether they still have all the private keys when they're caught is not a sure deal, either. Cracking these encryptions is not something that's going to happen in the near future, even if we do catch them."

With no way to prevent CryptoLocker in sight, the most imporant thing, said Nachreiner, is to make sure people know about the virus before they get infected.

“Awareness is the first step,” he said. “Make sure your employees, or your family, know this virus is out there.”

A message from First Choice Computers (West Midlands) Ltd.

Do not open attachments from recipients that you don’t recognise. And remember HMRC, Amazon, British Banks and many other named institutions do not send email attachments. Spread the word!

To outwit these crooks; you must have an effective backup strategy (USB Pendrive, External Storage device, CD/RW, any backup would do. For a full automated backup procedure. *Call FCC on 01902 712166 or visit:*

www.fcc-online.co.uk