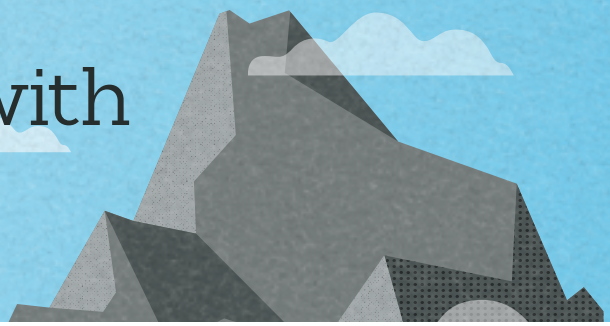
Fast-thinking admin thwarts crypto attack with Carbonite Safe Backup



"I'm familiar with how crypto viruses work and there's really only two ways to get your files back: either restore from backup or pay the ransom."

— **Chad Mockensturm,** Diverse Technology Solutions

An Ohio-based systems administrator's quick thinking and fast action saved a healthcare facility from certain disaster when a crypto virus attack threatened to wipe out hundreds of important digital files and the server on which they reside.

Chad Mockensturm is an assistant systems administrator with Diverse Technology Solutions, a Carbonite Partner. An important part of his job is to monitor and maintain the IT systems of one of Diverse Technology's customers, an Ohio-based healthcare facility. Mockensturm was doing just that one evening when he received a dire warning.

"We have an enterprise console that alerts us to any major problems and I got a text message on my phone that a virus was repeatedly being blocked on one of the nursing station computers," he said. "We later found out that one of the nurses had gone online to check messages and received a crypto virus through email."

When the nurse clicked the executable file, the crypto virus found its way from the nursing station computer to the healthcare facility's file server and began compromising important files. Mockensturm learned that the nurse had received a digital ransom note threatening to destroy the healthcare facility's files unless $500 was paid.

"I immediately shut the computer down and proceeded to scan the file server for any infections related to the virus. We found that there were 200-300 files that were infected," Mockensturm explained. "We scanned the rest of the network as a precaution and then used our Carbonite Safe™ Backup account to restore good clean copies of the files that were infected."

Case Study

Fast-thinking admin thwarts crypto attack with Carbonite Safe Backup

What is a crypto virus?

There are several different crypto-style viruses with various names, but the key thing to remember is that they are all forms of ransomware.

Ransomware is any virus that infects a computer, encrypts files and threatens to render them useless unless the victim pays money for a key code that decrypts the information. Crypto viruses such as CryptoLocker – one of the most infamous examples – typically demand ransom in the form of bitcoins, digital currency that is difficult to trace. Some well-known crypto variants include CryptoWall, TorrentLocker and CryptoDefense.

The best way to stay clear of a crypto infection is to use caution when clicking on links inside of emails, according to Mockensturm. Emails containing links to crypto executable files can be very convincing and may even seem like they're coming from familiar places.

"Know who your email is coming from," he said. "Even if it's coming from a person you think you know, be cautious when you're opening the email."

But even the most vigilant can be duped from time to time. That's why it's also important to create backups of home computers and business servers.

"It's always good to have a backup and the best backup is one that you don't have to think about because it runs in the background and it runs seamlessly," Mockensturm explained. "Carbonite is a great choice."

Fight back against a crypto attack in five steps

When a crypto virus attacks, Carbonite Safe Backup users can retrieve their files quickly without paying the ransom. Here's a quick guide to getting your files back following a crypto attack:

1. As soon as you're aware of the crypto attack on a computer, file server or network, immediately shut down all file sharing activity.
2. Use your antivirus software to determine where the infection happened. If you can't determine where the infection originated using antivirus software, right click on an infected file to find out the last user or computer to make changes to the file. This will tell you where the infection originated.
3. Assess the extent of the infection and the extent of the damage.
4. Remove the virus by deleting all infected files.
5. Use Carbonite Safe Backup to recover clean versions of the infected files.

Case Study

Fast-thinking admin thwarts crypto attack with Carbonite Safe Backup

Quickly restore files with Carbonite Safe Backup

Diverse Technology Solutions has been using Carbonite to protect many of its clients' database and file servers for years. But the incident at the healthcare facility was the first time the company used Carbonite Safe Backup to restore files infected by a crypto virus.

To get the job done, Mockensturm simply logged into the healthcare facility's file server. He then did a quick search for the root folder that contained all of the subfolders and files that needed to be recovered.

"I restored the folders to a separate part of the hard drive, deleted the original ones that were encrypted from the virus and then copied the new ones back," he explained. "Then I made sure that any programs linking to those files were able to work again."

The process was simple, painless and quick. Mockensturm was able to restore clean copies of the infected files in about a half hour.

"You just go in and select the 'restore' task, choose the files that you want to restore, and wait for them to download," he said. "It was all really easy."

Learn more about becoming a Carbonite Partner today.

Visit Carbonite.com.