



Case Study:

Quick reaction time and a dedicated, knowledgeable, team cracked the CryptoLocker virus code and restore new client's data with zero downtime.

The CryptoLocker Virus was no match for the Epoch team.

Challenge:

On June 13th, 2016 we met with our soon to be clients and they signed a three-year contract. The nature of their business would keep them very busy over the Independence Day holiday. In an effort to ensure there were no disruptions to service over their busiest time we scheduled an onboarding date of July 8th.

The first step in Epoch's onboarding process is to lock down a new client's security. Unfortunately for this client, about a week before they were to be onboarded they were infected with the CryptoLocker ransomware. On June 16th just as they were gearing up for their busy holiday season the CryptoLocker virus locked down their system and was holding their data for ransom.

What is CryptoLocker?

The CryptoLocker virus is malicious software which, once it's penetrated your computer, begins encrypting files and holding them for ransom. After encrypting your files, the hacker sends you a message demanding payment to restore your files or to prevent them from destroying your information. Once infected you generally have two options, pay up or restore to your most recent backup. Unfortunately, the CryptoLocker virus generally goes after backups as well, encrypting the data and rendering your backup useless. With ransomware like this time is of the essence! The faster you detect and stop them from gaining more access the faster you can get your business back to normal.

Results:

The contract was signed but due to the client not being onboarded Epoch had no tools in place to detect the ransomware at its initial stages. Since we were unaware of the quality or depth of the clients prior backup procedures we were blind entering the scene. Epoch's team went to work as soon as they received the clients distress call. Our team was able to crack the CryptoLocker code and unencrypt certain client files. Luckily, the client's backups were in ok shape, allowing the team to quickly restore the client to working order. Epoch's team removed and recovered the data all remotely without disrupting the client, getting them back up and running with no business downtime.

“ It certainly caught me by surprise to have a potentially crippling virus show up only days after deciding to contract with Epoch for IT support. Although you guys had not started the on-board process, I was amazed at the efficiency that you were able to remotely identify, address, and resolve our issue before we experienced any downtime. Kudo's to you. Thanks for your diligence.”

- New Client Business Owner