Documents & Design, LLC.
PHONE 605.232.4170
WEB www.d2worldwide.com
ADDRESS P.O. Box 644, North Sioux City, SD 57049

CryptoLocker aka the Ransom Virus

Tony Olson, November 2013

Malware is malicious software. All forms of malware are on the rise these days. Over the past month, our region has been under attack by a Trojan virus called CryptoLocker. It is a ransom virus. It is installed on your system by criminals.

Ransomware is a particularly insidious category of malware that can infect your system. CryptoLocker is a new variant of ransomware that is very damaging. It encrypts files that are important to you, such as pictures, songs, documents, etc. and demands money from you to restore your files to their normal, usable form. It is infecting both consumers and businesses.

CryptoLocker

The first notice that you receive that your system has been attacked, is a ransom note. It will be in the form of a pop up on your screen. The note demands a significant amount of money, and gives you 72 hours to pay, or your files will be lost forever. You will feel fear as you notice a timer counting down in the pop-up window. What will you do?

Hype or Hurt

This threat is real. Last week, the United States Computer Emergency Readiness Team (US-CERT) issued Alert (TA 13-309A). At D2 we received numerous calls from people that have been infected. They had trouble. Using our system monitors, we also have been able to see this virus trying, unsuccessfully, to infect some of our existing customers. Fortunately, they remained safe and secure.

Extent of Potential Damage

The US-CERT Alert states that this virus has the ability to find and encrypt files, not only on the main infected system, but on attached Flash drives, external hard drives, network attached storage and even mapped network drives. The form of encryption they are using is quite secure. Given the 3-day limit it will be very difficult for business, and probably impossible for individuals, to crack this code. Once the time limit is up without payment, the key is thrown away and the files are lost for good.

Prevention is the Best Approach

First, before you are attacked, back up your files. Ensure that you have, and are following, a sound backup and archival procedure. Second, ensure that you are using a professional anti-virus program and that all aspects of it are up-to-date. Do not click on unsolicited web links in email messages, or submit any information to webpages. Also, don't open attachments from unknown sources. CryptoLocker has been distributed through emails that mimic the look of those from legitimate businesses. Some of these include LinkedIn resume attachments, and FedEx and UPS tracking notices.

Recovery

If you believe that your system has become infected, quickly disconnect it from the network (both wired and wireless). If there are files that were not backed up, try to save them. If you already have backed up your files, D2 recommends that you perform a complete format and reload of your system to ensure removal of the virus. The US-CERT discourages people from paying the extortion money. Instead, US-CERT recommends reporting the crime to the FBI.