PO Box 1494, Whittier, CA 90609
www.istechsupport.com
www.evoerp.com

la habra tech

Cryptolocker Info Sheet

Prepared by La Habra Tech

1 Ransomware

Cryptolocker is a type of malicious software commonly known as *ransomware* that will restrict your computer in some way and then demand a ransom payment. There are also other pieces of ransomware that mimic Cryptolocker's functionality. When your computer becomes infected with this type of ransomware, it will begin encrypting files based on the file extensions (e.g., `.exe` or `.doc`). The malware will then inform you that it has encrypted your files and demand a payment before providing the decryption key to you.

IS Tech Support has received several support requests per month over the past few months that have turned out to be some variant of ransomware necessitating the restoration of backup files. This is a real threat, not a theoretical exercise. The most important message of this paper is to *make backups* and know how to restore them. The targeted files include many common file types that could be disastrous if lost.

1.1 Cryptolocker's Encryption

Cryptolocker and its variants use a method of encryption known as RSA. This type of encryption allows the malware to connect to a server and have it generate an encryption key that is kept secret while using a different but related key to actually perform the encryption of the files on your computer. The key used to encrypt your files can't be used to decrypt them. This encryption is extremely strong and it is effectively impossible for you to recover any data that has been encrypted by the malware except by recovering from a backup created before the malware's encryption.

1.2 Affected Files

Cryptolocker targets file extensions it believes will hold information that is important to you. Microsoft Office extensions such as `.docx` or `.xlsx` are common targets. Fortunately, Cryptolocker is not currently known to target the files that store company data for Evo or DBA systems. It will target some files used to store information such as user menus and Evo will not function properly until these files have been recovered. IS Tech Support can recover default files that will allow Evo to function properly again, but customized user menus will need to be replaced manually.

The Evo and DBA files known to be targeted by cryptolocker and its variants are files with `.DBF` extensions which include Evo-ERP menu files, data dictionary, and lookup grid files. These `.DBF` files are paired with files of the same name and the `.MDX` and sometimes `.DBT` extensions. They are located both in the main application folder (DBAMFG or EVOERP) and the DRILL subfolder.

If you are a victim of Cryptolocker malware, you need to restore these files from a backup in matched sets (`.DBF`, `.MDX`, and if it exists `.DBT`). These files are not modified daily so if the backup is a few days old you can safely restore them. However, if you have loaded a system update (version number change update, not just patches downloaded from SM-V) these files do change with updates so you cannot restore from a backup made prior to loading the update. If you do not have a backup, all of the affected files are something we can provide to get you running again but you will need to redefine your user menus. If your daily backup is only backing up the company data subfolders, we recommend a periodic backup of `*.DBF`, `*.DBT`, and `*.MDX` from the root folder and DRILL subfolder.

2 Protecting Yourself

Although the affected files are on your server, the server itself may *not* be infected. Cryptolocker can run across a network to any shared drives so only one workstation must be infected to endanger all of the files on the servers that station has access to.

The most important way to protect against such ransomware is to backup your data. However, be careful when using real-time cloud synchronization services. As soon as the file is encrypted it will be backed up overwriting the good version. Ensure your service provider also stores previous versions of files so that you can recover the version before the encryption. A good policy is to create a zip archive of the entire application folder and then back up the archive daily when no users are using the system.

2.1 Spread of Cryptolocker

Cryptolocker is most commonly spread via phishing emails. A phishing email is an email that will try to convince the recipient to open an attachment or visit a malicious website by pretending to be an authentic email. Modern phishing attacks have become very sophisticated. A variant known as spear-phishing uses some information known or guessed about potential victims to appear authentic. For example, some recent phishing emails will look like a UPS or FedEx shipment email. If you are expecting a delivery, you are more likely to read the email. If you are not expecting a delivery, you will likely become concerned and read it anyway assuming that someone has used your identity to order some product.

It is important for all employees to understand the best practices to take when reading email.

1. Verify the sender of the email. It is possible to spoof a sender's name so be very careful that the sender is who you are expecting.

   However, sometimes even verifying the sender is not enough. If the sender of the email has already been compromised, the malicious software may have used their email account to send itself to you. If the email doesn't look like it was written by that sender, be wary.

2. Are you expecting this email? If an email is not expected, be extra careful. If it states there is some problem with an online account claiming the account will be closed unless action is taken, it would be best to contact that service's customer support or go login to the account manually instead of going where ever the email wants you to go.

3. Never click on a web link in an email. It is possible to make the text of a link appear as if it is directing you to a different web site than you expect. For example, try clicking the following link: http://www.google.com.

   If you need to visit a web link in an email, first mouse over the link. Your email client should show the actual web address to which the link is connected. If the address matches the address you are expecting, it is safe to click the link. To be completely sure, it is best to type the address in to your browser manually to ensure that you are going to the web site you are expecting.

4. Never open an attachment directly from an email without verifying it. If you are expecting an attachment in the email, first check that the attached file is the type of file you are expecting. By default, Microsoft Windows hides file extensions. If you see a file named `Important.pdf` but you have file extensions hidden, then it may *not* be a PDF file. Phishing emails often use this trick. They will send something like `Important.pdf.exe` and use the Adobe Acrobat icon on the file to make you believe it is a pdf but it is actually an executable program file that will install the malware. It is best to enable showing file extensions for all files.

There are other ways to acquire the malware such as a vulnerability in a web site that delivers content through tools like Flash Player and Java. It is best to have these tools set to "ask to activate" when visiting web sites instead of having them activate automatically. This prevents automatically installing the malware when you accidentally visit a malicious site. As an example, Adobe's Flash Player was recently found to have a severe vulnerability that has since been patched. It is importatnt to ensure that you are using the latest version so that you are not exposed to the vulnerability.

LA HABRA TECH provides computer, network, and cybersecurity services for homes and small businesses.

contact@lahabratech.com