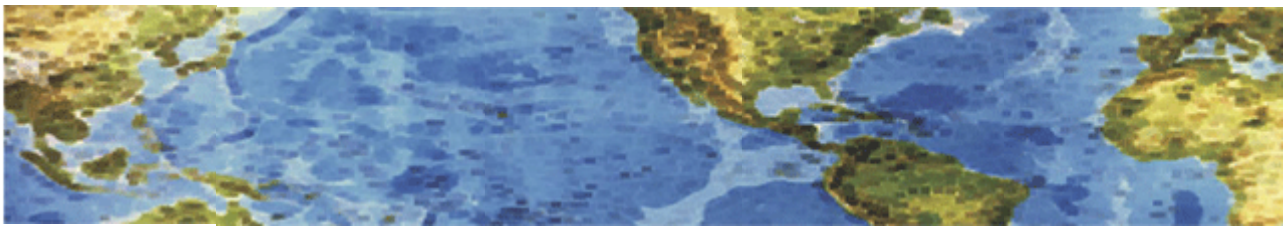
# HALL ASSOCIATES



# Risk-Based Decision Making Commentary
# 29 Oct 2013 Newsletter

## CryptoLocker: A Vicious Virus

Online attackers are using encryption to lock up our files and demand a ransom — and AV software probably won't protect you. Since this can hit anyone, please pass this information along to friends, family, and business associates.

This is a new threat to our data that we need to take seriously. I**t's already hit many consumers and small businesses.** Called CryptoLocker, this infection shows up in two ways. First, you see a red banner (Figure 1) on your computer system, warning that your files are now encrypted — and if you send money to a given email address, access to your files will be restored to you.


The other sign you've been hit: you can no longer open Office files, database files, and most other common documents on your system. When you try to do so, you get another warning, such as "Excel cannot open the file [filename] because the file format or file extension is not valid". This virus finds and encrypts all files you have access to — including those located on any attached drives or mapped network drives.

Cryptolocker comes in the door through social engineering. There are typically three ways you can receive the virus:

1) **Via an email attachment.** For example, you receive an email from a shipping company you do business with. **Attached to the email is a .zip file.** The phishing message could be purporting to be from a business copier like Xerox that is delivering a PDF of a scanned image, from a major delivery service like UPS or FedEx offering tracking information or a bank letter confirming a wire or money transfer.

2) **You browse a malicious website** that exploits vulnerabilities in an out-of-date version of Java.


# HALL ASSOCIATES

3) Most recently, **you're tricked into downloading a malicious video driver or codec file**.

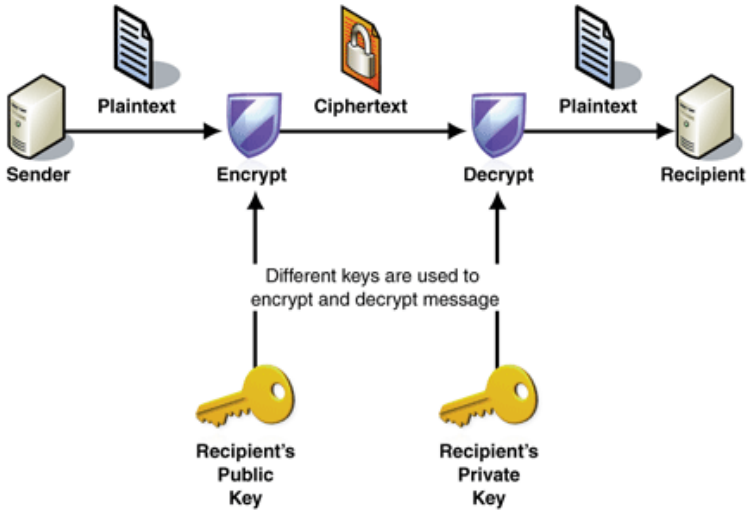
The virus is an executable attachment, but interestingly the icon representing the executable is a PDF file. With Windows' hidden extensions feature, the sender simply adds ".pdf" to the end of the file (Windows hides the .exe) and the unwitting user is fooled into thinking the attachment is a harmless PDF file from a trusted sender. It is, of course, anything but harmless. Once Cryptolocker is in the door, it targets files with the following extensions:
*.odt, *.ods, *.odp, *.odm, *.odc, *.odb, *.doc, *.docx, *.docm, *.wps, *.xls, *.xlsx, *.xlsm, *.xlsb, *.xlk, *.ppt, *.pptx, *.pptm, *.mdb, *.accdb, *.pst, *.dwg, *.dxf, *.dxg, *.wpd, *.rtf, *.wb2, *.mdf, *.dbf, *.psd, *.pdd, *.pdf, *.eps, *.ai, *.indd, *.cdr, *.jpg, *.jpe, img_*.jpg, *.dng, *.3fr, *.arw, *.srf, *.sr2, *.bay, *.crw, *.cr2, *.dcr, *.kdc, *.erf, *.mef, *.mrw, *.nef, *.nrw, *.orf, *.raf, *.raw, *.rwl, *.rw2, *.r3d, *.ptx, *.pef, *.srw, *.x3f, *.der, *.cer, *.crt, *.pem, *.pfx, *.p12, *.p7b, *.p7c

When it finds a file matching that extension, it encrypts the file using a public key and then makes a record of the file in the Windows registry under HKEY_CURRENT_USER\Software\CryptoLocker\Files. It then prompts the user that his or her files have been encrypted and that he or she must use prepaid cards or Bitcoin to send hundreds of dollars to the author of the virus. Once the payment has been made, the decryption usually begins. There is typically a four-day time limit on the payment option; the malware's author claims the private key required to decrypt files will be deleted if the ransom is not received in time. If the private key is deleted, your files will essentially never be able to be decrypted -- you could attempt to brute force the key, but as a practical matter, that would take on the order of thousands of years. Effectively, your files are gone.

There are no patches to undo CryptoLocker and, as yet, there's no clean-up tool — the only sure way to get your files back is to restore them from a backup. Some users have paid the ransom and, surprisingly, were given the keys to their data. This is, obviously, a risky option. But if it's the only way you might get your data restored, use a prepaid debit card — not your personal credit card. You don't want to add the insult of identity theft to the injury of data loss.

**In this case, your best defense is prevention.** Keep in mind that antivirus software **probably won't prevent a CryptoLocker infection**. In every case so far, the PC owner had an up-to-date AV application installed. Moreover, running Windows without admin rights does not stop or limit this virus. It uses social engineering techniques — and a good bit of fear, uncertainty, and doubt — to trick users into clicking a malicious download or opening a bogus attachment. There are several ways to prevent this from hitting you. The discussion below is only the basic method. For additional information on an advanced method and other options, such as application whitelisting, check out the articles noted at the end of this newsletter.

# HALL ASSOCIATES




**The basic prevention method is to ensure you keep complete and recent backups of your system.** Making an image backup once or twice a year isn't much protection. Given the size of today's hard drives on standalone PCs, an external USB hard drive is still your best backup option. A 1TB drive is relatively cheap. For multiple PCs on a single local-area network, there are both local backup options as well as cloud storage (which brings other security problems into the mix). Small businesses with networked PCs should have automated workstation backups enabled, in addition to server backups.

Once again, keeping your antivirus software up-to-date is not the panacea for CryptoLocker. The hackers using this exploit are adapting the virus so quickly that AV vendors can't keep up with the many CryptoLocker variations in play. **It's up to individual users to stay vigilant about what they click**. The bad guys just keep getting badder.

To see additional information on the advanced and stronger protection methods, as well as more information on Cryptolocker, check out the following articles:

http://windowssecrets.com/top-story/cryptolocker-a-particularly-pernicious-virus/

http://www.computerworld.com/s/article/9243537/Cryptolocker_How_to_avoid_getting_infected_and_what_to_do_if_you_are_

http://www.ibtimes.com/cryptolocker-virus-new-malware-holds-computers-ransom-demands-300-within-100-hours-threatens-encrypt

http://blog.malwarebytes.org/intelligence/2013/10/cryptolocker-ransomware-what-you-need-to-know/

http://www.theregister.co.uk/2013/10/18/cryptolocker_ransmware/