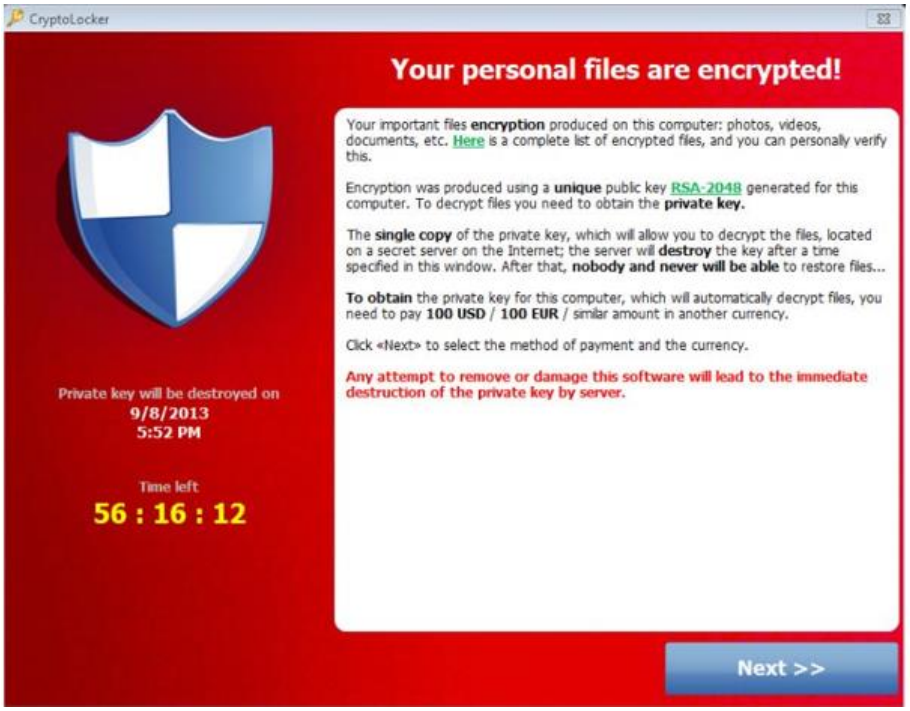
CryptoLocker – Newest “Hostageware”

Pay $300 within 100 hours or your hard drive will be encrypted forever!

There’s a new and the **most dangerous “Ransomware” virus** ever to roar its ugly presence that locks (encrypts) your hard drive files and demands payment. This **IS NOT** just another iteration virus where a decent virus removal company can resolve.

This is a valid threat **“They DID ENCRYPT you hard drive files!**

Crypto Locker (deemed “Crilock by Microsoft) – At first glance looks like a legit encryption program but this is malicious software that encrypts the user’s files and then demands the user ***pay $300 in Bitcoins*** or risk having all the files on the computer cryptographically locked forever, currently making it impossible of ever accessing them again! The most aggravating is the intimation factor the author added to this threat is the constant countdown clock ticking down the minutes being displayed on the victim’s screen.



Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **100 USD** / **100 EUR** / similar amount in another currency.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
9/8/2013
5:52 PM

Time left
56 : 16 : 12

Okay so how does this virus gain access to one’s computer? Have you received one of those phony FedEx or UPS tracking notifications? That's just one way they're spreading this virus. Another way is unsuspecting users seek out file encrypting programs to download over the Internet and find CryptoLocker which is designed to look like they're from legitimate company. Once activated, CryptoLocker installs itself into the “Documents and Settings” folder, then scans the hard drive and encrypts certain file types, including documents associated with Microsoft Word and Adobe Photoshop. CryptoLocker then launches a pop-up window with the 100-hour countdown and provides details on how to pay the ransom and they will decrypt you files.

Here is the list of file extensions encrypted by this virus as of the writing of this article:

```
*.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,
```

*.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.

It even detects and encrypts/locks files on networked/shared drives and computers. MSN Group is aware of two **ENTIRE NETWORKS** of a California company and a Georgia company had all of its computers infected. If your computers operate on a domain or LAN environment be very vigilant as one computer infected can quickly spread throughout your network. As of this writing, we have not discover this infecting across a WAN (Multi-site) environment.

AVG, Bit Defender, Kaspersky, MacAfee, Symantec, and other top Internet security companies successfully developed the script to remove the virus, but unfortunately have yet to find a way to decrypt the victim's computer hard drive.

The GOOD NEWS (if you can label it as such). These crooks are somewhat honest (?) up to date, if you pay the ransom, Crypto Locker hackers will provide the key to decrypt your files. So far there have been no reports of reinfection after the ransom had been paid!

Precautions: *Instead of an ounce of prevention, use a pound!*

ALWAYS USE and keep your virus protection up to date!

BACKUP your data regularly on an external drive that is not normally connected to your computer or network

Users should remain cautious about their online security, double-check links received in emails and social media messages by verifying their legitimacy via a phone call. Make sure the source is a reliable one!

For network/internet infected computers **IMMEDIATELY DISSCONNECT** from the environment. This will help reduce the number of files from being encrypted because the virus needs to connect to a remote server to enable/continue the encryption process.

Should you suspect or see any suspicious activity – PLEASE contact MSN Group Remote support at 800-460-9280 Option 3, live chat, Online Remote Support, or via email at support@msngroup.com

Read more…

http://www.ibtimes.com/cryptolocker-virus-new-malware-holds-computers-ransom-demands-300-within-100-hours-threatens-encrypt?ft=61pb1

A new malware spreading around the Internet in recent months holds every file on a computer for ransom. Unless the user pays $300 in Bitcoins to the hacker responsible for the infection within 100 hours, the hacker threatens to forever deny the user access to his or her files.

The malware, which is known as CryptoLocker, is not just an empty threat. If the hacker's demands aren't met, the computer files get cryptographically locked, *.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, *.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 A ticking clock showing the time limit makes CryptoLocker just a bit more terrifying.

CryptoLocker is spread through phony emails designed to look like they're from legitimate businesses and fake FedEx and UPS tracking notifications. Once opened, CryptoLocker installs itself in the "Documents and Settings" folder, scans the hard drive and encrypts certain file types, including documents associated with Microsoft Word and Adobe Photoshop. CryptoLocker then launches a pop-up window with the 100-hour countdown and provides details on how to pay the ransom.

Related

- 44% Of Andriod Users Are Vulnerable To Attacks: Report
- Android Malware Surging In 2013

Even advanced software security companies don't really have ways to restore the locked hard drive. Catching the hackers behind CryptoLocker may be the only way to retrieve the files.

The hackers are covering their tracks by using Bitcoins, a digital currency designed to be as anonymous as cash. Payments are made with a Green Dot MoneyPak, a reloadable debit card.

There is a growing trend in this type of malware, known as “ransomware,” but CrytpoLocker is the most dangerous one to pop up so far. Normally the threats are empty or the malware does something completely fixable, such as freezing the computer.

The good news is that paying the ransom does actually decrypt the files, and the hackers behind CryptoLocker so far have been honest and not reinfected computers after the ransom is paid.

Unfortunately, there is currently no way for us to decrypt those files