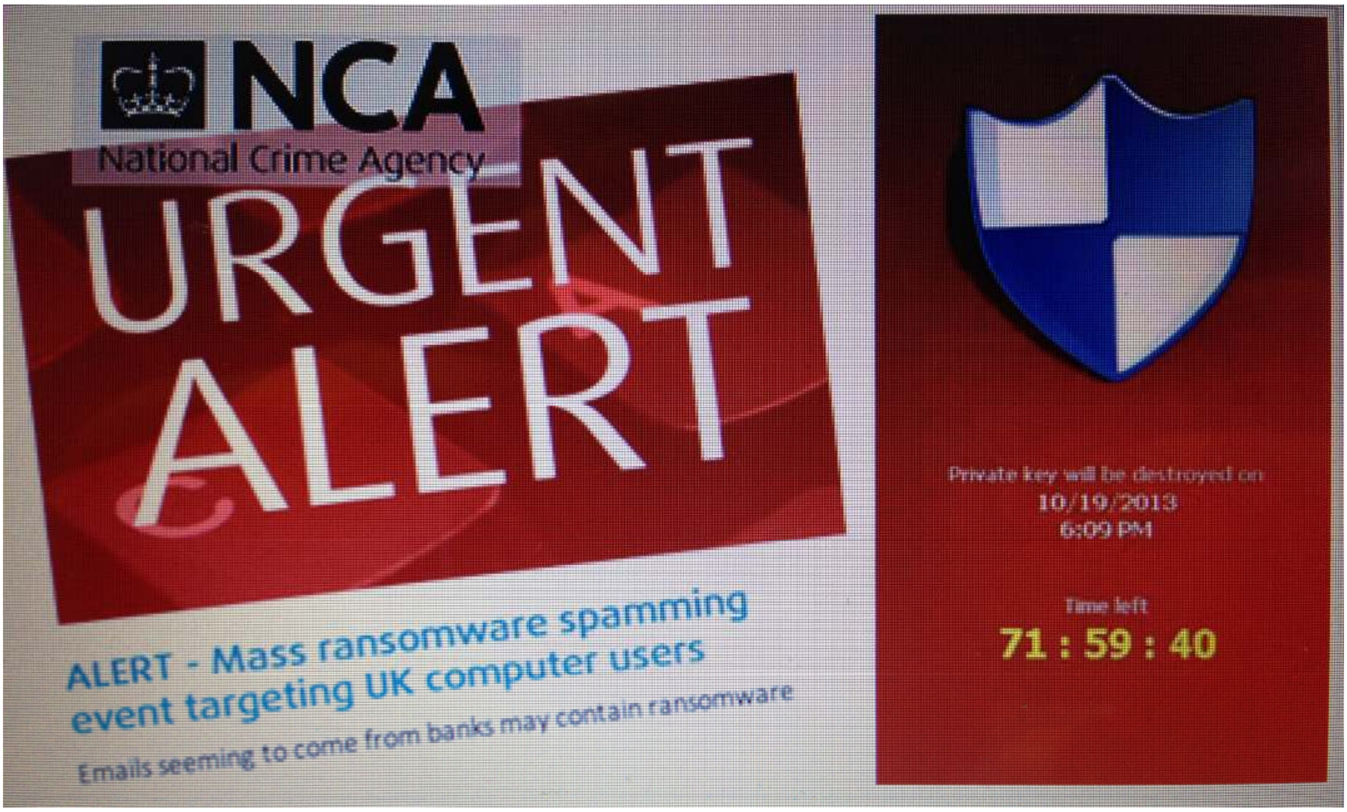
Octagon Technology Ltd

Octagon House, Gibson Close Branston LN4 1NF
t: 01522 797 520
e: info@octagontech.com

Computer, Technology and Cloud Services – Support and Supply

date: January 2014

Ref: Cryptolocker


NCA
National Crime Agency
URGENT ALERT
ALERT - Mass ransomware spamming event targeting UK computer users
Emails seeming to come from banks may contain ransomware
Private key will be destroyed on
10/19/2013
6:09 PM
Time left
71 : 59 : 40

What is Cryptolocker?

It is a program that when it infects your computer will encrypt your vital files and data, making them inaccessible to you unless you go online and pay a release fee. The following is a list of file types that are attacked – but this list could change at any time.

```
????????.jpe, ????????.jpg, *.3fr, *.accdb, *.ai, *.arw, *.bay, *.cdr, *.cer,
*.cr2, *.crt, *.crw, *.dbf, *.dcr, *.der, *.dng, *.doc, *.docm, *.docx, *.dwg,
*.dxf, *.dxg, *.eps, *.erf, *.indd, *.kdc, *.mdb, *.mdf, *.mef, *.mrw, *.nef,
*.nrw, *.odb, *.odc, *.odm, *.odp, *.ods, *.odt, *.orf, *.p7b, *.p7c, *.p12,
*.pdd, *.pef, *.pem, *.pfx, *.ppt, *.pptm, *.pptx, *.psd, *.pst, *.ptx, *.r3d,
*.raf, *.raw, *.rtf, *.rw2, *.rwl, *.sr2, *.srf, *.srw, *.wb2, *.wpd, *.wps,
*.x3f, *.xlk, *.xls, *.xlsb, *.xlsm, *.xlsx, img_*.jpg
```

(source grahamcluley.com)

If your files are encrypted then unless you pay for the key to unlock them, the files will be lost forever.

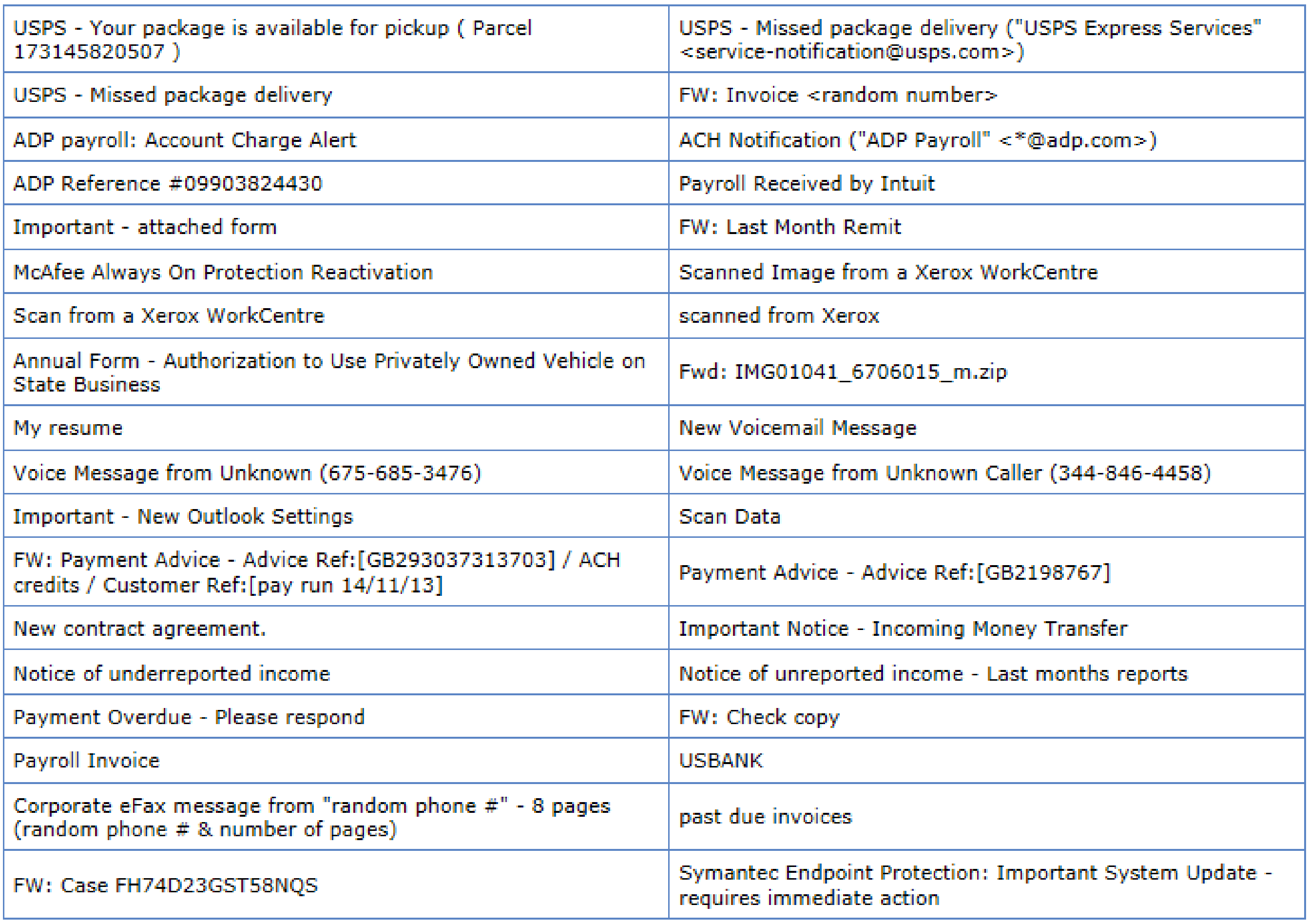
Cryptolocker is this the worst computer virus ever?

The quick answer to this is probably no, but it could be the most devastating malware infection you ever get on your computers. Virus software will remove the problem software but the encrypted files will be gone – unless you pay.

How is Cryptolocker spread?

The primary way this ransomware gets to a computer is in an attachment on an email – the attachment is usually a small .zip file or a PDF file ending .pdf.exe. The best security is not to open **any** .zip attachment on an email or open a .pdf file from an unexpected source. Unfortunately the latest version of the ransomware is also spreading via infected USB dongles and portable hard drives so extra care must be taken when plugging these devices into your computer. (Your business should put a policy in place about the use of external drives.)

Some examples of Cryptolocker subject lines:



USPS - Your package is available for pickup (Parcel 173145820507)	USPS - Missed package delivery ("USPS Express Services" <service-notification@usps.com>)
USPS - Missed package delivery	FW: Invoice <random number>
ADP payroll: Account Charge Alert	ACH Notification ("ADP Payroll" <*@adp.com>)
ADP Reference #09903824430	Payroll Received by Intuit
Important - attached form	FW: Last Month Remit
McAfee Always On Protection Reactivation	Scanned Image from a Xerox WorkCentre
Scan from a Xerox WorkCentre	scanned from Xerox
Annual Form - Authorization to Use Privately Owned Vehicle on State Business	Fwd: IMG01041_6706015_m.zip
My resume	New Voicemail Message
Voice Message from Unknown (675-685-3476)	Voice Message from Unknown Caller (344-846-4458)
Important - New Outlook Settings	Scan Data
FW: Payment Advice - Advice Ref:[GB293037313703] / ACH credits / Customer Ref:[pay run 14/11/13]	Payment Advice - Advice Ref:[GB2198767]
New contract agreement.	Important Notice - Incoming Money Transfer
Notice of underreported income	Notice of unreported income - Last months reports
Payment Overdue - Please respond	FW: Check copy
Payroll Invoice	USBANK
Corporate eFax message from "random phone #" - 8 pages (random phone # & number of pages)	past due invoices
FW: Case FH74D23GST58NQS	Symantec Endpoint Protection: Important System Update - requires immediate action

(source bleepingcomputer.com)

What files will Cryptolocker attack?

The ransomware will encrypt any of the files listed above if they are stored in a location accessible from your computer. These will include:

- The local hard drive
- My Documents
- Mapped drives (look in My Computer to see what is mapped on your computer)
- Portable hard drives or memory sticks plugged into the USB ports of your computer
- NAS drives
- Folders shared by users on a network

Cryptolocker will also attack files and data stored online in services such as DropBox or Google Drive if they are shared or synchronised from an infected computer – and then these encrypted files can be passed onto other computers in the share group.

The Best Defence

For peace of mind you will need a backup of your data and files, stored in a location that is not attached to your computer – this excludes online services which synchronise your data rather than back it up.

True online backup solutions are a suitable way to backup your data. Check the retention of your services as the encrypted files will be uploaded to the backup, replacing the good files, which means they could all be replaced before you realise there is a problem. *The impact of the only case of Cryptolocker software infection we have dealt with at Octagon so far, was greatly reduced as the company uses our monitored online backup service with a seven day retention plan.*

If you backup to a portable device make sure it is unplugged once the backup is finished – however remember that when you next plug it in, your backed up files will be vulnerable to attack.

A longer term archive drive or backup software that produces a file rather than copying the individual files would help to increase the protection offered by any backup solution you use.

Anti-virus and Anti-malware software

Make sure you have reputable anti-virus software installed on your computer, that it is regularly updated and that scans run on your computer at regular intervals. This will alert you to problems but remember that the people who write Cryptolocker (and other viruses, Trojans and ransomware) design their software to avoid detection and they constantly adapt their malware as the Anti-virus companies develop the protection you will be relying on. Hence backing up is the best way to protect yourself.

In Conclusion

This is not meant to be an extensive “how to” document – it is meant to raise people’s awareness of the issues, however here are a few useful resources for those who are more computer literate.

- Microsoft produce good anti-virus software – search Microsoft.com for Security Essentials
- Cryptolocker makes changes to the computer registry – search the registry for “cryptolocker”.
- At Octagon Technology we use Malwarebytes to deal with malware and trojans - malwarebytes.org
- ESET (eset.com) provide a free, well respected tool that can remove Cryptolocker – search for ESET Rogue Application Remover (ERAR) – however remember that if you find you are infected the damage has already been done – **get a good backup**.

Cryptolocker is a serious threat to everyone’s data and files – everyone should take some simple steps to help themselves:

- Develop a backup policy which is appropriate for your business or personal situation
- Use reputable anti-virus and anti-malware software
- Undertake staff training in the use of email and USB drives
- Keep reminding the people in your organisation that these threats exist
- If in doubt talk to someone who can help you make the decisions that will protect your information, data, files and business.

Clive

Clive Catton
Technical Director
M: 07943 537804
E: clive@octagontech.com