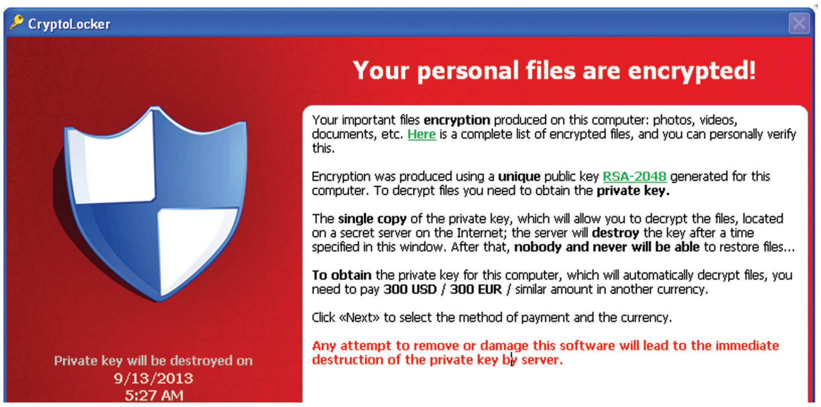
Expensive Malware

Cryptolocker and similar ransomware

There is a new breed of computer malware that is spreading rapidly. The first major manifestation of this new type is known as Cryptolocker. At present it's a Windows only problem (all versions), but it's likely that it won't be long until there are copycat versions targeting Apple MACs. It is also very likely that many more similar pieces of malware will crop up soon, as the technique is proving very lucrative for the creator(s) of the software. Cryptolocker started making headlines, even in the general press, in November 2013. In a nutshell the scenario usually unfolds as follows.

A user receives an email that either has an attachment or links to a file on the net. The emails can be very convincing, often masquerading as a bill or invoice. If a PC user makes the mistake of running the file, that's where the problems begin. If the user is lucky, up-to-date security software on the computer may catch and block the program running. Sadly, this is by no means a guarantee as Cryptolocker is being evolved quickly to avoid detection. If the software successfully runs, it silently gets to work looking for personal files. By this I mean files like photos, Word documents, PowerPoint presentations, Excel spreadsheets and tens of other types of files that can be created by users. Importantly, it reaches out as far as it can in search of these files. Open network connections to shared folders are vulnerable, as are USB sticks or hard drives that are plugged in. In fact, any files that that can be found through the 'My Computer' Explorer interface can be found by Cryptolocker. The software then converts the files into junk (via a very strong encryption method). At this point the user's computer is still working fine and will still load, but all created documents and photos have effectively now been lost! At this point there are only two ways to retrieve the files:

1. Follow the instructions then presented on the user's computer instructing them how to securely pay around $300 (Figure 1). There is a 72 hour countdown and users are informed that the data will be lost for good if timely payment is not made. If payment is made the files are almost always restored and the user can then busy themselves removing the remnants of the malware.



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 **300 USD / 300 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
9/13/2013
5:27 AM

2. The only other way to replace the files is to restore them from a backup (once Cryptolocker has been eradicated). Not every backup will do. If the user's backup was a USB hard drive, permanently plugged into the computer it is very likely any backups on there will have been encrypted too.

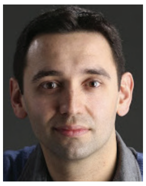
There really is no other way to get the files back. So, if no usable backups are available, pay up and hope for the best. Alternatively, live without all those files. The advice from security firms and the police is generally not to pay up as that encourages the criminals. In reality, if one is faced with the loss of many personal files and photos paying £300 may be the best option under the circumstances. Virus killers will be able to remove the malware, but this will NOT decrypt the files. They will be completely useless. If you are in the unfortunate position of considering paying, don't remove the malware as it will make the task of getting your files back less straightforward.

Protecting yourself from infection

Hopefully most readers will be in position to take precautions to avoid the scenario above. Here are a few ideas to help lower the risk of becoming a victim of this type of scam:

- Never open unsolicited files or attachments
- Keep malware software updated
- Make sure you have contemporary backups that are not connected. USB hard drives are OK as long as they are not connected. Remember though, if you plug one into a machine that is still infected, say goodbye to the files. Online backup services, such a Carbonite, will protect your data up to a point. Carbonite may start to back up the encrypted files over the original files in time. They will keep older versions of files for 30 days. So, in the case of an infection, Carbonite should be disabled (to prevent backup of the encrypted files), the malware removed and then the data restored from Carbonite.
- If you have network shares and multiple computers in the house, consider limiting access to the files from high risk computers. As an example, my kids use a laptop that was (until recently) connected to my shared files and photos drive. I have now limited the access that computer has to my network. In the scenario that the kids' computer becomes infected, at least it won't be able to encrypt files on the shared drive and other connected computers. Also be wary about giving your home Wifi password out to visiting friends if you have shared drives.

The suggestions above should be observed from now on, as this problem is likely to only get worse in the future. For those interested in learning more, Google 'Cryptolocker'. The Wikipedia entry for Cryptolocker is a good place to start.



Mr David Haider,
Consultant Ophthalmologist,
Royal Bolton Hospital, UK.
E: david@drhaider.co.uk

Declaration of Competing Interests
The author has no proprietary interest in any of the products discussed.