RANSOMWARE

Contents

1. Introduction

This guide examines a new and dangerous type of computer virus known as 'ransomware'. The virus has caused severe problems for computer users in a number of universities. The guide identifies the main characteristics of the virus and considers a number of situations where it has occurred. Finally, a number of steps to follow should you encounter the virus are set out.

2. Ransomware – What is it?

Ransomware is a new and especially dangerous type of computer virus or malware. It is known as "ransomware" because it prevents you from accessing your files unless you pay money to the authors of it. Some versions of the virus will claim that your computer has been 'used for illegal activity' and has been 'locked by the police'. There may be other messages like this, all aimed at getting you to pay money to the person or organisation that created the virus. Essentially, you lose control of your computer and the data that it contains.

The virus works by 'scrambling' or encrypting the files on all local and mapped network drives that your computer can access, including staff and student home folders, departmental shares, and removable media such as memory sticks and USB-connected drives. If there's a drive letter for it (e.g. C: D: E: H: S: etc) then it is at risk. Affected files can only be unencrypted using a key that you are forced to pay for.

Occurrences of this virus have grown immensely over the last year. In June 2013, security software vendor McAfee released data showing that it had collected over 250,000 unique samples of ransomware in the first quarter of 2013—more than double the number it had obtained in the first quarter of 2012.

The method of infection depends on what ransomware is being distributed, but the most common means of infection are:

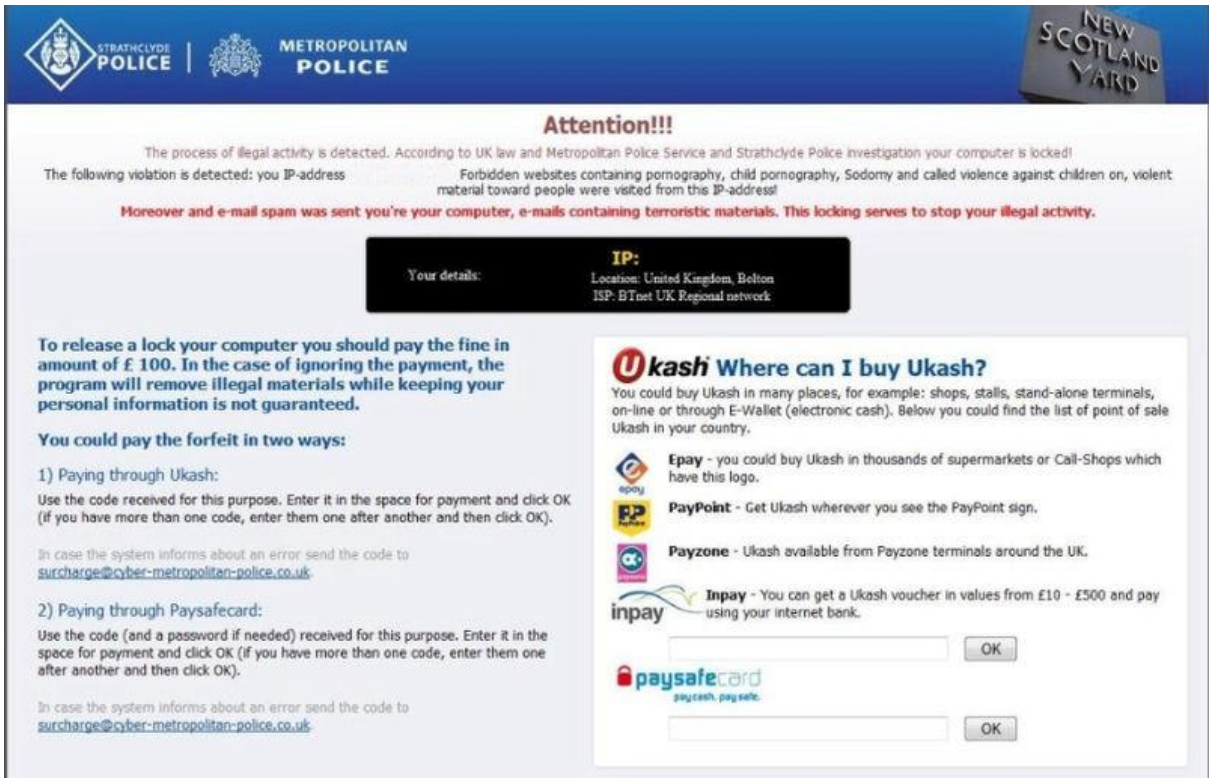
1. Emails with an attachment containing some enticing document. The person will click on the attachment only to find out it is a normal Windows executable; it is possible for the attacker to hide the .EXE extension and make it appear more like a document with a fake .PDF extension.
2. Downloading content from the web. Perhaps it is advertised as an interesting document, but against turns out to be a Windows executable.
3. Drive-by infections via compromised advertising banners. Those 'ad banners' you find on web sites, can (and sometimes do) contain malware … including ransomware.

In theory anti-virus protection should prevent this sort of thing from happening, and it is still essential that you have an up to date anti-virus protection on your PC. But it is not a guarantee that you will not get infected. Whilst IT Services are taking steps to help prevent infection of this virus, please be vigilant when opening emails and attachments and when downloading files, especially if you are not expecting such an email. **If you're not expecting it you should delete it**.

3. How to recognise it

The virus has several versions, with the '**cryptolocker**' version (below) being the most prevalent at the moment. The example below demands a payment of USD 300 in return for regaining access to your files.

Other variants of the virus will claim to be from the Police or from other security agencies (either in the UK or elsewhere). The **Metropolitan Police** example is below. Again, the aim is to scare people into 'paying a fine' (in this case of £100) so as to regain access to their computer.



4. Troubleshooting

It is important to take a 'defence in depth' approach. This means taking the following steps:

1. You should have saved / backed up copies of your documents in another location. This could be on another computer (at home or work) or it could be through a cloud storage company. This will need to be regularly updated (synchronised) however.
2. If you are using a computer at home, ensure that your antivirus package is up to date (and is being regularly updated).
3. Given that ransomware frequently exploits the weaknesses in older versions of Java and Adobe software, it is important to use the latest versions of these and to update them regularly.
4. If your computer has been infected you will see something like the dialog boxes above. If a pop up window like this should appear on your PC, you should IMMEDIATELY POWER OFF YOUR COMPUTER and seek help. The reason for this advice is that the message is displayed early in the encryption process. By stopping it as soon as possible you reduce the number of files that you might lose.
5. **Contact ITS as a matter of urgency (its@bbk.ac.uk)**
6. It goes without saying that you should not attempt to pay any ransom / money that might be demanded.

Contact Us

ITS Service Desk is located in the Student Service Centre on the ground floor of the Malet St. building
We are open from Monday to Friday, 10 am – 6pm.

Phone: 020 7631 6543
Email: its@bbk.ac.uk
Web: www.bbk.ac.uk/its

Further Information

How ransomware works

http://studentnews.southwales.ac.uk/news/2013/nov/06/new-nasty-computer-virus-ransom-warning/

Simple advice about how to deal with ransomware

http://www.gla.ac.uk/services/it/helpdesk/emailadvice/

Cryptolocker – How it works and what to do about it

http://nakedsecurity.sophos.com/2013/10/18/cryptolocker-ransomware-see-how-it-works-learn-about-prevention-cleanup-and-recovery/

A short Youtube video explaining what is meant by ransomware and why it is important

http://www.youtube.com/watch?v=NVrXp_QaifY