CYBER AWARE

south east
Regional Organised Crime Unit

Ransomware

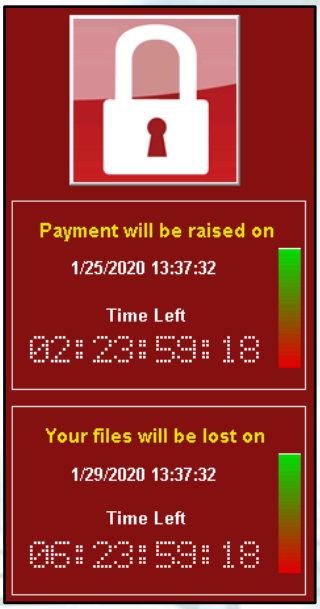
Surrey & Sussex CCU Newsletter – September 2020

Ransomware remains one of the biggest problems for businesses and individuals alike. It is defined as 'a type of malicious software designed to block access to a computer system until a sum of money is paid.' Many of you will remember the 'WannaCry' ransomware attack in 2017 which seriously affected the operational capability of the NHS and spread across the globe in record time. There are many variants of ransomware – Locky, Bad Rabbit, Petya, NotPetya, Ryuk, Dharma to name but a few. Most have the same purpose in life – to encrypt your files and demand a ransom to get your files back. More recently, to strengthen their demands, ransomware coders have opted to steal information as well as encrypting it and then threaten to expose it on the Internet.

How does ransomware work?

Ransomware is generally contained in an executable programme and needs to be run on a device. The nature of execution is beyond the scope of this newsletter but once it is running, it will encrypt files so they are unreadable and, once complete, a message will be left explaining how much the ransom is and how to pay it. Some will have a timer running detailing when your files will be permanently destroyed – adding to the pressure.

Modern ransomware uses strong cryptography and the encryption is likely to be uncrackable. You therefore have 2 choices if you want your files back – either pay the ransom or restore from a backup.



Please note that law enforcement does not encourage, endorse nor condone the payment of ransom demands.

How do I get ransomware on my computer?

The most common way of being infected is by clicking an attachment on a spam or phishing e-mail. Mobile users are also susceptible to malicious links from communication platforms such as Facebook and WhatsApp. Criminals that already have some form of remote access to your devices can also deploy malicious software and there are even cases of websites that can detect vulnerabilities in client browsers and deploy malicious software through the compromised web pages. Be aware – ransomware can attack any operating system.

Are you interested in a free cyber awareness presentation? Our Protect & Prepare team can deliver online presentations to businesses and other groups (20+ attendees) across Surrey & Sussex. These are approximately 1 – 1½ hours in duration and cover a range of current cyber topics.

Please e-mail CyberCrimeUnit@surrey.pnn.police.uk for further information.

SEROCU: serocu.police.uk/cyber | Cyber Aware: www.ncsc.gov.uk/cyberaware | NCSC: www.ncsc.gov.uk

CYBER AWARE

south east
Regional Organised Crime Unit

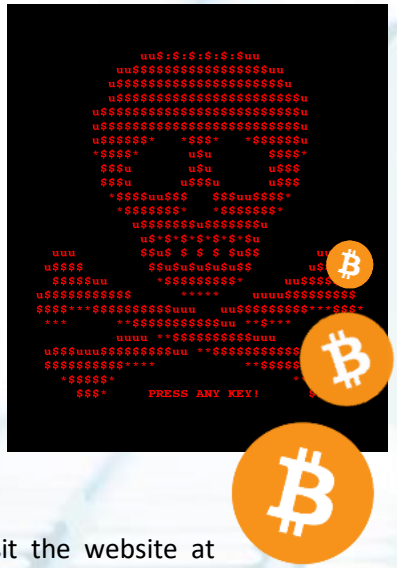
How can I stop this happening to me?

Getting infected by ransomware is an horrendous experience whether you are an individual or a business. By far in a way, the best thing to do is to prevent it from happening in the first place by taking some simple precautions:

- Be ultra-cautious of clicking links and opening attachments in e-mails.
- Ensure your anti-virus / anti malware software is current and up to date.
- Backup your data and other important files.

Be aware that ransomware can traverse network connections as well as USB. As such, it is highly likely that a permanently attached Network Storage Device or external hard drive will get infected and data contained on them destroyed. It is vital that any local backup devices are disconnected from the network after the backup process has completed. Many cloud-based backup services now offer ransomware protection and individuals may benefit from similar free cloud storage services offered by their operating system providers.

What should I do if I get infected with Ransomware?



Ordinarily, once you are aware you have been infected with ransomware, the damage is already done. If you have a large network, it would be sensible to consider unplugging network cables to prevent the spread, but you are generally left with one realistic option – resetting the machine and restoring your files from a backup.

Ransomware messages will always contain contact details for the criminal and ways to pay the ransom in exchange for a decryption key. Contacting these criminals provides them with some key information: (1) the attack has been successful, (2) there is something important that has been encrypted which you need and (3) you probably have no backups. The ball is therefore in their court and we have often seen ransom demands increase after communication has been initiated. In many cases, even after a ransom is paid, no decryption key will be provided.

Who do I report this to?

Action Fraud is the first port of call for any cyber-crime reporting. You can visit the website at https://www.actionfraud.police.uk/. You will need to create an account, but this can then be used for any subsequent reports. Please include as much information as you can, including Bitcoin addresses, contact e-mail addresses of the criminal and details of how you think you could have been infected.

If you are a business, charity or other organisation which is currently suffering a live cyber-attack (in progress), you can call 0300-1232040. This number is available 24/7.

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

Are you interested in a free cyber awareness presentation? Our Protect & Prepare team can deliver online presentations to businesses and other groups (20+ attendees) across Surrey & Sussex. These are approximately 1 – 1½ hours in duration and cover a range of current cyber topics.

Please e-mail CyberCrimeUnit@surrey.pnn.police.uk for further information.

SEROCU: serocu.police.uk/cyber | Cyber Aware: www.ncsc.gov.uk/cyberaware | NCSC: www.ncsc.gov.uk