Ransomware

Guide

IN PARTNERSHIP WITH

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

Cyber and Fraud Centre Scotland

Ransomware Guide.

Ransomware attacks have become common place in our society, where a new attack is reported almost daily. It is a growing cause of concern as more and more businesses have shifted their workforce to working remotely, which increases vulnerabilities and elevates the chances of a security breach.

Ransomware is one of the most significant cyber security threats facing businesses and organisations in the UK. When ransomware is successfully deployed, it has the potential to prevent public services and businesses operating and put their data at significant risk. (NCSC Annual Review 2022).

To understand what ransomware is helps identify ways to mitigate or even prevent a security breach from happening.

Ransomware is a type of malware which prevents access to certain files, usually important files containing sensitive data. Often the files are encrypted so they cannot be opened and can only be decrypted if a ransom is paid, usually in the form of Bitcoin.

Ransomware attacks are on the rise because they are effectively disguised as legitimate files, also known as a trojan attack. Once the malicious files are installed the malware infects the network it has gained access to.

The emphasis on being cyber aware by being suspicious of unusual emails is because it is the easiest target for hackers to get into a network. Having the capacity for emails is essential for businesses to communicate with clients. This creates a revolving door of information exchange that is vital in the digital age, but it is also an attack vector for unauthorized access to a device or network.

Garmin, a global brand who made fitness trackers amongst other things, ended up paying out millions of dollars in 2020 because they were targeted by a notorious hacking group. They used the WastedLocker malware that effectively shut down Garmin from operating, using email as the attack vector.

The NHS was vulnerable to a WannaCry ransomware attack in 2017 which cost £19 million in lost output, £72 million on restoring systems and data and over 19,000 appointments had to be cancelled as a consequence of this attack (New Statesman, 2018).

In late 2020, SolarWinds had been infiltrated by malicious hackers through the supply chain of the company. It was a complex cyber-attack with the fallout still been seen. SolarWinds was a trusted company providing software to many high-level organisations. Every time customers downloaded the undetected compromised packages from SolarWinds, the attackers were able to access the systems running the SolarWinds products (Center for Internet Security, 2021).

In late 2020, the Scottish Environmental Agency (SEPA) were targeted by a ransomware attack which affected its internal systems, processes, and internal communications as well as its contact centre operations. Data including personal information from staff was also stolen. SEPA has stated that the recovery from this will take some time and will be looking at acquiring an entirely new system to put into the organisation (TechHQ, 2021) .

From paralysing businesses to compromising national networks, there are no industries that are immune from ransomware attacks.

Attacks on government organisations, businesses, and now remote workers, shows why cyber security must be a key consideration for any organisation to function securely in the digital world. As the possibility of falling victim to a cyber-attack grows, so does the risk of losing business and suffering reputational damage.

Ransomware myths, true or false.

Ransomware can't infect my devices, I have a firewall.

False. Whilst having a firewall is advisable, it is not uncommon for forms of ransomware to infect users by passing themselves off as legit items. These items most commonly tend to be attached to seemingly innocent documents emailed to users. These types of malware are known as Trojans, named after the famous Greek story, "The Trojan Horse".

I am better off paying the ransom.

False. No matter how much the ransom may be, there can be no certainty that you will regain access to your device, or any guarantee the ransomware itself will actually remove itself from your device. It may hide itself and return at a later date. Clean, updated backups of any affected systems should be held in secure, separate locations outside of the internet to allow for the rebuilding of a broken system. (What is Ransomware?, 2021)

My data encrypted and is irretrievable.

False. (In some circumstances). After disconnecting the device from the network, Cyber forensic specialists and malware researchers work in conjunction to analyse the ransomware for its cryptographic keys through technical means such as deep packet inspections. This involves looking at packets sent through the network, and its sometimes possible to retrieve the keys from these packets. In some cases, it is possible for these keys to be extracted and used to reverse the encryption process. It is therefore important that organisations should make the NCSC aware of major incidents involving malware as it may be possible to retrieve encrypted data.

I've visited a website and a pop-up said something like "Your computer has been locked, send money to xxx or xxx", am I infected?

False. Pop ups asking the user to send money to suspicious cryptocurrency accounts are normally just phishing pop ups coded into the website on the server side, making them unable to affect you on the client side (unless you download an object). These are normally harmless and can be ignored and avoided by simply closing the browser or the affected webpage. Do not follow any suspicious link as they may land you on a malicious website. These pop ups will generally prey on the average users fear and may look like those examples listed below:

"Oh no! Your antivirus is out of date, click here to fix",

"A Police/Government organisation have locked down this computer on due to suspicious activity, pending a fine of £xxx".

"A hacker/virus has encrypted all your files! Pay here at _____ by xx/xx/xxxx or risk losing them!"

Please note that in the above examples, a website is generally unlikely to detect if your antivirus is out of date. If you think it is, you can easily check by going into your antivirus and checking if the latest updates have been applied. Police and Government "organisations" will never lock down computers or ask you to pay a ransom to remove the restrictions. Generic messages stating that a malicious actor has encrypted your files followed by a time limit of some sort are designed to make you panic. Do not worry, simply shutting the browser or webpage will make this message disappear.

I get pop-ups from my browser, even when I am not using it, saying I need to buy new antivirus from a website, or it will infect my PC, have I been infected by ransomware?

False. This is unlikely to be the case as pop ups such as these are generally the result of accidentally downloading adware. (Advertising malware). This type of adware is unlikely to become ransomware as it relies upon the user noticing these pop ups in the hope they visit the website. Adware was likely downloaded when accepting the "This website would like to show you notification" checkbox when visiting a website. This can be halted by visiting the settings within the affected browsing and clearing cookies and other site data. Within these settings you can normally find a list of all the cookies you have downloaded. You may also be able to find the cookie causing the pop-ups. Clearing browser data may also work if you are unable to find the cause of the pop up.

Do I need to keep up to date backups if I've never been infected before?

True. It is best practice to keep backups for "rainy days". Ransomware is just one way sensitive data might be lost, amongst a host of other ways such as device failure (Example: through physical damage like fire). By keeping backups, it is possible to mitigate for any loss of data. It is also important that any cloud services keeping backups can be disconnected and allow for data to be reverted, in the case that the local environment becomes infected. Backups should ideally be kept separately from the network. Multi factor authentication (MFA) can be utilised to protect them, however, in the event high value information must be retrieved in an attack where the admin may be compromised, the device that administers the backups should use a privileged access system. (Mitigating malware and ransomware attacks, 2020)

Ransomware.

"I've been infected but I have recent backups. If I restore these..."

or

"I've been infected however I was able to restore from new backups..."

... am I safe from further infection?

False. Unfortunately, some ransomware payloads are like timebombs. They have been sitting dormant since they were first downloaded and have been waiting for certain conditions to occur before executing. When restoring/ creating backups it is important these are scanned to make sure they are clean from any possible infection.

I followed a suspicious link to a website, have I downloaded malware?

False, in most cases. However, if something has been downloaded it is important to run an antivirus scan and delete the untrusted file. Most types of virus rely on a payload being executed by a series of events. Firewalls can help block remote signals to the payload to prevent execution. It is always possible to remove malware before it has a chance to execute by keeping anti-virus software up to date, allowing it quarantine and remove any discovered threats.

Who can help me deal with Ransomware?

Ransomware infection is a serious concern for businesses and organisations alike. The Cyber and Fraud Centre is on hand to help you deal with it through the incident response service. The Cyber and Fraud Centre is in partnership with the Scottish Government and Police Scotland and has created an Incident Response Helpline for SME's and third sector to help support victims of cybercrime. The free helpline can identify if an attack has taken place and will offer expert guidance to alleviate the problem. Any organisation that is concerned about having the right security processes in place can also use this helpline.

Businesses can reach the Incident Response Helpline by calling

0800 1670 623

Our Incident Response and Threat Intelligence Manager, Mike Smith will act as your first point of contact and will be on hand to help your business resume operations. Visit our website for more information.

cyberfraudcentre.com/prevent/cyber-services/incident-response

Ransomware is illegal, if you think you have been a victim of cybercrime the first step is to contact Police Scotland via

101

Additional Information

How can I help fight against ransomware?

Cyber security researchers and organisations from across the world have collaborated together form the "No More Ransom" project, creating the Crypto Sheriff tool which will attempt to decrypt a sample of infected files from an infected machine as well as identifying the perpetrators behind the attack. (The No More Ransom Project, 2020) Crypto Sheriff can be found at:

https://www.nomoreransom.org/crypto-sheriff.php

Crypto Sheriff also lists a long list of in-house decryption tools for the recovery of encrypted data.

How can I keep myself ahead of ransomware?

CyberScotland post updates about current news and guidance for organisations and individuals across Scotland. Visit the CyberScotland website to find out more - Hyperlink CyberScotland. Other services provided by the Cyber and Fraud Centre such as our cyber services which include our Exercise in a Box, CiSP Cyber Essentials and various Security assessments can be found here.

Exercise in a Box

Running a business is even more challenging in the current climate. To help organisations, the Cyber and Fraud Centre are running NCSC's Exercise in a Box sessions to provide insight into any areas that could be enhanced to minimise cyber threats and to be as compliant to security practices as possible.

How do I respond to questions about an incident?

Dealing with the aftermath of a ransomware attack can be challenging. Journalists might begin calling you with questions regarding the attack. Remember there are laws regarding how you inform your clients that your organisation has been the victim of a ransomware attack, as well as what details you can give to the press.

Guidance on from the ICO on what, how, and when you should notify clients about a current incident with a view to press considerations can be found here:

https://ico.org.uk/for-organisations/report-a-breach/

Make sure what you are as truthful with your employees as you are with the public. This helps improve the coherency of how your colleagues respond to questions from journalists.

Ultimately, try to make it a one-day story. By communicating early and delivering on promised updates, the company reduces the chances the media may make more of the story than it might deserve. The harder a journalist has to work to dig up the information about a breach, the more value the reporter and their editors will place on the story — and this will be reflected in where it is played and how long it is considered newsworthy.

Please also refer to the guide from VISA on handling any type of breach. In this document are good pointers as to how the organisation should address their customers/ clients, such as by addressing to your organisation as "currently investigating" the status of an ongoing incident, by detailing and tackling any fears people may have regarding the time-consuming processes such as the investigation itself or data recovery, rather than simply announcing that the organisation is a "victim" of an attack. The guide can be found here:

https://www.visa.com.my/dam/VCOM/global/support-legal/documents/responding-to-a-data-breach.pdf

Useful Links

If you think you have been breached the Cyber and Fraud Centre provides an incident response service:

https://cyberfraudcentre.com/prevent/cyber-services/incident-response

If you want to learn about the Exercise in a Box programme:

https://cyberfraudcentre.com/prevent/cyber-services/exercise-in-a-box

Other services provided by the Cyber and Fraud Centre:

https://www.sbrcentre.co.uk/prevent-protect/cyber-services

Police Scotland Advice on staying safe from cybercrime:

https://www.scotland.police.uk/keep-safe/keep-secure-online/cybercrime

No More Ransomware's Crypto - Sherriff

https://www.nomoreransom.org/crypto-sheriff.php

Additional information for keeping safe on-line:

https://www.scotland.police.uk/keep-safe/keep-secure-online

For more information on ransomware prevention advice:

https://www.nomoreransom.org/en/prevention-advice.html

Guidance from VISA on handling a security breach with a view to press considerations:

https://www.visa.com.my/dam/VCOM/global/support-legal/documents/responding-to-a-data-breach.pdf

Guidance from the ICO on reporting an incident:

https://ico.org.uk/for-organisations/report-a-breach/

References

Center for Internet Security. (2021, 01 20). Retrieved from https://www.cisecurity.org/solarwinds/

New Statesman. (2018, 10 12). Retrieved from NS: https://tech.newstatesman.com/security/cost-wannacry-ransomware-attack-nhs

NCSC Annual Review 2022 https://www.ncsc.gov.uk/files/NCSC-Annual-Review-2022.pdf

TechHQ. (2021). Retrieved from https://techhq.com/2021/01/significant-and-sophisticated-ransomware-hits-uk-agency/

UK ransomware attacks. (2019). Retrieved from https://www.cbronline.com/news/uk-ransomware-attacks

Ncsc.gov.uk. 2020. Mitigating Malware And Ransomware Attacks. [online] Available at: https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks#stepsifinfected [Accessed 26 January 2021].

Nomoreransom.org. 2020. The No More Ransom Project. [online] Available at: https://www.nomoreransom.org/en/about-the-project.html [Accessed 3 February 2021].

Image of WastedLocker Kill chain taken from: https://unit42.paloaltonetworks.com/wastedlocker/

Cyber and Fraud Centre Scotland

Oracle Campus
Blackness Road
Linlithgow
West Lothian
EH49 7LR

01786 447 441
enquiries@cyberfraudcentre.com
www.cyberfraudcentre.com
@cyberfraudcen

IN PARTNERSHIP WITH

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

A Company Limited by guarantee and registered in Scotland
No. SC170241 | VAT Registration Number: 717 2746 27