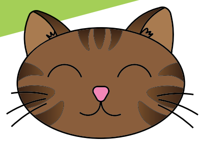
RANSOMWARE

What is Ransomware?

Ransomware is a type of malicious software (malware) that prevents you from accessing your data by encrypting it.

The data may be exfiltrated before being encrypted. Once encrypted the victim is sent a ransom demand - pay us to decrypt your data and regain access to your system. If data has been exfiltrated they may request payment or they'll publically release your data.



A HISTORY

The First Ransomware Attack: AIDS Trojan

In 1989 an AIDS researcher gave out 20,000 infected floppy disks to those who attended the World Health Organization's AIDS conference.

They contained malware that hid file directories, locked file names, and demanded victims send $189 to a PO Box in Panama if they wanted their data back.

The researcher didn't get rich and many victims, who mainly worked in the medical field, wiped their hard drives resulting in loss of valuable research data.

Ministry of Justice

GPCode and Archiveus Trojan 2006

In 2006 the Archiveus Trojan encrypted everything in the MyDocuments directory for PC users. Victims were required to purchase items from an online pharmacy in order to get a 30-digit key code that would unlock their files.

The same year, GPcode ransomware infected PCs through spear phishing attacks in the form of email attachments that looked like job applications.

WinLock Trojan 2007

WinLock displayed pornographic images until the users sent a $10 premium-rate SMS to receive an unlocking code.

CryptoLocker 2013

CryptoLocker spread through downloads from a compromised website or was sent in the form of email attachments made to look like customer complaints.

Victims had to pay through cryptocurrency or money cards to regain access. If payment wasn't received within three days, the user was given a second opportunity to pay a much higher ransom.

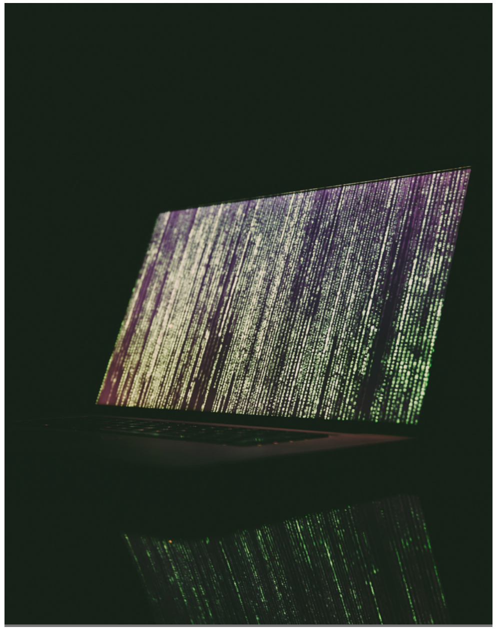
2009 Bitcoin

Invention of Bitcoin, a decentralized digital currency allowing for peer-to-peer transactions, providing a new, mostly anonymous system for transferring money – making it the perfect way for cybercriminals to extort their victims

WannaCry 2017

The UK's National Health Service was brought to a standstill for several days due to WannaCry ransomware.

The WannaCry ransomware cryptoworm propagated through a Windows exploit called EternalBlue.



There were over 230,000 computers in over 150 countries affected. The attack resulted in the cancellation of thousands of operations and appointments.

Staff were forced to revert to pen and paper and use their own mobiles as the ransomware affected key systems including telephones and databases of patient records.

The cybersecurity company Avast identified Wannacry as one of the broadest and most damaging cyber attacks in history.

Ministry of Justice

2016 No More Ransom

No More Ransom is a project that helps victims of ransomware get their encrypted files back for free by providing free decryption services and support to victims

Travelex 2019

The London-based foreign currency exchange Travelex was subject to a ransomware attack where customers' data, including dates of birth, credit card information, and insurance details, were obtained.

Travelex took down its website in 30 countries in an attempt to contain the virus.

The ransom demand was $6 million (£4.6 million) which was negotiated to $2.3 million (roughly £1.6 million) to get its data back.

Redcar and Cleveland Council 2020

The ransomware attack left the council's website inoperable with some officials having to use pen and paper to keep services running.

The online public services were down for over a week for the 135,000 locals and the attack cost the council an estimated of over £10million.

Hackney Council 2020-2021

Hackney council was also hit by ransomware that impacted services for local residents and companies, including derailing house purchases. In January 2021 their data was published on the dark web.

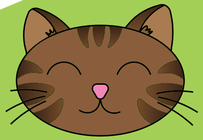
Colonial Pipeline 2021

America's largest fuel pipeline went offline due to this ransomware attack. The Colonial Pipeline covers over 5,500 miles and transports more than 100 million gallons of fuel daily.

After the attack the average price of a gallon of gas in the US increased to more than $3 for the first time in seven years due to the shortage of fuel caused by the pipeline being offline.

The President of the United States of America, Joe Biden, became involved as Americans began panic buying fuel and many stations ran out completely in the Washington DC area.

The company paid the ransom demand and their CEO stated they did so in the best interests of the country, and acknowledged it was a controversial decision.



PROTECTION

How can you protect yourself?

The Ministry of Justice has an excellent cyber security programme to defend against attacks such as ransomware.

However, there are many things you can do to help protect your work and personal devices from being impacted by a ransomware attack.

By following these security best practices, even if you are hit by a ransomware attack, you should be fully prepared and able to cope.

- Report if you get attacked. Call the helpdesk and contact your line manager
- Have good passwords to reduce the risk of bad actors guessing them and gaining access to accounts
- Use Multi-factor Authentication (MFA) to reduce risk of account access in case of password compromise
- Don't re-use passwords
- Schedule regular back-ups of your data
- MoJ back-ups team does this for work data and devices, but you will need to do this for your own personal data on personal devices
- Use cloud back-up systems
- If you are doing a physical back-up of your personal data then make sure you are not connected to the internet when you do it
- If you have particularly important data then back it up in two or more places for extra security
- Good back-ups mean that you can quickly recover your systems and data if you are hit by ransomware
- Don't download software or items from non-official websites
- Don't allow remote desktop access to your devices
- Avoid enabling macros on attachments sent via email unless you are certain the email is legitimate
- Avoid entering credentials when requested unexpectedly via email or text
- Don't panic! If you do get attacked these protections will help you recover fast