Ransomware

Miina-stiina Tanskanen

What is Ransomware ?

- Type of malware
- threatens to publish the victim's personal data or permanently block access to it
- Blackmailing victim to do a payment in order to avoid threat
- Bitcoin and other cryptocurrencies are used for the ransoms which leads to challenges to trace and procecute the perpetrator
- Internationally known attack was in 1989 with the name AIDS trojan.

How it works?

- Ransomware attacks are typically carried out disguised as a legitimate file that the user is tricked into downloading or opening when it arrives as an email or from other source as attachment.
- They pop up to the screen as notification informing about illegal actions on the computer which user can get rid of doing payment.

Defenses against ransomware + recovery

- Controlled folder access - On Windows operating system users are able to add specific file systems to it in Windows Defender.
- VSS (Volume shadow copy) – used to store backups -> ransoms tend to target these to prevent recovery

Recovery : several tools intended to decrypt locked files. Recovery keys are used to unlock the files.