An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

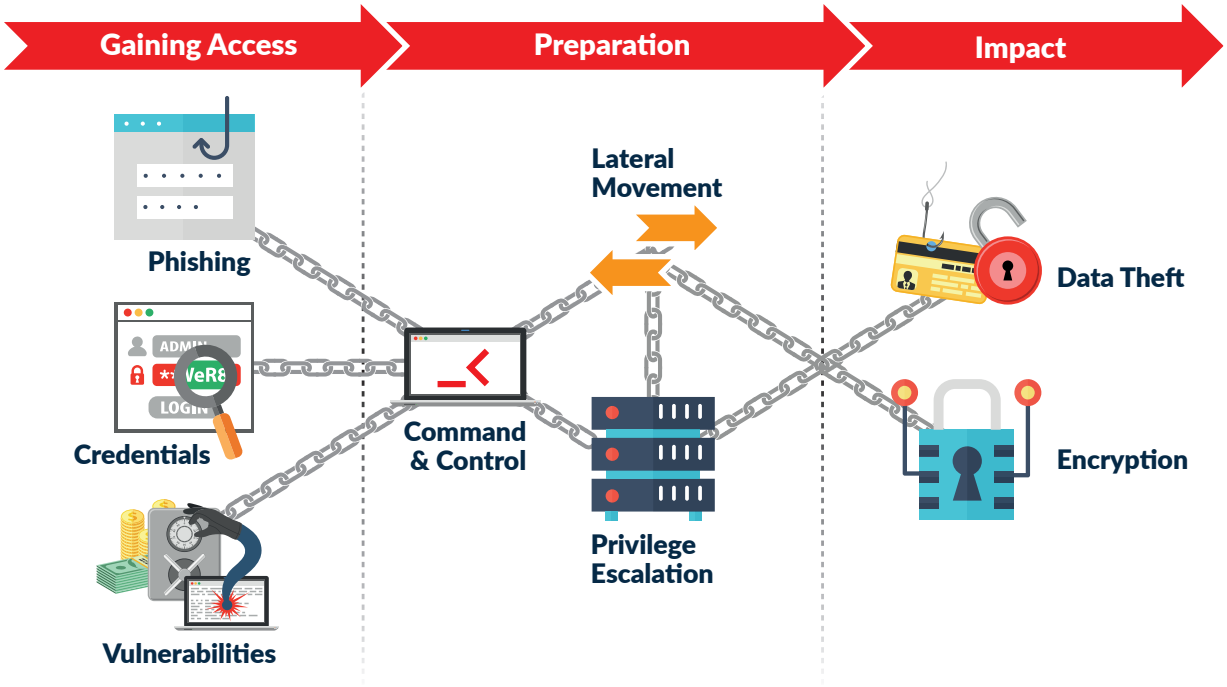
NCSC

NATIONAL CYBER SECURITY CENTRE

Quick Guide: Ransomware

How to #BreakTheChain

The Ransomware Attack Chain



Background

Ransomware is malware designed to encrypt files on a device, rendering files and the systems that rely on them unusable. Attackers typically demand ransom in exchange for a decryption key and/or to prevent sensitive data being leaked or sold on the internet.

Ransomware has been with us for at least three decades (the first recorded example was the PC Cyborg trojan of 1989), however the past several years has seen a significant increase in both the number and severity of ransomware attacks. 2021 was notable for serious attacks against critical infrastructure, including the Colonial Pipeline attack, the attack on the IT systems of the Italian region of Lazio, a supply chain attack on MSPs who used software from Kaseya, as well as a plethora of other incidents in sectors such as healthcare, pharmaceuticals, education, food distribution and public services. Ireland was not immune to this surge of ransomware incidents, with a hugely disruptive ransomware attack being carried out on the healthcare system in May 2021.

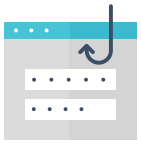
Ransomware operators are not just focussed on critical infrastructure, ransomware attacks can affect all organisations, both large and small. It is important for the management and IT staff of all organisations to understand the Ransomware Attack Chain, and importantly how you can **#BreakTheChain**.

The Ransomware Attack Chain

No attack is exactly the same, and there are steps that occur both before and after the attack itself, however, a ransomware attack broadly follows three key steps: **Gaining Access**, **Preparation**, and **Impact**.

Gaining Access

In order to carry out a ransomware attack, the attacker needs to gain access to your network. There are a number of ways an attacker may access your network, the most common ways being:



Phishing

The attacker sends an email which tricks a user in to downloading a malicious file or clicking on a malicious link. This will result in some form of malware being downloaded, usually a backdoor, which will provide the attacker with initial access to the system. Phishing can also be used to trick a user to reveal their credentials, using convincing fake login pages for services like email or other office applications.

Credentials

The attacker will obtain credentials which can be used to log in to devices on the edge of the network. They may steal the credentials using phishing, obtain them through a previously discovered data breach or simply guess the credentials through a brute force attack.

Vulnerabilities

An attacker may exploit a known, or in some rare cases unknown (0-day), vulnerabilities in systems that are exposed to the internet, such as remote access points (VPN, RDP), email servers, or security devices like firewalls. Some critical vulnerabilities allow the attacker to conduct unauthorised Remote Code Execution (RCE), meaning they can execute their malicious code remotely without having to log in to the device.

Preparation

Once an attacker has gained an initial entry to the network, they will need to consolidate their foothold on the network and prepare to cause as much damage as possible. They achieve this by:

Command and Control

The attacker needs to be able to communicate and exhibit control of the infected system. They will generally deploy malware for this purpose and control it using an attacker-controlled server (C2 server) either to take commands, download additional components, or to exfiltrate information.

Once C2 is established, the attacker will now attempt to move around the system and gain high level privileges. This is achieved through **Lateral Movement** and **Privilege Escalation**. They may use specific malware or malicious tools, or often they will use local operating system programs in order to avoid detection.

The attacker will continuously cycle through this process of hopping between systems and compromising privileged accounts, until they have high level access, such as an admin account. They may also use this access to disable security features like Anti-Virus protection.

Impact

The attacker then executes the attack. They generally have two goals:

Encryption

The attacker will push out their encryption to as many devices as possible, likely using local operating system programs to do so. The attacker will also focus on encrypting backups they can access in order to prevent recovery. The attacker will demand a ransom payment in return for a decryption key.

Data Theft

Before encrypting the system, the attacker will likely have stolen sensitive and personal data, in order to conduct ‘double extortion’ whereby they will demand a further ransom payment to prevent the data being leaked or sold.

Breaking the Chain

There are many opportunities throughout the Ransomware Attack Chain, whereby good cybersecurity practices will allow you to stop an attacker and **#BreakTheChain**. This is not an exhaustive list, but represents the priority actions you can take:

Reduce Attack Surface

Attackers are scanning your attack surface, make sure you understand it well. Make sure you minimise the parts of your network that are exposed to the internet by keeping edge devices to a minimum and closing unused ports and protocols. This reduces the entry points for attackers.

Patching

Conduct vulnerability scanning and make sure all of your hardware and software, particularly edge devices, are kept up to date with the latest security patches. This prevents attackers exploiting known vulnerabilities to access the network, moving laterally and escalating their privileges.

Multi-Factor Authentication

Make sure all remote access and privileged user accounts have MFA enabled. This makes it more difficult for an attacker to use stolen credentials. Where possible, avoid SMS as the second factor, and instead use an authenticator app.

Logging and Monitoring

By implementing effective logging and monitoring you will be able to detect attackers on your network and take action to remove them from the network. It will also allow you to understand what has happened and in turn, aid in the recovery process.

Backups

Make sure you keep backups of all of your data. Try to follow the 3-2-1 rule – 3 copies, on 2 separate systems, with 1 being 'offline'. This will allow you to restore if your data is encrypted.

Have a plan

Make sure you have a plan for what you will do if you are attacked. It should include key actions to take and people to contact. Test the plan! This will allow you to contain and effectively remediate a ransomware incident. You should also rehearse how you would deal with a serious data breach – a good response to a data breach is crucial for your reputation.

User Awareness

Make sure you educate all your users about the threat of ransomware and how they can prevent it. This will help reduce the chances of a user being tricked by phishing. A well-educated workforce is key to preventing and responding well to incidents.

Additional Resources

For more information and resources on protecting against and responding to ransomware please see the following resources:

- **An Garda Síochána** Increase in the Number of Ransomware Attacks in 2021
- **No More Ransomware** The No More Ransom Project
- **ENISA** ENISA Threat Landscape 2020 - Ransomware
- **EUROPOL** Ransomware: The Malware that Holds Your Computer Data Hostage for a Price
- **NCSC UK** Mitigating Malware and Ransomware Attacks
- **US Cybersecurity and Infrastructure Agency** Stop Ransomware
- **NIST Guidance** Ransomware Protection and Response

Reporting

Ransomware is a crime and should be reported to the Garda Síochána at your local garda station. You may also report ransomware incidents to the NCSC at incident@ncsc.gov.ie