GUIDANCE

Mitigating malware and ransomware attacks

How to defend organisations against malware or ransomware attacks

This guidance helps private and public sector organisations deal with the effects of malware (which includes ransomware). It recommends steps to take before a malware infection has occurred, but also suggests steps to take if you're already infected.

Following this guidance will reduce:

- the likelihood of becoming infected
- the spread of malware throughout your organisation
- the impact of the infection

If you've already been infected with malware, please refer to our list of urgent steps to take

For information about protecting your devices at home, please read our guidance especially for individuals and families. Smaller organisations should consider the tips presented in the NCSC's Small Business Guide.

In this guidance

What is malware?

Malware is malicious software, which - if able to run - can cause harm in many ways, including:

- causing a device to become locked or unusable
- stealing, deleting or encrypting data
- taking control of your devices to attack other organisations
- obtaining credentials which allow access to your organisation's systems or services that you use
- 'mining' cryptocurrency
- using services that may cost you money (e.g. premium rate phone calls).

What is ransomware?

Ransomware is a type of malware that prevents you from accessing your computer (or the data that is stored on it). The computer itself may become locked, or the data on it might be stolen, deleted or encrypted. Some ransomware will also try to spread to other machines on the network, such as the Wannacry malware that impacted the NHS in May 2017.

Normally you're asked to make a payment (often demanded in a cryptocurrency such as Bitcoin), in order to unlock your computer (or to access your data). However, even if you pay the ransom, there is no guarantee that you will get access to your computer, or your files. Occasionally malware is presented as ransomware, but after the ransom is paid the files are not decrypted. This is known as wiper malware. **For these reasons, it's essential that you always have a recent offline backup of your most important files and data**.

Should I pay the ransom?

The NCSC supports the National Crime Agency (NCA) recommendations. The NCA generally advise **not** to pay the ransom, as there is no guarantee that you will get access to your device (or data).

Using a defence in depth strategy

Since there's no way to **completely** protect your organisation against malware infection, you should adopt a 'defence-in-depth' approach. This means using layers of defence with several mitigations at each layer. You'll have more opportunities to detect malware, and then stop it before it causes real harm to your organisation. You should assume that some malware **will** infiltrate your organisation, so you can take steps to limit the impact this would cause, and speed up your response.

Tip 1: Make regular backups

The key action to take to mitigate ransomware is to ensure that you have up-to-date backups of important files; if so, you will be able to recover your data without having to pay a ransom.

- Make regular backups of your most important files - it will be different for every organisation - and check that you know how to restore the files from the backup.
- Ensure that a backup is kept separate from your network ('offline'), or in a cloud service designed for this purpose - our blog on offline backups in an online world provides useful additional advice for organisations.
- Cloud syncing services (like Dropbox, OneDrive and SharePoint, or Google Drive) should **not** be used as your only backup. This is because they may automatically synchronise immediately after your files have been 'ransomwared', and then you'll lose your synchronised copies as well.
- Make sure the device containing your backup (such as an external hard drive or a USB stick) is not permanently connected to your network and that you ideally have multiple copies. An attacker may choose to launch a ransomware attack when they know that the storage containing the backups is connected.

Tip 2: Prevent malware from being delivered to devices

You can reduce the likelihood of malicious content reaching your network through a combination of:

- filtering to only allow file types you would expect to receive
- blocking websites that are known to be malicious
- actively inspecting content
- using signatures to block known malicious code

These are typically done by network services rather than users' devices. Examples include:

- mail filtering (in combination with spam filtering) which can block malicious emails and remove executable attachments
- intercepting proxies, which block known-malicious websites

- internet security gateways, which can inspect content in certain protocols (including some encrypted protocols) for known malware
- safe browsing lists within your web browsers which can prevent access to sites known to be hosting malicious content

Public sector organisations are encouraged to subscribe to the NCSC Protective DNS service; this will prevent users from reaching known malicious sites.

Some ransomware attacks are deployed by attackers who have gained access to networks through remote access software like RDP. You should prevent attackers from being able to brute-force access to your networks through this (or similar) software by either:

- authenticating using Multi-Factor Authentication (MFA)
- ensuring users have first connected through a VPN that meets our recommendations.

Tip 3: Prevent malware from running on devices

A 'defence in depth' approach assumes that malware will reach your devices. You should therefore take steps to prevent malware from running. The steps required will vary for each device type and OS , but in general you should look to use device-level security features such as:

- Centrally manage enterprise devices in order to either:

  • only permit applications trusted by the enterprise to run on devices using technologies including AppLocker, or

  • only permit the running of applications from trusted app stores (or other trusted locations)

- Consider whether enterprise antivirus or anti-malware products are necessary, and keep the software (and its definition files) up to date.

- Provide security education and awareness training to your people, for example NCSC's Top Tips For Staff.
- Disable or constrain macros in productivity suites, which means:
  - disabling (or constraining) other scripting environments (e.g. PowerShell)
  - disabling autorun for mounted media (prevent the use of removable media if it is not needed)
  - protect your systems from malicious Microsoft Office macros

In addition, attackers can force their code to execute by exploiting vulnerabilities in the device. Prevent this by keeping devices well-configured and up to date. We recommend that you:

- install security updates as soon as they become available in order to fix exploitable bugs in your products. The NCSC has produced guidance on how to manage vulnerabilities within your organisation
- enable automatic updates for operating systems, applications, and firmware if you can
- use the latest versions of operating systems and applications to take advantage of the latest security features
- configure host-based and network firewalls, disallowing inbound connections by default

The NCSC's End User Devices Security Guidance provides advice on how to achieve this across a variety of platforms.

Tip 4: Limit the impact of infection and enable rapid response

If put in place, the following steps will ensure your incident responders can help your organisation to recover quickly.

- Help prevent malware spreading across your organisation by following NCSC guidance on preventing lateral movement. This will help because attackers

aim to move across machines on the network. This might include targeting authentication credentials or perhaps abusing built-in tools.

- Use two-factor authentication (also known as 2FA) to authenticate users so that if malware steals credentials they can't be reused.
- Ensure obsolete platforms (OS and apps) are properly segregated from the rest of the network (refer to NCSC guidance on Obsolete Platforms for further details).
- Regularly review and remove user permissions that are no longer required, to limit malware's ability to spread. Malware can only spread to places on your network that infected users' accounts have access to.
- System Administrators should avoid using their administrator accounts for email and web browsing, to avoid malware being able to run with their high levels of system privilege.
- Architect your network so that management interfaces are minimally exposed (our blog post on protecting management interfaces may help).
- Practice good asset management, including keeping track of which versions of software are installed on your devices so that you can target security updates quickly if you need to.
- Keep your infrastructure patched, just as you keep your devices patched and prioritise devices performing a security-related function on your network (such as firewalls), and anything on your network boundary.
- Develop an incident response plan and exercise it.

Steps to take if your organisation is already infected

If your organisation has already been infected with malware, these steps may help limit the impact of the infection. You should also refer to the NCSC's Cyber Incident Response scheme.

1. Immediately disconnect the infected computers, laptops or tablets from all network connections, whether wired, wireless or mobile phone based.

2. Consider whether turning off your Wi-Fi and disabling any core network connections (including switches) might be necessary in a very serious case.
3. Reset credentials including passwords (especially for administrators)- but verify that you are not locking yourself out of systems that are needed for recovery.
4. Safely wipe the infected devices and reinstall the operating system.
5. Before you restore from a backup, verify that it is free from malware and ransomware. You should only restore from a backup if you are **very** confident that the backup is clean.
6. Connect devices to a clean network in order to download, install and update the operating system and all other software.
7. Install, update, and run antivirus software.
8. Reconnect to your network.
9. Monitor network traffic and run antivirus scans to identify if any infection remains.

Note: Files encrypted by most ransomware have no way of being decrypted by anyone other than the attacker. Don't waste your time or money on services that promise to do it. In some cases, security professionals have produced tools that can decrypt files due to weaknesses in the malware (which may be able to recover some data), but you should take precautions before running unknown tools on your devices.

Further advice

- The National Crime Agency encourages anyone who thinks they may have been subject to online fraud to contact Action Fraud at https://www.actionfraud.police.uk.
- The National Cyber Security Centre (NCSC) runs a commercial scheme called Cyber Incident Response, where certified companies provide crisis support to affected organisations.

- The Cyber Security Information Sharing Partnership (CiSP) offers organisations in the UK a safe portal in which to discuss and share intelligence that can assist the community and raise the UK's cyber resilience. We encourage our members to share technical information and indicators of compromise so that the effects of new malware, and particularly ransomware, can be largely reduced.
- You may also wish to consider the Cyber Essentials certification scheme (which covers a number of these mitigations) so your customers and partners can see that you have addressed these risks. Many of these mitigations also work well against other types of attack, such as phishing.
- Consider following the NCSC guidance on protecting your organisation from phishing attacks.

PUBLISHED

13 February 2020

REVIEWED

13 February 2020

VERSION

1.0

WRITTEN FOR

Public sector

Cyber security professionals

Large organisations