National Cyber Security Centre
a part of GCHQ (/)

Guidance

# Mitigating Malware

Created: 09 Feb 2018
Updated: 09 Feb 2018

How organisations and home users can reduce the likelihood of malware infection.

This guidance describes how organisations of all sizes - and home users - can reduce the likelihood of being infected by malware.

It recommends **steps to take before a malware infection has occurred**. If you are dealing with an incident caused by malware infection, you can refer to the NCSC's Cyber Incident Response schemes(/scheme/cyber-incidents).

Note that:

- smaller organisations should consider the tips presented in the NCSC's Small Business Guide(/blog-post/cyber-security-small-business-guide)
- home users may also want to read GetSafeOnline (https://www.getsafeonline.org/protecting-yourself/viruses-and-spyware/) for guidance about how to protect your personal devices from malware infection
- your organisation should consider following our principles around response and recovery(/guidance/d1-response-and-recovery-planning) planning in case an incident occurs

#### Contents

### 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 (i.e. ransomware)
- stealing, deleting or encrypting data
- taking control of your devices to attack other organisations
- obtaining credentials to your organisation's systems
- 'mining' cryptocurrency
- using services that may cost you money (e.g. premium rate phone calls).

#### About ransomware

Ransomware has been used in multiple high-profile cyber crime incidents such as the Wannacry incident that impacted the NHS in May 2017. Ransomware is a growing class of malware and comes in two types. The first type encrypts the files on a computer or network; the second type locks a user's screen. Some ransomware will also act like a worm (as was the case with WannaCry) and once inside a network, will spread laterally to other machines without interaction by the attacker or the infected user.

Ransomware requires users to make a payment (the 'ransom') before the computer can be used normally again. This ransom is often demanded in a cryptocurrency (https://en.wikipedia.org/wiki/Cryptocurrency) (such as Bitcoin), as a prepaid card or gift voucher. In many cases the ransom amount is quite modest, a tactic designed to make paying the ransom the quickest and cheapest way to resume use. However, there is no guarantee that the key or password to 'unlock' the computer will be provided upon payment of the ransom.

The scale and automated nature of a ransomware attack makes it profitable through economies of scale, rather than through extorting large amounts from targeted victims. They are attacks of opportunity; they are not normally targeted at specific individuals or systems, so infections can occur in any sector or organisation. However there are cases where ransomware attacks are directed specifically at an organisation with much larger ransom demands. In some cases, due to the automation involved in the attacks, ransomware has struck the same victim more than once in succession.

Occasionally malware is *presented* as ransomware, but after the ransom is paid the files are not decrypted. This is known as wiper malware (https://en.wikipedia.org/wiki/Wiper_(malware)).

**Should I pay a ransom?**

If you become infected with ransomware, the National Crime Agency encourages industry and the public **not** to pay the ransom (http://www.nationalcrimeagency.gov.uk/crime-threats/cyber-crime/online-safety-guidance-for-businesses). If you do pay:

- there is no guarantee that you will get access to your data/device
- your computer will still be infected unless you complete extensive clean-up activities
- attackers may assume that you would be open to paying ransoms in the future
- you will be funding criminal groups

## Protecting your devices

Applying the following protections will reduce the likelihood of your device being damaged by malware.

**1. Keep your devices and software updated**

Malware generally exploits security issues that are publicly known. By keeping your software, and especially your operating system (OS), up to date, you greatly reduce the risk of malware infection. Nearly all platforms/OS's today come with automatic updates enabled, and we advise that you should keep them on.

To update your operating system:

- Windows users running Windows 7 (and later versions) should configure Windows Update (https://support.microsoft.com/en-us/help/12373) and apply any updates
- Apple users should follow the instructions for your particular OS (i.e. macOS or iOS) on Apple's security updates page (https://support.apple.com/en-us/HT201222)
- Android users should read Google's help page (https://support.google.com/nexus/answer/4457705?hl=en) with instructions for their own devices (this should also apply to those from other manufacturers, but you may need to find specific help for your device)

**Note:** The NCSC strongly recommend that you do **not** continue to use unsupported operating systems or devices. Upgrade to an operating system that receives regular security updates from the vendor, and check on their support sites how long they will be supported for. For example Microsoft provides a lifecycle fact sheet (https://support.microsoft.com/en-gb/help/13853/windows-lifecycle-fact-sheet).

**2. Protect your PCs and laptops**

- Make sure you have an antivirus or anti-malware product installed, turned on, and up to date. Windows built-in malware protection tool (Windows Defender (https://www.microsoft.com/en-us/safety/pc-security/windows-defender.aspx)) is likely to be suitable for most users.
- Run full scans to make sure your computer is currently free of all known malware. This will usually be done on a per-access basis (such as when you plug in a USB drive or download a file), but can also be automated to run periodically (for example every week).

**3. Protect your mobile devices**

- Only download apps from official stores (e.g. Google Play and the iOS App Store).
- The Home Office and the NCSC have jointly published a guide to choosing and using mobile devices (https://www.gov.uk/government/publications/mobile-device-security-a-buyers-guide-to-choosing-and-using-mobile-devices),

which you can use to help you chose and securely configure your device.

**4. Keep a safe backup of your important files**

If you have access to backups of files that you can easily recover, then you can't be blackmailed if you are affected by ransomware. For this reason you should:

- Regularly create a backup copy of your important files (such as photos, documents, and other files that can't be replaced).
- Make sure that the backup is **kept separately from your computer**. If the backup is on a USB stick, or a hard drive, or on any type of removable media, do **not** leave it connected (or **anywhere** on your network) or it may also be attacked by ransomware. This is an especially important point if your backups are stored on a network drive, because if you are infected by ransomware, data on network drives is likely to also be affected.
- Consider using cloud services to back up your files. Many cloud service providers (for example, email providers) offer an amount of cloud storage space for free.

## Protecting your organisation

As there are no mitigations that are *completely effective* against malware infection, you should develop a defence-in-depth strategy in your organisation. This consists of multiple layers of defence with several mitigations at each layer. This will improve your resilience against malware *without* disrupting the productivity of your users. You'll also have multiple opportunities to detect malware, and then stop it before it causes real harm to your organisation. Accepting the fact that some **will** get through will help you plan for the day when an attack is successful, and minimise the damage caused.

When building defences against malware, we recommend developing mitigations in each of the following three layers:

1. Layer 1: preventing malicious code from being delivered to devices
2. Layer 2: preventing malicious code from being executed on devices
3. Layer 3: increasing resilience to infection, and to enable rapid response should an infection occur

Each layer is addressed in the following sections. You may also wish to consider the Cyber Essentials (https://www.cyberaware.gov.uk/cyberessentials/) 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 are also effective mitigations against other types of attack, such as phishing. Consider following also the NCSC guidance on protecting your organisation from phishing attacks(/guidance/avoiding-phishing-attacks).

**Layer 1: Prevent malicious code from being delivered to devices**

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

- whitelisting file types that you would expect to receive
- blacklisting websites
- actively inspecting content
- using signatures to block known malicious code.

All these mitigations are typically used as network services rather than deployed to endpoints. Examples of these include:

- mail filtering(/guidance/email-security-and-anti-spoofing) (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(/information/uk-public-sector-dns-service); this will prevent users from reaching known malicious sites.

**Layer 2: Prevent malicious code from being executed on devices**

It is good practice to assume that malware will reach devices, you should therefore take steps to prevent malicious code from executing correctly. The steps required will vary for each device type and OS in use, but in general you should look to use device-level security features such as:

- centrally managing enterprise devices in order to either-
  (i) configure application whitelisting to ensure only code explicitly trusted by the enterprise can run on end user devices, or
  (ii) only permit the running of applications from trusted app stores (or other trusted locations)

- installing enterprise antivirus or anti-malware products, and keeping both the software and its definition files up to date
- informing users by providing user education and awareness training
- disabling or constraining macros in productivity suites, which means:
  (i) disabling (or constraining) other scripting environments (e.g. PowerShell)
  (ii) disabling autorun for mounted media (prevent the use of removable media if it is not needed)

Note that the NCSC has published guidance on configuring Microsoft Office macro security(/guidance/macro-security-microsoft-office).

In addition, attackers can force their code to execution by exploiting vulnerabilities in the device. To prevent such exploitation, it is important to keep 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
- enable automatic updates for operating systems, applications, and firmware (/blog-post/automating-uefi-firmware-updates)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(/guidance/end-user-device-security) provides advice on how to achieve this across a variety of platforms.

**Layer 3: Limit the impact of infection**

Should your organisation become infected with malware, your incident responders can help your organisation recover quickly if the following steps to improve resilience have been taken:

- help prevent malware spreading across your organisation by following our companion guidance on lateral movement(/guidance/preventing-lateral-movement)
- ensure obsolete platforms (OS and apps) are properly segregated from the rest of the network (refer to our Obsolete Platforms Guidance(/guidance/obsolete-platforms-security-guidance) for further details)
- review user permissions regularly and remove accesses that are no longer required by the user (this will ensure that malware can only spread to network locations that the infected user has access to - system administrators with high levels of access should avoid using their administrator accounts for email and web browsing)
- take regular backups of important files and test your backup restore/process regularly
- make sure backups are kept separate; if located on USB stick (or a hard drive, or on any type of removable media) do not leave it connected or anywhere on your network, or it may also be attacked by ransomware
- 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 (the Incident Management section of 10 Steps To Cyber Security(/guidance/10-steps-incident-management) may help here)

## What to do if you (or your organisation) has been infected with malware

If your organisation has already been infected with malware, these steps may help limit the impact of the infection.

1. Immediately disconnect the infected computers, laptops or tablets from network.
2. Turn off your Wi-Fi and unplug any ethernet or network carrying cables.
3. Safely format or replace your disk drives and reinstall the OS.
4. Connect the device to a clean network in order to download, install and update the OS and all other software.
5. Install, update, and run antivirus software.
6. Reconnect to your network.
7. Monitor network traffic and run antivirus scans to identify if any infection remains.

**Note**: Files encrypted by most ransomware variants have no way of being decrypted by anyone other than the attacker. Don't waste your time or money on services that are promising 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.

For further advice and guidance following malware infection.

- 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 (https://www.actionfraud.police.uk/).
- The National Cyber Security Centre (NCSC) runs a commercial scheme called Cyber Incident Response(/scheme/cyber-incidents), where certified companies provide crisis support to affected organisations.

- The Cyber Security Information Sharing Partnership (CiSP)(/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.

## Topics

Malware protection(/topics/malware-protection)

### Was this guidance helpful?

We need your feedback to improve this content.

Yes No