

Guide to Malware and Malware Detection

clickandprotect.co

Helping You Build Your Cyber Security



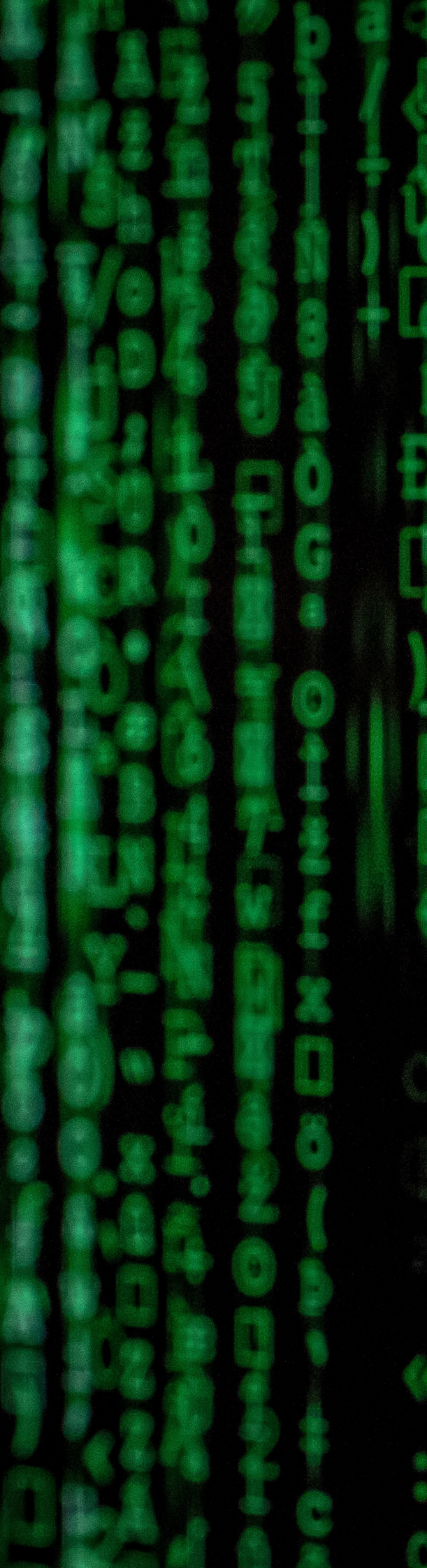


Table of Contents

01	What is malware	Page 1
02	Different kinds of malware	Page 1-2
03	How malware infects your computer	Page 2-3
04	How to tell if your computer has been infected	Page 3
05	What anti-malware programs do	Page 4
06	How malware detection works	Page 5-8
07	How malware is dealt with once identified	Page 8
08	How to prevent malware infection	Page 9
09	Summary and next steps	Page 10

1. What is malware?

Malware is malicious software. This means any software intentionally designed to steal, encrypt, corrupt or delete information. This can be from your computer, other electronic devices or network. Malware can also change the way your system works, without your consent.

Attackers want to do this for a number of reasons, ranging from making money, or sabotaging your business, through to making a political statement or just for fun and bragging rights.

They may want to:

- Steal your personal data.
- Commit identity fraud.
- Steal financial information or other sensitive information.
- Disrupt your business or steal your intellectual property.
- Get control of your computer, along with many others, to launch denial-of-service attacks on other networks or websites.
- Use your computer resources to mine cryptocurrency.



2. What kinds of malware are there?

There are various types of malware and the impact of an infection can range from annoying, to catastrophic for your business. They include:

- Adware, which displays adverts on your screen. These could be innocuous or could themselves contain malware should you click on any of them.
- Spyware, which collects information about you, your device or your network, to send back to the attacker. With this information, the attacker may then be able to commit fraud or identity theft.
- A keylogger records your interaction with your keyboard, and sends it back to the attacker, who is looking for bank details, usernames and passwords.
- Viruses often arrive as email attachments, which once opened, infect your device. They attach themselves to harmless programs, and when triggered by the user (usually inadvertently) they will spread and infect other programs.
- Worms are like viruses, except that they can spread without human intervention.
- Rootkits bury themselves deep in your computer and grant remote administrative access to the attacker. This means that the attacker could do anything that an administrator could do. They could install and hide other malware, steal data, deactivate your security programs, intercept your internet traffic, or create a 'backdoor' so the attacker can come back later.
- Trojans. These programs appear to be harmless or useful programs, but once installed the

- ... attackers can steal valuable information or install other malware, often crypto-jacking software or ransomware.
- Crypto-jacking uses your computer's resources to mine cryptocurrency on behalf of the attacker.
- Ransomware locks you out of your computer or encrypts your data and demands a ransom to restore your access—but there's no guarantee that paying the ransom would give you back your data.

All these types of malware rely on the installation of malicious files on your computer, but there is another type of malware, which is becoming increasingly common: fileless malware.

Fileless malware is not written to disk, but is written to memory (RAM). It uses the trusted software that is already installed on your computer, to create and carry out malicious activity. Because the malware isn't saved as a file on your computer, it doesn't leave behind any traces, making the malware harder to detect.

Fileless malware that is written to memory, stops working when your computer is rebooted but some sophisticated attacks store code deep in device firmware (such as the BIOS), or in a peripheral device (such as a USB), so that the attacks can recur even after a system reboot.

Fileless malware attacks might involve:

- Making changes to your registry.
- Injecting malicious code into the memory of legitimate applications.
- Using macros, which are used in Office applications to automate tasks, to execute tasks with malicious intent.
- Using scripts (that are normally used by system administrators) to load executable files to launch attacks without leaving a footprint.

The intentions of fileless malware are the same as file-based malware, but it is harder to spot and control. It uses trusted tools that are intended for normal day-to-day use by administrators, so it is hard to detect if these are being used for malicious purposes.

3. How does malware infect my computer?

File-based malware infections are typically caused by; someone clicking a link in an email or a fake alert message, visiting a malicious website, inserting an infected USB stick or unintentionally downloading the malware alongside other software. Perhaps from file-sharing services or free software download sites. Once the malware has been downloaded to the user's computer, it will carry out whatever instructions have been encoded within it. Fileless malware uses similar infection techniques. A typical scenario might be an email with a password protected zip file attachment that contains a macro and executes malware and then deletes any files or other traces created in the process. The person receiving the email is persuaded by the content of the email to not only use the password provided in the email, but to enable macros. This persuasion is known as social engineering, similar to typical phishing attacks, and works like this:



- The email pretends to come from an authority, such as HMRC or DVLA, or suggests that the attachment contains sensitive information or embarrassing photos, to persuade the recipient that they should open it.
- When they try to open the attachment, it presents a fake alert, informing the recipient that the attachment was created in an earlier version of the application. This alert looks convincing, and indicates that the user should click 'enable content' to be able to see the document. This, of course, will enable macros, and the cascade of infection begins.

4. How can I tell if my computer has been infected?

Symptoms of malware infection will depend on what the program was intended to do. Sometimes there will be no symptoms at all, but you might notice one or more of the following:

- You may have noticed that your computer has slowed down. This might not indicate malware (there are other reasons why this might happen), but it could be that malware is consuming the available resources and causing the poor performance.
- Your computer is working too hard (you can hear unusual noise from the fan). This usually means that something is using your computer resources intensively—and if it's not you, it might be malware.
- Your computer crashes, won't start or shut down properly, or is otherwise unresponsive. This could be due to malware, but there might be other reasons too, such as a hardware failure.
- Your internet connection may be slower than usual. Check there are no downloads running in the background and no-one gaming or watching videos. If there are no such resource-intensive activities going on, then malware might be using your bandwidth for its own purposes.
- You might be using your data allowance on your mobile device quicker than usual. If you're not doing anything different, malware might be
 - ... using your data allowance for its own purposes
 - Sometimes you'll see additional ads popping up, there might be unexpected extensions added to your browser, or even unexpected programs. This could be due to subsets of malware known as adware or bloatware. These types of malware add unwanted programs to your computer.
 - You might see threat warnings from antivirus programs that you don't recognise. These might be genuine messages from an unwanted program that you didn't intend to install, but was bundled with one that you did want, or the alerts may be trying to get you to click on a dodgy link.
 - Your browser might open websites that you didn't expect or want to visit. These are typically malicious sites and will ask for your personal information, or will add further infections to your computer.
 - Your contacts may be getting spam messages that appear to be from you (but are being sent by malware).
 - Your security programs have been disabled or deleted.
 - You might not be able to get at some files and there might be a warning that your data has been encrypted.

5. What do anti-malware programs do?

Anti-malware programs are intended to perform one or more of the following tasks:

- Prevention of malware infection,
- Detection of infection,
- Removal of infection.

It is important to understand that not all programs can do all of these tasks. The best solution for your business will depend on your circumstances, though you will definitely need some form of anti-malware protection.

Some anti-malware programs are intended to protect single devices (such as a laptop) and some work to defend networks. They typically work in real-time (run all the time in the background), but can also conduct one-off scans as needed.

Note that most free anti-malware programs do not remove infections, but will quarantine them. You may need to buy a removal program in order to remove any infection completely. Also, free software doesn't usually offer all the features of paid-for versions, and won't provide support if you have a problem.

```
window.confirm  
) .fadeOut(35  
trigger("the  
otCheck:func  
.close-full  
view"), render  
.navigate(c.  
l.addClass("  
moveClass("i  
ger("preview  
is.$el.toggl  
w-device",c)  
tr("aria-pre  
disabled")||  
)}}),c.view.  
arentTheme(
```

6. How does malware detection work?

Malware detection techniques are continually evolving as malware becomes more sophisticated and as new technologies appear. There are nine approaches outlined below that you should be aware of...

1 Signature Analysis

Traditionally, malware detection has been based on comparison against known malware. Every piece of software or file has unique characteristics, known as a footprint or signature. The known signatures for malware are recorded in a database. Your anti-malware product will check an incoming file against the set of known malware signatures, to decide whether it is known to be malware or not.

Of course, new malware is developed all the time, so it is important that your product is regularly updated with newly identified signatures. Newer forms of malware try to evade this kind of detection by mutating. Known as polymorphic malware, they can hide from signature-based detection by changing certain features. This is so that they become unrecognisable, even minor changes are enough to do this.

Another way that malware evades detection is by code obfuscation (making it harder to interpret). This is done by compressing the malware code, encrypting it or inserting complex and irrelevant code. Signature-based detection won't work on fileless malware, as there's no file to use for comparison. Another technique is needed, and this is typically behaviour-based analysis.

2 Heuristics, or behaviour-based analysis

Heuristic or behaviour-based analysis looks for unusual activity. It would begin by establishing a baseline of the activity levels that are normal for a particular environment. Then if that activity level changes, it would regard whatever caused the change as a threat.

This type of analysis requires that the initial baseline is indeed normal, and not already distorted by malware. Once working, this type of analysis can detect polymorphic malware where signature-based analysis cannot, because it is searching for the way the malware behaves, rather than for its characteristics. Behaviour based analysis can also help to detect fileless malware, by looking for processes behaving unusually. For example, by executing shell commands, or unexpected deletions of administrative command (bash) history, excessive network communications or privilege escalation.

9 Intelligence sharing

While not a way of protecting your systems immediately, information sharing is a vital part of anti-malware protection. We recognise that not everyone is a cyber security professional, and we don't all have the time for reviewing threat intelligence sources, but keeping up with malware trends, at least at some level, will help you prepare your defences.

Share what you learn about current threats with your colleagues and other connections. For example, consider signing up with CiSP (Cyber Security Information Sharing Partnership), which is a threat sharing service run by NCSC. It provides early warning of cyber threats, the opportunity to learn from others, and access to free network monitoring reports tailored to your organisation's requirements, and access to free network monitoring reports tailored to your organisation's requirements.

7. How is malware dealt with once identified?

Anti-malware tools all work slightly differently, but when your anti-malware tool identifies something as potentially being malware, it will probably either remove it for you, or quarantine it. This is so you can check and decide whether you want to leave it quarantined, restore it (unlikely, but false positives do happen), or delete it.

When a file is quarantined, it is usually moved and renamed, so that it can't be called by another program and executed. It might also be hidden or have its permissions reset, so it can't be opened or executed. It could also be encrypted. In any case, it is extremely unlikely to run once quarantined, and can be regarded as 'safe'.

However, if the malware successfully ran before it was detected, your operating system, applications and data may be corrupted or lost. In this case, it is best to ask for professional help to recover whatever you can.



8. How can I prevent malware infection?

The installation of anti-malware software in whatever combination, needs to be the right one for you and your business. This will go a long way towards protecting you from malware.

However, there is more that you could do to shore up your defences, whether this is by further hardening your environment (strengthening your technical defences), or by developing a strong security culture in your business.

8.1 Hardening your environment

Systems hardening is reducing the security risk, by reducing the ways in which you could be attacked. There are a number of ways in which your system could be hardened; the ones you choose will depend on the scale and needs of your organisation.

Options include:

- Keep your devices secured physically.
- Require strong authentication to gain access to your devices.
- Update software regularly, for all devices: operating system, browsers, applications, extensions and plugins.
- Delete programs or apps that you no longer need (and clean up any devices that are no longer in use too).
- Remove any unnecessary accounts and privileges.
- Prevent unauthorised devices from being plugged into desktops or laptops.
- Consider blocking unauthorised applications and code from running or even being downloaded.
- Consider the installation of a host-based intrusion protection system (HIPS) and/or a network-based intrusion protection system (NIPS). Similar to the HIDS and NIDS discussed above, but these block the threats (P=prevention) as well as detecting them.

8.2 Strengthening your security culture

The purpose of strengthening the security culture of your organisation is to ensure that everyone understands the importance of security and the potential threats, and works to support the security of your business.

This will involve security awareness training for all employees (full-time, part-time, paid or unpaid) and the clear and continuing demonstration of the importance of security from top management. It may also require the creation or review of your security policies.

Most importantly, the awareness training should reinforce suitable user behaviour to help prevent malware attacks:

- Don't open/download attachments from an unknown sender.
- Don't insert unknown mobile storage devices, such as USB sticks that you might find lying about.
- Don't click on suspicious links or popup ads.
- Make sure that macros are disabled in your Office applications.
- Don't download pirated software or software from untrustworthy sites.
- Be wary of unusual domain names or domain name extensions.
- Take backups—this won't prevent an attack but may help you recover from one.

Culture change is a slow process, and will take more than awareness training, but the human firewall—composed of your employees—is a vital component of your security defences.

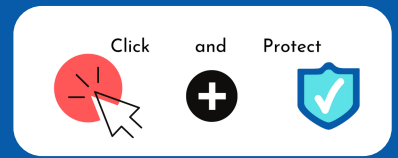
9. Summary and next steps

As long as cyber criminals can make money through malware, the risk to your business will continue to exist. We must make it as difficult as possible for them to succeed, thereby minimising your risk.

In this guide, we have:

- Outlined the different types of malware.
- Explained how malware is injected into your system.
- How to tell if your system has been infected.
- How malware detection works.
- What to do to build strong anti-malware defences for your business through
- Installing appropriate anti-malware software.
- Building your technical cyber security defences.
- Strengthening your security culture.

If you are wondering how best to implement malware protection in your organisation, call Click and Protect on 0113 733 6230 to find out how we can help.



clickandprotect.co
Helping You Build Your
Cyber Security

10. Contact C&P

Email: contactus@clickandprotect.co

Website: www.clickandprotect.co

Tel: 0113 733 6230

LinkedIn: Click and Protect

Facebook: Click and Protect

