

# How to respond to a ransomware attack

## Cyber Fact sheet

Ransomware is a type of malware that restricts access to systems in some way, often by encrypting files and then demanding a ransom to obtain access.

The attacks target both technical and human weaknesses, often combining both to successfully infect a machine. Such attacks can be damaging to businesses of all sizes and the disruption caused by an attack can last for days or even weeks.

Ransomware has grown into a significant industry for criminal enterprises due to its relatively low sophistication and the ability for it to be performed remotely.

In addition, the fact that it is supported by the existence of crypto currencies (typically Bitcoin) which facilitate remuneration, also makes it appealing to cyber criminals. As a result, the likelihood of the perpetrators getting caught is currently extremely low for well executed campaigns.

The malicious code which powers ransomware campaigns denies a user, or organisation, access to their data with the hope that backups don't exist, presenting the target with the dilemma of 'pay and support criminal enterprise in order to get the data back' or 'writing off the data'.

In the past, malware writers were sometimes quite careless and there was often a way to retrieve files. However, writers have improved their capabilities and data retrieval is usually no longer a possibility.

Other forms of ransomware simply lock systems and display messages to try and persuade the user to part with their cash to regain access.

So how does an organisation become infected, what does ransomware actually do, and what can be done to prevent this type of attack?

### Key takeaways


- Prevention is much better than cure when ransomware is concerned.
- Backups are your ultimate defence so don't neglect them.
- Good general cyber hygiene will prevent many attacks.

### How infections occur

Many ransomware attacks are delivered via phishing emails. These are often well crafted and disguised to resemble something non-malicious to fool the recipient.

Phishing emails often take the form of parcel delivery notifications, imaginary customer complaints and/or fake official letters.

A phishing email will either contain an attachment or a link to a malicious website encouraging the user to open a document or click through to a 'drive-by download'. Often the user doesn't realise they are infected until a ransom notification appears.



A “drive-by download” is another common technique used by attackers to install ransomware on a machine. This involves a computer being infected while the user browses the Internet, often through legitimate websites that have already been hacked and modified by an attacker. This method relies on exploiting technical weaknesses such as unpatched or out-of-date software, often in browser plugins such as Flash.

Devices can also become infected when used in an unsafe environment, such as at home or when using a public Wi-Fi connection that is outside the protection of the corporate network, the user has to rely upon local security such as anti-virus or endpoint security controls.

Once the ransomware is installed it needs to ‘call home’ to servers run by the attacker in order to obtain encryption keys. This uses a standard Internet connection and usually relies on websites which have been already hacked so that it can bypass corporate website filtering systems.

Once encryption keys have been obtained, the ransomware then begins encrypting every file, both on the local device and on any connected shared drives like mapped drives. Any files to which the user has access to, can potentially be encrypted if permissions are not appropriately set.

## Getting the basics right

Unfortunately there is no silver bullet and there isn't one piece of software or single solution that can stop this type of attack, despite many vendors' claims.

A successful defence against malicious outsiders trying to gain access to your organisation involves a multi-layered approach, applying robust controls from the strategic to the tactical.

### Backups

Keeping an up-to-date backup of your critical data is essential. Should you get hit by a ransomware attack you have the assurance that in the worst case you can always restore the backups. A word of warning though – don't have your backups on permanently connected network shares as these can also be attacked by ransomware.

### Patch & update

Malware often exploits software weaknesses (vulnerabilities) so updating is still one of the best forms of defence. Every organisation should implement a regular patching process to ensure security resilience. Moving away from legacy, unsupported operating systems such as Windows XP, is essential.

### Use anti-virus & update regularly

Installing up-to-date antivirus on all machines is a vital mechanism for preventing many attacks, including ransomware. It is often advisable to adopt a layered approach, using a different vendor on local machines from that used on servers or email gateways.

### Test & scan

Regular vulnerability scanning will show weaknesses that many attackers could exploit, while penetration testing will give you the full picture of what can be achieved by a malicious outsider.

The general advice of conducting a full and thorough test at least every six months or after any significant change still stands.

### Educate

As malware attacks often rely on exploiting human weaknesses, employee awareness is an effective way of preventing many attacks. Educating users on how to detect phishing attacks is beneficial for both the user and the organisation.

### Restrict access control

Access control is important. Restricting user privileges can limit the extent of the encryption to just the data owned by the affected user.

Check permissions on shared network drives regularly to prevent ransomware spreading to mapped and unmapped drives. System administrators with high levels of access should avoid using their admin accounts for email and web browsing.

## WHAT ABOUT MORE SPECIFIC PREVENTION?

### Backup regularly

Unfortunately ransomware attacks are more often than not successful and the majority of the time the only way to retrieve files is by restoring from the latest backup.

The longer the period between backup and attack, the more painful the result of the malware attack will be, so backup regularly and test data retrieval procedures.

### Lock down permissions

Malware requires permission to execute in order to successfully infect a device. Removing the permission to run new executable files for certain users is a useful mechanism to prevent a piece of malware being loaded on to a machine.

Many users don't require administrator rights, so if they don't need them, don't give them. The same applies to file permissions. The majority of people inside an organisation only need to access files to read them, so lock the permissions down, granting users "read only" privileges by default. If the malware doesn't have permission to write it can't encrypt the files.

### Threat monitoring

In many cases, malware can exist inside an organisation while having not yet made contact with its command and control server (servers run by the attacker) in order to obtain its encryption keys. In this instance, threat monitoring solutions can be useful in detecting and alerting an organisation to its location.

### Software Restriction Policies

Most cases of ransomware are delivered either by a malicious website exploiting vulnerabilities in a web browser, or as an email attachment. Therefore it is essential to restrict access to file system locations from which programmes are likely to be executed. These locations are usually temporary directories used by software such as Internet Explorer, WinZip, WinRAR, or 7-Zip. Software Restriction Policies (SRP) are a feature introduced in Windows XP and Server 2003, allowing users and domain administrators to control the ability of programmes to execute.

## Frequently asked questions

### Can ransomware spread?

Ransomware doesn't usually spread in the same way as some other malware does but malicious emails could be forwarded unintentionally by users not understanding what the attachment is.

For example, if a user receives an email and then forwards the email to a group, every member of the group who opens the attachment will become infected with the ransomware.

The end result could be that many hundreds or thousands of files become encrypted.


### Do ransomware removal tools, work?

Anti-virus vendors offer tools that can get rid of the malware itself, but these will not usually decrypt your files if they have already been encrypted.

For many modern ransomware variants there is no way to decrypt files without paying the ransom. Be careful of claims suggesting that a downloadable tool can unencrypt your files. Any tool that claims this could itself be malware and you could end making the problem worse.

### Should I pay?

Paying the ransom to recover data funds further criminal activity and provides a viable market for criminals to operate within.



Payment may also leave victims open to future extortion and does not guarantee that data will be recovered. NCC Group recommends that companies should not pay any ransom.

Microsoft also advises against paying ransoms. It stated: "We recommend that you do not pay the ransom. There is no guarantee that paying the ransom will return your PC to a usable state."<sup>1</sup>

The UK's National Crime Agency (NCA) also suggests the same thing. It stated: "The NCA would never endorse the payment of a ransom to criminals and there is no guarantee that they would honour the payments in any event."<sup>2</sup>

### **If I have recovered the files from backup and removed the malware correctly is there anything else I should do?**

It is important to remember that sometimes the malware may have been installed elsewhere in the organisation, or perhaps an email has been forwarded onto someone else who may not yet have opened the file (perhaps someone on leave).

Ensuring that there is no further malware on the network is vital for avoiding further outbreaks.

1 <https://www.nccgroup.trust/uk/our-research/ransomware-what-organisations-can-do-to-survive/>

2 <http://www.nationalcrimeagency.gov.uk/news/256-alert-mass-spamming-event-targeting-uk-computer-users>