PROTECTING FROM RANSOMWARE

Ransomware attacks are becoming increasingly common, with attackers using more sophisticated methods to try and get their hands on your data. This guide looks at how ransomware attacks happen and recommends steps you and your IT provider can take to help protect you or your business.

Ransomware is a type of malicious software that makes your computer or files unusable if it gets into your device. Like most cyber attacks, ransomware can be financially motivated and you may be asked to pay a ransom.

Attackers often target a business and set the ransom demand based on what they believe the business would be willing to pay to recover their encrypted data.

PaCSON does not recommend paying the ransom. It will not guarantee your files will be returned and it can make you a target for further attacks. Paying the ransom can encourage the activity and further attacks on you or other businesses.

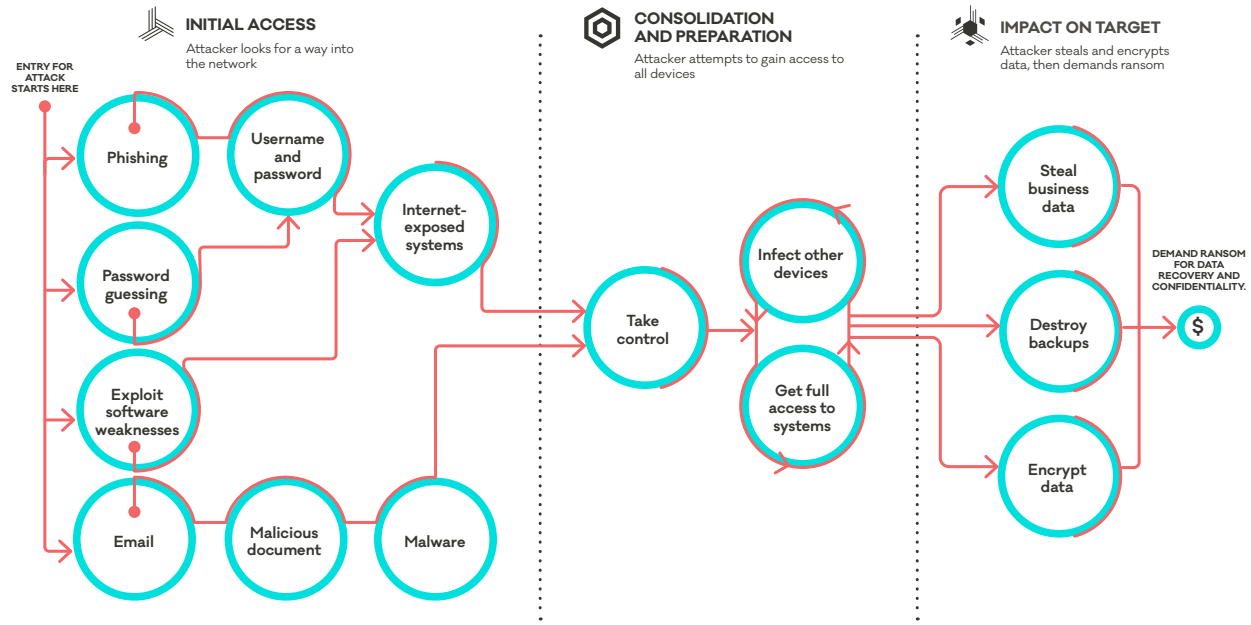
There is no guarantee that paying the ransom will result in the attacker providing you with an unlock key or protection from future attacks.

Although there are different types of ransomware, most attacks follow one of a few predictable pathways. The upside of this means there are preventative steps all businesses can take to protect from an attack. These steps act as roadblocks that we call *security controls*. These controls can be as simple as applying software updates or turning on two-factor authentication (2FA).

The diagrams below outline different ransomware attack pathways and illustrate where relevant security controls work to protect or stop an attack.

The common attack paths of a human-operated ransomware incident based on examples CERT NZ has seen.

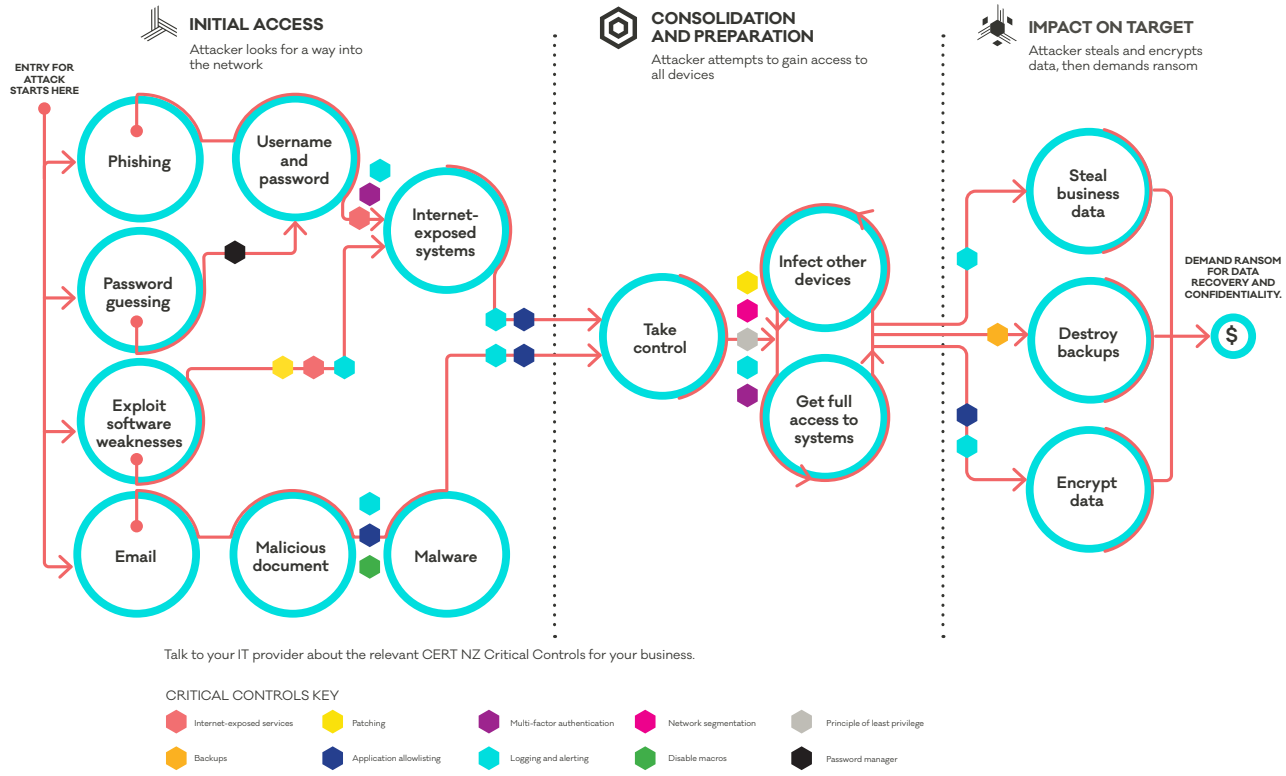
HOW RANSOMWARE WORKS



Working from left to right the attacker starts with one of the four entry for attack channels and follows the pathway across until it reaches a point where it can demand a ransom. We break these down step by step.

Defending against ransomware doesn't need to be complicated. By analysing the pathways that attackers follow, we have shown which security controls stop a ransomware attack. No single tool or control can be relied on stop all attacks, but in combination these controls put you in a good position to protect against any attack (not just ransomware) you are likely to face.

HOW TO PROTECT YOUR BUSINESS AGAINST A RANSOMWARE ATTACK



There are lots of points where security controls can stop an attack. When combined you create a strong defence that can protect you against a variety of cyber security incidents—no matter how it starts or what the end goal of the attacker is. Some of these controls might be easy for you to do, for example applying regular updates on all your devices. Others may require support from an IT provider.

By using this diagram you can step through the pathways and discuss with an IT provider how to implement the relevant security controls for your business and know what sorts of questions to ask.

One security control that appears a lot along the pathway is logging and alerting. This is because the first step in responding to a security incident is being able to detect it and investigate. Having good logging and alerting is one of the key ways that your IT provider can spot something happening before it gets too serious.

INITIAL ACCESS

In the initial access phase an attacker is trying to find a way into your computer networks and systems. The most common ways the attackers get in are:

- getting usernames and passwords to log in to your computer,
- exploiting weaknesses in systems that are exposed to the internet such as email or remote access systems, and
- sending malware via malicious email attachments.

By making these methods more difficult, you reduce the likelihood of an attacker being able to get onto your computers and carry out their attack. The best place to stop an attack is before it begins. Here's how you can stop each of those methods.

1. Attackers use phishing or password guessing to get valid username and password combinations and use that information to log in to systems such as email or remote access systems. To protect against an attacker logging in to your remote access system, use long, strong, unique passwords and turn on 2FA. This will make it very difficult for an attacker to get access.
2. By keeping all your operating systems and software up-to-date you limit the number of weaknesses an attacker could exploit to gain access to your computers. You should identify any systems that might be exposed to the internet and lock these down; you might need some help from an IT provider to do this. Internet-exposed systems are much easier for an attacker to access so having your internet firewall blocking that access helps keep you safe.
3. The other common thing attackers might try is sending a document or spreadsheet that, if opened, will try to load malware onto your computer without you knowing. Stopping the attack here can be achieved by using modern endpoint protection software, for example your IT provider might talk about Endpoint Detection and Response (EDR) tools they support. This replaces traditional anti-virus software and is better suited to stopping these modern threats.

CONSOLIDATION AND PREPARATION

In this phase the attacker will look to move from the initial computer they compromised, and gain administrative access to all the computers and devices in your business.

Taking control is where an attacker will load malware on to the compromised device. This allows them to maintain their access (for example, if you reboot the computer), and issues commands for the computer to access other devices in your network. Once again EDR tools are one of the best defences to stop the attack.

The principle of least privilege is the securest approach. It gives people access to only what they need to perform their job. Enacting this practice might help defend against a ransomware attack spreading too far within your network.

Once the attacker has established their ability to take control and deploy additional malware, they look to expand their access and gain full administrative access to all the devices in your network. Locking down use of administrative accounts as well as using network controls like firewalls can help you stop an attacker from being able to move from one device to another. Limiting the attacker to only a subset of your business devices can limit the damage and might allow you to keep operating even if some of the devices have been encrypted.

IMPACT ON TARGET

At this phase the attacker has gained access to the different systems in your business and is now ready to carry out the most damaging part of the attack.

Attackers will often steal sensitive data and demand payment in order to not release or sell that information. They may also delete backup copies of your data and finally, encrypt your data and systems to disrupt your operations.

If you have good logging on your network infrastructure (for example, firewall), you might be able to detect data being copied out of your network which could be a sign of malicious activity.

To get your business back up and running quickly it's important to have robust and tested backups. These should be kept offline and/or disconnected from your computers so that an attacker can't delete them.

Regularly backing up your data is a simple but important precautionary measure. It means that your information is accessible in case it's ever lost, stolen or damaged through a ransomware attack. Testing your backups to make sure they're working is recommended.

Just as important as protecting your network from attacks is being prepared to recover from one if it occurs. The best way to prepare to deal with a ransomware incident is having an incident response plan, to detail what to do when things have gone wrong and your computers aren't working. The plan should include items such as coordinating the response, investigating the incident, communicating with staff and stakeholders and managing business as usual. Keep a printed copy of this along with key contacts so you have it to refer to even if your business documents have been encrypted.

TIP: *The No More Ransom Project has keys for some (but not all) commonly used ransomware. It allows you to upload a file to determine the ransomware variant.*

Do not upload a file containing sensitive information. For more information on the No More Ransom Project visit ***www.nomoreransom.org/***

If you think you or your business has been impacted by ransomware, please report it to your local PaCSON member. Find more information on how to do that by visiting this webpage: (https://pacson.org/members)

For IT specialists, you can find more detailed information about the security steps to block each ransomware pathway on the CERT NZ website. https://www.cert.govt.nz/it-specialists/guides/how-ransomware-happens-and-how-to-stop-it/

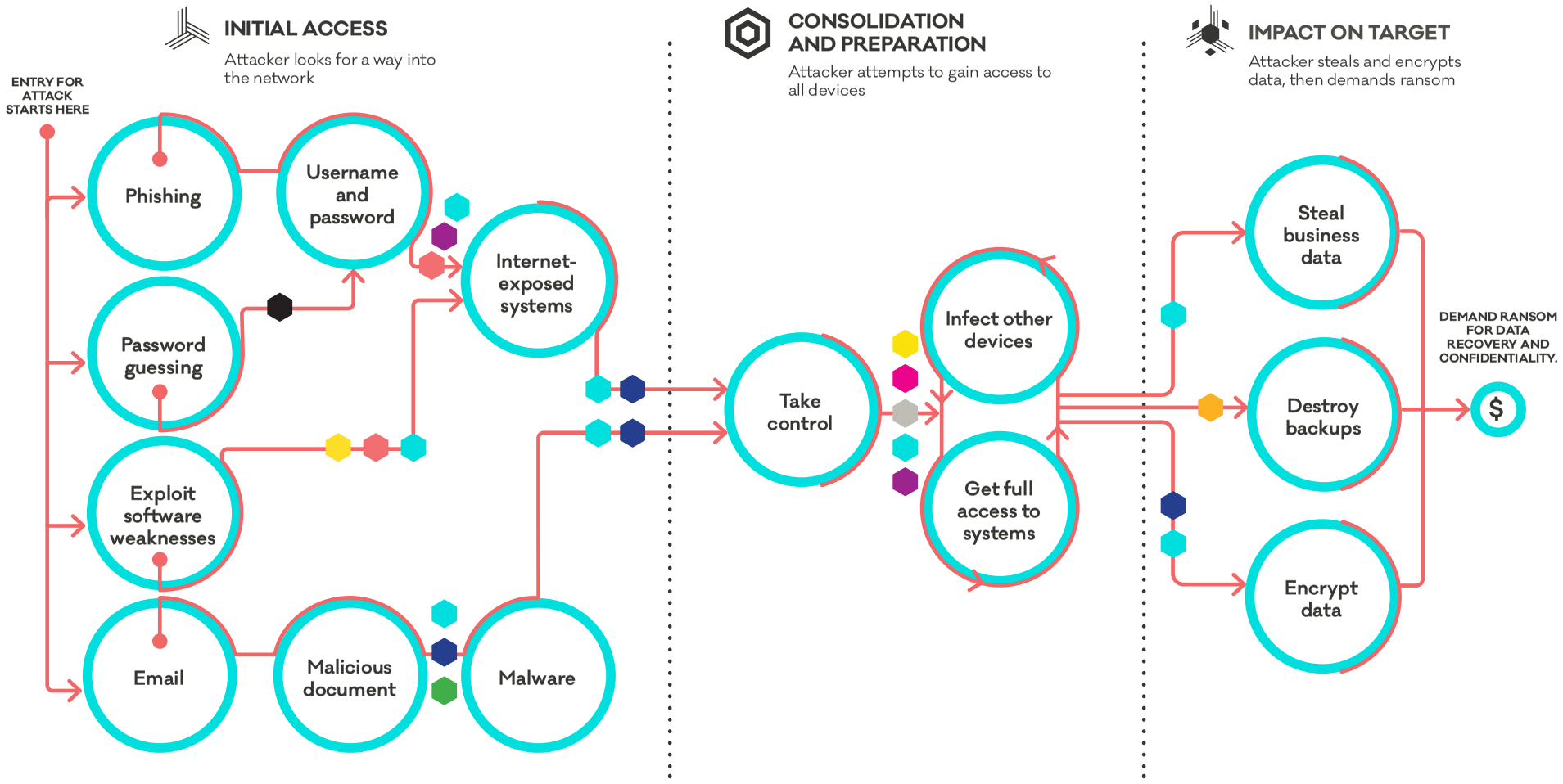
Further resources on logging and alerts; password security; preparing an incident response plan; and more are available on the CERT NZ website: https://www.cert.govt.nz/business/guides/.

CYBER SMART PACIFIC ///

HOW RANSOMWARE WORKS

certnz

How you can protect your business against a ransomware attack.



Talk to your IT provider about the relevant CERT NZ Critical Controls for your business.

CRITICAL CONTROLS KEY

- Internet-exposed services
- Patching
- Multi-factor authentication
- Network segmentation
- Principle of least privilege
- Backups
- Application allowlisting
- Logging and alerting
- Disable macros
- Password manager