30 April 2024

The webinar will start shortly…

own
your
online

certnz

30 April 2024

Own Your Online

Protecting your organisation against ransomware

own your online

certnz

Who are we?

Sam Leggett

Senior Analyst

Threat and Incident Response

Hadyn Green

Senior Advisor

Engagement, Communications and Partnerships

About CERT NZ

CERT NZ is a government cyber security agency. We help individuals and small businesses.

CERT NZ provides incident response for people and businesses affected by cyber incidents.

CERT NZ’s Own Your Online website has easy to understand resources and guides to help build cyber resilience for all New Zealanders.

Today's agenda

- What is ransomware?
- The phases of a ransomware lifecycle:

  1. How attackers get in
  2. What they do once inside
  3. The impacts caused by attackers.

- Controls you can implement to prevent ransomware.

What is ransomware?

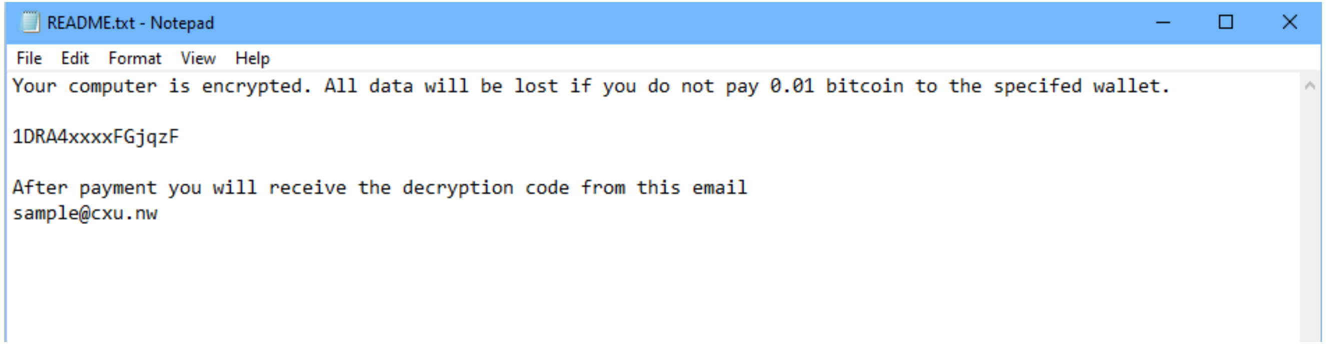
A type of malicious software designed to lock files or computer systems unless a ransom is paid.

Attackers will:

- target systems that have open avenues for attack,
- block access to systems and files that are critical to running a business,
- demand payment, often in cryptocurrency, and
- threaten to leak data if their demands are not met.

How will you know if it’s happened to you?

- You won’t be able to access your desktop, apps or files.
- You get a message telling you that you need to pay a ransom to get access back.
- The message might be a text file, application window or email.



```
Your computer is encrypted. All data will be lost if you do not pay 0.01 bitcoin to the specifed wallet.

1DRA4xxxxFGjqzF

After payment you will receive the decryption code from this email
sample@cxu.nw
```

What should you do next?

- Contact your IT provider immediately.
- Get your network offline as quickly as possible.
- Restore your system from the most recent backup.
- Check to see if you have ‘real’ ransomware.
- Report to CERT NZ: https://www.cert.govt.nz/individuals/report-an-issue/

Should you pay a ransom?

It is ultimately your call about whether you pay a ransom but consider the following:

- The New Zealand government recommends against paying ransoms.
- Paying doesn’t guarantee you’ll get your data or systems back.
- In some instances, once paid, attackers may ask for more money.
- Paying could expose you to future attacks, as the attackers know you will pay.
- Paying creates a financial incentive for online criminals.

What can you do to prepare and protect against ransomware?

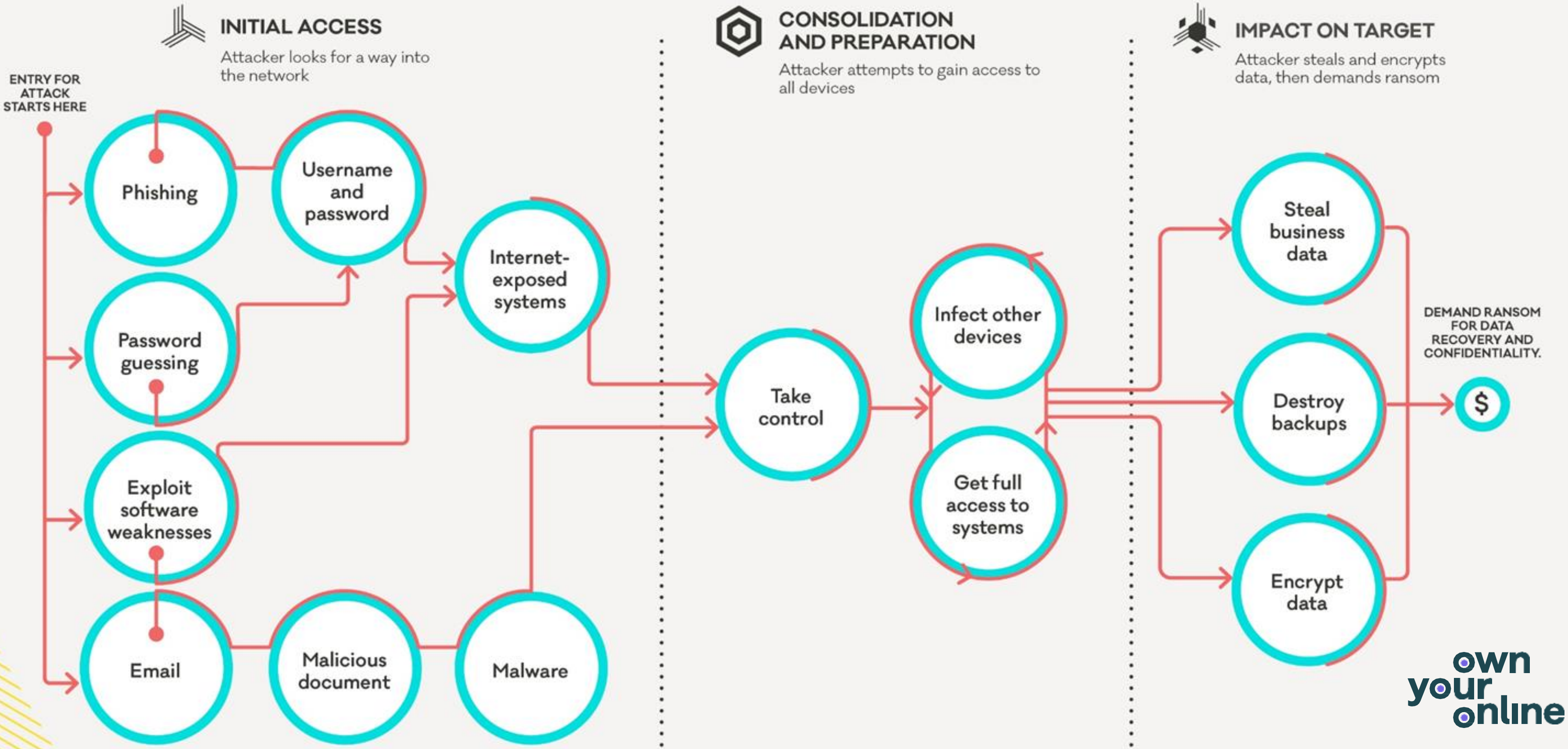
- Think ahead and have an incident response plan.
- Build cyber security awareness within your organisation.
- Implement controls to prevent or limit the damage caused by ransomware.

own your online

certnz

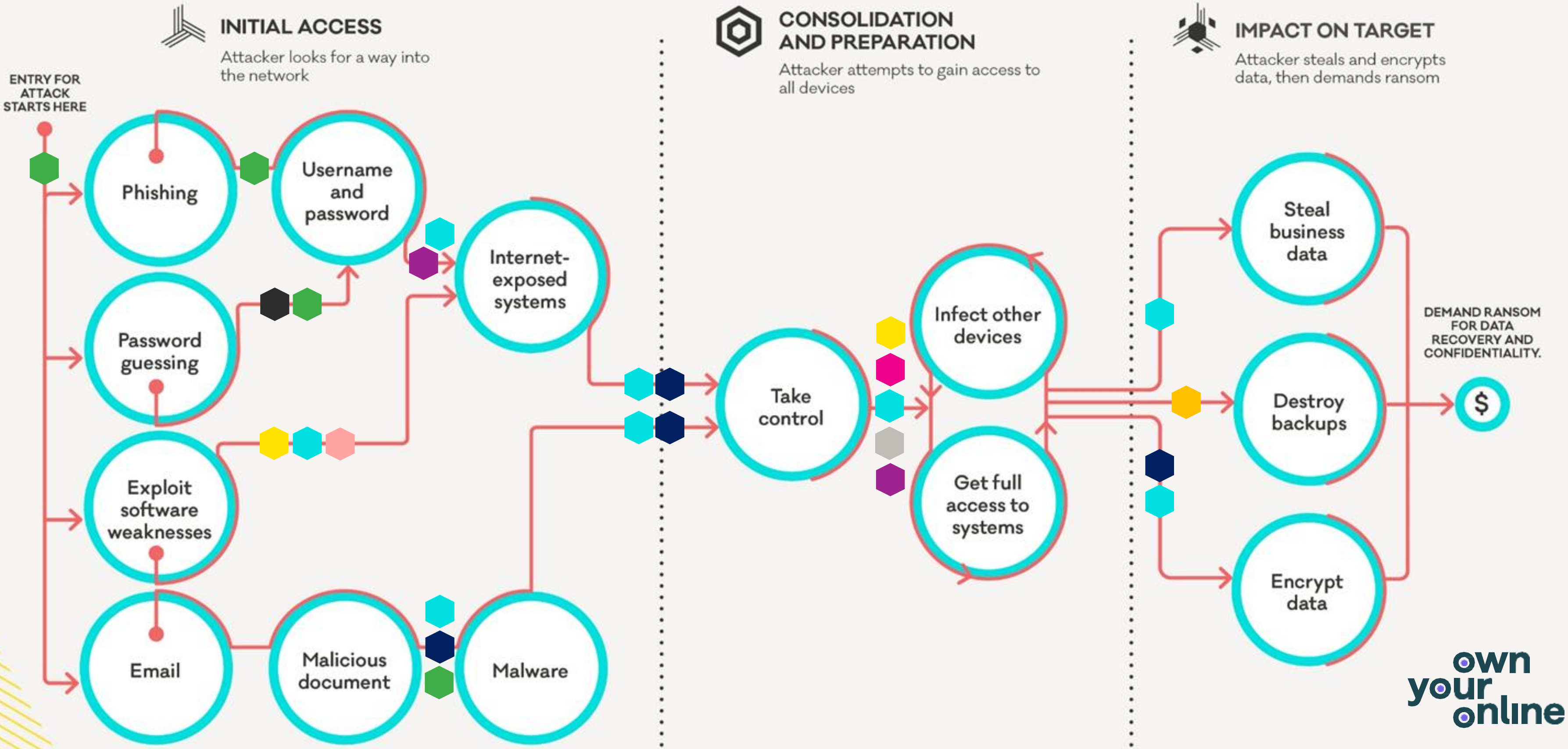
HOW RANSOMWARE WORKS

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


INITIAL ACCESS
Attacker looks for a way into the network
CONSOLIDATION AND PREPARATION
Attacker attempts to gain access to all devices
IMPACT ON TARGET
Attacker steals and encrypts data, then demands ransom
ENTRY FOR ATTACK STARTS HERE
Phishing
Username and password
Password guessing
Internet-exposed systems
Exploit software weaknesses
Email
Malicious document
Malware
Take control
Infect other devices
Get full access to systems
Steal business data
Destroy backups
Encrypt data
DEMAND RANSOM FOR DATA RECOVERY AND CONFIDENTIALITY.
$

HOW RANSOMWARE WORKS

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

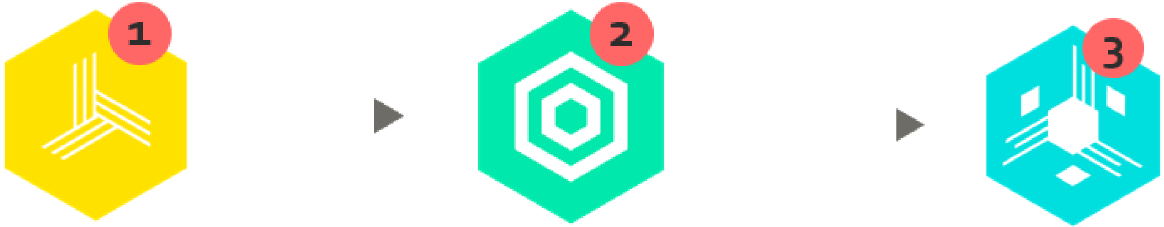

INITIAL ACCESS
Attacker looks for a way into the network
ENTRY FOR ATTACK STARTS HERE
Phishing
Username and password
Password guessing
Internet-exposed systems
Exploit software weaknesses
Email
Malicious document
Malware
CONSOLIDATION AND PREPARATION
Attacker attempts to gain access to all devices
Take control
Infect other devices
Get full access to systems
IMPACT ON TARGET
Attacker steals and encrypts data, then demands ransom
Steal business data
Destroy backups
Encrypt data
DEMAND RANSOM FOR DATA RECOVERY AND CONFIDENTIALITY.
$

CERT NZ's 10 critical controls

These controls would mitigate nearly every cyber incident reported to CERT NZ.

- Patch software and systems
- Implement multi-factor authentication
- Provide and use a password manager
- Centralised logging
- Asset lifecycle management
- Security awareness building
- Implement and test backups
- Implement network segmentation
- Implement application control
- Enforce the principle of least privilege

Three phases of a ransomware attack

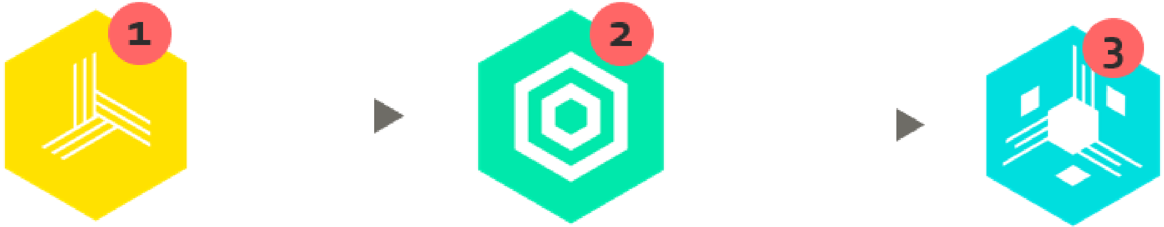


Initial access

Consolidation and preparation

Impact on target

Phase 1: initial access



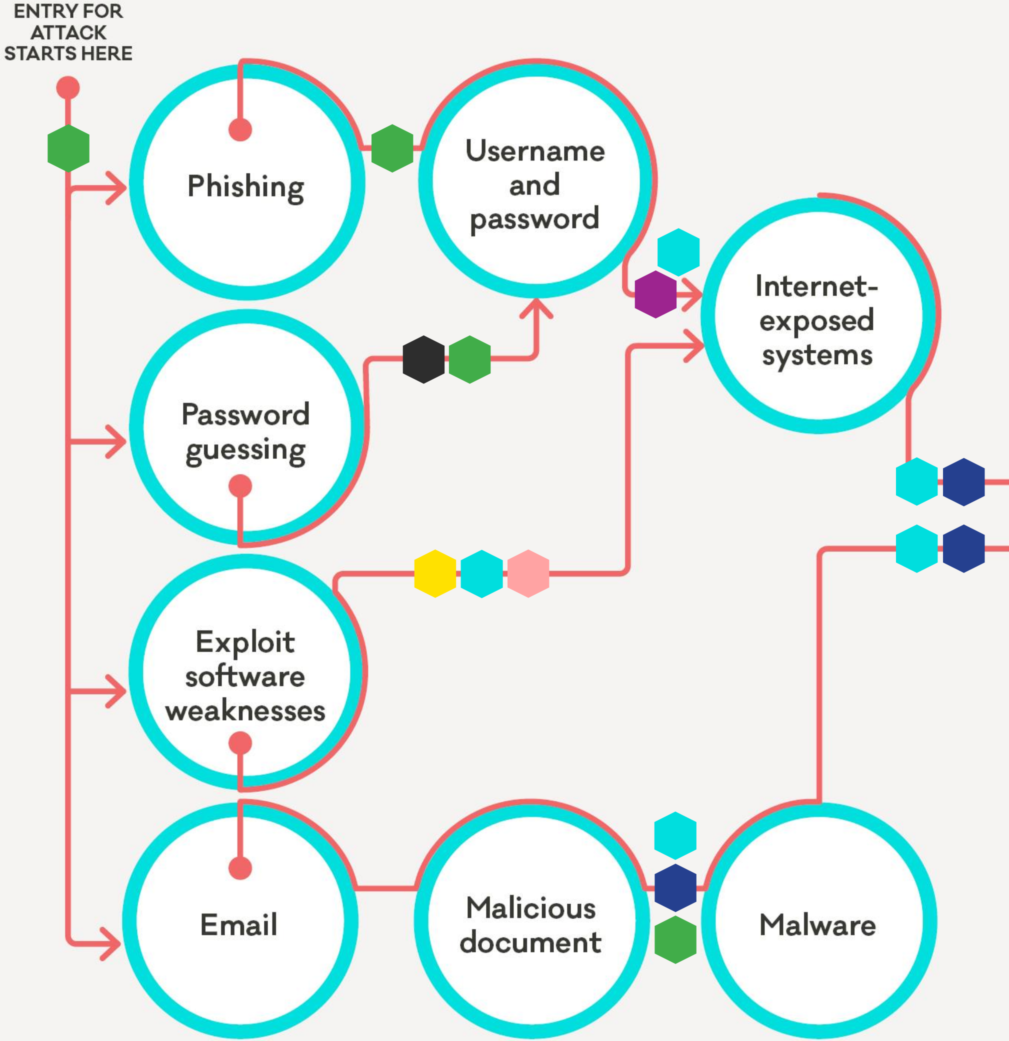
Initial access

Consolidation and preparation

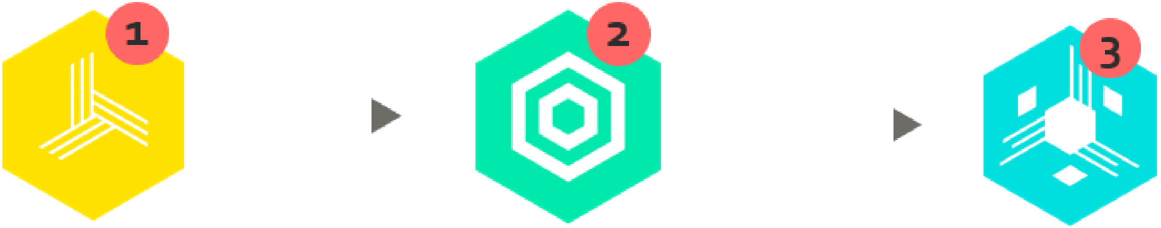
Impact on target

INITIAL ACCESS

- ⬢ Security awareness building
- ⬢ Password manager
- ⬢ Centralised logging
- ⬢ Application control
- ⬢ Multi-factor authentication
- ⬢ Patching
- ⬢ Asset lifecycle management



Phase 2: consolidation and preparation



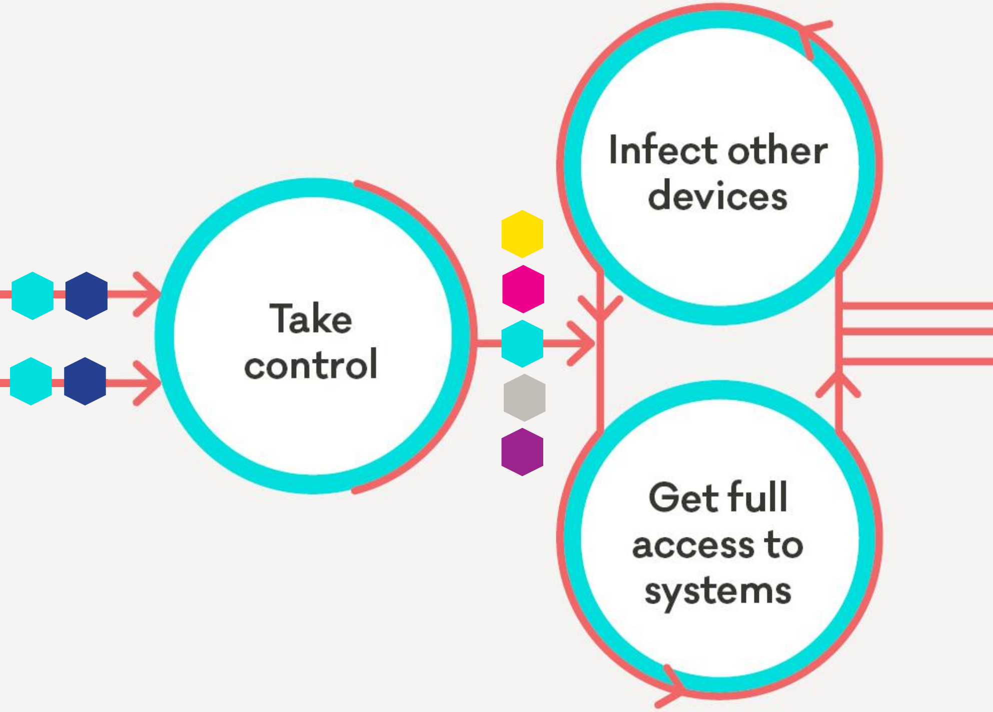
Initial access

Consolidation and preparation

Impact on target

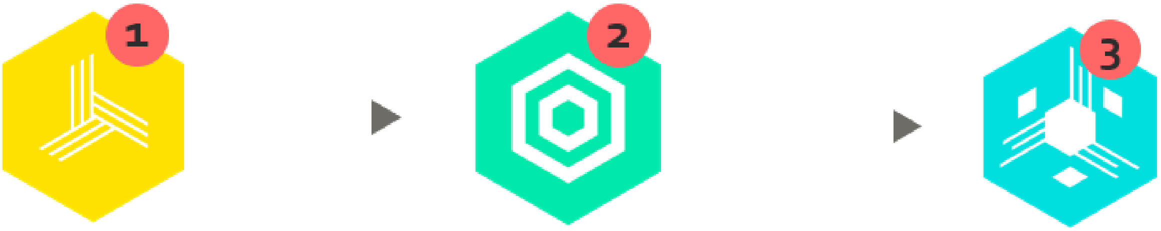
CONSOLIDATION & PREPARATION

- ⬢ Centralised logging
- ⬢ Application control



- ⬢ Patching
- ⬢ Network segmentation
- ⬢ Principle of least privilege
- ⬢ Multi-factor Authentication (MFA)

Phase 3: impact on target



Initial access

Consolidation and preparation

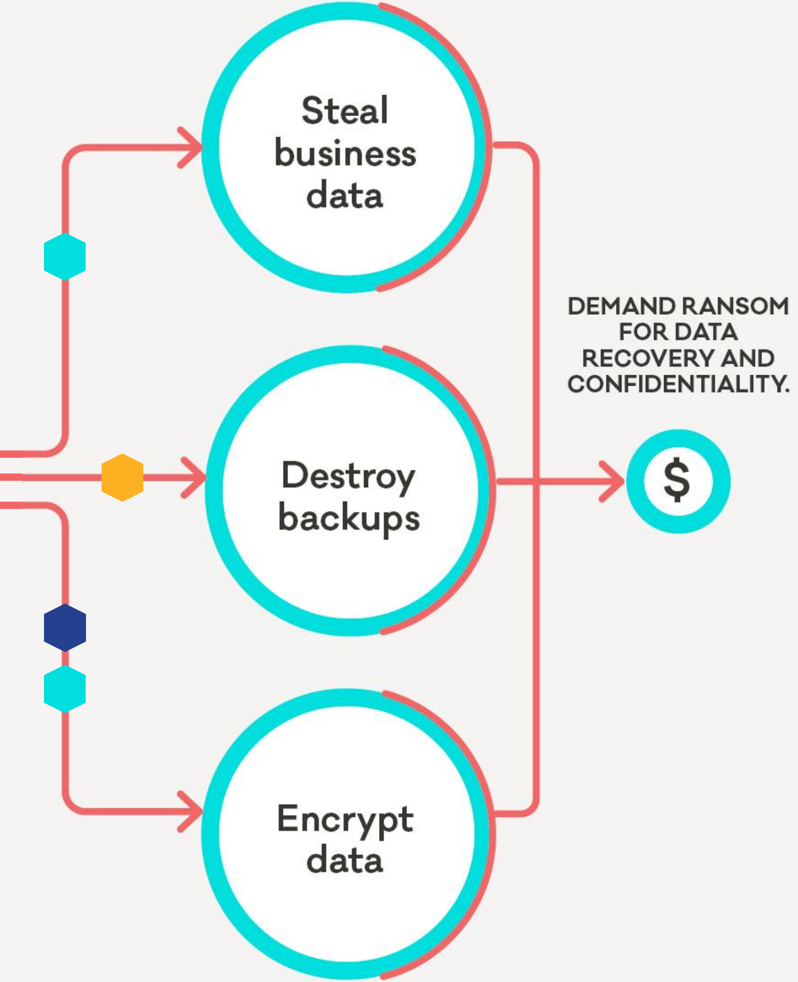
Impact on target

IMPACT ON TARGET

⬢ Centralised logging

⬢ Application control

⬢ Backups



Recap of today's content

- Ransomware can have a devastating impact on an organisation.
- There are numerous controls which can stop or limit the impact of ransomware across the three phases of its lifecycle.
- Implementing even a few controls will significantly improve your security against the risk of ransomware.

Key takeaway

Two-factor authentication is one of the most powerful controls against ransomware. Specifically in preventing the initial access.

Backups are the most important control when it comes to recovering for a ransomware attack.

Additional resources

Find more information about ransomware here:

https://www.ownyouronline.govt.nz/business/know-the-risks/common-risks-and-threats-for-business/businesses-and-ransomware/

https://www.ownyouronline.govt.nz/business/get-protected/guides/protect-your-business-against-ransomware/

All the links:

CERT NZ Critical Controls

When correctly implemented, these controls would prevent, detect, or contain the majority of the attacks we've seen in the past year.
https://www.cert.govt.nz/it-specialists/critical-controls/10-critical-controls/

Incident response plan

An incident response plan is a step-by-step guide that documents who will do what, if a cyber security incident occurs.
https://www.ownyouronline.govt.nz/business/get-protected/guides/create-an-incident-response

Reporting

Report online incidents to CERT NZ at www.cert.govt.nz/individuals/report-an-issue/

Technical diagram

Common attack paths of a human-operated ransomware incident https://www.cert.govt.nz/it-specialists/guides/how-ransomware-happens-and-how-to-stop-it/

Thanks for your time

Sam Leggett & Hadyn Green

0800 CERT NZ

info@cert.govt.nz

www.cert.govt.nz

www.ownyouronline.govt.nz/business

own
your
online

certnz