LIFECYCLE OF A RANSOMWARE INCIDENT

cert nz

How the CERT NZ Critical Controls can help you stop a ransomware attack in its tracks.

INITIAL ACCESS
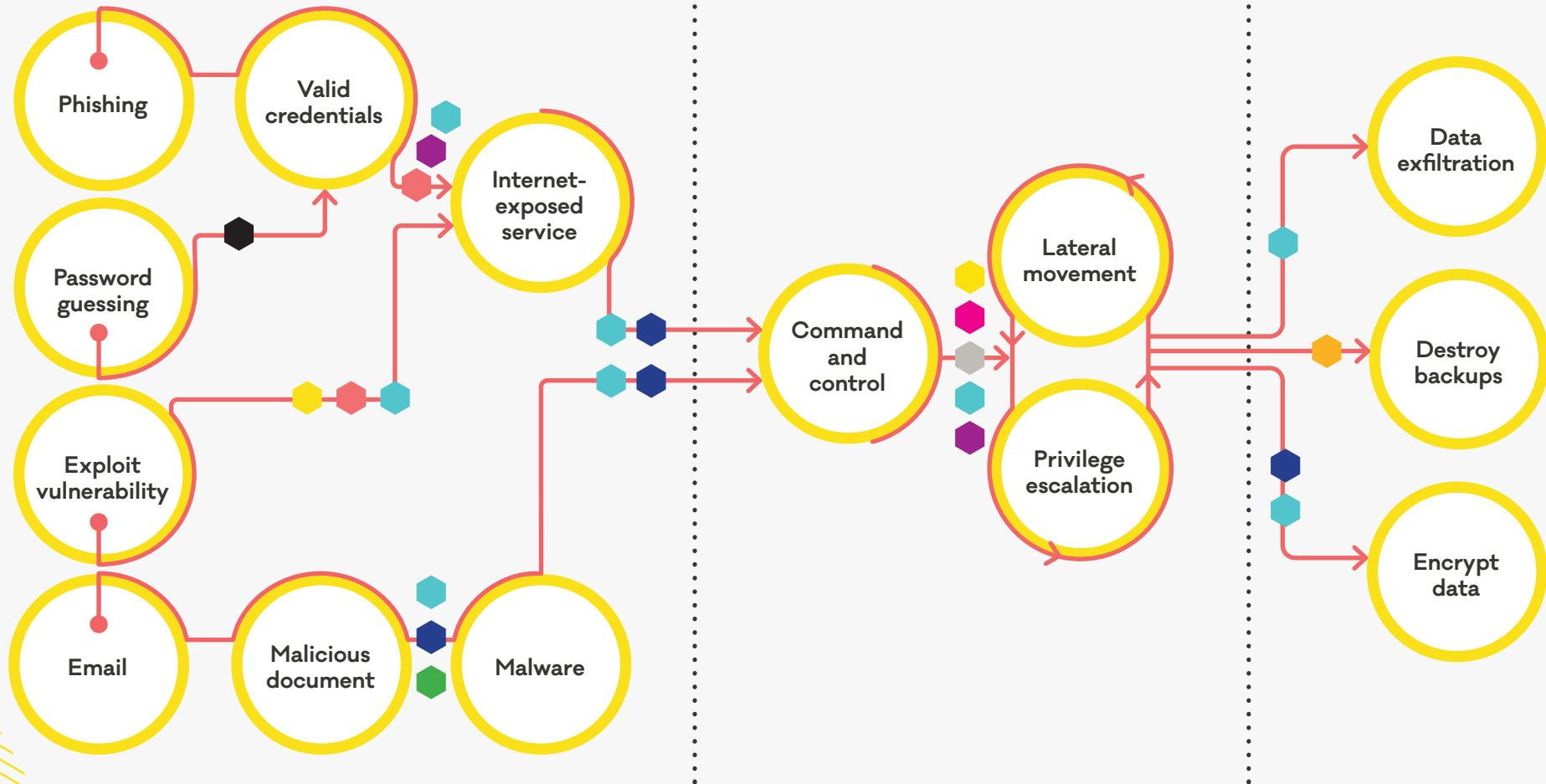Attacker looks for a way into the network

CONSOLIDATION AND PREPARATION
Attacker attempts to gain access to all devices

IMPACT ON TARGET
Attacker steals and encrypts data, then demands ransom

- Phishing
- Valid credentials
- Internet-exposed service
- Password guessing
- Exploit vulnerability
- Email
- Malicious document
- Malware
- Command and control
- Lateral movement
- Privilege escalation
- Data exfiltration
- Destroy backups
- Encrypt data

CRITICAL CONTROLS KEY

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

New Zealand Government