LIFECYCLE OF A RANSOMWARE INCIDENT

certnz

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

INITIAL ACCESS

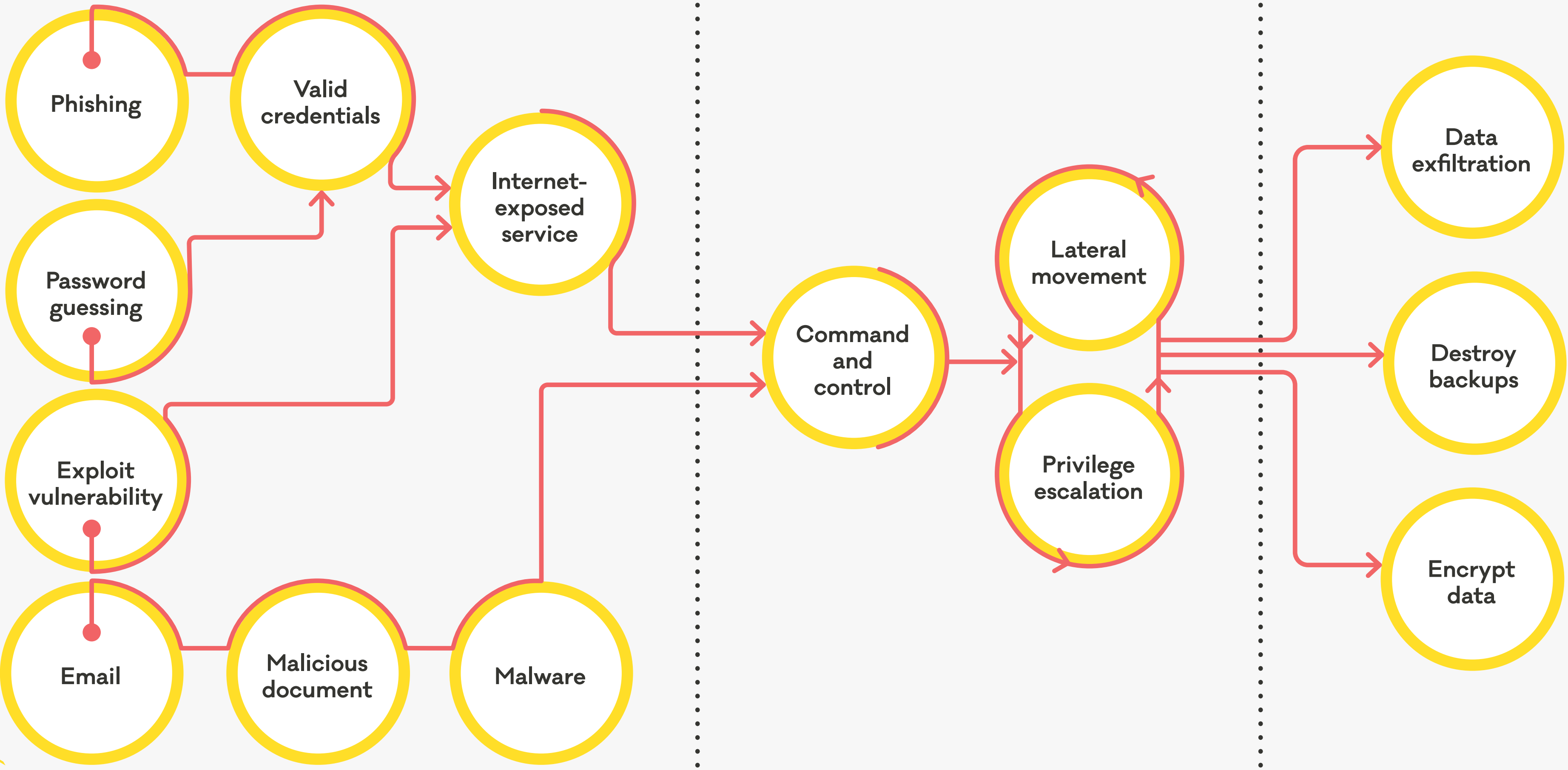
Attacker looks for a way into the network

CONSOLIDATION AND PREPARATION

Attacker attempts to gain access to all devices

IMPACT ON TARGET

Attacker steals and encrypts data, then demands ransom



New Zealand Government

LIFECYCLE OF A RANSOMWARE INCIDENT

certnz

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

INITIAL ACCESS

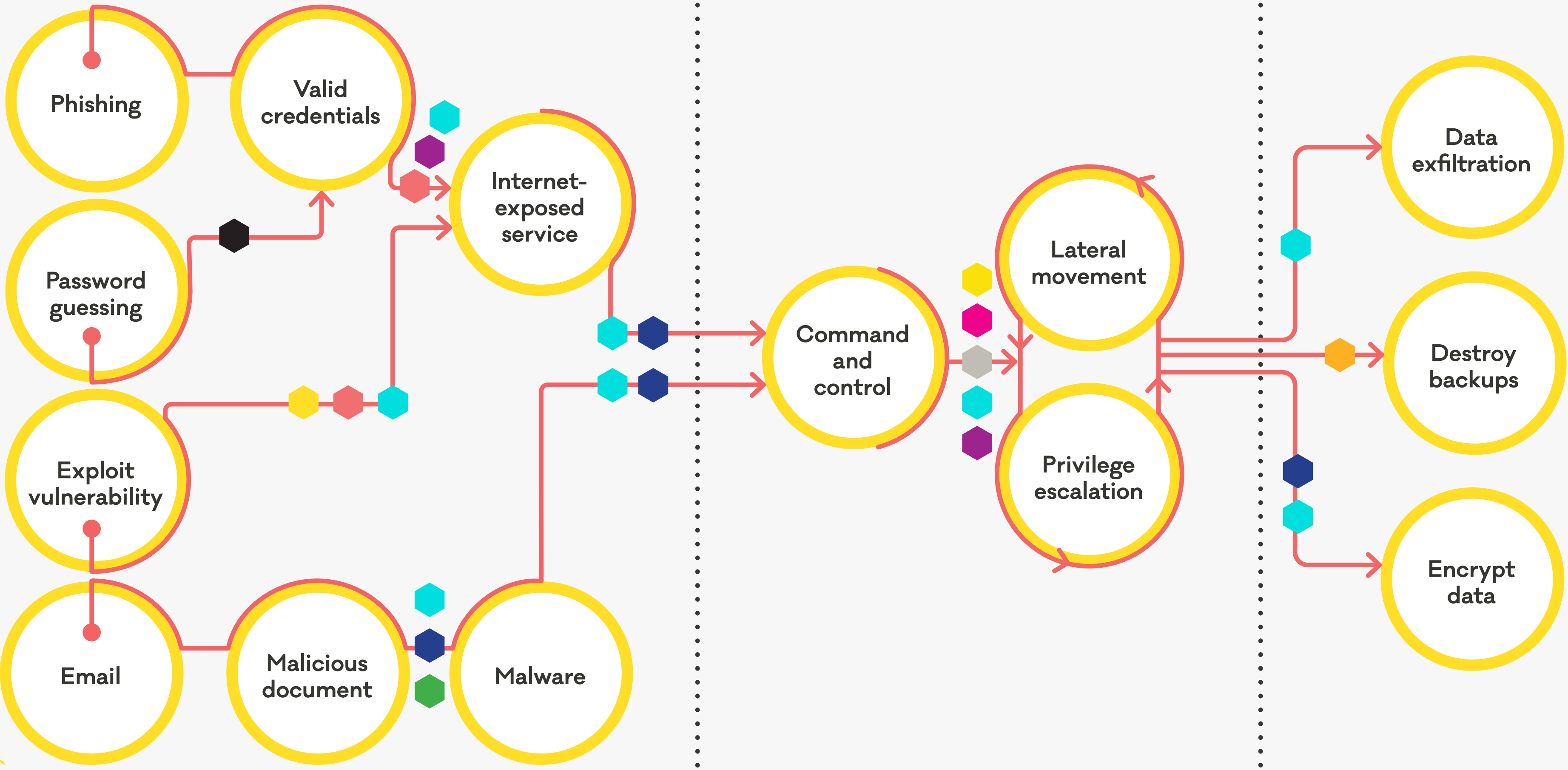
Attacker looks for a way into the network

CONSOLIDATION AND PREPARATION

Attacker attempts to gain access to all devices

IMPACT ON TARGET

Attacker steals and encrypts data, then demands ransom



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