LIFECYCLE OF A RANSOMWARE INCIDENT

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

certnz

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