VERSIVO

ACTIVE CYBER DEFENSE

Anatomy of a targeted Cyber attack

Cybersecurity from the Attacker's point of view

www.versivo.it

Rocco Sicilia

Cyber Security Consultant

Ethical Hacker

CISO*

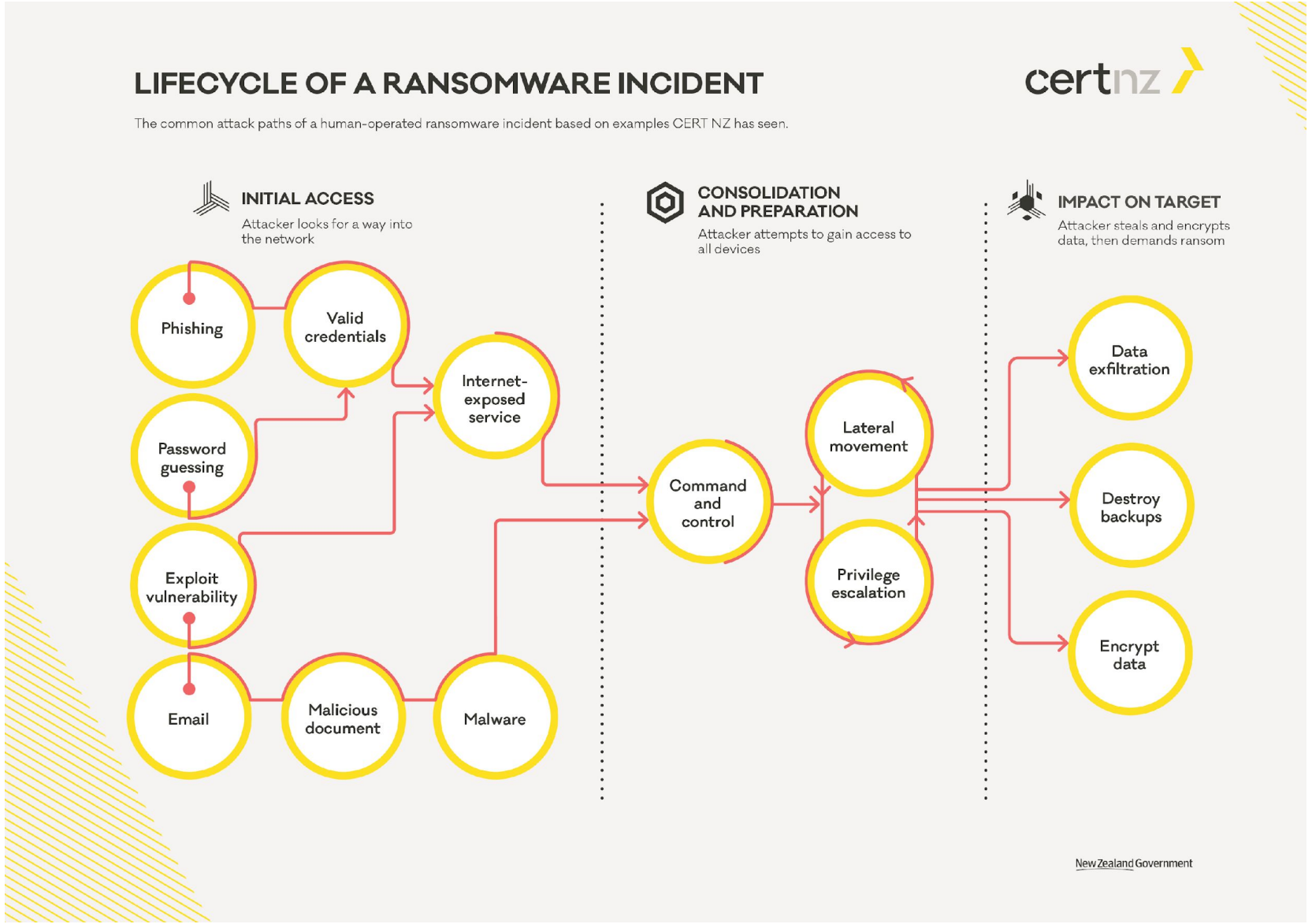
https://www.linkedin.com/in/roccosicilia/

@roccosicilia

Cyber Attack Phases

VERSIVO
ACTIVE CYBER DEFENSE

Cyber Attack Phases



INSPIRED BY TRUE STORIES

BANKING SCAM

VERSIVO
ACTIVE CYBER DEFENSE

Inspired by a true story: banking scam

- Organization reports a successful banking scam.
- Customer affirms that an authentic email has been sent from the key account manager.

Evidence (from the DFIR report):

- KAM email delivered to the customer is **authentic**.
- **Unauthorized access** to the KAM email account has been detected.
- **Personal KAM email** is included in «have i been pwned».
- No **MFA** is configured.

VERSIVO
ACTIVE CYBER DEFENSE

Inspired by a true story: banking scam

Speculation:

- KAM **re-uses mnemonic passwords** for personal and work accounts.
- Attacker, targeting the organization, conducted an analysis through social networks (LinkedIn), and **past data breaches**.
- Attacker found a **valid account** (the KAM one).
- Attacker **analyzed past email conversations** and waited for the best «time window»
- Attacker sends an authentic email requesting a bank transfer using a different IBAN (**evidence**).
- Attacker **sells collected data** on dark web marketplaces.

VERSIVO
ACTIVE CYBER DEFENSE

Inspired by a true story: banking scam

MITRE ATT&CK™

Techniques:

- T1589 Gather Victim Identity Information
  - 0001 Credentials -> T1110.0001
  - 0002 Email Addresses -> RocketReach
  - 0003 Employee Names -> LinkedIn, RocketReach
- T1591 Gather Victim Org Information
  - 0002 Business Relationships -> LinkedIn
  - 0004 Identify Roles -> LinkedIn
- T1110 Brute Force
  - 0001 Credential Stuffing

VERSIVO
ACTIVE CYBER DEFENSE

Inspired by a true story: banking scam

Remediation plan:

- MFA
- Policies and contracts
- Awareness

SPEAR PHISHING

VERSIVO
ACTIVE CYBER DEFENSE

Inspired by a true story: spear phishing

- Organization reports highly targeted malicious emails delivered to several critical employees and customers.

Evidence (from the DFIR report):

- Minor email account has been compromised.
- **One-touch MFA** was configured.
- Targeted user accepted a login request.

Inspired by a true story: spear phishing

Speculation:

- The attacker **known the password** associated to the compromised email account.
- The attacker **collected interesting information** from the compromised email account (conversations, address book, enterprise contacts, public folders…)
- The attacker used that information to launch highly targeted attacks to **VIP** (employees and customers).

Inspired by a true story: spear phishing

MITRE ATT&CK™

Techniques:

- T1589 Gather Victim Identity Information
  - 0001 Credentials -> T1110.0001
  - 0002 Email Addresses -> RocketReach
- T1110 Brute Force
  - 0001 Credential Stuffing
- T1621 Multi-Factor Authentication Request Generation
- T1566 Phishing
  - 002 Spearphishing Link

VERSIVO
ACTIVE CYBER DEFENSE

Inspired by a true story: spear phishing

Remediation plan:

- MFA redesign
- Antispam
- Policies and contracts
- Improve detection
- Awareness

LESSON LEARNED

VERSIVO
ACTIVE CYBER DEFENSE

Lesson learned

- Social Engineering based attacks are actually effective.
- Email compromises are «personal data breach».
- Security controls are useless unless they are designed taking into account the attacker's mindset.
  - Evaluate the risk of knowing the attackers.

Cyber Security Mindset

VERSIVO

ACTIVE CYBER DEFENSE

VERSIVO

Active Cyber Defense

Via Giovanni Felisati, 61

30171 Mestre-Venezia (VE) Italia

info@versivo.it

www.versivo.it