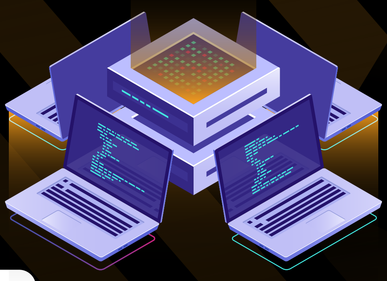
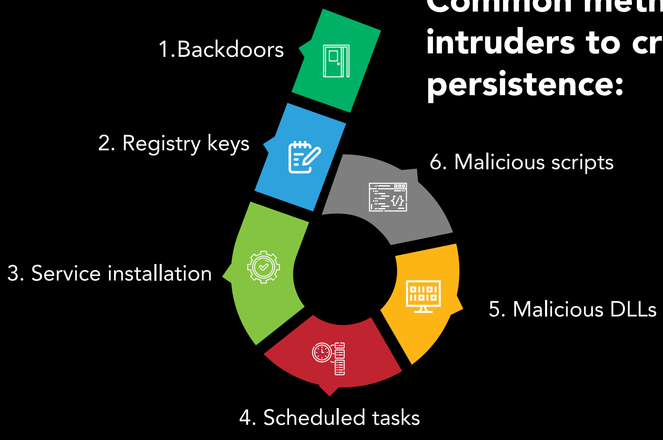


The Power of Progression:
Intruder Lateral Movement in Action

Lateral movement occurs in about 70% of cyberattacks, navigating through a compromised network via -

- Privilege Escalation
- Defence Evasion
- Credential Access
- Discovery
- Collection
- Command and Control

Common methods used by intruders to create persistence:



Popular tools used for performing lateral movement:

01 **BloodHound:** AD vulnerabilities

02 **Cobalt Strike:** C2 communication

03 **Mimikatz:** Credentials extraction

04 **PowerShell Empire:** Post-exploitation tasks execution

05 **File System Scanning Scripts:** PII & password scanning

Key lapses leading to lateral movement:

- Improper segmentation of **VLAN**
- Ineffective implementation of **MFA**
- Weak credential storage/management

Don't let lateral movement go undetected. Learn how to end their free rein!

Download the latest **SISA Top 5 Forensic-driven Learnings 2023-24 report**