

**LATERAL MOVEMENT, C2, EXFILTRATION**



**INITIAL ACCESS**



**INITIAL ACCESS**



**INITIAL ACCESS**



**INITIAL ACCESS**

**LATERAL MOVEMENT, C2, EXFILTRATION**

**LATERAL MOVEMENT, C2, EXFILTRATION**

**LATERAL MOVEMENT, C2, EXFILTRATION**



**LATERAL MOVEMENT, C2, EXFILTRATION**

**LATERAL MOVEMENT, C2, EXFILTRATION**

**LATERAL MOVEMENT, C2, EXFILTRATION**

**LATERAL MOVEMENT, C2, EXFILTRATION**

**TRAFFIC DUPLICATION**

The hacker uses traffic mirroring to exfiltrate data over an already compromised network.

MITIGATION

Encrypt sensitive information

DETECTION

Monitor network traffic for uncommon data flows

**EXFILTRATION OVER USB**

The hacker tries to move data between two disconnected networks using a USB device.

MITIGATION

Limit the use of USB devices

DETECTION

Monitor file access on removable media

**PASS THE HASH**

The hacker uses Mimikatz to authenticate himself as a user without having the clear text password.

MITIGATION

Enable pass the hash mitigations

DETECTION

Monitor for lsass.exe

**SSH HIJACKING**

The hacker hijacks a legitimate user's SSH session to move laterally within an environment.

MITIGATION

Disable agent forwarding

DETECTION

Monitor user SSH-agent socket files



**INITIAL ACCESS**



**INITIAL ACCESS**



**INITIAL ACCESS**



**INITIAL ACCESS**

**VBA STOMPING**

The hacker hides Visual Basic for Application payloads within MS Office documents.

MITIGATION

Restrict access to unneeded VB components

DETECTION

Detection for p-code

**WEB PROTOCOLS**

The hacker uses web traffic protocols for unnoticed communication such as HTTP or HTTPS.

MITIGATION

Network intrusion detection

DETECTION

Analyze network data for uncommon data flows

**NON-STANDARD PORT**

The hacker does not use conventional ports (port 587) to communicate via HTTPS.

MITIGATION

Network intrusion detection

DETECTION

Analyze packet contents

**MAIL PROTOCOLS**

The hacker uses electronic mail delivery for unnoticed communication such as SMTP or POP3.

MITIGATION

Network intrusion detection

DETECTION

Analyze network data for uncommon data flows