

**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**

**URL PHISHING**

The hacker sends emails to all employees containing a malicious URL to a website that executes crypto jacking scripts.

MITIGATION

Restrict Web-Based Content

DETECTION

Email Sandbox

**ATTACHMENT PHISHING**

The hacker sends emails to all employees containing a malicious Microsoft Office document which executes scripts to collect user and environment data.

MITIGATION

Disable MS Office macros

DETECTION

Email Sandbox

**VALID ACCOUNT VPN**

The hacker discovered a valid VPN account for your network during a data breach that you don't know about.

MITIGATION

Store credentials securely

DETECTION

Monitor sites like haveibeenpwned.com for your data

**SPEARPHISHING**

The hacker sends an email to employees pretending to be the managing director and asking for sensitive data.

MITIGATION

Anti-impersonation technology

DETECTION

Check the Sender & Domain



**INITIAL ACCESS**



**INITIAL ACCESS**



**INITIAL ACCESS**



**INITIAL ACCESS**

**SQL INJECTION**

The hacker finds an SQL injection on a website that is used for applications at your company, with which he can execute commands on the server.

MITIGATION

Sanitize input

DETECTION

Extended Events and SQL Monitor

**TRUSTED RELATIONSHIP**

The hacker hacked another company that has a trusted active directory relationship with your network.

MITIGATION

Network segmentation

DETECTION

Monitoring for activity conducted by trusted entities

**WATERING HOLE ATTACK**

The hacker has infected a website that he knows that employees in your company use regularly to obtain credentials.

MITIGATION

2 factor authentication

DETECTION

Splunk User Behaviour Analytics

**USB RUBBER DUCKY**

The hacker was left alone at the reception for a short time and had the opportunity to connect a Rubber Ducky which steals saved passwords from the browser.

MITIGATION

Blocking USB

DETECTION

Keystroke speed