Lateral Movement

Blue Team Level 1 Certification (Standard) > IR6) MITRE ATT&CK > Lateral Movement IN PROGRESS

This lesson is going to cover the eighth stage in the MITRE ATT&CK framework, Lateral movement. An adversary commonly has to exploit multiple machines within a network to reach their primary objective, the movement between these hosts is called 'Lateral movement'. At the time of writing this there are currently 9 techniques mapped to Lateral Movement, but we're going to focus on:

- Remote Services
- Internal Spearphishing

MITRE Technique T1021

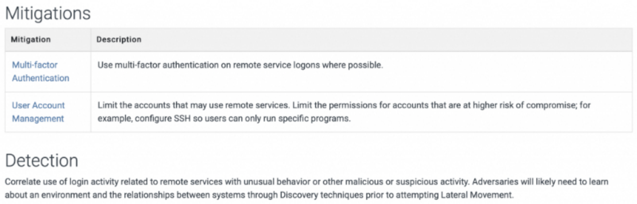
Adversaries commonly use legitimate accounts, previously stolen or not, to log into a service designed to accept remote connections, such as RDP. In a large environment IT administrator will quite often use the same password across multiple machines meaning the leverage of genuine remote services not only works, but is harder to spot. At the time of writing Remote Services is split down into 6 sub-techniques as listed below:

- **Remote Desktop Protocol (RDP)**
- **SMB/Windows Admin Shares**
- **Distributed Component Object Model**
- **SSH**
- **VNC**
- **Windows Remote Management (WINRM)**

For mitigating use of this technique we can enforce multi-factor authentication (MFA) on remote services where possible to significantly reduce the chances of successful password spraying and password reuse attacks. We should also routinely audit which user accounts are able to use remote servers, and assess whether they actually need these permissions or if they can be removed.

When we scroll down to look at detection methods, well, it's pretty straightforward. Three words – Timeline, timeline, timeline. Adversaries need to know the environment they have landed in; this involves enumeration and other malicious/suspicious activity. Correlate this with logon activity to services and ask questions such as:

- **Was this person in work?**
- **What happened 10 minutes before and 10 minutes after?**
- **Is this a new account?**



Mitigations

Mitigation	Description
Multi-factor Authentication	Use multi-factor authentication on remote service logons where possible.
User Account Management	Limit the accounts that may use remote services. Limit the permissions for accounts that are at higher risk of compromise; for example, configure SSH so users can only run specific programs.

Detection

Correlate use of login activity related to remote services with unusual behavior or other malicious or suspicious activity. Adversaries will likely need to learn about an environment and the relationships between systems through Discovery techniques prior to attempting Lateral Movement.

MITRE Technique T1534

Once a malicious actor has gained a foothold in the network and has gained access to email accounts they can send internal spearphishing emails with links to malicious resources in an attempt to gain access to new systems within the target organisation. These emails are going to be a **LOT** more effective than external phishing emails because they are coming from a legitimate address, and the attacker may actually reply to emails in previous email chains to make them look completely convincing.

5 Topics | 1 Quiz

○ IR5) Lessons Learned and Reporting

7 Topics

○ IR6) MITRE ATT&CK

13 Topics | 2 Quizzes

○ Section Introduction, ATT&CK

○ Initial Access

○ Execution

○ Persistence

○ Privilege Escalation

○ Defense Evasion

○ Credential Access

○ Discovery

○ Lateral Movement

○ Collection

○ Command and Control

○ Exfiltration

○ Impact

Activity) ATT&CK Navigator

Activity) End of Section Review, ATT&CK

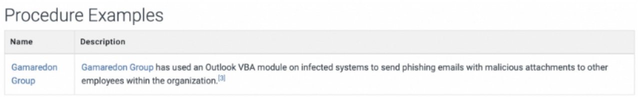
BTL1 EXAM

○ Exam Preparation

○ Using RDP and SSH

○ How to Start Your Exam

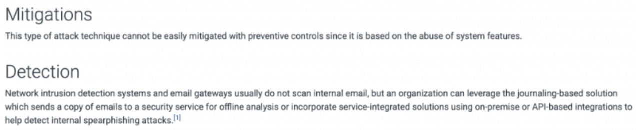
Below we can see that Gamaredon Group has previously used a custom VBA module to send phishing emails when they have compromised a system and gained access to the mailbox, allowing them to quickly spread their presence and gain a foothold in other systems within the environment.



Procedure Examples

Name	Description
Gamaredon Group	Gamaredon Group has used an Outlook VBA module on infected systems to send phishing emails with malicious attachments to other employees within the organization.[3]

Scanning all URLs and attachments that pass through an organisation's Exchange server can help with the detection of internal spearphishing. If we're not able to prevent the attack at this stage we would hopefully detect it during the Exploitation stage when the downloaded payload is run by the phishing victim.



Mitigations

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.

Detection

Network intrusion detection systems and email gateways usually do not scan internal email, but an organization can leverage the journaling-based solution which sends a copy of emails to a security service for offline analysis or incorporate service-integrated solutions using on-premise or API-based integrations to help detect internal spearphishing attacks.[1]

Previous Topic

Mark Complete ✓

Next Topic

Back to Lesson