Cybersecurity Strategies to Stop Lateral Movement Attacks & Leave Your Adversaries Marooned

beyondtrust.com/blog/entry/cybersecurity-strategies-to-stop-lateral-movement-attacks-leave-your-adversaries-marooned

To a cyber threat actor, lateral movement means all the difference between compromising a single asset and potentially navigating throughout an organization to establish a persistent presence. While a hacker might initially succeed in infiltrating an environment via a number of methods, such as an opportunistic phishing attack, or a targeted attack based on stolen credentials or an exploit, lateral movement is the means to find data of value, compromise additional assets, and, ultimately, execute malware for reconnaissance and command and control.

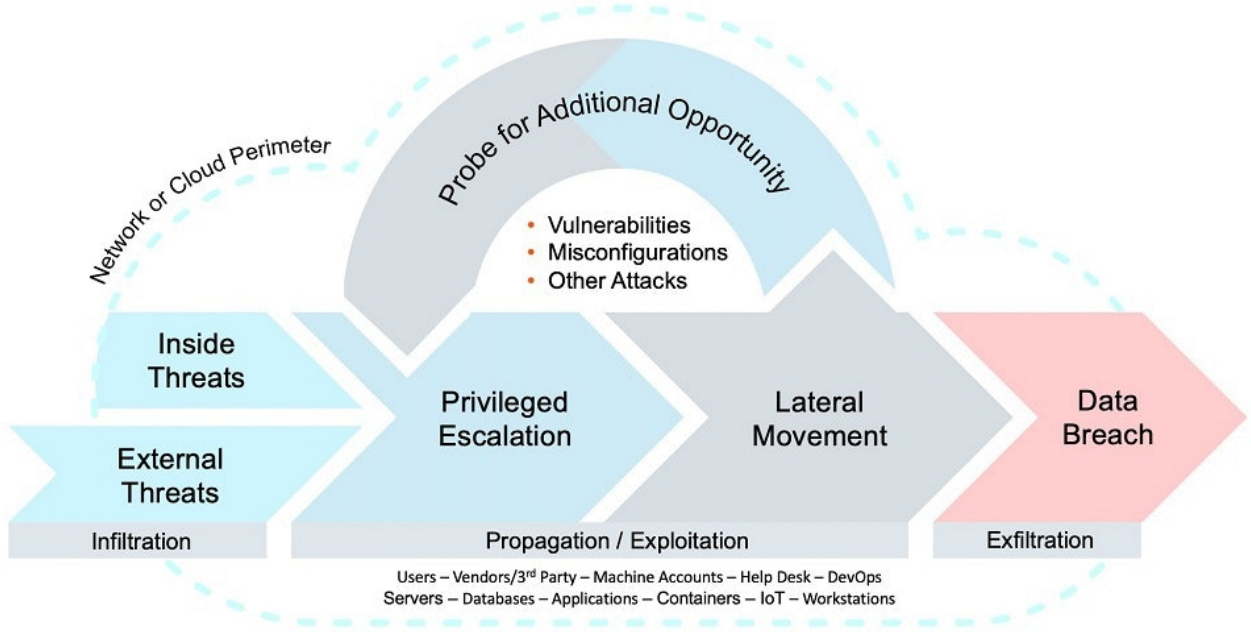

Illustration of the cyberattack chain

Lateral movement, in this context, refers to the ability to pivot from one asset (identity, account, database, system resource, etc.) to another. Lateral movement is a key stage of the cyberattack chain, and published studies have found that it occurs in about 70% of cyberattacks.

Try thinking of the approach to stopping lateral movement in these terms. – an attacker opportunistically exploits a vulnerability, or uses a compromised credential, etc., to gain an initial beachhead in your environment. It's very unlikely that this initial landing spot/beachhead is going to give the attacker direct access to what they want. Again, it's

merely a weak spot they found in your security and were able to compromise. However, the danger is that this foothold in the environment can be used as a pivot point to obtain further privileges and access to get closer and closer to the more desirable assets the attacker seeks.

With the right security strategies, you can ensure that the attacker's beachhead is essentially a (very) small island, with no routes to other bodies of resources, and no chance to island hop. Done right, a defensive posture against lateral movement leaves attackers marooned, limiting the damage, while giving the defender time to detect, and ultimately, eject the attacker from the environment. What is key, however, is this lateral movement is not just island jumping hosts, it can occur in a variety of ways– and protection strategies need to guard against each one of them.

Resources Leveraged in Lateral Movement Attacks

When we talk about the security importance of lateral movement, the focus is not only assets, it is about "resources" since they can be so much more than just computers. Resources engaged in lateral movement can be any of the following and, most importantly, any combination of them:

Resources	Privileged Attack	Asset Attack
Operating System	Credential, Hash-Based Attacks, or Golden Ticket	Vulnerabilities, Exploits, and Misconfigurations
Applications	Credential or Application-to-Application Attacks, including Man-in-the-Middle Threats	Vulnerabilities, Exploits, Misconfigurations, Insecure Architectures, and End-of-Life
Containers	Credential, or Insecure Connectivity	Vulnerabilities, Exploits, Misconfigurations, Insecure Architectures, and Agile DevOps
Virtual Machines	Credential, Hash, or Hypervisor-based Credential Attacks	Vulnerabilities, Exploits, Misconfigurations, Insecure Architectures and Agile DevOps, and CPU and Memory-Based Vulnerabilities
Accounts	Credential Theft or Abuse, or Identity Theft (including brute force, password spraying, reuse, etc.)	Credential Theft, Abuse, Memory-Scraping, and Insecure Credential Storage
Identities	Credential Reuse and Account to Identity Associations (i.e. via email account names)	Inappropriate Account Linkage

Resources exploited in the lateral movement phase of cyberattacks

While the techniques for lateral movement vary substantively between these resources (including for privileged and asset attack vectors), the threat actor's objective is the same – to laterally move between resources that are similar or share underlying services. For example, an attacker may laterally move from an operating system to an application and then compromise additional accounts using any combination of the attack vectors (and there are definitely more) referenced above. This raises the obvious question—how do you protect against lateral movement when it can occur in so many different ways?

First, consider the underlying faults that allow lateral movement to occur. They occur due to privileged attacks or asset attacks. Network segmentation is one way to restrict lateral movement in broad stroke across an IT environment, but to stop attackers in their tracks, we need to understand and implement security controls specific to privileged or asset attack vectors. In many ways, this is a combination of zero trust, just in time, and universal privilege management.

Mitigating Lateral Movement from Asset Attack Vectors

Asset attacks are typically addressed, or at least mitigated, through vulnerability, patch, and configuration management. These are traditional cybersecurity best practices that every organization should be doing well, but as we all know, very few organizations have them working like well-oiled machines.

The conversation we need to have with our teams is that, lateral movement, due to poor basic cybersecurity hygiene, is the primary attack vector for modern threats like ransomware, bots, worms, and other malware. Contemporary concepts like zero trust and just-in-time privileged access management provide a foundation to mitigate the threats from privileged attack vectors (covered below), but do not mitigate asset or identity-based attacks. A successful attack is based on software flaws and not credentials used for the interaction of resources when modern security strategies are deployed. Therefore, for lateral movement based on asset attacks, we need to ensure the basics are being done well week after week, month after month, and year over year to ensure we do not expose cracks in our security posture that could lead to a vulnerability and exploit combination.

Mitigating Lateral Movement from Privileged Attack Vectors

The second method of lateral movement is based on privileged attack vectors. This typically includes some form of privileged remote access. The attack techniques include:

- Password Guessing
- Dictionary Attacks
- Brute Force Attacks (including techniques like Password Spraying)
- Pass-the-Hash
- Security Questions

- Password Reset
- Multifactor Authentication Flaws
- Default Credentials
- Backdoor Credentials
- Anonymous Access
- Predictable Password Creation
- Shared Credentials
- Temporary Password
- Reused or Recycled Passwords

If multiple accounts are compromised for the same identity, then the attack vector can evolve into an identity attack vector in which everything a person owns (and their accounts), is responsible for, or has privileged or unprivileged access to, becomes a form of lateral movement based on the account / identity relationship. This is important in our conversation about lateral movement because the resource is not always electronic. The resource can be abstract like an identity or software in the form of a container. Regardless, the movement is a pivot and a form of lateral movement between the resources.

Lateral movement by privileged attack vectors can be drastically curtailed by effectively executing the universal privilege management fundamentals. For instance:

- Applying the principle of least privilege will not only reduce the risk that an attacker gains a foothold in the first place (i.e. executing privileges to install malware), but it limits the access pathways available to the threat actor. Removing admin rights can broadly reduce access to those internal corridors across the entire IT environment. An important piece of enforcing true least privilege requires just-in-time privileged access management, a strategy that aligns real-time requests for usage of privileged accounts directly with entitlements, workflow, and appropriate access policies. By enforcing true least privilege, the lateral access pathways are limited in number as well as in windows of time and duration in which they can be accessed (in other words, eliminating persistent access).
- Enforcing privilege separation and separation of duties. When applied to users, this involves segmenting user privileges across separate users and accounts, and ensuring certain duties can only be performed with specific accounts. Thus, if one account is compromised, the range of privileges it affords the attacker is fairly restricted in scope.
- Implementing Privileged Credential Management, such as securing passwords, keys, and secrets in a centralized safe and rotating credentials, eliminating default/re-used credentials, etc. This best practice eliminates a broad swathe of attack methods, while reducing the effectiveness of others. For instance, implementing one-time passwords (OTPs) for highly privileged accounts will prevent password re-use attacks. Frequent rotation of credentials also means that the threat window for which an account can be compromised via stolen credentials is time-limited.

- Privileged threat analytics and session management/monitoring: Rapid detection and response to indicators of compromise is an important part of stopping attacks before they become worse. All privileged sessions should be monitored for unusual activity (i.e. trying to execute certain commands). Additionally, the ability to centrally assert control over sessions, including pausing and terminating them, is a powerful defensive capability.

Additionally, the concept of zero trust, which requires a multi-faceted approach, can be applied to defend against lateral movement attacks. A zero-trust approach emphasizes upholding strict access controls and not trusting anyone, anywhere, at any time—even those who are already inside the network perimeter—by default. Zero trust strives to ensure that authorization or authentication is not allowed between resources unless a third-party trust and approval has been granted. Remember, lateral movement can happen in between resources and it is that inappropriate trust between them that should be prevented to mitigate the threats of lateral movement.

Final Thoughts on Lateral Movement

To a threat actor, lateral movement is a crucial strategy. It allows them to move from where they opportunistically landed within an organization via the initial exploit, to other, more desired resources. The techniques for lateral movement can be based on the resource's asset or privilege characteristics, and include resources that span a human identity all the way through unpatched vulnerabilities on an operating system. When exploited, either method can allow a threat actor to move laterally among resources to achieve their objectives. Our conversations on lateral movement should always include the resources involved in a technology implementation and how are we securing privileged access and maintaining foundational security to protect the asset.