What Is Lateral Movement?

fortinet.com/resources/cyberglossary/lateral-movement

Lateral Movement Definition

Lateral movement refers to a group of methods cyber criminals use to explore an infected network to find vulnerabilities, escalate access privileges, and reach their ultimate target. It is called lateral movement because of the way the hacker moves sideways from device to application and so forth. However, the intent is actually to move upwards in terms of access or deeper in terms of data.

Cyberattacks are by no means a new threat, but one of the rising concerns for network security professionals is attempts at lateral movement after an infection. A recent report states that lateral movement was seen in 25% of all cyberattacks.

So what is lateral movement and what is its purpose? More importantly, how can organizations detect and prevent it?

Lateral Movement Techniques

Some examples of lateral movement paths (LMPs) that criminals would pursue in an infected system are:

1. Internal spear phishing, which is when someone gains access to a company's email network by hacking a user's account and then targeting specific people or groups within the organization
2. Pass the hash (PtH) attacks. PtH attacks are when a hacker gets the hash of a password, which is created by an encryption system, and passes that through the authentication system to gain access.
3. Pass the ticket (PtT) attacks, which happen when an attacker gains inside access and steals Kerberos tickets to gain access to other computers or files
4. Remote services exploitation. This is when an attacker uses someone's access to remote services, such as Zoom video conferences, to gain access to sensitive resources within a company.
5. Secure Shell (SSH) hijacking, SSH enables users to access macOS and Linux systems, and SSH hijacking is when a hacker deploys a legitimate user's SSH session to move laterally to infect other users or systems.

6. Windows admin shares. Windows admin shares enable someone to access user computers that are connected to a network, so hackers steal them to spread infections to other computers.

These lateral movement examples demonstrate that attackers leverage systematic vulnerability exploitation to exfiltrate data and/or steal credentials to gain network access.

Understanding the 5 Stages of Lateral Movement

While there are numerous methods and tools criminals can use to execute lateral movement, the attack has five basic stages, regardless of how it is done. It begins with infecting the system with malware.

1. Infection

Normally, exterior cyber defenses are relatively robust, so cyber criminals rely principally on human error to accomplish to infect target systems. These are some of the techniques they are likely to use:

1. Drive-by download attacks: Hackers plant malicious scripts on an unsecured website. This results in a user downloading malware without their knowledge.
2. Exploit kits: These are automated toolkits or exploit packs that attack system vulnerabilities to install malware. Exploit kits often consist of compromised websites or target vulnerable browser-based applications.
3. Malicious email: Attackers send out messages with a malicious link or attachments, hoping the recipient will click on the link or open the attachment.
4. Phishing emails: The hacker sends an email that appears to originate from a legitimate source, requiring a user to log in to their account or provide personal information that the perpetrator would then steal.
5. Compromised hardware: A flash drive or other external storage device can have malware on it. When connected to a device on the network, it installs the malware without the user's knowledge.

2. Compromise

Once the device has been infected, it will likely communicate back to the hacker's command-and-control server, also known as C2 or C&C server, to indicate it is ready to receive commands. Using a remote shell and possibly a graphical user interface (GUI), attackers can issue commands to the infected machine undetected. At this point, the device is ready for reconnaissance.

3. Reconnaissance

The reconnaissance stage is all about observing and mapping. The infected device is rarely the ultimate target of the attack, so the attacker uses it to determine how to reach their end goal.First, they have to know where they are in the network—not just physically, but what permissions and access they have and what barriers are in place. Secondly, they need to learn organizational policies, such as file-naming standards, access levels, hierarchy, etc.

4. Credential Theft

To begin moving laterally, the attacker needs login credentials. Using software tools such as keyloggers and Windows Credential Editor is one way to perform credential dumping, which involves stealing login information from software or an operating system, but other common methods are social engineering and brute-force attacks.

Cyberattacks That Use Lateral Movement to Penetrate Through the Network

Lateral movement has two main objectives—access a specific account or data or control as many devices as possible. Whether for financial gain, the theft of data or proprietary information, or further criminal activity, the type of attack usually indicates the ultimate goal of the perpetrator.

1. Ransomware

Ransomware is a type of malware that encrypts data or a section of the network, locking out users' access. The attacker sends the victim a message requiring a ransom in exchange for access or a decryption key. Ransomware criminals usually coerce victims into paying by threatening to delete or publish their data if payment is not made by a certain deadline.

2. Espionage

Cyber espionage has become a global threat and can go undetected for a long time. In this type of attack, the attacker does not steal anything or make demands; rather, they perform reconnaissance. Staying hidden as long as possible typically results in the greatest yield of information, as the criminal eavesdrops on company activity.

3. Data Exfiltration

Data exfiltration can be accomplished through social engineering, malware, or hacking, to steal confidential or sensitive information. This can include the theft of intellectual property or the identities of personnel, or transferring data and holding it for ransom.

4. Botnet Infection

Sometimes, infecting a network is just the first step. Cybercriminals with more long-term ambitions attack systems with inadequate security to command and control enough machines to create a botnet. Botnet is short for "robotic network," a network of computers with enough computing power to launch a more serious attack, such as a distributed denial-of-service (DDoS) attack.

Top 7 Strategies How To Detect and Prevent Lateral Movement

Attacks that move laterally from one area of the network to another can go undetected for a long period. Having processes in place to detect lateral movement—or even better, prevent it in the first place—is critical to safeguarding your organization.

Detecting Lateral Movement

The time it takes for an attacker to move laterally after gaining access now averages less than half an hour, so security teams should ramp up their detection and response strategies. Here are some ideas:

1. Map lateral movement paths (LMPs): Begin by identifying possible LMPs in your organization's network. Review the infrastructure and hierarchy to spot vulnerable connections between devices, data, and systems. Removing them may not be possible, but you can monitor and secure them.
2. Leverage reporting tools]: Tools for monitoring and reporting are essential for recognizing suspicious activity. However, beware of alert fatigue, and aggregate alerts for prioritization.
3. Investigate and analyze user behavior: Analyzing behavioral patterns through machine learning can help isolate and investigate anomalies. While some abnormal behavior is no cause for concern, analysis and investigation may uncover unauthorized activity.
4. Monitor unknown devices: In this day and age of "bring your own device" (BYOD) to work, it is normal that unknown devices may register on the network, but do not be quick to conclude it is an employee. Monitor such devices for suspicious activity.
5. Investigate abnormal administrative tasks and file sharing. Attackers will try to avoid detection by using native tools, but this produces anomalies that can be detected. Additionally, hackers doing reconnaissance will test access to servers containing confidential data, so discrepancies in file-sharing access can be an indicator of lateral movement.
6. Monitor logins, especially on devices using multiple credentials. Principally, users logging in at strange times or after hours, or multiple logins on a single device may be indicators of lateral movement.

7. Identify port scans and abnormal network protocols. Hackers perform port scans as part of their reconnaissance, but these scans can be detected by intrusion detection systems. Additionally, there may be abnormalities between a protocol used for a connection and the data that was transmitted or received, indicating encryption was not used.

Preventing Lateral Movement

A security posture that prevents intrusion is preferable to one that merely provides detection and response. So while it may not always be possible to prevent an attack and subsequent lateral movement, there are things your security team can do to prevent it as much as possible.

1. Install software updates and system patches regularly. All operating systems, software, services, endpoints, and systems should be kept up-to-date and patches should be applied regularly.
2. Update endpoint security solutions. Endpoints are most vulnerable to unauthorized access, so tools to monitor and secure them are important. Cybercriminals often do not care which device gets them in, as long as they can move laterally after gaining access, so no endpoint should be left vulnerable.
3. Enforce the principle of least privilege (PoLP). Ensure that users only have access to what they need to perform their assigned tasks.
4. Use multi-factor authentication (MFA). MFA adds layers of security to user logins, so that even if a user's credentials are compromised, access is not granted if each layer of security is not satisfied with the identity of the person requesting access.
5. Implement network segmentation. Segmentation or micro-segmentation ensures that sensitive parts of the network are isolated, without pathways for lateral movement, strategically positioned in relation to the rest of the system for secure, privileged access.
6. Backup critical data. Having data backups reduces the threat of ransomware, and it means that even in the event of a system compromise, data can be fully restored.
7. Implement zero-trust security. Because a zero-trust solution assumes every user is a threat until proven otherwise, it makes lateral movement very difficult.

How Fortinet Can Help

Fortinet's Network Detection and Response (NDR) uses artificial intelligence and intelligent analytics to identify suspicious network activity and detect anomalies that may be indicators of lateral movement. Besides monitoring and analytics, FortiNDR identifies new threats to help security teams adapt threat containment and protection to new risks.

FAQs

What does lateral movement mean?

Lateral movement refers to a group of methods cyber criminals use to explore an infected network to find vulnerabilities, escalate access privileges, and reach their ultimate target. The designation “lateral” aptly describes the way the hacker moves sideways from device to app and so forth.

Why would an attacker use the lateral movement technique?

There are two main objectives of lateral movement—access to a specific account or data, or control of as many devices as possible. Much depends on the ultimate goal of the perpetrator, whether it is for financial gain, the theft of data or proprietary information, or further criminal activity.

What would be an example of a lateral movement attack?

Some examples of lateral movement paths (LMPs) that criminals would pursue in an infected system are internal spear phishing, pass the hash (PtH) attacks, pass the ticket (PtT) attacks, remote services exploitation, secure shell (SSH) hijacking, and Windows admin shares.