Lateral Movement in Cybersecurity: Understanding and Preventing Attacks

FADDOM | JUNE 18, 2023

Lateral movement attacks are one of the most prevalent methods used by threat actors today. Gaining access to the network through phishing attempts or malware is the first step for any attacker. But the most sophisticated attackers seek ways to move around throughout a network. This lateral movement leads to the greatest potential for long-term data loss for small- to medium-sized businesses, with this method accounting for 25% of all cyberattacks in 2022.

Deterring such persistent threats is becoming increasingly challenging considering the expanding complexity of today's networks. By understanding the nature of lateral movement, IT leaders and security specialists can work collaboratively to detect and prevent the threat posed by these attacks.

Table of Contents

What is Lateral Movement?

A key tactic of advanced persistent threats (APTs), lateral movement is a set of techniques that threat actors use to identify high-value targets in multiple network systems. A lateral movement attack is a long-game approach for attackers skilled at avoiding detection for weeks or months as they gather information on network systems. The ultimate target: high-value data that provides control over specific company assets—or even the entire company—which are held for ransom.

The ability to move from side to side within the network through applications, devices, and other gateways and endpoints enables attackers to find new ways to move deeper into the network to reach critical data. By gaining access to user account credentials, admin accounts, and passwords, and other entry points, attackers can escalate their privileges to access more and more data, and eventually move it to their own environments. Detection of these threat actors can take weeks or months, and many organizations detect them only after they have completely exited the system.

How Lateral Movement Works: The Stages of Attack

Although lateral movement has many methods and tools that attackers use (discussed later), the stages of a lateral movement attack are far more standardized. Cybersecurity experts and organizations have identified three stages of lateral attacks:

1. Infection

The attacker must first gain access to the network to begin the process of infiltration. Since exterior network security systems like next-generation firewalls are more robust, attackers seek out entry points that rely on humans and the high probability of human error. Malicious emails with links that lure the recipient into clicking them and phishing emails that appear to come from a known source are two of the most widely used tactics. There were more than one million recorded phishing attacks in Q3 of 2022 alone.

Other infection approaches include exploit kits (also known as exploit packs) and drive-by download attacks, which use malicious scripts to attack vulnerable websites or applications. Additionally, external devices like flash drives and external storage drives can carry malware into the network.

2. Reconnaissance

Once attackers gain network entry, they begin exploring and mapping the network, users, and devices. This information enables malicious actors to determine possible access permissions, along with policies like standardized file naming and access protocols.

3. Credential Theft

After carrying out reconnaissance, an attacker will then look for login credentials, such as keyloggers, man-in-the-middle attacks, phishing, brute force attacks, and other sources that enable them to steal that information from operating systems. These and other lateral movement paths (LMP) allow threat actors to infiltrate as many devices or systems as possible so they can escalate the attack and gain greater access to devices, systems, and applications. Attackers then continue to obtain additional credentials until they have reached their ultimate data or control objective.

Common Lateral Movement Techniques

There are many tools and techniques that threat actors can use to determine access possibilities, firewalls, and their location in the network. Built-in network tools for specific functions have the most difficulty in detecting a compromised network.

Netstat—a command line network utility that shows various network connections–can be used to identify network assets. PowerShell—a command line scripting tool—enables attackers to infiltrate network systems with local admin access. Others, like ARP cache (which provides IP address paths), enable attackers to target machines on the network while local routing table access displays connected host communication paths that are ideal for threat actor reconnaissance.

Privilege Escalation Techniques

After mapping the network and searching for vulnerabilities, attackers aim to steal valid login credentials, known as credential dumping. As previously mentioned, relying on human error and tricking users into revealing credentials through social-engineering tactics are the easiest means of achieving this.

Other methods include pass-the-hash (PtH) and pass-the-ticket (PtT) attacks. PtH enables attackers to gain access to the network through the authentication system by stealing the hash that was created by the encryption system. In a PtT attack, malicious actors can create a Kerberos (service request authentication protocol) ticket that is valid indefinitely. Attackers are then able to use these for account impersonation, even after a password reset.

Pass-the-hash lets an attacker bypass password-authentication steps to manipulate local and remote systems. External tools like keyloggers and Mimikatz can capture passwords entered directly from a keyboard or steal cached passwords and authentication certificates from a compromised endpoint computer, respectively.

The list of tools and techniques cyber attackers leverage also includes hacking into remote services like Zoom to access sensitive data. Other methods like Secure Shell (SSH) hijacking enable attackers to gain access to macOS and Linux systems, where they can deploy a user's SSH session for lateral user and system infections.

Windows Admin shares is yet another method to gain access to network-connected computers to spread infections to other systems. These tools and techniques are constantly evolving, providing threat actors with more sophisticated attack vectors that are increasingly difficult to detect and thwart.

Detecting and Preventing Lateral Movement

The stakes are high for lateral-prevention cybersecurity, with a global average cost of a data breach of $4.35 million in 2022. Luckily, there are effective prevention approaches, methods, and tools.

Monitoring Logins and Unknown Devices

Security teams should monitor user logins and anomalous network behavior via monitoring and reporting tools like identity access management (IAM) and user and entity behavior analysis (UEBA) tools. These and other access solutions, ML-based tools, and intrusion-detection systems can help to identify lateral movement through network monitoring and reports of deviation from baseline behavior. When paired with network mapping tools, these solutions become even more effective.

Endpoint Protection, Threat Hunting, Deception Technology, and Alerts

As networks and network traffic grow, it is imperative to upgrade to endpoint security solutions that go beyond the standardized security measures of legacy devices to ensure ongoing threat protection to any network-connected device. As part of monitoring detection and response functions, these tools can prevent unauthorized application downloads from endpoint devices, such as computers connected to the network.

Updated endpoint security solutions should also cover IOT devices and external IoT devices (XIoT), ranging from surveillance cameras, native device cameras, door locks, and printers to operational technology devices, such as robots and other industrial devices.

Threat-Hunting Tools

Threat-hunting tools provide a far more comprehensive approach to combating lateral movement attacks across the network. These can include integrated security information and event management (SIEM); security orchestration, automation, and response (SOAR); and managed detection and response (MDR) systems. Note that these and other monitoring and prevention tools deliver alerts, which must have carefully set parameters to avoid false alerts and to catch all anomalous behavior while monitoring.

Deception Technologies

Deception technologies pose as false IT network assets and entice attackers to interact with them. These fake assets can consist of honeypots, which are decoy systems or servers. There are also honeypot users—fake user accounts to attract threat actors—along with honey credentials, which are fake credentials added to an endpoint device. When attackers go for the bait, security personnel receive high-confidence alerts.

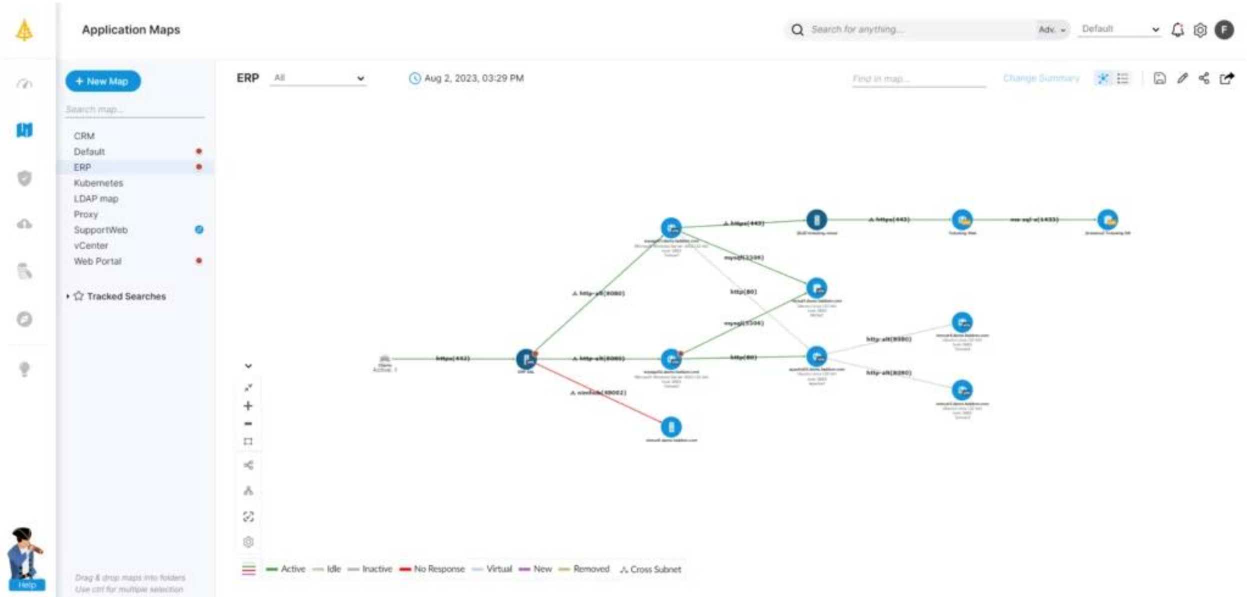
Network Segmentation, LMP Mapping, and ADM

Another important tool in lateral movement cybersecurity is microsegmentation, which isolates the network into different parts. Segmentation is helpful in preventing lateral movement by containing threats in a single segment.

The ability to map lateral movement paths is another important proactive approach to thwarting lateral movement. This methodology requires security personnel to review the network infrastructure to uncover weaknesses via data, device, system, and user connections.

Network mapping via an IT architecture/infrastructure/ADM mapping tool can deliver a comprehensive view of a network, including all connected devices and applications across physical, virtual, and cloud-connected assets. This becomes a foundation for all lateral movement tools, approaches, rules, and protocols.

Gain Visibility into Your Network with Faddom



Lateral movement cybersecurity is constantly changing to meet the growing threat vectors in today's digital ITC device world. Every organization, from SMBs to enterprises, must constantly evaluate their security strategy to include preventative, detection, and response solutions for automatic identification of threats. The more visibility organizations have into their networks, the more effective their defense will be against lateral movement.

Protect your organization from lateral movement and other pervasive security threats. Faddom supports a holistic security approach through segmentation and network visibility. Start a free trial today!