ANOMALI

GUIDE

Proactively Detecting Lateral Movement to Mitigate Cybersecurity Risks

ANOMALI

GUIDE

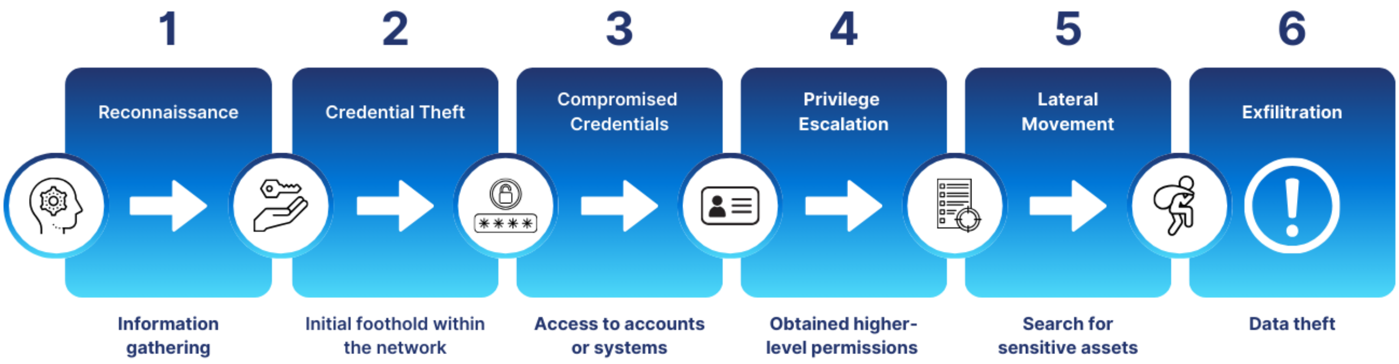
Proactively Detecting Lateral Movement to Mitigate Cybersecurity Risks

Lateral movement across an IT infrastructure is among the most insidious and effective techniques attackers employ during advanced cyberattacks. The basic scenario is this: once an attacker gains initial access to an enterprise network — often through techniques such as phishing, stolen credentials, or vulnerability exploitation — they move laterally within the network to escalate privileges, gain access to sensitive systems, and exfiltrate data.

Lateral movement allows threat actors to remain undetected while quietly mapping and exploiting other vulnerable systems, significantly expanding a cyber attack's potential blast radius. Lateral movement is critical to advanced persistent threats (APTs), ransomware campaigns, and other large-scale cyber incursions.

Six Stages of Lateral Movement in Cybersecurity

Adversaries use many techniques and tactics to infect a network to find vulnerabilities, escalate privileges, and ultimately reach their targets. According to the MITRE ATT&CK® framework, the following stages enable adversaries to easily move sideways from a device to an application across an organization:



1 Reconnaissance — Information gathering

2 Credential Theft — Initial foothold within the network

3 Compromised Credentials — Access to accounts or systems

4 Privilege Escalation — Obtained higher-level permissions

5 Lateral Movement — Search for sensitive assets

6 Exfiltration — Data theft

Reconnaissance

In the preliminary phase of an attack, an adversary gathers intelligence about a target system, network, or organization to identify potential vulnerabilities and plan their attack strategy. This process includes collecting data before launching an attack to understand its weaknesses and planning an effective attack strategy. It may also incorporate scanning for open ports, analyzing network traffic, searching for publicly available information on websites and social media, and social engineering.

Credential Theft

The first stage of an attack involves the adversary gaining a point of entry into a target system or network. It usually means that an adversary has executed harmful code on one or more corporate systems (via phishing emails, malicious websites, or other tactics) to access user and system credentials.

Compromised Credentials

Attackers use credentials — usernames, passwords, security questions, and so on — to access user accounts and systems within an organization.

Privilege Escalation

After gaining access, the adversary attempts to acquire the credentials of identities with higher privileges or to escalate the privileges of an account they currently have access to. They accomplish this by exploiting vulnerabilities, bugs, or misconfigurations, for example, gaining access to the command prompt with administrator privileges.

Lateral Movement

Once they have successfully escalated privileges, adversaries quickly move sideways into other systems within the network. This enables them to expand the attack to search for other vulnerabilities and reach their targets. There are five common techniques that attackers use to move across a network, utilizing legitimate system tools to remain undetected:

1. **Internal spear phishing:** With access to a legitimate account, the adversary can send targeted phishing emails to other employees within the organization.
2. **Pass the hash (PtH) attacks:** This tactic takes advantage of the way passwords are commonly stored — as cryptographic depictions known as hashes — to enter secured systems without needing the actual password. It accomplishes this by capturing a "hashed' user credential (a stored version of the password).
3. **Pass the ticket (PtT) attacks:** The Kerberos protocol is a computer network authentication protocol that uses cryptography to verify user identities and to authenticate applications. A PtT attack uses stolen Kerberos ticket granting tickets (TGTs, user authentication tokens) to gain unauthorized access to target systems.
4. **Exploiting remote services:** Attackers may exploit programming errors in a program, service, or operating system to execute malicious code. Several such vulnerabilities currently exist in common services, such as remote desktop protocol (RDP) and server message block (SMB).
5. **Living-off-the-land tools:** Living-off-the-land attacks exploit existing system functionalities, such as PowerShell or Windows Management Instrumentation (WMI), to carry out malicious activity. This tactic allows the attacker to blend in with normal operations.

Exfiltration

With elevated privileges, the attacker can copy, transfer, or retrieve sensitive information — such as personal data, financial records, intellectual property, confidential business data, and so on — from a computer network.

The Limitations of Current Solutions in Detecting Lateral Movement

Despite advancements in security technology, detecting lateral movement remains challenging, thanks to the diverse range of attack techniques and their ability to mimic legitimate user behavior. Here are three key limitations:

1. Insufficient Network Visibility

Lateral movement initiates through external systems, where it slips through unnoticed. At this point, the intrusion becomes more difficult to detect, as traditional security solutions like firewalls and perimeter-based defenses have limited visibility inside the network. Attackers can exploit these blind spots, moving undetected between systems. Current solutions may not have the granular visibility needed to monitor internal network traffic effectively, especially in complex, segmented environments or when attackers use encrypted traffic to mask their actions.

2. Limited Contextual Understanding

Another reason it can be difficult to detect the hidden indicators of lateral movement is that many cybersecurity solutions struggle to correlate events across different systems and environments. Because attackers frequently leverage legitimate credentials or tools (such as PowerShell or RDP) to mimic regular network activity, it is difficult to distinguish their actions from benign behavior. Without sufficient context — such as a baseline understanding of normal user and system behavior — these subtle anomalies often go undetected.

3. Inadequate Detection of stealthy Techniques

As described earlier, attackers frequently use advanced techniques like living off the land or disabling security logging to avoid detection during lateral movement. These “low-and-slow” tactics often generate fewer logs or alerts, making them harder for many cybersecurity tools to detect. This makes it difficult for solutions that rely on signatures or basic anomaly detection to spot lateral movement before it causes significant damage.

These limitations underscore the need for advanced, behavior-based detection and better network traffic analysis to improve lateral movement detection in today’s cybersecurity environments.

Indicators of Lateral Movement

Adversaries will try every tool in their arsenals to avoid detection. It’s imperative for organizations and users to continually monitor systems to detect lateral movement. Indicators of lateral movement may include:

- **Suspicious network connections:** Significant data transfers between systems that normally do not communicate, spikes in traffic, or unusual port usage
- **Abnormal access patterns:** A user account suddenly accesses a much wider range of systems than usual
- **Uncommon application activity:** Unusual use of PowerShell or WMI, especially on a system where such activity is unexpected
- **Unusual file activity:** Large or unusual file transfers between systems, especially when they involve sensitive data

Strategies to Detect Lateral Movement in 2025

Since lateral movement often mimics legitimate user behavior, organizations may struggle to prevent it entirely. However, the risk can be mitigated by implementing the tools and strategies outlined below:

- **Security information and event management (SIEM):** Collects event log data from various sources, such as operating systems, databases, and applications, and uses analytics to detect threats and prioritize alerts. Modern SIEMs can detect unusual patterns and utilize AI-powered analytics to reduce noise by minimizing false positives/negatives, enabling security teams to focus on critical alerts.
- **Endpoint detection and response (EDR):** Much like a SIEM, EDR uses data analytics to identify suspicious activity. However, EDR focuses solely on endpoints, such as laptops, desktops, mobile phones, and virtual machines.
- **Implement user entity and behavior analytics (UEBA) capabilities:** UEBA collects information from various systems, applications, networks, and devices to establish baseline behavior patterns. Using machine learning and advanced analytics, UEBA identifies abnormal behavior patterns to help identify sophisticated cyberattacks. UEBA helps organizations detect techniques more quickly than rules-based detections.
- **Elevate threat intelligence:** AI-enabled threat intelligence platforms (TIPs) analyze threat data from multiple sources (both internal and external) to identify indicators of lateral movement. Machine learning algorithms can automatically correlate data across threat reports, identify lateral movement patterns, and generate actionable intelligence for security teams. By continuously refining threat models, AI improves the accuracy and relevance of threat intelligence in detecting lateral movement.
- **Continuously monitor the attack surface:** Actively monitor digital assets for potential vulnerabilities, such as outdated software, misconfigurations, or exposed sensitive data, to help identify new threats and points of exploitation.
- **Enable multifactor authentication (MFA):** Also known as two-step authentication, MFA requires users to provide multiple forms of identification (such as a one-time password plus a biometric, such as face identification) to log in to an account. MFA acts as an additional layer of security to prevent unauthorized users from accessing these accounts, even when a password has been stolen.
- **Set up user accounts with "least privilege:"** Limit user access to the minimum resources and permissions required to complete their jobs and/or tasks.
- **Enforce password management across the organization:** Implement organization-wide strategies to encourage the creation of unique, strong passwords for all online accounts and help users securely store them. If selecting a password management platform, make sure that it uses end-to-end encryption.
- **Segment networks:** Divide larger computer networks into smaller, distinct subnetworks. This allows administrators to control traffic flow between segments and implement specific security policies for each.
- **Regular vulnerability scanning:** Use automated tools to find and assess security flaws in an organization's IT systems, networks, and software. This will help organizations identify potential weaknesses, such as missing security updates and misconfigurations.

Detecting Lateral Movement with Anomali

The Anomali Security and IT Operations Platform is optimized to address the challenges involved with detecting lateral movement, offering real-time threat intelligence, advanced analytics, and seamless integration with existing security tools. It safeguards enterprise networks through:

- **Real-time advanced threat detection:** Anomali's AI-driven analytics provide real-time visibility into lateral movement activity. This enables security teams to detect and respond to threats before attackers can escalate privileges or exfiltrate data.
- **Comprehensive threat intelligence:** By aggregating threat data from multiple sources and correlating it with internal telemetry, Anomali ensures that security teams have the most up-to-date, relevant intelligence to help detect lateral movement.
- **Security orchestration and response (SOAR):** With SOAR integration, Anomali can automate responses to lateral movement threats, such as quarantining compromised systems or blocking network traffic. By coordinating actions among people and tools within a unified system, Anomali's platform minimizes the time and complexity involved in investigating and responding to lateral movement.
- **Seamless integration with existing security tools:** Anomali's integrations ensure that intelligence related to lateral movement is shared across the organization's security infrastructure, enhancing the detection and response capabilities of other security tools.
- **Scalability and future-proofing:** At the core of the Anomali platform is an integrated Data Lake that does not depend on an external big data provider. Anomali's Data Lake offers a lookback period of over seven years. It enables you to search petabytes of structured and unstructured data, delivering results in seconds, not hours or days. It is built to scale with the dynamic nature of the cybersecurity landscape, so you can detect and neutralize lateral movement effectively, even as attackers evolve their tactics.

Anomali: The Future of SIEM

Anomali is a groundbreaking AI-Powered Security and IT Operations Platform that provides comprehensive visibility, speed, AI, and world-class threat intelligence in one easy-to-use integrated platform. Only Anomali combines ETL, SIEM, Next-Gen SIEM, XDR, UEBA, SOAR, and TIP to consolidate your tech stack and empower your team to do more with less.

Discover how Anomali can help you prevent lateral movement within your organization — schedule a demo.

Security and IT Operations Done Differently.

Anomali delivers the leading AI-Powered Security and IT Operations Platform. Only Anomali integrates ETL, SIEM, Next-Gen SIEM, XDR, UEBA, SOAR, and TIP into one powerful platform. At the center is the Anomali Copilot that navigates a proprietary cloud-native security and IT data lake to drive first-in-market speed, scale, and performance at a fraction of the cost. Modernize security and IT operations to protect and accelerate your organization with better analytics, visibility, productivity, and talent retention.

Be Different. Be the Anomali. **Request a demo** to learn more.

ANOMALI