What is Lateral Movement?

crowdstrike.com/cybersecurity-101/lateral-movement

Lateral Movement

February 18, 2022

Lateral movement refers to **the techniques that a cyberattacker uses, after gaining initial access, to move deeper into a network** in search of sensitive data and other high-value assets. After entering the network, the attacker maintains ongoing access by moving through the compromised environment and obtaining increased privileges using various tools.

> Lateral movement is a key tactic that distinguishes today's advanced persistent threats (APTs) from simplistic cyberattacks of the past.

Lateral movement allows a threat actor to avoid detection and retain access, even if discovered on the machine that was first infected. And with a protracted dwell time, data theft might not occur until weeks or even months after the original breach.

After gaining initial access to an endpoint, such as through a phishing attack or malware infection, **the attacker impersonates a legitimate user and moves through multiple systems in the network** until the end goal is reached. Attaining that objective involves gathering information about multiple systems and accounts, obtaining credentials, escalating privileges and ultimately gaining access to the identified payload.

2022 CrowdStrike Global Threat Report

Download the **2022 Global Threat Report** to find out how security teams can better protect the people, processes, and technologies of a modern enterprise in an increasingly ominous threat landscape.

Download Now

Common Stages of Lateral Movement

There are three main stages of lateral movement: reconnaissance, credential/privilege gathering, and gaining access to other computers in the network.

Reconnaissance

During reconnaissance, the attacker observes, explores and maps the network, its users, and devices. This map allows the intruder to understand host naming conventions and network hierarchies, identify operating systems, locate potential payloads and acquire intelligence to make informed moves.

Threat actors deploy a variety of tools to find out where they are located in the network, what they can get access to and what firewalls or other deterrents are in place. An attacker can leverage many external custom tools and open-source tools for port scanning, proxy connections and other techniques, but employing built-in Windows or support tools offer the advantage of being harder to detect.

Here are some of the built-in tools that can be used during reconnaissance:

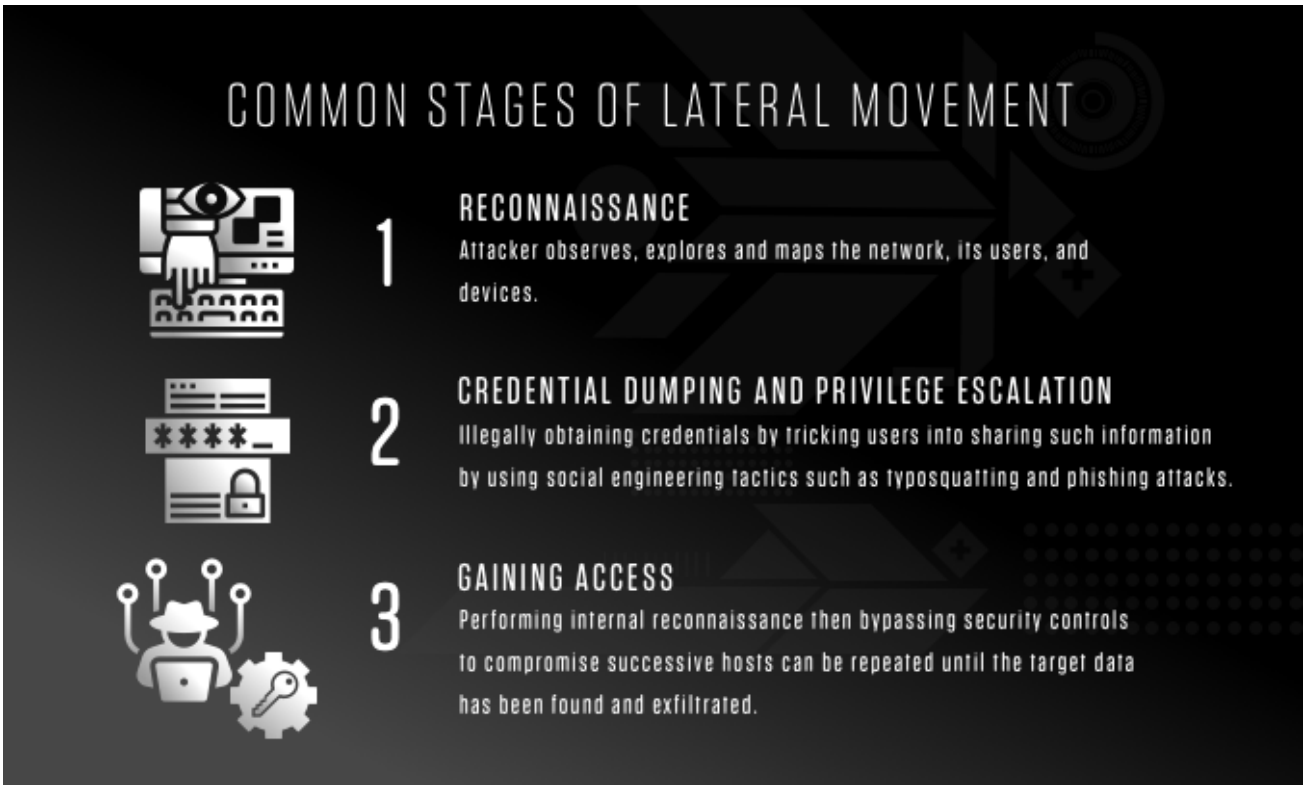
- **Netstat** shows the machine's current network connections. This can be used for identifying critical assets or for gaining knowledge about the network.
- **IPConfig/IFConfig** provides access to the network configuration and location information.
- **ARP cache** gives information about the IP address to physical address. This information can be used to target individual machines inside the network.
- **The Local Routing** table displays current communication paths for the connected host.
- **PowerShell**, a powerful command line and scripting tool, allows quick identification of network systems to which the current user has local admin access.

Once the attacker has identified critical areas to access, the next step is gathering login credentials that will allow entry.

Credential Dumping and Privilege Escalation

To move through a network, an attacker needs valid login credentials. The term used for illegally obtaining credentials is called "credential dumping." One way to obtain these credentials is to trick users into sharing them by using social engineering tactics such as typosquatting and phishing attacks. Other common techniques for stealing credentials include:

- **Pass the Hash** is a method of authenticating without having access to the user's password. This technique bypasses standard authentication steps by capturing valid password hashes that once authenticated allow the attacker to perform actions on local or remote systems.
- **Pass the Ticket** is a way of authenticating using Kerberos tickets. An intruder that has compromised a domain controller can generate a Kerberos "golden ticket" offline that remains valid indefinitely and can be used to impersonate any account, even after a password reset.
- **Tools like Mimikatz** are used to steal cached plaintext passwords or authentication certificates from the memory of a compromised machine. They can then be used to authenticate to other machines.
- **Keylogging tools** allow the attacker to capture passwords directly when an unsuspecting user enters them via the keyboard.



Gaining Access

The process of performing internal reconnaissance and then bypassing security controls to compromise successive hosts can be repeated until the target data has been found and exfiltrated. And, as cyberattacks become more sophisticated, they often contain a strong human element. This is particularly true for lateral movement, when an organization might be faced with moves and countermoves from an adversary. But human behavior can be detected — and intercepted — by a robust security solution.

Detecting and Preventing Lateral Movement

Once an attacker secures administrative privileges and gains deeper access into a network, malicious lateral movement can be very difficult to detect because it can appear to be "normal" network traffic. Also, a human attacker has the ability to change plans and deploy different techniques and tools based on the information collected. And when the adversary utilizes built-in system tools, detection becomes even harder. It's essential to find and remove these intruders as quickly as possible to avoid costly losses.

Breakout Time and the 1-10-60 Rule

Breakout time is the time it takes for an intruder to begin moving laterally into other systems in the network after initially compromising a machine. Last year, CrowdStrike tracked an average breakout time of 1 hour and 58 minutes. This means an organization has roughly two hours to detect, investigate and remediate or contain the threat. If it takes longer, you run the risk of the adversary stealing or destroying your critical data and assets.

> To win a battle in cyberspace, speed is paramount. The only way to beat an adversary is by being faster — by detecting, investigating and containing an intrusion within "breakout time."

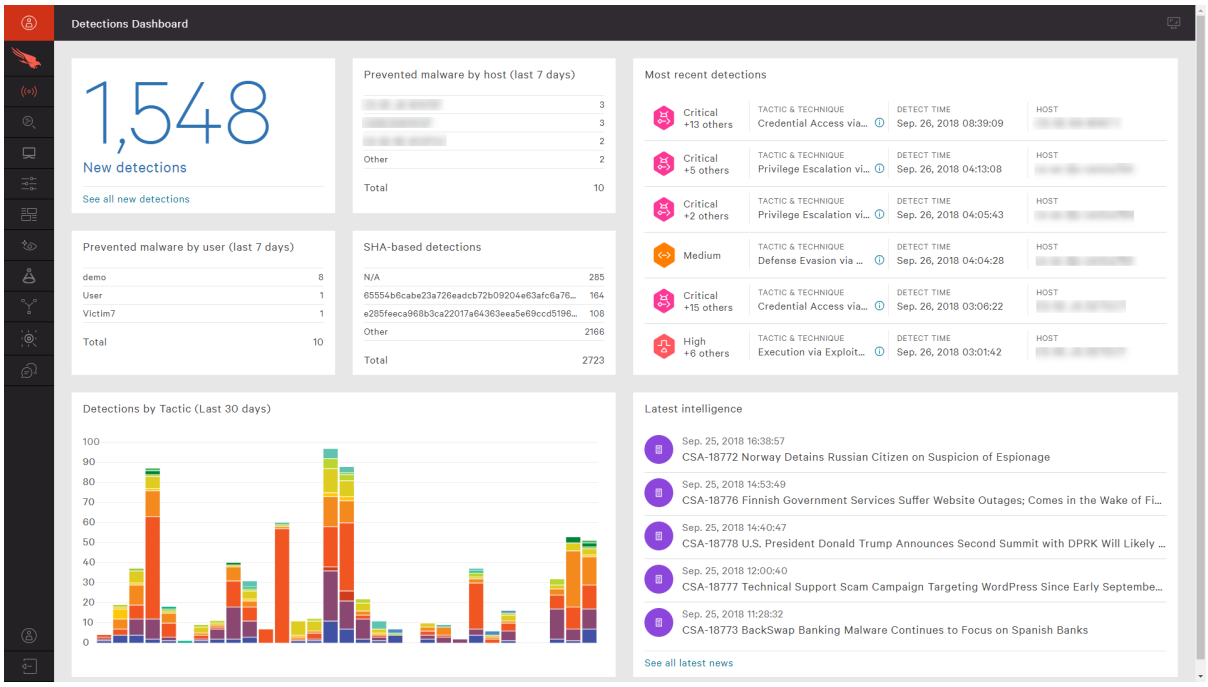
Top private-sector companies strive to adhere to what CrowdStrike refers to as **the 1-10-60 rule — detecting an intrusion within 1 minute, investigating within 10 minutes and isolating or remediating the problem within 60 minutes**. The longer an adversary is allowed to engage in lateral movement over a protracted dwell time, the more likely an attack will eventually succeed.

Steps to Preventing Lateral Movement

There are three critical steps you can and should take to strengthen your defenses and diminish or eliminate dwell time and its consequences.

Step 1: Update Your Endpoint Security Solution

Many high-profile attacks occurred over months of dwell time and moved laterally to easily evade standard security. Modern attackers count on the fact that many organizations continue to rely on legacy or standard security solutions — the kind of technology that is easily bypassed by modern hacking tools. Now it's mandatory to upgrade to comprehensive technology that includes next-gen AV and behavioral analysis capabilities if you aim to combat today's sophisticated attacks.



CrowdStrike's dashboard provides immediate visibility into detections

Also, reevaluate your security strategy to ensure that you have the most effective security approach possible — one that includes both prevention technology to stop intrusion attempts and full EDR (endpoint detection and response) to automatically detect suspicious activity. Having both capabilities in a single agent is an essential first step.

Step 2: Proactively Hunt for Advanced Threats

Many organizations fall victim to breaches not because of a lack of alerts but because they have too many to investigate. Over-alerting and false positives can result in alert fatigue.

If your security solutions are delivering too many false positives, or you're getting alerts with no context and no way to prioritize them, then it's only a matter of time before a critical alert gets missed. It's vitally important to have real experts proactively looking at what's occurring in your environment and sending detailed alerts to your team when unusual activity is detected.

Consider augmenting your internal teams with a security solution that provides hands-on expert threat hunting that can monitor proactively for hidden threats and minimize false positives, while providing prioritization to ensure that the most critical alerts are addressed immediately.

Step 3: Maintain Proper IT Hygiene

Eliminate vulnerabilities such as outdated or unpatched systems and software that may be lurking in your network environment. Exploits can remain hidden for long periods of time before becoming active, and organizations will be exposed if they fail to apply patches and updates across all of their endpoints.

Ultimately, your best defense is to make sure your organization is deploying the most effective technology currently available and incorporating the 1-10-60 rule in your cybersecurity strategy.

Achieving this benchmark requires true next-generation solutions such as the CrowdStrike Falcon® platform, which offers endpoint detection and response (EDR), managed threat hunting, next-gen AV with behavioral analytics and machine learning, and automated threat intelligence. These tools are key to gaining the visibility and context you need to meet critical, outcome-driven metrics and win the race against today's — and tomorrow's — most sophisticated adversaries.