Lateral Movement, Tactic TA0033 - Mobile

Archived: 2026-04-05 15:31:00 UTC

The adversary is trying to move through your environment.

Lateral movement consists of techniques that enable an adversary to access and control remote systems on a network and could, but does not necessarily, include execution of tools on remote systems. The lateral movement techniques could allow an adversary to gather information from a system without needing additional tools, such as a remote access tool.

ID: TA0033

Created: 17 October 2018

Last Modified: 25 April 2025

Techniques

Techniques: 2

ID	Name	Description
T1428	Exploitation of Remote Services	Adversaries may exploit remote services of enterprise servers, workstations, or other resources to gain unauthorized access to internal systems once inside of a network. Adversaries may exploit remote services by taking advantage of a mobile device’s access to an internal enterprise network through local connectivity or through a Virtual Private Network (VPN). Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. A common goal for post-compromise exploitation of remote services is for lateral movement to enable access to a remote system.
T1458	Replication Through Removable Media	Adversaries may move onto devices by exploiting or copying malware to devices connected via USB. In the case of Lateral Movement, adversaries may utilize the physical connection of a device to a compromised or malicious charging station or PC to bypass application store requirements and install malicious applications directly. In the case of Initial Access, adversaries may attempt to exploit the device via the connection to gain access to data stored on the device. Examples of this include:

Source: https://attack.mitre.org/tactics/TA0033