MITRE ATT&CK Enterprise Techniques for Windows

The MITRE ATT&CK framework provides a comprehensive knowledge base of adversary tactics and techniques based on real-world observations. Enterprise techniques specifically target Windows environments, representing the "how" behind cyber attacks. Each technique demonstrates how adversaries achieve tactical objectives through specific actions, such as dumping credentials for credential access or exploiting vulnerabilities for initial access.

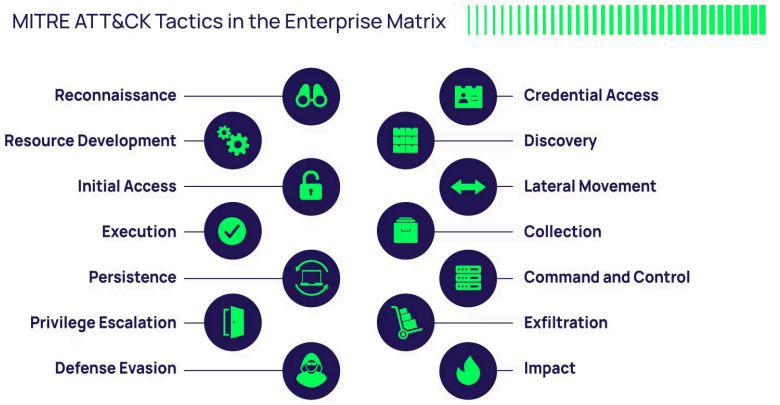
This framework serves as the foundation for threat hunting, detection engineering, and security operations across enterprise Windows infrastructures.

Introduction to the MITRE ATT&CK Framework

MITRE ATT&CK (Adversarial Tactics, Techniques & Common Knowledge) is a globally accessible knowledge base that catalogs adversary behavior across the cyber attack lifecycle. Originally developed by MITRE Corporation, it has become the industry standard for understanding and defending against advanced persistent threats.

The framework organizes adversary behavior into tactics (the "why") and techniques (the "how"), providing security teams with a common language to describe, detect, and respond to cyber threats. For Windows enterprise environments, it covers 14 tactical categories spanning initial access through impact.

Security practitioners use ATT&CK to develop detection rules, conduct threat hunting operations, and assess defensive coverage gaps across their Windows infrastructure.



Tactics

The adversary's tactical goal - the reason for performing an action

Techniques

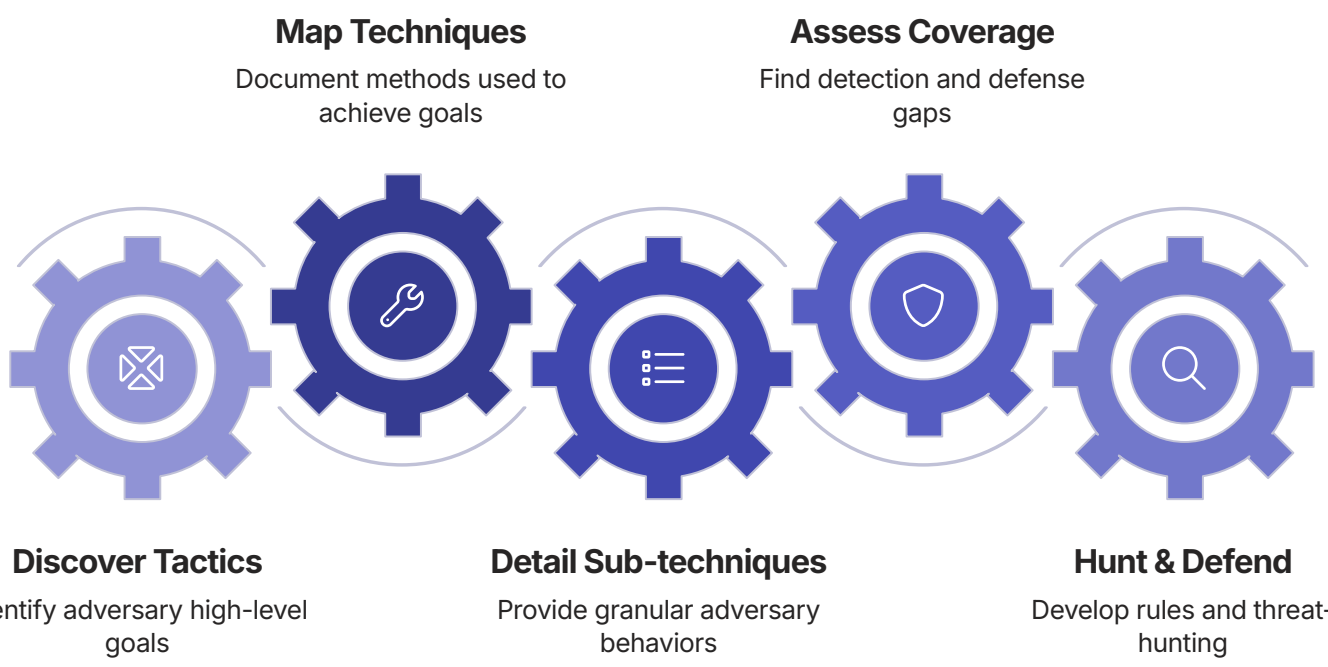
How an adversary achieves a tactical goal by performing an action

Sub-techniques

More specific descriptions of adversarial behavior used to achieve a technique

Enterprise Windows Techniques Summary

The MITRE ATT&CK Enterprise matrix contains 14 tactical categories with hundreds of specific techniques targeting Windows environments. Each tactic represents a different phase of the adversary lifecycle, from gaining initial access to achieving their ultimate objectives.



01

Initial Access

Techniques for gaining entry into networks through spear-phishing, exploiting public-facing applications, or using valid accounts. Common Windows vectors include malicious Office documents and RDP exploitation.

02

Execution

Running malicious code on Windows systems using PowerShell, Windows Command Shell, scheduled tasks, or exploiting Windows services and applications to execute payloads.

03

Persistence

Maintaining access through registry modifications, scheduled tasks, Windows services, or creating new user accounts to survive system reboots and maintain long-term presence.

04

Privilege Escalation

Elevating permissions using techniques like UAC bypass; **User Account Control (UAC) bypass** is a technique used by attackers to execute malicious code or perform administrative actions with **elevated privileges** on a Windows system, **without triggering the user prompt** that typically asks for permission. Exploiting unquoted service paths, DLL hijacking, or leveraging Windows vulnerabilities for higher-level access.

05

Defense Evasion

Avoiding detection through process injection, disabling Windows Defender, clearing event logs, or using legitimate Windows tools to blend in with normal activity.

06

Credential Access

Obtaining credentials through LSASS memory dumping; The Windows **Local Security Authority Subsystem Service (LSASS)**, or `lsass.exe`, is a core security process responsible for enforcing local security policies, validating users for local and remote sign-ins, and creating access tokens. Because it stores sensitive authentication data like passwords and Kerberos tickets in memory, it is a common target for attackers seeking to steal credentials. **Kerberoasting**; is a post-exploitation cyberattack technique used to steal the credentials of service accounts in a Microsoft Active Directory (AD) environment. Attackers exploit a legitimate function of the Kerberos authentication protocol to obtain encrypted password hashes, which they then crack offlinepassword spraying, or accessing Windows Credential Manager to harvest stored authentication data.

Discovery

Gathering information about the Windows environment, including network shares, running processes, system information, and domain reconnaissance using built-in Windows commands.

Lateral Movement

Moving through the network using Windows protocols like SMB; **SMB** (Server Message Block) file sharing is a network protocol that allows computers to share files, printers, and other resources over a network, primarily used in Windows environments. WMI, RDP, or exploiting Windows services to access additional systems and expand their foothold.

Collection & Exfiltration

Gathering sensitive data from Windows file systems, email, and applications, then transferring it outside the network through various channels and protocols.

Impact

Achieving final objectives through data destruction, ransomware deployment, or service disruption, often targeting critical Windows infrastructure and business operations.

Example of a technique used against Windows machines for each Tactic.

Below are concrete examples of how adversaries might leverage specific techniques within each MITRE ATT&CK tactic, targeting Windows environments.

1

Initial Access

Phishing: Spearphishing Attachment (T1566.001)

Adversaries send malicious email attachments (e.g., weaponized Office documents or executables) to gain initial access when opened by a user on a Windows machine.

2

Execution

Command and Scripting Interpreter: PowerShell (T1059.001)

Attackers use PowerShell to execute arbitrary commands, download additional payloads, or configure system settings on compromised Windows systems without relying on external tools.

3

Persistence

Boot or Logon Autostart Execution: Scheduled Task/Job (T1053.005)

An adversary creates or modifies a Windows scheduled task to automatically run malicious code at specific times, during system startup, or upon user logon to maintain access.

4

Privilege Escalation

Bypass User Account Control (T1548.002)

Attackers exploit vulnerabilities or misconfigurations in UAC to execute processes with elevated administrative privileges without prompting the user for approval.

5

Defense Evasion

Impair Defenses: Disable or Modify System Firewall (T1562.004)

Adversaries use commands like `netsh advfirewall` to disable the Windows Firewall or add rules that allow their C2 traffic and prevent detection.

6

Credential Access

OS Credential Dumping (T1003)

Techniques such as dumping the Local Security Authority Subsystem Service (LSASS) process memory are used to extract hashed or clear-text credentials from a Windows system.

7

Discovery

System Information Discovery (T1082)

Attackers run commands like `systeminfo` or query the Windows Registry to gather details about the operating system version, installed hotfixes, network configuration, and other system properties.

8

Lateral Movement

Remote Services: SMB/Windows Admin Shares (T1021.002)

Adversaries use valid credentials to access shared folders (e.g., C$, ADMIN$) on remote Windows machines via SMB to execute remote commands or transfer files.

9

Collection & Exfiltration

Data from Local System (T1005) & **Exfiltration Over Web Service** (T1041)

Sensitive data (e.g., documents, databases) is located on the local system, compressed into an archive, and then sent out of the network over common web protocols like HTTPS.

10

Impact

Data Encrypted for Impact (T1486)

Ransomware attacks encrypt critical files on Windows servers and workstations, rendering them inaccessible until a ransom is paid, directly impacting business operations.

Example of a sub-technique used against Windows machines for each tactic.

Below are concrete examples of how adversaries might leverage specific sub-techniques within each MITRE ATT&CK tactic, targeting Windows environments.

1

Reconnaissance

Active Scanning: Vulnerability Scan (T1595.002)

Adversaries may perform vulnerability scans against public-facing Windows servers or services to identify exploitable weaknesses for initial access.

2

Resource Development

Develop Capabilities: Malware (T1587.001)

Threat actors develop custom malware, often designed to run on Windows, such as backdoors, ransomware, or infostealers, before deploying it in an attack.

3

Initial Access

Phishing: Spearphishing Attachment (T1566.001)

Adversaries send malicious email attachments (e.g., weaponized Office documents) to gain initial access when opened by a user on a Windows machine, leveraging the built-in macro functionality or vulnerabilities.

4

Execution

Command and Scripting Interpreter: PowerShell (T1059.001)

Attackers use PowerShell to execute arbitrary commands, download additional payloads, or configure system settings on compromised Windows systems, often through obfuscated scripts to evade detection.

5

Persistence

Boot or Logon Autostart Execution: Scheduled Task/Job (T1053.005)

An adversary creates or modifies a Windows scheduled task to automatically run malicious code at specific times, during system startup, or upon user logon to maintain long-term access.

6

Privilege Escalation

Bypass User Account Control (T1548.002)

Attackers exploit vulnerabilities or misconfigurations in UAC to execute processes with elevated administrative privileges on Windows without prompting the user for approval.

7

Defense Evasion

Impair Defenses: Disable or Modify System Firewall (T1562.004)

Adversaries use commands like `netsh advfirewall` to disable the Windows Firewall or add rules that allow their C2 traffic and prevent detection.

8

Credential Access

OS Credential Dumping: LSASS Memory (T1003.001)

Techniques such as dumping the Local Security Authority Subsystem Service (LSASS) process memory are used to extract hashed or clear-text credentials from a Windows system's memory.

9

Discovery

System Information Discovery (T1082)

Attackers run commands like `systeminfo` or query the Windows Registry to gather details about the operating system version, installed hotfixes, network configuration, and other system properties.

10

Lateral Movement

Remote Services: SMB/Windows Admin Shares (T1021.002)

Adversaries use valid credentials to access shared folders (e.g., C$, ADMIN$) on remote Windows machines via SMB to execute remote commands or transfer files.

11

Collection

Data from Local System (T1005)

Sensitive data (e.g., documents, databases, browser history) is located and staged from various locations on the local Windows file system for exfiltration.

12

Exfiltration

Exfiltration Over Web Service: Exfiltration to Cloud Storage (T1567.002)

Collected data from Windows systems is transferred out of the network by uploading it to cloud storage services (e.g., Dropbox, OneDrive) controlled by the attacker.

13

Command and Control

Application Layer Protocol: Web Protocols (T1071.001)

Adversaries use common web protocols like HTTP or HTTPS for command and control communication, blending in with legitimate Windows network traffic.

14

Impact

Data Encrypted for Impact (T1486)

Ransomware attacks encrypt critical files on Windows servers and workstations, rendering them inaccessible until a ransom is paid, directly impacting business operations and data availability.