PICUS

THE RED REPORT 2023

The Top 10 Most Prevalent MITRE ATT&CK Techniques Used by Adversaries

CISO EDITION

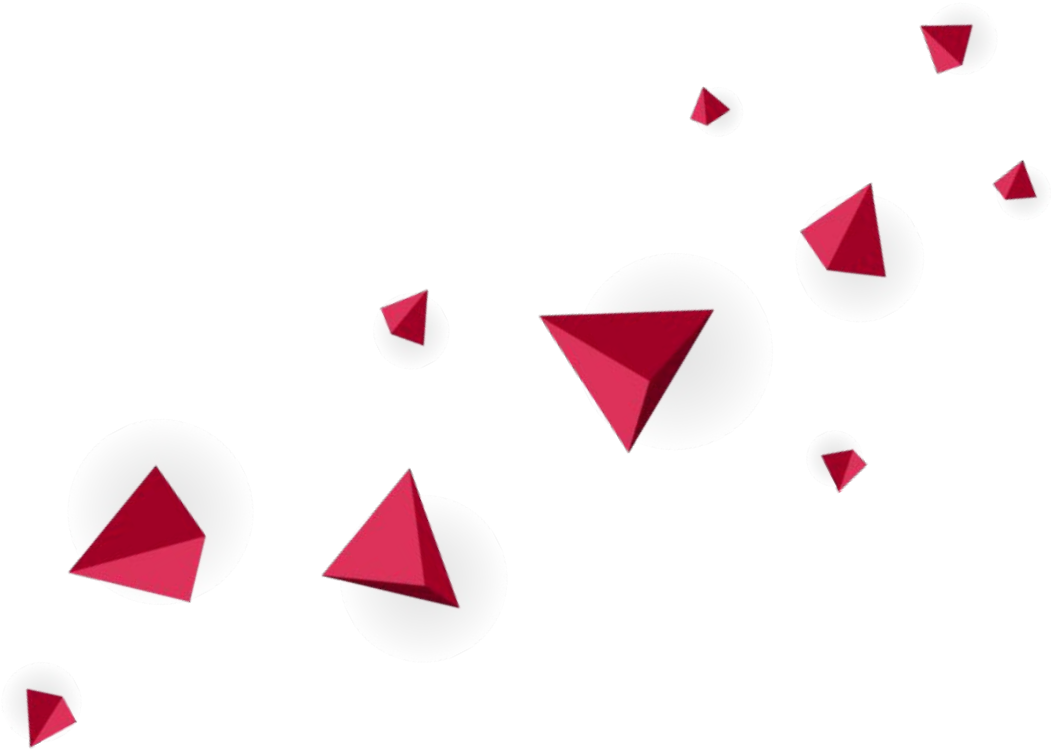
Introduction

Welcome to The Red Report 2023, a comprehensive analysis of the most prevalent MITRE ATT&CK® tactics and techniques used in 2022 and how they were leveraged by threat actors. This research was conducted by Picus Labs, the research arm of Picus Security, and is based on an in-depth analysis of over 500,000 real-world malware samples collected from a wide range of sources.

The goal of the Red Report is to share our knowledge about the most commonly used attack techniques and their use cases, so that security teams can adopt a more threat-centric approach and prioritize threat prevention, detection, and response efforts.

Please note that this CISO Edition of the Red Report 2023 is designed to be read by security leaders that want an overview of the research's findings. Consult the full report for more detailed insights.

Table of Contents



Executive Summary

Picus Labs analyzed over 500,000 malware samples between January 2022 and December 2022 to identify the tactics, techniques, and procedures (TTPs) they exhibited. Each observed TTP was categorized using the MITRE ATT&CK® Framework. In total, Picus Labs observed more than 4.3 million ATT&CK techniques and used this data to identify the most prevalent.

The Red Report 2023 highlights the ten most common ATT&CK techniques identified and provides insights to help security teams prioritize their defensive actions accordingly.

Highlighting Lateral Movement of Adversaries

The most significant insight from this year's report is that attackers are increasingly leveraging malware to perform Lateral Movement. Lateral Movement is a tactic that attackers use to move from one compromised system in a network to another, helping them to further their objectives.

T1021 Remote Services and *T1018 Remote System Discovery* are new techniques in this year's Red Report Top Ten that are primarily used for Lateral Movement. The third newcomer in the list, *T1047 Windows Management Instrumentation,* is abused by attackers to execute files and commands in remote systems.

In addition to the techniques above, attackers also leverage *T1059 Command and Scripting Interpreter* and *T1003 OS Credential Dumping*, the first and second most prevalent techniques identified, to execute commands on remote systems and obtain account credentials. These also aid Lateral Movement.

An increase in the prevalence of techniques being performed to conduct lateral movement highlights the importance of enhancing threat prevention and detection both at the security perimeter as well as inside networks.

Methodology

Between January 2022 and December 2022, Picus Labs analyzed 556,107 unique files, with 507,912 (91%) categorized as malicious.

Sources of these files include but are not limited to:

- commercial and open-source threat intelligence services
- security vendors and researchers
- malware sandboxes
- malware databases

From these files, a total of 5,388,946 actions were extracted, an average of 11 malicious actions per malware. These actions were then mapped to MITRE ATT&CK techniques, revealing an average of 9 techniques per malware.

To compile the Red Report 2023 Top Ten, Picus Labs researchers calculated the percentage of malware in the dataset that utilized each ATT&CK technique. For example, the T1059 Command and Scripting Interpreter technique was exhibited by 159,196 (31%) of the 507,912 malicious files analyzed.

556,107
unique files were analyzed

507,912
files were categorized as malicious

91%
categorized as malicious

5,388,946
actions were extracted

11
actions per malware
on average

4,329,142
instances of ATT&CK techniques were identified in total

9
identified per malware
on average

The Red Report Top 10 MITRE ATT&CK Techniques

The most prevalent ATT&CK techniques identified in 2022, listed by the percentage of malware samples in which exhibited the behavior.

T1059 Command and Scripting Interpreter

Execution

T1003 OS Credential Dumping

Credential Access

T1486 Data Encrypted for Impact

Impact

T1055 Process Injection

Defense Evasion | Privilege Escalation

T1082 System Information Discovery

Discovery

T1021 Remote Services

Lateral Movement

T1047 Windows Management Instrumentation

Execution

T1053 Scheduled Task/Job

Execution | Persistence | Privilege Escalation

T1497 Virtualization/Sandbox Evasion

Defense Evasion | Discovery

T1018 Remote System Discovery

Discovery

Key Findings

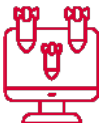
The main insights of the Red Report 2023 for security teams:

Lateral Movement on the Rise:
Attackers Utilize New as well as Tried and Tested Techniques

Attackers are increasingly using techniques to perform Lateral Movement, a tactic to move from one compromised system in a network to another. In addition to *Command and Scripting Interpreter* and *OS Credential Dumping*, which are widely prevalent, new techniques such as *Remote Services*, *Remote System Discovery*, and *WMI* are also increasingly being leveraged to discover remote systems, execute commands on remote systems, and obtain account credentials.

Ransomware Remains Rife:
Data Encryption is a Top Threat

Data Encrypted for Impact has maintained its position as the third most commonly used technique by adversaries for the second consecutive year. This technique, exhibited by nearly a quarter of all malware analyzed, encrypts files and highlights the ongoing threat of ransomware to organizations.



Abuse of Remote Discovery and Access:
Attackers Leverage Windows, Linux, and macOS Built-in Tools

New techniques, *Remote System Discovery* and *Remote Services,* also feature in this year's Red Report Top Ten. These techniques involve abusing built-in tools and protocols in operating systems, such as net, ping, RDP, SSH, and WinRM for malicious purposes. This allows attackers to gather information about targets, including Windows, Linux, and macOS systems in a compromised network, and move laterally throughout the network without being detected by security controls. This trend indicates that attackers are increasingly utilizing legitimate remote discovery and access tools and services.

Identity and Credentials Are the New Perimeter:
Traditional Perimeter Security Is No Longer Enough

T1003 OS Credential Dumping has moved up the Red Report list since last year's report and is now the second most prevalent technique observed. This technique allows attackers to obtain account login and credential information from compromised machines. Any information obtained can then be used to move laterally in a network, elevate privileges, and access restricted information.

The rise in credential dumping emphasizes the fact that traditional perimeter security is no longer enough to protect against cyber attacks. Instead, organizations need to strengthen cyber resilience by preparing to defend against pre-compromise and post-compromise attacks.

Uncovering the Dark Side of Legitimate Tools:
Adversaries Are Weaponizing Legitimate Software in Cyberattacks

The Red Report 2023 reveals the extent to which adversaries prefer using legitimate tools over custom-developed ones. This is highlighted by the most common technique in the Red Report Top Ten list being, *T1059 Command and Scripting Interpreter*, which involves the abuse of legitimate interpreters such as PowerShell, AppleScript, and Unix shells to execute arbitrary commands. Other examples of legitimate tools that are commonly abused by adversaries include utilities for *OS Credential Dumping*, *System Information Discovery*, *Remote Services*, *WMI*, *Scheduled Task/Job*, and *Remote System Discovery*.

Malware Continues to Evolve Rapidly:
The Rise of Multi-faceted Tactics in Cyber Attacks

According to our analysis, on average, malware uses 11 different TTPs (Tactics, Techniques and Procedures). One-third of malware (32%) leverages more than 20 TTPs, and one-tenth of malware employs more than 30 TTPs. These findings suggest that malware developers behind these attacks are highly sophisticated. They have likely invested significant resources into researching and developing a wide range of techniques for evading detection and compromising systems.

Recommendations for Security Teams

To enhance resilience against the techniques listed in The Red Report Top Ten, Picus Labs recommends that security teams should:

Regularly Test and Optimize Security Controls

The Red Report Top 10 highlights the threat landscape is constantly evolving, as attackers continuously develop new attack and evasion techniques. Regular testing and tuning of security controls is essential to ensure that security measures are able to detect and prevent the latest evasive attack techniques. By optimizing security controls, organizations can improve their overall cyber defense posture and reduce the risk of successful cyber attacks.

Leverage Behavioral Detection

Adversaries are increasingly using legitimate tools and services for malicious purposes and evading detection. Security teams should use behavioral detection techniques that focus on identifying malicious activity based on how it deviates from normal behavior, rather than trying to identify and block known static Indicators of Compromise (IOCs). This will allow teams to detect attacks that may not be caught by traditional security controls.

Uncover Attack Paths

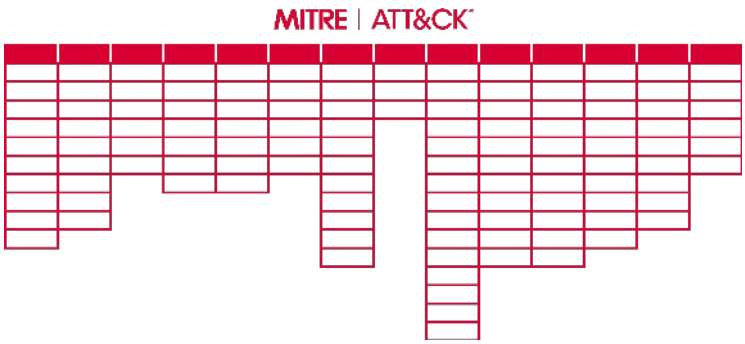
Attackers are using a variety of techniques to move laterally through networks and obtain account credentials. Security teams should reveal attack paths to understand how attackers are moving through a network and what techniques they are using. This will allow teams to identify the root cause of breaches and to focus on the most critical security gaps to prioritize for mitigation. Hereby, organizations can develop a better understanding of the specific steps in an attack, identify the systems and data that are at risk, and implement appropriate security controls to detect and respond to attacks.

Operationalize MITRE ATT&CK

Adversaries use a diverse and evolving set of tactics, techniques, and procedures (TTPs) to carry out cyber attacks. Operationalizing MITRE ATT&CK can help organizations identify, detect, and prevent cyber attacks by providing a comprehensive understanding of the TTPs used by attackers. It also enables organizations to prioritize their defensive efforts, detect and prevent attacks, and improve collaboration.

The MITRE ATT&CK Framework

MITRE ATT&CK (**A**dversarial **T**actics, **T**echniques **& C**ommon **K**nowledge) is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The MITRE ATT&CK framework helps organizations to identify adversary behaviors and prioritize defensive measures accordingly.

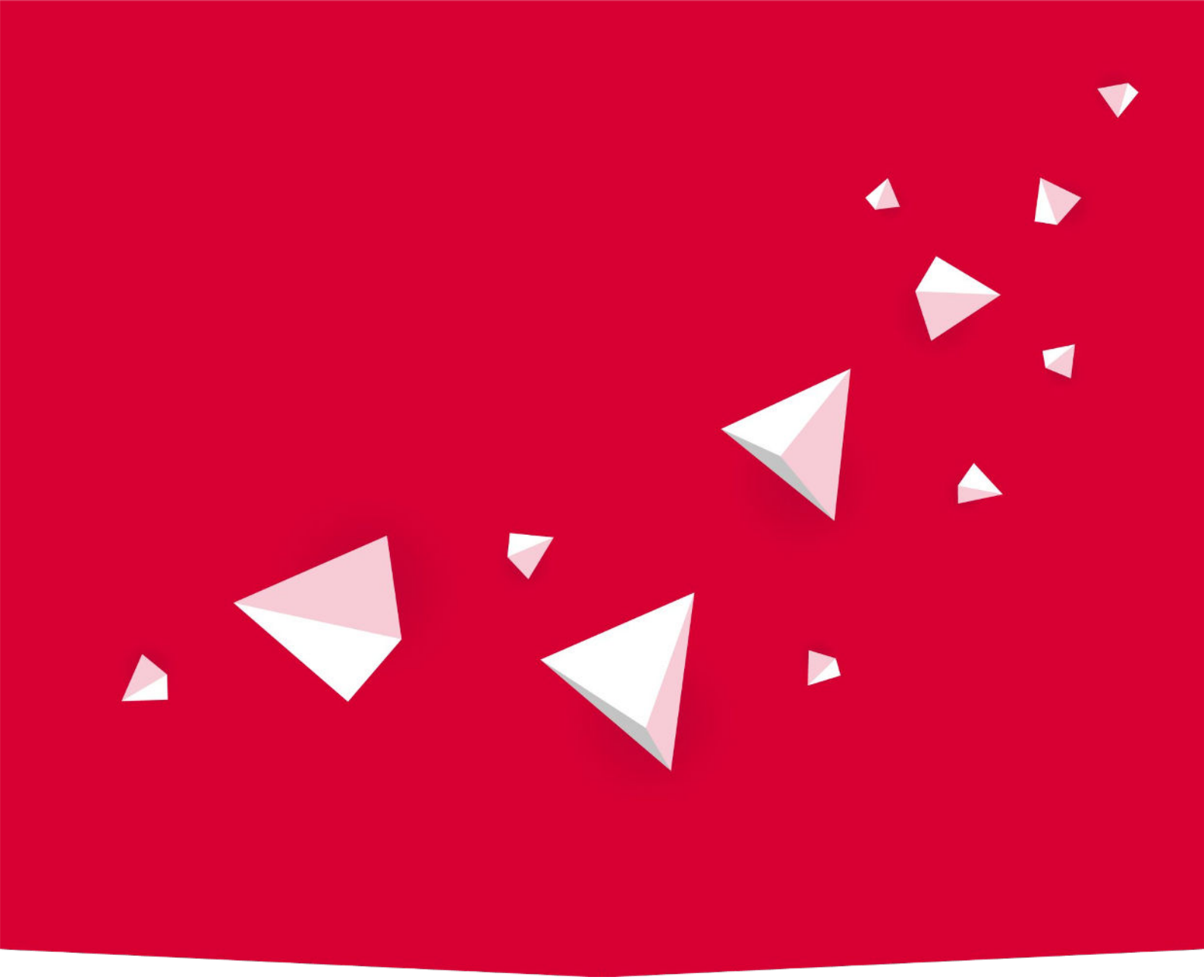


In the MITRE ATT&CK Framework, a "**tactic**" refers to a high-level objective that an adversary is trying to achieve.

For example, an adversary might leverage the "Lateral Movement" tactic, which involves moving from one compromised system to another within a network to further objectives. A "**technique**" is a specific method used by an adversary to achieve a tactic. For instance, an adversary might use the "Remote Services" technique to perform Lateral Movement. A "**sub-technique**" is a specific variation or implementation of a technique. For instance, T1021.001 for Remote Desktop Protocol is a sub-technique of the "Remote Services" technique. The MITRE ATT&CK Matrix for Enterprise v12.1 [1] consists of **14 tactics**, **193 techniques**, and **401 sub-techniques**.

ATT&CK also provides information about threat “**groups**” that are related to an intrusion activity, as well as software utilized by these groups. ATT&CK uses the term "**software**" to define malware, custom or commercial tools, open-source software, and OS utilities that adversaries use. Currently, ATT&CK contains **135 groups** and **718** pieces of **software**.

ATT&CK also includes **43 mitigations**, which describe security concepts and classes of technologies that can be employed to prevent the successful execution of a technique or sub-technique. For detection, ATT&CK provides **39 data sources** with **data components**, which identify specific properties and values of a data source pertinent to identifying a particular ATT&CK technique or sub-technique.



About PICUS

At Picus Security, our priority is making it easy for security teams to continuously validate and enhance organizations' cyber resilience.

Our Complete Security Validation Platform simulates real-world threats to automatically measure the effectiveness of security controls, identify high-risk attack paths to critical assets, and optimize threat prevention and detection capabilities.

As the pioneer of Breach and Attack Simulation, our people and technology empower customers worldwide to be threat-centric and proactive.

For more information, visit **www.picussecurity.com**

THE RED REPORT 2023

CISO EDITION

picussecurity

www.picussecurity.com

PICUS