Sightings Ecosystem: A data-driven Analysis of MITRE ATT&CK® in the Wild 2023 Report

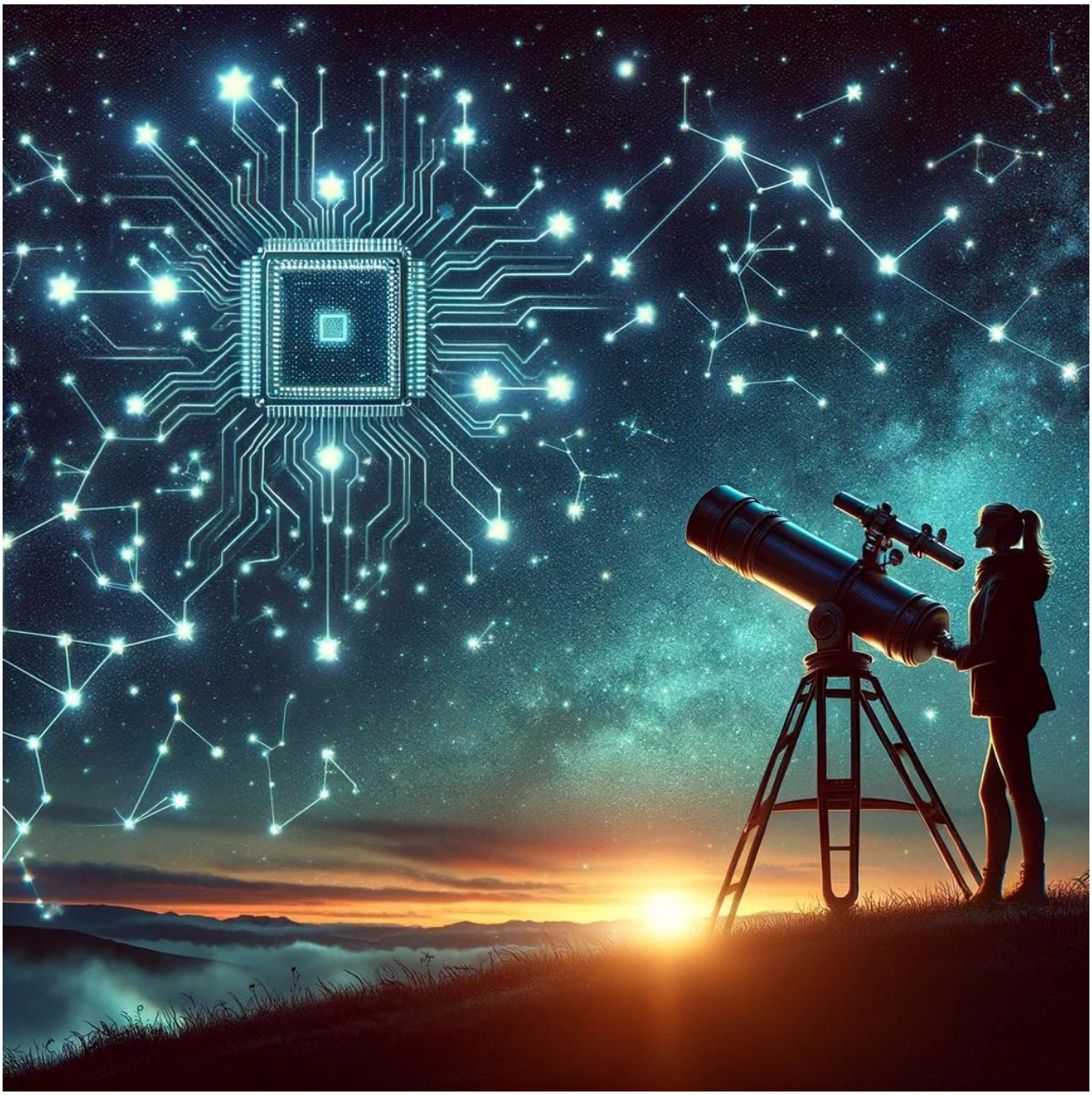


Table of Contents

SIGHTINGS ECOSYSTEM

A DATA-DRIVEN ANALYSIS OF ATT&CK IN THE WILD

Received 1.6m+ Sightings of 353 unique techniques, from 198 countries, observed between August 2021 and September 2023

2021 - 2023
AUGUST SEPTEMBER

1.6M+
SIGHTINGS

353
UNIQUE TECHNIQUES

198
COUNTRIES

COMMON ADVERSARY BEHAVIORS

Which techniques adversaries use

How their use changes over time

How adversaries use techniques together

Top 15 Techniques

Of all techniques observed between 1 August 2021 to 30 September 2023, the top 15 most observed techniques comprise 82 percent of our sightings. This is lower than our last report, where the top 15 techniques comprised 90 percent of all observed techniques. This difference is likely due to the larger data set analyzed for this report, as well as a wider array of unique techniques seen during this timeframe.

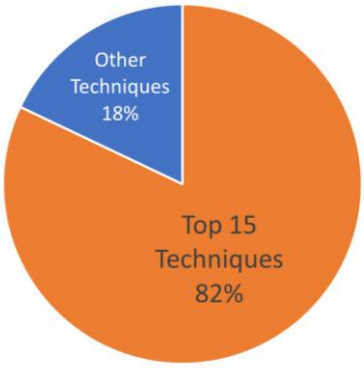


Figure 1. Percentage of top 15 Techniques.

The Top 15 Enterprise Techniques:

1. Command and Scripting Interpreter [T1059]
2. Obfuscated Files or Information [T1027]
3. Ingress Tool Transfer [T1105]
4. Modify Registry [T1112]
5. Indicator Removal [T1070]
6. User Execution [T1204]
7. Hide Artifacts [T1564]
8. Process Injection [T1055]
9. OS Credential Dumping [T1003]
10. Remote Services [T1021]
11. Data Encrypted for Impact [T1486]
12. Replication Through Removable Media [T1091]
13. System Information Discovery [T1082]
14. Windows Management Instrumentation [T1047]
15. Impair Defenses [T1562]

The top 15 Enterprise techniques represent 9 out of 14 ATT&CK Tactics. This demonstrates the range and scope of our most observed data.

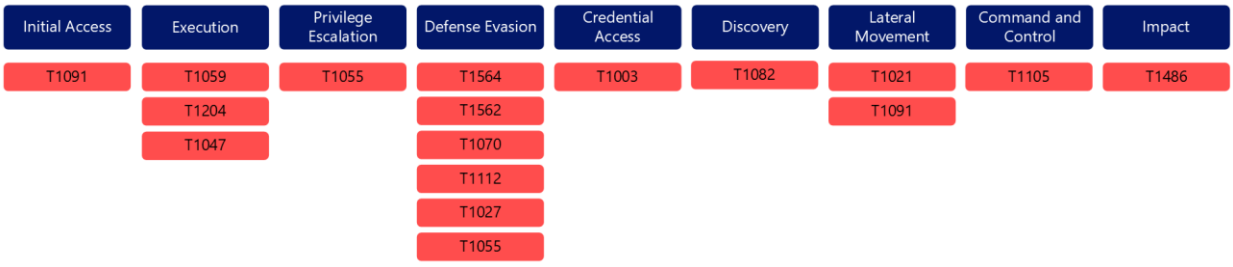


Figure 2. Breakdown of Top 15 Techniques by Tactic[1].

[1] T1055 applies to both Privilege Escalation and Defense Evasion. Similarly, T1091 applies to Initial Access and Lateral Movement.

Top 10 NIST 800-53 Controls

Using the Center's mappings of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 revision 5 to ATT&CK, we can identify which NIST controls are the most effective in protecting against our top 15 techniques. Overall, Access Control, System and Information Integrity, and Configuration Management controls are the most frequently seen.

1. SI-3 Malicious Code Protection
2. SI-4 System Monitoring
3. CM-6 Configuration Settings
4. CM-2 Baseline Configuration
5. AC-3 Access Enforcement
6. AC-6 Least Privilege
7. CM-7 Least Functionality
8. SI-7 Software, Firmware, and Information Integrity
9. CA-7 Continuous Monitoring
10. AC-2 Account Management

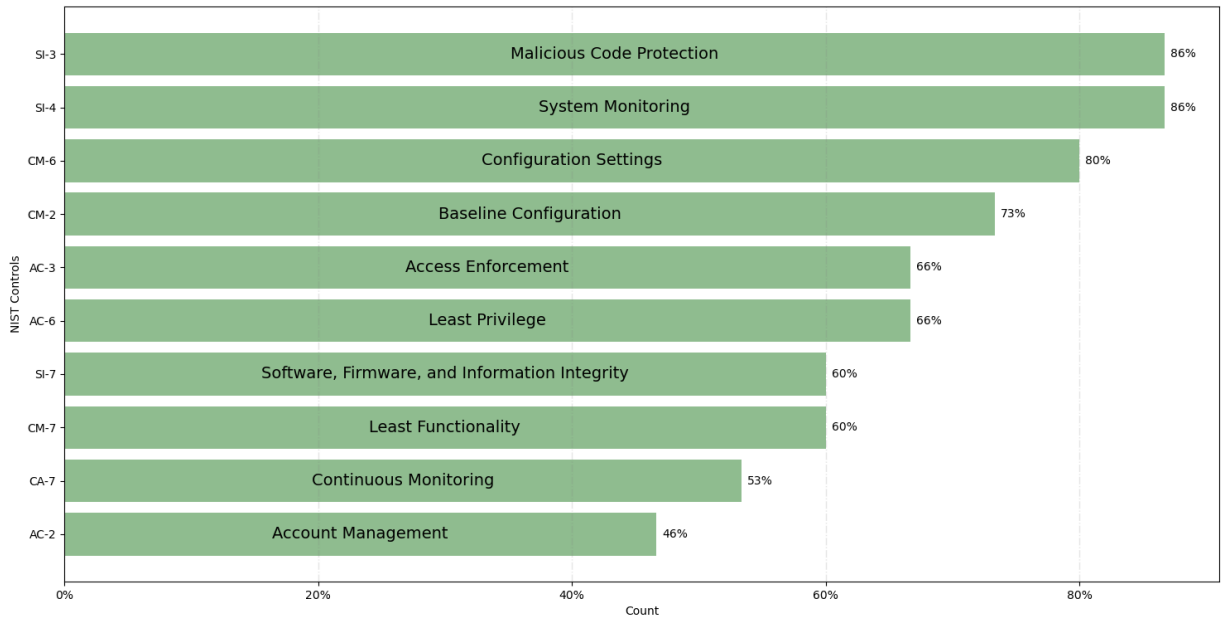


Figure 3. Top 10 NIST Controls and their coverage of the Top 15 Techniques.

Introduction

Adversaries are constantly evolving their attacks, driving up the cost of intrusions. Consequently, defenders must continue to protect against an increasing amount of adversary techniques and behaviors. Despite their best efforts, it is not possible to defend against all potential scenarios. This raises the questions, "How many MITRE ATT&CK techniques apply to the average organization?" and "Which techniques does an organization realistically need to defend against?"

MITRE's Center for Threat-Informed Defense (the Center) began addressing these questions with the Sightings Ecosystem. The project focused on creating an anonymous, community-sourced repository of technique detections to identify when and where ATT&CK techniques occurred in the wild. The Center, in collaboration with AttackIQ Inc., Cyber Threat Alliance, Fortinet's FortiGuard Labs, HCA Healthcare, JP Morgan Chase, and Verizon Business Solutions, released a report in 2021 highlighting their key findings. Now, in collaboration with the same partners, the Center is updating the 2021 report to include current technique sightings and additional analysis. Since the last iteration of the Sightings Ecosystem, the Center has expanded the project's repository and updated its data model to include additional fields. This information details common adversary behaviors and techniques, targeted industries, and observed software and accompanying privilege levels. With this data, defenders can develop a threat-informed defense strategy focused on the top techniques observed in the wild and the threats to their organization based on location, industry sector, and deployed platforms.

Framing our Analysis

While our volume of data has increased significantly, there are caveats to keep in mind when reading our results. Primarily, we are limited to the data we were provided. While getting the data straight from vendors is beneficial, it introduces biases. To ameliorate this bias, we have a diverse set of providers and a large data set, which reduces some skewing within the data.

Additionally, the quality of the data is limited to what the vendors generate. We provided a data model for submitting data, but it is up to the vendors which fields to include. Some fields are required, such as technique and data source; others are optional, such as region or privilege level. While we cannot verify the authenticity or accuracy of the data, we trust our contributors to provide complete and accurate data. Mapping observed events to adversary techniques is an art form and therefore has some degree of subjectivity. Where an adversary is using PowerShell to run an executable with a valid account, one analyst may mark the event as PowerShell Scripting, while another might mark it as Valid Accounts; it depends on the context and the analyst's perspective. One mitigation for this bias is to mark the data with all relevant techniques (both PowerShell and Valid Accounts). However, due to our data model, we do not have any context about the event. We rely on the vendors to correctly assign techniques to the events.

Furthermore, not all events are validated by human analysts. Around 20% of the events we received were reviewed by human analysts; the rest were tagged as generated from raw events (likely, machine generated). This means that the labelling for those events is dependent on the tools and configurations used by the vendor. This can lead to a significant number of false positives, potentially skewing our data in unknown ways.

Of course, we are not omniscient. We cannot verify whether the data we received is representative of all global attacks. Our data is based on events that were found, not necessarily all attacks that occurred.

Therefore, the shifts in techniques that occur over time may more accurately reflect the community's ability to detect certain techniques, rather than those techniques being used more frequently. Despite these limitations, our data still gives us a unique insight into common techniques occurring in the wild.

Due to our time range (26 months) and variances in the ATT&CK version used by contributors, the Sightings we receive are sometimes notated in deprecated versions of ATT&CK. As the ATT&CK Framework evolves, techniques are added, removed, or merged. This causes issues when interpreting our data. For example, Timestomp was in our top 15 techniques. However, it has since been merged into Indicator Removal. This presents a challenge for us as we normalize the data and for the readers, who may be using different versions of ATT&CK. We have done our best to normalize all Techniques to the current version of ATT&CK (V14) for consistency.

What's in the Data

Overview

In the last paper, we had around 1.1M normalized sightings. This round we have around 1.6M sightings. Consequently, we have nearly twice as many unique techniques this round for analysis. This provides the Center with a more comprehensive view of what techniques are being used in the wild.

Figure 4. Top 100 Techniques.

Out of 201 core Enterprise techniques, we saw 173 techniques, or 86% of the ATT&CK Framework, in our data (see Appendix A). When including sub-techniques, we saw 353 out of 625 techniques and sub-techniques, or nearly 57%. This percentage is lower than the overall technique percentage because we tended to only see a small number of sub-techniques per single technique. However, each Tactic was well-represented in our data.

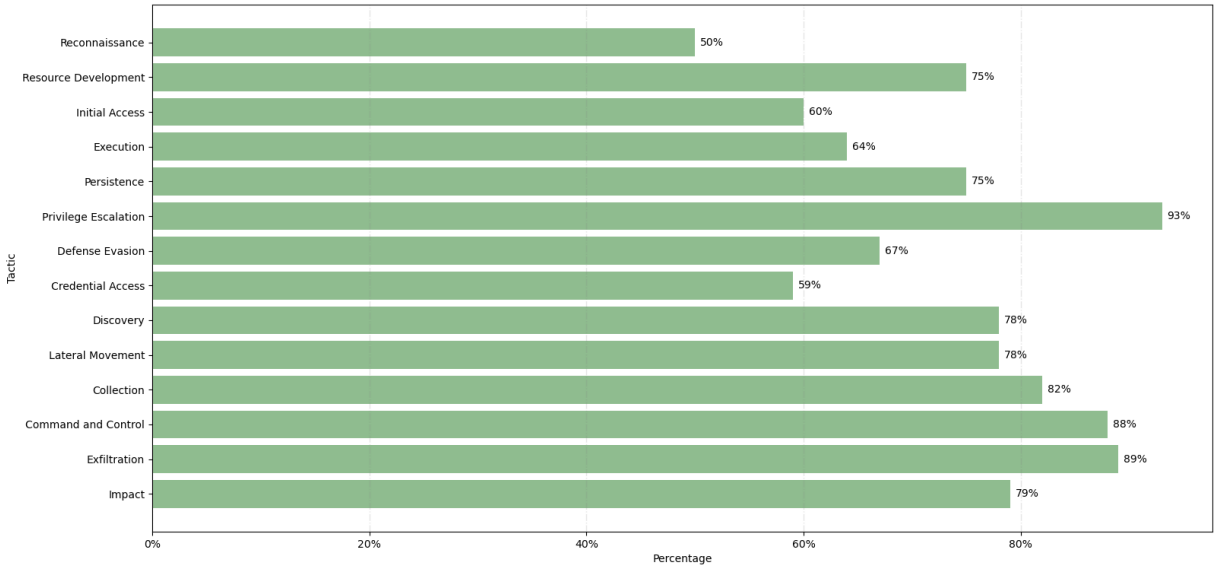


Figure 5. Percentage of Techniques seen per Tactic

Compared to our previous report, we observed some variations across the top 15 techniques. T1059 rose in rank from #2 to #1, and Scheduled Task (T1053), which was the #1 technique last time, didn't rank in the top 15. Additionally, Proxy (T1090), Masquerading (T1036), Create or Modify System Process (T1543), Hijack Execution Flow (T1574), Non-Application Layer Protocol (T1095), and Signed Binary/Proxy Execution (T1218) were also not seen in our top 15 techniques.

While the last Sightings report focused mainly on analyzing the top techniques, this time our data included some new information, allowing for additional analysis. We were able to observe the top techniques by sector, regions, software, platform, and privilege level. We also analyzed the correlation between sectors and regions and how software was used in sectors, platforms, and regions. Overall, over 300 different software was seen in our data. Additionally, 20 sectors and almost all countries were represented (198). To our surprise, outside of the US, nations in South America represented some of our highest sightings. Out of the sectors, most sightings came from the manufacturing sector - twice as much as the next closest sector. We anticipated a more uniform distribution across sectors or the highest sightings from a sector that cyber threat intelligence tends to report on, like the Professional, Scientific, and Technical Services or Information sectors. While we collected sightings from multiple platforms, the vast majority still came from Windows environments. Similarly, while we collected sightings from different privilege levels, most only used user permissions. For future reports, we hope to have more sightings from other platforms and privilege levels.

Top 15 Techniques

The following is a more in-depth review of the top 15 most observed techniques. If a technique has sub-techniques in the ATT&CK framework, then we divided it into its sub-techniques; however, we only focused on the sub-techniques seen in our data. This provides a more granular glimpse into each technique for defenders. The majority of the top 15 techniques abuse legitimate system tools. This underscores the idea that adversaries are attempting to appear as legitimate users.

We have incorporated prevention methods from the Center's mappings of ATT&CK to the NIST SP 800-53 and detection methods from the Cyber Analytics Repository and the Center's Sensor Mappings for ATT&CK, which connects conceptual data sources to sensors and other tools[2]. Due to the number of Windows events in our data, we chose to focus on sensor mappings for Sysmon and Windows event logs (WinEvtx)[3]. Overall, several prevention and detection controls focused on creating strong baselines, restricting permissions, and refining logs for process creation to detect and disrupt adversary behaviors.

1. Command and Scripting Interpreter [T1059]

Description

Command and Scripting Interpreter is a commonly used living-off-the-land technique. Most platforms have built-in command-line interfaces or scripting capabilities, allowing adversaries to use them for executing arbitrary commands, scripts, or binaries.

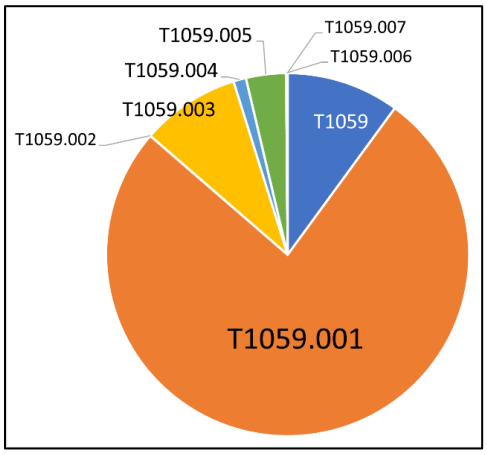


Figure 6. Breakdown of T1059.

Overall, T1059 is the most sighted technique in our data, in part because we normalized our data, which included T1064 and T1086 from previous ATT&CK versions, to T1059. The overwhelming majority of the sightings came from PowerShell (T1059.001). This is not surprising as it is a common tool used by adversaries for its ubiquity, versatility, and ability to obfuscate activity. The second most observed sub-technique the Windows Command Shell (T1059.003), which is similarly unsurprising for its ubiquity in Windows environments. The remaining sub-techniques make up less than 5% and include Visual Basic (T1059.005), Unix Shell (T1059.004), Python (T1059.006), JavaScript (T1059.007), and AppleScript (T1059.002). While these techniques are not difficult to monitor for, they are regularly used by benign programs, which could cause false positives for defenders to investigate.

T1059 was evenly distributed between user and SYSTEM level privileges. It followed the overall data trends, with the US as the top region, Windows as the top platform, Manufacturing as the top sector, and Heodo (another name for Emotet) as the top software.

Prevention

NIST lists 24 security controls to mitigate Command and Script Interpreter:

[2] The included prevention and detection methods are intended to be a starting point for defenders, not a comprehensive list.

[3] Additional mappings for Zeek, CloudTrail, OSQuery, and AuditD are available at the project's website.

- AC-2 Account Management (Also mitigates PowerShell, AppleScript, Visual Basic, Windows Command Shell, Unix Shell, Python, JavaScript)
- AC-3 Access Enforcement (Also mitigates PowerShell, AppleScript, Visual Basic, Windows Command Shell, Unix Shell, Python, JavaScript)
- AC-5 Separation of Duties (Also mitigates PowerShell)
- AC-6 Least Privilege (Also mitigates PowerShell, AppleScript, Visual Basic, Windows Command Shell, Unix Shell, Python, JavaScript)
- AC-17 Remote Access (Also mitigates PowerShell, AppleScript, Visual Basic, Windows Command Shell, Unix Shell, Python, JavaScript)
- CA-7 Continuous Monitoring (Also mitigates Visual Basic and JavaScript)
- CA-8 Penetration Testing
- CM-2 Baseline Configuration (Also mitigates PowerShell, AppleScript, Visual Basic, Windows Command Shell, Unix Shell, Python, JavaScript)
- CM-5 Access Restrictions for Change (Also mitigates PowerShell and Python)
- CM-6 Configuration Settings (Also mitigates PowerShell, AppleScript, Visual Basic, Windows Command Shell, Unix Shell, Python, JavaScript)
- CM-7 Least Functionality (Also mitigates Visual Basic and JavaScript)
- CM-8 System Component Inventory (Also mitigates PowerShell, Visual Basic, JavaScript)
- CM-11 User-Installed Software (Also mitigates Python)
- IA -2 Identification and Authentication (organizational Users) (Also mitigates PowerShell)
- IA-8 Identification and Authentication (non-organizational Users) (Also mitigates PowerShell)
- IA-9 Service Identification and Authentication (Also mitigates PowerShell and AppleScript)
- RA-5 Vulnerability Monitoring and Scanning (Also mitigates PowerShell, Visual Basic, and JavaScript)
- SC-18 Mobile Code (Also mitigates Visual Basic and JavaScript)
- SI-2 Flaw Remediation (Also mitigates PowerShell, Visual Basic, Python)
- SI-3 Malicious Code Protection (Also mitigates PowerShell, AppleScript, Visual Basic, Windows Command Shell, Unix Shell, Python, JavaScript)
- SI-4 System Monitoring (Also mitigates PowerShell, AppleScript, Visual Basic, Windows Command Shell, Unix Shell, Python, JavaScript)
- SI-7 Software, Firmware, and Information Integrity (Also mitigates PowerShell, AppleScript, Visual Basic, Windows Command Shell, Unix Shell, Python, JavaScript)
- SI-10 Information Input Validation (Also mitigates PowerShell, AppleScript, Visual Basic, Windows Command Shell, Unix Shell, Python, JavaScript)
- SI-16 Memory Protection (Also mitigates PowerShell, AppleScript, Visual Basic, Windows Command Shell, Unix Shell, Python, JavaScript)

NIST lists 1 security controls to mitigate Python (T1059.006):

- CM-3 Configuration Change Control

NIST lists 4 security controls to mitigate AppleScript (T1059.002):

- SR-4 Provenance
- SR-5 Acquisition Strategies, Tools, and Methods

- SR-6 Supplier Assessments and Reviews
- SR-11 Component Authenticity

Detections

CAR

Rules for the core technique:

- CAR-2021-01-002: Unusually Long Command Line Strings

Rules for PowerShell:

- CAR-2014-04-003: PowerShell Execution
- CAR-2014-11-004: Remote PowerShell Sessions

Rules for Windows Command Shell:

- CAR-2013-02-003: Processes Spawning cmd.exe
- CAR-2014-11-002: Outlier Parents of Cmd

Rules for Visual Basic:

- CAR-2013-04-002: Quick execution of a series of suspicious commands

Sensor Mappings for ATT&CK

Sysmon	1,7,30
WinEvtx	4103, 4104, 4688, 4696

2. Obfuscated Files or Information [T1027]

Description

Adversaries may encrypt, encode, or otherwise obfuscate payloads, files, scripts, or commands to avoid detection. Attackers can use T1027 to compress, archive, encrypt, or split payloads into multiple files; password protect or encode portions of files; or obfuscate commands in scripts. T1027 is often combined with Deobfuscate/Decode Files or Information (T1140), User Execution (T1204), Command and Scripting Interpreter (T1059), and others depending on how obfuscation was used during the attack.

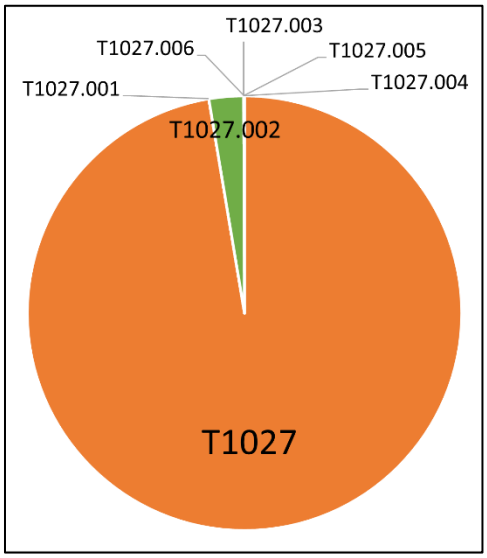


Figure 7. Breakdown of T1027.

A majority of T1027 sightings did not include sub-techniques. This is likely due in part to normalizing our data, which included T1045 and T1066 from previous ATT&CK versions, to T1027. The most observed sub-technique was Software Packing (T1027.002). Adversaries use this sub-technique to evade detection of their code, particularly from signature-based detections. We also saw a small amount of HTML

Smuggling (T1027.006), Binary Padding (T1027.001), Steganography (T1027.003), Compile After Delivery (T1027.004), and Indicator Removal from Tools (T1027.005).

T1027 was evenly distributed between different software. It followed the overall data trends, with the US as the top region, Windows as the top platform, and Manufacturing as the top sector. Notably, it deviated from the overall privilege level trend, with more SYSTEM level permissions seen.

Prevention

NIST lists 6 security controls to mitigate Obfuscated Files or Information:

- CM-2 Baseline Configuration
- CM-6 Configuration Settings
- SI-2 Flaw Remediation (Also mitigates Software Packing)
- SI-3 Malicious Code Protection (Also mitigates Software Packing)
- SI-4 System Monitoring (Also mitigates Software Packing)
- SI-7 Software, Firmware, and Information Integrity (Also mitigates Software Packing)

Detections

CAR

None

Sensor Mappings for ATT&CK

Sysmon	1, 11, 12, 15, 19, 20, 7
WinEvtx	4103, 4104, 4657, 4663, 4664, 4688, 4696, 5857, 5858, 5859, 5860, 5861

3. Ingress Tool Transfer [T1105]

Description

Adversaries may transfer tools or other files from a command-and-control system into a compromised environment. They can conduct living-of-the-land attacks using native utilities or installers and package managers in Windows, Linux, and MacOS systems to download files. Adversaries can also download files through Cloud-based services, such as Dropbox or OneDrive, that sync with the targeted systems.

Nearly all instances of this technique came from the US on Windows-based systems, with SYSTEM or user-level privileges, in the Manufacturing or Administrative and Support and Waste… Services sectors. T1105 was distributed evenly across different software. Given this technique's high occurrence, it is notable that it was not reported at higher rates in other sectors or with administrative level privileges.

Prevention

NIST lists 8 security controls to mitigate Ingress Tool Transfer:

- AC-4 Information Flow Enforcement
- CA-7 Continuous Monitoring
- CM-2 Baseline Configuration
- CM-6 Configuration Settings
- CM-7 Least Functionality

- SC-7 Boundary Protection
- SI-3 Malicious Code Protection
- SI-4 System Monitoring

Detections

CAR

Rules for the core technique:

- CAR-2013-07-001: Suspicious Arguments
- CAR-2021-05-005: BITSAdmin Download File
- CAR-2021-05-006: CertUtil Download With URLCache and Split Arguments
- CAR-2021-05-007: CertUtil Download With VerifyCtl and Split Arguments

Sensor Mappings for ATT&CK

Sysmon	11, 15, 3
WinEvtx	4663, 5031, 5154, 5155, 5156, 5157, 5158, 5159

4. Modify Registry [T1112]

Description

Adversaries may use built-in command line tools or the Win32 API to interact with the Windows Registry to hide configuration information, remove information, or as part of other techniques for Execution and Persistence. Specific areas of the registry depend on account permissions to access, potentially requiring adversaries to gain administrator-level privileges to modify. The Windows registry is a significant component of Windows, making it an attractive tool for adversaries to use.

T1112 sightings occur on Windows-based platforms and were evenly distributed across different countries, sectors, and software. We lacked a meaningful amount of data for privilege level analysis. Overall, we received significantly more sightings of T1112 in 2023 than in 2022; this could be due to attackers using this technique more frequently during their operations. However, the registry has been a common attack vector for years, so this sudden increase in Sightings is likely due to statistical noise.

Prevention

NIST lists 2 security controls to mitigate Modify Registry:

- AC-6 Least Privilege
- CM-7 Least Functionality

Detections

CAR

Rules for core technique:

- CAR-2013-01-002: Autorun Differences
- CAR-2013-03-001: Reg.exe called from Command Shell
- CAR-2013-04-002: Quick execution of a series of suspicious commands
- CAR-2014-11-005: Remote Registry

- CAR-2020-05-003: Rare LolBAS Command Lines
- CAR-2021-11-001: Registry Edit with Creation of SafeDllSearchMode Key Set to 0
- CAR-2021-11-002: Registry Edit with Modification of Userinit, Shell, or Notify
- CAR-2021-12-002: Modification of Default Startup Folder in the Registry Key 'Common Startup'

Sensor Mappings for ATT&CK

Sysmon	1, 12, 13, 14
WinEvtx	4103, 4657, 4660, 4670, 4688, 4696

5. Indicator Removal [T1070]

Description

Various platform-specific artifacts may be created by an adversary or expose an adversary's actions. Adversaries may delete or modify these artifacts to remove any evidence of their presence or hinder defenses. Because these artifacts are used during forensic and incident response efforts, their removal could impede an investigation or lengthen the intrusion detection process.

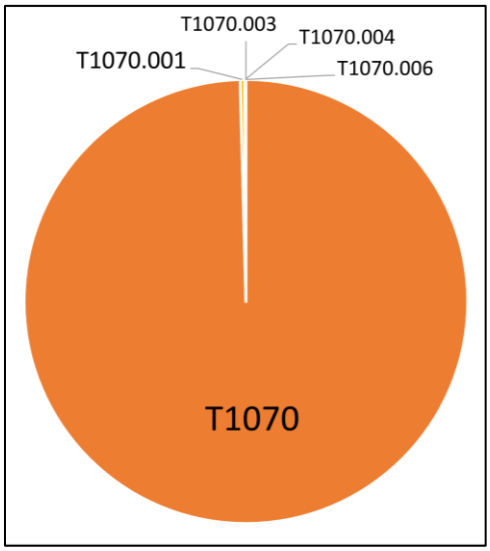


Figure 8. Breakdown of T1070.

A majority of T1070 sightings did not include sub-techniques. This is likely due in part to normalizing our data, which included T1099 and T1107 from previous ATT&CK versions, to T1070. Less than 1% of sightings were Clear Windows Event Logs (T1070.001), File Deletion (T1070.004), Clear Command History (T1070.003), and Timestomp (T1070.006).

T1070 occurred mostly on Windows-based platforms and was distributed evenly across different countries and sectors. Only a small sub-set of sightings contained privilege levels and software information. However, it followed the overall data trend, with user-level permissions and Heodo being the most observed privilege levels and software, respectively.

Prevention

NIST lists 21 security controls to mitigate Indicator Removal:

- AC-2 Account Management (Also mitigates Clear Windows Event Logs and Clear Command History)
- AC-3 Access Enforcement (Also mitigates Clear Windows Event Logs and Clear Command History)
- AC-5 Separation of Duties (Also mitigates Clear Windows Event Logs and Clear Command History)
- AC-6 Least Privilege (Also mitigates Clear Windows Event Logs and Clear Command History)
- AC-16 Security and Privacy Attributes (Also mitigates Clear Windows Event Logs)
- AC-17 Remote Access (Also mitigates Clear Windows Event Logs)
- AC-18 Wireless Access (Also mitigates Clear Windows Event Logs)
- AC-19 Access Control for Mobile Devices (Also mitigates Clear Windows Event Logs)

- CA-7 Continuous Monitoring (Also mitigates Clear Windows Event Logs and Clear Command History)
- CM-2 Baseline Configuration (Also mitigates Clear Windows Event Logs and Clear Command History)
- CM-6 Configuration Settings (Also mitigates Clear Windows Event Logs and Clear Command History)
- CP-6 Alternate Storage Site (Also mitigates Clear Windows Event Logs)
- CP-7 Alternate Processing Site (Also mitigates Clear Windows Event Logs)
- CP-9 System Backup (Also mitigates Clear Windows Event Logs)
- SC-4 Information in Shared System Resources (Also mitigates Clear Windows Event Logs)
- SC-36 Distributed Processing and Storage (Also mitigates Clear Windows Event Logs)
- SI-3 Malicious Code Protection (Also mitigates Clear Windows Event Logs and Clear Command History)
- SI-4 System Monitoring (Also mitigates Clear Windows Event Logs and Clear Command History)
- SI-7 Software, Firmware, and Information Integrity (Also mitigates Clear Windows Event Logs and Clear Command History)
- SI-12 Information Management and Retention (Also mitigates Clear Windows Event Logs)
- SI-23 Information Fragmentation (Also mitigates Clear Windows Event Logs)

Detections

CAR

Rules for Clear Windows Event Logs:

- CAR-2016-04-002: User Activity from Clearing Event Logs
- CAR-2021-01-003: Clearing Windows Logs with Wevtutil

Rules for Clear Command History:

- CAR-2020-11-005: Clear Powershell Console Command History

Sensor Mappings for ATT&CK

Sysmon	1, 12, 13, 14, 2, 23, 26
WinEvtx	2004, 2005, 2006, 2033, 4103, 4625, 4648, 4657, 4660, 4663, 4664, 4670, 4688, 4696, 4700, 4701, 4702, 4726, 4743, 4776, 4946, 4947, 4948

6. User Execution [T1204]

Description

An adversary may rely upon user actions to gain Initial Access or execute malicious software on a system. Common examples of user execution include phishing and social engineering attacks. Adversaries may send a malicious link, file, or image for a user to open or deceive users into enabling Remote Access Software to give them direct control of the system.

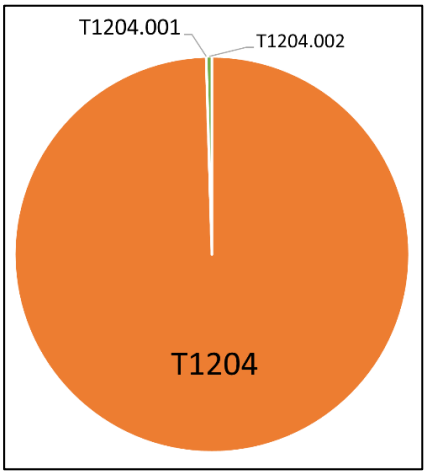


Figure 9. Breakdown of T1204.

A majority of T1204 sightings did not contain a sub-technique. Less than 1% contained Malicious Link (T1204.001) and Malicious File (T1204.002). Most sightings occurred on Windows-based systems and were almost evenly distributed across countries and sectors. Only a small sub-set included privilege level information and software, with user level privileges and Cobalt Strike seen the most frequently.

Prevention

NIST lists 13 security controls to mitigate User Execution:

- AC-4 Information Flow Enforcement (Also mitigates Malicious Link and Malicious File)
- CA-7 Continuous Monitoring (Also mitigates Malicious Link and Malicious File)
- CM-2 Baseline Configuration (Also mitigates Malicious Link and Malicious File)
- CM-6 Configuration Settings (Also mitigates Malicious Link and Malicious File)
- CM-7 Least Functionality (Also mitigates Malicious File)
- SC-7 Boundary Protection (Also mitigates Malicious Link and Malicious File)
- SC-44 Detonation Chambers (Also mitigates Malicious Link and Malicious File)
- SI-2 Flaw Remediation (Also mitigates Malicious Link)
- SI-3 Malicious Code Protection (Also mitigates Malicious Link and Malicious File)
- SI-4 System Monitoring (Also mitigates Malicious Link and Malicious File)
- SI-7 Software, Firmware, and Information Integrity (Also mitigates Malicious File)
- SI-8 Spam Protection (Also mitigates Malicious Link and Malicious File)
- SI-10 Information Input Validation (Also mitigates Malicious File)

Detections

CAR

Rules for Malicious File:

- CAR-2021-05-002: Batch File Write to System32

Sensor Mappings for ATT&CK

Sysmon	1, 11, 15, 3
WinEvtx	4103, 4663, 4688, 4696, 5031, 5154, 5155, 5156, 5157, 5158, 5159

7. Hide Artifacts [T1564]

Description

Adversaries may attempt to hide artifacts, such as files, user accounts, or directories, to evade detection. They may exploit operating system features to hide the artifacts or use virtualization to create isolated computing regions to avoid common security tools and configurations.

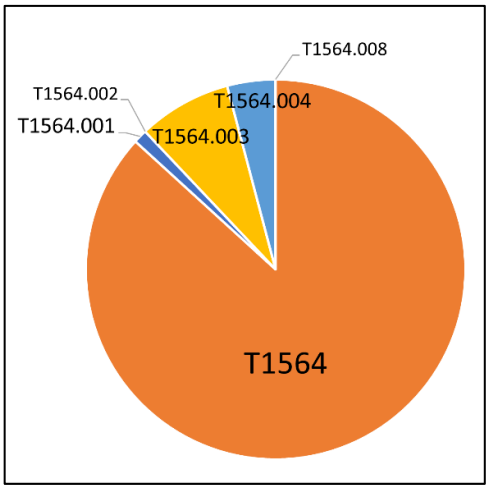


Figure 10. Breakdown of T1564.

A majority of T1564 sightings did not include sub-techniques. This is likely due in part to normalizing our data, which included T1143 and T1158 from previous ATT&CK versions, to T1564. The most observed sub-technique was Hidden Window (T1564.003). Adversaries can use this technique to hide activities from plain sight. The second most-observed sub-technique was NFTS File Attributes (T1564.004). Adversaries can exploit the file attribute metadata to hide malicious data. Less than 2% of sightings included Hidden Files and Directories (T1564.001), Email Hiding Rules (T1564.008), and Hidden Users (T1564.002).

T1564 occurred mostly on Windows-based systems and was about evenly distributed across countries and sectors. Only a small sub-set of sightings contained privilege levels and software information. However, it followed the overall data trend, with user-level permissions and Heodo being the most observed privilege levels and software, respectively.

Prevention

NIST lists 3 security controls to mitigate Hidden Window (T1564.003):

- CM-7 Least Functionality (Also mitigates Email Hiding Rules and Hidden Users)
- SI-7 Software, Firmware, and Information Integrity (Also mitigates NTFS File Attributes and Email Hiding Rules)
- SI-10 Information Input Validation

NIST lists 5 security controls to mitigate NFTS File Attributes (T1564.004):

- AC-3 Access Enforcement
- AC-16 Security and Privacy Attributes
- CA-7 Continuous Monitoring
- SI-3 Malicious Code Protection (also mitigates Email Hiding Rules)
- SI-4 System Monitoring (Also mitigates Email Hiding Rules and Hidden Users)

NIST lists 4 security controls to mitigate Email Hiding Rules (T1564.008):

- AC-4 Information Flow Enforcement
- CM-3 Configuration Change Control
- CM-5 Access Restrictions for Change
- IR-5 Incident Monitoring

NIST lists 1 security controls to mitigate Hidden Users (T1564.002):

- CM-6 Configuration Settings

Detections

CAR

Rules for NTFS File Attributes:

- CAR-2020-08-001: NTFS Alternate Data Stream Execution – System Utilities
- CAR-2020-08-002: NTFS Alternate Data Stream Execution - LOLBAS

Sensor Mappings for ATT&CK

Sysmon	1, 11, 13, 14, 15, 2
WinEvtx	4103, 4104, 4657, 4663, 4664, 4670, 4674, 4688, 4696, 4697, 4720, 4741

8. Process Injection [T1055]

Description

Adversaries may inject code into live processes to access the process's memory or elevate privileges. There are several ways to inject code into other processes, many of which are platform specific. By performing process injection, adversaries are able to hide inside legitimate processes to evade process-based defenses.

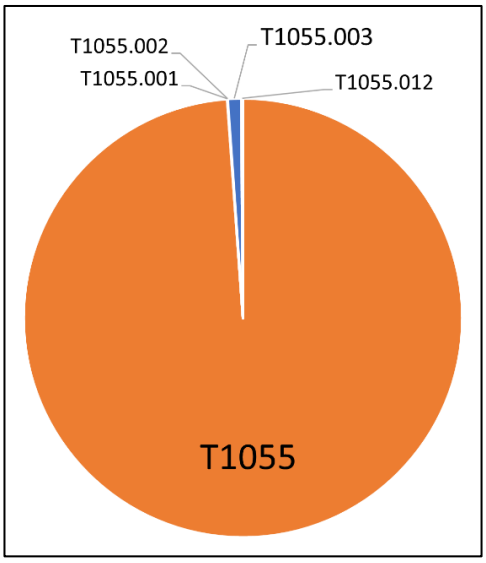


Figure 11. Breakdown of T1055.

A majority of T1055 sightings did not include sub-techniques. This is likely due in part to normalizing our data, which included T1093 from previous ATT&CK versions, to T1055. Less than 2% of sightings included Dynamic-link Library Injection (T1055.001), Portable Executable Injection (T1055.002), Thread Execution Hijacking (T1055.003), and Process Hollowing (T1055.012).

This technique occurred consistently throughout 2022 and 2023. T1055 occurred mostly on Windows-based systems and was about evenly distributed across countries. It followed the overall data trend, with user-level permissions and Heodo being the most observed privilege levels and software, respectively. Notably, it deviated from the overall trend by occurring more frequently in the Professional, Scientific, and Technical Services sector.

Prevention

NIST lists 12 security controls to mitigate Process Injection:

- AC-2 Account Management
- AC-3 Access Enforcement
- AC-5 Separation of Duties
- AC-6 Least Privilege (Also mitigates Portable Executable Injection, Thread Execution Hijacking, Process Hollowing, and Dynamic-link Library Injection)

- CM-5 Access Restrictions for Change
- CM-6 Configuration Settings
- IA-2 Identification and Authentication (organizational Users)
- SC-7 Boundary Protection (Also mitigates Portable Executable Injection, Thread Execution Hijacking, Process Hollowing, and Dynamic-link Library Injection)
- SC-18 Mobile Code (Also mitigates Portable Executable Injection, Thread Execution Hijacking, Process Hollowing, and Dynamic-link Library Injection)
- SI-2 Flaw Remediation (Also mitigates Portable Executable Injection, Thread Execution Hijacking, Process Hollowing, and Dynamic-link Library Injection)
- SI-3 Malicious Code Protection (Also mitigates Portable Executable Injection, Thread Execution Hijacking, Process Hollowing, and Dynamic-link Library Injection)
- SI-4 System Monitoring (Also mitigates Portable Executable Injection, Thread Execution Hijacking, Process Hollowing, and Dynamic-link Library Injection)

Detections

CAR

Rules for Dynamic-link Library Injection:

- CAR-2013-10-002: DLL Injection via Load Library
- CAR-2020-11-003: DLL Injection with Mavinject

Rules for Process Hollowing:

- CAR-2020-11-004: Processes Started From Irregular Parent

Detections for ATT&CK Mapping

Sysmon	10, 2, 30, 7, 8
WinEvtx	4656, 4663, 4664, 4670

9. OS Credential Dumping [T1003]

Description

Adversaries can use dumped credentials to obtain account login and credential material to access restricted information or perform Lateral Movement.

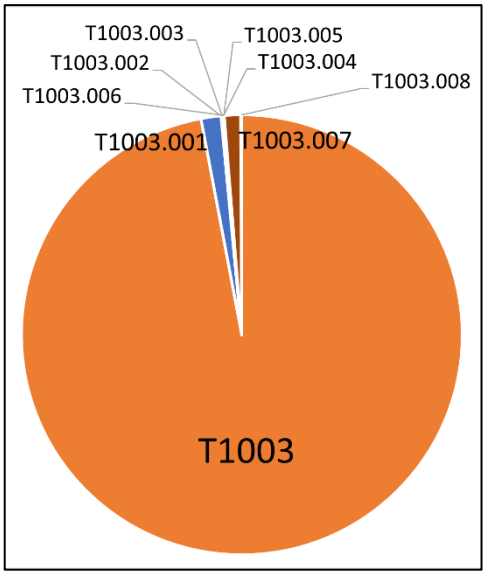


Figure 12. Breakdown of T1003.

A majority of T1003 sightings did not contain sub-techniques. However, less than 3% of the sightings contained LSASS Memory (T1003.001), Proc Filesystem (T1003.007), NTDS (T1003.003), /etc/passwd and /etc/shadow (T1003.008), DCSync (T1003.006), Cached Domain Credentials (T1003.005), Proc Filesystem (T1003.007), LSA Secrets (T1003.004), and Security Account Manager (T1003.002).

Most T1003 sightings were received during 2022 and dropped off in 2023. This could be due to random statistical noise in the data, or attackers using this technique less in the wild. Most sightings occurred on Windows-based systems and used user level privileges. Only a small sub-set contained location and sector information, with most sightings occurring in the US. Notably, T1003 deviated from overall trends on the data, with AgentTesla as the most frequently seen software and Information as the most frequently seen sector.

Prevention

NIST lists 22 security controls to mitigate OS Credential Dumping:

- AC-2 Account Management (Also mitigates LSA Secrets, Cached Domain Credentials, DCSync, Proc Filesystem, /etc/passwd and /etc/shadow, LSASS Memory, Security Account Manager, and NTDS)
- AC-3 Access Enforcement (Also mitigates LSA Secrets, Cached Domain Credentials, DCSync, Proc Filesystem, /etc/passwd and /etc/shadow, LSASS Memory, Security Account Manager, and NTDS)
- AC-4 Information Flow Enforcement (Also mitigates Cached Domain Credentials, DCSync, and LSASS Memory)
- AC-5 Separation of Duties (Also mitigates LSA Secrets, Cached Domain Credentials, DCSync, Proc Filesystem, /etc/passwd and /etc/shadow, LSASS Memory, Security Account Manager, and NTDS)
- AC-6 Least Privilege (Also mitigates LSA Secrets, Cached Domain Credentials, DCSync, Proc Filesystem, /etc/passwd and /etc/shadow, LSASS Memory, Security Account Manager, and NTDS)
- AC-16 Security and Privacy Attributes (Also mitigates NTDS)
- CA-7 Continuous Monitoring (Also mitigates LSA Secrets, Cached Domain Credentials, DCSync, Proc Filesystem, /etc/passwd and /etc/shadow, LSASS Memory, Security Account Manager, and NTDS)
- CM-2 Baseline Configuration (Also mitigates LSA Secrets, Cached Domain Credentials, DCSync, Proc Filesystem, /etc/passwd and /etc/shadow, LSASS Memory, Security Account Manager, and NTDS)

- CM-5 Access Restrictions for Change (Also mitigates LSA Secrets, Cached Domain Credentials, DCSync, Proc Filesystem, /etc/passwd and /etc/shadow, LSASS Memory, Security Account Manager, and NTDS)
- CM-6 Configuration Settings (Also mitigates LSA Secrets, Cached Domain Credentials, DCSync, Proc Filesystem, /etc/passwd and /etc/shadow, LSASS Memory, Security Account Manager, and NTDS)
- CM-7 Least Functionality (Also mitigates Cached Domain Credentials, LSASS Memory, and Security Account Manager)
- CP-9 System Backup (Also mitigates NTDS)
- IA-2 Identification and Authentication (organizational Users) (Also mitigates LSA Secrets, Cached Domain Credentials, DCSync, Proc Filesystem, /etc/passwd and /etc/shadow, LSASS Memory, Security Account Manager, and NTDS)
- IA-4 Identifier Management (Also mitigates Cached Domain Credentials and DCSync)
- IA-5 Authenticator Management (Also mitigates LSA Secrets, Cached Domain Credentials, DCSync, Proc Filesystem, /etc/passwd and /etc/shadow, LSASS Memory, Security Account Manager, and NTDS)
- SC-28 Protection of Information at Rest (Also mitigates LSA Secrets, Cached Domain Credentials, DCSync, Proc Filesystem, /etc/passwd and /etc/shadow, LSASS Memory, Security Account Manager, and NTDS)
- SC-39 Process Isolation (Also mitigates LSA Secrets, Cached Domain Credentials, DCSync, Proc Filesystem, /etc/passwd and /etc/shadow, LSASS Memory, Security Account Manager, and NTDS)
- SI-2 Flaw Remediation (Also mitigates LSASS Memory)
- SI-3 Malicious Code Protection (Also mitigates LSA Secrets, Cached Domain Credentials, DCSync, Proc Filesystem, /etc/passwd and /etc/shadow, LSASS Memory, Security Account Manager, and NTDS)
- SI-4 System Monitoring (Also mitigates LSA Secrets, Cached Domain Credentials, DCSync, Proc Filesystem, /etc/passwd and /etc/shadow, LSASS Memory, Security Account Manager, and NTDS)
- SI-7 Software, Firmware, and Information Integrity (Also mitigates NTDS)
- SI-12 Information Management and Retention (Also mitigates NTDS)

NIST lists 2 security controls to mitigate LSASS Memory (T1003.001):

- SC-3 Security Function Isolation
- SI-16 Memory Protection

Detections

CAR

Rules for LSASS Memory:

- CAR-2013-07-001: Suspicious Arguments
- CAR-2019-04-004: Credential Dumping via Mimikatz
- CAR-2019-07-002: Lsass Process Dump via Procdump
- CAR-2019-08-001: Credential Dumping via Windows Task Manager
- CAR-2021-05-011: Create Remote Thread into LSASS

Rules for NTDS:

- CAR-2019-08-002: Active Directory Dumping via NTDSUtil
- CAR-2020-05-001: MiniDump of LSASS

Rules for Security Account Manager:

- CAR-2013-04-002: Quick execution of a series of suspicious commands

Sensor Mappings for ATT&CK

Sysmon	1, 10, 9
WinEvtx	4103, 4656, 4661, 4662, 4663, 4688, 4690, 4696, 4773, 4932

10. Remote Services [T1021]

Description

Adversaries may use Remote Services, coupled with Valid Accounts (T1078), to exploit services that accept remote connections, such as RDP, telnet, SSH, or VNC. Some platforms also have native remote management utilities, such as the Apple Remote Desktop on MacOS, that adversaries can also use for remote code execution. If the servers and workstations are joined to a domain, adversaries could use a single set of login credentials to move laterally and access additional systems.

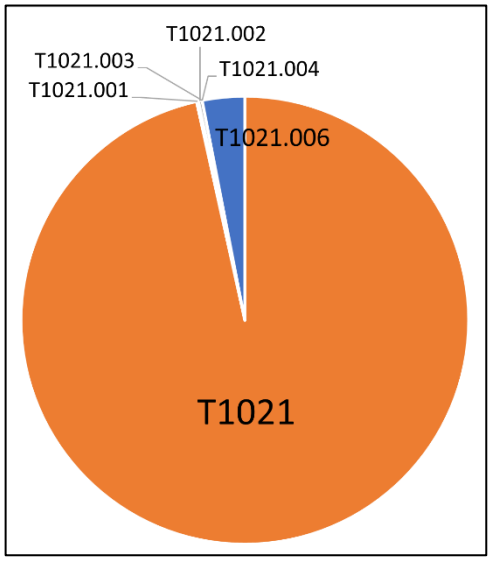


Figure 13. Breakdown of T1021.

A majority of T1021 sightings did not include sub-techniques. This is likely due in part to normalizing our data, which included T1175 from previous ATT&CK versions, to T1021. The most observed sub-technique was Windows Remote Management (T1021.006). Less than 3% of sightings were from Remote Desktop Protocol (T1021.001), SMB/Windows Admin Shares (T1021.002), Distributed Component Object Model (T1021.003), and SSH (T1021.004).

Most T1021 sightings occurred on Windows-based systems and used user level permissions; however, we had a couple thousand Nix sightings, which is unusual but unsurprising since many intrusions use remote services. Only a small sub-set of sightings contained location and sector information, with most occurring in the US and in the Professional, Scientific, and Technical Services sector. Notably, T1021 deviated from overall trends on the data, with SnakeKeylogger as the most frequently seen software.

Prevention

NIST lists 12 security controls to mitigate Remote Services:

- AC-2 Account Management (Also mitigates Remote Desktop Protocol, SMB/Windows Admin Shares, Distributed Component Object Model, SSH, and Windows Remote Management)
- AC-3 Access Enforcement (Also mitigates Remote Desktop Protocol, SMB/Windows Admin Shares, Distributed Component Object Model, SSH, and Windows Remote Management)

- AC-5 Separation of Duties (Also mitigates Remote Desktop Protocol, SMB/Windows Admin Shares, Distributed Component Object Model, SSH, and Windows Remote Management)
- AC-6 Least Privilege (Also mitigates Remote Desktop Protocol, SMB/Windows Admin Shares, Distributed Component Object Model, SSH, and Windows Remote Management)
- AC-7 Unsuccessful Logon Attempts (Also mitigates Remote Desktop Protocol and SSH)
- AC-17 Remote Access (Also mitigates Remote Desktop Protocol, SMB/Windows Admin Shares, Distributed Component Object Model, SSH, and Windows Remote Management)
- AC-20 Use of External Systems (Also mitigates Remote Desktop Protocol and SSH)
- CM-5 Access Restrictions for Change (Also mitigates Remote Desktop Protocol, SMB/Windows Admin Shares, Distributed Component Object Model, SSH, and Windows Remote Management)
- CM-6 Configuration Settings (Also mitigates Remote Desktop Protocol, SMB/Windows Admin Shares, Distributed Component Object Model, SSH, and Windows Remote Management)
- IA-2 Identification and Authentication (organizational Users) (Also mitigates Remote Desktop Protocol, SMB/Windows Admin Shares, Distributed Component Object Model, SSH, and Windows Remote Management)
- IA-5 Authenticator Management (Also mitigates Remote Desktop Protocol and SSH)
- SI-4 System Monitoring (Also mitigates Remote Desktop Protocol, SMB/Windows Admin Shares, Distributed Component Object Model, SSH, and Windows Remote Management)

NIST lists 12 security controls to mitigate Remote Desktop Protocol (T1021.001):

- AC-4 Information Flow Enforcement (Also mitigates SMB/Windows Admin Shares, Distributed Component Object Model, and Windows Remote Management)
- AC-11 Device Lock
- AC-12 Session Termination
- CA-8 Penetration Testing
- CM-2 Baseline Configuration (Also mitigates SMB/Windows Admin Shares, Distributed Component Object Model, and Windows Remote Management)
- CM-7 Least Functionality (Also mitigates SMB/Windows Admin Shares, Distributed Component Object Model, and Windows Remote Management)
- CM-8 System Component Inventory (Also mitigates Distributed Component Object Model, SSH, and Windows Remote Management)
- IA-4 Identifier Management
- IA-6 Authentication Feedback
- RA-5 Vulnerability Monitoring and Scanning (Also mitigates Distributed Component Object Model, SSH, and Windows Remote Management)
- SC-7 Boundary Protection (Also mitigates SMB/Windows Admin Shares, Distributed Component Object Model, and Windows Remote Management)
- SC-46 Cross Domain Policy Enforcement (Also mitigates Distributed Component Object Model and Windows Remote Management)

NIST lists 3 security controls to mitigate SMB/Windows Admin Shares (T1021.002):

- CA-7 Continuous Monitoring
- SI-10 Information Input Validation

- SI-15 Information Output Filtering

NIST lists 3 security controls to mitigate Distributed Component Object Model (T1021.003):

- SC-3 Security Function Isolation
- SC-18 Mobile Code
- SI-3 Malicious Code Protection

Detections

CAR

Rules for core technique:

- CAR-2013-07-001: Suspicious Arguments

Rules for Remote Desktop Protocol:

- CAR-2013-07-002: RDP Connection Detection
- CAR-2013-10-001: User Login Activity Monitoring
- CAR-2016-04-005: Remote Desktop Logon

Rules for SMB/Windows Admin Shares:

- CAR-2013-01-003: SMB Events Monitoring
- CAR-2013-04-002: Quick execution of a series of suspicious commands
- CAR-2013-05-003: SMB Write Request
- CAR-2013-05-005: SMB Copy and Execution
- CAR-2014-05-001: RPC Activity

Rules for Distributed Component Object Model:

- CAR-2014-05-001: RPC Activity

Rules for Windows Remote Management:

- CAR-2014-05-001: RPC Activity
- CAR-2014-11-004: Remote PowerShell Sessions
- CAR-2014-11-006: Windows Remote Management (WinRM)

Sensor Mappings for ATT&CK

Sysmon	1, 3, 7
WinEvtx	4103, 4624, 4688, 4696, 4778, 4964, 5031, 5140, 5145, 5154, 5155, 5156, 5157, 5158, 5159

11. Data Encrypted for Impact [T1486]

Description

Adversaries may encrypt data on target systems to interrupt availability to system and network resources. In some cases, File and Directory Permissions Modification (T1222) or System Shutdown/Reboot (T1529) are necessary to access targeted file types. To maximize impact, malware

with wormlike properties may be used in conjunction with Valid Accounts (T1078), OS Credential Dumping (T1003), or SMB/Windows Admin Shares (T1021.002). These attacks may be used by adversaries for monetary gain or data destruction.

Most T1486 events occurred in 2022, on Windows-based platforms, with user level permissions. Notably, T1486 deviated from overall trends on the data, with AgentTesla as the most frequently seen software. We lacked a meaningful amount of data for location or sector analysis.

Prevention

NIST lists 11 security controls to mitigate Data Encrypted for Impact:

- AC-3 Access Enforcement
- AC-6 Least Privilege
- CM-2 Baseline Configuration
- CP-2 Contingency Plan
- CP-6 Alternate Storage Site
- CP-7 Alternate Processing Site
- CP-9 System Backup
- CP-10 System Recovery and Reconstitution
- SI-3 Malicious Code Protection
- SI-4 System Monitoring
- SI-7 Software, Firmware, and Information Integrity

Detections

CAR

None

Detections for ATT&CK Mapping

Sysmon	1, 11, 15, 2
WinEvtx	4103, 4663, 4670, 4688, 4696, 5140, 5145

12. Replication Through Removable Media [T1091]

Description

Adversaries may gain initial access to systems by modifying systems that format removable media, modifying the media's firmware, or copying malware to removable media and exploiting Autorun features on a system. Lateral movement can occur when stored executable files are modified or renamed to appear legitimate. Mobile devices can also be targeted to infect and spread malware when connected to a system.

We observed a significant increase of T1091 sightings in February 2023, which has remained. Nearly all sightings occurred on Windows-based platforms. T1091 was most frequently seen in India and in the Professional, Scientific, and Technical Services sector, but was otherwise almost evenly distributed across other regions and sectors. Only a small sub-set of sightings contained privilege level and software information. While T1091 aligned with the overall data trend of mostly user level permissions, it deviated from software trends, with njrat as the most frequently seen software.

Prevention

NIST lists 10 security controls to mitigate Replication Through Removable Media:

- AC-3 Access Enforcement
- AC-6 Least Privilege
- CM-2 Baseline Configuration
- CM-6 Configuration Settings
- CM-8 System Component Inventory
- MP-7 Media Use
- RA-5 Vulnerability Monitoring and Scanning
- SC-41 Port and I/O Device Access
- SI-3 Malicious Code Protection
- SI-4 System Monitoring

Detections

CAR

None

Sensor Mappings for ATT&CK

Sysmon	1, 11, 15, 9
WinEvtx	4656, 4661, 4663, 4688, 4690, 4696, 6416, 6423, 6424

13. System Information Discovery [T1082]

Description

An adversary may use information about the operating system and hardware to shape code development and follow-on behaviors. These attacks can use native tools, such as systeminfo on Windows, the systemsetup configuration tool on MacOS, or the command-line interface of a network device, to gather detailed system information. Adversaries can use this information, coupled with other forms of Discovery or Reconnaissance, to avoid detections and conduct more targeted attacks.

Sightings for T1082 occurred mostly on Windows-based platforms; however, we had a couple thousand Nix sightings, which is unusual but unsurprising since many networks contain at least some Nix systems which would be identified during discovery efforts. T1082 followed the overall data trend, with user-level permissions and Heodo being the most observed privilege levels and software, respectively. We lacked a meaningful amount of data for location or sector analysis.

Prevention

NIST lists no security controls to mitigate System Information Discovery.

Detections

CAR

Rules for the core technique:

- CAR-2013-04-002: Quick execution of a series of suspicious commands

- CAR-2016-03-001: Host Discovery Commands

Sensor Mappings for ATT&CK

Sysmon	1
WinEvtx	4656, 4661, 4663, 4688, 4690, 4696, 6416, 6423, 6424

14. Windows Management Instrumentation [T1047]

Description

Windows Management Instrumentation (WMI) is a native Windows administration feature used to access Windows system components. Adversaries may abuse WMI to interact with local systems to execute malicious commands and payloads. To interact with remote systems, adversaries can use WMI in conjunction with Remote Services, such as Distributed Component Object Model (DCOM) and Windows Remote Management (WinRM).

Most sightings for T1047 occurred in 2022, on Windows-based platforms, with user level permissions. We saw a significant reduction in sightings in 2023, likely the result of some change in the data provided to us. Only a small sub-set of sightings contained location and sector information. However, it followed the overall data trend, with the US and Manufacturing being the most observed location and sector, respectively. Notably, T1047 deviated from overall software trends, with RedLineStealer as the most frequently seen software.

Prevention

NIST lists 18 security controls to mitigate Windows Management Instrumentation:

- AC-2 Account Management
- AC-3 Access Enforcement
- AC-5 Separation of Duties
- AC-6 Least Privilege
- AC-17 Remote Access
- CM-2 Baseline Configuration
- CM-5 Access Restrictions for Change
- CM-6 Configuration Settings
- CM-7 Least Functionality
- IA-2 Identification and Authentication (organizational Users)
- RA-5 Vulnerability Monitoring and Scanning
- SC-3 Security Function Isolation
- SC-34 Non-modifiable Executable Programs
- SI-2 Flaw Remediation
- SI-3 Malicious Code Protection
- SI-4 System Monitoring
- SI-7 Software, Firmware, and Information Integrity
- SI-16 Memory Protection

Detections

CAR

Rules for the core technique:

- CAR-2014-11-007: Remote Windows Management Instrumentation (WMI) over RPC
- CAR-2014-12-001: Remotely Launched Executables via WMI
- CAR-2016-03-002: Create Remote Process via WMIC

Sensor Mappings for ATT&CK

Sysmon	1, 3
WinEvtx	4103, 4688, 4696, 5031, 5154, 5155, 5156, 5157, 5158, 5159

15. Impair Defenses [T1562]

Description

Adversaries may maliciously modify components of a victim's environment to hinder or disable preventative and defensive mechanisms. They may also target event aggregation and analysis mechanisms to impede auditing and detection efforts. These attempts can span native defenses and supplemental capabilities installed on a system.

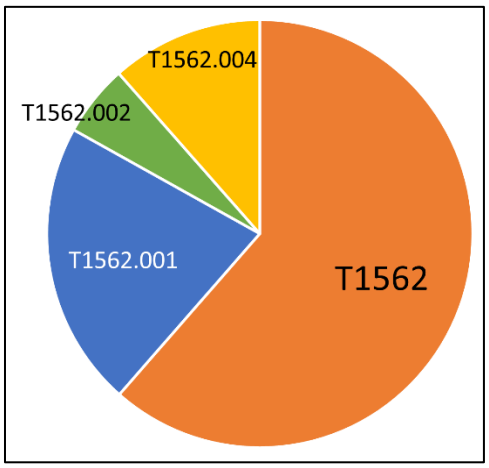


Figure 14. Breakdown of T1562.

A majority of T1562 sightings did not include sub-techniques. This is likely due in part to normalizing our data, which included T1089 from previous ATT&CK versions, to T1562. The most observed sub-technique was Disable or Modify Tools (T1562.001). Adversaries may use this sub-technique to stop defensive services, edit or delete Registry keys, or modify configuration files. The second most-observed sub-technique was Disable or Modify System Firewall (T1562.004). This sub-technique allows adversaries to perform C2 communications, data exfiltration, or lateral movement. Less than 6% of sightings were Disable Windows Event Logging (T1562.002), which reduces the amount of evidence left by adversaries and hinders incident response and forensics efforts.

Most T1562 sightings occurred on Windows-based systems and were almost evenly distributed across the top countries. They followed the overall data trend, with user-level permissions as the most observed privilege level. Notably, T1562 deviated from the overall data trends with Professional, Scientific, and Technical Services and Tofsee as the most observed sector and software, respectively.

Prevention

NIST lists 16 security controls to mitigate Impair Defenses:

- AC-2 Account Management (Also mitigates Disable or Modify Tools, Disable Windows Event Logging, and Disable or Modify System Firewall)
- AC-3 Access Enforcement (Also mitigates Disable or Modify Tools, Disable Windows Event Logging, and Disable or Modify System Firewall)

- AC-5 Separation of Duties (Also mitigates Disable or Modify Tools, Disable Windows Event Logging, and Disable or Modify System Firewall)
- AC-6 Least Privilege (Also mitigates Disable or Modify Tools, Disable Windows Event Logging, and Disable or Modify System Firewall)
- CA-7 Continuous Monitoring (Also mitigates Disable or Modify Tools, Disable Windows Event Logging, and Disable or Modify System Firewall)
- CA-8 Penetration Testing
- CM-2 Baseline Configuration (Also mitigates Disable or Modify Tools, Disable Windows Event Logging, and Disable or Modify System Firewall)
- CM-5 Access Restrictions for Change (Also mitigates Disable or Modify Tools, Disable Windows Event Logging, and Disable or Modify System Firewall)
- CM-6 Configuration Settings (Also mitigates Disable or Modify Tools, Disable Windows Event Logging, and Disable or Modify System Firewall)
- CM-7 Least Functionality (Also mitigates Disable or Modify Tools, Disable Windows Event Logging, and Disable or Modify System Firewall)
- IA-2 Identification and Authentication (organizational Users) (Also mitigates Disable or Modify Tools, Disable Windows Event Logging, and Disable or Modify System Firewall)
- IA-4 Identifier Management
- RA-5 Vulnerability Monitoring and Scanning
- SI-3 Malicious Code Protection (Also mitigates Disable or Modify Tools, Disable Windows Event Logging, and Disable or Modify System Firewall)
- SI-4 System Monitoring (Also mitigates Disable or Modify Tools, Disable Windows Event Logging, and Disable or Modify System Firewall)
- SI-7 Software, Firmware, and Information Integrity (Also mitigates Disable or Modify Tools, Disable Windows Event Logging, and Disable or Modify System Firewall)

Detections

CAR

Rules for Disable or Modify Tools:

- CAR-2013-04-002: Quick execution of a series of suspicious commands
- CAR-2016-04-003: User Activity from Stopping Windows Defensive Services
- CAR-2021-01-007: Detecting Tampering of Windows Defender Command Prompt

Rules for Disable Windows Event Logging:

- CAR-2022-03-001: Disable Windows Event Logging

Sensor Mappings for ATT&CK

Sysmon	1, 12, 13, 14, 4, 5, 6
WinEvtx	1100, 1101, 1102, 1104, 2004, 2005, 2006, 2033, 4103, 4104, 4616, 4657, 4660, 4670, 4688, 4689, 4696, 4703, 4717, 4718, 4722, 4723, 4724, 4725, 4738, 4740, 4742, 4767, 4781, 4946, 4947, 4948, 5025, 5034, 6005, 6006

Top 15 Techniques by Year

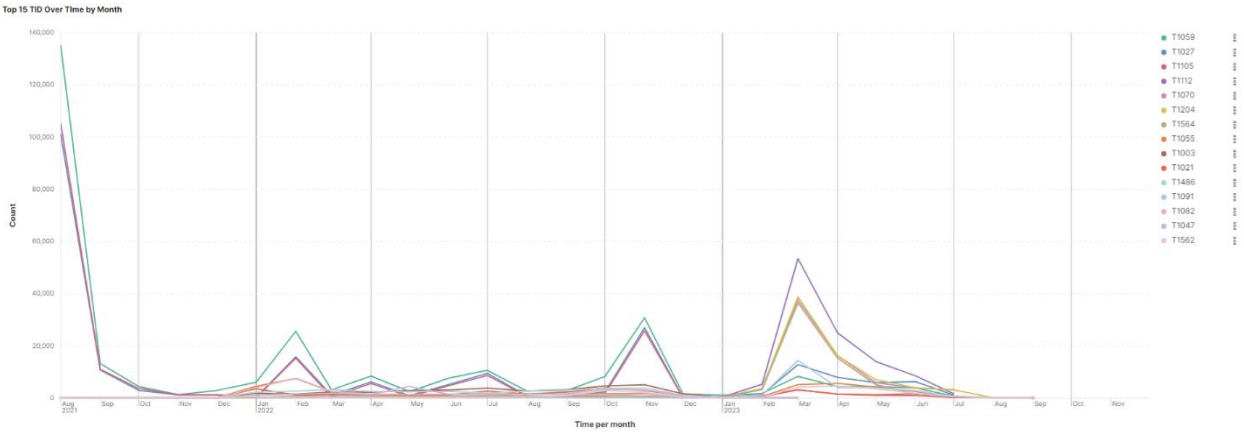


Figure 15. Techniques by Year.

By reviewing the top 15 techniques across the entire timeline, we can use frequency analysis to identify any patterns or anomalies. Note from Figure 15 that there are abrupt increases in our sightings at different times throughout the 26 months. We do not have enough information to know definitively why these spikes occurred. It could be due to an increase of attacks in the wild, or a modified detection capability that suddenly started finding and reporting new techniques. Nearly 80% of our data is raw, meaning it has not been validated by a human. Any misconfigurations or adjusted configurations could result in a data surge.

We also noted changes in the top technique over time. T1059 dominated the top spot until 2023, when T1112 became the most reported technique. This is unsurprising given their ranking in our top 15 techniques. Command and Scripting Interpreter [T1059] and Modify Registry [T1112] are extremely common techniques used by attackers. However, it is unusual that these techniques are part of our data surges. For T1059, it was consistently reported prior to these increases, so a configuration change would likely not be the cause for a sudden increase in sightings. Instead, this technique may have truly been seen more frequently in the wild during these times, or perhaps Sightings received data from additional contributors, causing our sightings to spike. For T1112, we did not have significant reporting of this technique prior to the data surge at the beginning of 2023. This could also be due to its more frequent use in the wild or changes in defense configurations. To truly know why we have these sudden increases, we will have to collaborate more closely with our data contributors.

Technique Co-Occurrence

For the purposes of this paper, a co-occurrence means that a sighting event contains more than one technique. Within our data, around 19% of events contained co-occurrences. Interestingly, we discovered multiple events contained the same cluster of techniques.

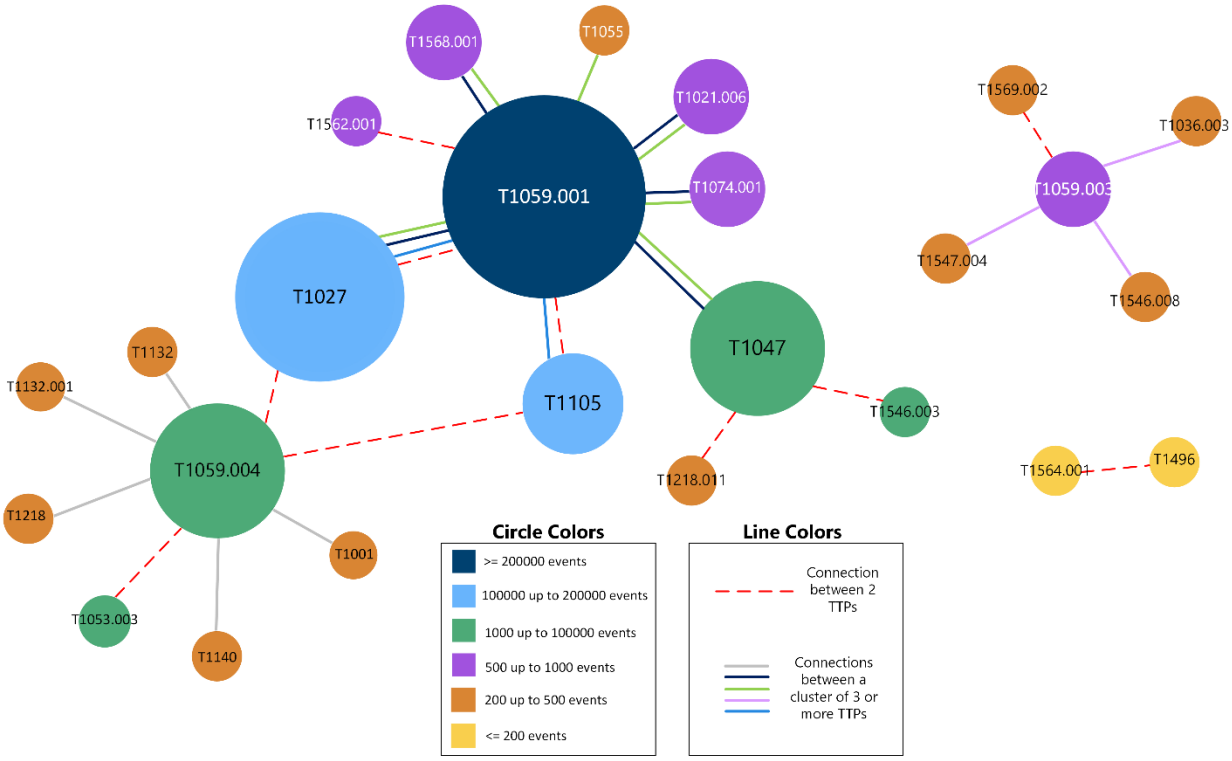


Figure 16. Top 15 Technique Co-occurrences.

This graphic shows several attributes of the top 15 co-occurrences. The size of each sphere represents how frequently the technique occurred within the top 15 events. In size order,

1. Command and Scripting Interpreter: PowerShell [T1059.001]
2. Obfuscated Files or Information [T1027]
3. Windows Management Instrumentation [T1047]
4. Command and Scripting Interpreter: Unix Shell [T1059.004]
5. Ingress Tool Transfer [T1105]
6. Remote Services: Windows Remote Management [T1021.006]
7. Data Staged: Local Data Staging [T1074.001]
8. Dynamic Resolution: Fast Flux DNS [T1568.001]
9. Command and Scripting Interpreter: Windows Command Shell [T1059.003]
10. Event Triggered Execution: Windows Management Instrumentation Event Subscription [T1546.003]
11. Scheduled Task/Job: Cron [T1053.003]
12. Impair Defenses: Disable or Modify Tools [T1562.001]
13. System Binary Proxy Execution [T1218]
14. Masquerading: Rename System Utilities [T1036.003]
15. Event Triggered Execution: Accessibility Features [T1546.008]

The color of the sphere shows how many events contained the co-occurred technique. Different lines were used to show each co-occurrence grouping. When an event contained only two techniques, a dashed, red line was used. When an event contained three or more techniques, a solid line was used.

The different colors of the solid lines are associated with the different groupings of co-occurrences. For example, T1564.001 is a small, yellow sphere, indicating that it was seen the least number of times out of the top 15 co-occurrences and in less than 200 events; it is connected by a red, dashed line to T1496, indicating that it co-occurred only with this technique. Conversely, T1059.001 is a large, blue sphere, indicating that it was seen the greatest number of times and in over 200,000 events; it is connected by both types of lines and several colored lines. It was grouped with T1027 and T1105 in over 140,000 events (represented by the blue line), the most out of any co-occurrences, and seen nearly 40,000 times with T1105 and around 34,500 times with T1027. It is also included in the largest grouping we saw – T1059.001, T1021.006, T1027, T1047, T1055, T1074.001, and T1568.001, represented by the light green line. Similarly, the same cluster of techniques, without T1055, was seen just as frequently, represented by the black line.

Most co-occurrence events include region, sector, platform, and privilege level information, providing insight into how adversaries are using these techniques. Over 200,000 events occur in the United States, with much smaller amounts occurring in Ukraine, Turkey, and Bangladesh. This aligns with the broader regional trend in our data, with a significant majority of events occurring in the US. Additionally, over 98% of co-occurrence events are Windows-based, which also aligns with the overall trend in our data. Adversaries used co-occurring techniques mostly in the Manufacturing and Administrative and Support and Waste… Services sectors. This is semi-similar to our broader data trend, where Manufacturing constitutes around 24% of sighting events, the most of any sector, and Administrative and Support and Waste… Services comprises around 9% of sighting events, the 3rd most out of all sectors. Overall, our data shows around 91% of events using user-level privileges, with around 8% using SYSTEM level privileges. However, co-occurrences swap these amounts, with around 97% using SYSTEM level privileges and around 2% using user-level privileges. When comparing multiple attributes at once (e.g., co-occurrences by region and platform), these trends remain the same.

Figure 17. Co-occurrence Software.

When reviewing the software for co-occurrences, Cobalt strike was seen most frequently, followed by AgentTesla. In our overall data trends, AgentTesla was seen the second most frequently; however, Cobalt Strike was not even in the top 50.

Out of the top 15 co-occurrences, only 6 techniques, or 7 sub-techniques, are not in the top 15 techniques. When we pivot to Tactics, co-occurrences are observed at a similar percentage as our top 15 techniques. However, co-occurrences cover 10% of Persistence tactics and around 5% of Collection tactics, neither of which are covered by our top 15 techniques.

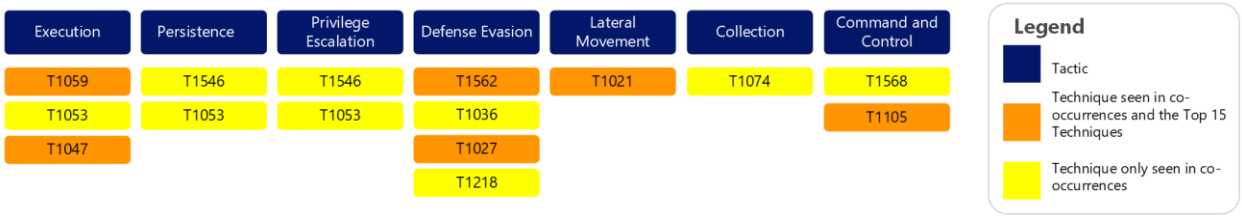


Figure 18. Co-occurrence Tactics.

Additional Analysis

Sectors

The sectors within our data are labeled with the corresponding North American Industry Classification System (NAICS) codes. NAICS organizes sectors into the following categories:

- Agriculture, Forestry, Fishing, and Hunting
- Mining, Quarrying, and Oil and Gas Extraction
- Utilities
- Construction
- Manufacturing
- Wholesale Trade
- Retail Trade
- Transportation and Warehousing
- Information
- Finance and Insurance
- Real Estate and Rental and Leasing
- Professional, Scientific, and Technical Services
- Management of Companies and Enterprises
- Administrative and Support and Waste Management and Remediation Services
- Educational Services
- Health Care and Social Assistance
- Arts, Entertainment, and Recreation
- Accommodation and Food Services
- Other Services (except Public Administration)
- Public Administration

Overall, nearly 25% of sightings occurred within the Manufacturing sector, which was twice as much as the next most frequently seen sector. There are also 4 sectors that are seen in less than 1% of sightings - Retail Trade, Real Estate and Rental and Leasing, Utilities, and Arts, Entertainment, and Recreation. It should be noted that 66% of our data contained sector information.

Techniques

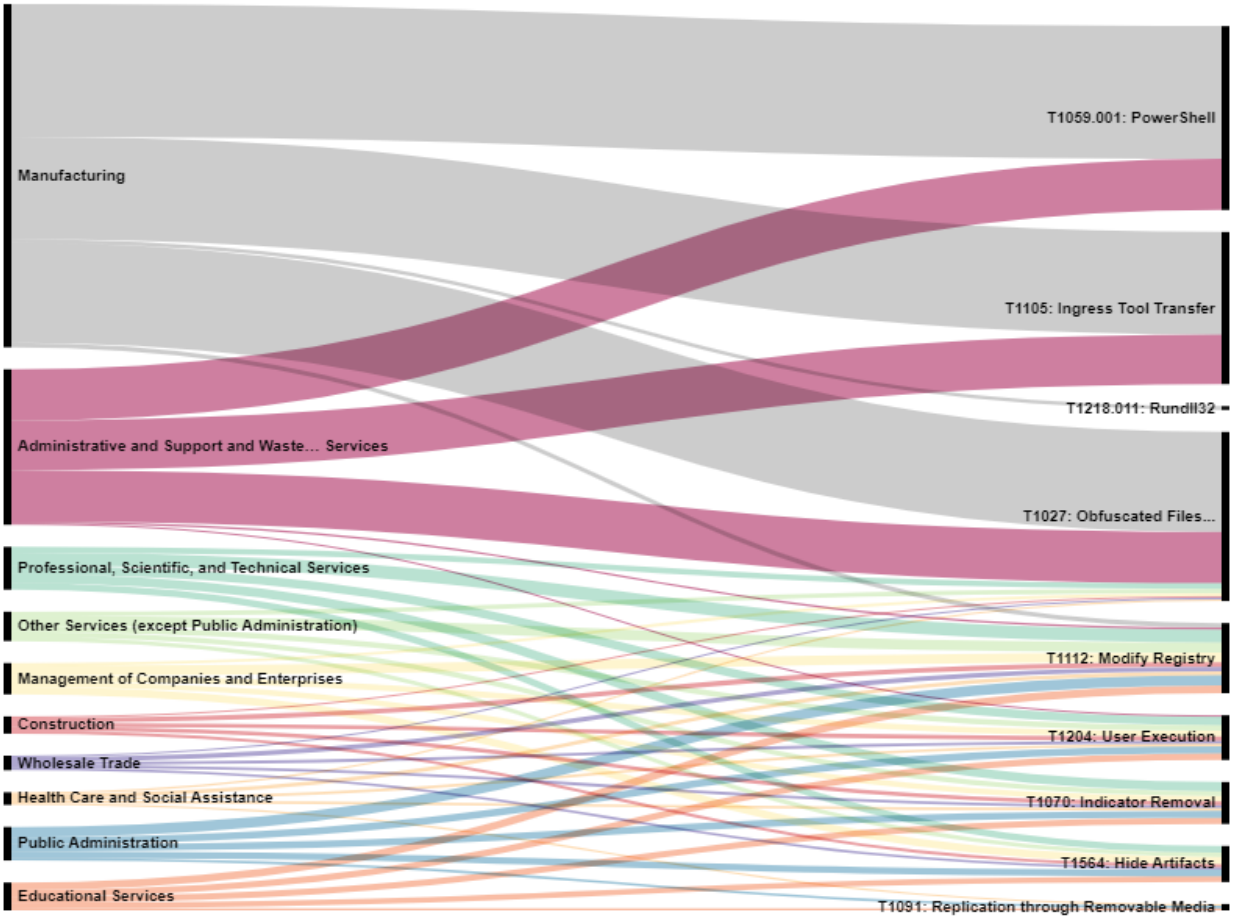


Figure 19. Top 5 Techniques for the Top 10 Sectors.

Identifying the top techniques by sector is important when tailoring defenses. Each sector has different software and hardware requirements; even within a sector, different organizations have unique network configurations and settings. However, despite these differences, there are relatively few techniques observed across the top sectors, and all but one technique, T1218.011, are covered in the top 15 techniques. Cyber defenders can use this breakdown to gain insight into the techniques, corresponding defenses, and NIST controls observed in their specific sector.

Regions

Most sectors are going to be seen in each region. Therefore, we focused on the outliers in this area. Because most of our data is from the US, we would expect to see the US as one of the top countries targeted within each sector. However, only half of the sectors (10 out of 20) have the US as part of their top 5 countries – Manufacturing; Professional, Scientific, and Technical Services; Administrative …; Health Care…; Information; Finance and Insurance; Retail Trade; Real Estate…; Utilities; and Arts…. Of these, only Professional, Scientific, and Technical Services; Health Care…; and Finance and Insurance do not primarily or exclusively target the US.

Regions

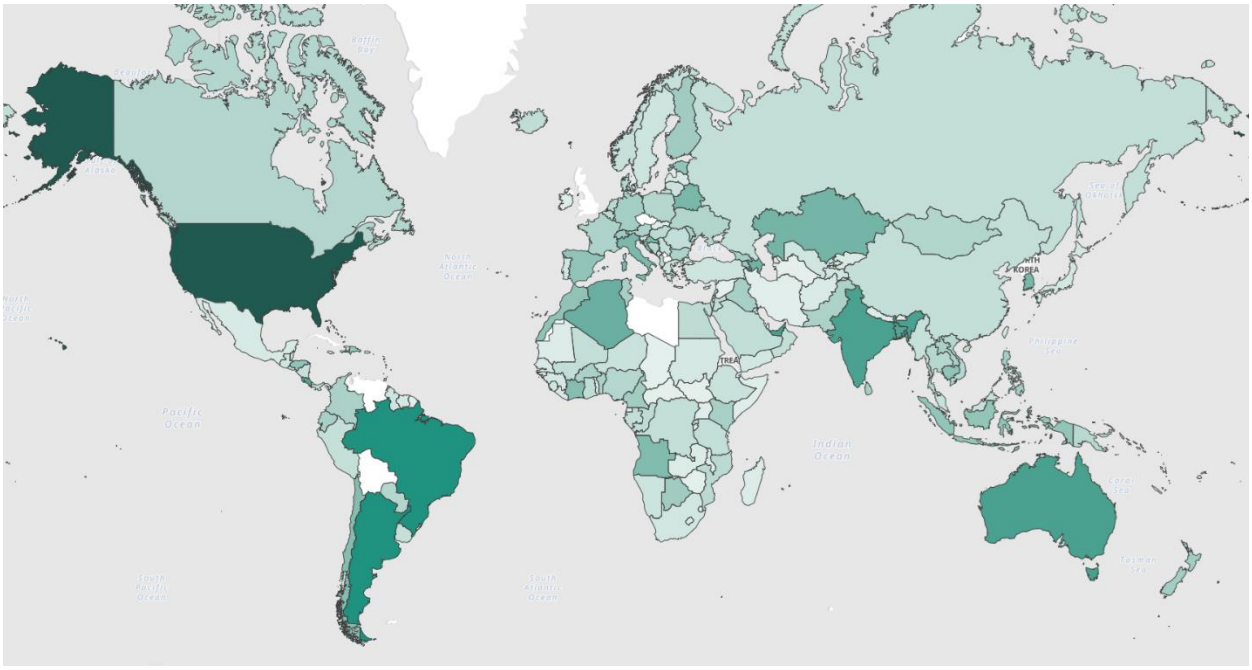


Figure 20. Sightings by Country.

We were provided with the corresponding ISO Alpha-2 country code for our sightings. The above image represents a world view of our data set. The color is darker where more Sightings were seen. Where necessary, the country code has been changed to the country's name for clarity. It should also be noted that 66% of our data contains regional information.

Unsurprisingly, the United States dominated the count by an order of magnitude above the next closest country. We can likely attribute this to several causes:

- As the second largest economy in the world (by Gross Domestic Product[4] (GDP)), the US presents a lucrative target for cyber-attacks.
- Due to its progressive economy, a high percentage of companies and organizations within the US likely have advanced cyber defense methods, resulting in more collected data to analyze.
- Many of our providers operate in the US.

Overall, we expected to see the number of sightings observed to be roughly similar to global GDP rankings. Countries with a higher GDP are likely to have more targets with higher potential value and more cyber defense capabilities (resulting in more sightings attributed to them). However, we do not have significant sightings from China, Japan, or Russia, which are ranked in the top 5 world economies by GDP. The most likely reason for this lack of data is due to who our contributors are and where they have visibility. After the US, our next largest contributors were Brazil and Argentina. This was due to a large number of sightings from a single contributor whose primary market was South America, in particular,

[4] https://www.worldeconomics.com/Rankings/Economies-By-Size.aspx

Argentina and Brazil. We also saw a larger number of sightings from developed countries, such as Western Europe, South and East Asia, and Oceania.

Techniques

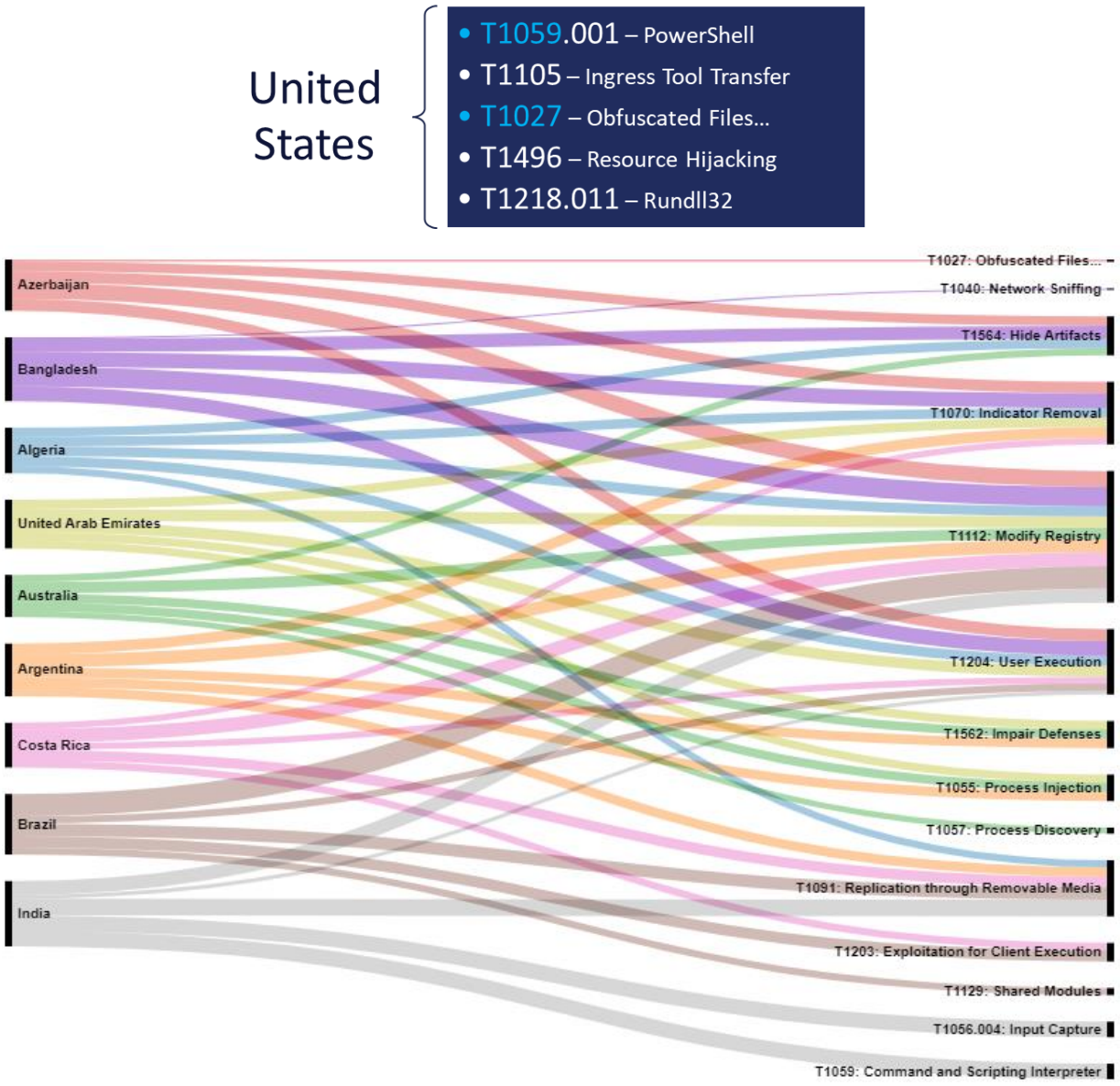


Figure 21. Top 5 Techniques for the Top 10 Countries.

We can observe the top five techniques within the top 10 countries. Because there was not much overlap between the techniques seen in the US compared to other countries, we put the US techniques in their own chart. Any overlap is indicated in light blue font under the US techniques. When compared to the overall top 15 techniques, T1059, T1027, and T1105 are mostly seen in the US; T1091, T1112, T1204, T1564, T1070, T1562, and T1055 are seen in multiple countries. Only a few techniques are not seen in the top 15 techniques – T1496, T1218.011, T1203, T1040, T1057, and T1056. These techniques span the Execution, Defense Evasion, Credential Access, Discovery, Collection, and Impact Tactics. Cyber

defenders can use this breakdown to gain insight into the techniques, corresponding defenses, and NIST controls observed in their specific regions.

Sector

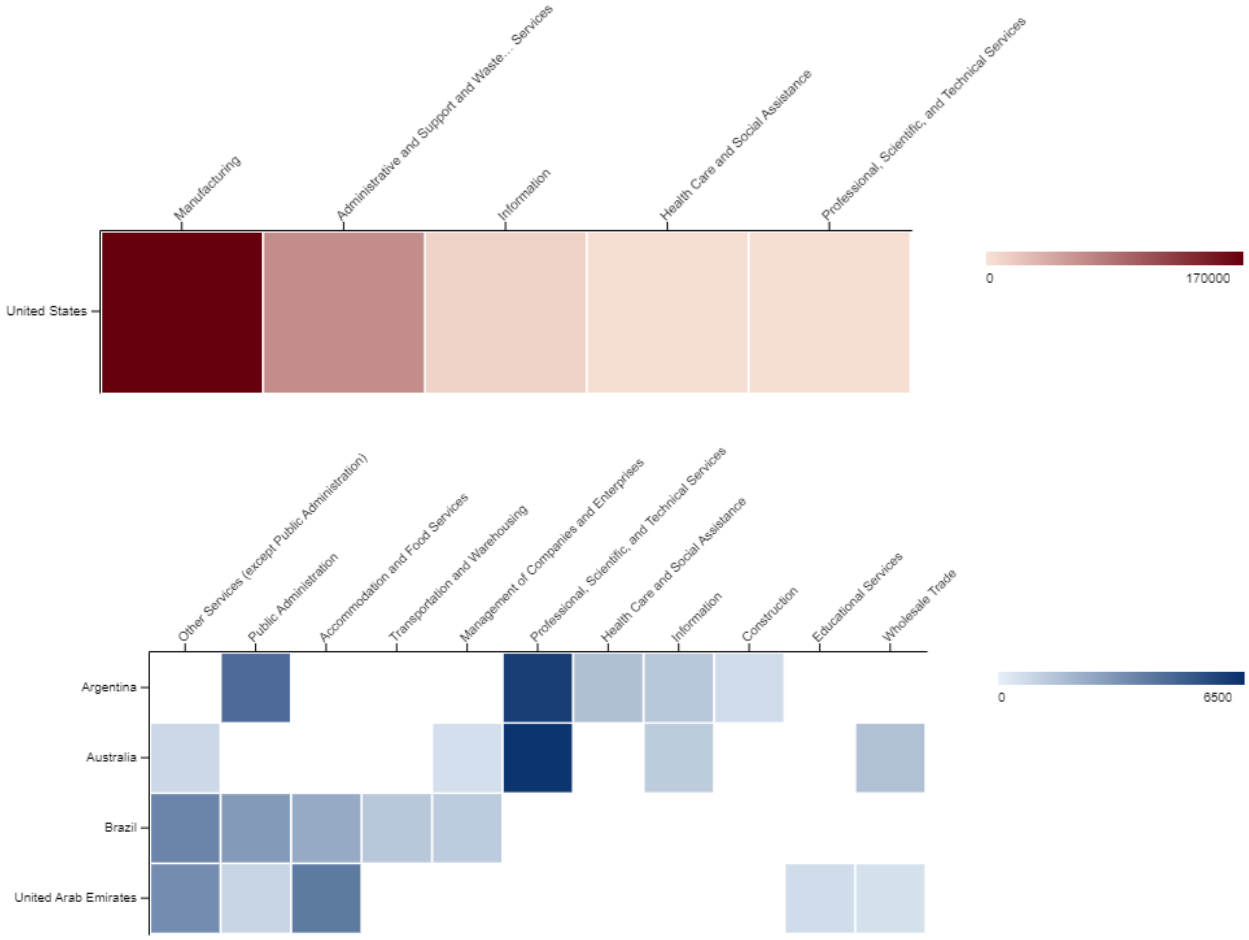


Figure 22. Top 5 Sectors for the Top 5 Countries.

We can observe the top five sectors from each country to gain insights into where adversaries have recently attacked. Because our data heavily favors the US, splitting the graphs between the US and other top 4 countries was necessary again. Within the US, the Manufacturing sector was seen at a higher rate than any other sector. However, none of the other top 4 countries had any events observed in the Manufacturing sector. These countries saw a wider range of sectors and more evenly distributed sightings per sector.

Software

It should be noted that 25% of our data contained software information.

Techniques

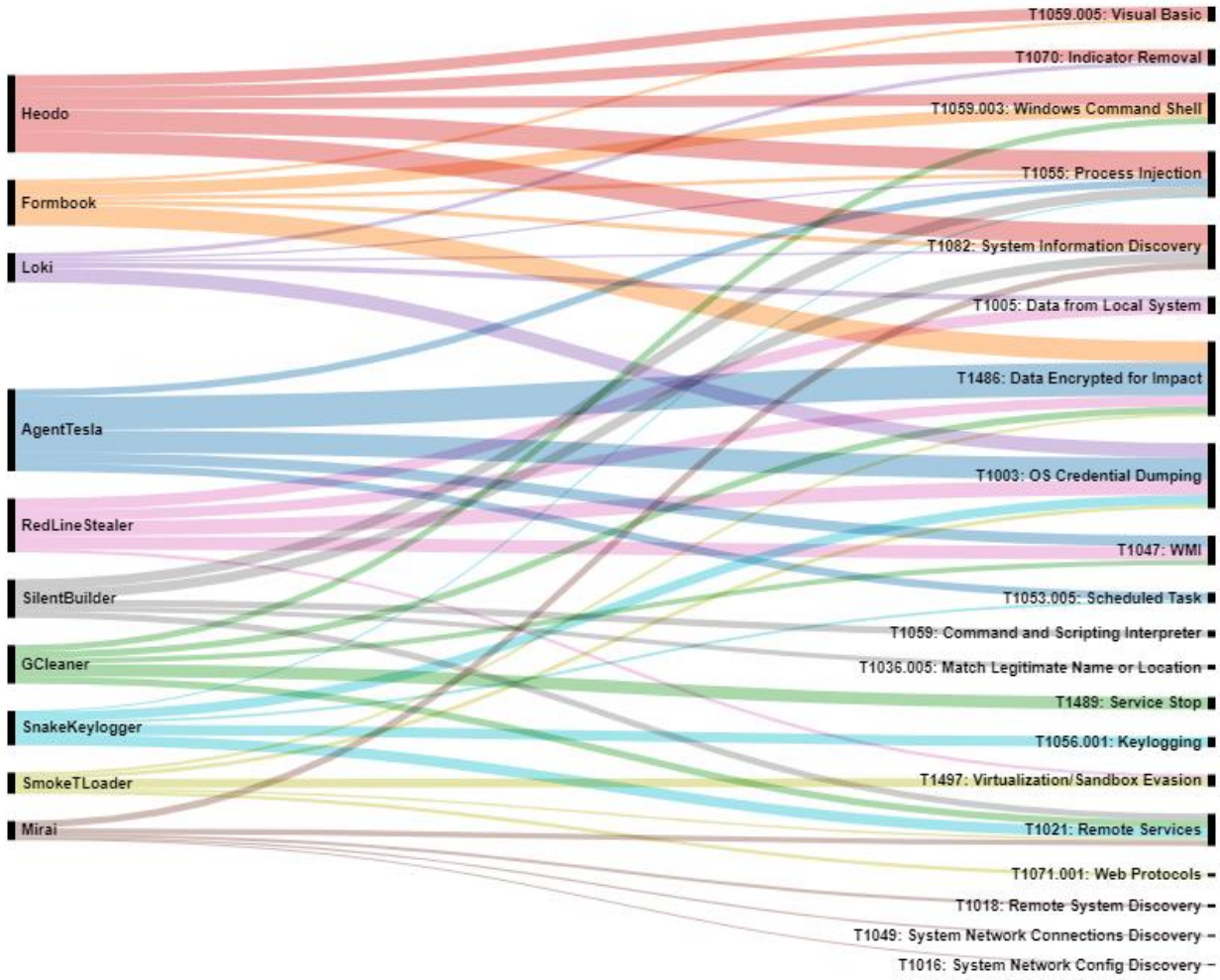


Figure 23. Top 5 Techniques for the Top 10 Software.

By viewing the top techniques used by different software, we can gain insights into how adversaries are using each software to conduct their attacks. Within our data, about half of the top techniques used by software are in our top 15 techniques. These techniques comprise nearly all of our sightings. For T1059, its sub-techniques are observed being used by Heodo, Formbook, and GCleaner. The other top techniques seen were used by only one or two software. These are used by attackers for Discovery, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Collection, Command and Control (C2), and Impact Tactics. Cyber defenders can use this breakdown to gain insight into the techniques, corresponding defenses, and NIST controls observed by specific software.

Platform

Figure 24. Top 10 Nix Software.

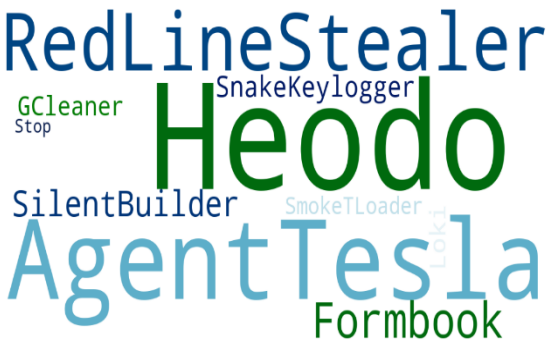


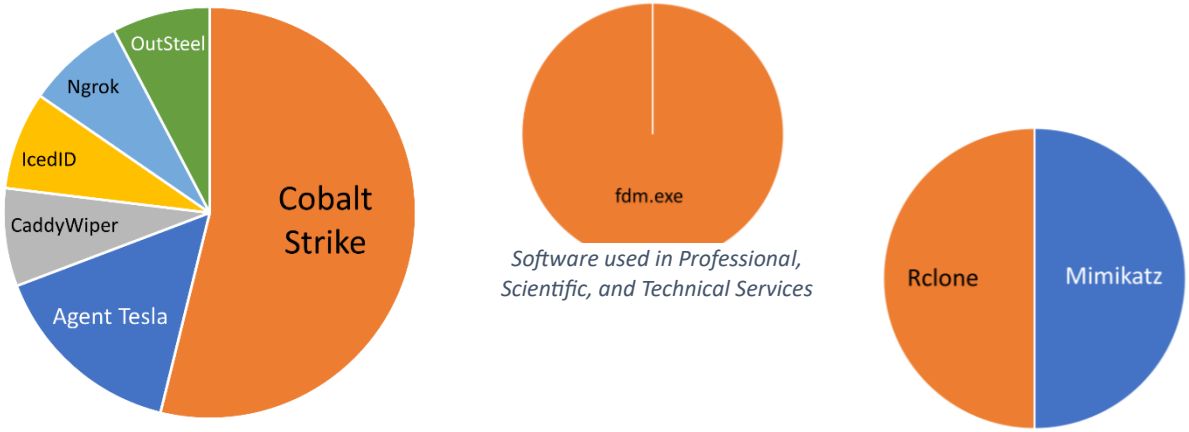
Figure 25. Top 10 Windows Software.

Organizations are focused on providing their employees with appropriate computing technology to maximize their productivity, but cyber defenders must track that technology and ensure appropriate defenses are in place. By knowing which software is most observed by platform, defenders can hone their defenses and verify their visibility into each platform to detect the different software used by attackers. Within our data, we can observe software usage by Windows and Nix platforms. For Nix, our sightings were primarily comprised of Mirai usage. For Windows, our sightings were spread more evenly across the top 10 software. However, our top 3 were Heodo, AgentTesla, and RedLineStealer. As evidenced by the wordclouds, AgentTesla, Formbook, and SnakeKeylogger were the main 3 software that spanned Windows and Nix platforms.

Sector and Region

Observed software can be categorized by sector or region to gain insights into how adversaries are currently using different software in the wild. Within our data, we saw software used in the Public Administration, Utilities, and Professional, Scientific, and Technical Services sectors. For Public Administration, we observed the following software: Cobalt Strike, AgentTesla, CaddyWiper, IcedID, Ngrok, and OutSteel. However, Cobalt Strike was seen significantly more than other software. For

Utilities, we saw an even split between Mimikatz and Rclone. For Professional, Scientific, and Technical Services, we only saw fdm.exe in our sightings.



Software used in Public Administration.

Software used in Professional, Scientific, and Technical Services

Software used in Utilities.

Figure 26. Top 10 Software for the Top 3 Sectors.

Within our data, the same sightings marked with sector information included region information. The software used in the Public Administration sector occurred, in the same percentages, in the United Arab Emirates. The software used in the Utilities sector occurred, in the same percentages, in Turkey. The software used in Professional, Scientific, and Technical Services sector occurred in Bangladesh. While this is an interesting observation, these sightings compose an extremely small portion of all sightings. The correlation between sector and region software is most likely due to the sightings coming from the same anonymous contributor.

Techniques by Platform

Within our data, we have Windows-, Nix-, and MacOS-based platforms. We also have an "Other" option, which includes data from Software as a Service (SaaS), Infrastructure as a Service (IaaS), Containers, Network, and cloud sources. It should be noted that 93% of our data contained platform information.

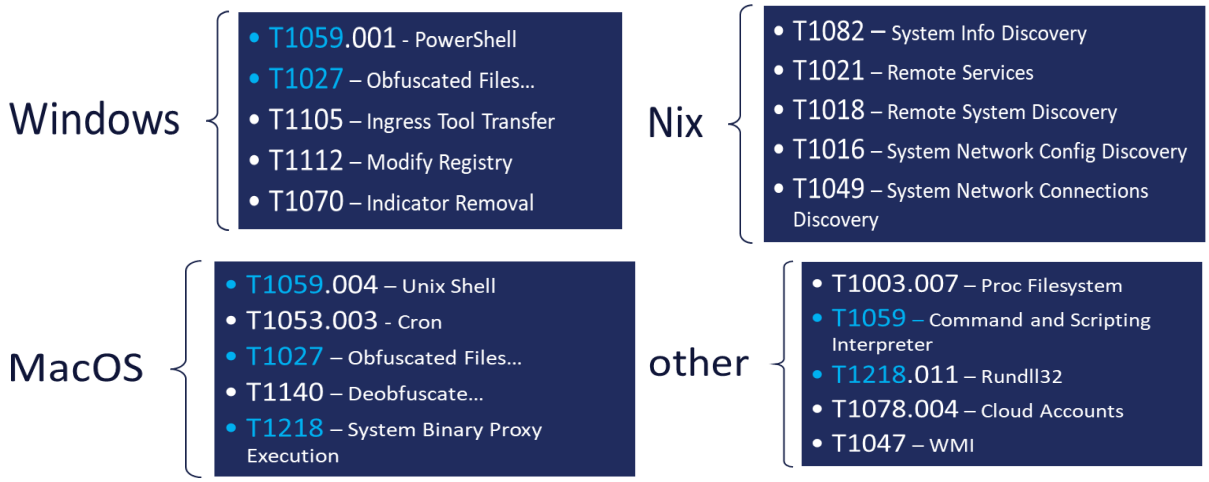


Figure 27. Top 5 Techniques by Platform.

The MITRE ATT&CK matrix includes platform information for each technique; however, with sightings data, we can observe which platform-based techniques are seen most frequently in the wild. Since around 90% of our data is Windows-based, we would expect to see the Windows techniques comprised mostly of the top 15 techniques. As the chart demonstrates, this hypothesis was correct. We also see some of the top 15 techniques associated with the other 3 platforms as well. The light blue font highlights any technique overlap between platforms. Surprisingly, there is no overlap between Nix and Windows and Nix and MacOS platforms. T1027 and T1059 were seen on Windows and MacOS platforms, and T1218 overlaps with MacOS and Other platforms. For the remaining techniques (that are not in the top 15 techniques), attackers focused on varying Tactics. For Nix, the techniques seen were Discovery focused. For MacOS, the techniques span the Execution, Persistence, Privilege Escalation, and Defense Evasion Tactics. For Other platforms, the techniques cover Defense Evasion, Persistence, Privilege Escalation, and Initial Access Tactics. Cyber defenders can use this breakdown to gain insight into the techniques, corresponding defenses, and NIST controls observed by specific platforms.

Techniques by Privilege Level

It should be noted that 35% of our data contains relevant privilege level information.

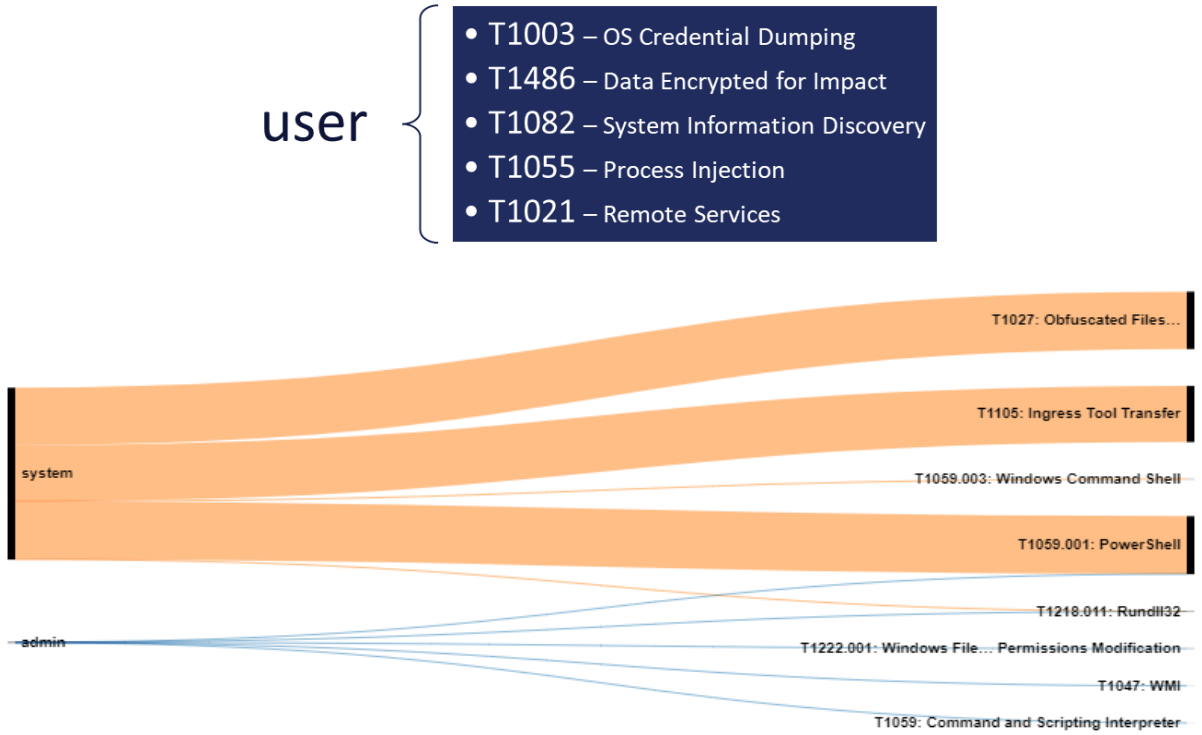


Figure 28. Top 5 Techniques for Privilege Levels.

Similar to platforms, the MITRE ATT&CK matrix includes information on what permissions are required for each technique. By using sightings data, we can observe the top techniques seen by privilege level. Overall, most techniques are in the top 15 techniques. The remaining techniques, T1218.011 and T1222.001, are used by adversaries for Defense Evasion. Cyber defenders can use this breakdown to gain insight into the techniques, corresponding defenses, and NIST controls observed by specific permissions.

Missing Techniques

In total, 61 techniques from the current version of ATT&CK were not in our Sightings Data. This represents about 26% of the current Techniques. When reviewing the techniques at a Tactic level, Defense Evasion has the most missing techniques; however, Reconnaissance has the highest percentage of missing techniques. This is likely due to Defense Evasion having the most techniques overall, making the percentage of missing techniques smaller. Out of the missing techniques, around 19% (12 out of 61) are for Cloud, Containers, and Infrastructure as a Service platforms; around 11% (7 out of 61) are Pre-ATT&CK techniques (under Reconnaissance and Resource Development Tactics); and around 6% (4 out of 61) are network-based. The rest of the missing techniques can be detected on Windows, Linux, or MacOS. Overall, the missing techniques are only a small sub-set of each Tactic.

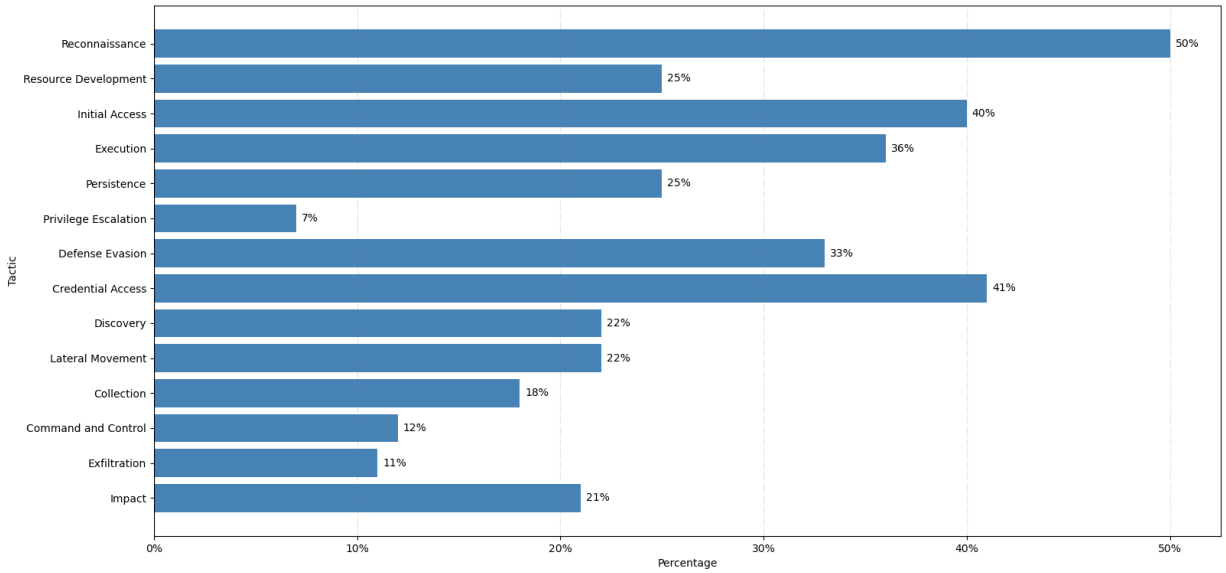


Figure 29. Percentage of Missing Techniques for each Tactic.

Defenses in Summary

For our report, we included prevention controls from NIST 800-53r5 and detections from CAR analytics, and Sysmon and Windows Event Logs from Sensor Mappings to ATT&CK. These preventions and detections are intended to be a starting point for defenders to protect against the top 15 most observed techniques. From NIST, Access Control, System and Information Integrity, and Configuration Management were the main categories. Controls from these families were seen numerous times as preventions for the top 15 techniques and sub-techniques. For CAR mappings, CAR-2013-04-002: Quick execution of a series of suspicious commands detected 6 out of 15 techniques; CAR-2013-07-001: Suspicious Arguments detected 3 out of 15 techniques; and CAR-2014-11-004: Remote PowerShell Sessions detected 2 out of 15 techniques. Out of all CAR analytics, applying these three would provide the best return on investment (ROI).

For Windows event logs, there are numerous helpful event IDs for each technique. The top event IDs focus on process creation (4688), assigning process tokens (4696), and logging PowerShell activities (4103).

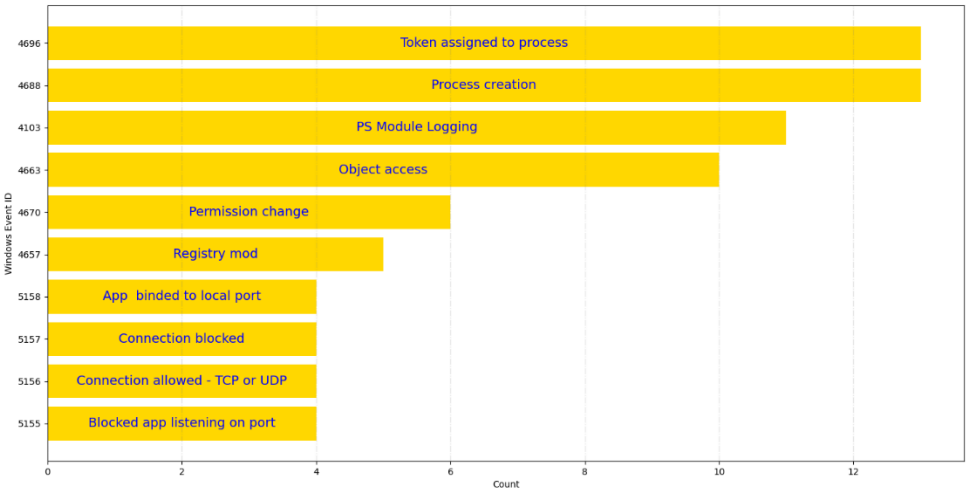


Figure 30. Coverage of the Top 10 Windows Event IDs.

The top Sysmon IDs focus on process creation (1), file creation (11), and named file stream creation (15). Interestingly, the top Sysmon ID (1) and the top Winevtx event ID (4688) focus on monitoring process creation.

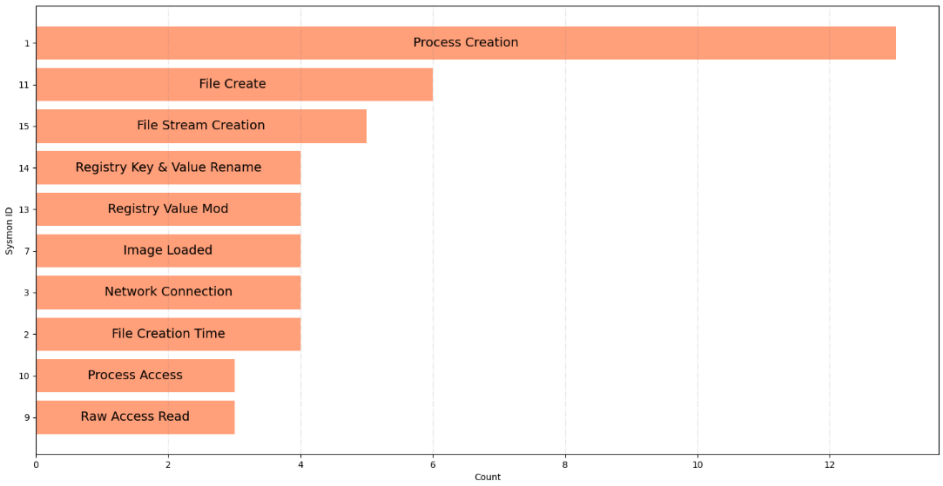


Figure 31. Coverage of the Top 10 Sysmon IDs.

There are other detections that we were not able to include in this paper but want to highlight for defenders. Sigma provides numerous detection rules, based on operating system or platform. However, many rules are experimental and need to be tuned to prevent false positives. There are also tools to convert Sigma rules into different formats, such as sigconverter.io or Sigma Command Line Interface. MITRE's CAR repository also includes a comparison chart for each ATT&CK technique, showing its coverage by CAR, Sigma, Elastic Detection (ES), and Splunk rules. It provides links to each repository for defenders to quickly identify relevant detections by technique/sub-technique. In addition to Sysmon and WinEvtx, Sensor Mappings to ATT&CK includes mappings for Auditd, CloudTrail, OSQuery, and Zeek. While we were only able to include WinEvtx and Sysmon in our report, we encourage defenders to visit the project's website for a complete list of all mappings.

To identify which prevention and detection methods are needed in their environment, defenders can use the Sightings data to assess their current security products and inform their security strategy. With ATT&CK Navigator, defenders can document what techniques they can detect and how they prioritize

those detections. Resources, such as the Center's Adversary Emulation Library, MITRE's CALDERA platform, or Red Canary's Atomic Red Team library, can test an organization's defenses and detections on a recurring basis. These libraries contain tests for the specific adversary behaviors observed in our Sightings dataset. These resources, and others, allow defenders to identify coverage gaps and test their tools against the top 15 techniques observed in the wild.

Sightings Data Model and Lessons Learned

Data Model

We provide a data model to potential contributors that shows the format for submitting information and includes required and optional fields. Between the first round of Sightings and this round, our data model changed slightly with the elimination of size, end_time, attribution, and attribution_type fields. Size, when combined with data from other fields, could reveal victim information despite our anonymizing attempts. It is also a difficult field to collect, like end_time, because contributors likely do not include this information in their own data collection. Additionally, attribution is a notoriously difficult problem in the cyber security community. It takes contributors significant time and effort to identify attribution, if it's even possible to do. Because of these considerations and the lack of data for these fields in round 1, we removed them for round 2. We also added a platform field for round 2. This allowed us to easily view sightings across different operating systems.

Field	Datatype	Description
version	String	Required version string for the data model. **MUST** be set to `2.0`
id	String	Required ID for this event. **MUST** be in UUIDv4 format
start_time	Timestamp	Time the activity started, in UTC. **MUST** be in RFC 3339, section 5.6 **date-time** format. For example: `2018-11-13T20:20:39+00:00`
tid	Array	Array of techniques, including subtechniques that were observed. One or many techniques can be accepted
detection_type	String	**MUST** be one of the following values: `human_validated` or `raw`. Use `human_validated` when a human analyst has reviewed the detection and determined it to not be a false positive. Use `raw` when no validation has occurred.
detection_source	String	**MUST** be one of the following values: `host_based`, `network_based`, or `cloud_based`
software_name	String	**Only if available** Malicious software that was observed. **SHOULD** ideally be an exact name from the list of Software Names or Associated Software already in ATT&CK
hash	String	**Only if available**. Value **MUST** be MD5, SHA-1, or SHA-256 hash of the software
sector	String	**MUST** be NAICS code for the sector(s) in which the victim belongs, such as `22` (utilities). *Only include the first 2 digits
country	String	**MUST** be the ISO 3166-1 alpha-2 country code of the victim. For example, United States is `us`
region	String	**Only submit if not submitting** `country`. The IANA Regional Internet Registry code of the victim, e.g. `ARIN`
platform	String	The platform on which this technique was observed. Valid options are `windows`, `macos`, `nix`, `other`
privilege_level	String	**MUST** be one of the following values: `system`, `admin`, `user`, `none`

Figure 32. Sightings II Data Model.

Lessons Learned

We discovered multiple issues during analysis. One of the most significant issues was the different ATT&CK versions present in our data. While ATT&CK updates occur twice per year, often they are minor updates. However, our data spans 26 months and includes data from older ATT&CK versions, such as ATT&CK version 7 which introduced many new techniques and depreciated/revoked several others. While this was released in 2020, we still found data using old Technique IDs pre-version 7. As a short-term solution, we used specific queries in ELK or wrote our own python scripts to generate correct visualizations and statistics. However, this proved extremely time-consuming. In future versions of the Sightings Ecosystem, we would limit which versions of ATT&CK that contributions could contain. By requiring data to be in ATT&CK version 12 and up, for example, we can mitigate how much normalization is required to have all data aligned with the most current version of ATT&CK.

While our data model includes many interesting fields, their lack of reporting resulted in analysis that was not completely representative and had to be heavily caveated. Optional fields, such as software_name, were reported in only a small sub-set of our data. In many cases, privilege_level and sector, though required fields, contained nondescript answers, such as none and unknown, respectively. This severely reduced the amount of data that contained descriptive answers in these fields, resulting in analysis that tended to cover only a third of our data. For future versions of the Sightings Ecosystem, we would strongly encourage all fields to be included and contain descriptive information. This allows us to provide additional and more detailed analysis to the public regarding some interesting fields, such as privilege levels and software used in the wild.

While we improved our methods and infrastructure to ingest and analyze data, we still encountered several issues. We had many instances where wiping and re-ingesting the data into Elastic was required to fix different issues. In some cases, the ingest process would stall due to our large data set, adding additional time to our troubleshooting. While mitigating data discrepancies, we exported the data for analysis. However, this was also time-consuming due to our large data set. Since we expect our data set to continue to grow, it will be crucial to identify better ways to ingest and analyze the data.

Sightings Ecosystem in the Future

While we are always looking for more contributors for the Sightings Ecosystem project, it is a tricky balance between encouraging maximum contribution and imposing more stringent rules on data contribution. This is why our data model has optional fields, even if the data would provide added benefits and additional analysis. This iteration, we decided to include analysis of these areas, despite only having a small sub-set of data with that information. In future iterations, we hope to receive more data labeled with the optional data fields, allowing us to continue to provide new and better analysis. Our data model will also continue to change as we determine important and relevant fields for analysis. We hope to continue expanding the Sightings Ecosystem to provide insights and analysis to better inform the cyber security community.

About Center for Threat Informed Defense

The Center is a non-profit, privately funded research and development organization operated by MITRE Engenuity. The Center's mission is to advance the state of the art and the state of the practice in threat-informed defense globally. Comprised of participant organizations from around the globe with highly sophisticated security teams, the Center builds on MITRE ATT&CK®, an important foundation for threat

informed defense used by security teams and vendors in their enterprise security operations. Because the Center operates for the public good, outputs of its research and development are available publicly and for the benefit of all.

https://ctid.mitre-engenuity.org

For more information:

Center for Threat-Informed Defense

ctid@mitre-engenuity.org

Appendix A

Each Technique seen in the sightings data under their corresponding Tactic.

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
T1595	T1583	T1189	T1059	T1098	T1548	T1548	T1110	T1087	T1210	T1560	T1071	T1020	T1485
T1592	T1586	T1190	T1203	T1197	T1134	T1134	T1555	T1010	T1570	T1123	T1659	T1030	T1486
T1589	T1584	T1566	T1559	T1547	T1098	T1197	T1056	T1217	T1563	T1119	T1132	T1048	T1565
T1590	T1587	T1091	T1106	T1037	T1547	T1622	T1621	T1526	T1021	T1185	T1001	T1041	T1491
T1598	T1588	T1195	T1053	T1176	T1037	T1140	T1040	T1613	T1091	T1115	T1568	T1052	T1561
	T1608	T1078	T1129	T1554	T1543	T1006	T1003	T1622	T1080	T1213	T1573	T1567	T1499
			T1569	T1136	T1484	T1484	T1649	T1482	T1550	T1005	T1008	T1029	T1490
			T1204	T1543	T1546	T1211	T1558	T1083		T1039	T1105	T1537	T1498
			T1047	T1546	T1068	T1222	T1539	T1046		T1025	T1104		T1496
				T1574	T1574	T1564	T1552	T1135		T1074	T1095		T1489
				T1137	T1055	T1574		T1040		T1114	T1571		T1529
				T1542	T1053	T1562		T1120		T1056	T1572		
				T1053	T1078	T1070		T1069		T1113	T1090		
				T1505		T1036		T1057		T1125	T1219		
				T1078		T1112		T1012			T1102		
						T1027		T1018					
						T1542		T1518					
						T1055		T1082					
						T1620		T1614					
						T1207		T1016					
						T1014		T1049					
						T1553		T1033					
						T1218		T1007					
						T1221		T1124					
						T1127		T1497					
						T1550							
						T1078							
						T1497							
						T1220							

Appendix B

Each Technique missing from the sightings data under their corresponding Tactic.