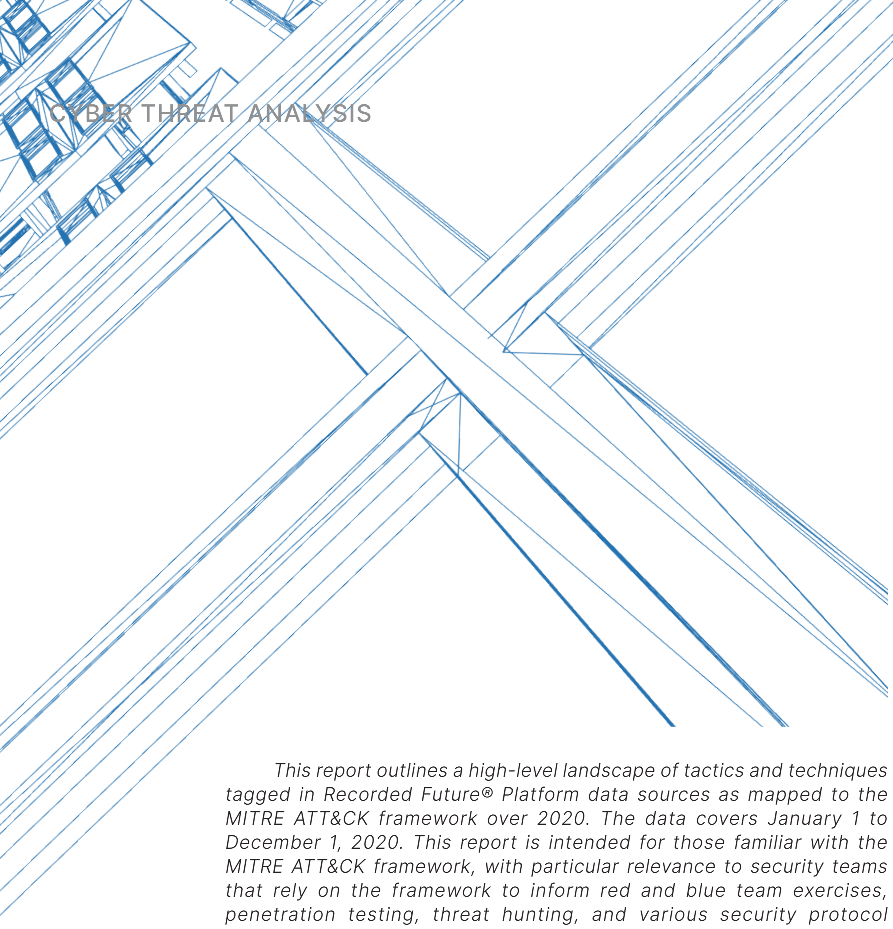
CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

CTA-2021-0203

TOP 6 MITRE ATT&CK TECHNIQUES IDENTIFIED IN 2020, DEFENSE EVASION TACTICS PREVAIL



This report outlines a high-level landscape of tactics and techniques tagged in Recorded Future® Platform data sources as mapped to the MITRE ATT&CK framework over 2020. The data covers January 1 to December 1, 2020. This report is intended for those familiar with the MITRE ATT&CK framework, with particular relevance to security teams that rely on the framework to inform red and blue team exercises, penetration testing, threat hunting, and various security protocol prioritizations.

Executive Summary

In 2020, the six most widely used techniques according to the Recorded Future Platform were T1027 — Obfuscated Files and Information, T1055 — Process Injection, T1098 — Account Manipulation, T1219 — Remote Access Tools, T1082 — System Information Discovery, and T1018 — Remote System Discovery. Additional "Associated Techniques", or MITRE ATT&CK techniques that were related to the top six, included the following three: T1497 — Virtualization/Sandbox Evasion, T1083 — File and Directory Discovery, and T1036 — Masquerading.

Four of these techniques are categorized under the Defense Evasion tactic, followed by Persistence and Discovery. Seeing Defense Evasion tactics prevail in the data is in line with Insikt Group's observations that these tactics are becoming more commonplace in malware. Identifying these techniques helps to identify what the cyber threat landscape looked like in the last year: from opportunistic threat actors taking advantage of a remote workforce due to COVID-19 to major expansions of prominent ransomware operators to include exfiltration and extortion. All of the techniques identified were critical to the success of cyberattacks in 2020.

The challenge for defenders is making this information actionable. Detection of some of these techniques can be difficult as more advanced threat actors attempt to hide their true intentions or blend in with normal activities. As mentioned in the MITRE ATT&CK glossary, data should not be viewed in isolation, but rather as a pattern of activity that highlights tactics like Defense Evasion or Persistence. By correlating these techniques with additional high-fidelity events, defenders can find better indications of suspicious activity. We have included detections for both individual malware observed using the highlighted techniques and more high-level detection strategies in this report.

Background

MITRE ATT&CK is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK framework is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. With the help of the ATT&CK framework, security teams have a wider picture of adversary behavior, allowing mitigation and detection methods to be tested against the techniques. It has become a useful tool across many cybersecurity disciplines to provide intelligence, track trends in tactics and techniques, perform testing through red teaming or adversary emulation, and improve network and system defenses against intrusions.

The ATT&CK framework has evolved since its publication in 2018, containing almost 200 unique tactics, techniques, and procedures (TTPs). The recent consolidation of the Pre-ATT&CK framework with the main Enterprise ATT&CK framework, as well as the introduction of subtechniques, have only furthered the usability of the framework.

Methodology

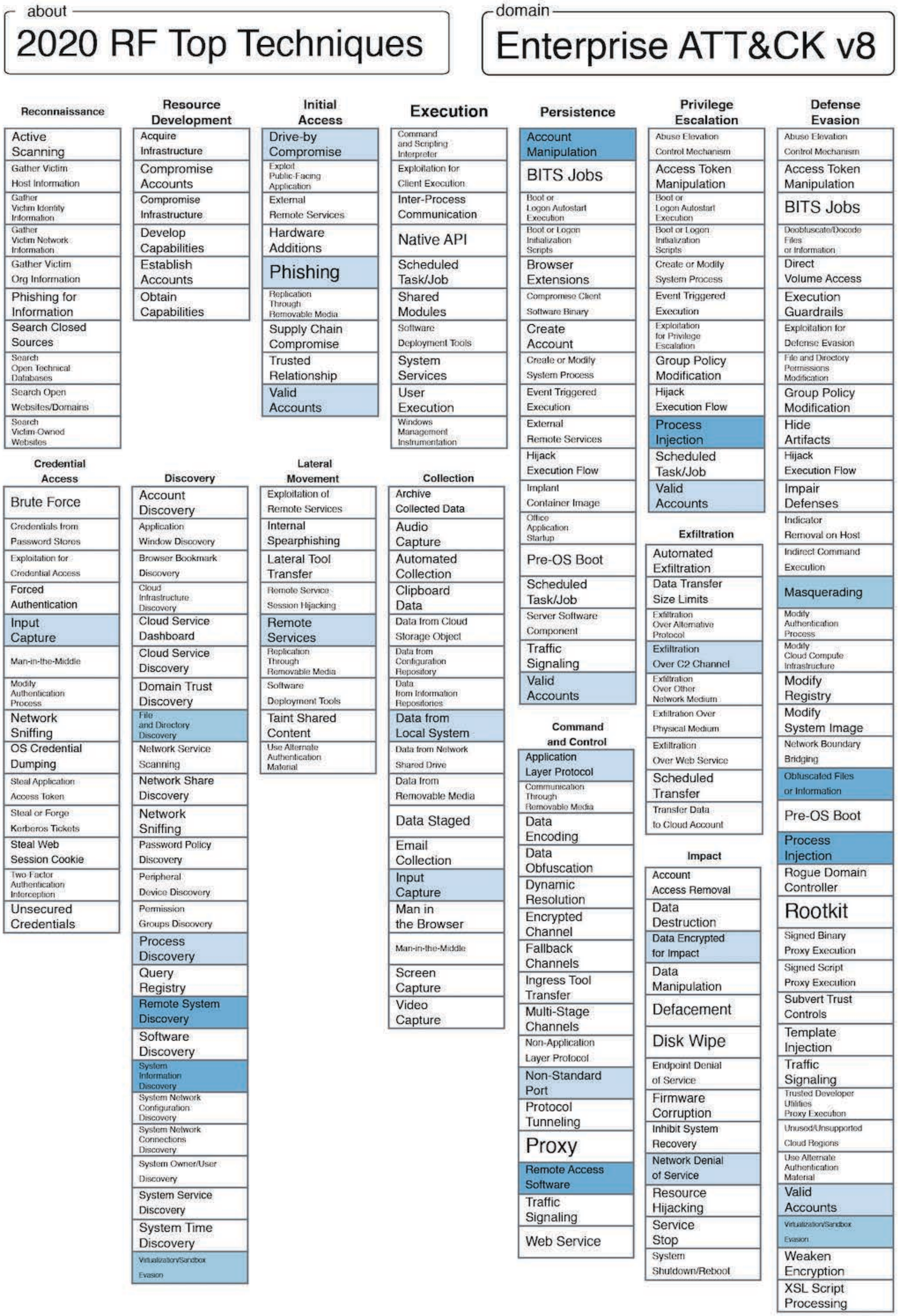
In our 2019 report, Insikt Group relied on the Recorded Future Malware Detonation Sandbox as a source for finding top ATT&CK techniques. Based on the changes to the ATT&CK framework and the continued improvement of Recorded Future data, we used three queries in the Recorded Future Platform to aid in identifying the "top" MITRE ATT&CK techniques used in 2020. Data from each query is taken from Insikt Notes, Recorded Future Malware Detonation Sandbox samples, and Attack Vectors as automatically categorized by Recorded Future.

Insikt Group notes cover a wide range of threat intelligence and cyberattacks, which is represented in the first query. The second query, using the Malware Detonation Sandbox sample analysis as a source, provides a technical perspective focused on execution of malware. The third query looks for Cyber Attack events where a MITRE ATT&CK technique was specified as an attack vector to try and capture any additional information. The queries were separated to tune out false positives and to provide a more holistic picture of techniques used.

The mid-year revision of the ATT&CK framework, which included Pre-ATT&CK and subtechniques, created what we believe to be a more accurate and detailed representation of the Cyber Kill Chain from Reconnaissance to Exfiltration and beyond. Insikt Group notes cover pre- and post- exploitation tactics (Reconnaissance, Initial Access, Impact, and so on) by nature of the fact that they cover finished intelligence or "hearsay" (for example, a threat actor claiming to have access to credentials). Malware Detonation Sandbox results, however, are focused on exploitation tactics (such as Execution, Persistence, or Privilege Escalation) based on dynamic analysis of the malicious samples submitted. Attack Vector results are based on Recorded Future's processing and classification of tactics used in cyberattacks globally, which varied substantially.

Because Insikt Notes ,Malware Detonation Sandbox results, and references to Attack Vectors cover different ranges of tactics ,the three queries together better capture the full lifecycle of what core techniques were used in cyberattacks in.2020

Each column below is populated with the top-referenced MITRE ATT&CK techniques per appearance in Insikt Notes, appearance in our Malware Detonation Sandbox source ,or association with Attack Vector entities in the Recorded Future Platform .The lists in this table are ordered in descending order of reference count.



about
2020 RF Top Techniques

domain
Enterprise ATT&CK v8

Reconnaissance

- Active Scanning
- Gather Victim Host Information
- Gather Victim Identity Information
- Gather Victim Network Information
- Gather Victim Org Information
- Phishing for Information
- Search Closed Sources
- Search Open Technical Databases
- Search Open Websites/Domains
- Search Victim-Owned Websites

Resource Development

- Acquire Infrastructure
- Compromise Accounts
- Compromise Infrastructure
- Develop Capabilities
- Establish Accounts
- Obtain Capabilities

Initial Access

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing
- Replication Through Removable Media
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts

Execution

- Command and Scripting Interpreter
- Exploitation for Client Execution
- Inter-Process Communication
- Native API
- Scheduled Task/Job
- Shared Modules
- Software Deployment Tools
- System Services
- User Execution
- Windows Management Instrumentation

Persistence

- Account Manipulation
- BITS Jobs
- Boot or Logon Autostart Execution
- Boot or Logon Initialization Scripts
- Browser Extensions
- Compromise Client Software Binary
- Create Account
- Create or Modify System Process
- Event Triggered Execution
- External Remote Services
- Hijack Execution Flow
- Implant Container Image
- Office Application Startup
- Pre-OS Boot
- Scheduled Task/Job
- Server Software Component
- Traffic Signaling
- Valid Accounts

Privilege Escalation

- Abuse Elevation Control Mechanism
- Access Token Manipulation
- Boot or Logon Autostart Execution
- Boot or Logon Initialization Scripts
- Create or Modify System Process
- Event Triggered Execution
- Exploitation for Privilege Escalation
- Group Policy Modification
- Hijack Execution Flow
- Process Injection
- Scheduled Task/Job
- Valid Accounts

Defense Evasion

- Abuse Elevation Control Mechanism
- Access Token Manipulation
- BITS Jobs
- Deobfuscate/Decode Files or Information
- Direct Volume Access
- Execution Guardrails
- Exploitation for Defense Evasion
- File and Directory Permissions Modification
- Group Policy Modification
- Hide Artifacts
- Hijack Execution Flow
- Impair Defenses
- Indicator Removal on Host
- Indirect Command Execution
- Masquerading
- Modify Authentication Process
- Modify Cloud Compute Infrastructure
- Modify Registry
- Modify System Image
- Network Boundary Bridging
- Obfuscated Files or Information
- Pre-OS Boot
- Process Injection
- Rogue Domain Controller
- Rootkit
- Signed Binary Proxy Execution
- Signed Script Proxy Execution
- Subvert Trust Controls
- Template Injection
- Traffic Signaling
- Trusted Developer Utilities Proxy Execution
- Unused/Unsupported Cloud Regions
- Use Alternate Authentication Material
- Valid Accounts
- Virtualization/Sandbox Evasion
- Weaken Encryption
- XSL Script Processing

Credential Access

- Brute Force
- Credentials from Password Stores
- Exploitation for Credential Access
- Forced Authentication
- Input Capture
- Man-in-the-Middle
- Modify Authentication Process
- Network Sniffing
- OS Credential Dumping
- Steal Application Access Token
- Steal or Forge Kerberos Tickets
- Steal Web Session Cookie
- Two-Factor Authentication Interception
- Unsecured Credentials

Discovery

- Account Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Scanning
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery
- System Information Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion

Lateral Movement

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking
- Remote Services
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material

Collection

- Archive Collected Data
- Audio Capture
- Automated Collection
- Clipboard Data
- Data from Cloud Storage Object
- Data from Configuration Repository
- Data from Information Repositories
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged
- Email Collection
- Input Capture
- Man in the Browser
- Man-in-the-Middle
- Screen Capture
- Video Capture

Command and Control

- Application Layer Protocol
- Communication Through Removable Media
- Data Encoding
- Data Obfuscation
- Dynamic Resolution
- Encrypted Channel
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy
- Remote Access Software
- Traffic Signaling
- Web Service

Exfiltration

- Automated Exfiltration
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium
- Exfiltration Over Physical Medium
- Exfiltration Over Web Service
- Scheduled Transfer
- Transfer Data to Cloud Account

Impact

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation
- Defacement
- Disk Wipe
- Endpoint Denial of Service
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

Insikt Notes	Malware Detonation Sandbox	Attack Vectors
T1005 — Data from Local System	T1082 — System Information Discovery	T1598 — Phishing
T1078 — Valid Accounts	T1027 — Obfuscated Files and Information	T1498 — Network Denial of Service
T1098 — Account Manipulation	T1055 — Process Injection	T1102 - Web Service (Web Application Exploitation)
T1486 — Data Encrypted for Impact	T1497 — Virtualization /Sandbox Evasion	T1189 — Drive-by Compromise
T1055 — Process Injection	T1036 — Masquerading	T1055 — Process Injection
T1219 — Remote Access Tools	T1571 — Non-Standard Port	T1219 — Remote Access Tools
T1082 — System Information Discovery	T1057 — Process Discovery	T1041 — Exfiltration Over C2 Channel
T1056 — Input Capture	T1083 — File and Directory Discovery	T1098 — Account Manipulation
T1105 — Remote File Copy	T1018 — Remote System Discovery	T1018 — Remote System Discovery
T1027 — Obfuscated Files and Information	T1071 — Standard Application Layer Protocol	T1027 — Obfuscated Files and Information

Table 1: Top 10 MITRE ATT&CK Techniques categorized by query (Source: Recorded Future)

Top Six ATT&CK Technique Analysis

Top ATT&CK Techniques (All Source)	Tactics	Insikt Notes	Malware Detonation Sandbox	Attack Vectors
T1027 — Obfuscated Files and Information	Defense Evasion	X	X	X
T1055 — Process Injection	Defense Evasion, Privilege Escalation	X	X	X
T1098 — Account Manipulation	Persistence	X		X
T1082 — System Information Discovery	Discovery	X	X	
T1018 — Remote System Discovery	Discovery		X	X
T1219 — Remote Access Tools	Command and Control	X		X

Table 2: Overall Top Six ATT&CK Techniques in 2020 (Source: Recorded Future)

We identified six techniques that were observed in two or more sources, and of those, only two techniques were present in all three source groups: T1027 — Obfuscated Files and Information and T1055 — Process Injection. These two techniques, which fall under the Defense Evasion (TA0005) and Privilege Escalation (TA0004) tactics, respectively, have such prolific use among threat actors because they are essential to most successful cyber threat operations, unlike specific techniques such as T1486 — Data Encrypted for Impact, which is only useful to ransomware operators.

The additional techniques, T1098 — Account Manipulation, T1219 — Remote Access Tools, T1082 — System Information Discovery, and T1018 — Remote System Discovery, were present in only two of the three source types. These techniques represent a small fraction of the cyber landscape of 2020, including opportunistic threat actors taking advantage of a remote workforce due to COVID-19 and major expansions of prominent ransomware operators to include exfiltration and extortion.

In line with 2019's results, the top tactic these techniques share is Defense Evasion. Threat actors deploying ransomware, remote access tools (RATs), or infostealers, will all look to evade detection whether that is through obfuscated files that remain undetected by static file detections, or masquerade as legitimate services through process injection techniques.

Insikt Group has compiled relevant examples of each of the six techniques from the past year, including associated malware, threat actors, and associated techniques. Suggestions for mitigations and detections for each malware mentioned are linked in line.

T1027 — Obfuscated Files and Information Tactic: Defense Evasion | Insikt Notes, Malware Detonation Sandbox, and Attack Vectors *In 2019 Report

Obfuscated Files and Information is a catchall term for methods that adversaries can employ to encrypt or otherwise manipulate the structure of a file, such as using a standard cryptographic protocol. The goal of T1027 is to make detection or follow-up research difficult and is inclusive of these subtechniques: T1027.001 — Binary Padding, T1027.002 — Software Packing, T1027.003 — Steganography, T1027.004 — Compile After Delivery, and T1027.005 — Indicator Removal from Tools.

T1027 in Action

- Netwalker ransomware employs multiple layers of obfuscation in an attempt to remain hidden and undetectable to defenders. The attackers deliver a PowerShell loader script that contains a base64-encoded text blob that is converted to a byte array, which gets decrypted using a single-byte XOR algorithm. Inside the resulting byte array is the malicious dynamic-link library (DLL).
- Egregor ransomware uses multiple layers of obfuscation, and a unique password associated with the sample must be provided at runtime in order to fully decrypt the payload.
- Emotet includes a hashbusting technique that adds randomized data to each file, to guarantee every infection has a unique hash to evade hash based detections.

Mitigating T1027

Unless the artifacts left behind by the obfuscation process are uniquely detectable with a signature, the detection of T1027 may be challenging. If detecting the obfuscation itself is not possible, it may be possible to detect the malicious activity — if the method was used to write, read, or modify the file on the file system — that created the obfuscated file. Additionally, obfuscation used in payloads for Initial Access techniques can be detected at the network level. Network intrusion detection systems (IDS) and email gateway filtering are also ways to identify compressed and encrypted attachments and scripts.

Associated Techniques

Insikt Group found these three ATT&CK techniques were the most commonly referenced in the Malware Detonation Sandbox in relation to T1027:

- T1055 — Process Injection
- T1082 — System Information Discovery
- T1497 — Virtualization/Sandbox Evasion

T1055 — Process Injection Tactic: Defense Evasion, Privilege Escalation | Insikt Notes, Malware Detonation Sandbox, and Attack Vectors *In 2019 Report

Process Injection (T1055) is a technique of running custom code within the address space of another process. It is a technique within Defense Evasion, Privilege Escalation, and in some instances, Persistence. The popularity of T1055 can be attributed to the benefits of hiding behind legitimate processes, which includes DLL injection, portable executable injection, ptrace system calls, VDSO hijacking, and others. This technique is critical for a threat actor to pull off a successful cyberattack.

T1055 in Action

- Netwalker ransomware uses reflective DLL loading to inject the ransomware into the explorer.exe process and evade detection.
- Qakbot malware injects itself into either explorer.exe, Iexplorer.exe, or Mobsync.exe.
- A new variant of Trickbot uses process injection to map its core DLL into other processes memory while remaining completely fileless on disk to avoid detection.

Mitigating T1055

Mitigating T1055 is possible using endpoint security solutions and heuristic tools to identify and halt processes exhibiting known patterns of process injection behavior, such as allocating and writing memory in other processes. On Linux systems, limit the use of ptrace system calls to privileged users only. For process injection to occur, the malicious DLL or PE must be present on the system before it can be injected into another process, so mitigations for this technique start at the network and endpoint level. Ensuring up-to-date detection rules and endpoint protection software can help thwart this attack technique.

Associated Techniques

Insikt Group found these three ATT&CK techniques were the most commonly referenced in the Malware Detonation Sandbox in relation to T1055:

- T1082 — System Information Discovery
- T1036 — Masquerading
- T1083 — File and Directory Discovery

T1098 — Account Manipulation
Tactic: Persistence | Insikt Notes, Attack Vectors

Account Manipulation (T1098) is a technique attackers use to modify existing accounts for the purpose of preserving their access to the target system. Subtechniques include: T1098.001 — Additional Cloud Credentials, T1098.002 — Exchange Email Delegate Permissions, T1098.003 — Add Office 365 Global Administrator Role, and T1098.004 — SSH Authorized Keys.

T1098 in Action

- The threat group BeagleBoyz has been reported to use Account Manipulation techniques to maintain access to compromised credentials and manipulate permission levels within the target environment.
- PowerZure, an exploit framework designed to perform reconnaissance and exploitation of the Azure cloud platform, was updated to include credential dumping of key vault secrets and automation accounts, and exfiltration of account keys.
- An unnamed threat actor was discovered manually generating SSH keys using the AWS command line interface (CLI) allowing them persistent remote access to the target cloud environment.

Mitigating T1098

Adversaries using the Account Manipulation technique are often required to have elevated privileges on the target system or domain since a non-privileged user cannot perform typical account manipulation actions. Requiring multi-factor authentication (MFA) on privileged accounts, as well as having dedicated privileged accounts used only for domain administration activities and not used for other daily administration tasks, helps mitigate this technique. Another way to mitigate this technique is using network segmentation to configure access controls to limit administrative access to critical assets such as domain controllers.

Associated Techniques

Insikt Group found these three ATT&CK techniques were the most commonly referenced in the Malware Detonation Sandbox in relation to T1098:

- T1136 — Create Account
- T1114 — Email Collection
- T1078 — Valid Accounts

T1082 — System Information Discovery
Tactic: Discovery | Malware Detonation Sandbox, Attack Vectors *In 2019 Report

Similar to T1063 (Security Software Discovery), System Information Discovery (T1082) is an additional way for an adversary to get detailed information about a computer's operating system and hardware, including versions, patches, hotfixes, service packs, and architectures. This informs adversary decisions and shapes the vectors in which an adversary pursues an attack.

T1082 in Action

- FickerStealer, an Infostealer RAT, collects data including running processes and system information from the infected machine.
- An update to the Apfell Linux and MacOS malware, which was rebranded to Mythic in 2020 with the inclusion of support for Windows environments, included additional capabilities to collect running processes and system information.
- Agent Tesla collects system information such as BIOS data and processor information.

Mitigating T1082

The data set needed to detect T1082 may be noisy, as techniques used by threat actors to perform System Information Discovery are often used by legitimate programs and services as well. However, monitoring command arguments (or native logging in cloud-based systems) that capture system and network information used in conjunction with other techniques can help identify adversary behavior.

Associated Techniques

Insikt Group found these three ATT&CK techniques were the most commonly referenced in the Malware Detonation Sandbox in relation to T1082:

- T1055 — Process Injection
- T1036 — Masquerading
- T1083 — File and Directory Discovery

T1018 — Remote System Discovery
Tactic: Discovery | Malware Detonation Sandbox, Attack Vectors

Remote System Discovery (T1018) is a way adversaries collect information about remote systems accessible from the current system. Adversaries collect IP addresses and host names from local host files, used in conjunction with system tools such as Ping and Net to discover which systems are reachable from the current system. The information collected using T1018 is often used to perform Lateral Movement within the connected network.

T1018 In Action

- Cobalt Strike Beacon includes a net module which provides tools to interrogate and discover targets in a Windows active directory network. This module is built on top of the Windows Network Enumeration API and replicates many of the native net commands.
- A new Trickbot variant includes functionality to gather all trusted domains, and domain controllers on the network as part of its reconnaissance operation.
- Ryuk ransomware operators used BazarLoader to perform mapping of their victims network domain controllers and trust relationships using built-in Windows utilities such as Nltest.

Mitigating T1018

Detecting and mitigating T1018 can be done using network and endpoint protections; however, most actions used by adversaries to enumerate and discover remote systems, such as Ping, Net, WMI, and PowerShell, have legitimate uses. Monitoring these environments and being able to distinguish between typical and malicious actions will be crucial to mitigating this technique. Remote System Discovery is often used before a lateral movement technique, so data used to mitigate T1018 will need to be used in conjunction with other techniques to help identify adversary behavior.

Associated Techniques

Insikt Group found these three ATT&CK techniques were the most commonly referenced in the Malware Detonation Sandbox in relation to T1018:

- T1082 — System Information Discovery
- T1055 — Process Injection
- T1497 — Virtualization/Sandbox Evasion

T1219 — Remote Access Tools
Tactic: Command and Control | Insikt Notes, Attack Vectors

Remote Access Tools (RATs) (T1219), now referred to as Remote Access Software, is a technique attackers use to install malicious software that allows them to establish an interactive command and control (C2) session with a target system. RATs can be legitimate desktop support and remote access software that can be used maliciously such as TeamViewer, or custom remote access software developed by adversaries. Attackers use the RAT to perform tasks related to reconnaissance, credential harvesting, data exfiltration, and lateral movement within the target environment. The versatility of a RAT, as well as the source code for multiple RATs being easily available via open sources, makes these tools appealing to attackers looking to gain remote access to a target system.

T1219 in Action

- The Dark Crystal RAT is a custom RAT used by attackers to perform remote tasks on a target machine. A few examples of the built-in tasks that give attackers full control of the target machine include executing shell commands, controlling the desktop, and stealing cookies and browser credentials.
- An unidentified threat group has been reportedly installing a modified version of the TeamViewer application which hides the graphical user interface so the attackers can interact with the infected machine without the user knowing.
- TA505 threat actors have been deploying the SDBbot RAT to enable their reconnaissance, data exfiltration, and lateral movement.

Mitigating T1219

Mitigating T1219 requires network and endpoint protections to prevent remote access software from executing and communicating over the network. Implement application installation controls to prevent the installation and execution of unapproved RATs. Restrict outgoing network traffic using filtering and signature-based detections to sites and services used by unauthorized RATs.

Associated Techniques

Insikt Group found these three ATT&CK techniques were the most commonly referenced in the Malware Detonation Sandbox in relation to T1219:

- T1082 — System Information Discovery
- T1219 — Remote Access Software
- T1055 — Process Injection

Additional ATT&CK Technique Analysis and Detections

Insikt Group identified 16 additional MITRE ATT&CK techniques (Table 3) that were widely used by threat actors in 2020. While they were identified within one of the three queries' "Top 10" list, they were not present in more than one of the queries and therefore not detailed in the "Top Techniques Analysis" section above.

Some of these are referenced in the "Associated Techniques" subsections, including three techniques mentioned more than once: T1497 — Virtualization /Sandbox Evasion, T1083 — File and Directory Discovery, and T1036 — Masquerading. These techniques, categorized under Defense Evasion and Discovery tactics, derive their references from the Malware Sandbox query.

Detection of these techniques can be difficult as all three incorporate some attempt to hide their true intentions or blend in with normal activities. As mentioned in the MITRE ATT&CK glossary, data should not be viewed in isolation, but rather has a pattern of activity that highlights tactics like Defense Evasion or Persistence. By correlating these techniques with additional high-fidelity events, defenders can find better indications of suspicious activity.

Additional ATT&CK Techniques	Tactics	Insikt Notes	Malware Sandbox	Attack Vectors
T1189 — Drive-by Compromise	Initial Access			X
T1598 — Phishing	Initial Access			X
T1078 — Valid Accounts	Defense Evasion, Persistence, Privilege Escalation, Initial Access	X		
T1497 — Virtualization /Sandbox Evasion	Defense Evasion, Discovery		X	
T1036 — Masquerading	Defense Evasion		X	
T1057 — Process Discovery	Discovery		X	
T1083 — File and Directory Discovery	Discovery		X	
T1056 — Input Capture	Collection, Credential Access	X		
T1005 — Data from Local System	Collection	X		
T1105 — Remote File Copy	Command And Control, Lateral Movement	X		
T1102 - Web Service (Web Application Exploitation)	Command And Control, Defense Evasion			X
T1071 — Standard Application Layer Protocol	Command and Control		X	
T1571 — Non-Standard Port	Command and Control		X	
T1041 — Exfiltration Over C2 Channel	Exfiltration			X
T1486 — Data Encrypted for Impact	Impact	X		
T1498 — Network Denial of Service	Impact			X

Table 3: Remaining MITRE ATT&CK Techniques as displayed in Methodology (Source: Recorded Future)

T1497 — Virtualization/Sandbox Evasion is not a new technique, but its use grew last year, manifesting in malware variants like Pysa Ransomware or BABAX Stealer. Detection of T1497 — Virtualization /Sandbox Evasion techniques can be performed with the YARA rule Antidebug_antivm from The Yara Rules Project. This Yara rule detects only a subset of Virtualization/Sandbox Evasion tactic and should be considered a starting point or used in conjunction with other detection techniques or tools.

Detection of both techniques T1083 — File and Directory Discovery and T1036 — Masquerading can be done by monitoring for suspicious activity in your monitoring tools. For T1083 — File and Directory Discovery, there are certain commands typically executed when a threat actor is actively enumerating a network. JPCERT has outlined some of the more common commands abused by adversaries. The commands most relevant to file discovery and enumeration are "dir", "type", "net view" and "net use".

Detections of the commands such as "dir", "type", "net view", and "net use" alone are not enough to alert you of malicious activity, as they are also used by system administrators. However, the execution of those commands combined with the activity of downloading a file from a remote drive within 30 minutes of each other, for example, would be better indicative of malicious activity. In addition to this, a threat actor will likely use multiple Discovery tactics including T1082 — System Information Discovery and T1018 — Remote System Discovery, as we observed in the "Associated Techniques" category.

Similar to T1083 — File and Directory Discovery, detection for T1036 — Masquerading relies on identifying improper use of legitimate applications and tools. The Sunburst malware is a good example of masquerading malware as the code is executed under SolarWinds processes and the code also uses the SolarWinds Orion Improvement Program (OIP) for its C2 communication. Detection of this activity requires understanding the normal behavior of such tools and then identifying anomalies. While the Sunburst malware uses sophisticated techniques for masquerading, detection could still be possible by monitoring outbound connections, or monitoring for activity from SolarWinds processes, users, or hosts indicative of credential harvesting or privilege escalation.

Outlook

The ATT&CK framework is designed to map the lifecycle of a cyberattack to a set of TTPs acknowledged by the cybersecurity community. Defenders can map cyberattacks to this framework to prioritize which techniques to defend against. As network and endpoint defense technologies adapt to the most novel threats, attackers will continue focusing on creating innovative ways to evade detections put in place by defenders. The constant struggle between attackers and defenders is why Defense Evasion remains the most prevalent tactic each year.

While defenders should prioritize tooling and detections to identify attackers during the Initial Access phase to stop the attack before it infects the victim, that is not always possible or easy to do. Defenders should also prioritize the 37 techniques encapsulated by the Defense Evasion tactic, specifically the ones outlined in this report that were most common in 2020. One challenge defender's face when building detections for a particular Defense Evasion technique such as T1140 — Deobfuscate/Decode Files or Information is the wide variety of implementations attackers use. In these cases, it is more important to focus on the underlying detectable artifacts and behavior hidden underneath the specific technique than the technique itself.

In line with last year's findings, the second most common tactic after Defense Evasion was Discovery in 2020. The extensive use of the Discovery tactic highlights the common goal among almost all attackers to discover and steal sensitive information. This includes ransomware operators such as those behind Netwalker discovering and exfiltrating data for extortion purposes, info stealers such as FickerStealer looking for Bitcoin wallets, and RATs such as SDBbot running network scans for future lateral movement. Many of the techniques used by threat actors to perform Discovery have legitimate uses, as described above, so defenders should focus on building detections to identify improper use of these legitimate applications and tools.

Identifying techniques encapsulated by the Defense Evasion and Discovery tactics often gives the defender the opportunity to detect an attack during an active operation, which is crucial to mitigating damages. Although these two tactics should be prioritized by defenders, it is still important to build detections for the other 12 tactics. Every time an attacker uses another technique in the ATT&CK matrix, a new opportunity is presented to the defender to detect the malicious activity. Using the mitigations, as prescribed in each section, publicly available ATT&CK-mapped detection mechanisms, and Insikt Group Hunting Packages, defenders can stay up to date with defenses against the latest TTPs.

About Recorded Future

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by hundreds of businesses and government organizations around the world.