

Using MITRE ATT&CK™ in Threat Hunting and Detection

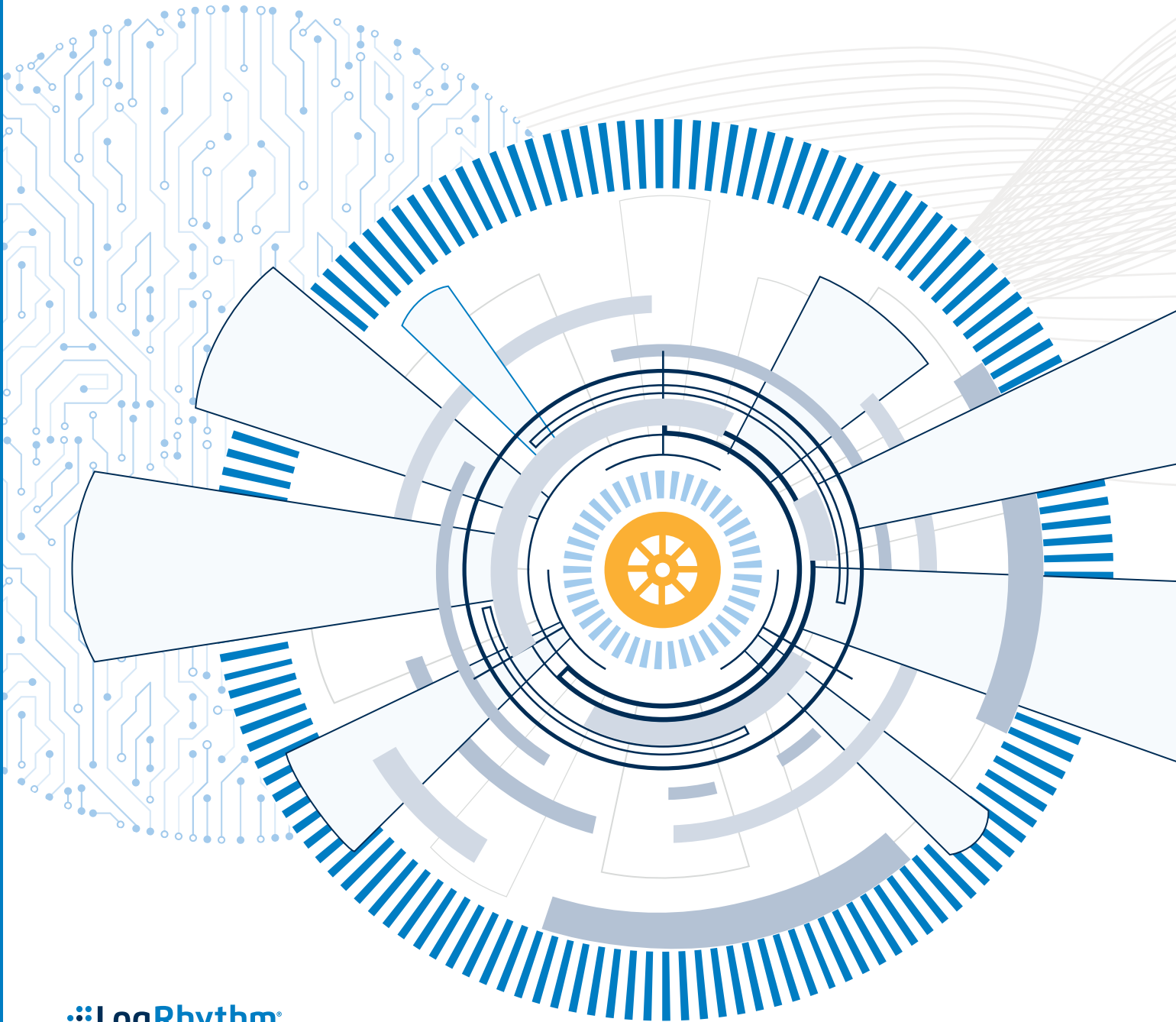


TABLE OF CONTENTS

- Executive Summary 3**
- Understanding MITRE ATT&CK 4
- Using MITRE ATT&CK 4
- Threat Detection and Hunting with Five Common Techniques 4

- Understanding MITRE ATT&CK™ 5**
- Tactics 5
- Techniques 7
- Examples 8
- Mitigation 8
- Detection 9
- ATT&CK Stays Up to Date 9

- Using ATT&CK™ 10**
- Assess 10
- Enhance 10
- Test 11
- Resources 11

- Threat Detection and Hunting with Five Common Techniques 12**
- ATT&CK Clients 12
- Masquerading (T1036) 14
- Connection Proxy (T1090) 15
- Exfiltration Over Alternative Protocol (T1048) 16
- Drive-By Compromise (T1189) 17
- Service Execution (T1035) 18

- Conclusion 20**

- About 21**



Executive Summary

MITRE ATT&CK¹ is an open framework and knowledge base of adversary tactics and techniques based on real-world observations. ATT&CK provides a common taxonomy of the tactical objectives of adversaries and their methods. Having a taxonomy by itself has many valuable uses, such as providing a common vocabulary for exchanging information with others in the security community. But it also serves as a real technical framework for classifying your current detection efforts and identifying gaps where you are blind to certain types of attack behaviors.

This paper will introduce you to ATT&CK and related tools and resources based on ATT&CK. Then it will discuss how to make practical use of ATT&CK with a focus on threat hunting and detection.

LogRhythm Labs is a dedicated team within LogRhythm that delivers security research, analytics, and threat intelligence services to protect your security operations center and your organization from damaging cyberthreats. The LogRhythm Labs team continually creates content based in research to help you detect and respond to threats and risks by combining actionable intelligence with advanced analytics.

1. This paper includes portions of the MITRE ATT&CK work. © 2018 The MITRE Corporation. This work is reproduced and distributed with the permission of The MITRE Corporation. Most uses of italics in this document indicate an excerpt from ATT&CK.

Understanding MITRE ATT&CK

In this section, we'll introduce you to ATT&CK's structure, comprising tactics, techniques, examples, mitigation, and detection.

Using MITRE ATT&CK

After a quick overview of the wide range of ATT&CK uses cases, we'll zero in on using ATT&CK to:

- perform a gap analysis of the malicious behavior you are currently monitoring for
- enhance your threat detection and hunting efforts
- test your detection rules to provide assurance that you are alerted as intended

Threat Detection and Hunting with Five Common Techniques

In the closing section, we will look at five specific techniques from ATT&CK that were selected based on prevalence and other criteria that make them especially applicable to threat hunting and detection. We'll explore each one of these techniques in-depth, highlighting how the attackers use them and how you can detect them. We will discuss which logs you need to collect, what audit policy you need to enable, and what you need to look for in those logs. You will see how LogRhythm Labs has built detection logic for these techniques into the LogRhythm NextGen SIEM Platform.



ATT&CK is a normalized, structured approach to classifying and describing the methods adversaries use to attack systems. ATT&CK starts out high level and provides a solid framework of concepts and relationships for understanding attack methods. But ATT&CK goes beyond the theoretical with highly detailed and constantly updated technical information that can be applied in many different use cases. ATT&CK describes each method and provides suggested ways to both mitigate and detect the threat.


Understanding MITRE ATT&CK™

Tactics

The highest level of organization in ATT&CK is Tactics. The strategic goal of an attacker may be to extort ransom, steal information, or simply destroy an organization's IT environment. But attackers must reach a series of incremental, short-term objectives to achieve their ultimate, strategic goal. Most attacks begin with trying to gain Initial Access (TA0001). Then other fundamental tactics, including Execution (TA0002) and Persistence (TA0003), are usually necessary intermediate goals no matter the end goal of the attack. An attacker trying to steal information will need to accomplish Collection (TA0009) and finally

Exfiltration (TA0010). Attackers may engage many other tactics in order to reach their goal, such as hopping from system to system or account to account through Lateral Movement (TA0008) or attempting to hide from your monitoring through Defense Evasion (TA0005).

It's important to understand though that tactics are a classification and description of short-term intent. Tactics describe what the attacker is trying to do at any given phase of the attack – not how they are specifically going about it.

 The table on the following page explains the tactics that currently comprise ATT&CK.

ID	NAME	DESCRIPTION
TA0001	Initial Access	The initial access tactic represents the vectors adversaries use to gain an initial foothold within a network.
TA0002	Execution	The execution tactic represents techniques that result in execution of adversary-controlled code on a local or remote system. This tactic is often used in conjunction with initial access as the means of executing code once access is obtained, and lateral movement to expand access to remote systems on a network.
TA0003	Persistence	Persistence is any access, action, or configuration change to a system that gives an adversary a persistent presence on that system. Adversaries will often need to maintain access to systems through interruptions such as system restarts, loss of credentials, or other failures that would require a remote access tool to restart or alternate backdoor for them to regain access.
TA0004	Privilege Escalation	Privilege escalation is the result of actions that allows an adversary to obtain a higher level of permissions on a system or network. Certain tools or actions require a higher level of privilege to work and are likely necessary at many points throughout an operation. Adversaries can enter a system with unprivileged access and must take advantage of a system weakness to obtain local administrator or SYSTEM/root level privileges. A user account with administrator-like access can also be used. User accounts with permissions to access specific systems or perform specific functions necessary for adversaries to achieve their objective may also be considered an escalation of privilege.
TA0005	Defense Evasion	Defense evasion consists of techniques an adversary may use to evade detection or avoid other defenses. Sometimes these actions are the same as or variations of techniques in other categories that have the added benefit of subverting a particular defense or mitigation. Defense evasion may be considered a set of attributes the adversary applies to all other phases of the operation.
TA0006	Credential Access	Credential access represents techniques resulting in access to or control over system, domain, or service credentials that are used within an enterprise environment. Adversaries will likely attempt to obtain legitimate credentials from users or administrator accounts (local system administrator or domain users with administrator access) to use within the network. This allows the adversary to assume the identity of the account, with all of that account's permissions on the system and network, and makes it harder for defenders to detect the adversary. With sufficient access within a network, an adversary can create accounts for later use within the environment.
TA0007	Discovery	Discovery consists of techniques that allow the adversary to gain knowledge about the system and internal network. When adversaries gain access to a new system, they must orient themselves to what they now have control of and what benefits operating from that system give to their current objective or overall goals during the intrusion. The operating system provides many native tools that aid in this post-compromise information-gathering phase.
TA0008	Lateral Movement	Lateral movement consists of techniques that enable an adversary to access and control remote systems on a network and could, but does not necessarily, include execution of tools on remote systems. The lateral movement techniques could allow an adversary to gather information from a system without needing additional tools, such as a remote access tool.
TA0009	Collection	Collection consists of techniques used to identify and gather information, such as sensitive files, from a target network prior to exfiltration. This category also covers locations on a system or network where the adversary may look for information to exfiltrate.
TA0010	Exfiltration	Exfiltration refers to techniques and attributes that result or aid in the adversary removing files and information from a target network. This category also covers locations on a system or network where the adversary may look for information to exfiltrate.
TA0011	Command and Control	The command and control tactic represents how adversaries communicate with systems under their control within a target network. There are many ways an adversary can establish command and control with various levels of covertness, depending on system configuration and network topology. Due to the wide degree of variation available to the adversary at the network level, only the most common factors were used to describe the differences in command and control. There are still a great many specific techniques within the documented methods, largely due to how easy it is to define new protocols and use existing, legitimate protocols and network services for communication.
TA0040	Impact	The Impact tactic represents techniques whose primary objective directly reduces the availability or integrity of a system, service, or network; including manipulation of data to impact a business or operational process. These techniques may represent an adversary's end goal, or provide cover for a breach of confidentiality.

Table 1. MITRE ATT&CK Tactics

TACTICS

Persistence

**TECHNIQUES**

Registry Run Keys

New Service

Applnit DLLs

Techniques

While tactics specify what the attacker is trying to do, techniques describe the various technical ways attackers have developed to employ a given tactic. For instance, attackers usually want to maintain their presence in your network over reboots or logon sessions. This is *Tactic TA0003: Persistence*. But you can achieve persistence many different ways. For instance, on Windows systems, you can leverage certain keys in the registry whose values are executed as system commands in connection with predictable events, such as system start or logon (which is the *T1060 - Registry Run Keys/Startup Folder* technique). Or you can simply install your malicious program as a system service using technique *T1050: New Service*. Another technique is *T1103: Applnit DLLs*, which is a way of getting every process that loads user32.dll to also load your malicious DLL. There are many more techniques, and others will be developed in the future, but they all revolve around giving the attacker persistent access to the victim's system or network. Hence, they are all grouped under the same tactic.

While tactics specify what the attacker is trying to do, techniques describe the various technical ways attackers have developed to employ a given tactic.

Some techniques help facilitate more than one tactic, and this is reflected in ATT&CK. For instance, *T1050: New Service* is listed under two tactics – Persistence and Privilege Escalation.

For each technique, ATT&CK lists the applicable platforms (e.g., Windows, Linux), the permissions prerequisite to exploiting the technique, sources of data for detecting the technique (e.g., logs) and a cross-reference to any related attack patterns in CAPEC, which is a related catalog of common attack patterns focused on application security.

Examples

For each technique, ATT&CK provides examples of known cases where the technique is:

- used by a group (group is an ATT&CK-specific term described later in this section) in one or more attacks
- implemented by software (software is an ATT&CK-specific term described later in this section)

For each example, documentary references are provided. These are often blog posts or threat alerts from various security analyst teams across the cybersecurity community. The value of these examples go beyond justifying the technique's inclusion in ATT&CK. For instance, cybersecurity professionals can use them to learn how attackers operate and how they combine various techniques and tactics in a larger campaign.

Mitigation

For each technique, ATT&CK makes an effort to specify any preventive controls that can be brought to bear by defenders. Such mitigations aren't practical for some techniques, and ATT&CK faithfully points this out. For instance, on *T1055: Process Injection*, the mitigation section in ATT&CK points out:

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of operating system design features. For example, mitigating specific Windows API calls will likely have unintended side effects, such as preventing legitimate software (i.e., security products) from operating properly. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identification of subsequent malicious behavior.²

² MITRE ATT&CK Process Injection, MITRE ATT&CK, 2018

MITRE defines “groups” as sets of related intrusion activity that are tracked by a common name in the security community.

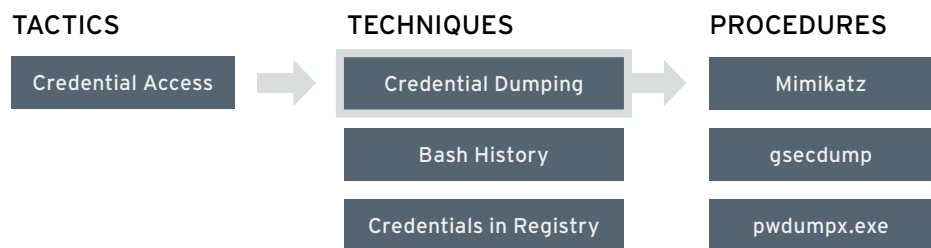
Groups, MITRE ATT&CK
<https://attack.mitre.org/groups/>

MITRE defines “software” as a generic term for custom or commercial code, operating system utilities, open-source software, or other tools used to conduct behavior modeled in ATT&CK.

Software, MITRE ATT&CK
<https://attack.mitre.org/software/>

Detection

Preventing attackers from using techniques is critical. Implementing detective controls is also important because 1) defense-in-depth requires layered defenses against any given threat (all eggs in one basket), and 2) as mentioned earlier, you can't prevent all techniques. Therefore, ATT&CK provides extensive guidance on how to detect the use of techniques by attackers with logs and other sources of security analytics at your disposal.



ATT&CK Stays Up to Date

Attackers and defenders constantly respond to each other, which means, on either side, what works today might not tomorrow. MITRE works with the community to keep ATT&CK up to date with the ever-changing threatscape. As just one example, an entirely new tactic, Impact, was recently added to ATT&CK. This tactic was timely, given the dramatic rise in destructive attacks – the most well-known being Not Petya. *TA0040: Impact* comprises 14 different techniques whose primary objective directly reduces the availability or integrity of a system, service, or network; including manipulation of data to impact a business or operational process.³

3. [MITRE ATT&CK Impact](#), MITRE ATT&CK, 2018



Using ATT&CK™

ATT&CK is a versatile tool and can be used by all roles within the cybersecurity community. ATT&CK can make red teams more effective and ensure they are more closely emulating the methods of an actual adversary. ATT&CK provides blue teams a concise, comprehensive way to understand attackers and to assess their current controls and defense efforts to identify gaps. ATT&CK also delivers a standardized way to compare the threat coverage of vendor products.

But for the purposes of this paper, we will focus on the detective use cases for ATT&CK with a particular emphasis on SIEM technology.

Assess

There are so many threats. No organization is always up to date with detective controls for every adversary technique across their entire network. It's a matter of constant prioritization. But where do you begin? Which tactics are we weakest on monitoring? And which ones are the biggest risk for your environment? Which techniques can be detected using the

information and tools we have right now and perhaps should be given attention first? Which techniques lack practical preventive controls and therefore become more critical for detection? ATT&CK provides a structured and current method for answering these questions.

Enhance

When you identify tactics or techniques where your organization needs better detection, ATT&CK provides the technical details to help you build automated monitoring rules or the basis for conducting threat hunts.

How do you prioritize threats to your organization? What can you address with the tools you have now? ATT&CK provides a structured and current method for answering these questions.

Test

No technology or control should be assumed to be effective. If at all possible, all controls should be tested with using the most realistic activity possible. By mapping your detective controls to ATT&CK Techniques, you can then try performing those techniques in your environment to see if your SIEM and related security technologies detect the activity, alert and respond as desired.

In particular, Red Canary's Atomic Red Team is a valuable tool for testing your detective controls with ATT&CK as the basis.

Red Canary maintains **Atomic Red Team**. It is described as "a library of simple tests that every security team can execute to test their defenses. Tests are focused, have few dependencies, and are defined in a structured format that can be used by automation frameworks." Atomic Red Team provides an automated, scriptable way to test your SIEM's ability to detect many of ATT&CK's techniques. In the threat hunting scenarios below, we will feature applicable Atomic Red Teams tests.

RESOURCES

MITRE and others in the cybersecurity community have built a variety of tools for leveraging ATT&CK. The ATT&CK knowledge base itself is accessible via:

- **MITRE ATT&CK website:**
<https://attack.mitre.org>
- **ATT&CK Navigator web application:**
<https://mitre-attack.github.io/attack-navigator/enterprise/>
This app allows you to navigate ATT&CK content in a more dynamic, powerful way than is possible with the more static attack.mitre.org website. The GitHub repository for ATT&CK Navigator explains, "The principal feature of the Navigator is the ability for users to define layers – custom views of the ATT&CK knowledge base – e.g., showing just those techniques for a particular platform or highlighting techniques a specific adversary has been known to use. Layers can be created interactively within the Navigator or generated programmatically and then visualized via the Navigator."
- **Programmatically accessible formats of ATT&CK for automation:**
 - TAXII Server: Trusted Automated Exchange of Intelligence Information (TAXII™) is an application layer protocol for the communication of cyberthreat information in a simple and scalable manner.
 - STIX: Structured Threat Information Expression (STIX™) is a language and serialization format used to exchange cyberthreat intelligence (CTI). You can find ATT&CK expressed in STIX 2.0 format at <https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterprise-attack.json>.

Threat Detection and Hunting with Five Common Techniques

ATT&CK Clients

The community has created tools for querying ATT&CK using TAXII and STIX, such as:

- **PoSh_ATTCK:** <https://github.com/SadProcessor/SomeStuff>
- **ATTACK-Python-Client:** <https://github.com/Cyb3rWardOg/ATTACK-Python-Client>
- **DIY (Python with Python-Stix2 library):** <https://github.com/mitre/cti/blob/master/USAGE.md>

In the preceding sections, we discussed the structure of ATT&CK and some of its tools and resources. In this section, we will focus on how to make practical use of ATT&CK for threat hunting and threat detection.

The techniques we will focus on are *T1036: Masquerading*, *T1090: Connection Proxy*, *T1048: Exfiltration Over Alternative Protocol*, *T1189: Drive-By Compromise*, and *T1035: Service Execution*.

We selected these five ATT&CK techniques because:

- of their prevalence in attacks
- threat detection is particularly applicable to these techniques
- many organizations are already collecting the logs and information that match the data sources necessary to detect these techniques

The **LogRhythm MITRE ATT&CK Module** provides prebuilt content mapped to ATT&CK for your LogRhythm NextGen SIEM Platform, including analytics, dashboard views, and threat hunting tools. This content enables you to detect adversaries and improve your security program as prescribed by the MITRE ATT&CK framework.

ATT&CK delivers actionable intelligence based on known adversary behavior modeled from specific threat observation. The LogRhythm MITRE ATT&CK Module applies this methodology to deliver immediate insight so your team can respond effectively and address gaps in your security visibility, operations, and infrastructure. Like all LogRhythm Labs-created modules, the MITRE ATT&CK Module is free for customers.

IN THIS SECTION, WE WILL

- explore each one of these techniques in-depth, highlighting how the attackers use them and how you can detect them.
- identify which logs you need to collect and what you need to look for in those logs.
- point out relevant tests from Atomic Red Team that you can use to test your detection logic. You will also see how LogRhythm Labs has built detection logic for these techniques into the LogRhythm SIEM. Some of these detection rules depend on Microsoft Sysmon.

```
PS /> $ATTCK.Technique|where {$_.DataSource -eq 'Process command-line parameters'}|select ID, Name, Tactic, DataSource
```

ID	Name	Tactic	DataSource
T1156	.bash_profile and .bashrc	{persistence}	{File monitoring, Pro
T1134	Access Token Manipulation	{defense-evasion, privilege-escalation}	{API monitoring, Acco
T1087	Account Discovery	{discovery}	{API monitoring, Pro
T1155	AppleScript	{execution, lateral-movement}	{API monitoring, Sys
T1138	Application Shimming	{persistence, privilege-escalation}	{Loaded DLLs, System
T1010	Application Window Discovery	{discovery}	{API monitoring, Pro
T1119	Automated Collection	{collection}	{File monitoring, Da
T1139	Bash History	{credential-access}	{File monitoring, Pro
T1217	Browser Bookmark Discovery	{discovery}	{API monitoring, Fil
T1088	Bypass User Account Control	{defense-evasion, privilege-escalation}	{System calls, Proce
T1191	CMSTP	{defense-evasion, execution}	{Process monitoring,
T1042	Change Default File Association	{persistence}	{Windows Registry, P
T1059	Command-Line Interface	{execution}	{Process monitoring,
T1500	Compile After Delivery	{defense-evasion}	{Process command-lin
T1223	Compiled HTML File	{defense-evasion, execution}	{File monitoring, Pro

Figure 1: PoSh_ATTCK query for ATT&CK techniques requiring Command Line parameters

Masquerading (T1036)

Adversaries use Masquerading as a Defense Evasion: TA0005 tactic. ATT&CK states, “Defense evasion consists of techniques an adversary may use to evade detection or avoid other defenses. Sometimes these actions are the same as or variations of techniques in other categories that have the added benefit of subverting a particular defense or mitigation. Defense evasion may be considered a set of attributes the adversary applies to all other phases of the operation.”

Despite increasing efforts to “live off the land,” attackers still use malicious executables, and they know it’s important to hide them. Hiding applies not just to where they are stored on the file system but also how they appear in logs and process queries. ATT&CK describes masquerading as “when the name or location of an executable, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. Several different variations of this technique have been observed.”⁴

ATT&CK describes several variations of masquerading, but [Masquerading as Windows LSASS process](#) is a great example where cmd.exe is copied to c:\windows\system32\temp and

renamed to lsass.exe. It’s then used to run arbitrary commands and executables, but in logs and process queries, it will look like the trusted processes Local Security Authority System Service showing up in logs as c:\windows\system32\temp\lsass.exe which is very close to c:\Windows\System32\lsass.exe.

LogRhythm Labs implemented a rule to detect this variation of masquerading in Windows. First, you must generate a list of hashes of all the executables in the system root using a PowerShell script:

```
get-childitem c:\windows\system32
-recurse|where {$_.extension -eq
'.exe'}|Get-FileHash -Algorithm md5|select
hash|Out-File '.\hashes.txt'
```

That file is imported as list in LogRhythm. Then an AI Engine Rule looks for [Microsoft Sysmon Event ID 1 - Process Creation](#) where the executable’s hash is on the list but resides outside the system root. The hash list needs to be updated as Windows executables are patched.

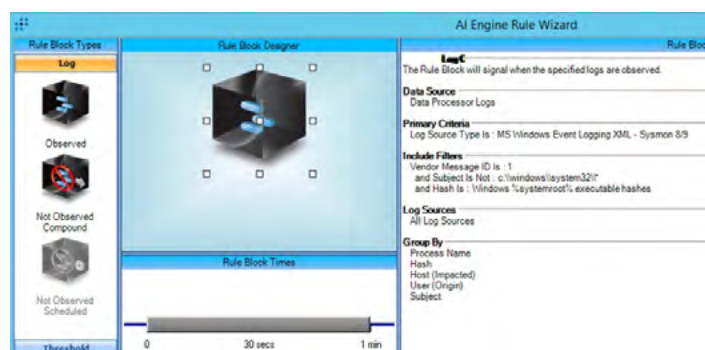


Figure 2: AI Engine looks for Microsoft Sysmon Event ID 1: Process Creation

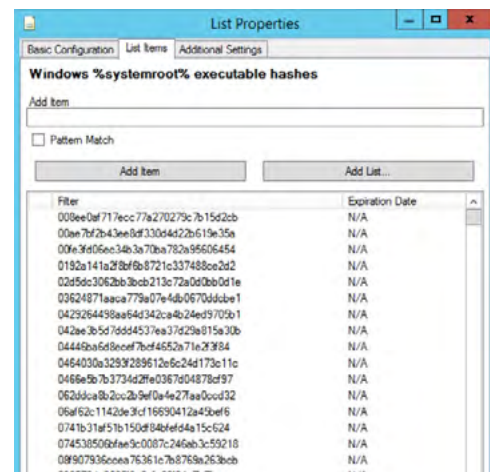


Figure 3: Importing the list in LogRhythm

4. MITRE ATT&CK Masquerading, MITRE ATT&CK, 2018

Connection Proxy (T1090)

The next technique is used by attackers to facilitate the Command and Control Tactic (*TA0011*), which represents how adversaries communicate with systems under their control within a target network. There are many ways an adversary can establish command and control with various levels of covertness, depending on system configuration and network topology. Due to the wide degree of variation available to the adversary at the network level, only the most common factors were used to describe the differences in command and control. There are still a great many specific techniques within the documented methods, largely due to how easy it is to define new protocols and use existing, legitimate protocols and network services for communication.⁵

Connection Proxy “is used to direct network traffic between systems or act as an intermediary for network communications. Many tools exist that enable traffic redirection through proxies or port redirection, including HTRAN, ZXProxy, and ZXPortMap.”

To detect Connection Proxy, ATT&CK recommends “processes utilizing the network that do not normally have network communication or have never been seen before are suspicious.” Network activities disassociated from user-driven actions from processes that normally require user direction are suspicious.⁶

Analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server or between clients that should not or often do not communicate with one another). Processes utilizing

the network that do not normally have network communication or have never been seen before are suspicious. Analyze packet contents to detect communications that do not follow the expected protocol behavior for the port that is being used.⁷

LogRhythm Labs developed a rule that looks for connection proxy tools like HTRAN based on the network connections they open as recorded by [Microsoft Sysmon Event ID 3 – Network Connection](#). It tests for the same process receiving a network connection internally and then initiating an outbound connection. Note that this rule depends on the entity structure being set up accurately so that the SIEM knows the directionality of the traffic.

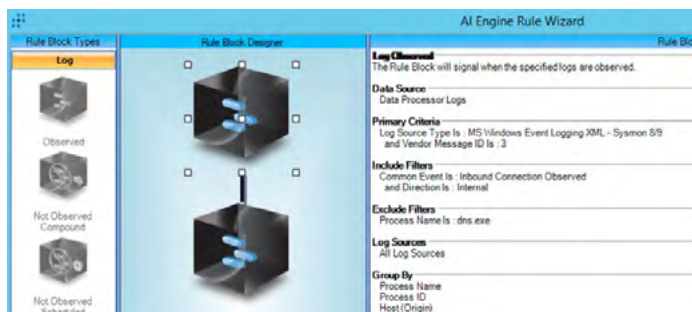


Figure 4: AI Engine rule looks for connection proxy tools (e.g., HTRAN)

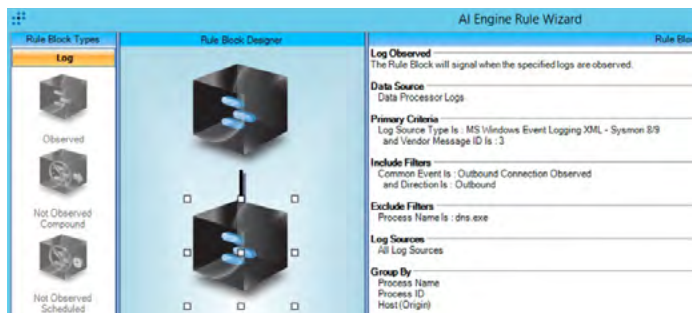


Figure 5: Rule Block 2 of the AI Engine rule to detect the Connection Proxy technique

5. MITRE ATT&CK Command & Control, MITRE ATT&CK, 2018 6. MITRE ATT&CK Connection Proxy, MITRE ATT&CK, 2018 7. MITRE ATT&CK Command & Control, MITRE ATT&CK, 2018

Exfiltration Over Alternative Protocol (T1048)

Once an attacker obtains the desired information, the attacker must get that data out of the victim’s network without being noticed. This is part of the Exfiltration Tactic (*TA0010*) and a common Technique is Exfiltration Over Alternative Protocol where the “exfiltration is performed with a different protocol from the main command and control protocol or channel. The data is likely to be sent to an alternate network location from the main command and control server. Alternate protocols include FTP, SMTP, HTTP/S, DNS, or some other network protocol. Different channels could include Internet Web services such as cloud storage.”⁸

To detect, ATT&CK suggests you “analyze network data for uncommon data flows (e.g., a client sending significantly more data than it receives from a server).” Atomic Red Team provides several tests for this Technique including [Exfiltration Over Alternative Protocol – SSH](#), which attempts to send a large tarball to a specified domain name.

LogRhythm Labs built detection for this technique using a trend rule to first learn by observing data from LogRhythm NetMon which network applications (http, ftp, smtp, etc.) typically receive more traffic than they send. Then the rule triggers if these applications are sending more traffic than they receive.

```

The rule block will signal when the overall result of the criteria expressions is true.

Data Source
Data Processor Logs

Primary Criteria
Log Source Type Is : Syslog - LogRhythm Network Monitor

Include Filters
Host (Impacted) KBytes Sent Is Not = 0.0000 KB
and Host (Impacted) KBytes Rcvd Is Not = 0.0000 KB
and Direction Is : Outbound
and Common Event Is : End Of Flow

Exclude Filters
Application Is : unknown
UB_UNKNOWN
Unknown Port
Unknown TCP Port
Unknown UDP Port

Log Sources
All Log Sources

Group By
Application

Data Fields
Host (Impacted) KBytes Rcvd
Host (Impacted) KBytes Sent

Time and Schedule
Live Time Period: 0 Day(s) 00:01 hour(s), minute(s)
Baseline Time Period: 7 Day(s) 00:00 hour(s), minute(s)
Evaluation Frequency: Auto
Evaluation Schedule: Always active

Expressions
1. Rate(live:Host (Impacted) KBytes Rcvd) > Rate(live:Host (Impacted) KBytes Sent) [Basis: Minute]
2. Rate(baseline:Host (Impacted) KBytes Rcvd) > Rate(baseline:Host (Impacted) KBytes Sent) [Basis: Minute]
    
```

Figure 6: AI Engine detection rule for Exfiltration over Alternative Protocol technique

1	Application	Host (Impacted) KBytes Rcvd	Host (Impacted) KBytes Sent	Outbound percent of Inbound
188	stickyards	3.651367188	9.385742188	39%
189	stun	122.6367188	112.5019531	109%
190	symantec	2.853515625	6.615234375	43%
191	t_mobile_app	4.754882813	306.4355469	2%
192	taboola	30.06835938	13.54296875	222%
193	tcp	539.9072266	3697.595703	15%
194	teads	6.299804688	21.07910156	30%
195	teamviewer	1.93359375	2.16796875	89%
196	telegram	2.594726563	2.05859375	126%
197	tidaltv	13.5	6.525390625	207%
198	truste	18.41210938	81.93261719	22%

Figure 7: Analysis of outbound vs inbound traffic volume for network applications

8. MITRE ATT&CK Exfiltration Over Alternative Protocol, MITRE ATT&CK, 2018

Drive-By Compromise (T1189)

Before an attacker can do anything – establish persistence, move laterally, or steal information – they must gain Initial Access (TA0001). This tactic represents the vectors adversaries use to gain an initial foothold within a network. There are many such vectors. One technique is “Drive-By Compromise,” which is “when an adversary gains access to a system through a user visiting a website over the normal course of browsing. With this technique, the user’s web browser is targeted for exploitation.”⁹

ATT&CK’s detection guidance for this technique admits, “detecting compromise based on the drive-by exploit from a legitimate website may be difficult. Also look for behavior on the endpoint system that might indicate successful compromise, such as abnormal behavior of browser processes. This could include suspicious files written to disk, evidence of Process Injection for attempts to hide execution, evidence of Discovery, or other unusual network traffic that may indicate additional tools transferred to the system.”¹⁰

In this case, LogRhythm Labs built a rule to help provide context around a drive-by compromise once the malware has already been detected. The rule relies on detection of malware (via IDS or AV logs) and then attempts to correlate to a browser process saving a file to %temp%.

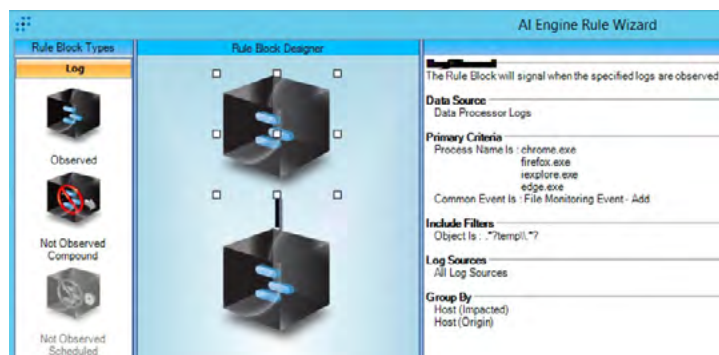


Figure 8: Rule Block 1 of the AI Engine detection rule for the Drive by Compromise attack technique

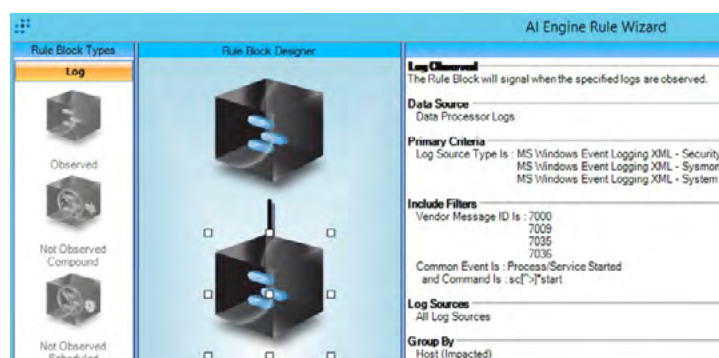


Figure 9: Rule Block 2 of AI Engine detection rule for the Drive by Compromise attack technique

9. MITRE ATT&CK Drive-by Compromise, MITRE ATT&CK, 2018 10. IBID

Service Execution (T1035)

Early on in most attacks, adversaries need to accomplish Execution (TA0002). This tactic is a group techniques that result in execution of adversary-controlled code on a local or remote system. This tactic is often used in conjunction with initial access as the means of executing code once access is obtained, and lateral movement to expand access to remote systems on a network.

“Service execution” is a common technique in which the attacker uses Windows Service Control Manager as a way to execute their code. “Adversaries may execute a binary, command, or script via a method that interacts with Windows services, such as the Service Control Manager. This can be done by either creating a new service or modifying an existing service. This technique is the execution used in conjunction with New Service and Modify Existing Service during service persistence or privilege escalation.”¹¹

For detection, ATT&CK suggests changes to service Registry entries and command-line invocation of tools capable of modifying services that do not correlate with known software, patch cycles, etc., may be suspicious. If a service is used only to execute a binary or script and not to persist, then it will likely be changed back to its original form shortly after the service is restarted so the service is not left broken, as is the case with the common administrator tool PsExec.¹²

Atomic Red Team includes a test for this technique: [Execute a Command as a Service](#).

This technique can be detected by enabling registry auditing of changes to the keys where services are defined (SYSTEM\CurrentControlSet\Services) and then monitoring for [Event ID 4657](#) (registry value modified) and especially where the affected value’s name is ImagePath. This event identifies

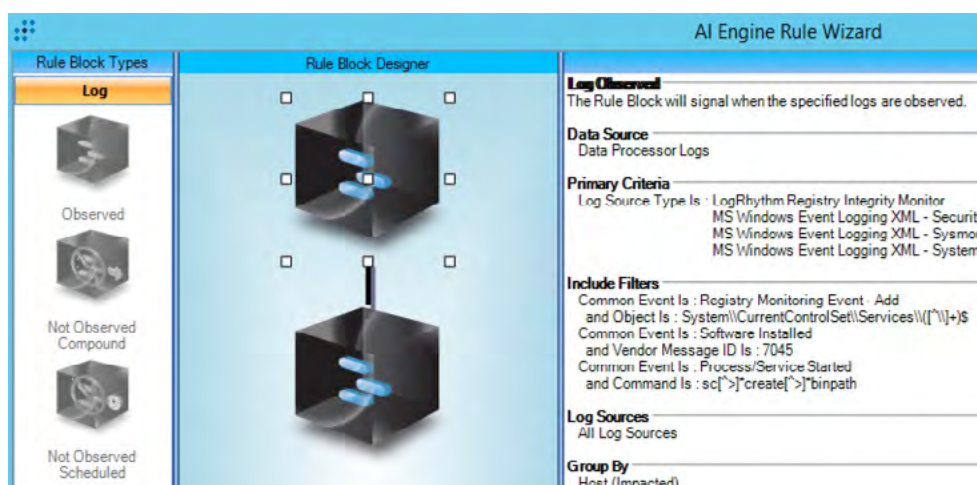


Figure 10: Rule Block 1 of the AI Engine rule to detect the Service Execution technique

11. [MITRE ATT&CK Service Execution](#), MITRE ATT&CK, 2018 12. [MITRE ATT&CK Execution](#), MITRE ATT&CK, 2018

the root activity of creating a new service or modifying an existing service, regardless of the method used.

Other events that log when a service creation and service start are potentially useful as well if compared against a whitelist of known services. For instance, monitoring [Security Log Event ID 4697](#) indicates a new service has been created. You could also monitor process start events (4688) where the command line is similar to “sc start” or “sc create,” which indicates the sc command was used to create or start a service. However, these latter events are not

comprehensive compared to Event ID 4657, because attackers could bypass “sc” such as by directly modifying the ImagePath registry value of an existing service or calling the Win32Api StartService.

LogRhythm Labs built a ruleset for detecting Service Execution. This rule takes advantage of complex include filters to encompass criteria for different log source types. We are detecting service installation through registry modification, through command-line invocation of a service and through Windows Events showing the installation of software via event id 7045.

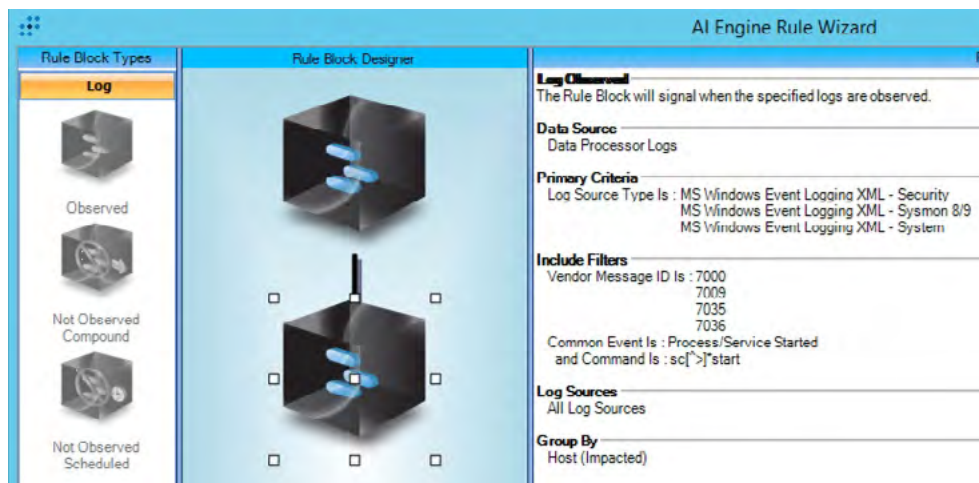


Figure 11: Rule Block 2 of the AI Engine rule to detect the Service Execution technique



CONCLUSION

MITRE ATT&CK is a powerful way to classify and study adversary techniques and understand their intent.

ATT&CK can be used many different ways to improve cybersecurity efforts. This paper has focused on how you can use ATT&CK to enhance, analyze, and test your threat detection efforts.

The LogRhythm Labs team is dedicated to building ATT&CK into the LogRhythm NextGen SIEM Platform to ensure comprehensive, up-to-date, and verifiable threat detection.

⚙️ About the Authors



Randy Franklin Smith

Randy Franklin Smith is an internationally recognized expert on the security and control of Windows and AD security. Randy publishes www.UltimateWindowsSecurity.com and wrote *The Windows Server 2008 Security Log Revealed* – the only book devoted to the Windows Security Log. Randy is the creator of LOGbinder software, which makes cryptic application logs understandable and available to log management and SIEM solutions. As a Certified Information Systems Auditor, Randy performs security reviews for clients ranging from small, privately held firms to Fortune 500 companies, national, and international organizations. Randy is also a Microsoft Security Most Valuable Professional.



Brian Coulson

As Threat Research Senior Engineer for LogRhythm Labs, Brian Coulson works to keep abreast of current cyberthreats and news, develop threat detection and response content, and demonstrate how the LogRhythm NextGen SIEM Platform detects and responds to threats. In this role, he engages with the LogRhythm Community and offers advice and solutions to remediate security-related issues. Prior to LogRhythm, Brian was a lead information security engineer for a LogRhythm customer.



Dan Kaiser

As a Threat Research Engineer for LogRhythm Labs, Dan Kaiser develops content for the security-focused modules in the LogRhythm Knowledge Base, such as UEBA, NDR, and CIS Controls. Before LogRhythm, Dan worked as a network engineering manager for an oil and gas company and as an IT director at a law firm. He also worked as an engineer at a Citrix Metaframe-based application service provider.



About LogRhythm

LogRhythm is a world leader in NextGen SIEM, empowering thousands of enterprises on six continents to successfully reduce cyber and operational risk by rapidly detecting, responding to and neutralizing damaging cyberthreats.

The LogRhythm NextGen SIEM Platform combines advanced security analytics; user and entity behavior analytics (UEBA); network detection and response (NDR); and security orchestration, automation, and response (SOAR) in a single end-to-end solution. LogRhythm's technology serves as the foundation for the world's most modern enterprise security operations centers (SOCs), helping customers measurably secure their cloud, physical, and virtual infrastructures for both IT and OT environments.

Built for security professionals by security professionals, the LogRhythm NextGen SIEM Platform has won countless customer and industry accolades. For more information, visit logrhythm.com.

