基于 ATT&CK 框架的红蓝对抗 有效提升检测能力

目前，ATT&CK 框架已成为安全圈新宠，相信大家对于 ATT&CK 框架都有一定的了解。但是，对于该如何使用该框架、如何实现其价值，我们或许心存疑惑。本文将主要介绍如何基于 ATT&CK 框架来制定分析方案，检测攻击行为，有效提升检测能力；制定对抗模拟方案，提高企业防御能力。

想要对攻击者渗透后的入侵行为进行分析，首先让我们来了解一下攻击者是如何进行攻击的。

一个真实的攻击场景

攻击者首先是对其最近感兴趣的一个事件发送了一个钓鱼邮件。攻击载荷（payload）是一个 .zip 文件，其中包含了一个诱饵 PDF 文件和一个恶意可执行文件，该恶意文件使用系统上已经安装的 Acrobat Reader 来进行伪装。

运行时，可执行文件将下载第二阶段使用的远程访问工具（RAT）有效负荷，让远程操作员可以访问受害计算机，并可让远程操作员在网络中获得一个初始访问点。然后，攻击者会生成用于“命令控制”的新域名，并通过定期更改自己的网络用户名，将这些域发送到受感染网络上的远程访问工具（RAT）。用于“命令控制”的域和 IP 地址是临时的，并且攻击者每隔几天就会对此进行更改。攻击者通过安装 Windows 服务——其名称很容易被计算机所有者认为是合法的系统服务名称，从而看似合法地保留在受害计算机上。在部署该恶意软件之前，攻击者可能已经在各种防病毒（AV）产品上进行了测试，以确保它与任何现有或已知的恶意软件签名都不匹配。

为了与受害主机进行交互，远程操作员使用 RAT 启动 Windows 命令提示符，例如 cmd.exe。然后，攻击者使用受感染计算机上已有的工具来了解有关受害者系统和周围网络的更多信息，以便提高其在其它系统上的访问级别，并朝着实现其目标进一步迈进。

更具体地说，攻击者使用内置的 Windows 工具或合法的第三方管理工具来发现内部主机和网络资源，并发现诸如帐户、权限组、进程、服务、网络配置和周围的网络资源之类的信息。然后，远程操作员可以使用 Invoke-Mimikatz 来批量捕获缓存的身份验证凭据。在收集到足够的信息之后，攻击者可能会进行横向移动，从一台计算机移动到另一台计算机，这通常可以使用映射的 Windows 管理员共享和远程 Windows（服务器消息块 [SMB]）文件副本以及远程计划任务来实现。随着访问权限的增加，攻击者会在网络中找到感兴趣的文档。然后，攻击者会将这些文档存储在一个中央位置，使用 RAR 等程序通过远程命令行 shell 对文件进行压缩和加密，最后，通过 HTTP 会话，将文件从受害者主机中渗出，然后在其方便使用的远程计算机上分析和使用这些信息。

传统检测方案捉襟见肘

现有的检测方案难以检测到上述情景中所介绍的 APT 攻击。大多数防病毒应用程序可能无法可靠地检测到自定义工具，因为攻击者在使用这些工具之前，已经对其进行了测试，甚至可能包含一些混淆技术，以便绕开其它类型的恶意软件检测。此外，恶意远程操作员还能够在他们所攻击的系统上使用合法功能，逃避检测。而且许多检测工具无法收集到足够的数据，来发现此类恶意使用合法系统的行为。

当前其它的网络安全方法，例如威胁情报信息共享，可能对于检测攻击者基础设施也无济于事，因为攻击者指标可能变化太快。典型的网络流量检查也将于事无补，因为 APT 的流量（例如上述示例中所述的流量）已通过有效的 SSL 加密。SSL 拦截可能有用，但是要将恶意行为从善意网络行为中区分出来，实在太困难了。

提升检测能力：开发基于 ATT&CK 框架的对抗赛

自 2012 年 MITRE 进行网络竞赛以来，MITRE 主要通过研究对抗行为、构建传感器来获取数据以及分析数据来检测对抗行为。该过程包含三个重要角色：“白队”、“红队”和“蓝队”，如下所示：

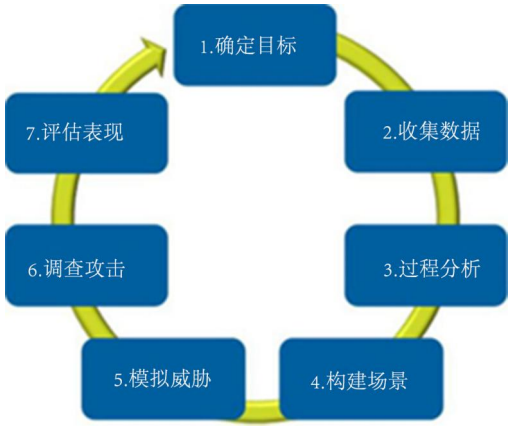
- 白队——开发用于测试防御的威胁场景。白队与红队

和蓝队合作，解决网络竞赛期间出现的问题，并确保达到测试目标。白队与网络管理员对接，确保维护网络资产。

◆ 红队——扮演网络竞赛中的攻击者。执行计划好的威胁场景，重点是对抗行为模拟，并根据需要与白队进行对接。在网络竞赛中出现的任何系统或网络漏洞都将报告给白队。

◆ 蓝队——在网络竞赛中担任网络防御者，通过分析来检测红队的活动。他们也被认为是一支狩猎队。

基于 ATT&CK 框架，开发网络对抗赛主要包含以下七个步骤：



开发网络对抗赛的七个步骤

下面，我们将对这七个步骤进行详细介绍。

第 1 步：确定目标

第一步是确定要检测的对抗行为的目标和优先级。在决定优先检测哪些对抗行为时，需要考虑以下几个因素：

(1) 哪种行为最常见？

优先检测攻击者最常使用的 TTP，并解决最常见的、最常遇到的威胁技术，这会对组织机构的安全态势产生最广泛的影响。拥有强大的威胁情报能力后，组织机构就可以了解需要关注哪些 ATT&CK 战术和技术。

(2) 哪种行为产生的负面影响最大？

组织机构必须考虑哪些 TTP 会对组织机构产生最大的潜在不利影响。这些影响可能包括物理破坏、信息丢失、系统受损或其它负面后果。

(3) 容易获得哪些行为的相关数据？

与那些需要开发和部署新传感器或数据源的行为相比，对于已拥有必要数据的行为进行分析要容易得多。

(4) 哪种行为最有可能表示是恶意行为？

只是由攻击者产生的行为而不是合法用户产生的行为，对于防御者来说用处最大，因为这些数据产生误报的可能性较小。

第 2 步：收集数据

在创建分析方案时，组织机构必须确定、收集和存储制定分析方案所需的数据。为了确定分析人员需要收集哪些数据来制定分析方案，首先要了解现有传感器和日志记录机制已经收集了哪些数据。在某些情况下，这些数据可能满足给定分析的数据要求。但是，在许多情况下，可能需要修改现有传感器和工具的设置或规则，以便收集所需的数据。在其它情况下，可能需要安装新工具或功能来收集所需的数据。在确定了创建分析所需的数据之后，必须将其收集并存储在将要编写分析的平台上。例如，可以使用 Splunk 的体系结构。

由于企业通常在网络入口和出口点部署传感器，因此，许多企业都依赖边界处收集的数据。但是，这就限制了企业只能看到进出网络的网络流量，而不利于防御者看到网络中及系统之间发生了什么情况。如果攻击者能够成功访问受监视边界范围内的系统并建立规避网络保护的命令和控制，则防御者可能会忽略攻击者在其网络内的活动。正如上文的攻击示例所述，攻击者使用合法的 Web 服务和通常允许穿越网络边界的加密通信，这让防御者很难识别其网络内的恶意活动。

由于使用基于边界的方法无法检测到很多攻击行为，因此，很有必要通过终端（主机端）数据来识别渗透后的操作。下图展示的是企业边界网络传感器在 ATT&CK 框架中的覆盖范围。红色表示未能检测到攻击行为，黄色表示有一定检测能力。如果在终端上没有传感器来收集相关数据，比如进程日志，就很难检测到 ATT&CK 模型描述的许多入侵。目前，国内外一些新一代主机安全厂商，都是采用在主机端部署 Agent 方式，比如青藤云安全，通过 Agent 提供主机端高价值数据，包括操作审计日志、进程启动日志、网络连接日志、DNS 解析日志等。

此外，仅仅依赖于通过间歇性扫描端点来收集端点数据或获取数据快照，这可能无法检测到已入侵网络边界并在网络内部进行操作的攻击者。间歇性地收集数据可能会导致错过检测快照之间发生的行为。例如，攻击者可以使用技术将未知的 RAT 加载到合法的进程（例如 explorer.exe）中，然后使用 cmd.exe 命令行界面通过远程 Shell 与系统进行交互。攻击者可能会在很短的时间内采取一系列行动，并且几乎不会在任何部件中留下痕迹让网络防御者发现。如果在加载 RAT 时执行了扫描，则收集信息（例如正在运行的进程、进程树、已加载的 DLL、Autoruns 的位置、打开的网络连接以及文件中的已知恶意软件签名）的快照可能只会看到在 explorer.exe 中运行的 DLL。但是，快照会错过将 RAT 实际注入到 explorer.exe、

cmd.exe 启动、生成的进程树以及攻击者通过 shell 命令执行的其它行为，因为数据不是持续收集的。

图 2：企业边界网络传感器在 ATT&CK 框架中的覆盖范围

第 3 步：过程分析

组织机构拥有了必要的传感器和数据后，就可以进行分析了。进行分析需要一个硬件和软件平台，在平台上进行设计和运行分析方案，并能够让数据科学家设计分析方案。尽管通常是通过 SIEM 来完成的，但这并不是唯一的方法，也可以使用 Splunk 查询语言来进行分析，相关的分析分为四大类：

◆ 行为分析——旨在检测某种特定对抗行为，例如创建新的 Windows 服务。该行为本身可能是恶意的，也可能不是恶意的。并将这类行为映射到 ATT&CK 模型中那些确定的技术上。

◆ 情景感知——旨在全面了解在给定时间，网络环境中正在发生什么事情。并非所有分析都需要针对恶意行为生成警报。相反，分析也可以通过提供有关环境状态的一般信息，证明对组织机构有价值。诸如登录时间之类的信息并不表示恶意活动，但是当与其它指标一起使用时，这种类型的数据也可以提供有关对抗行为的必要信息。情景感知分析还可以有助于监视网络环境的健康状况（例如，确定哪些主机上的传感器运行出错）。

◆ 异常值分析——旨在分析检测到非恶意行为，这类行为表现异常，令人怀疑，包括检测之前从未运行过的可执行文件，或者标识网络上通常没有运行过的进程。和情景感知分析一样，分析出异常值，不一定表示发生了攻击。

◆ 取证——这类分析在进行事件调查时最为有用。通常，取证分析需要某种输入才能发挥其作用。例如，如果分析人员发现主机上使用了凭据转储工具，进行此类分析会告诉你，哪些用户的凭据受到了损坏。

防御团队在网络竞赛演习期间或制定实际应用中的分析时，可以结合使用这四种类型的分析。下文将介绍如何综合使用这四种类型的分析：

1. 首先，通过在分析中寻找远程创建的计划任务，向安全运营中心（SOC）的分析人员发出警报，警告正在发生攻击行为（行为分析）。

2. 在从受感染的计算机中看到此警报后，分析人员将运行分析方案，查找预计执行计划任务的主机上是否存在任何异常服务。通过该分析，可以发现，攻击者在安排好远程任务之后不久，就已在原始主机上创建了一个新服务（异常点分析）。

3. 在确定了新的可疑服务后，分析人员将进行进一步调查。通过分析，确定可疑服务的所有子进程。这种调查可能会显示一些指标，说明主机上正在执行哪些活动，从而发现 RAT 行为。再次运行相同的分析方案，寻找 RAT 子进程的子进程，就会找到 RAT 对 PowerShell 的执行情况（取证）。

4. 如果怀疑受感染机器可以远程访问其它主机，分析人员会决定调查可能从该机器尝试过的任何其它远程连接。为此，分析人员会运行分析方案，详细分析相关计算机环境中所有已发生的远程登录，并发现与之建立连接的其它主机（情景感知）。

第 4 步：构建场景

传统的渗透测试侧重于突出攻击者可能在某个时间段会利用不同类型系统上的哪些漏洞。MITRE 的对抗模拟方法不同于这些传统方法。其目标是让红队成员执行基于特定或许多已知攻击者的行为和技术，以测试特定系统或网络的防御效果。对抗模拟演习由小型的重复性活动组成，这些活动旨在通过系统地将各种新的恶意行为引入环境，来改善和测试网络上的防御能力。进行威胁模拟的红队与蓝队紧密合作（通常称为紫队），以确保进行深入沟通交流，这对于快速磨练组织机构的防御能力至关重要。因此，与全范围的渗透测试或以任务目标为重点的红队相比，对抗模拟测试测试速度更快、测试内容更集中。

随着检测技术的不断发展成熟，攻击者也会不断调整其攻击方法，红蓝对抗的模拟方案也应该围绕这种思想展开。大多数真正的攻击者都有特定的目标，例如获得对敏感信息的访问权限。因此，在模拟对抗期间，也可以给红队指定特定的目标，以便蓝队能够针对最可能的对抗技术对网络防御和功能进行详细测试。

（1）场景规划

为了更好地执行对抗模拟方案，需要白队传达作战目标，而又不向红队或蓝队泄露测试方案的详细信息。白队应该利用其对蓝队的了解情况以及针对威胁行为的分析来检测差距，并根据蓝队所做的更改或需要重新评估的内容来制定对抗模拟计划。白队还应确定红队是否有能力充分测试对抗行为。如果没有，白队应该与红队合作解决存在的差距，包括可能需要的任何工具开发、采购和测试。对抗模拟场景可对抗计划为基础，传达要求并与资产所有者和其它利益相关者进行协调。

模拟场景可以是详细的命令脚本，也可以不是。场景规划应该足够详细，足以指导红队验证防御能力，但也应该足够灵活，可以让红队在演习期间根据需要调整其行动，以测试蓝军可能未曾考虑过的行为变化。由于蓝队的防御方案也可能已经很成熟，可以涵盖已知的威胁行为，因此红队还必须能够自由扩展，不仅仅局限于单纯的模拟。通过由白队决定应该测试哪些新行为，蓝队可能不知道要进行哪些特定活动，而红队可以不受对蓝队功能假设的影响，因为这可能会影响红队做出决策。白队还要继续向红队通报有关环境的详细信息，以便通过对抗行为全面测试检测能力。

(2) 场景示例

举个例子，假设在 Windows 操作系统环境中，红队采用的工具提供了一个访问点和 C2 通道，攻击者通过交互式 shell 命令与系统进行交互。蓝队已部署了 Sysmon 作为探针，对过程进行持续监控并收集相关数据。此场景的目标是基于 Sysmon 从网络端点中收集数据来检测红队的入侵行为。

场景详情：

1. 为红队确定一个特定的最终目标。例如，获得对特定系统、域帐户的访问权，或收集要渗透的特定信息。

2. 假设已经入侵成功，让红队访问内部系统，以便于观察渗透后的行为。红队可以在环境中的一个系统上执行加载程序或 RAT，模拟预渗透行为，并获得初始立足点，而不考虑先前的了解、访问、漏洞利用或社会工程学等因素。

3. 红队必须使用 ATT&CK 模型中的“发现”技术来了解环境并收集数据，以便进一步行动。

4. 红队将凭证转储到初始系统上，并尝试定位周围还有哪些系统的凭证可以利用。

5. 红队横向移动，直到获得目标系统、账户、信息为止

使用 ATT&CK 作为对抗模拟指南，为红队制定一个明确的计划。技术选择的重点是基于在已知的入侵活动中通常使用的技术，来实现测试目标，但是允许红队在技术使用方面进行一些更改，采用一些其它行为。

(3) 场景实现

上述场景示例的具体实现步骤如下所示：

1. 模拟攻击者通过白队提供的初始访问权限后，获得了“执行”权限。以下内容可以表示攻击者可以使用通用的、标准化的应用层协议（如 HTTP、HTTPS、SMTP 或 DNS）进行通信，以免被发现。例如远程连接命令，会被嵌入到这些通信协议中。

ATT&CK 战术	技术	ID
命令与控制	标准应用层协议	T1071
命令与控制	常用端口	T1043
命令与控制	远程文件拷贝	T1105

2. 建立连接后，通过远程访问工具启动反弹 shell 命令界面:

ATT&CK 战术	技术	ID	工具 / 命令
执行	命令行界面	T1059	cmd.exe

3. 通过命令行界面执行“执行”技术：

ATT&CK 战术	技术	ID	工具 / 命令
发现	账户发现	T1087	net localgroup administrators net group <groupname> /domain net user /domain
发现	文件与目录发现	T1083	dir cd
发现	局域网络配置发现	T1016	ipconfig /all
发现	局域网络连接发现	T1049	netstat -ano
发现	权限组发现	T1069	net localgroup net group /domain
发现	进程发现	T1057	tasklist /v
发现	远程系统发现	T1018	net view
发现	系统信息发现	T1082	systeminfo
发现	系统服务发现	T1007	net start

4. 获得了足够的信息后，可以根据需要，自由执行其它战术和技术。以下技术是基于 ATT&CK 的建议措施，以建立持久性或通过提升权限来建立持久性。获得足够的权限后，使用 Mimikatz 转储凭据，或尝试使用键盘记录器获取凭据，捕获的用户输入信息。

ATT&CK 战术	技术	ID
持久化	新服务	T1050
持久化	注册表运行键 / 启动文件夹	T1060
提升权限、防御绕过	绕过用户账户控制	T1088
凭据访问	凭据转储	T1003
凭据访问	输入捕获	T1056

5. 如果获得了凭据并且通过“发现”技术对系统有了全面的了解，就可以尝试横向移动来实现该方案的主要目标了。

ATT&CK 战术	技术	ID	工具 / 命令
横向移动	Windows Admin 共享	T1077	net use * \\<remote system>\ADMIN$ <password> /user:<domain>\<account>
横向移动	远程文件拷贝	T1105	copy <source path to file> <remote share destination>
执行	服务执行	T1035	psexec

6. 根据需要使用上文提到的技术，继续横向移动，获取并渗透目标敏感信息。建议使用以下 ATT&CK 技术来收集和提取文件：

ATT&CK 战术	技术	ID
收集	本地系统数据	T1005
收集	网络共享驱动中的数据	T1039
渗透	数据压缩	T1002
渗透	数据加密	T1022
渗透	通过命令与控制渠道渗透	T1041

第 5 步：模拟威胁

在制定好对抗模拟方案和分析方案之后，就该使用情景来模拟攻击者了。首先，让红队模拟威胁行为并执行由白队确定的技术。在对抗模拟作战中，可以让场景的开发人员来验证其网络防御的有效性。红队则需要专注于红队入侵后的攻击行为，通过给定网络环境中特定系统上的远程访问工具访问企业网络。白队预先给红队访问权限可以加快评估速度，并确保充分测试入侵后的防御措施。然后，红队按照白队规定的计划和准则行动。

白队应与组织机构的网络资产所有者和安全组织协调任何对抗模拟活动，确保及时了解网络问题、用户担忧、安全事件或其它可能发生的问题。

第 6 步：调查攻击

一旦在给定的网络竞赛中红队发起了攻击，蓝队要尽可能发现红队的所作所为。在 MITRE 的许多网络竞赛中，蓝队中有负责创建场景的开发人员。这样做的好处是，场景开发者人员可以亲身体验他们的分析方案在现实模拟情况下表现如何，并从中汲取经验教训，推动未来的发展和完善。

在网络竞赛中，蓝队最开始有一套高度可信的过程分析方案，如果执行成功，就会了解一些初步指标红队，例如，红队时何时何地活跃起来的。这很重要，因为除了模糊的时间范围（通常是一个月左右）之外，没有向蓝队提供任何有关红队活动的信息。有时，蓝队的过程分析属于“行为”分析类别，而有些分析可能属于“异常”类别。应用这些高可信度的分析方案会促使蓝队使用先前描述的其它类型的分析（情景感知、异常情况和取证）进一步调查单个主机。当然，这个分析过程是反复迭代进行的，随着收集到新信息，在整个练习过程中，这一过程会反复进行。

最终，当确定某个事件是红队所为时，蓝队就开始形成自身的时间表。了解时间表很重要，可以帮助分析人员推断出只靠分析方案无法获得的信息。时间表上的活动差距可以确定需要进一步调查的时间窗口期。另外，通过以这种方式查看数据，即便没有关于红队活动的任何证据，蓝队成员也可以推断出在哪些位置能够发现红队的活动。例如，看到一个新的可执行文件运行，但没有证据表明它是如何放置在机器上的，这可能会提醒分析人员有可能存在红队行为，并可以提供有关红队如何完成其横向移动的详细信息。通过这些线索，还可以形成一些关于创建新分析的想法，以便用于基于 ATT&CK 的分析开发方法的下一次迭代。

在调查红队的攻击时，蓝队会随着自身演习的进行而制定出几大类信息。这些信息是他们希望发现的信息，例如：

◆ 受到影响的主机——在演习时，这通常表示为主机列表以及每个主机视为可疑主机的原因。在尝试补救措施时，这些信息至关重要。

◆ 帐户遭到入侵——蓝队能够识别网络上已被入侵的帐户，这一点非常重要。如果不这样做，则红队或现实生活中的攻击者就可以从其它媒介重新获得对网络的访问权限，以前所有的补救措施也就化为泡影了。

◆ 目标——蓝队还需要努力确定红队的目标以及他们是否实现了目标。这通常是最难发现的一个内容，因为这需要大量的数据来确定。

◆ 使用的 TTP——在演习结束时，要特别注意红队的 TTP，这是确定未来工作的一种方式。红队可能已经利用了网络中需要解决的错误配置，或者红队可能发现了蓝队当前无法识别而无法进一步感知的技术。蓝队确定的 TTP 应该与红队所声称的 TTP 进行比较，识别任何防御差距。

第 7 步：评估表现

蓝队和红队活动均完成后，白队将协助团队成员进行分析，将红队活动与蓝队报告的活动进行比较。这可以进行全面的比较，蓝队可以从中了解他们在发现红队行动方面取得了多大程度上的成功。蓝队可以使用这些信息来完善现有分析，并确定对于哪些对抗行为，他们需要开发或安装新传感器、收集新数据集或制定新分析方案。

写在最后

ATT&CK 是 MITRE 提供的“对抗战术、技术和常识”框架，是由攻击者在攻击企业时会利用的 12 种战术和 300 多种技术组成的精选知识库，对于企业识别差距，提高防御能力有重大意义。而本文则通过详细介绍如何基于 ATT&CK 框架制定分析方案，如何根据分析方案检测入侵行为从而发现黑客，为防御者提供了一款强大的工具，可以有效提高检测能力，从而增强企业的防御能力。

看 ATT&CK 框架，攻击者最常用的 TOP7 攻击技术及其检测策略

之前，我们已经对 ATT&CK 进行了一系列的介绍，相信大家都已了解，Mitre ATT&CK 通过详细分析公开可获得的威胁情报报告，形成了一个巨大的 ATT&CK 技术矩阵。诚然，这对于提高防御者的防御能力、增加了攻击者的攻击成本都有巨大作用。但或许是出于猎奇心理，很多威胁情报报告更多地是在报道攻击者使用的比较新颖有趣的技术方法，而却忽视了攻击者反复使用的普通技术。这也是 Mitre 公司在 2019 年 10 月份的 ATT&CKcon2.0 大会上，推出了 ATT&CK Sightings 项目，以期借助社区力量收集更多直接观察数据的原因所在。

对此，一些安全公司通过在真实环境中所收集的直接观察数据所检测到的技术直观性更强，也更具说服力。Red Canary 是美国一家从事信息安全的网络安全公司，负责对客户环境中的终端数据进行大规模检索，来寻找攻击者。Red Canary 分析了过去五年里，其客户环境中发生的一万多起恶意事件，并将恶意事件中使用的技术与 ATT&CK 框架进行了映射。

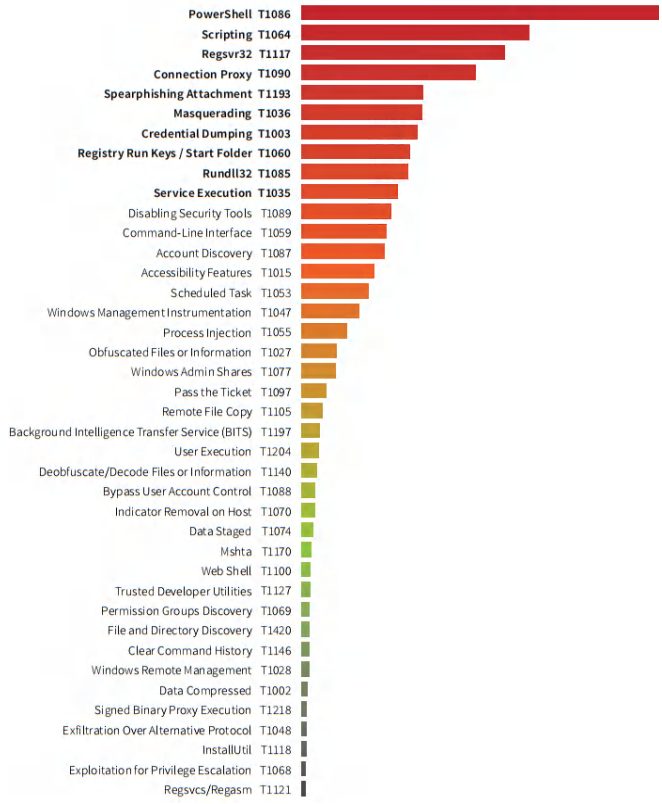
本文将通过对比 Mitre ATT&CK 的 Top 20 攻击技术及 Red Canary 基于 ATT&CK 的 Top 20 攻击技术，确定了攻击者最常用的七项 ATT&CK 技术，并对其进行了详细分析。

Mitre 公司 VS Red Canary Top 20 攻击技术

Mitre ATT&CK 通过整合、分析 400 多份公开的威胁情报报告，将技术报告中的内容与 ATT&CK 技术进行了映射，MITRE ATT&CK 整理得出的 Top 20 攻击技术为：

1. 标准应用层协议	11. 凭据转储
2. 远程文件拷贝	12. 屏幕捕获
3. 系统信息发现	13. 输入捕获
4. 命令行界面	14. 系统所有者 / 用户发现
5. 文件和目录发现	15. 脚本执行
6. 注册表 Run Key/ 启动文件夹	16. 常用端口
7. 混淆文件或信息	17. 标准加密协议
8. 文件删除	18. PowerShell
9. 进程发现	19. 伪装
10. 系统网络配置发现	20. 新服务

Red Canary 通过对过去五年里，其客户环境中发生的一万多起恶意事件进行分析，得出了威胁事件利用每种 ATT&CK 技术的频率，如下图所示：



从图中我们看到，Red Canary 分析得出的 Top 20 攻击技术为：

1. PowerShell	11. 禁用安全工具
2. 脚本执行	12. 命令行界面
3. Regsvr32	13. 账户发现
4. 连接代理	14. 辅助功能
5. 鱼叉式钓鱼附件	15. 计划任务
6. 伪装	16. WMI
7. 凭据转储	17. 进程注入
8. 注册表 Run Key/ 启动文件夹	18. 混淆文件或信息
9. Rundll32	19. Windows Admin 分享
10. 服务执行	20. 票据传递

对 Mitre ATT&CK 和 Red Canary 分别整理得出的 Top 20 技术进行对比分析，我们可以发现有 7 项技术是重合的，分别为 PowerShell、脚本执行、命令行界面、注册表 Run Key/ 启动文件夹、伪装、混淆文件或信息、凭据转储。或许，这应该是防御者建立防御方案的着手点。

下表展示了这七项技术在 Red Canary 和 Mitre ATT&CK Top 20 攻击技术中的排名次序和出现次数。

技术	Red Canary 排名	MITRE 排名	Red Canary 出现次数	MITRE 出现次数
T1086 PowerShell	1	18	1,774	46
T1064 脚本执行	2	15	794	53
T1059 命令行界面	12	4	294	112
T1060 注册表 Run Keys / 启动文件夹	8	6	377	93
T1036 伪装	6	19	419	45
T1027 混淆文件或信息	18	7	120	88
T1003 凭据转储	7	11	405	61

希望读者能够通过上表中的数据，进一步了解攻击者对这七种技术的使用频率和在攻击者中的流行程度。下面，我们详细分析这七种技术。

攻击者最常用的 TOP7 攻击技术

“Powershell”备攻击者青睐

PowerShell 是 Windows 操作系统中包含的功能强大的交互式命令行界面和脚本环境。攻击者可以使用 PowerShell 执行许多操作，包括发现信息和执行代码，例如，用于运行可执行文件的 Start-Process cmdlet 和在本地或在远程计算机上运行命令的 Invoke-Command cmdlet。

默认情况下，PowerShell 基本上已包含在每个 Windows 操作系统中，提供了对 Windows API 的完全访问权限，包括数百个供开发人员和系统管理员使用的功能，但同样也遭到攻击者的大肆利用。像许多核心平台实用程序一样，PowerShell 库很容易获得，因此也很容易实现，能够暴露任意进程中的完整 PowerShell 功能。

那么该如何进行检测呢？进程监控是最普遍有效的技术。进程监控可以让防御者确定在其环境中使用 PowerShell 的基准。进程命令行监控则更有效，可以洞悉哪些 PowerShell 实例试图通过编码命令传递有效负载并以其他方式混淆其最初意图。除了 PowerShell 脚本的默认主机之外，脚本还可以在加载 PowerShell 框架库的其他进程中执行。要查看该行为，观察模块负载以及进行分析以提供其他上下文，从而为检测提供支持。

“脚本执行”不容忽视

攻击者可能会使用脚本来帮助进行操作并执行其他本来应该是手动进行的多项操作。脚本执行对于加快操作任务，减少访问关键资源所需的时间很有用。通过直接在 API 级别与操作系统交互，而无需调用其他程序，某些脚本语言可以用于绕过过程监视机制。Windows 的常用脚本语言包括 VBScript 和 PowerShell，但也可以采用命令行批处理脚本的形式。

安全工具和人工分析的快速发展让攻击者很难使用公开的攻击载荷或者直接从磁盘获取相关载荷。因此，攻击者需要找到替代方法来执行有效载荷并执行其他恶意活动，这是脚本相关技术日益流行的主要原因。此外，该技术利用的运行时环境、库和可执行文件是每个现代计算平台的核心组件，不能轻易禁用，并且没有始终对其进行密切监视。

在 Windows 上，Windows 脚本宿主（WSH）最简单的检测用例是基于 process ancestry 的。这包括监视从 shells 命令（cmd.exe、powershell.exe）、Office 应用程序、Web 浏览器和 Web 服务处理程序中生成的 wscript.exe 或 cscript.exe。还建议监视从非标准

位置执行的脚本，例如用户可写路径，包括 appdata\local*、其他类似路径以及临时目录。

此外，监视进程元数据、进程命令行和文件修改都是非常重要的策略。检测与托管脚本相关的二进制文件的可疑模块加载（例如 vbscript.dll）的检测系统也是值得采取的策略。

当然最彻底的办法就是禁用 Windows 脚本宿主，也可以强制对脚本进行签名，以确保仅执行批准的脚本。诸如 AppLocker 之类的工具还提供了与脚本执行相关的其他约束。这些是预防策略，但也可用于检测之用，因为尝试执行未经授权的脚本应产生更高质量的报警信号。

“命令行界面”也是黑客最爱

命令行界面提供了一种与计算机系统进行交互的方式，并且是许多类型的操作系统平台的共同功能。Windows 系统上的令行界面是 cmd，可用于执行许多任务，包括执行其他软件。命令行界面可以通过远程桌面应用程序、反弹 Shell 会话等在本地或远程进行交互。执行的命令以命令行界面进程的当前权限级别运行，除非该命令进行进程调用，更改执行权限（例如计划任务）。

命令行界面发展至今，已经有大量的成熟工具可以使用。此外，命令行界面是一个非常轻便的应用程序，打开时不会给硬件带来负担，因此打开起来更快。而且在基于 GUI 的应用程序上完成的所有任务，能够通过命令行界面更快地打开。

针对这类攻击，可以通过使用命令行参数正确记录进行执行情况来捕获命令行界面活动。通过深入了解攻击者时如何使用本地进程或自定义工具的，可以进一步了解攻击者的行为。这就需要做到以下两方面：（1）了解组织机构中应用程序的常见来源；（2）收集命令行和相关的检测数据 .

“注册表 run key/ 启动文件夹”是实现持久化关键动作

在注册表的“run keys”或启动文件夹中添加一个条目，将会导致用户登录时，该程序会运行该条目。这些程序将在用户的上下文中执行，并具有与账户相同的权限级别。

注册表 run key 和启动文件夹历来都是各类攻击者实现持久化的重要目标。根据 Microsoft 文档，对注册表 run key 的支持至少可以追溯到 Windows95。有可靠记录表明，作为一种持久化机制，加之易于实施，该技术在一定程度上解释了其为何在攻击者中使用非常普遍。攻击者仅需要用户级别的权限，并具有写入注册表或将有效负载拖放到启动文件夹的功能。

虽然实现起来相对简单，但非常有效。随着时间的推移，该技术已经从引用可执行有效负载发展为加载动态库，并利用了其他技术（例如 regsvr32 和脚本执行）。针对该攻击技术，可以在持久化机制生命周期的三个不同点上有效地实现检测：安装时、休眠时以及触发时。

在安装时检测 run key 和启动文件夹项目需要监视特定注册表和文件系统路径的变更情况。可以通过平台文档或通过引用一些实用程序来报告是否存在这些配置来列举这些路径。此外，可能会成功检查任何已知与这些路径结合使用的文件类型，例如 LNK。要检测已安装且处于休眠状态的持久化，可以检查同一注册表和文件系统路径的内容中是否存在可疑条目。创建一个基准并定期监视是否有偏移基准的情况，以此来减少调查工作量。

当然，持久化永远不会单独发生，它始终是达到目的的手段。因此，监视预期某些变更会涉及哪些进程以及尚未观察到的进程之间的关系也是非常有效的。

“伪装”是绕过防御最佳办法

伪装是指为了逃避防御和观察而操纵或滥用合法或恶意的可执行文件的名称或位置的情况。攻击者利用伪装作为绕过防御技术的手段或欺骗手段。攻击者使用该技术通过使恶意可执行文件和软件看起来合法或预期来破坏机器和人工分析。伪装的实现范围很广，从简单地重命名可执行文件（从而让这些文件看起来更像是正常系统进程）到更复杂的方法（例如命令行欺骗）。伪装在攻击者中使用很普遍，因为它满足了绕过防御技术和人为分析的简单需求，并且相对容易实施。

检测伪装技术的一种策略是利用二进制元数据，例如在文件创建或签名时的原始文件名。例如，如果要查找 wscript.exe，则应查找具有该名称的二进制文件，也应查找具有原始文件名 WScript 的任何二进制文件。

虽然，可以检测名称或元数据为 wscript.exe 的任何二进制文件，但基于文件的签名、哈希或其他标识符并不可信。因此可对文件位置建立一个基准，对上述方法进行补充。如果我们了解给定二进制文件通过哪个路径执行，则可以在其他任何地方看到该标志时，就可以触发报警。

“混淆文件或信息”可逃避基于签名检测系统

攻击者可能会试图通过加密、编码或其他方式混淆系统上或传输中的可执行文件或文件内容，从而使其难以发现或分析。

这是一种可以跨不同的平台和网络使用，以绕过防御的常见行为。

许多网络安全检测产品（防病毒软件、IDS 等）设计为基于恶意软件的签名运行。一旦发现了在野使用的特定恶意软件变体，便会提取出该恶意软件的独特功能，并用于在未来感染中对其进行检测和识别。将通过网络边界或下载到主机的每条数据与这些签名进行比较。如果找到匹配项，则将采取措施（删除、隔离、警报等）。

混淆的目的是绕过这些基于签名的检测系统，并增加对恶意软件样本进行取证分析的难度。如果以某种方式混淆了签名所基于的数据或代码，则检测引擎在寻找纯文本签名时就无法找到匹配项。

存在许多混淆算法，例如压缩、编码、加密、隐写等等。恶意软件使用者可以隐藏各种不同类型的文件和数据。例如，恶意软件可能被设计为使用混淆来隐藏其恶意代码。或者，恶意软件变体可能会对其配置文件进行加密，从而使恶意软件分析师更难于理解其功能。

想要检测混淆文件或者信息，除非在混淆过程留下了可以检测到的独特伪像，否则很难检测文件混淆。如果无法检测，则可以去检测执行混淆文件的恶意活动（例如，用于在文件系统上写入、读取或修改文件的方法）。标记并分析包含混淆指示符和已知可疑语法（例如未解释的转义字符，如 "^" 和 """"）的命令。反混淆工具可以用来检测文件 / 有效载荷中的这些指标。

此外，可以在网络上检测到用于初始访问的有效载荷中使用了哪些混淆方法。还可以使用网络入侵检测系统和电子邮件网关筛选来识别压缩和加密的附件和脚本。某些电子邮件附件展示系统可以打开压缩和加密的附件。通过网站从加密连接传递的有效载荷需要进行加密的网络流量检查。

“凭据转储”让黑客在内网为所欲为

凭据转储是从操作系统和软件获取帐户登录名和密码信息的过程，通常是哈希或明文密码形式的信息。进行凭据转储后，攻击者就可以使用凭据进行横向移动及访问受限信息。

凭据转储是攻击者访问目标组织中的用户帐户和其他资源的共同需求。攻击者还利用转储的凭据来实现权限提升和横向移动。凭据对于攻击者而言是如此重要，以致在许多情况下，获取用户名和密码不仅是达到目的的手段，而且是攻击的整个目标。因此，在各种犯罪论坛上，凭据都是可出售的商品，并且有些网站可以追踪公开的凭据转储情况。除了将转储凭据用于出售和初始访问外，凭据是漏洞利用后的一个重要部分。一旦攻击者获得对环境的初始访问权限，通常需要某种级别的特权访问权限才能实现攻击活动中的进一步目标。虽然有很多方法可以提高特权级别，但是最有效和可靠的方法之一是使用具有特定级别权限的人员的合法凭据。

凭据可以从内存中以纯文本格式提取。监视对特定进程的访问可以为防御者提供一种检测凭据转储的方式。这种检测方法很容易产生大量误报事件，因为操作系统的内置功能也可以访问这些过程。防御者要重点关注潜在问题进程之间的交互来减少这种噪声。

检测是否存在凭据转储的另一种方法是分析常用工具，并使用其他数据源作为相关点，基于留下的指纹来制定检测策略。注册表项和文件修改就是一个很好的切入点。

写在最后

我们之前已经针对 ATT&CK 框架进行了一系列的介绍，有兴趣的读者可以阅读一下之前的相关文章。但是，ATT&CK 框架包含了 300 多种技术，而且每种技术又包含多种变体。面对一个体型如此庞大的框架，可能会让人有些望而却步，一脸茫然，不知该从何处入手。本文通过对比分析 MITRE ATT&CK 和 Red Canary 总结分析的 Top 20 攻击技术，发现其中有七项技术是重合的，突出说明了这七项攻击技术在攻击者中的普遍性，是需要防御者重点关注或是建立防御方案时的着手点。本文对这七项技术进行了简单的介绍，说明了这些技术能够得到攻击者青睐的原因所在，并给出了检测策略，希望能够为读者使用 ATT&CK 框架带来一些帮助。