# 一、ATT&CK框架背景介绍

MITRE是美国政府资助的一家研究机构，该公司于1958年从MIT分离出来，并参与了许多商业和最高机密项目。其中包括开发FAA空中交通管制系统和AWACS机载雷达系统。MITRE在美国国家标准技术研究所（NIST）的资助下从事了大量的网络安全实践。

MITRE在2013年推出了**ATT&CK模型**，它是**根据真实的观察数据来描述和分类对抗行为**。**ATT&CK将已知攻击者行为转换为结构化列表，将这些已知的行为汇总成战术和技术，并通过几个矩阵以及结构化威胁信息表达式（STIX）、指标信息的可信自动化交换（TAXII）来表示。**由于此列表相当全面地呈现了攻击者在攻击网络时所采用的行为，因此对于各种进攻性和防御性度量、表示和其他机制都非常有用。

MITRE 对于ATT&CK 框架的解释是「**将攻击者所使用的攻击和其生命周期的各个阶段，与网路攻击者可能攻击的目标及平台，浓缩唯一个共同的知识库及框架**」。

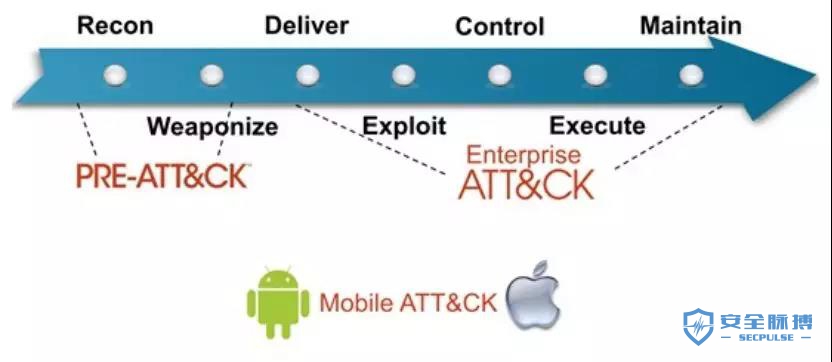
MITRE ATT&CK的目标是**创建网络攻击中使用的已知对抗战术和技术的详尽列表**。在过去的一年中，MITRE  ATT&CK框架在安全行业中广受欢迎。简单来说，ATT&CK是MITRE提供的“对抗战术、技术和常识”框架，是由攻击者在攻击企业时会利用的**12种战术**和**244种企业技术**组成的**精选知识库**。

ATT&CK会详细介绍每一种技术的利用方式，以及为什么了解这项技术对于防御者来说很重要。这极大地帮助了安全人员更快速地了解不熟悉的技术。例如，对于甲方企业而言，平台和数据源非常重要，企业安全人员需要了解应该监控哪些系统以及需要从中收集哪些内容，才能减轻或检测由于入侵技术滥用造成的影响。这时候，ATT&CK场景示例就派上用场了。针对每种技术都有具体场景示例，说明攻击者是如何通过某一恶意软件或行动方案来利用该技术的。ATT&CK每个示例都采用Wikipedia的风格，引用了许多博客和安全研究团队发表的文章。因此如果ATT&CK中没有直接提供内容，通常可以在这些链接的文章中找到。

因此，现在很多企业都开始研究ATT&CK，在这一过程中通常会看到企业组织采用两种方法。首先是**盘点其安全工具**，让安全厂商提供一份对照ATT&CK覆盖范围的映射图。尽管这是最简单、最快速的方法，但供应商提供的覆盖范围可能与企业实际部署工具的方式并不匹配。此外，也有些企业组织在**按照战术逐项进行评估企业安全能力**。以持久化战术为例，这些技术可能非常复杂，而且，仅仅缓解其中一部分技术，并不意味着攻击者无法以其它方式滥用这项技术。

# 二、MITRE ATT＆CK与Kill Chain的对比

总体来说，ATT&CK模型是在洛克希德-马丁公司提出的KillChain模型的基础上，构建了一套更细粒度、更易共享的知识模型和框架。目前ATT&CK模型分为三部分，分别是**PRE-ATT&CK，ATT&CK for Enterprise和ATT&CK for Mobile**。其中PRE-ATT&CK覆盖Kill Chain模型的前两个阶段，包含了与攻击者在尝试利用特定目标网络或系统漏洞进行相关操作有关的战术和技术。ATT&CK for Enterprise覆盖Kill Chain的后五个阶段，ATT&CK for Enterprise由适用于Windows、Linux和MacOS系统的技术和战术部分。ATT&CK for Mobile包含适用于移动设备的战术和技术。

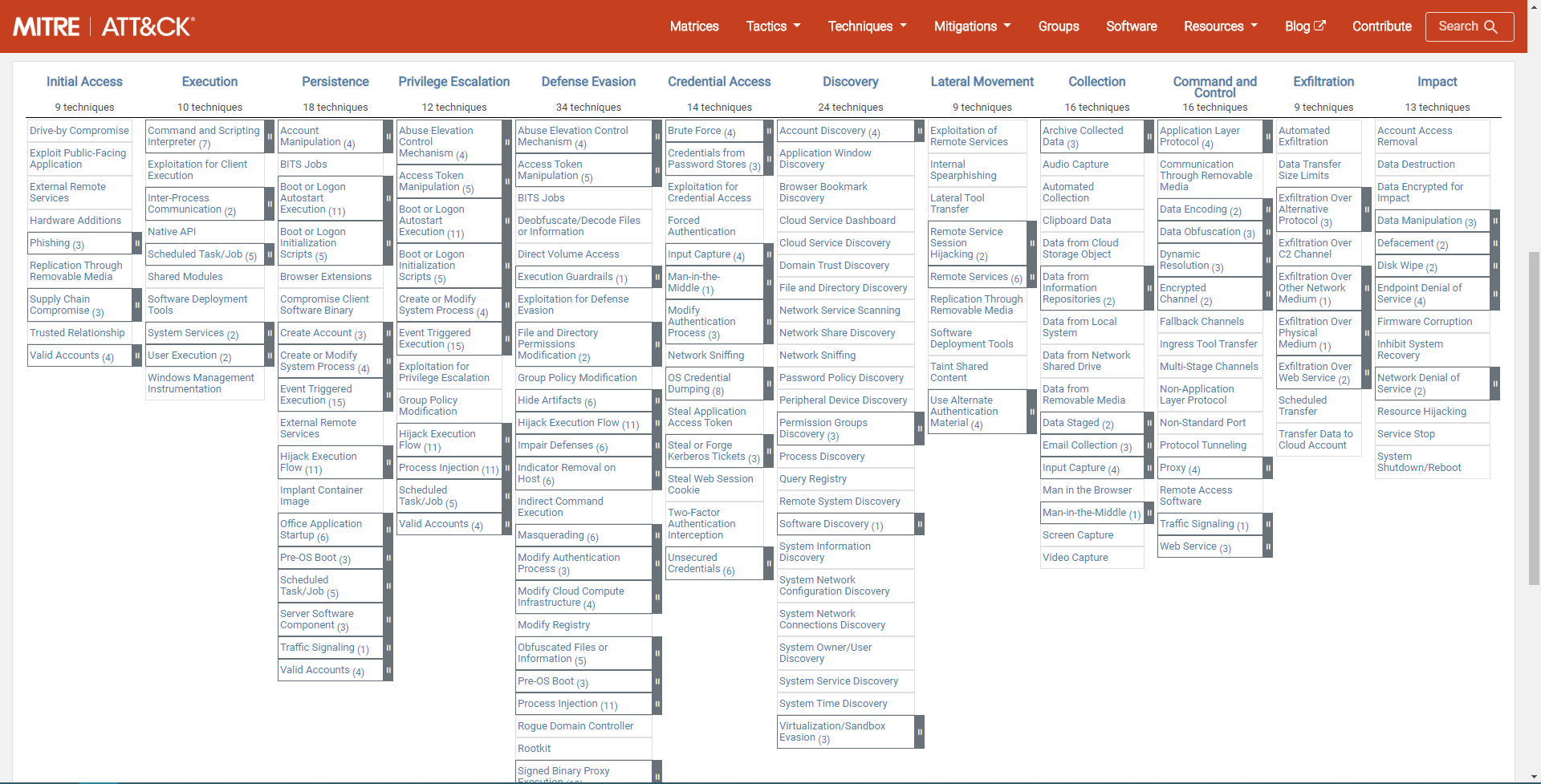
[](https://secpulseoss.oss-cn-shanghai.aliyuncs.com/wp-content/uploads/2019/10/%E5%BE%AE%E4%BF%A1%E5%9B%BE%E7%89%87_20191017163754.jpg)

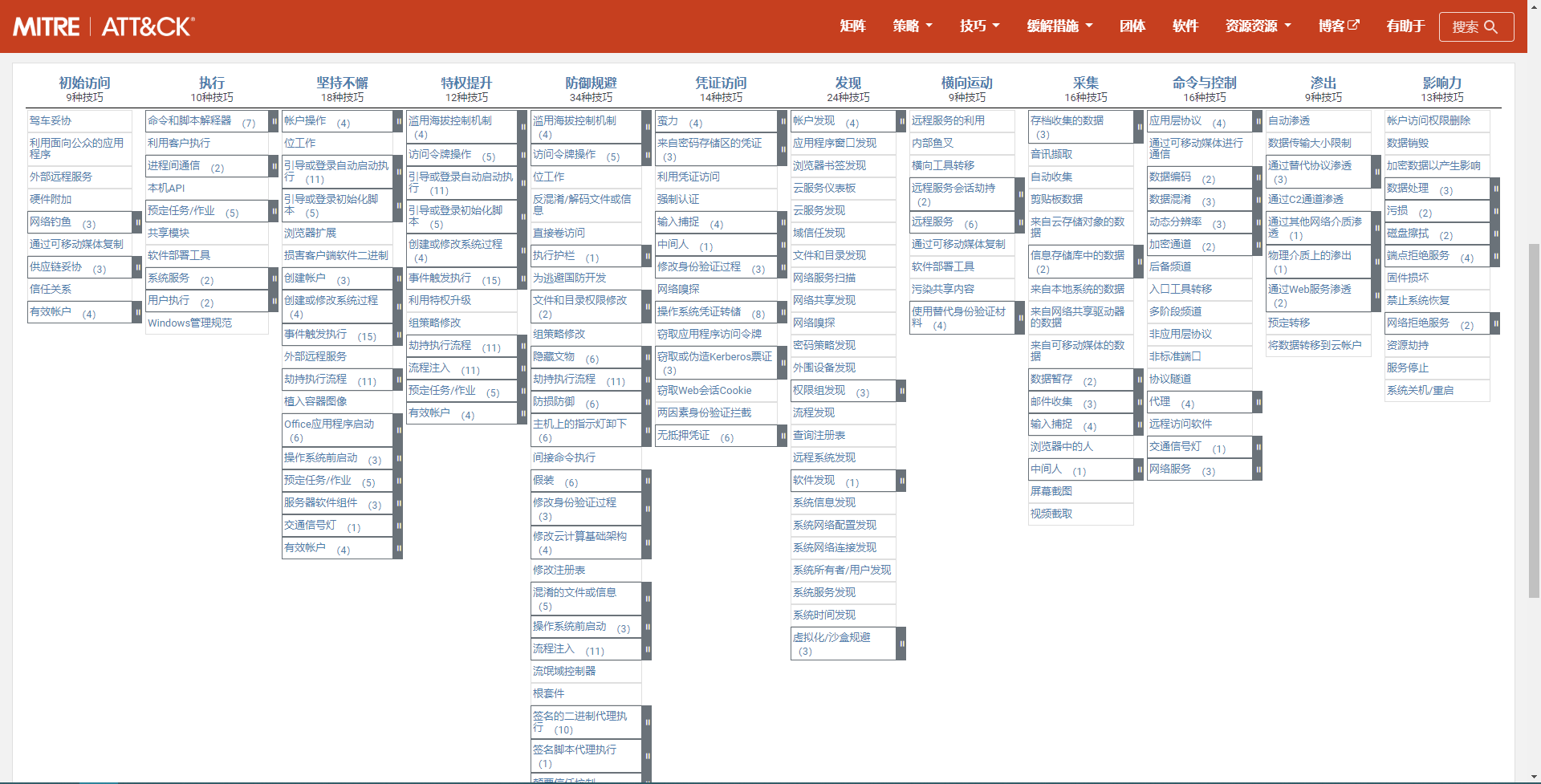
但是，ATT&CK的战术跟洛克希德·马丁的网络杀伤链不一样，并没有遵循任何线性顺序。相反，攻击者可以随意切换战术来实现最终目标。没有一种战术比其它战术更重要。企业组织必须对当前覆盖范围进行分析，评估组织面临的风险，并采用有意义措施来弥合差距。

除了在Kill Chain战术上更加细化之外，ATT＆CK还描述了可以在每个阶段使用的技术，而Kill Chain则没有这些内容。

# 三、ATT＆CK框架的使用

从视觉角度来看，MITRE ATT＆CK矩阵按照一种易于理解的格式将所有已知的战术和技术进行排列。**攻击战术展示在矩阵顶部，每列下面列出了单独的技术。一个攻击序列按照战术，至少包含一个技术，并且通过从左侧（初始访问）向右侧（影响）移动，就构建了一个完整的攻击序列。**一种战术可能使用多种技术。例如，攻击者可能同时尝试鱼叉式网络钓鱼攻击中的钓鱼附件和钓鱼链接。

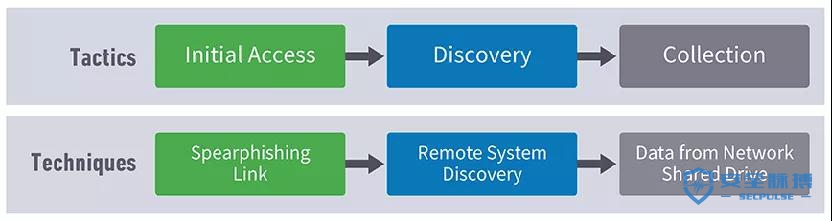




**ATT＆CK矩阵顶部为攻击战术，每列包含多项技术**

ATT＆CK战术按照逻辑分布在多个矩阵中，并以“初始访问”战术开始。例如：发送包含恶意附件的鱼叉式网络钓鱼邮件就是该战术下的一项技术。ATT＆CK中的每种技术都有唯一的ID号码，例如，此处所使用的技术T1193。矩阵中的下一个战术是“执行”。在该战术下，有“用户执行/ T1204”技术。该技术描述了在用户执行特定操作期间执行的恶意代码。在矩阵中后面的阶段中，您将遇到“提升特权”、“横向移动”和“渗透”之类的战术。

攻击者无需使用矩阵顶部所示的所有12项战术。相反，**攻击者会使用最少数量的战术来实现其目标，因为这可以提高效率并且降低被发现的几率**。例如，对手使用电子邮件中传递的鱼叉式网络钓鱼链接对CEO行政助理的凭据进行“初始访问”。获得管理员的凭据后，攻击者将在“发现”阶段寻找远程系统。接下来可能是在Dropbox文件夹中寻找敏感数据，管理员对此也有访问权限，因此无需提升权限。然后攻击者通过将文件从Dropbox下载到攻击者的计算机来完成收集。

[](https://secpulseoss.oss-cn-shanghai.aliyuncs.com/wp-content/uploads/2019/10/20191014104359dfd.jpg)

**攻击示例（攻击中使用了不同战术中的技术）**

ATT＆CK 导航工具是一个很有用的工具，可用于映射针对ATT＆CK技术的控制措施。可以添加不同的层，来显示特定的检测控制措施、预防控制措施甚至观察到的行为。导航工具可以在线使用，快速搭建模型或场景，也可以下载下来，进行内部设置，作为一个持久化的解决方案。

下文将针对ATT&CK框架中的12种战术的中心思想以及如何缓解和检测战术中的某些技术进行一些解读。

## 01、初始访问

尽管ATT&CK并不是按照任何线性顺序排列的，但初始访问是攻击者在企业环境中的立足点。对于企业来说，该战术是从PRE-ATT&CK到ATT&CK的理想过渡点。攻击者会使用不同技术来实现初始访问技术。

例如，假设攻击者使用Spearphishing（鱼叉式）附件。附件本身将利用某种类型的漏洞来实现该级别的访问，例如PowerShell或其它脚本技术。如果执行成功，可以让攻击者采用其它策略和技术来实现其最终目标。幸运的是，由于这些技术众所周知，因此有许多技术和方法可用于减轻和检测每种技术的滥用情况。

此外，安全人员也可以将ATT&CK和CIS控制措施相结合，这将发挥更大作用。对于初始访问这种战术，我认为其中**三项CIS控制措施**能发挥极大作用。

（1）控制措施4：**控制管理员权限的使用。**如果攻击者可以成功使用有效帐户或让管理员打开spearphishing附件，后续攻击将变得更加轻松。

（2）控制措施7：**电子邮件和Web浏览器保护。**由于这些技术中的许多技术都涉及电子邮件和、Web浏览器的使用，因此，控制措施7中的子控制措施将非常有用。

（3）控制措施16：**帐户监视和控制。**充分了解帐户应执行的操作并锁定权限，不仅有助于限制数据泄露造成的损害，还可以发挥检测网络中有效帐户滥用的功能。

初始访问是攻击者将在企业环境中的落脚点。想要尽早终止攻击，那么“初始访问”将是一个很合适的起点。此外，如果企业已经采用了CIS控制措施并且正在开始采用ATT&CK的方法，这将会很有用。

## 02、执行

在对手在进攻中所采取的所有战术中，应用最广泛的战术莫过于“执行”。攻击者在考虑现成的恶意软件、勒索软件或APT攻击时，他们都会选择“执行”。由于恶意软件必须运行，因此防御者就有机会阻止或检测到它。但是，并非所有恶意软件都是可以用杀毒软件轻松查找其恶意可执行文件。

此外，对于命令行界面或PowerShell对于攻击者而言非常有用。许多无文件恶意软件都专门利用了其中一种技术或综合使用这两种技术。这些类型的技术对攻击者的威力在于，终端上已经安装了上述技术，而且很少会删除。系统管理员和高级用户每天都依赖其中一些内置工具。ATT&CK中的缓解控制措施甚至声明了，这些控制措施也无法删除上述技术，只能对其进行审计。而攻击者所依赖的就是，终端上安装采用了这些技术，因此要获得对攻击者的优势，只能对这些技术进行审计，然后将它们相关数据收集到中央位置进行审核。

最后，**应用白名单**是缓解恶意软件攻击时最有用的控制措施。但和任何技术一样，这不是解决所有问题的灵丹妙药。但是，应用白名单会降低攻击者的速度，并且还可能迫使他们逃离舒适区，尝试其它策略和技术。当攻击者被迫离开自己的舒适区之外时，他们就有可能犯错。

如果企业当前正在应用CIS关键安全控制措施，该战术与控制措施2——已授权和未授权软件清单非常匹配。从缓解的角度来看，企业无法防护自己未知的东西，因此，第一步是要了解自己的财产。要正确利用ATT&CK，企业不仅需要深入了解已安装的应用程序。还要清楚内置工具或附加组件会给企业组织带来的额外风险。在这个环节中，可以采用一些安全厂商的资产清点工具，例如青藤等主机安全厂商都能提供详细的软件资产清单。

## 03、持久化

除了勒索软件以外，持久化是最受攻击者追捧的技术之一。攻击者希望尽可能减少工作量，包括减少访问攻击对象的时间。即便运维人员采取重启、更改凭据等措施后，持久化仍然可以让计算机再次感染病毒或维护其现有连接。例如注册表Run键、启动文件夹是最常用的技术，这些注册表键或文件系统位置在每次启动计算机时都会执行。因此攻击者在启动诸如Web浏览器或Microsoft Office等常用应用时开始获得持久化。

此外，还有使用“镜像劫持（IFEO）注入”等技术来修改文件的打开方式，在注册表中创建一个辅助功能的注册表项，并根据镜像劫持的原理添加键值，实现系统在未登录状态下，通过快捷键运行自己的程序。

在所有ATT&CK战术中，笔者认为持久化是最应该关注的战术之一。如果企业在终端上发现恶意软件并将其删除，很有可能它还会重新出现。这可能是因为有漏洞还未修补，但也可能是因为攻击者已经在此或网络上的其它地方建立了持久化。与使用其它一些战术和技术相比，使用持久化攻击应该相对容易一些。

## 04、提升权限

所有攻击者都会对提权爱不释手，利用系统漏洞达到root级访问权是攻击者核心目标之一。其中一些技术需要系统级的调用才能正确使用，Hooking和进程注入就是两个示例。该战术中的许多技术都是针对被攻击的底层操作系统而设计，要缓解可能很困难。

ATT&CK提出“应重点防止对抗工具在活动链中的早期阶段运行，并重点识别随后的恶意行为。”这意味着需要利用纵深防御来防止感染病毒，例如终端的外围防御或应用白名单。对于超出ATT&CK建议范围之外的权限升级，一种良好的防止方式是在终端上使用加固基线。例如CIS基线提供了详细的分步指南，指导企业如何加固系统，抵御攻击。

应对此类攻击战术另一个办法是审计日志记录。当攻击者采用其中某些技术时，它们将留下蛛丝马迹，暴露他们的目的。尤其是针对主机侧的日志，如果能够记录服务器的所有运维命令，进行存证以及实时审计。例如，实时审计运维人员在服务器上操作步骤，一旦发现不合规行为可以进行实时告警，也可以作为事后审计存证。也可以将数据信息对接给SOC、态势感知等产品，也可以对接给编排系统。

## 05、防御绕过

到目前为止，该战术所拥有的技术是MITRE ATT&CK框架所述战术中最多的。该战术的一个有趣之处是某些恶意软件，例如勒索软件，对防御绕过毫不在乎。他们的唯一目标是在设备上执行一次，然后尽快被发现。

一些技术可以骗过防病毒（AV）产品，让这些防病毒产品根本无法对其进行检查，或者绕过应用白名单技术。例如，禁用安全工具、文件删除和修改注册表都是可以利用的技术。当然防御者可以通过监视终端上的更改并收集关键系统的日志将会让入侵无处遁形。

## 06、凭据访问

毫无疑问，攻击者最想要的凭据，尤其是管理凭据。如果攻击者可以登录，为什么要用0Day或冒险采用漏洞入侵呢？这就犹如小偷进入房子，如果能够找到钥匙开门，没人会愿意砸破窗户方式进入。

任何攻击者进入企业都希望保持一定程度的隐身。他们将希望窃取尽可能多的凭据。他们当然可以暴力破解，但这种攻击方式噪声太大了。还有许多窃取哈希密码及哈希传递或离线破解哈希密码的示例。最后，攻击者最喜欢方式是窃取明文密码。明文密码可能存储在明文文件、数据库甚至注册表中。攻击者入侵一个系统、窃取本地哈希密码并破解本地管理员密码并不鲜见。

应对凭据访问最简单办法就是采用复杂密码。建议使用大小写、数字和特殊字符组合，目标是让攻击者难以破解密码。最后一步就是监视有效帐户的使用情况。在很多情况下，是通过有效账户发生的数据泄露。

当然最稳妥办法办法就是启用多因素验证。即使存在针对双重验证的攻击，有双重验证（2FA）总比没有好。通过启用多因素验证，可以确保破解密码的攻击者在访问环境中的关键数据时，仍会遇到另一个障碍。

## 07、发现

“发现”战术是一种难以防御的策略。它与洛克希德·马丁网络Kill Chain的侦察阶段有很多相似之处。组织机构要正常运营业务，肯定会暴露某些特定方面的内容。

最常用的是应用白名单，可以解决大多数恶意软件。此外，欺骗防御也是一个很好方法。放置一些虚假信息让攻击者发现，进而检测到对手的活动。通过监视，可以跟踪用户是否正在访问不应访问的文档。

由于用户通常在日常工作中执行各种技术中所述的许多操作，因此，从各种干扰中筛选出恶意活动可能非常困难。理解哪些操作属于正常现象，并为预期行为设定基准时，会在尝试使用这一战术时有所帮助。

## 08、横向移动

攻击者在利用单个系统漏洞后，通常会尝试在网络内进行横向移动。甚至通常一次只针对单个系统的勒索软件也试图在网络中移动以寻找其它攻击目标。攻击者通常会先寻找一个落脚点，然后开始在各个系统中移动，寻找更高的访问权限，以期达成最终目标。

在缓解和检测对该特定技术的滥用方面，适当的网络分段可以在很大程度上缓解风险。将关键系统放置在一个子网中，将通用用户放置在另一个子网中，将系统管理员放置在第三个子网中，有助于快速隔离较小网络中的横向移动。在终端和交换机级别都设置防火墙也将有助于限制横向移动。

遵循CIS 控制措施 14——基于需要了解受控访问是一个很好的切入点。除此之外，还应遵循控制措施4——控制管理员权限的使用。攻击者寻求的是管理员凭据，因此，严格控制管理员凭据的使用方式和位置，将会提高攻击者窃取管理员凭据的难度。此控制措施的另一部分是记录管理凭据的使用情况。即使管理员每天都在使用其凭据，但他们应该遵循其常规模式。发现异常行为可能表明攻击者正在滥用有效凭据。

除了监视身份验证日志外，审计日志也很重要。域控制器上的事件ID 4769表示，Kerberos黄金票证密码已重置两次，这可能表明存在票据传递攻击。或者，如果攻击者滥用远程桌面协议，审计日志将提供有关攻击者计算机的信息。

## 09、收集

ATT&CK “收集”战术概述了攻击者为了发现和收集实现目标所需的数据而采取的技术。该战术中列出的许多技术都没有关于如何减轻这些技术的实际指导。实际上，大多数都是含糊其辞，称使用应用白名单，或者建议在生命周期的早期阶段阻止攻击者。

但是，企业可以使用该战术中的各种技术，了解更多有关恶意软件是如何处理组织机构中数据的信息。攻击者会尝试窃取有关当前用户的信息，包括屏幕上有什么内容、用户在输入什么内容、用户讨论的内容以及用户的外貌特征。除此之外，他们还会寻求本地系统上的敏感数据以及网络上其它地方的数据。

了解企业存储敏感数据的位置，并采用适当的控制措施加以保护。这个过程遵循CIS控制措施14——基于需要了解受控访问,可以帮助防止数据落入敌手。对于极其敏感的数据，可查看更多的日志记录，了解哪些人正在访问该数据以及他们正在使用该数据做什么。

## 10、命令和控制

现在大多数恶意软件都有一定程度的命令和控制权。黑客可以通过命令和控制权来渗透数据、告诉恶意软件下一步执行什么指令。对于每种命令和控制，攻击者都是从远程位置访问网络。因此了解网络上发生的事情对于解决这些技术至关重要。

在许多情况下，正确配置防火墙可以起到一定作用。一些恶意软件家族会试图在不常见的网络端口上隐藏流量，也有一些恶意软件会使用80和443等端口来尝试混入网络噪音中。在这种情况下，企业需要使用边界防火墙来提供威胁情报数据，识别恶意URL和IP地址。虽然这不会阻止所有攻击，但有助于过滤一些常见的恶意软件。

如果边界防火墙无法提供威胁情报，则应将防火墙或边界日志发送到日志服务处理中心，安全引擎服务器可以对该级别数据进行深入分析。例如Splunk等工具为识别恶意命令和控制流量提供了良好的方案。

## 11、数据渗漏

攻击者获得访问权限后，会四处搜寻相关数据，然后开始着手数据渗透。但并不是所有恶意软件都能到达这个阶段。例如，勒索软件通常对数据逐渐渗出没有兴趣。与“收集”战术一样，该战术对于如何缓解攻击者获取公司数据，几乎没有提供指导意见。

在数据通过网络渗漏的情况下，建立网络入侵检测或预防系统有助于识别何时传输数据，尤其是在攻击者窃取大量数据（如\*\*\*\*库）的情况下。此外，尽管DLP成本高昂，程序复杂，但可以确定敏感数据何时会泄露出去。IDS、IPS和DLP都不是100%准确的，所以部署一个纵深防御体系结构以确保机密数据保持机密。

如果企业组织机构要处理高度敏感的数据，那么应重点关注限制外部驱动器的访问权限，例如USB接口，限制其对这些文件的访问权限，即可禁用他们装载外部驱动器的功能。

要正确地解决这个战术，首先需要知道组织机构的关键数据所在的位置。如果这些数据还在，可以按照CIS 控制措施14——基于需要了解受控访问，来确保数据安全。之后，按照CIS控制措施13——数据保护中的说明了解如何监视试图访问数据的用户。

## 12、影响

攻击者试图操纵、中断或破坏企业的系统和数据。用于影响的技术包括破坏或篡改数据。在某些情况下，业务流程可能看起来很好，但可能已经更改为有利于对手的目标。这些技术可能被对手用来完成他们的最终目标，或者为机密泄露提供掩护。

例如攻击者可能破坏特定系统数据和文件，从而中断系统服务和网络资源的可用性。数据销毁可能会通过覆盖本地或远程驱动器上的文件或数据使存储的数据无法恢复。针对这类破坏可以考虑实施IT灾难恢复计划，其中包含用于进行可用于还原组织数据的常规数据备份的过程。

# 四、ATT&CK使用场景

ATT＆CK在各种日常环境中都很有价值。开展任何防御活动时，可以应用ATT＆CK分类法，参考攻击者及其行为。ATT＆CK不仅为网络防御者提供通用技术库，还为渗透测试和红队提供了基础。提到对抗行为时，这为防御者和红队成员提供了通用语言。企业组织可以使用多种方式来使用MITRE ATT＆CK。下文是一些常见的主要场景：

## （1）对抗模拟

ATT＆CK可用于创建对抗性模拟场景，测试和验证针对常见对抗技术的防御方案。

## （2）红队/渗透测试活动

红队、紫队和渗透测试活动的规划、执行和报告可以使用ATT＆CK，以便防御者和报告接收者以及其内部之间有一个通用语言。

## （3）制定行为分析方案

ATT＆CK可用于构建和测试行为分析方案，以检测环境中的对抗行为。

## （4）防御差距评估

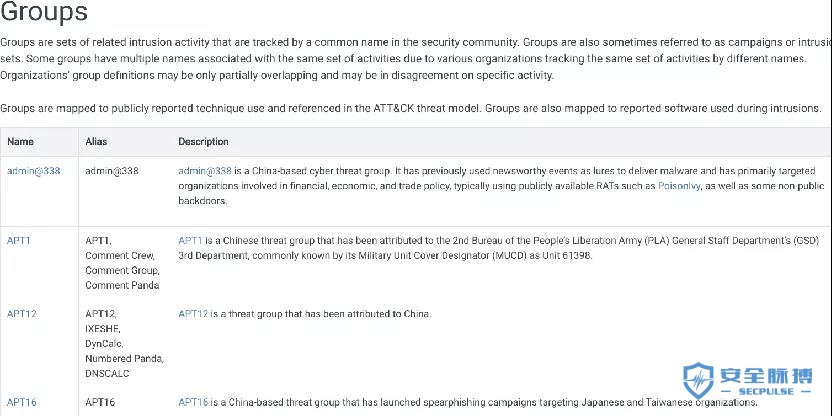
ATT＆CK可以用作以行为为核心的常见对抗模型，以评估组织企业内现有防御方案中的工具、监视和缓解措施。在研究MITRE ATT＆CK时，大多数安全团队都倾向于为Enterprise矩阵中的每种技术尝试开发某种检测或预防控制措施。虽然这并不是一个坏主意，但是ATT＆CK矩阵中的技术通常可以通过多种方式执行。因此，阻止或检测执行这些技术的一种方法并不一定意味着涵盖了执行该技术的所有可能方法。由于某种工具阻止了用另一种形式来采用这种技术，而组织机构已经适当地采用了这种技术，这可能导致产生一种虚假的安全感。但是，攻击者仍然可以成功地采用其他方式来采用该技术，但防御者却没有任何检测或预防措施。

## （5）SOC成熟度评估

ATT＆CK可用作一种度量，确定SOC在检测、分析和响应入侵方面的有效性。SOC团队可以参考ATT＆CK已检测到或未涵盖的技术和战术。这有助于了解防御优势和劣势在哪里，并验证缓解和检测控制措施，并可以发现配置错误和其他操作问题。

## （6）网络威胁情报收集

ATT＆CK对于网络威胁情报很有用，因为ATT＆CK是在用一种标准方式描述对抗行为。可以根据攻击者已知利用的ATT＆CK中的技术和战术来跟踪攻击主体。这为防御者提供了一个路线图，让他们可以对照他们的操作控制措施，查看对某些攻击主体而言，他们在哪些方面有弱点，在哪些方面有优势。针对特定的攻击主体，创建MITRE ATT＆CK 导航工具内容，是一种观察环境中对这些攻击主体或团体的优势和劣势的好方法。ATT＆CK还可以为STIX 和 TAXII 2.0提供内容，从而可以很容易地将支持这些技术的现有工具纳入中。

[](https://secpulseoss.oss-cn-shanghai.aliyuncs.com/wp-content/uploads/2019/10/%E5%BE%AE%E4%BF%A1%E5%9B%BE%E7%89%87_201910121646195.jpg)

ATT＆CK提供了将近70个攻击主体和团体的详细信息，包括根据开放源代码报告显示，已知他们所使用的技术和工具。

使用ATT＆CK的通用语言，为情报创建过程提供了便利。如前所述，这适用于攻击主体和团体，但也适用于从SOC或事件响应活动中观察到的行为。也可以通过ATT＆CK介绍恶意软件的行为。任何支持ATT＆CK的威胁情报工具都可以简化情报创建过程。将ATT＆CK应用于任何提及的行为的商业和开源情报也有助于保持情报的一致性。当各方围绕对抗行为使用相同的语言时，将情报传播到运维人员或管理人员变得容易得多了。如果运营人员确切地知道什么是强制验证，并且在情报报告中看到了这一信息，则他们可能确切地知道应该对该情报采取什么措施或已经采取了哪些控制措施。以这种方式，实现ATT＆CK对情报产品介绍的标准化可以大大提高效率并确保达成共识。

**写在最后**

MITRE为大家提供了ATT＆CK及其相关工具和资源，为安全界做出了重大贡献。它的出现恰合时宜。由于攻击者正在寻找更隐蔽的方法并避免传统安全工具的检测，因此防御者不得不改变检测和防御方式。ATT＆CK改变了我们对IP地址和域名等低级指标的认知，并让我们从行为的视角来看待攻击者和防御措施。与过去“一劳永逸”的工具相比，检测和预防行为之路要困难得多。此外，随着防御者带来新的功能，攻击者肯定会作出相应调整。ATT＆CK提供了一种方法来描述他们开发的新技术，并希望防御者能够紧随技术发展的新步伐。