ATT＆CK使用的方法的总结分析

如若要对目标网络进行APT攻击，首先应该想办法攻入到目标网络中去，即对目标发动攻击，包含这一部分的攻击techniques的内容为Initial Access。在Initial Access中共有九种方法来实现对目标网络/系统的攻击。

驾车妥协(Drive-by compromise):攻击者可以通过用户在正常访问网页的流程中攻击用户的系统，通过驾车妥协可以将用户的web浏览器作为攻击者攻击的目标。

利用面向公众的应用程序([Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190)):攻击者可能会通过软件，数据或者命令通过目标计算机/系统中的计算机或者程序中的漏洞来实施入侵操作。

外部远程服务([External Remote Services](https://attack.mitre.org/techniques/T1133)):有的企业网络内部会有面向外部的访问功能如VPN,Citrix或者其他的访问机制。攻击者可以据此而对网络用户进行攻击或者对网络的远程服务器网关进行攻击来获得相应权限。

外部远程服务不仅能用在initial access中，也可以用在Persistence等其他进程中。

附加硬件(Hardware Additions):攻击者通过在系统内部引入的电脑配件，计算机或者网络硬件来获取被攻击网络的访问权限。

网络钓鱼(Phishing):网络钓鱼攻击为社会工程学攻击，通过向目标网络的用户发送钓鱼信息来获得系统的敏感信息或者获取目标网络的访问权限。

通过可移动媒介进行传播([Replication Through Removable Media](https://attack.mitre.org/techniques/T1091)):通过可移动媒介进行传播的恶意软件具有在将可移动媒介插入到系统中的时候就能自动运行的功能。由于恶意软件这种特性的存在，因此有时候可能会成功攻入与外网物理隔绝的互联网中去。

供应链攻击([Supply Chain Compromise](https://attack.mitre.org/techniques/T1195)):供应链攻击是攻击者通过攻击感染合法应用分发恶意软件来访问源代码，构建过程或者更新机制来实现对其他信任这些软件的用户的攻击。

信任关系([Trusted Relationship](https://attack.mitre.org/techniques/T1199)):攻击者通过利用有权接触被攻击者的组件对目标网络进行攻击。通过受信第三方与被攻击网络的连接对目标网络进行攻击。通过受信第三方进行攻击所收到的审查会比较少，容易攻击成功。

有效账户([Valid Accounts](https://attack.mitre.org/techniques/T1078)):攻击者通过获取目标网络中的有效账户来获取网络中的数据，并以此为基础获得目标网络的访问权，同时也可以在目标网络中长期存在，进而可以提高权限规避目标网络内部的审查。有效账户中共有四类账户，分别为：默认账户，域账户，本地账户，云账户四类账户。

有效账户的方法不仅能应用在初始访问(Initial Access)中，还能用在很多其他的方法中。

Execution

恶意代码的执行技术的目的是远程运行恶意代码，在执行(execution)中共包括10种的techniques。

命令和脚本解释器([Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059))：攻击者可以通过使用命令和脚本解释器来执行发动攻击的命令，脚本或者二进制文件。命令和脚本解释器使得文件具有了跨平台运行的能力，他们在不同的平台之间都具有相同的功能。

利用客户执行([Exploitation for Client Execution](https://attack.mitre.org/techniques/T1203))：攻击者通过有针对性的利用用户客户端软件中存在的漏洞来执行任意代码。一般来说最具价值的攻击是可以用于在远程系统上执行代码的攻击，可以通过这种攻击方式获取系统的访问权限。

进程间通信([Inter-Process Communication](https://attack.mitre.org/techniques/T1559))：攻击者可能会应用进程之间的通信(IPC)机制来执行本地代码或命令。进程通常使用IPC来共享数据，相互通信或同步执行。

本机API([Native API](https://attack.mitre.org/techniques/T1106))：攻击者可以直接与本机OS应用程序编程接口(API)进行交互以进行执行行为。

预定的任务/作业([Scheduled Task/Job](https://attack.mitre.org/techniques/T1053))：攻击者滥用任务计划功能来促进恶意代码的初始或者重复执行。在所有的操作系统中都存在有用于在指定时间来执行程序的程序或者脚本。

共享模块([Shared Modules](https://attack.mitre.org/techniques/T1129))：攻击者可能会使用操作系统中的共享模块来执行恶意负载。在windows系统中这一功能位于ntdll.dll中。

软件部署工具([Software Deployment Tools](https://attack.mitre.org/techniques/T1072))：攻击者可以访问并使用安装在企业网络内的第三方软件以实现在目标网络中横向移动。通过第三方部署工具实现对目标网络的攻击还能应用到其他的攻击方法中去。

系统服务([System Services](https://attack.mitre.org/techniques/T1569))：攻击者可能会使用系统服务或者守护进程来执行命令或者程序。攻击者可以通过服务交互或者是创建服务来进行恶意内容的执行。

用户执行([User Execution](https://attack.mitre.org/techniques/T1204))：用户执行这种攻击方式依赖于用户的特定操作才能进行更进一步的操作。这种攻击方式得以实现的原因是用户可能会受到社会工程的攻击，例如通过打开恶意文档文件或者链接导致恶意代码的执行。

Windows管理规范([Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047))：WMI为本地和远程访问windows系统组件提供了统一的环境。攻击者依靠WMI服务进行本地和远程访问，并依靠服务器消息块(SMB)和远程过程调用服务(RPCS)来进行远程访问。

Persistence

Persistence技术的作用是攻击者尝试可以一直对被攻击的网络/主机进行访问。

账户操作([Account Manipulation](https://attack.mitre.org/techniques/T1098))：攻击者可以通过操纵系统中的合法账户来维持其对受害系统的访问。对账户进行操作包括保留对受感染账户的攻击者访问权限的任何操作，例如修改数据或者修改账户的权限。为了创建或者操纵账户，攻击者需要对系统或者系统域具有足够的权限。

位工作([BITS Jobs](https://attack.mitre.org/techniques/T1197))：攻击者可能滥用BITS作业来在恶意代码执行后持续执行或清理。BITS为windows系统中的后台智能传输服务。

引导或登录自动启动并执行([Boot or Logon Autostart Execution](https://attack.mitre.org/techniques/T1547))：攻击者将系统设置配置为在系统启动或登录期间自动执行程序，以保持持久性或在受到感染的系统上获得更高级别的特权。操作系统可能具有在系统引导或帐户登录时自动运行程序的机制。这些机制可能包括自动执行放置在特别指定的目录中或由存储配置信息的存储库中引用的程序。

引导或初始化登录脚本([Boot or Logon Initialization Scripts](https://attack.mitre.org/techniques/T1037))：攻击者可以使用在启动或登录初始化时自动执行的脚本来建立入侵的持久性。初始化脚本可用于执行管理功能，该管理功能通常可以执行其他程序或将信息发送到内部日志服务器。

浏览器扩展([Browser Extensions](https://attack.mitre.org/techniques/T1176))：攻击者可能通过使用Internet浏览器扩展来建立对受害者系统的持久访问。浏览器扩展或插件是小程序，它们可以直接安装，也可以通过浏览器的应用商店安装，并且通常具有浏览器可以访问的所有内容的访问权限。

损害客户端软件的二进制文件([Compromise Client Software Binary](https://attack.mitre.org/techniques/T1554))：由于客户端软件使用户能够访问服务器提供的服务，因此对手可能会修改客户端软件二进制文件以建立对系统的持久访问。

创建账号([Create Account](https://attack.mitre.org/techniques/T1136))：攻击者可以创建一个帐户来维护对受害者系统的访问。可以使用创建具有访问足够访问权限的帐户来建立辅助凭据访问，而无需在系统上部署持久性远程访问工具。创建的账号分为本地账号，域账号，云账号。

创建或修改系统进程([Create or Modify System Process](https://attack.mitre.org/techniques/T1543))：攻击者可能会创建或修改系统级流程，以作为持久性的一部分重复执行恶意有效负载。在操作系统启动时，它们可以启动执行后台系统功能的进程。

事件触发执行([Event Triggered Execution](https://attack.mitre.org/techniques/T1546))：攻击者可以使用基于特定事件触发执行的系统机制来建立持久性和/或提升特权。

外部远程服务([External Remote Services](https://attack.mitre.org/techniques/T1133))：有的企业网络内部会有面向外部的访问功能如VPN,Citrix或者其他的访问机制。攻击者可以据此而对网络用户进行攻击或者对网络的远程服务器网关进行攻击来获得相应权限。

劫持执行流程([Hijack Execution Flow](https://attack.mitre.org/techniques/T1574))：攻击者可以通过劫持操作系统运行程序的方式来执行自己的恶意负载。劫持执行流可能出于持久性目的，同时也可以使用这些机制来提升特权或者规避防御。

植入容器映像([Implant Container Image](https://attack.mitre.org/techniques/T1525))：对手可能会在云容器映像中植入恶意代码以建立持久性。即在Amazon Web Service（AWS），Amazon Machine Images（AMI），Google Cloud Platform（GCP）映像和Azure Images以及可以在Docker等容器运行时植入后门，据此可以实现持久访问。

Office应用程序([Office Application Startup](https://attack.mitre.org/techniques/T1137))：对手可能会利用基于Microsoft Office的应用程序来保持启动之间的持久性。启动基于Office的应用程序时，Office可以使用多种机制来实现持久性。

在操作系统之前启动([Pre-OS Boot](https://attack.mitre.org/techniques/T1542))：在计算机的引导过程中，将在操作系统之前加载固件和各种启动服务。这些程序控制操作系统启动之前的执行流程。因为这些数据位于操作系统的下一层，由于基于主机软件的防御检测不到这一层，所以这很难被检测。

计划任务/工作([Scheduled Task/Job](https://attack.mitre.org/techniques/T1053))：所有主要操作系统中都存在的实用程序，用于计划要在指定日期和时间执行的程序或脚本。只要满足正确的身份验证，也可以在远程系统上安排任务。

服务器软件组件([Server Software Component](https://attack.mitre.org/techniques/T1505))：攻击者可能滥用服务器的合法可扩展开发功能来建立对系统的持久访问。企业服务器应用程序可能包含允许开发人员编写和安装软件或脚本以扩展主应用程序功能的功能。攻击者可能会借此来安装和恶意组件来扩展和滥用服务器的应用程序。

交通信号([Traffic Signaling](https://attack.mitre.org/techniques/T1205))：攻击者可能使用流量拦截来隐藏开放端口或其他用于持久性或命令和控制的恶意功能。流程是：在打开端口之前，发送带有某些特征的数据包，以使对手可以将其用于命令和控制。

有效账户([Valid Accounts](https://attack.mitre.org/techniques/T1078))：攻击者通过获取目标网络中的有效账户来获取网络中的数据，并以此为基础获得目标网络的访问权，同时也可以在目标网络中长期存在，进而可以提高权限规避目标网络内部的审查。有效账户中共有四类账户，分别为：默认账户，域账户，本地账户，云账户四类账户。

[Privilege Escalation](https://attack.mitre.org/tactics/TA0004" \o ")

特权升级包含攻击者用来在系统或网络上获取更高级别权限的技术。对手通常可以进入和探索具有无特权访问权限的网络，但是需要提升的权限才能实现他们的目标。常见方法是利用系统漏洞，配置错误和漏洞。

滥用权限控制机制([Abuse Elevation Control Mechanism](https://attack.mitre.org/techniques/T1548))：对手可能会规避旨在控制提升特权以获得更高级别权限的机制。必须授予特定用户授权才能执行可以被认为具有较高风险的任务。对手可以执行多种方法来利用系统内置的控制机制来提升系统上的特权。

操纵访问令牌([Access Token Manipulation](https://attack.mitre.org/techniques/T1134))：攻击者可以修改访问令牌以在不同的用户或系统安全性上下文下运行，以执行操作并绕过访问控制。

引导或登录自动启动并执行([Boot or Logon Autostart Execution](https://attack.mitre.org/techniques/T1547))：攻击者将系统设置配置为在系统启动或登录期间自动执行程序，以保持持久性或在受到感染的系统上获得更高级别的特权。操作系统可能具有在系统引导或帐户登录时自动运行程序的机制。这些机制可能包括自动执行放置在特别指定的目录中或由存储配置信息的存储库中引用的程序。

引导或初始化登录脚本([Boot or Logon Initialization Scripts](https://attack.mitre.org/techniques/T1037))：攻击者可以使用在启动或登录初始化时自动执行的脚本来建立入侵的持久性。初始化脚本可用于执行管理功能，该管理功能通常可以执行其他程序或将信息发送到内部日志服务器。

创建或修改系统进程([Create or Modify System Process](https://attack.mitre.org/techniques/T1543))：攻击者可能会创建或修改系统级流程，以作为持久性的一部分重复执行恶意有效负载。在操作系统启动时，它们可以启动执行后台系统功能的进程。

事件触发执行([Event Triggered Execution](https://attack.mitre.org/techniques/T1546))：攻击者可以使用基于特定事件触发执行的系统机制来建立持久性和/或提升特权。

利用特权升级([Exploitation for Privilege Escalation](https://attack.mitre.org/techniques/T1068))：攻击者可能利用软件漏洞来尝试收集提升的特权。当攻击者利用程序，服务或操作系统软件或内核本身内的编程错误来执行攻击者控制的代码时，就会利用软件漏洞。诸如权限级别之类的安全性结构通常会阻碍信息的访问和某些技术的使用，因此对手可能需要执行特权升级，甚至包括使用软件开发来规避这些限制。

组策略修改([Group Policy Modification](https://attack.mitre.org/techniques/T1484))：攻击者可能会修改组策略对象（GPO），以颠覆域的预期设置的自由访问控制机制，通常是为了提升域的特权。

劫持执行流程([Hijack Execution Flow](https://attack.mitre.org/techniques/T1574))：攻击者可以通过劫持操作系统运行程序的方式来执行自己的恶意负载。劫持执行流可能出于持久性目的，同时也可以使用这些机制来提升特权或者规避防御。

流程注入([Process Injection](https://attack.mitre.org/techniques/T1055))：攻击者可以将代码注入到程序执行的流程中，从而规避基于流程的防御以及可能的特权提升。进程注入是一种在单独的活动进程的地址空间中执行任意代码的方法。

计划任务/工作([Scheduled Task/Job](https://attack.mitre.org/techniques/T1053))：所有主要操作系统中都存在的实用程序，用于计划要在指定日期和时间执行的程序或脚本。只要满足正确的身份验证，也可以在远程系统上安排任务。

有效账户([Valid Accounts](https://attack.mitre.org/techniques/T1078))：攻击者通过获取目标网络中的有效账户来获取网络中的数据，并以此为基础获得目标网络的访问权，同时也可以在目标网络中长期存在，进而可以提高权限规避目标网络内部的审查。有效账户中共有四类账户，分别为：默认账户，域账户，本地账户，云账户四类账户。

[Defense Evasion](https://attack.mitre.org/tactics/TA0005" \o ")

防御包括对手用来避免在整个攻击过程中被发现的技术。逃避防御所使用的技术包括卸载/禁用安全软件或对数据和脚本进行混淆/加密。攻击者还利用和滥用受信任的进程来隐藏和伪装其恶意软件。

滥用权限控制机制([Abuse Elevation Control Mechanism](https://attack.mitre.org/techniques/T1548))：对手可能会规避旨在控制提升特权以获得更高级别权限的机制。必须授予特定用户授权才能执行可以被认为具有较高风险的任务。对手可以执行多种方法来利用系统内置的控制机制来提升系统上的特权。

滥用权限控制机制除了应用在防御规避([Defense Evasion](https://attack.mitre.org/tactics/TA0005" \o "))中还应用在特权提升([Privilege Escalation](https://attack.mitre.org/tactics/TA0004" \o "))中。

操纵访问令牌([Access Token Manipulation](https://attack.mitre.org/techniques/T1134))：攻击者可以修改访问令牌以在不同的用户或系统安全性上下文下运行，以执行操作并绕过访问控制。

操纵访问令牌除了应用在防御规避([Defense Evasion](https://attack.mitre.org/tactics/TA0005" \o "))中还应用在特权提升([Privilege Escalation](https://attack.mitre.org/tactics/TA0004" \o "))中。

位工作([BITS Jobs](https://attack.mitre.org/techniques/T1197))：攻击者可能滥用BITS作业来在恶意代码执行后持续执行或清理。BITS为windows系统中的后台智能传输服务。

位工作除了应用在防御规避([Defense Evasion](https://attack.mitre.org/tactics/TA0005" \o "))中还应用在持久性潜入(Persistence)中

反混淆/解码文件或信息([Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140))：攻击者可能会使用混淆文件或信息来隐藏入侵的分析结果。他们可能需要使用单独的机制来解码或模糊处理该信息，具体取决于他们打算如何使用它。

直接访问卷([Direct Volume Access](https://attack.mitre.org/techniques/T1006))：攻击者可以直接访问卷(Volume)，以绕过文件访问控制和文件系统监视。 Windows允许程序直接访问逻辑卷。具有直接访问权限的程序可以通过分析文件系统数据结构直接从驱动器读取和写入文件。

执行护栏([Execution Guardrails](https://attack.mitre.org/techniques/T1480))：对手可以使用执行防护栏基于目标提供的对手和特定于环境的条件来限制执行或操作。护栏确保仅对预定目标执行有效载荷，并减少敌方攻击造成的附带损害。

在这里所提到的防护栏更像模拟沙盒一类的模拟环境。作用是可用于在不希望受到损害或在其中运行的环境中暴露功能。

规避防御开发([Exploitation for Defense Evasion](https://attack.mitre.org/techniques/T1211))：攻击者可能利用系统或应用程序漏洞来绕过安全功能。在防御性安全软件中可能存在漏洞，可以使用这些漏洞来禁用或规避它们。

修改文件和目录权限([File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222))：攻击者可以修改文件或目录的权限/属性，以逃避访问控制列表（ACL）和访问受保护的文件。文件和目录权限通常由文件或目录所有者或具有适当权限的用户配置的ACL管理。

组策略修改([Group Policy Modification](https://attack.mitre.org/techniques/T1484))：攻击者可能会修改组策略对象（GPO），以颠覆域的预期设置的自由访问控制机制，通常是为了提升域的特权。

组策略修改除了应用在防御规避([Defense Evasion](https://attack.mitre.org/tactics/TA0005" \o "))中还应用在特权提升([Privilege Escalation](https://attack.mitre.org/tactics/TA0004" \o "))中。

隐藏文件([Hide Artifacts](https://attack.mitre.org/techniques/T1564))：攻击者可能试图隐藏与其行为相关的文件，以逃避检测。操作系统可能具有隐藏各种文件的功能，例如重要的系统文件和管理任务执行，以避免破坏用户的工作环境并防止用户更改系统上的文件或功能。攻击者可能滥用这些功能来进行隐藏文件，目录，用户帐户或其他系统活动之类的工件，以逃避检测。

劫持执行流程([Hijack Execution Flow](https://attack.mitre.org/techniques/T1574))：攻击者可以通过劫持操作系统运行程序的方式来执行自己的恶意负载。劫持执行流可能出于持久性目的，同时也可以使用这些机制来提升特权或者规避防御。

劫持执行流程除了应用在防御规避([Defense Evasion](https://attack.mitre.org/tactics/TA0005" \o "))中还应用在持久性潜入(Persistence)和特权提升([Privilege Escalation](https://attack.mitre.org/tactics/TA0004" \o "))中。

损害防御机制([Impair Defenses](https://attack.mitre.org/techniques/T1562))：攻击者可能会恶意修改受害者环境的组件，以阻止或禁用防御机制。这不仅会削弱被感染系统的防火墙和防病毒等预防性防御功能，而且同时还会弱化防御者可以用来检测活动和识别恶意行为的检测功能。通过恶意修改环境组件，还可能会影响到本机防御以及用户和管理员安装的补充功能。

卸掉主机的指示符([Indicator Removal on Host](https://attack.mitre.org/techniques/T1070))：攻击者可能会删除或更改主机系统上生成的文件，包括日志或捕获的文件。通过这些操作可能会干扰被攻击系统的事件收集，报告或其他用于检测入侵活动的通知。导致发生未报告的重大事件，这可能会损害安全解决方案的完整性。由于缺乏足够的数据来确定发生了什么，该活动还可能会妨碍分析机制对其进行分析和响应。

执行间接命令([Indirect Command Execution](https://attack.mitre.org/techniques/T1202))：攻击者可能滥用允许命令执行的实用程序，从而绕过限制命令行解释器使用的安全限制。可能会使用各种Windows实用程序来执行命令，而可能无需调用cmd。

伪装([Masquerading](https://attack.mitre.org/techniques/T1036))：攻击者可能试图操纵其文件的特征，以使其对用户和/或安全工具显得合法或良性。当为了逃避防御和观察而操纵或滥用合法或恶意物体的名称或位置时，就会发生伪装。这可能包括处理文件元数据，诱使用户误认文件类型以及提供合法的任务或服务名称。

修改身份验证过程([Modify Authentication Process](https://attack.mitre.org/techniques/T1556))：攻击者可能会修改身份验证机制和流程，以访问用户凭据，或者启用未经授权的帐户访问。

修改云计算基础框架([Modify Cloud Compute Infrastructure](https://attack.mitre.org/techniques/T1578))：攻击者可能试图修改云帐户的计算服务基础结构以规避防御。对云计算服务基础结构的修改可以包括创建，删除或修改一个或多个组件。

修改注册表([Modify Registry](https://attack.mitre.org/techniques/T1112))：攻击者可以与Windows注册表进行交互，以在注册表项中隐藏配置信息，作为清理的一部分或作为其他有助于持久性和执行的技术的一部分，删除信息。

混淆的文件或信息([Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027))：攻击者可能试图通过加密，编码或其他方式混淆可执行文件或文件在系统中或传输过程中的内容，以使其难以发现或分析，这种方法可以跨不同的平台和网络使用。

在操作系统之前启动([Pre-OS Boot](https://attack.mitre.org/techniques/T1542))：在计算机的引导过程中，将在操作系统之前加载固件和各种启动服务。这些程序控制操作系统启动之前的执行流程。因为这些数据位于操作系统的下一层，由于基于主机软件的防御检测不到这一层，所以这很难被检测。

在操作系统之前启动除了应用在防御规避([Defense Evasion](https://attack.mitre.org/tactics/TA0005" \o "))中还应用在持久性潜入(Persistence)中。

流程注入([Process Injection](https://attack.mitre.org/techniques/T1055))：攻击者可以将代码注入到程序执行的流程中，从而规避基于流程的防御以及可能的特权提升。进程注入是一种在单独的活动进程的地址空间中执行任意代码的方法。

流程注入除了应用在防御规避([Defense Evasion](https://attack.mitre.org/tactics/TA0005" \o "))中还应用在特权提升([Privilege Escalation](https://attack.mitre.org/tactics/TA0004" \o "))中。

流氓域控制器([Rogue Domain Controller](https://attack.mitre.org/techniques/T1207))：对手可能会注册恶意域控制器以启用对Active Directory数据的操作。 DCShadow可以用于创建恶意域控制器（DC）。

根套件([Rootkit](https://attack.mitre.org/techniques/T1014))：攻击者可能使用rootkit来隐藏程序，文件，网络连接，服务，驱动程序和其他系统组件的存在。 Rootkit是通过拦截/钩住和修改提供系统信息的操作系统API调用来隐藏恶意软件存在的程序。

签名的二进制文件代理([Signed Binary Proxy Execution](https://attack.mitre.org/techniques/T1218))：攻击者可以通过使用签名的二进制文件代理恶意内容的执行来绕过基于过程和/或基于签名的防御。使用受信任的数字证书签名的二进制文件可以在受数字签名验证保护的Windows系统上执行。

执行签名脚本代理([Signed Script Proxy Execution](https://attack.mitre.org/techniques/T1216))：攻击者可以使用用受信任证书签名的脚本来代理恶意文件的执行。 Windows安装中默认使用的几种Microsoft签名脚本可用于代理其他文件的执行。

颠覆信任执行([Subvert Trust Controls](https://attack.mitre.org/techniques/T1553))：攻击者可能破坏安全控制，从而警告用户不信任的活动或阻止执行不信任的程序。操作系统和安全产品可能包含将程序或网站标识为具有某种程度的信任的机制。

交通信号([Traffic Signaling](https://attack.mitre.org/techniques/T1205))：攻击者可能使用流量拦截来隐藏开放端口或其他用于持久性或命令和控制的恶意功能。流程是：在打开端口之前，发送带有某些特征的数据包，以使对手可以将其用于命令和控制。

交通信号不止能用在防御规避([Defense Evasion](https://attack.mitre.org/tactics/TA0005" \o "))中还应用在持久性潜入(Persistence)中

执行受信任的开发人员实用程序代理([Trusted Developer Utilities Proxy Execution](https://attack.mitre.org/techniques/T1127))：对手可能会利用受信任的开发人员实用程序来代理恶意负载的执行。这些实用程序通常可以使用合法证书进行签名，以使它们可以在系统上执行并通过有效绕过应用程序控制解决方案的受信任进程代理执行恶意代码。

未使用/不受支持的云区域(Unused/Unsupported Cloud Regions)：攻击者可能会在未使用的地理服务区域中创建云实例，以逃避检测。通常是通过破坏用于管理云基础架构的帐户来获得访问权限。

使用备份身份验证材料([Use Alternate Authentication Material](https://attack.mitre.org/techniques/T1550))：攻击者可以使用备用身份验证材料，例如哈希密码，Kerberos票证和应用程序访问令牌，以便在环境中横向移动并绕过正常的系统访问控制。

有效账户([Valid Accounts](https://attack.mitre.org/techniques/T1078))：攻击者通过获取目标网络中的有效账户来获取网络中的数据，并以此为基础获得目标网络的访问权，同时也可以在目标网络中长期存在，进而可以提高权限规避目标网络内部的审查。有效账户中共有四类账户，分别为：默认账户，域账户，本地账户，云账户四类账户。

有效账户几乎可以用在 ATP攻击所有的流程中。

虚拟化/沙盒规避([Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497))：对手可以采用各种手段来检测并避免虚拟化和分析环境。这可能包括根据检查指示虚拟机环境（VME）或沙箱的文件是否存在的结果来更改行为。

XSL脚本处理([XSL Script Processing](https://attack.mitre.org/techniques/T1220))：攻击者可以通过将脚本嵌入XSL文件中来绕过应用程序控制并模糊代码的执行。可扩展样式表语言（XSL）文件通常用于描述XML文件中数据的处理和呈现。为了支持复杂的操作，XSL标准包括对各种语言的嵌入式脚本的支持。