ID：T1189

战术：初始访问

平台：Windows、Linux、MacOS

所需权限：用户

数据源：数据包捕获、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

drive-by compromise

drive-by compromise 是，攻击者通过用户正常浏览过程中访问一个网站而获得对系统的访问权。使用这种技术，用户的 Web 浏览器将成为攻击的目标。这可以通过几种方式实现，但有几个主要组成部分：

多种向浏览器提交漏洞代码的方法，包括：

一个合法的网站被攻陷，被攻击者注入了某种形式的恶意代码（如 javascript、iframes、跨站点脚本）

恶意广告，通过合法的广告提供商支付和提供服务。

内置的 Web 应用程序接口可用于插入任何其他类型的对象，这些对象可用于显示 Web 内容或包含在访问客户端上执行的脚本（例如论坛帖子、评论和其他用户可控制的 Web 内容）。

通常，攻击者使用的网站是特定的人群会访问的网站，例如政府、特定行业或地区，其目标是基于共享的兴趣来危害某一个特定用户或一组用户。这种有针对性的攻击是指一种战略性的网络攻击或水坑攻击。有几个已知的例子说明了这一点。〔1〕

典型 drive-by compromise 过程：

用户访问攻击者控制的网站。

脚本会自动执行，通常根据浏览器和插件的版本搜索易受攻击的版本。

有时候需要用户通过启用脚本或激活网站组件并忽略警告对话框。

一旦发现一个易受攻击的版本，漏洞代码就会被发送到浏览器。

如果攻击成功，那么攻击者的代码将在用户系统上，除非有其他保护措施。

在某些情况下，在执行漏洞代码之前，需要用户在初始扫描后再次访问网站。

与利用面向公共的应用程序不同，此技术的重点是在目标访问网站时利用客户端端点上的软件漏洞。这通常会让攻击者获取访问内部网络系统的权限，而不是 DMZ 中的外部系统。

APT19　2014 年，APT19 在福布斯网站上进行了一次水坑攻击，以破坏目标。

APT32　APT32 通过诱骗受害者访问泄密的水坑网站来感染他们。

缓解

drive-by compromise 依赖于客户端系统上存在易受攻击的软件。使用打开安全功能的现代浏览器。确保所有浏览器和插件都保持更新，可以防止这种技术的漏洞利用阶段。对于通过广告进行攻击的恶意代码，adblocker 可以帮助防止代码执行。脚本阻塞扩展工具可以帮助防护在利用过程中可能常用的 javascript 的执行。
浏览器沙箱可以用来减少一部分漏洞的影响，但沙盒可以逃逸。
其他类型的虚拟化和应用程序微细分也可以减轻客户端开发的影响。额外利用的风险和实施中的弱点可能仍然存在。〔20〕
安全应用程序可以查找在攻击过程中使用的行为，例如 WDEG 和增 EMET,可以缓解某些攻击行为。[21]控制流完整性检查是识别和阻止软件漏洞发生的另一种方法。[22]其中许多防护技术依赖于体系结构和目标应用程序二进制的兼容性。

检测

防火墙和代理可以检查 URL 中潜在的已知坏 domain 或参数。他们还可以对网站和他们请求的资源进行基于声誉的分析，例如域名的历史、注册对象、黑名单中，或者有多少其他用户以前连接过它。

网络入侵检测系统，有时用 SSL/TLS MITM 检查，可以用来查找已知的恶意脚本（Reon，heap spray，和浏览器标识脚本已经被频繁重用），通用脚本混淆，漏洞利用代码。

从合法的网站上检测基于漏洞攻击的失陷可能是困难的。还可以在端点系统上查找可能表明失陷的行为，例如浏览器进程的异常行为。这可能包括写入可疑文件、试图隐藏执行的进程注入证据、可以证明向系统传送了其他工具的异常网络流量

Aomic test:

No

规则：

No

ID：T1190

战术：初始访问

平台：Linux、Windows、MacOS

数据源：数据包捕获、Web 日志、Web 应用程序防火墙日志、应用程序日志

利用面向公众的应用程序

使用软件、数据或命令来利用面向因特网的计算机系统或程序中的弱点，以引起意外或不可预料的行为。系统中的弱点可能是缺陷、故障或设计漏洞。这些应用程序通常是网站，但可以包括数据库（如 SQL）[1]、标准服务（如 SMB[2]或 SSH）和任何其他具有 Internet 可访问开放套接字的应用程序，如 Web 服务器和相关服务。[3]根据所利用的缺陷这可能包括利用 “防御逃逸 “。
对于网站和数据库，OWASP top 10 给出了前 10 名最常见的基于 Web 的漏洞。

缓解

应用程序隔离和最小特权原则有助于减少漏洞的影响。应用程序隔离将限制被利用目标可以访问的其他进程和系统功能，服务帐户的最低权限将限制被利用进程对系统其余部分获得的权限。Web 应用程序防火墙可用于限制应用程序的对外暴露。
使用 DMZ 或独立的托管基础设施将面向外部的服务器和服务与内网的其余部分进行分段。

在设计用于部署到外部可访问系统的自定义软件时，请使用安全编码最佳实践准则。避免 OWASP、CWE 和其他软件缺陷识别工作记录的问题。
定期扫描外部可访问系统的漏洞，并建立流程，以便在通过扫描和公开披露发现关键漏洞时快速修补系统。

检测

监视应用程序日志中是否存在可能表明尝试或成功利用的异常行为。使用深度包检查来查找常见的漏洞攻击流量的组件，如 SQL 注入。Web 应用程序防火墙可能检测到试图利用漏洞的不正确输入。

ID：T1200

策略：初始访问

平台：Windows、Linux、MacOS

数据来源：资产管理、数据丢失预防

硬件添加(Hardware Additions)

计算机附件、计算机或网络硬件可以作为一种媒介引入系统以获得执行。虽然 APT 组使用此方法的公开参考很少，但许多渗透测试人员利用硬件添加进行初始访问。商业和开源产品经常被使用，他们有如下的功能：passive network tapping [1]、中间人加密破解[2]、键盘输入注入[3]、通过 DMA 读取内核内存[4]、为现有网络添加新的无线访问[5]等功能。

缓解

建立网络访问控制策略，例如使用设备证书和 802.1X 标准。[6]限制对已注册设备使用 DHCP，以防止未注册设备与受信任系统通信。
通过端点安全配置和监视代理阻止未知设备和附件。

检测

资产管理系统可能有助于检测不应存在于网络内的计算机系统或网络设备。
端点安全设备可以检测通过 USB、Thunderbolt 和其他外部设备通信端口添加的新设备。

ID：T1091

策略：横向移动，初始进入

平台：Windows

所需权限：用户

数据源：文件监控、数据丢失预防

Replication Through Removable Media 通过可移动媒体传播

攻击者可以通过将恶意软件复制到可移动介质上，并利用介质插入系统时自动执行的功能，将恶意软件转移到系统上，包括那些处于隔离网络上的系统。在横向移动的情况下，这个战术可以通过修改存储在可移动媒体上的可执行文件或通过复制恶意软件并将其重命名为合法文件来欺骗用户在隔离的系统上执行。在初始访问的情况下，可能通过手动操作介质、修改用于初始格式化介质的系统或修改介质固件本身来实现。

缓解

如果不必要，请禁用自动运行功能。[11]如果业务操作不需要可移动介质，则在组织策略级别上禁用或限制可移动介质。〔12〕
识别可能用于感染可移动介质或可能由受污染的可移动介质传播的潜在恶意软件，并通过使用白名单[13]工具（如 AppLocker，[14][15]或软件限制策略[16]）进行审计和/或阻止。〔17〕

检测

监视可移动介质上的文件访问。检测在装入可移动介质后或由用户启动时从该介质执行的进程。如果以这种方式使用远程访问工具进行横向移动，那么执行之后可能会发生其他操作，例如打开网络连接以进行命令和控制以及系统和网络信息发现。

ID：T1193

策略：初始访问

平台：Windows、MacOS、Linux

数据来源：文件监控、数据包捕获、网络入侵检测系统、电子邮件网关、邮件服务器

Spearphishing Attachment　鱼叉式邮件附件

鱼叉式邮件附件是鱼叉式攻击的特定变体。鱼叉式邮件附件与其他形式的鱼叉式攻击不同，它使用电子邮件附件来投递恶意软件。所有形式的网络钓鱼都是针对特定个人、公司或行业的电子交付的社会工程学。在这种情况下，攻击者会将一个文件附加到鱼叉式攻击邮件上，依靠用户执行来获得执行的机会。
附件有许多方式，如 Microsoft Office 文档、可执行文件、PDF 或存档文件。打开附件（可能通过单击过掉保护）后，攻击者的有效负载会利用漏洞或直接在用户系统上执行。鱼叉式电子邮件的文本通常试图给出打开该文件的合理理由，并可能解释如何绕过系统保护才能打开该文件。邮件还可能包含有关如何解密附件（如 zip 文件密码）的说明，以避免电子邮件边界防御设备。攻击者经常伪装文件扩展名和图标，以使附加的可执行文件看起来像文档文件，或者利用一个应用程序的文件看起来像是另一个应用程序的文件。

缓解

网络入侵预防系统和旨在扫描和删除恶意电子邮件附件的系统可用于阻止这个活动。解决方案可以基于签名和行为，但攻击者可以通过某种方式构建附件来绕过这些安全系统。
默认情况下，阻止不应通过电子邮件传输的未知或未使用的附件是一种很好的办法，可以防护某些攻击向量，如.scr、.exe、.pif、.cpl 等。某些电子邮件扫描设备可以打开和分析压缩和加密格式，如 zip 和 rar，这些格式可用于隐藏混淆文件中的的恶意附件。
因为这项技术在端点上涉及用户交互，所以很难完全缓解。然而，也有潜在的缓解措施。用户可以接受培训，以识别社会工程技术和鱼叉式电子邮件。为了防止附件执行，可以使用应用程序白名单。反病毒程序也可以自动隔离可疑文件。

检测
网络入侵检测系统和电子邮件网关可用于检测带有恶意附件的鱼叉式电子邮件。Detonation chambers 也可用于识别恶意附件。解决方案可以基于签名和行为，但攻击者可以通过某种方式构建附件来绕过这些系统。
当恶意文档和附件被扫描到存储在电子邮件服务器或用户计算机上时，反病毒程序可能会检测到它们。一旦打开附件（如 Microsoft Word 文档或 PDF 尝试访问 Internet 或生成 PowerShell.exe）并尝试通过漏洞利用来在客户端执行恶意代码，端点检测或网络检测设备可能会检测恶意事件，

ID：T1192

策略：初始访问

平台：Windows、MacOS、Linux

数据源：数据包捕获、Web 代理、电子邮件网关、爆炸室、SSL/TLS 检查、DNS 记录、邮件服务器

Spearphishing Link　鱼叉式链接

带链接的鱼叉式攻击是鱼叉式攻击的特定变体。与其他形式的鱼叉式攻击不同的是，它把恶意软件的下载链接放在电子邮件中，而不是将恶意文件附加到电子邮件本身，以避免安全设备检查电子邮件附件。

所有形式的网络钓鱼都是针对特定个人、公司或行业的电子社会工程学。在这种情况下，恶意电子邮件包含链接。通常，链接将伴随社会工程学文字，并要求用户主动单击或复制 URL 并将其粘贴到浏览器中，然后让用户执行。被访问的链接可能会利用漏洞攻击 Web 浏览器，或者会提示用户下载应用程序、文档、zip 文件，甚至是可执行文件。攻击者还可能放入旨在与电子邮件阅读者直接交互的链接，包括直接利用最终系统或验证电子邮件是否接收（即网络漏洞/网络信标）的嵌入式图像。

缓解

因为这项技术在端点上涉及用户交互，所以很难完全缓解。然而，也有潜在的缓解措施。用户可以接受培训，以识别社会工程学和使用恶意链接的电子邮件。

检测

检查电子邮件中的 URL（包括扩展缩短的链接）可以检测已知恶意站点的链接。Detonation chambers 可以用来检测这些链接，或者自动进入这些站点以确定它们是否有潜在的恶意，或者等待用户访问链接时捕获内容。因为这种技术通常涉及到端点上的用户交互，许多可能的鱼叉式链接的检测方法都需要用户执行。

ID：T1194

策略：初始访问

平台：Windows、MacOS、Linux

数据来源：SSL/TLS 检查、反病毒、Web 代理

Spearphishing via service　通过第三方服务进行的鱼叉式攻击

通过第三方服务进行的鱼叉式攻击是鱼叉式攻击的一个特定变体。它不同于其他形式的鱼叉式攻击，因为它使用第三方服务，而不是直接通过企业电子邮件渠道。

所有形式的网络钓鱼都是针对特定个人、公司或行业的电子的社会工程学。在这种情况下，攻击者通过各种社交媒体服务、个人网络邮件和其他非企业控制的服务发送消息。与企业相比，这些服务的安全策略更不严格。和大多数的钓鱼行动一样，目的是与攻击目标建立融洽的关系，或者以某种方式获得攻击目标的兴趣。攻击者将创建假社交媒体账户，并向员工传达潜在就业机会的信息。这样就可以为询问在环境中运行的服务、策略和软件提供一个合理的理由。然后，攻击者可以通过这些服务发送恶意链接或附件。
一个常见的例子是通过社交媒体与攻击目标建立融洽关系，然后将内容发送到目标在其工作计算机上使用的个人电子邮件服务上。这能让攻击者绕过工作帐户上的一些电子邮件限制，而且攻击目标更可能打开文件，因为这些文件的内容是他们所期待看到的。如果有效载荷不能按预期工作，攻击者可以继续正常与被攻击目标交流，并协助目标排除故障让载荷工作起来。

缓解

确定某些社交媒体网站、个人网络邮件服务或其他可用于鱼叉式攻击的服务对于业务运营是否是必要的，并考虑在无法很好地监控这些第三方服务时或其存在重大风险时阻止访问。由于此技术涉及在端点上使用合法的服务和用户交互，因此很难完全缓解。然而，也有潜在的缓解措施。用户可以接受培训，以识别社会工程学技术和带恶意链接攻击的电子邮件。为了防止下载执行恶意文件，可以使用应用程序白名单。杀毒软件也可以自动隔离可疑文件。

检测

由于最常见的用于鱼叉式攻击的第三方服务都是利用 TLS 加密的，因此通常需要 SSL/TLS 检查来检测初始通信/传递。使用 SSL/TLS 检查入侵检测签名或其他安全网关设备可能能够检测恶意软件。杀毒软件可能会检测到下载到用户计算机上的恶意文档和文件。端点检测或网络检测设备可能会在打开文件（如 Microsoft Word 文档或 PDF 连接到 Internet 或生成 PowerShell.exe）后检测恶意事件行为。
ID：T1195

策略：初始访问

平台：Linux、Windows、MacOS

数据源：Web 代理、文件监视

Supply Chain Compromise　供应链攻击

供应链攻击是指在最终消费者收到产品之前，为了控制数据或系统而对产品或者产品交付机制进行的操纵。供应链攻击可以在供应链的任何阶段发生，包括：

开发工具的操纵

开发环境的操纵

操纵源代码存储库（公共或私有）

操纵软件更新/分发机制

受损/受感染的系统映像（工厂感染的多个可移动媒体案例）

用修改版本替换合法软件

向合法分销商销售改良/仿冒产品

禁止装运

虽然供应链攻击可能影响硬件或软件的任何组件，但想要让恶意软件执行的攻击者往往将注意力集中在软件分发或更新渠道对合法软件的恶意增加附件上。[1][2][3]目标可能是特定所需的受害者集[4]或恶意软件可能分发给广泛的消费者集，但仅限于针对特定受害者才进行下一步攻击。〔1〕〔3〕

缓解：
在系统的整个生命周期中应用供应链风险管理（SCRM） [7]，如供应链分析和适当的风险管理。
利用已建立的软件开发生命周期（SDLC） [8]：
用唯一标识物来标识供应链要素、流程和参与者
限制供应链内的访问和暴露
建立和维护元素、过程、工具和数据的来源数据

严格限制共享信息
执行 SCRM 培训
对系统、元素和过程使用防御设计
进行持续的集成审查
强化交付机制
确保维持活动和过程
管理整个系统或要素生命周期中的处置和最终处置活动

检测：
使用 hash 检查或其他完整性检查机制来验证分布式二进制文件。在部署之前扫描下载下来的文件是否匹配恶意签名，并尝试测试软件和更新软件，同时注意潜在的可疑活动。对硬件进行物理检查，确认是否被篡改。

ID：T1199
策略：初始访问
平台：Linux，Windows，macOS
数据源：应用程序日志，身份验证日志，第三方应用程序日志

Trusted Relationship　值得信赖的关系

攻击者可能会破坏或以其他方式利用有权访问目标受害者的组织。 通过受信任的第三方关系进行访问会利用可能不受保护的现有连接，或者会比标准的网络访问权限申请机制审查的更少。
很多机构通常给第二或第三方外部提供商提升访问权限，以允许他们管理内部系统。这些关系的包括 IT 服务承包商，托管安全提供商，基础设施承包商（例如 HVAC，电梯，物理安全）。 第三方提供商的访问可能仅限于所维护的基础架构，但可能与企业的其他部分存在于同一网络中。 因此，用于访问内部网络系统的其他有效帐户可能会受到攻击和使用。

缓解

网络分段可用于隔离不需要大范围网络访问的基础架构组件。正确管理信任关系中各方使用的帐户和权限，以最大限度地减少当事人滥用的风险，以及当某些人已经被攻击者拿到权限后也可以减少风险。检查需要特权访问网络资源的组织的安全策略和过程。

检测：

建立对第二和第三方提供商以及其他可信实体进行的活动的监控，这些活动可以用作获取网络访问权的手段。根据关系的类型不同，攻击者可以在执行操作之前访问有关目标的大量信息，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对目标采取行动，因此对于与凭据访问，横向移动和收集相关的行为进行适当的监控对于检测入侵非常重要。

ID：T1078
战术：防御逃避，持久性，特权升级，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：身份验证日志，进程监控
防御绕过：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

Valid Accounts　有效帐户

攻击者可以使用凭证访问技术窃取特定用户或服务帐户的凭据，或者在其侦察过程中通过社交工程获取凭据以获取初始访问权限。
失陷的凭证可用于绕过对网络内系统上的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。失陷的凭证还可以给攻击者对特定系统提高访问权限或对受限区域的提供访问权限。攻击者可以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，以使其更难以检测其存在。
攻击者还可以创建帐户，有时使用预定义的帐户名和密码，通过备份访问进行持久化，以防其他方法失败。
跨越系统网络的凭证和许可的重叠应该被关注，因为攻击者可能能够跨帐户和系统进行转换以达到高级别的访问（即，域或企业管理员）以绕过在企业内设置的访问控制。 [1]

缓解：

采取措施检测或阻止凭证转储或安装键盘记录程序等技术。限制跨系统的凭据重叠，以防止在帐户凭据被获取后用于登录其他系统。确保本地管理员帐户在网络上的所有系统中都具有复杂，唯一的密码。不要将用户或管理域帐户放在跨系统的本地管理员组中，除非它们受到严格控制并且帐户的使用是分段的，因为这通常等同于在所有系统上使用具有相同密码的本地管理员帐户。遵循设计和管理企业网络的最佳实践，以限制跨管理层的特权帐户使用。 [29]。审核域和本地帐户以及他们的权限级别，查找是否存在可能让攻击者通过获取特权账户凭证来获得广泛访问权限的情况。 [1] [30]

检测：
在整个企业中使用配置健壮，一致的帐户活动审核策略，对外部可访问的服务也是如此。 [31]查找系统之间共享帐户（用户，管理员或服务帐户）的可疑帐户行为。示例：一个帐户同时登录多个系统;多个帐户同时登录到同一台机器;帐户在奇怪时间或营业时间之外登录。活动可以来自交互式登录会话或来自用于在远程系统上作为特定帐户执行二进制文件的进程所有者。将其他安全系统与登录信息相关联（例如，用户具有活动登录会话但尚未进入建筑物或者没有 VPN 访问权限）。
定期审核域和本地系统帐户，以检测攻击者为持久化创建的帐户。