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，