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。