FIREEYE™

FireEye SmartVision

检测企业网络中的可疑横向移动

亮点

- 检测以前无法检测到的可疑横向移动
- 帮助发现网络中可疑网络流量
- 采用先进的网络事件关联和分析引擎、机器学习技术和 120 多种技术入侵检测规则
- 作为 FireEye 网络安全的一部分，支持各种部署

当今不断变化的威胁形势

当今的威胁形势继续发展，使得阻止复杂攻击者的预防措施越来越不可靠。“强行夺取”的攻击时代已经结束。一旦进入网络，当今的攻击者可能会在被破坏的环境中保持活跃状态，进行秘密的内部侦察以完成他们的任务：窃取您的宝贵信息。

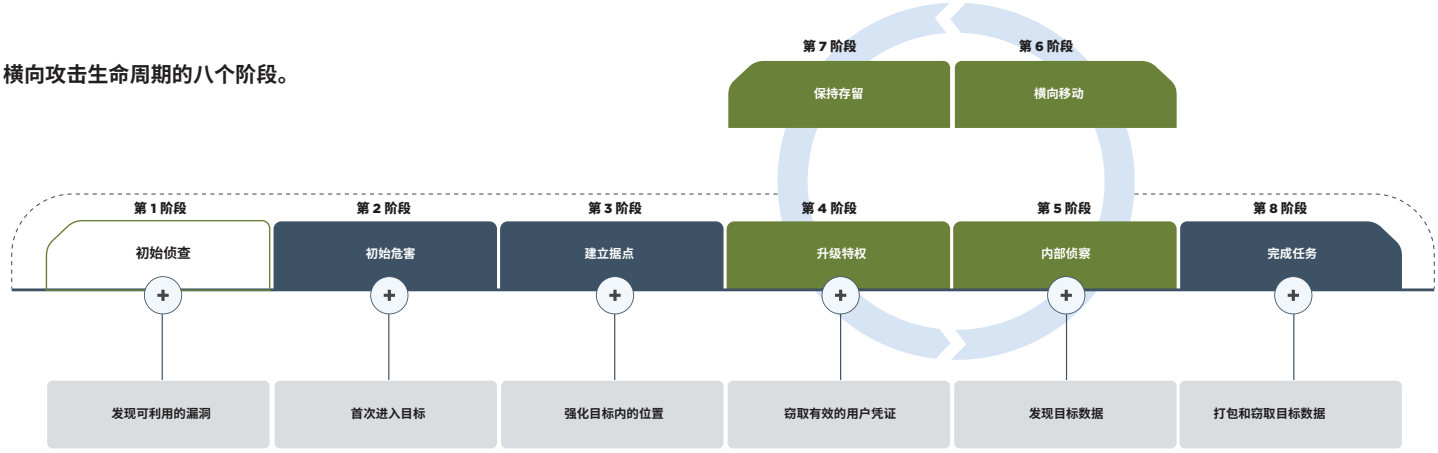
与此同时，改进的反取证技术让攻击者可以掩盖他们的横向“东-西”运动并隐藏他们的电子轨迹。这些网络犯罪分子经常为每个受损系统加载具有独特配置的自定义后门，以便他们可以维护未来的入口和网络访问。

入侵后检测所面临的挑战

不幸的是，目前可用于检测入侵后横向活动的工具有局限性，或根本无法检测到这些活动。例如，由于其繁琐的设置和复杂的管理，安全信息和事件管理系统 (SIEM) 经常错过横向移动，或者更糟糕的是，产生大量的误报警，使安全团队负担过重。

许多组织部署多个防火墙以限制攻击者的移动并控制对有限网段的损害。除了这种方法的高成本和复杂性之外，防火墙通常无法检测并阻止可疑的横向移动，因为攻击者已经获得了一定程度的信任、凭据访问权，从而完全绕过了防火墙。

横向攻击生命周期的八个阶段。



FireEye SmartVision

FireEye 已经确定了几个独特的指标和操作，这些指标和操作可以表明内部窃取数据所作的努力。凭借这种情报，FireEye 开发了 FireEye SmartVision™，这是一种检测以前无法检测到的横向移动攻击的新功能。

与 FireEye 网络安全平台结合使用时，SmartVision 允许安全管理员检测各种可疑的横向移动，从而帮助发现周边以及网络核心和服务器内可疑网络流量。

SmartVision 的核心组件包括：

高级关联和分析引擎

机器学习模块，用于检测数据泄露尝试

120 多种入侵检测规则，用于识别弱损害指标 (IOC)

SmartVision 如何检测无法检测到的活动

SmartVision 可检测企业网络中的大量恶意活动。由于攻击者在横向攻击生命周期中的移动所表现出的独特特征，SmartVision 可以键入特定的活动来触发警报。

特权升级阶段

在此阶段，SmartVision 确定：

- **“哈希值传递”攻击：**这种黑客技术允许攻击者通过使用用户密码的基础 NTLM 或 LanMan 哈希值向远程服务器或服务进行身份验证。
- **无文件恶意软件：**SmartVision 可检测无文件恶意软件，如“mimikatz”，这是一种用于提取纯文本密码、哈希值、PIN 码和 Kerberos 票据的著名工具。

内部侦察阶段

在此阶段，FireEye Network SmartVision 识别：

- **映射网络：**攻击者可使用基于 SNMP 的方法、主动探测或路由分析来发现网络上的设备（如端点和服务器）、其操作系统信息及其连接状态。
- **主机和服务枚举：**攻击者使用发现工具收集有关用户名、工作组、共享资源、开放端口、远程主机和其他网络服务的信息。
- **用户搜索：**为了确定谁拥有管理权限，攻击者利用使用 WinAPI 调用的工具，这提供有关服务器、Active Directory、域控制器和端点上的用户帐户信息。

横向移动阶段

在此阶段，SmartVision 可识别 SMB 协议上的流量，攻击者使用 SMB 和 SMB2 协议传输恶意软件、文件，特别是密码转储器。

数据泄漏阶段

在此阶段，SmartVision 通过其机器学习、数据泄漏模块检测与数据泄露相关的异常文件传输。

部署 SmartVision

作为 FireEye 网络安全环境的一部分，可以通过多种方式部署 SmartVision，以最好地满足网络设计和要求的任何组合。FireEye 网络安全传感器通常安装在面向服务器流量的内部防火墙后面。这允许传感器捕获客户端和服务器之间或对等系统之间的流量。

SmartVision 支持内联和带外部署，可用于内部部署和网络数据包代理/网络测试接入端口 (TAP) 环境。

总结

威胁形势继续发展，使得阻止复杂攻击者的预防措施越来越不可靠。因此，漏洞检测变得越来越重要，特别是当威胁者提高他们的能力轻松地通过网络偷偷移动时。

对横向攻击生命周期的剖析提出了现有安全解决方案无法完全解决的众多挑战。已经确定了几个独特的指标和操作，这些指标和操作可以表明内部窃取数据行为。

凭借这种情报，FireEye 开发了 SmartVision 作为一种创新解决方案，用于检测以前无法检测到的情况—横向移动攻击。现在，作为 FireEye 网络安全平台的一部分，SmartVision 可以部署在各种网络架构中，使企业能够了解横向威胁行为，帮助企业在威胁横向发展时保持安全。

若要了解更多关于 FireEye 的信息，请访问：**www.FireEye.com**

FireEye
26/F Time Square, 93 Middle Huaihai,
Huangpu, Shanghai, China
china@fireeye.com