合法软件感染特洛伊木马

利用 McAfee® 产品防止感染并减缓传播速度

通过互联网分发软件的机制可能会变成恶意软件和病毒攻击媒介。从十年前原始恶意联编程序出现，到如今合法软件在复杂的分发阶段之前或之中感染特洛伊木马，很明显取得了进步。

不管特洛伊木马程序复杂与否，其采用的基本步骤都一样：

- **软件“武器化”：**将恶意软件植入可传递的应用程序。
- **传递：**将未检测到的感染特洛伊木马的软件传输至攻击目标。
- **漏洞利用：**触发特洛伊木马程序代码，并设法规避检测。
- **安装：**建立据点，并尝试扩散。

最新的攻击技术采用了复杂的动态机制，在合法软件下载过程中植入恶意代码，从而规避检测。其采用的攻击原则是将原始应用程序与恶意代码捆绑在一起。

这种攻击技术可能会借助以下两个组件来找到可成功入侵目标的切入点：捕获并修改 HTTP 下载请求的侦听程序以及感染并分发二进制文件的联编程序。

最新的算法可部署恶意软件感染例程和网络重定向攻击，无需修改应用程序代码。这就为武器化商业或开源软件开启了方便之门，而且使其可以包含具有嵌入式签名的可执行文件。在首次尝试发起攻击之前，如未自动全面验证嵌入式签名，攻击则会成功。

一旦在攻击目标中启动感染特洛伊木马的应用程序，联编程序进程就会为其他嵌入式可执行文件创建其自身的文件，并在此文件中重建注入的所有代码，以便进一步发起攻击，并规避所有安全控制措施的检测。由于原始应用程序完好无损，因此，恶意软件可能会附加到包含签名的文件中，因此仍然可以成功。

策略和规程

最新的 McAfee® 网络防御最佳实践建议采用以下减轻网络和终端威胁的常规策略：

- 连接不受信任的网络时，应使用虚拟专用网。管理员应保持安全软件处于最新状态，并信任强有力的信任指标，而不是信任攻击中潜在的伪造指标。应对应用程序进行签名，并使用信任链进行验证。取证分析应包含带信任源的关联哈希。
- 不管是否检测初始二进制文件，安全软件都应执行动态分析来标记无管理系统操作，因为静态扫描仅限于此。在全面的解决方案中，行为监控、Web 和 IP 信誉、内存扫描以及应用程序遏制都是有用的措施。
- 供应商应通过安全连接下载应用程序，并对所有代码进行签名。这样就可以大幅减少中间人攻击。软件供应商应自我验证应用程序，定期审核应用程序的代码，使用静态代码分析工具分析代码，并执行对等项检查。建议创建受信任的企业应用程序库，并且仅允许用户从此应用程序库下载经过验证的安装程序。
- 应配置防恶意软件来确定是否存在联编程序。
- 应利用主机入侵检测和防范应用程序来检测数据包，从而确定恶意负载。
- 只使用与正确网段结合的受信任的虚拟化架构。受信任的虚拟化架构采用安全且可验证的引导进程。健全的网段可以监控通信量，并避免应用程序遭受成功利用漏洞发起的攻击。这种结合还可以防范恶意软件扩散。

- 通过监控出站通信，确定感染特洛伊木马的软件传递的恶意软件是否存在。通过监控计算机尝试发送至互联网的通信量，可能会发现受病毒感染的计算机，从而进一步采取补救措施。

McAfee 产品和解决方案

McAfee 产品和解决方案可以确定感染特洛伊木马的合法软件，识别和拦截嵌入式恶意软件威胁，发现入侵行为并快速做出响应。

McAfee VirusScan® Enterprise 8.8 或 McAfee Endpoint Security 10

- 保证 DAT 文件处于最新状态。
- 确保 **McAfee Global Threat Intelligence** (McAfee GTI) 已启用；McAfee GTI 可识别 6 亿多具有唯一性的恶意软件签名。
- 建立访问保护规则以阻止恶意软件安装和负载：
  - 请参阅访问保护规则知识库文章：KB81095 和 KB54812。
  - 请参阅 McAfee VirusScan 8.8 Enterprise 的最佳配置实践：**PD22940**。
  - 请参阅 McAfee Endpoint Security 的最佳配置实践：**KB86704**。

McAfee Host Intrusion Prevention

- McAfee Host Intrusion Prevention 可用于防范恶意软件扩散。利用自定义 IPS 签名，您可以创建规则来阻止恶意软件执行的文件操作（创建、写入、执行和读取等）。
- 启用 McAfee Host Intrusion Prevention 签名 3894，Access Protection—Prevent svchost.exe executing non-Windows executables（访问保护 - 可阻止 svchost.exe 执行非 Windows 可执行文件）。
- 启用 McAfee Host Intrusion Prevention 签名 6010 和 6011 可立即拦截植入恶意代码。
- 可利用以下两条子规则实现此目的：
  - 1)利用“Files”引擎和包含以下条件的子规则来创建自定义 IPS 签名：
    - Name: <插入名称>
    - Rule type: Files
    - Operations: Create, Execute, Read, Write
    - Parameters: Include - Files - <恶意软件路径/文件名>
      - 文件名必须包含路径。如果您想使用通配符表示路径，文件名开头请使用“**\”或“?:\”；如果您想使用通配符表示驱动器号，请使用“**\文件名.exe”或“?:\文件名.exe”。
      - 您不能使用包含“Files”参数的 MD5 哈希，则只能使用路径/文件名。
      - 您还可使用驱动器类型将路径限定为特定驱动器（例如，硬盘驱动器、CD-ROM、USB、网络和软盘）。
    - Executables: 可留空，除非您想将签名限定为执行文件操作的特定进程（例如，explorer.exe和cmd.exe 等）。
  - 2)利用“Program”引擎和包含以下条件的子规则来创

建自定义 IPS 签名：

- Name: <插入名称>
- Rule type: Program
- Operations: Run target executable
- Parameters: <保留为空>
- Executables:可留空，除非您想将签名作为源可执行文件限定为特定进程（例如，您想阻止 explorer.exe 运行 Target Executable（如 notepad.exe））。
- Target Executables: 定义要阻止执行的可执行文件属性（例如，如果您想阻止 notepad.exe 运行，可指定可执行文件的路径/文件名）。可通过一种或多种标准（如文件说明、文件名、指纹和签名者）来定义可执行文件。

McAfee SiteAdvisor® Enterprise 或 McAfee Web Protection

- 借助网站信誉来阻止用户使用分发特洛伊木马软件的网站或向用户发出警告。

McAfee Threat Intelligence Exchange 和 McAfee Advanced Threat Defense

- McAfee Threat Intelligence Exchange 策略配置：
  - 从观察模式开始：由于终端通过可疑进程发现，所以使用系统标记来应用 McAfee Threat Intelligence Exchange 实施策略。
  - 清理：Known Malicious（已知恶意）。
  - 拦截：Most Likely Malicious（很可能为恶意）的文件，拦截 Unknown（未知）文件可能会提供更好的防护，但也可能会增加初始管理工作负载。
  - 将“Unknown（未知）”信誉级别和更低级别的文件提交给 McAfee Advanced Threat Defense。
  - McAfee Threat Intelligence Exchange Server 策略：对于 McAfee Threat Intelligence Exchange 未识别的文件，接受 McAfee Advanced Threat Defense 提供的文件信誉。
- McAfee Threat Intelligence Exchange 人工干预：
  - 文件信誉强制实施（取决于操作模式）。Most likely malicious（很可能为恶意）：清理/删除。
  - Might be malicious（可能为恶意）：拦截。
- 企业（组织）提供的文件信誉优先于 McAfee Global Threat Intelligence。
  - 您可以选择阻止某个不需要的进程，比如不支持或有漏洞的应用程序。
  - 将文件标记为 Might be Malicious（可能为恶意）。
- 或选择“测试”某个不需要的进程：
  - 将文件标记为 Might be Trusted（可能为被信任的文件）。

McAfee Advanced Threat Defense

- 收件箱检测能力：
  - 基于签名的检测：McAfee Labs 维护的签名有 6 亿多个。
  - 基于信誉的检测：McAfee Global Threat Intelligence
  - 实时静态分析和模拟：用于无签名检测
  - 自定义 YARA 规则
  - 全静态代码分析：对文件代码实施逆向工程，以评估属性和功能集，并访问但不执行全分析源代码。
  - 动态沙盒分析
- 创建其中可能会运行感染特洛伊木马的软件的分析器配置文件：
  - 通用操作系统：Windows 7、Windows 8、Windows 10。
  - 安装 Windows 应用程序（Word 和 Excel）并启用宏。
- 将分析器配置文件接入互联网：
  - 很多样本运行 Microsoft 文档中的脚本，这个脚本进行出站连接并可能激活恶意软件。为分析器配置文件提供互联网连接可提高检测率。

McAfee Network Security Platform

- Network Security Platform 的默认策略中包含签名，用以检测可用来传输恶意软件相关文件的 TOR 网络。
- 与 McAfee Advanced Threat Defense 集成，可以防御各种攻击的新变体：
  - 在“高级恶意软件策略”中配置与 McAfee Advanced Threat Defense 集成。
  - 配置 McAfee Network Security Platform，以便将 .exe 文件、Microsoft Office 文档、Java 存档和 PDF 文件发送至 McAfee Advanced Threat Protection 以进行检测。
  - 验证 McAfee Advanced Threat Protection 配置是否在传感器级别应用。
- 更新回拨检测策略（以抗击僵尸网络）。

McAfee Web Gateway

- 启用 McAfee Gateway Anti-Malware 防恶意软件检测功能。
- 启用 McAfee Global Threat Intelligence 的 URL 和文件信誉功能。
- 与 McAfee Advanced Threat Defense 集成以实现沙盒和零日检测。

VirusTotal Convicter：自动干预

- Convicter 是一种 Python 脚本，可由 **McAfee ePolicy Orchestrator®** (McAfee ePO™) 自动响应系统触发，从而交叉引用由 VirusTotal 提供给 McAfee Threat Intelligence Exchange 的威胁事件文件。
- 可更改此脚本以参照其他 Threat Intelligence Exchange，例如 GetSusp。
- 如果达到了信任社区的阈值，此脚本会自动设置企业信誉。建议的确认阈值：30% 的供应商以及两家主要供应商必须认同此阈值。
- 过滤器：“Target file name does not contain（目标文件名不包含）：McAfeeTestSample.exe。”
- 这是一款社区支持的免费工具（McAfee 不支持）。

McAfee Endpoint Threat Defense and Response

- McAfee Endpoint Threat Defense and Response 可发现高级威胁并作出响应。该工具用于防御由 McAfee Labs、Dell SecureWorks 或 ThreatConnect 提供的威胁源时，可搜索到新威胁，并在这些威胁找到机会扩散之前将其扼杀。
- 自定义收集器，可创建专用工具来发现和识别与感染特洛伊木马的应用程序相关的攻陷指标。
- 满足特定条件时，用户可创建触发和反应来定义操作。例如，发现哈希或文件名时，可自动运行“删除”操作。

延伸阅读

Best Practices for how to use McAfee Host Intrusion Prevention rules for a malware outbreak（使用 McAfee Host Intrusion Prevention 规则来应对恶意软件爆发的最佳实践）：**KB84507**

SIEM Orchestration: Orchestration Triggers Signs of Malware Infection and Anomalous Behaviors（SIEM Orchestration：恶意软件感染和异常行为的 Orchestration 触发信号）：**PD24830**

白皮书：**超越特征码的安全防护**

FAQs for Network Security Platform: Advanced Malware Detection（Network Security Platform 的常见问题解答：高级恶意软件检测）：**KB75269**

McAfee Web Gateway 产品手册：Web 过滤：**PD26339**

北京市东城区北三环东路 36 号
北京环球贸易中心 D 座 18 层，100013
电话：8610 8572 2000
www.mcafee.com/cn