McAfee
Together is power.

防范基于脚本的恶意软件

恶意软件作者通过利用诸如多态性、植入看门狗软件和撤消权限等技术突破检测机制。

过去十年，攻击者利用各种功能（如 Microsoft Windows Management Instrumentation (WMI) 和 Windows PowerShell）攻击终端，并且由于直接将恶意代码植入遭到入侵的主机的注册表，所以不会在磁盘上存储任何二进制文件，导致跟踪攻击更加困难。

基于脚本的感染已经出现了多年。尽管无文件恶意软件一般不会留下任何文件，但是在渗入系统主内存前，以前的恶意软件系列在发动初始攻击时会在磁盘上放置一个小二进制文件。

不过，脚本恶意软件利用的最新规避技术不会在磁盘上留下痕迹，导致通常依赖静态文件的检测技术更加难以发现。阅读《McAfee Labs 威胁报告：2017 年 9 月》，了解对基于脚本的恶意软件的深入分析。

三种常见的基于脚本的恶意软件类型：

- **常驻内存型：**这种类型的恶意软件使用合法 Windows 文件的内存空间。它将代码加载到内存空间并保持常驻，直到被访问或重新激活。尽管是在合法文件的内存空间内执行，但是有用于启动或重新启动执行的休眠物理文件。
- **Rootkit：**一些恶意软件隐藏在用户或内核级应用程序编程接口 (API) 之后。它们在磁盘上有文件，但处于隐蔽模式。
- **Windows 注册表型：**一些高级脚本恶意软件类型驻留在 Windows 注册表中。恶意软件作者过去利用了各种功能，如用于存储资源管理器缩略图视图的图像的 Windows 缩略图缓存功能。缩略图缓存功能一直都是一种攻击机制。这种类型的恶意软件仍然必须通过静态二进制文件进入受害者的系统。大多数使用电子邮件作为找到系统的攻击媒介。一旦用户点击附件，恶意软件就会在 Windows 注册表配置单元中以加密形式写入完整的负载文件。随后，它会通过删除自身而从系统中消声灭迹。

现在，恶意软件作者会精心制作脚本恶意软件系列来执行完全无文件的 Windows 注册表攻击，而不会在文件系统中留下任何痕迹。尽管发起这些攻击的环境是通过在文件中执行代码来准备的，但文件会在系统准备进行恶意操作后自行删除。

防范基于脚本的恶意软件的策略和步骤

最新 McAfee 网络防御最佳实践建议采用以下常规策略来减轻网络和终端威胁：

- 保护系统免受脚本恶意软件感染的最佳方法是，在受感染之前就予以阻止。防御是关键。防御计算机感染各种恶意软件的最重要因素是用户。用户需要知道，下载和安装不了解或不信任的应用程序存在风险。另外，不知情的用户在浏览时，可能会不慎下载恶意软件。
- 对应用程序和操作系统应用安全更新和补丁。
- 保证 Web 浏览器和附加项是最新版本，并将终端上的防恶意软件和网络网关升级和更新为最新版本。
- 绝不使用不是企业 IT 安全团队分发和认证的计算机。脚本恶意软件可通过与企业网络连接的未受保护资产轻松传播。
- 在有本地管理员权限的用户自行安装应用程序时，指导用户仅安装已知供应商提供具有受信任特征码的应用程序。在线提供的一些应用程序看似“无害”，但嵌入 Rootkit 和其他脚本恶意软件类型的情况很常见。
- 切勿从非 Web 来源下载应用程序。从 Usenet 组、IRC 通道、即时消息客户端或对等网络下载到恶意软件的概率非常高。IRC 和即时消息中指向网站的链接也经常会连接到被感染的下载项。

- 针对阻止网络钓鱼攻击问题，实施教育计划。恶意软件通常通过有针对性的电子邮件进行分发。
- 结合防恶意软件技术，利用威胁情报源。结合使用有助于缩短新出现的和已知的恶意软件威胁的检测时间。

McAfee 如何帮助访问基于脚本的恶意软件

完全检测没有初始二进制文件的脚本恶意软件很棘手，往往要通过安全组织执行调查研究才能确定。但是，为了确保采取适当的控制措施来阻止攻击者攻击，保证切入点安全是阻止此类恶意软件的关键。

McAfee Endpoint Security

McAfee Endpoint Security (ENS) 提供了一个协作式安全框架来降低终端安全环境的复杂性，并且可以监控高级威胁（如脚本恶意软件），从而快速地检测并作出补救响应。它的可扩展架构提供了一个框架，从而让忙于应对多个解决方案的安全团队可以更轻松地查看、响应和管理威胁防御生命周期。

McAfee ENS 引入了多种新技术和改进：

- **Real Protect。**利用机器学习技术，根据代码形式，潜在行为（执行前分析）和具体行为（动态行为分析）识别恶意代码 — 无需特征码。Real Protect 是防范脚本恶意软件的一种有效防御策略。
- **动态应用程序遏制。**包括控制单个进程实例的功能。
- **McAfee Client Proxy 集成。**McAfee Endpoint Security 可以与多层 Web Gateway 安全结合使用，通过终端连接到 Web 网关云服务，消除脱机保护的差距，为旅行人士全程保驾护航。
- **防火墙模块。**由主动式安全策略保证的下一层保护机制是阻止您的计算机与网络犯罪分子控制的服务器之间的通信。
- **威胁防御模块。**按需扫描现在包括注册表扫描选项，对防范脚本恶意软件非常有用。管理员可以创建自定义服务访问保护规则，现在其中包括 Windows 服务。还与 McAfee 提供的入侵防护系统 (IPS) 特征码一起提供了自定义应用程序漏洞利用保护。最后，已将 Windows 应用程序保护添加到漏洞利用保护规则。

McAfee Advanced Threat Defense

McAfee Advanced Threat Defense (ATD) 是一款综合运用多个检查引擎的多层恶意软件检测产品。通过综合运用多个应用基于特征码和信誉的检查、实时模拟、全静态代码分析以及动态沙盒的检查引擎，McAfee ATD 可以防范最初在其目标系统中删除二进制文件的脚本恶意软件。

- **基于签名的检测：**检测病毒、蠕虫、间谍软件、僵尸程序、特洛伊木马、缓冲区溢出和混合型攻击。它全面的知识库由 McAfee Labs 创建和维护。

- **基于信誉的检测：**使用 McAfee Global Threat Intelligence (GTI) 查询文件的信誉，已检测各种新兴威胁。
- **实时静态分析和模拟：**提供实时静态分析和模拟，以快速查找基于特征码的技术或信誉未能识别的恶意软件和零日威胁。
- **全静态代码分析：**对文件代码实施逆向工程，以访问其所有属性和指令集，并且完全分析但不执行源代码。全面的解包能力可以打开所有类型的打包和压缩文件，以进行完整分析和恶意软件分类，从而使贵公司能够了解特定恶意软件所具有的威胁。
- **动态沙盒分析：**对于通过上述检测引擎无法建立安全的文件，McAfee ATD 可以在虚拟运行时环境中执行文件代码并观察由此引发的行为。可以根据主机环境来配置虚拟环境。

McAfee Threat Intelligence Exchange

拥有一个能够随时间不断调整的智能平台以满足环境要求是一件非常重要的事。McAfee Threat Intelligence Exchange (TIE) 可以大幅减少脚本恶意软件攻击，因为它能察觉各种即时威胁（如环境中正在执行的未知文件或应用程序）。

- **全面的威胁情报：**根据全球威胁情报数据源轻松定制全面的威胁情报。可以是 McAfee GTI 或第三方数据源，并且包含从通过终端、网关及其他安全组件传输的实时和历史事件数据收集而来的本地威胁情报。
- **执行防护和补救：**McAfee TIE 可以干预并防止未知应用程序在环境中执行。如果在允许运行后发现应用程序为恶意软件，那么 McAfee TIE 可以运用产品的强大的集中管理和策略实施能力在整个环境中禁用正在运行的与该应用程序相关的进程。
- **监控：**McAfee TIE 可以跟踪在环境中的所有打包可执行文件及其首次执行，以及之后执行的所有更改。这种对于应用程序或进程操作（从安装到当前状态）的可见性可以实现更加快速的响应和补救。
- **攻陷指标：**导入已知无效文件哈希并通过策略实施使您的环境免受这些已知无效文件威胁。如果在环境中触发任何攻陷指标，McAfee TIE 可以结束与该攻陷指标相关联的所有进程和应用程序。

McAfee Web Gateway

“随看随下”下载和嵌入网络钓鱼电子邮件中的恶意 URL 都是用于传递脚本恶意软件的主要攻击方法。McAfee Web Gateway (MWG) 是一款可以帮助贵公司防范此类威胁的强大产品。

- **Gateway Anti-Malware Engine：**无特征码意图分析功能会实时从 Web 流量中过滤恶意内容。模拟和行为分析可主动防范零日威胁和针对性威胁。Gateway Anti-Malware Engine 会检测文件，并在确定文件存在恶意企图后阻止用户下载文件。

- **集成 McAfee GTI：**带有 McAfee GTI 文件信誉、Web 信誉和 Web 分类功能的实时情报源可以防范最新威胁，因为 MWG 将拒绝尝试连接已知恶意网站或使用恶意广告网络的网站。除这些 McAfee 产品以外，我们还推荐了两款其他类型的安全技术。
  - **电子邮件网关安全：**大部分脚本恶意软件通过电子邮件的附件渗入系统，因此用来扫描所有恶意软件附件的功能强大的电子邮件网关安全产品应是可靠防御此类型攻击的必不可少的一部分。
  - **防火墙：**对于任何安全系统来说，最基本的安全技术是防火墙技术。防火墙可以检测到外围的许多威胁 — 在它们进入受信任的网络之前。由于脚本恶意软件是通过静态二进制文件进入系统，因此在许多攻击渗入受信任的网络中的系统之前就可以阻止它们。

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