停止后门特洛伊木马程序

Adwind 远程管理工具 (RAT) 是基于 Java 的后门特洛伊木马程序，旨在攻击支持 Java 文件的各种平台。Adwind 不利用任何漏洞。导致发生感染常见行为是，用户必须通过双击通常以邮件附件形式出现的 .jar 文件来执行恶意软件，或者打开受感染的 Microsoft Word 文档。如果用户安装了 Java Runtime Environment，则会开始发生感染。一旦恶意 .jar 文件得以在目标系统上成功运行，则恶意软件会悄悄地进行安装，并通过预配置端口接收远程攻击者发出的命令，从而连接到远程服务器，然后进一步执行恶意操作。

历史简介

Adwind 从 Frutas RAT 演变而来。Frutas 是基于 Java 的 RAT，最早在 2013 年初被发现，已广泛地用来抵御针对欧洲和亚洲的资深电信业、采矿业、政府和金融企业发起的网络钓鱼电子邮件传播活动。

从 2015 年第一季度开始，McAfee® Labs 发现以 Adwind 为标识进行提交的 .jar 文件的数量明显增加。

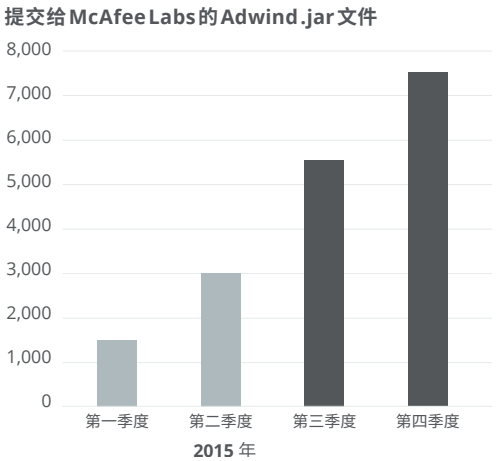

图 1. 提交到 McAfee Labs 的 Adwind .jar 文件的数量已经从 2015 年第一季度的 1,388 个增加到第四季度的 7,295 个，激增了 426%。

感染链

Adwind 一般通过使用恶意软件电子邮件附件、漏洞网页和通过下载进行传播。其分发机制也在不断演变。早期的垃圾邮件活动只会持续几天和几周，并使用相同的电子邮件主题和附件名称。这种一致性有助于安全供应商快速检测并减轻 Adwind 的威胁。现在，垃圾邮件活动持续时间短，并不断更改主题并精心撰写附件内容，从而使 Adwind 可以规避检测。

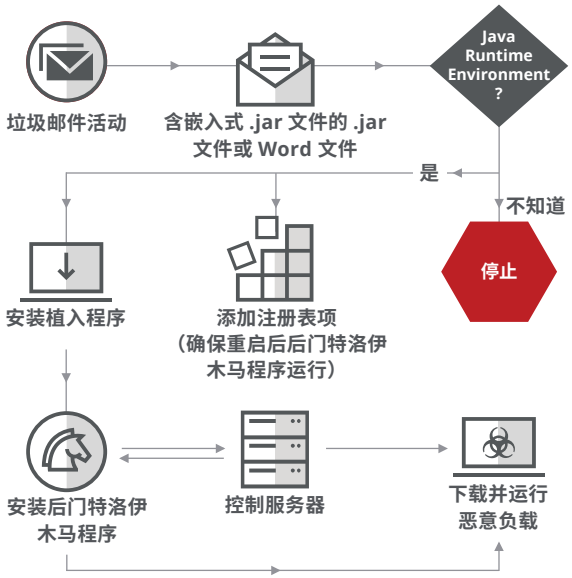

图 2. Adwind 感染链。

Adwind 成功感染系统后，我们发现它会记录击键、修改和删除文件，下载并执行更多恶意软件，截取屏幕快照，访问系统的摄像头，控制鼠标和键盘以及对自身进行更新等。

McAfee 帮助防御 Adwind 及其他后门特洛伊木马程序的方法

McAfee 可帮助防御 Adwind 等后门特洛伊木马程序。下面是有助于阻止此类攻击的部分产品。

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 可以大幅减少后门特洛伊木马程序攻击，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 Global Threat Intelligence (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 Threat Intelligence Exchange 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 Threat Intelligence Exchange 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 Threat Intelligence Exchange 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 Threat Intelligence Exchange 可以结束与该攻陷指标相关联的所有进程和应用程序。

McAfee Advanced Threat Defense

McAfee Advanced Threat Defense 是一款综合运用多个检查引擎的多层恶意软件检测产品。这些引擎对可疑对象执行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，防范最初在其目标系统中放置二进制文件的恶意软件。

- **基于特征码的检测：**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。全面的知识库由 McAfee Labs 创建和维护。
- **基于信誉的检测：**使用 McAfee GTI 查找文件的信誉，以检测各种新兴威胁。
- **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后门特洛伊木马程序和零日威胁。
- **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 Advanced Threat Defense 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 Advanced Threat Defense 支持 Windows XP（32 位和 64 位）、Windows 7（32 位和 64 位）、Windows 8（32 位和 64 位）、Windows Server 2003、Windows Server 2008（64 位）和 Android 的自定义操作系统映像。

McAfee Network Security Platform

McAfee Network Security Platform 是一款发现和阻止复杂网络威胁的独特智能安全产品。采用高级检测和模拟技术，超越单纯的模式限制，从而以极高的准确性抵御未知的隐匿攻击。我们开放、集成的安全管理方法通过将实时 McAfee GTI 信息与丰富的用户、设备和应用程序相关数据进行结合来简化安全操作，从而能够快速准确地对网络传播带来的攻击作出响应。

- **无特征码防御：**高级和未知的威胁，例如隐匿恶意软件、高级持久性威胁 (APT)、僵尸程序和零日攻击通常会规避基于特征码的防御。McAfee Network Security Platform 具有多个高级引擎，无需特征码便可防范这些高级和未知的威胁。无特征码检测使用模拟以接近实时的方式分析 Web 内容、PDF 文件、Flash 文件以及 JavaScript 行为。
- **Endpoint Intelligence Agent：**McAfee Network Security Platform 提供实时的每个流终端流量关联。代理将网络流量流行为分析和多个信誉情报源组合。该技术利用网络中以及每个 Windows 主机上的情报来揭示终端可执行文件和网络流量流之间的关系，从而能实时确定恶意的网络链接以及可执行文件。代理合并攻击、块恶意通信的详细过程上下文，防止高级恶意软件的传播，并且最终隔离和修复受害主机系统。

McAfee Web Gateway

恶意广告、“随看随下”下载和嵌入网络钓鱼电子邮件中的恶意 URL 都是一些用于传递后门特洛伊木马程序的主要攻击方法。McAfee Web Gateway 是一款可以帮助贵公司防范此类威胁的强大产品。

- **McAfee Gateway Anti-Malware Engine：**无特征码意图分析功能会实时从 Web 流量中过滤出恶意内容。模拟和行为分析可主动防范零日威胁和针对性威胁。McAfee 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 McAfee Web Gateway 将拒绝尝试连接已知恶意网站或已知用作控制服务器的网站。

除了前述这些 McAfee 产品以外，我们还推荐了一款其他类型的安全技术。

- **电子邮件网关安全：**大部分后门特洛伊木马程序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可以很好地防范此类攻击。

McAfee
Together is power.

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：861085722000
www.mcafee.com/cn