解决方案简介

防范密码窃取程序

因为我们越来越依赖个人电子设备，而企业也将有价值的信息移动到云，因此访问凭证的价值随之增加。现在，攻击者几乎会在所有主要高级持久性威胁的早期阶段使用盗取的密码。

密码窃取程序主要靠破坏网络和系统安全来获取关键的访问凭证。Fareit 密码窃取程序凭借其强大的能力成为最常见的密码盗取恶意软件，而这一“宝座”已蝉联五年以上。自从 2012 年发现此程序，Fareit 为了逃避最新的网络防御策略一直在不断变化。

最初，Fareit 主要是从 Web 浏览器窃取登录凭证来获取在线银行、电子邮件帐户之类的应用程序的访问权，进而窃取身份信息。从那时起，Fareit 演变为一种更具侵略性的信息窃取程序，这种程序使用一些模拟手段（如每次感染时更改其文件哈希）进行隐藏。2016 年，出现了新一代的 Fareit 密码窃取恶意软件，它使用受感染的网络资产发动分布式拒绝服务攻击。而现在，Fareit 甚至作为一种付费感染服务提供，这意味着网络犯罪分子现在可以靠分发恶意软件赚钱。他们完成的感染数量越多，赚的钱就越多。

在过去的十年中，传递密码窃取程序（如 Fareit）的网络钓鱼攻击是出现最多的初始攻击媒介之一。

防御密码窃取程序攻击的策略和程序

McAfee 建议组织采取以下步骤防范密码窃取程序攻击：

- 密码窃取程序通常通过恶意软件分发，因此标准安全原则是始终确保防恶意软件产品为最新。
- 恶意软件可能会在用户浏览时无意间下载。保持 Web 浏览器和插件为最新可提供一层额外的保护。
- 以具有有限权限（而不是管理员权限）的用户身份运行应用程序。

McAfee™
Together is power.

- 确保网络周边安全。对于之前已被密码窃取程序攻击成功侵害过的内部应用程序，防火墙可以阻止外部攻击者获取这些应用程序的访问权。
- 只有在使用企业资产时才使用企业身份验证凭证（例如那些用于互联网浏览的 Web 代理、数据库应用程序和共享文件夹等内容的凭证）。不允许使用不是由公司 IT 安全组分发和认证的受信任企业网络中的系统。
- 可能包含密码窃取程序的恶意软件可以嵌入已被攻击者感染特洛伊木马的合法软件内。为了防止此类攻击得逞，我们强烈建议您严格执行软件交付和分发机制。最好有专门的中心存储库来存放公司的应用程序，用户可以从中下载经过批准的软件。
- 如果用户有权安装 IT 安全组未验证的应用程序，请教导他们只安装来已知供应商的带有受信任签名的应用程序。在线提供的“无害”应用程序带有嵌入式密码窃取程序或其恶意软件的情况极其常见。
- 切勿从非 Web 来源下载应用程序。如果您是从 Usenet 组、IRC 通道、即时消息客户端或对等系统下载，则下载恶意软件的可能性非常高。IRC 和即时消息中指向网站的链接也经常会连接到受病毒感染的下载内容。
- 实行教育计划以阻止钓鱼攻击。密码窃取程序通常通过网络钓鱼攻击分发。

如果您认为系统已受到密码窃取程序的侵害，下面这些最佳做法可以帮助遏制感染扩散：

- 在支持双重身份验证的应用程序上启用此功能，以此减少攻击面。攻击者可能有窃取到的密码，但第二重验证将阻止渗透。
- 如果受感染的计算机已通过防火墙规则限制入站和出站流量，那么使用终端防火墙可以遏制凭借窃取密码进行的入侵扩展。

McAfee 产品如何防范密码窃取程序攻击

McAfee VirusScan® Enterprise 8.8 或 McAfee Endpoint Security 10

- 使用最新的修补程序、DAT 版本和扫描引擎，让终端防恶意软件保持在最新状态。确保使用 McAfee Global Threat Intelligence (McAfee GTI)。
- 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 Enterprise 8.8 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

入侵防护工具无法有效找到成功的密码窃取程序攻击。但是，McAfee Host Intrusion Prevention 可以帮助阻止恶意软件负载扩散，而其中可能包含密码窃取程序。

- 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 特征码 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。
- 利用以下两条子规则实现此目的：
  1. 使用“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。如果您希望在路径中使用通配符，请以“**\”或“?:\”作为文件名的开头。如果您希望使用通配符作为驱动器号，请使用“**\文件名.exe”或“?:\文件名.exe”（示例）。
       - 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、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. 使用“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 运行目标可执行文件（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密码窃取程序的站点或向用户发出警告。

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 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 GTI：
  - 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

- 收件箱检测功能：
  - 基于签名的检测：McAfee Labs 恶意软件库维护了 600 多万个签名。
  - 基于信誉的检测：McAfee GTI。
  - 实时静态分析和模拟：用于无特征码检测。
  - 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密码窃取程序恶意软件的分析器配置文件：
  - Windows 7、8、10 之类的常规操作系统。
  - 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

- McAfee Network Security Platform 的默认策略中包含签名，用以检测可用来传输密码窃取程序相关文件的 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 Defense 配置是否应用在传感器级别。
- 更新回拨检测策略（以抗击僵尸网络）。

McAfee Web Gateway

- 启用 McAfee Web Gateway 防恶意软件检测功能。
- 启用 McAfee GTI 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。
- 您可以更改此脚本以引用其他 McAfee 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 不提供支持）。

McAfee Active Response

- McAfee Active Response 查找并响应高级威胁。与来自 McAfee Labs、Dell SecureWorks 或 ThreatConnect 的威胁源配合使用时，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。
- 自定义收集器可用于构建专用工具，以查找和识别与密码窃取程序相关的迹象。
- 用户可构建触发器和反应来定义满足特定条件时的操作。例如，发现哈希或文件名时，可自动运行删除操作。

延伸阅读

Phishing Attacks Employ Old but Effective Password Stealer（钓鱼攻击利用老套而有效的方法窃取密码）

Fareit Virus Profile

Fareit Virus Profile

McAfee (Singapore) Pte Ltd
10 Kallang Avenue #08-10
Aperia Tower 2
Singapore 339510
www.mcafee.com/cn