解决方案简介

防御速记式加密威胁

速记式加密是秘密隐藏艺术与科学的结合，在数字世界中，也可使用速记式加密隐藏信息。可以在图像、音频轨道、视频剪辑或文本文件中隐藏消息。它可以用于合法目的，但更为常见的情况是恶意软件利用速记式加密从事非法活动。

为规避检测，某些恶意软件使用数字速记式加密，将其恶意内容隐藏在貌似无害的隐藏文件中。这种规避技术利用了这样一个事实，即大多数反恶意软件签名会检测恶意软件配置文件中的恶意内容。使用速记式加密，已将配置文件嵌入隐藏文件。此外，生成的速记式加密文件可在主内存中解密，进一步减少了检测机会。最后，在速记式加密文件中，很难检测到存在配置文件、二进制更新或僵尸程序命令等隐藏的信息。不幸的是，在网络攻击中使用速记式加密，实施容易，检测不容易。

防御速记式加密攻击的策略和步骤

McAfee 建议组织采取以下步骤来防御速记式加密威胁。

- **实施严格的软件传播和分发机制，防范内部威胁。**建立受信任的企业应用程序的中央存储库始终是一个不错的主意，用户可以从该存储库下载经过批准的软件 — 避免出现让用户从可能包含速记式加密代码的未知来源下载软件的风险。
- **仔细观察图片。**借助图像编辑软件，查找速记式加密标记，比如图像的细微色差。如果图像中有大量重复的颜色，也可能是速记式加密攻击的标志。
- **控制速记式加密软件的使用。**禁止任何企业系统存留速记式加密软件，除非有特别的业务要求。仅在受控网段部署这类软件。
- **只允许使用受信任的签名。**只安装受信任供应商提供受信任特征码的应用程序。
- **配置防恶意软件工具来检测联编程序。**应将反恶意软件配置为确定是否存在可能包含速记式加密图像的联编程序。
- **网络分段。**万一速记式加密攻击成功，受信任的虚拟化架构会与正确的网络分段相结合，这样有助于抑制攻击爆发，这是因为它们使用的安全可验证的引导进程和持续的流量监控将有助于确保应用程序的隔离。
- **监控出站流量。**通过监控出站流量，确定是否存在成功的速记式加密攻击。

McAfee
Together is power.

McAfee 产品如何防御恶意攻击中的速记式加密代码。

McAfee Endpoint Security

威胁预防

确保将 McAfee Endpoint Security (ENS) 配置为阻止可能包含速记式加密代码的恶意软件中的任何已知威胁：

- 使用最新的补丁、DAT 版本和扫描引擎，让 McAfee ENS 完全保持在最新状态。
- 确保环境中的所有系统均受到保护并且可更新。
- 设定实时扫描（访问时）以在读取时和写入时扫描所有文件。绝不能关闭读取时扫描，配置低风险进程时除外。
- 扫描排除项规则应降至最少，并且仅在必要时使用。如果怀疑有恶意软件，请确保暂时禁用任何扫描排除项。请参阅知识库文章 KB88595，了解如何设置排除项。
- 了解在频繁使用的环境或硬件安全性最低的环境中，使用高风险/默认/低风险进程配置来限制速记式加密威胁的性能含义。了解如何利用 McAfee Endpoint Security KB88205 改善性能。
- 配置 McAfee ENS 以使用 McAfee Global Threat Intelligence (GTI) 文件信誉功能。该技术有助于弥合零日威胁与基于签名的检测之间的差距。参阅 KB74983 了解建议的 McAfee GTI 文件信誉设置，参阅 KB53735 了解更多信息。
- 配置 McAfee ENS 访问保护规则，以阻止创建 autorun.inf 文件。
- 使用访问保护规则阻止安装未知威胁。

Web 控制

McAfee ENS 的 Web 控制功能基于 McAfee GTI 网站信誉和网络类别服务。感染了速记式加密风险的软件通常位于恶意软件分发网站上。

在访问之前，McAfee ENS 的 Web 控制功能识别出托管或感染了恶意软件，或者包含不适内容的站点。

McAfee Web 控制：

- 使用颜色方案表示网站的相对安全性：
  - 绿色 = 安全（风险极低或无风险）
  - 黄色 = 注意（轻微风险）
  - 红色 = 警告（严重风险）
  - 灰色 = 未知（尚未评级，谨慎使用）
  - McAfee Secure = 每日测试黑客漏洞
- 通过 McAfee ePolicy Orchestrator 轻松部署和配置。
- 提供另一层终端保护。可用于 Internet Explorer、Firefox 和 Chrome。
- 使用有效的反垃圾邮件保护来防止恶意电子邮件进入网络。

详细内容：McAfee Endpoint Security 产品指南 — 使用 ENS Web 控制

自适应威胁防护

- 支持 McAfee Real Protect 运用机器学习技术，根据威胁的潜在内容和行为（执行前分析）以及实际行为（动态行为分析）识别高级威胁 — 所有内容都无需特征码。了解更多：**自适应威胁防护 — Real Protect**
- 实施 McAfee 动态应用程序遏制功能并按照推荐的最佳做法操作。详细内容：KB87843.

McAfee VirusScan Enterprise

尚未部署最新 McAfee ENS 的客户应确保将 McAfee VirusScan Enterprise (VSE) 配置为阻止可能包含速记式加密代码的恶意软件中的任何已知威胁。

- 使用最新的补丁、DAT 版本和扫描引擎，让 McAfee VSE 完全保持在最新状态。
- 确保环境中的所有系统均受到保护并且可更新。
- 设定实时扫描（访问时）以在读取时和写入时扫描所有文件。绝不能关闭读取时扫描，配置低风险进程时除外。
- 扫描排除项规则应降至最少，并且仅在必要时使用。如果怀疑有恶意软件，请确保暂时禁用任何扫描排除项。请参阅知识库文章 KB50998，了解如何设置排除项。
- 在使用频繁的环境或硬件安全性最低的环境中，使用高风险/默认/低风险进程配置来减少遭遇速记式加密威胁的几率。参阅 KB55139 了解此功能，参阅 KB58692 了解如何进行配置。
- 配置 McAfee VSE 以使用 McAfee Global Threat Intelligence (GTI) 文件信誉功能。该技术有助于弥合零日威胁与基于签名的检测之间的差距。参阅 KB74983 了解建议的 McAfee GTI 文件信誉设置，参阅 KB53735 了解更多信息。
- 配置 McAfee VSE 访问保护规则，以阻止创建 autorun.inf 文件。
- 使用访问保护规则阻止安装未知威胁。

McAfee Application Control

McAfee Application Control 提供有效的方法阻止服务器、企业桌面机和固定功能设备上因速记式加密攻击而出现的未经授权的应用程序和代码。McAfee Application Control 可防止文件受到攻击，并阻止文件型病毒传播到整个网络。

McAfee Application Control 有助于确保两个主要方面的安全：

- **基于文件的保护：**防御基于文件的攻击，这在速记式加密威胁中是常见的类型。这些攻击可能会尝试执行新应用程序或修改当前应用程序。
- **内存保护：**防御基于内存的攻击，这些攻击可能在互联网上或整个网络中发生，或由于执行文件而在本地发生。

基于文件的保护

不属于白名单的应用程序既未经授权也不受保护。相反，列入白名单的项目均经过授权且受到保护。如果将未经授权的项目引入终端（例如，通过下载，通过网络进行访问，或通过闪存驱动器或 CD 进行本地访问），则可将其复制到终端，或者有所更改并从终端上的一个文件夹移动到另一个文件夹，但在任何情况下均无法执行。这些事件类型的示例如下。

执行已被拒绝	某个并未出现在白名单上的应用程序试图执行，但被 McAfee Application Control 阻止。
已禁止安装 ActiveX	McAfee Application Control 阻止安装未经授权的 ActiveX 控件。

如果未经授权的进程（例如，源自远程终端上执行的恶意文件）或未经授权的用户尝试修改、重命名、移动或删除已列入白名单并因此受保护的文件，McAfee Application Control 将阻止更改。这些事件类型的示例如下。

文件写入被拒绝	McAfee Application Control 阻止未经授权的进程修改列入白名单的应用程序。
已禁止包修改	McAfee Application Control 阻止使用基于 MSI 的安装程序包的应用程序利用未经授权的机制执行安装、修改或删除操作。

详细内容：McAfee Application Control 最佳实践

McAfee Advanced Threat Defense

McAfee Advanced Threat Defense (ATD) 通过创新的分层方法检测隐匿且高度复杂的打包程序，加密的负载和零日恶意软件。它将低级反恶意软件特征码、信誉和实时模拟防御与深层静态码和动态恶意软件分析（沙盒）相结合，以分析恶意软件的行为。

详细内容：McAfee Advanced Threat Defense 的常见问题

延伸阅读

McAfee Security Advice Center：网络钓鱼防护

威胁形势信息显示板：Sundown 漏洞攻击套件于 2016 年晚些时候更新，发现它使用速记式加密来隐藏漏洞代码

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