如何防范勒索软件

McAfee® 帮助您防御当今的勒索软件威胁

勒索软件是一种恶意软件，这种恶意软件利用非对称加密来劫持受害者的信息，从而索要赎金。非对称（公钥-私钥）加密是一种使用一对密钥来加密和解密文件的加密技术。这个公钥-私钥对是由攻击者专门针对受害者生成的，私钥用于解密存储在攻击者服务器上的文件。仅当受害者支付赎金之后，攻击者才让受害者拿到私钥，但情况并非总是如此，比如最近发生的勒索软件活动。在无权访问私钥的情况下，几乎不可能解密被劫持以进行勒索的文件。

勒索软件存在众多变体。勒索软件以及其他恶意软件通常借助垃圾电子邮件营销活动或定向攻击来分发。McAfee® 产品采用了大量有助于防范勒索软件的技术。以下 McAfee 产品以及相关配置旨在阻止许多类型的勒索软件。

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 包含 800 多万唯一的勒索软件特征码。
- 建立访问保护规则来阻止安装勒索软件负载：请参阅访问保护规则知识库文章：**KB81095** 和 **KB54812**。

McAfee Host Intrusion Prevention

- **观看有关**如何配置 McAfee Host Intrusion Prevention 以防范 CryptoLocker 负载的视频。
- 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 可立即阻止注入

McAfee Host Intrusion Prevention 规则

McAfee Host Intrusion Prevention 支持对文件的创建、读取、写入、执行、删除、重命名、属性修改和硬链接创建进行监控。定义您需要或不需要发出警报的文件路径/类型，以及任何您希望纳入的可执行文件（已知不良源）或排除的可执行文件（已知误报创建者）。该规则可能具有侵入性，因此可考虑在信息/日志模式下在试用期使用规则。注意，文件保护规则需要建立您受信任的应用程序数据库。

Rule: Cryptolocker—block EXE in AppData

Rule type: files

Operations: create, execute, write

Parameters:
- Include: Files: **\AppData*.exe
- Include: Files: **\AppData\Local*.exe
- Include: Files: **\AppData\Roaming*.exe

Executables: Include *.*

注意，以下示例由于空间限制省略了许多文件扩展名。务必为您的应用程序检查所有适用的文件扩展名。

```
Rule {
tag “Blocking a Non-Trusted program attempt to write to protected data file extensions”
Class Files
Id 4001
level 4
files {Include “*\\*.3DS” “*\\*.7Z” “*\\*.AB4” “*\\*.AC2” “*\\*.ACCDB” “*\\*.ACCDE” “*\\*.ACCDR” “*\\**.ACCDT” “*\\*.ACR” “*\\*.ADB” “*\\*.AI” “*\\*.AIT” “*\\*.al” “*\\*.APJ” “*\\*.ARW” “*\\*.ASM” “*\\*.ASP” “*\\*.BACKUP” “*\\*.BAK” “*\\*.BDB” “*\\*.BGT” “*\\*.BIK” “*\\*.BKP” “*\\*.BLEND” “*\\*.BPW” “*\\*.C” “*\\*.CDF” “*\\*. CDR” “*\\*.CDX” “*\\*.CE1” “*\\*.CE2” “*\\*.CER” “*\\*.CFP” “*\\*.SRF” “*\\*.SRW” “*\\*.ST4” “*\\*.ST5” “*\\*.ST6” “*\\*.ST7” “*\\*.ST8” “*\\*.STC” “*\\*.STD” “*\\*. STI” “*\\*.STW” “*\\*.STX” “*\\*.SXC” “*\\*.SXD” “*\\*.SXG” “*\\*.SXI” “*\\*.SXM” “*\\*.SXW” “*\\*.TXT” “*\\*.WB2” “*\\*.X3F” “*\\*.XLA” “*\\*.XLAM” “*\\*.XLL” “*\\*. XLM” “*\\*.XLS” “*\\*.XLSB” “*\\*.XLSM” “*\\*.XLSX” “*\\*.XLT” “*\\*.XLTM” “*\\*. XLTX” “*\\*.XLW” “*\\*.XML” “*\\*.ZIP”}
Executable {Include “*”}
user_name{Include “*”}
directives files:writefiles:renamefiles:delete
}
```

- 访问保护规则：您也可使用访问保护规则通过灵活运用通配符来增强 Host Intrusion Prevention 规则：**\Users**\AppData***.exe

注意：对于McAfeeVirusScan®Enterprise、McAfeeAgent、McAfee Host Intrusion Prevention 和 McAfee Data Loss Prevention 更新后的版本提供的更新版本的 SYSCore，** 在 File or folder name to block（要阻挡的文件或文件夹名）字段的开头不再起作用。对于更新的版本，您需要使用以下格式：

```
C:\**\AppData\**.exe
```

这旨在于 C: 盘上的根处和任何名为 AppData 的文件夹的根目录阻止任何随机 .exe。

该类型规则可能的迭代几乎没有限制，因此请仔细考虑规则的所有方面。您可能需要考虑规则的所有方面、针对其预期功能的所有可能条目以及如何在整体上配置规则（示例如下）：

```
Process to include: *
Process to exclude: [保留为空]
File or folder name to block: <路径或目录>
File actions to prevent: [您所需的任何操作（建议以不严格的操作开始，最小化可能对终端造成的损害）]
```

McAfee SiteAdvisor® Enterprise 或 Endpoint Security/Web Protection

- 使用网站信誉阻止或警告用户访问存在勒索软件的网站。

McAfee Threat Intelligence Exchange 和 McAfee Advanced Threat Defense

- McAfee Threat Intelligence Exchange 策略配置：
  - 以观察模式开始 - 由于端点是通过可疑进程发现，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量。
  - 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 尚未发现的文件，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（很可能为恶意的内容）- 清理/删除。
  - Might be malicious（可能为恶意内容）- 拦截。
- 企业（组织）提供的文件信誉优先于 McAfee GTI：
  - 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）。
- 或者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 Protection

- 收件箱检测能力：
  - 基于特征码的检测 - 特征码由 McAfee Labs 创建和维护，包含的勒索软件特征码已超过 800 万个，其中包括 CTB-Locker 和 CryptoWall 及其变体。
  - 基于信誉的检测 - McAfee GTI。
  - 实时静态分享和模拟 - 用于无特征码的检测。
  - 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勒索软件的分析器配置文件：
  - 通用操作系统：Microsoft Windows 7、8、XP。
  - 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 在其默认策略中使用特征码检测以下方面：
  - 验证文件是否具有特征码 id=0x4880f900（特定于勒索软件）。
  - McAfee Network Security Platform 也有特征码来识别 Tor，Tor 可用于传输和恶意软件相关的文件。
- 与 McAfee Advanced Threat Defense 集成防御新的攻击变体：
  - 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 来发送 .exe、Microsoft Office 文件、Java 存档以及 PDF 文件至 McAfee Advanced Threat Protection 以进行检查。
  - 验证 McAfee Advanced Threat Protection 配置是否在传感器级别应用。
- 更新回拨检测规则（僵尸网络）。

McAfee Web Gateway

- 启用 McAfee Gateway Anti-Malware 检查。
- 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。
- 注意，您可修改脚本来引用其他 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 Active Response

McAfee Active Response 发现并响应高级威胁。当结合威胁源（例如 McAfee GTI、Dell SecureWorks 或 Threat Connect）使用时，可搜索到新威胁（包括勒索软件），并在这些威胁找到机会扩散之前将其扼杀。

- 自定义收集器可让您构建专用的工具来查找和识别与勒索软件危害相关的迹象。
- 满足特定条件时，用户可创建触发和反应来定义操作。例如，当发现哈希值或文件名时，可自动采取删除操作。

延伸阅读

Protecting Against Ransomware（防范勒索软件）

该知识性文章为客户提供最新的在 McAfee 环境下用于防范勒索软件的详细信息。

有关不同 CryptoLocker 勒索软件变体、症状、攻击矢量和防范技术的深入信息，请观看以下视频：

- **CrytpoLocker Malware Session（CrytpoLocker 恶意软件会话）**
- **CryptoLocker Update（CryptoLocker 更新）**

McAfee Labs 威胁顾问：X97M/Downloader

本文章为客户提供最新版本勒索软件的详细分析。

抵御勒索软件：确保您的数据不会被挟持

四页解决方案简介概述了什么是勒索软件，以及部分（非全部）McAfee 解决方案如何帮助进行防范。

Advice for Unfastening CryptoLocker Ransomware（消灭 CryptoLocker 勒索软件的建议）

有关遭受勒索软件攻击后客户应当采取什么措施的详细博客文章。

勒索软件重现：新系列报复性涌现

McAfee Labs 威胁报告文章（第 14 页）重点讨论了新的和进化中的勒索软件。

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