保护医疗保健系统免受勒索软件的威胁

勒索软件是一种恶意软件，这种恶意软件通常利用非对称加密来劫持受害者的信息作为人质。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。

在过去几年中，勒索软件是每位安全专家关注的头号问题。不幸的是，勒索软件是一种简单、有效并且赚钱又轻松的网络攻击工具。去年，我们看到攻击目标从个人转向企业，因为后者可以支付更高的赎金。最近，医疗机构成为勒索软件作者的抢手货。在《McAfee Labs 威胁报告：2016 年 9 月》中，我们还分析了 2016 年第 1/2 季度针对医疗机构的勒索软件攻击，发现这些攻击尽管相对不太复杂，但这些攻击都获得成功，并且有相关性和针对性。我们还讨论了勒索软件对医疗机构造成的挑战，包括安全性不强的旧版系统和医疗设备以及立即访问信息的生死攸关需求。

防御勒索软件的策略和步骤

保护系统免遭宏勒索软件攻击的最重要一步是要了解问题及其传播方式。要最大程度降低勒索软件攻击的成功率，医疗机构应遵循下面几条策略和规程：

- 计划好在发生攻击的情况下要采取的操作。知道关键数据的所在位置并且了解是否有方法渗透。与医疗机构紧急情况管理团队一起执行业务连续性和灾难恢复演练，以验证恢复点和时间目标。这些练习揭示对医疗机构运作的隐藏影响力，这是在正常备份测试中无法显现出来的。大部分医疗机构支付赎金是因为他们没有应急计划！
- 保证系统补丁处于最新状态。通常，很多被勒索软件滥用的漏洞都是可修复的。请保证操作系统、Java、Adobe Reader、Flash 和应用程序的补丁处于最新状态。请执行修补程序，并验证补丁是否已成功应用。
- 对于无法修补的陈旧医疗机构系统和医疗设备，请使用应用程序白名单来降低风险，白名单可锁定系统并防止未批准的程序执行。使用防火墙或入侵检测系统将这些系统和设备与网络中的其他部分隔离。禁用这些系统上的不必要服务或端口以减少可能的感染入口点的暴露。
- 保护终端。请使用终端保护及其高级功能。在很多情况下，安装客户端时只会启用默认功能。通过实施某些高级功能（例如，“阻止Temp文件夹中的可执行文件运行”），可以检测到并阻止更多的恶意软件。
- 如果可能，阻止用户将敏感数据存储在本地磁盘上。要求用户将数据存储在安全的网络驱动器上。这会使停机仅限于一段时间，因为只需要对受感染的系统重新制作映像即可。
- 采取反垃圾邮件措施。大多数勒索软件活动都始于含有链接或某类附件的网络钓鱼电子邮件。对于将勒索软件封装在 .scr 文件或一些其他非常见文件格式中的网络钓鱼活动，可以轻松通过设置垃圾邮件规则来阻止这些附件。如果允许 .zip 文件通过，请对 .zip 文件至少执行两个级别的扫描，以识别可能存在的恶意内容。
- 阻止有害或不必要的程序和流量。如果不需要使用 Tor，请在网络上阻止该应用程序及其流量。通常，阻止 Tor 就能阻止勒索软件从控制服务器获取 RSA 公钥，进而阻止勒索软件加密进程。
- 添加网段以用于患者护理所需关键设备。
- “空隙”备份。确保备份系统、存储和磁带所在的位置不能由生产网络中的系统普遍访问。如果勒索软件攻击中的有效内容横向蔓延，则可能会影响备份的数据。
- 针对与生产网络中其余部分完全隔离的关键电子医疗记录系统，利用虚拟基础设施。
- 请持续开展用户意识教育。因为大多数的勒索软件攻击都始于网络钓鱼电子邮件，所以用户意识显得尤为重要。统计数据显示，攻击者发送的每十封电子邮件中至少会有一封成功。请不要打开来自未经验证或未知发件人的电子邮件或附件。

McAfee 技术如何帮助防御勒索软件

McAfee VirusScan Enterprise 和 McAfee Endpoint Security 10

- 借助 McAfee VirusScan Enterprise (VSE) 或 McAfee Endpoint Security (ENS)，实施以下各项措施：
  - 每天使用 McAfee ePolicy Orchestrator (ePO) 来部署更新的 DAT。
  - 确保 McAfee Global Threat Intelligence (McAfee GTI) 已启用；McAfee GTI 包含 700 多万唯一的勒索软件特征码。
  - 开发访问保护规则以阻止勒索软件的安装和负载；请参阅访问保护规则知识库文章 KB81095 和 KB54812。
  - 使用动态应用程序遏制来阻止未知应用程序执行恶意活动。

McAfee Threat Intelligence Exchange

- 通过 McAfee Threat Intelligence Exchange (TIE)，设置以下策略：
  - 从观察模式开始。
  - 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 TIE 实施策略。
  - 根据声誉清理：Known Malicious（已知恶意）。
  - 根据声誉阻止：Most Likely Malicious（很可能为恶意）- 根据 Unknown（未知）来阻止可能会提供，但可能会增加初始管理工作负载。
  - 将“未知”声誉级别和更低级别的文件提交给 McAfee Advanced Threat Defense (ATD)。
  - TIE 服务器策略：接受 McAfee TIE 未识别的文件的 McAfee ATD 声誉。
- McAfee Threat Intelligence Exchange 人工干预：
  - 文件声誉强制实施（取决于操作模式）。
  - 很可能为恶意：清理/删除。
  - 可能为恶意：阻止。
  - 企业（组织）声誉优先于 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）。
  - 通过贡献指标将第三方声誉数据提供给 McAfee TIE。

McAfee Advanced Threat Defense

- McAfee Advanced Threat Defense 具有以下开箱即用的检测功能：
  - 基于特征码的检测：特征码由 McAfee Labs 创建和维护，包含的特征码已超过 1.5 亿个，其中包括 CTB-Locker 和 CryptoWall 及其变体。
  - 基于声誉的检测：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勒索软件的分析器配置文件：
  - 通用操作系统：Windows 7、Windows 8、Windows XP。
  - 安装 Windows 应用程序（Word 和 Excel）并启用宏。
- 为面向不同操作系统的唯一分析器配置文件提供互联网访问：
  - 很多样本运行 Microsoft Office 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 Application Control

- McAfee Application Control 通过应用程序白名单提供保护。适合于保护所有类型的设备，特别是：
  - 静态设备，比如医疗设备。
  - 具有旧操作系统且没有收到更新的系统。
  - 提供有限数量服务的应用程序服务器。
  - 不常改动的系统。
- 初始安装
  - McAfee Application Control 将在安装期间完全扫描系统并创建要加入白名单的端点库存和应用程序。
- 观察模式
  - 允许管理员跟踪安装/启动的新应用，并包含将其合并为集中式白名单的选项（如果应用程序确定被授权）。
  - 通过在环境中识别应用程序的新可信更新来帮助进行编制白名单。
  - 确定更新白名单的方法，比如批准的进程、证书、目录或用户。
- 自批准模式
  - 用户将能够批准未加入白名单的应用程序。这提供了灵活性并最大限度降低业务影响。
  - 管理员将能够集中跟踪用户批准的内容并可根据声誉和组织的策略来接受或撤销应用程序的授权。
- 强制实施白名单
  - 系统全面防御未知应用程序，包括恶意应用程序（如勒索软件）。
  - 为程序提供最终用户通知以批准新的可执行文件。

进一步阅读

McAfee Expert Center 社区

- McAfee VirusScan Enterprise
- McAfee Endpoint Security
- McAfee Threat Intelligence Exchange
- McAfee Advanced Threat Defense
- McAfee Application Control

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