2016 年 10 月 19 日，星期三

MBRFilter - 不能碰！

作者：Edmund Brumaghin 和 Yves Younan

摘要

勒索软件在业内越来越猖獗，很多情况下，除非能获得公开发布的解密工具，否则系统被感染后往往很难提取被加密的文件。除了创建和维护定期系统备份之外，关注多层深度防御网络架构，努力防御初始终端感染也变得日益重要。在如今威胁不断演进的格局下，水平参差不齐的威胁发起者几乎每天都在开发和部署新勒索软件“家族”，这让实现上面的目标变得困难重重。

有些类型的勒索软件注重对目标系统中的全部或部分文件进行加密；还有些类型的勒索软件（例如 Petya）通过覆盖主引导记录 (MBR) 的内容强制系统重新引导，然后仅对受感染系统硬盘上的主文件表 (MFT) 进行加密，以此迫使用户向威胁发起者付钱购买解密文件的秘钥。

为了打击试图修改 MBR 的勒索软件，Talos 在开源社区中发布了新工具 MBRFilter 驱动程序，它能将 MBR 置于只读模式，防止恶意软件在存储设备的这个区域写入或修改内容。

详细信息

MBR 是位于大容量存储设备最开头（扇区 0）的一个特殊存储位置，其中存储与存储设备分区相关的信息，以及与设备上文件系统配置相关的详细信息。另外，MBR 还用于存储操作系统引导加载程序（加载程序用于在开机时加载系统上安装的操作系统）。

Petya 是勒索软件的一种变体，它发挥作用的方式是覆盖受感染系统的 MBR，并把正常的引导加载程序替换为恶意引导加载程序。恶意引导加载程序接着会对存储设备上的主文件表 (MFT) 进行加密。NTFS 文件系统依靠 MFT 存储与文件系统上存储的所有文件和目录相关的详细信息。虽然 Petya 不会对存储设备上的所有内容进行加密，但会导致系统无法读取 MFT。系统一旦被感染，就会变得很难检索或恢复文件。

为了防止 Petya 之类的恶意软件操控 MBR 的内容（包括 MFT），Talos 在开源社区中发布了 MBRFilter 驱动程序。MBRFilter 是基于 Microsoft diskperf 和 classpnp 示例驱动程序的简单磁盘过滤驱动程序。它可以防止恶意软件向连接到系统的所有磁盘服务的扇区 0 写入内容。安装 MBRFilter 后，系统若要修改磁盘扇区 0 中的内容，必须在引导时进入安全模式。

AccessMBR 实用程序发挥作用的方式是先在物理驱动器 0 上读取扇区 0，然后再将该扇区写回磁盘。使用 AccessMBR 可以测试 MBRFilter 驱动程序。但是，如果使用 MBRFilter 驱动程序的目的单纯是为了保护计算机的话，则无需使用 AccessMBR。

以下视频展示了 MBRFilter 驱动程序如何阻止试图操控系统 MBR 的恶意软件（视频中出现的是勒索软件 Ransomware）：

总结

Talos 在开源社区中发布此应用的目的是帮助社区解决与基于 MBR 的各类恶意软件和勒索软件相关的威胁。

点击此处可以获取我们发布的此开源软件。

除了发布开源代码之外，Talos 还发布了可在 32 位和 64 位 Windows 系统上安装的签名驱动程序。只需右键点击链接 Zip 归档中包含的 INF 文件，然后选择“安装”即可执行安装。需要重新启动系统才能完成安装。

点击此处可获取 32 位安装文件。
（SHA256：3696aaa457d611eb1843fa7ab9b2235ab09b4af7f4ba09c7b56603e87a5551e3）

点击此处可获取 64 位安装文件。
（SHA256：a1aa4c59258f3459fb9612eea81c3805ba23e2bd8ff28bad5cf40c94c099fd19）

发布者：EDMUND BRUMAGHIN；发布时间：14:41
标签： 恶意软件、PETYA、勒索软件