编写人员	陈维	修订人员	
发布日期		修订日期	
文档版本		发布范围	选择一项

修改 MBR 的敲诈者木马来袭

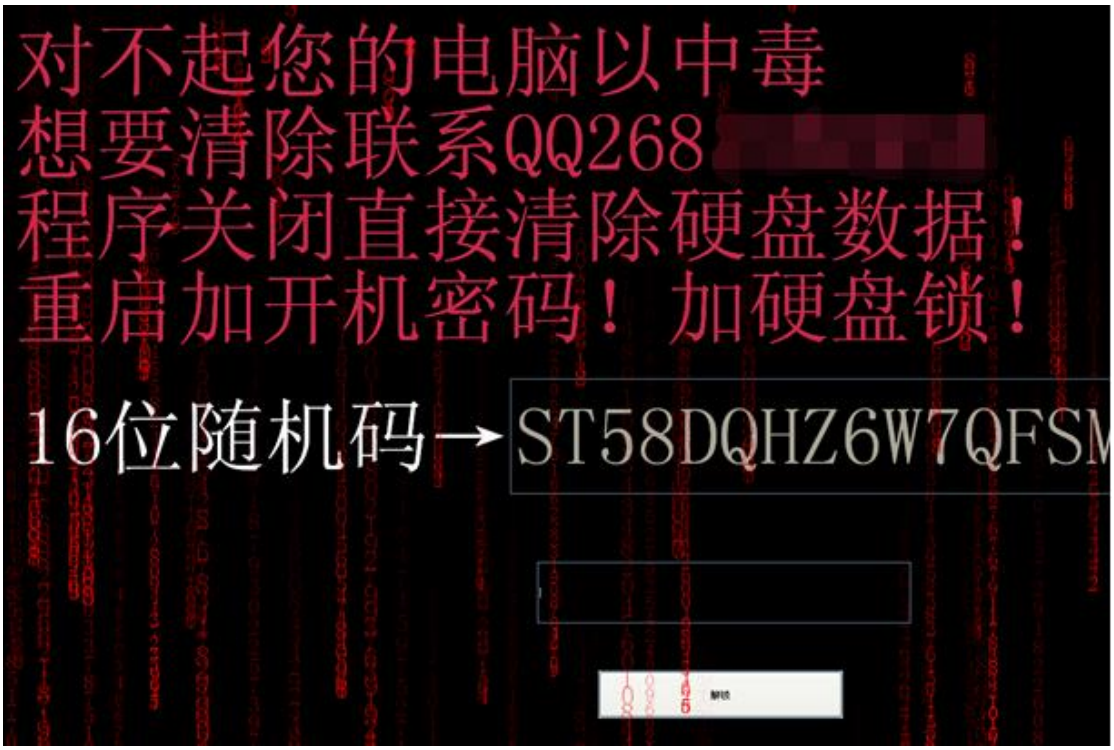
一、 事件简介

敲诈勒索病毒的传播成上升趋势，随着其勒索成功的案例越来越多，很多造马者开始使用不同的方法制作该类病毒，安天追影小组相继发表过 Locky 勒索软件的分析报告、TeslaCrypt 勒索软件的分析报告。2016 年 3 月底，安全厂商 G-Data 和趋势先后发布了修改 MBR、加密整个硬盘的勒索软件 Petya 的报告，值得关注的是，近期国内也出现了一款通过修改 MBR 来实现勒索的病毒软件，查询相关论坛得知，该病毒的作者并没有使用该病毒来敲诈且主动公开密码，也许只是为了炫耀技术。

二、 行为分析

运行该病毒后，屏幕如下图所示，文字不停的闪烁并伴有动画效果与音乐，重启后显示文字“mima lianxi qq 268****!!”提示输入密码。

经过分析得到密码后，输入正确的密码，则可以正常启动系统，以下为简要分析过程。

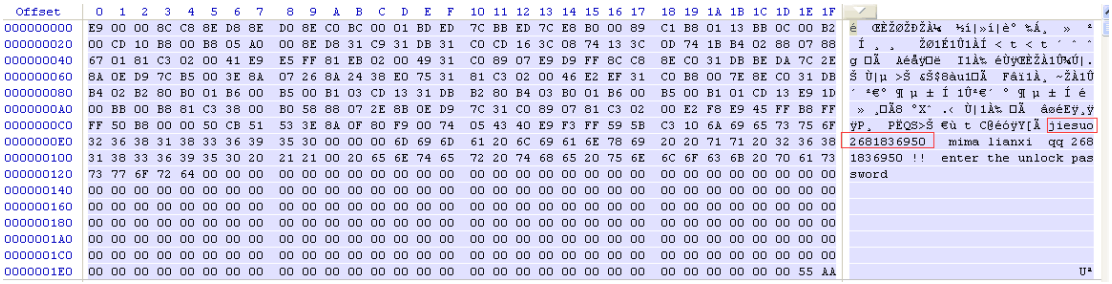


样本行为如下：

1、样本运行后，会直接获取\\.\PhysicalDrive0 的句柄，从第 1 扇区(偏移为

0x0)读取大小为 200 字节的内容写入到第 3 扇区(偏移为 0x400)中。其目的应该在输入正确密码后，重新恢复原有第 1 扇区的信息。

2、往第 1 扇区(偏移为 0x0)中写入大小为 200 字节的 MBR 敲诈信息（即重启后的开机界面，需要输入正确的密码才能恢复第 1 扇区）。



3、在创建输入密码界面的时候，则会不停的遍历进程比对来实现结束掉任务管理器进程 taskmgr.exe，主要是为了守护样本进程防止被任务管理器结束掉。

三、总结

敲诈勒索软件前期在国外传播较广，现在国内出现且以中文为提示语言、QQ 为联系方式，可见是国内的造马者制作或修改他人代码来进行传播的，也是该病毒在国内流行的一个开端，该类病毒破坏力较大，受害的机器除了按要求缴纳赎金，没有更好的选择。

安天追影小组提醒广大用户加强安全意识，不随意打开陌生链接及运行不明的应用程序，通过官方网站下载正版软件，我们会持续关注追踪勒索软件的发展态势。

MD5：3254ae13661fae33075349c3226fe940

相关报告及参考链接：

http://blogs.360.cn/360safe/2016/04/05/what_is_petya

http://bbs.kafan.cn/thread-2034951-1-1.html