

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

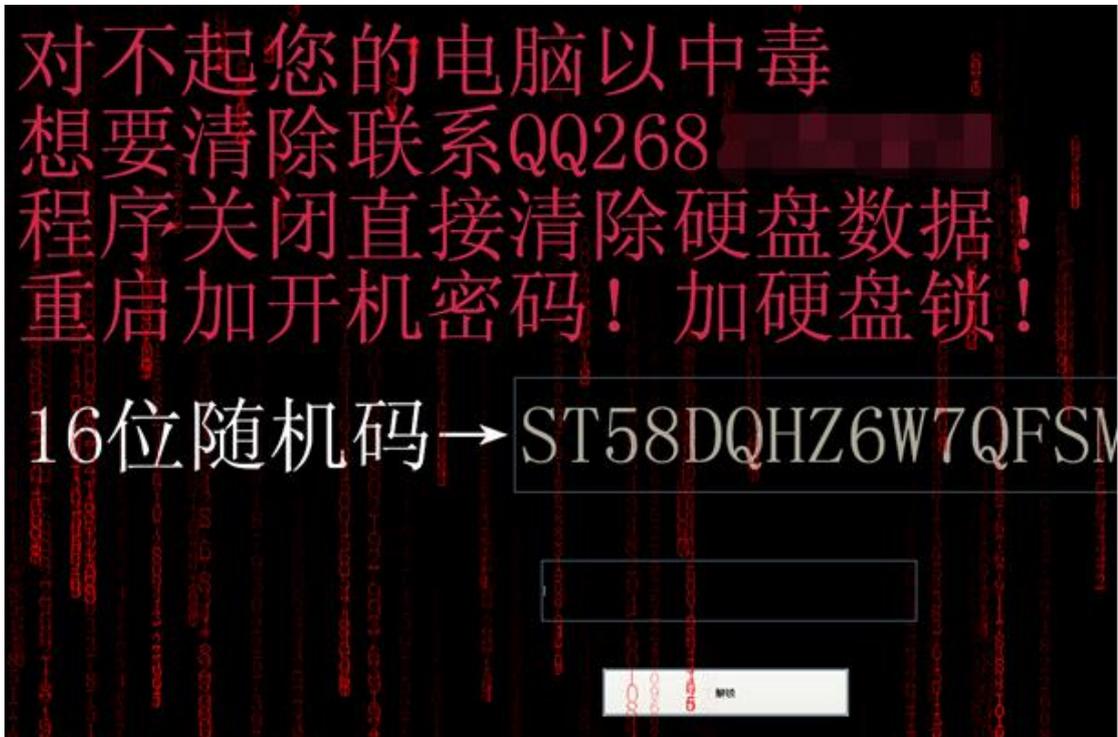
一、事件简介

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。



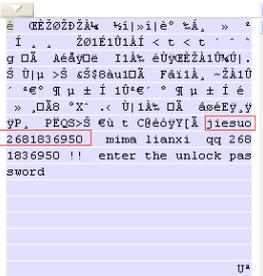
样本行为如下：

- 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)。

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F					
00000000	E9	00	00	8C	C8	8E	D8	8E	D0	8E	C0	BC	00	01	BD	ED	7C	BB	ED	7C	E8	B0	00	89	C1	B8	01	13	B8	0C	00	B2					
00000020	00	CD	10	B8	00	B8	05	A0	00	8E	D8	31	C9	31	DB	31	C0	CD	16	3C	08	74	13	3C	0D	74	1B	B4	02	88	07	88					
00000040	67	01	81	C3	02	00	41	E9	E5	FF	81	EB	02	00	49	31	C0	89	07	E9	D9	FF	8C	C8	8E	C0	31	DB	BE	DA	7C	2E					
00000060	8A	0E	D9	7C	B5	00	3E	8A	07	26	8A	24	38	E0	75	31	81	C3	02	00	46	E2	EF	31	C0	B8	00	7E	8E	C0	31	DB					
00000080	B4	02	B2	80	B0	01	B6	00	B5	00	B1	03	CD	13	31	DB	B2	80	B4	03	B0	01	B6	00	B5	00	B1	01	CD	13	E9	1D					
000000A0	00	BB	00	B8	81	C3	38	00	B0	58	88	07	2E	8B	0E	D9	7C	31	C0	89	07	81	C3	02	00	E2	F8	E9	45	FF	B8	FF					
000000C0	FF	50	B8	00	00	50	CB	51	53	3E	8A	0F	80	F9	00	74	05	43	40	E9	F3	FF	59	5B	C3	10	6A	69	65	73	75	6F					
000000E0	32	36	38	31	38	33	36	39	35	30	00	00	00	6D	69	6D	61	20	6C	69	61	6E	78	69	20	20	71	71	20	32	36	38					
00000100	31	38	33	36	39	35	30	20	21	21	00	20	65	6E	74	65	72	20	74	68	65	20	75	6E	6C	6F	63	6B	20	70	61	73					
00000120	73	77	6F	72	64	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00				
00000140	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
00000160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00			
00000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
000001A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
000001C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00		
000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	55	AA



3、在创建输入密码界面的时候,则会不停的遍历进程比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>