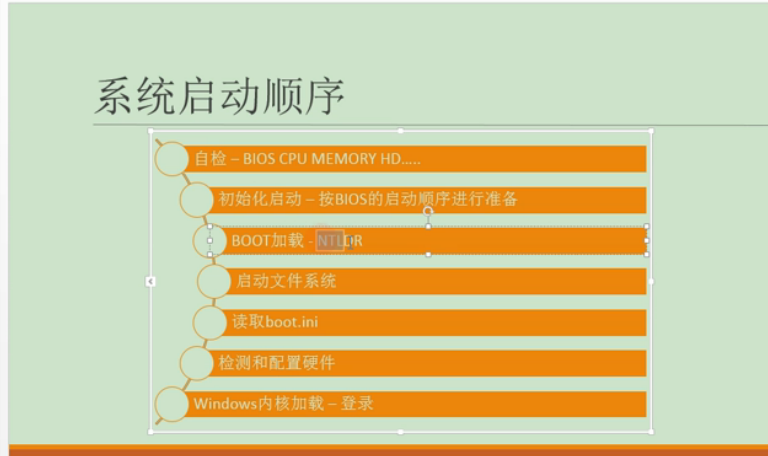
网易云课堂-超级硬盘锁笔记

程序的总体设计思路：

锁芯：用汇编写的代码，存放的是修改后的MBR的前446个字节，并且把后64个字节，置为0xF，隐藏真实的分区表。这部分就是我们的判断用户输入的逻辑代码，一旦密码正确，则从第3个扇区读取正确的分区表，异或解密447~510的分区表信息，然后重新写入第1扇区，重启完成解锁，否则一直处于待输入密码的状态。

锁体(包裹锁芯的外壳)：程序的主体，用c++写的代码，用于生成windows下的.exe，启动后来改写mbr信息。主要是将原始的mbr信息读出并异或加密其中447~510的64个字节，即硬盘的分区表信息，然后存入第3个扇区，然后将锁芯写入mbr，执行后，完成加锁。

NTLDR：NTLDR是一个隐藏的，只读的系统文件，位置在[系统盘](http://baike.baidu.com/view/299690.htm)的根目录，用来装载操作系统。是windows nt 4.0/windows 2000/windows xp/windows server 2003的[引导文件](http://baike.baidu.com/view/2141961.htm)，所以应该在系统正常的时候给予[备份](http://baike.baidu.com/view/235162.htm)。

全称是NT Loader，是系统加载程序，它的主要职责是解析Boot.ini文件

详细参见：http://baike.baidu.com/link?url=qbu6HqmhdodN-4D0vFvFE--4nRyDJFa5nh6dRCn--RAIuERlo767ePnHQNuNVsNjU2zP9or8DEemrA7r6pY9Tq

系统锁层级: 第二阶段

在这里做手脚，让BIOS找不到分区表。



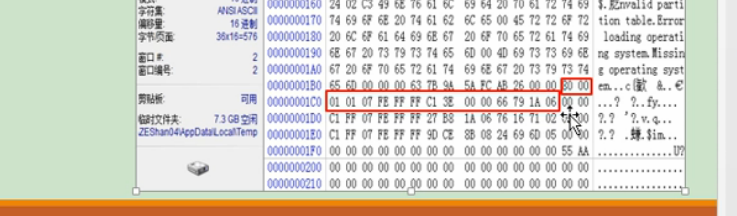
bootkit:主板级RootKit病毒，在第一层

512字节





上图红色的446个字节，检测分区表，失败会显示出右边的内容，今天就是改这段代码。



剩下的66个字节，圈出的16个字节代表C盘信息，后面依次每16个字节，代表接下来的一个磁盘的信息。。0X55AA是结束标记。 80表示主分区(活动分区)，可以启动磁盘，以上面圈出的c盘为例，00 01 01记载C盘内容是以分区00 磁头，01扇区，01柱面开始的磁盘内容，07表示系统指示符，指示磁盘是ntfs格式，FE,FF,FF分别表示分区结束磁头号，扇区和柱面号，指在物理硬盘结束的位置。后面8个字节，前四个表示分区该主分区第一个扇区的逻辑地址，后四个是分区中总的扇区数。

详细的MBR和硬盘知识，以及操作系统系统如何启动参见附件资料。

具体代码参加代码文件夹，主要是Config.ini，disklock.asm，mainlock.cpp和一个bin.h的十六进制机器代码(通过把disklock.asm用nasm生成.img后，用winHex 打开，然后复制成c语言格式保存生成)。

实验结果: