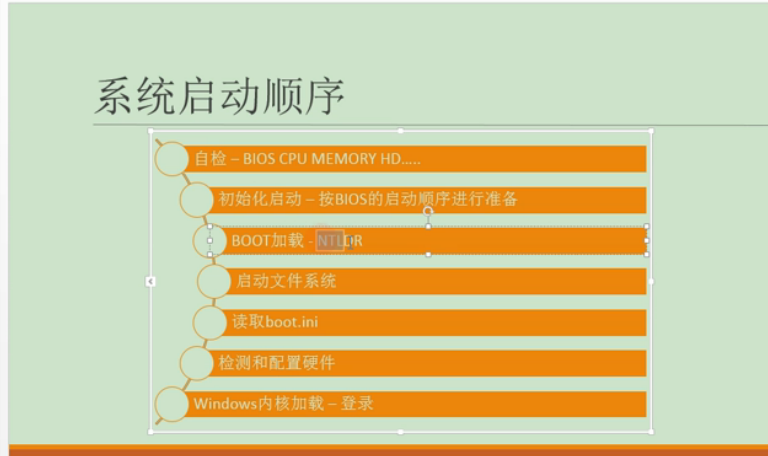
网易云课堂-超级硬盘锁笔记

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。



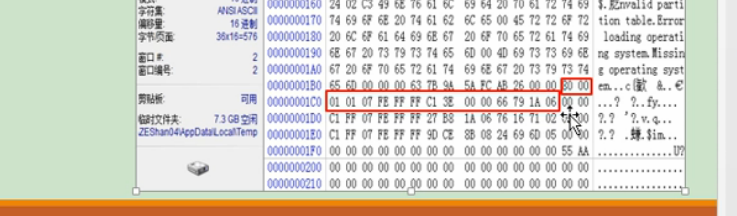
bootkit:主板级RootKit病毒，在第一层

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:

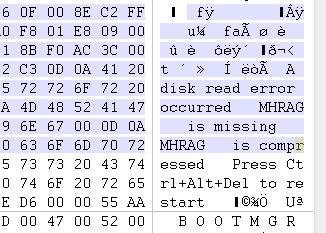
手贱，直接用codeblocks运行了，，，，结果是显示加密成功，winhex下查看c盘，确实提示信息，被改成了"Your pc is....."，不敢重启，原因有以下几个：

1.我用的是win7 64位，老师用的是win2003 server ，害怕两者的mbr不太一样，不过也不会。。。。因为mbr与硬盘有关和操作系统无关，毕竟是先于操作系统读入内存，所以冷静下来排除了这个问题。

2.那么问题就来了，我的机器是固态+机械硬盘，，，，固态....，完全不知道会不会有影响了，所以不能重启。

解决方法：

首先懵逼了一会......，然后冷静下来分析了代码，尝试反向破解。就是把3扇区读出来再异或一次直接写回1扇区，这里我担心的问题只有一个，就是readdisk那个函数，因为只有这个函数没有被两个扇区同时用过，所以我纠结了好久，这期间尝试系统还原，发现可以还原到昨天，但是查了下资料，好像没什了么卵用，，，放弃，然后终于决定执行修改后的程序了，运行，成功。打开winhex，又出现如下字样，



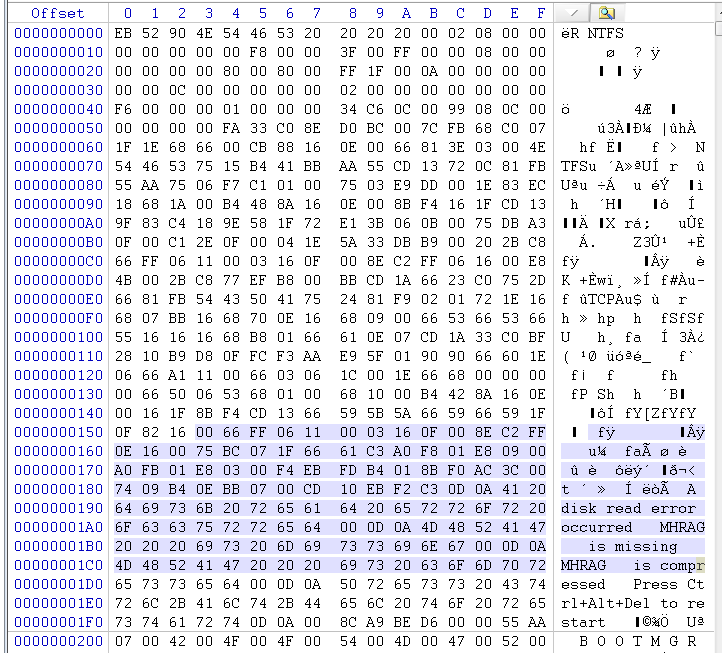
麻痹。。。。我怀疑这下GG了，可能读取那儿出问题了，然后开始用google搜，度娘查，都没有答案，然后心里有了一丝怀疑，难道原始mbr就是这样，莫非这是BIOS在硬盘出问题时，提前准备好的显示信息，抱着这种心理，我又看了遍视频，发现老师那里也有个操作系统不能加载的提示信息，和我的不一样。。。。。又一次陷入了绝望，完蛋，考虑重装吧，最差可能就是直接掏钱换固态了（哭。。。。（因为可能把解密代码破坏掉，彻底锁住），于是我开始备份，开始做启动盘，准备重启。

突然，灵光一现，DG为毛不试试？抱着这种态度，我下了个DG，开始进行分区表检查，竟然没错！！！！？？？？纳尼，但是我还是不敢重启，于是利用它重写了MBR，发现修改后的和我修改代码重写的竟然一样？？我还是不放心，选择了“搜索丢失分区表(重建)”，一遍操作下来，依然一样。。。。。我擦，难道我成功了，犹犹豫豫，狠狠心终于重启了系统。

奇迹出现了，（哭，竟然没坏，简直棒!!!!!!!!!!

经过这次手贱，我总结了，有危险的程序不要build&run。。。直接build，这次主要是因为makefile 不会玩，造成了直接点成运行。。。。不过也是一次丰富的经历，起码记住备份的重要性！！！！！！！！！！！！！！还有继续学习，，OS编程。下面开始在oracle虚拟机尝试。

下图是我win7 x64固态的MBR信息。（看来固态机械..没啥区别，主要还是看磁盘是MBR，还是GPT分区。又学会了一招

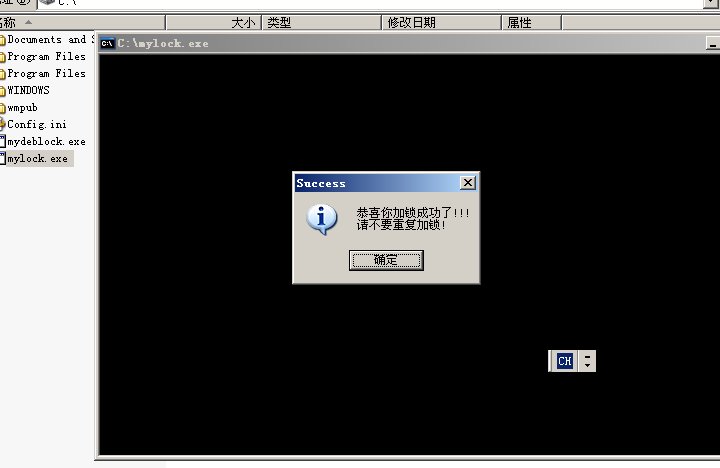


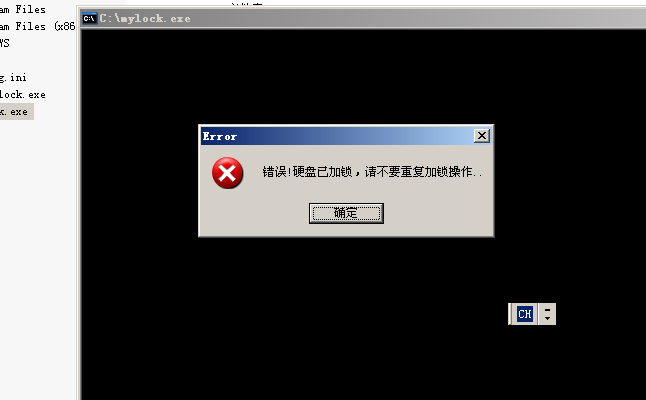
正式的测试:

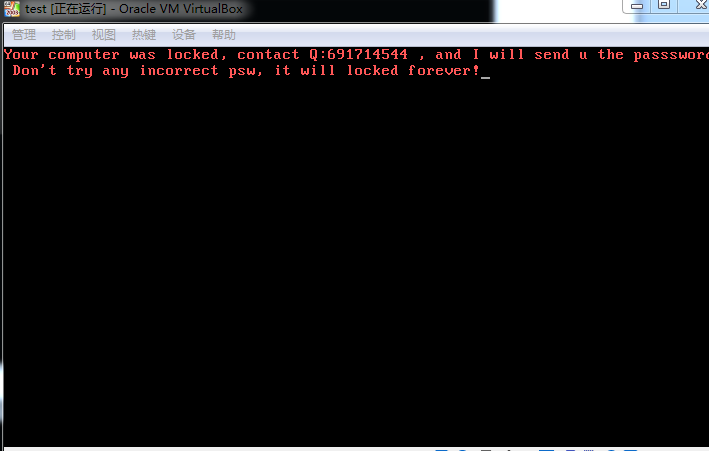
先进行了VM虚拟机下的win2003 x64测试，失败。可能是vmware自动的内存读写保护造成的，一直返回vcpu0 error。

在virtualBox下加锁、解锁、本地解锁均测试成功，截图如下：

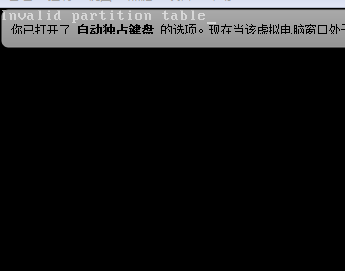
加锁：







前三位CaM输对，后面输错密码直接显示：



这就GG了，不可用分区表。

成功的就是直接启动了。

本地解锁成功，也就直接正常启动了。