原创 精选

近源渗透之：绕过锁屏和Bitlocker

简介：近源渗透中经常遇到电脑存在登录密码的情况。某些安全措施严格的目标，还会启用Bitlocker磁盘加密。本文将介绍两个工具，帮助绕过锁屏和Bitlocker。

发布时间：2022-07-22 18:21:39

近源渗透中经常遇到电脑存在登录密码的情况。某些安全措施严格的目标，还会启用Bitlocker磁盘加密。本文将介绍两个工具，帮助绕过锁屏和Bitlocker。

它们安装在U盘上。近源渗透时，将U盘插入电脑，并从U盘引导。即可绕过登录密码或Bitlocker。

工具1：Kon-Boot

Kon-Boot是最著名的密码绕过工具。其原理可谓神奇：在系统引导阶段，通过修改Windows内核，使验证用户凭证的代码失效。它不会删除密码，而是使登录时的密码验证失效，输入任意密码即可登录。

配置与使用

完整版本的Kon-Boot是付费软件，个人许可证价格为$50，商业许可证价格为$140。

如果不打算购买许可证，也可以使用免费版本。本文使用最后一个免费版本V2.5。该版本可以绕过除Windows 10的在线账户之外的密码。在绕过失败时，Kon-Boot可以添加账号，或安装Shift键后门。

1. 下载Kon-Boot后进入其根目录下的kon-bootUSB目录，目录结构如图：

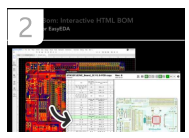

PushEAX

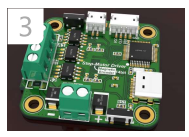
0 关注 | 9 粉丝 | 1 获赞 | 103 积分

+ 关注 私信

精选文章 更多>>

1 
Type-C边充边听PD协议芯片
作者：ZenasLDR 阅读量： 464

2 
立创EDA安装ibom插件
作者：doublemitg...

3 
如何渲染精美3D PCB
作者：超超

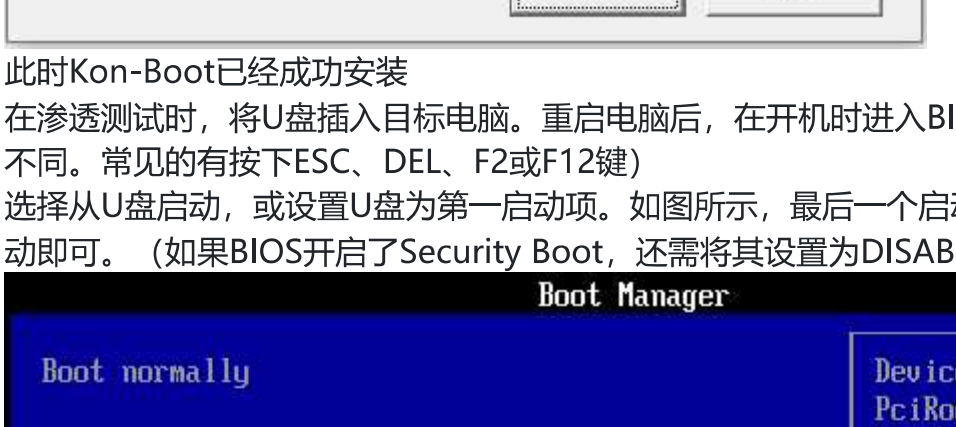
4 
《磁保持WIFI智能插座》配套...
作者：oldfox126

5 
【教育版】石家庄铁道大学202...
作者：立创EDA-小A

收起

名称	修改日期	类型	大小
EFI	2018/2/3 23:01	文件夹	
USBFILES	2018/2/3 23:01	文件夹	
auto.ps1	2018/2/3 23:01	Windows Power...	1 KB
COPYING	2000/12/19 12:47	文件	18 KB
grubinst.exe	2008/1/2 5:53	应用程序	61 KB
README.txt	2013/1/3 19:52	文本文档	1 KB
USB_INSTALL.vbs	2015/8/4 23:47	VBScript Script ...	4 KB
USB_INSTALL_DIFF.vbs	2015/8/4 23:47	VBScript Script ...	4 KB
usb_install_RUNASADMIN.bat	2012/9/5 11:36	Windows 批处理...	1 KB
usb_install2_NEEDADMIN.bat	2012/9/5 11:36	Windows 批处理...	1 KB

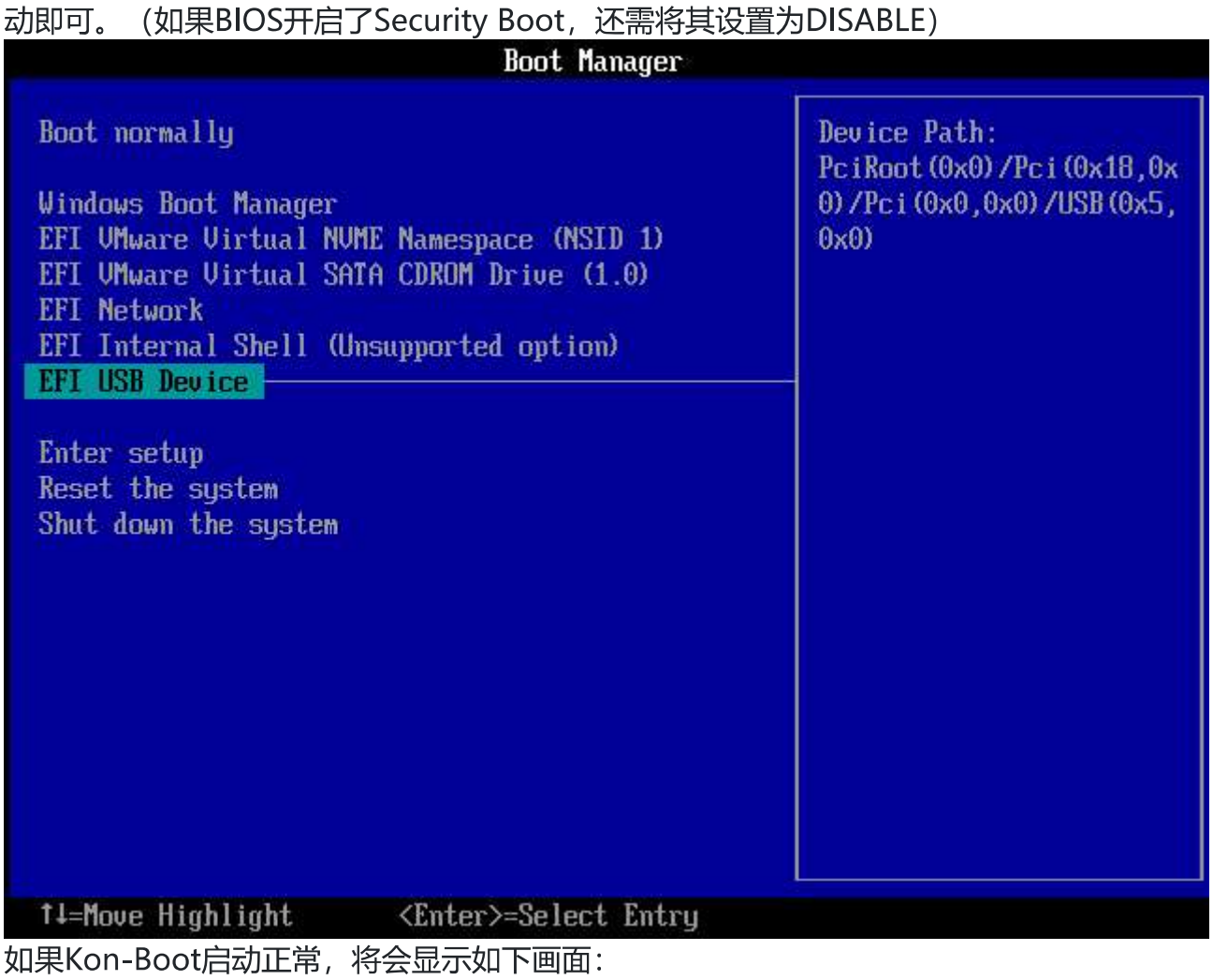
2. 准备一个空白U盘，接入电脑。注意：后续操作需要格式化此U盘。
3. 右键，以管理员身份运行usb_install_RUNASADMIN.bat。在弹出的对话框中点击确定



4. 如果显示的U盘信息无误，点击确定

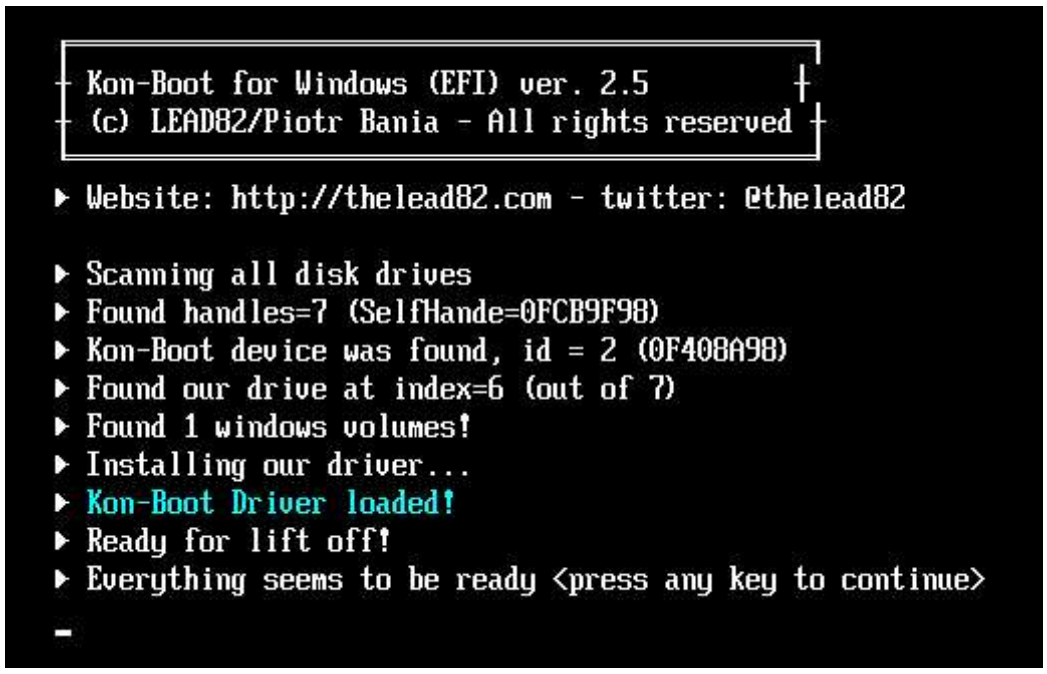
此时Kon-Boot已经成功安装

5. 在渗透测试时，将U盘插入目标电脑。重启电脑后，在开机时进入BIOS。（不同主板的方式不同。常见的有按下ESC、DEL、F2或F12键）
6. 选择从U盘启动，或设置U盘为第一启动项。如图所示，最后一个启动项是U盘，选择其启动即可。（如果BIOS开启了Security Boot，还需将其设置为DISABLE）

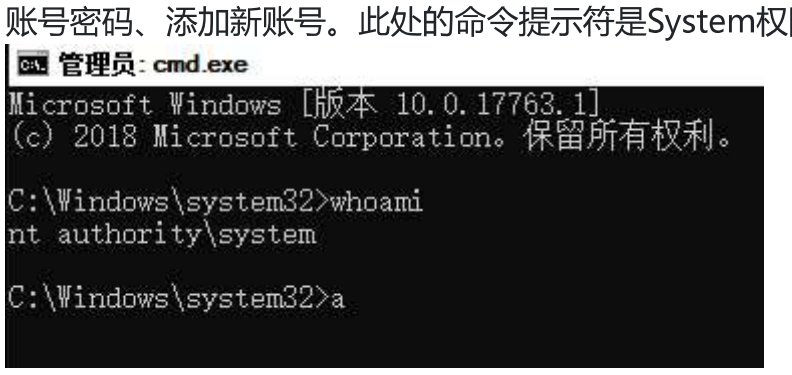


7. 如果Kon-Boot启动正常，将会显示如下画面：

收起



8. 按下回车键，即可正常启动系统。
9. 在登录界面，输入任意密码即可登录
10. 如果绕过密码失败，也可按下五次Shift键，呼出命令提示符。借此执行任意命令，或删除账号密码、添加新账号。此处的命令提示符是System权限。



Kon-Boot的缺陷

Kon-Boot可以满足大多数渗透场景的需求，但它有着几个缺点：

- 是付费软件，全功能版价格为140美元
- 无法绕过Bitlocker磁盘加密
- Kon-Boot绕过密码的成功率差强人意，经常需要重试

为弥补这些缺陷，我们介绍第二个密码绕过工具：GrabAccess。

工具2：GrabAccess

和Kon-Boot类似，GrabAccess也是密码绕过工具。对比起Kon-Boot，GrabAccess的优点有：

- 免费，并基于GPL协议开源
- 可以绕过Bitlocker植入后门
- 只要引导环境符合要求，成功率接近百分百
- 自动化植入木马。只需要一步操作，耗时短，适合近源渗透场景

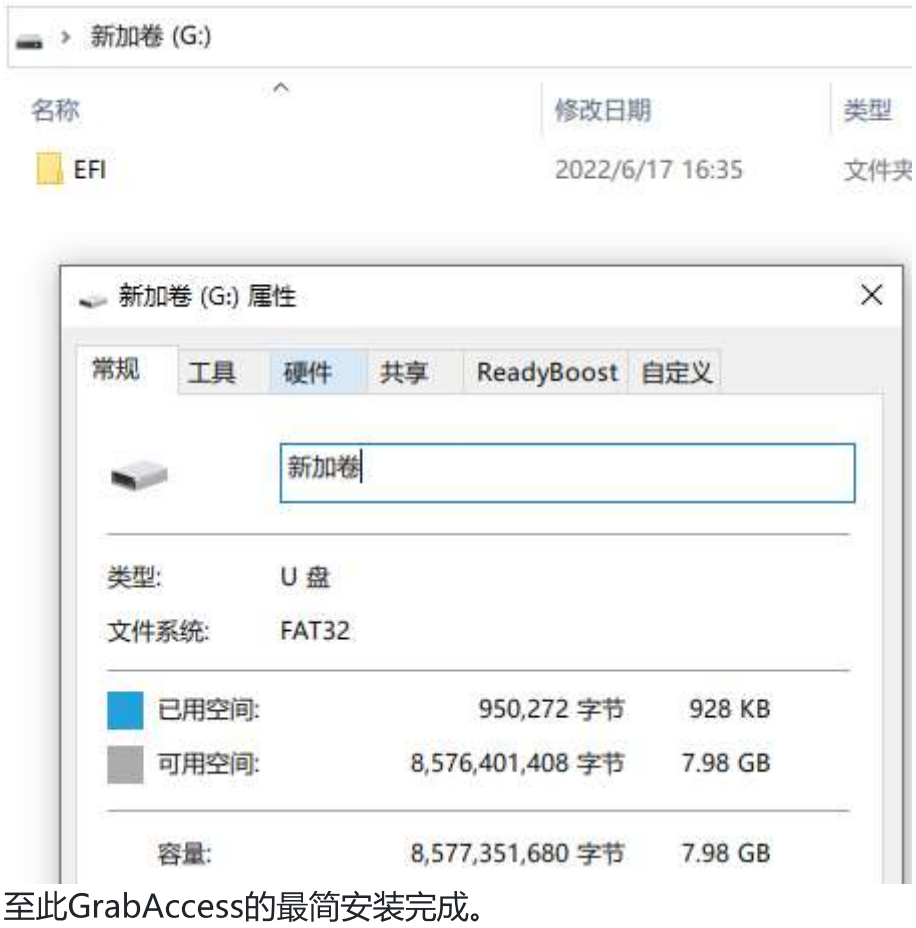
其最主要的优势是成功率高。在实战中我们发现Kon-boot绕过成功率非常之不稳定，尤其是针对Windows 10。

但在目前，GrabAccess仅支持UEFI引导的64位系统。针对Windows xp，或MBR引导的Windows 7，仍推荐Kon-Boot。

快速开始

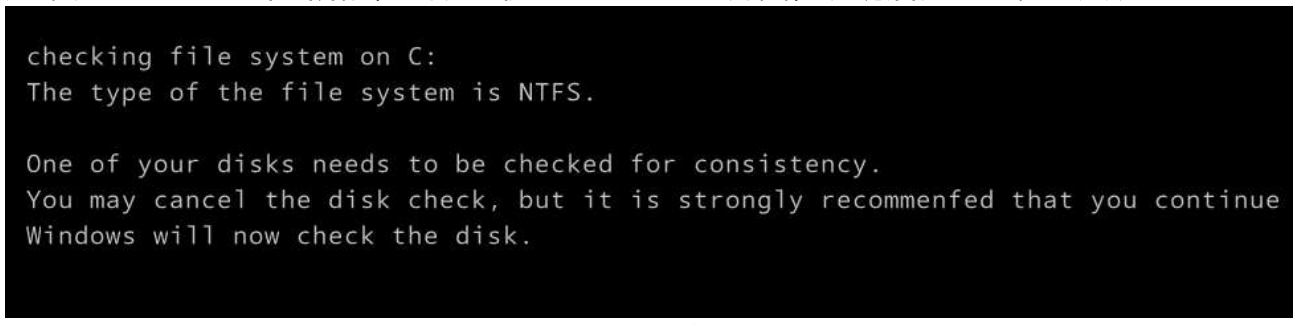
GrabAccess最基础的功能是安装Shift键后门，将Windows粘滞键替换为任务管理器。在不登陆的情况下，也可以执行系统命令或读写文件。

1. 准备一个U盘。如果是FAT、FAT16或FAT32格式，则可以不删除已有的文件。否则需要格式化为上述格式。
2. 下载GrabAccess，解压，将EFI文件夹拷贝到U盘根目录。



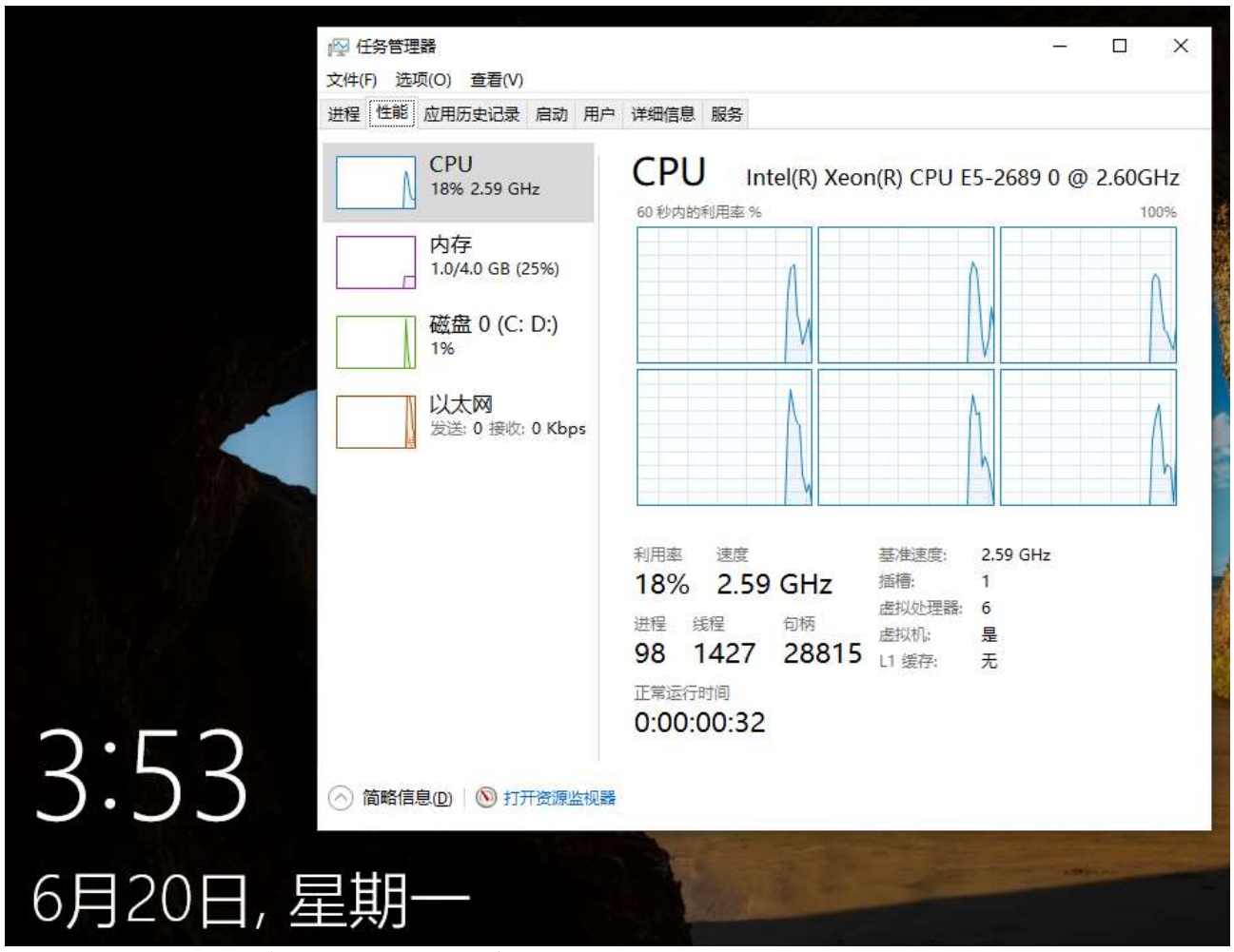
3. 至此GrabAccess的最简安装完成。
4. 将U盘插入电脑，重启电脑。在启动时进入BIOS菜单。
5. 选择从U盘启动，或设置U盘为第一启动项。如图所示，最后一个启动项是U盘，选择其启动即可。（如果BIOS开启了Security Boot，还需将其设置为DISABLE）

6. 如果在Windows引导阶段，出现了伪造的CHKDSK界面，说明后门已经植入成功。

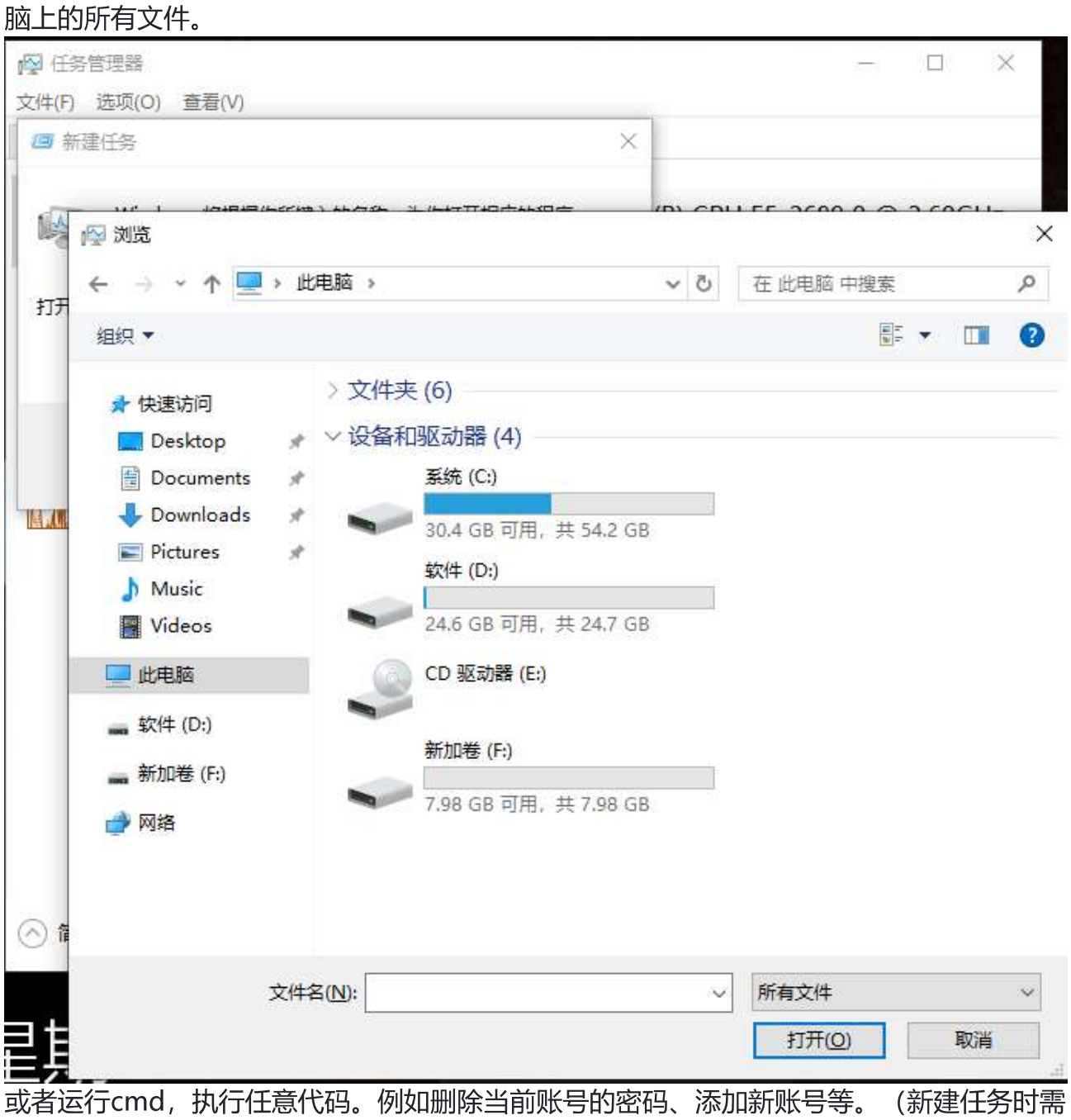


7. 在登录界面，连续按下五次Shift键，即可唤出任务管理器。

收起



8. 点击文件-运行新任务-浏览，将右下角的“文件类型”选择为所有文件，即可查看、读写电脑上的所有文件。



9. 或者运行cmd，执行任意代码。例如删除当前账号的密码、添加新账号等。（新建任务时需要勾选“以系统管理权限创建此任务“）

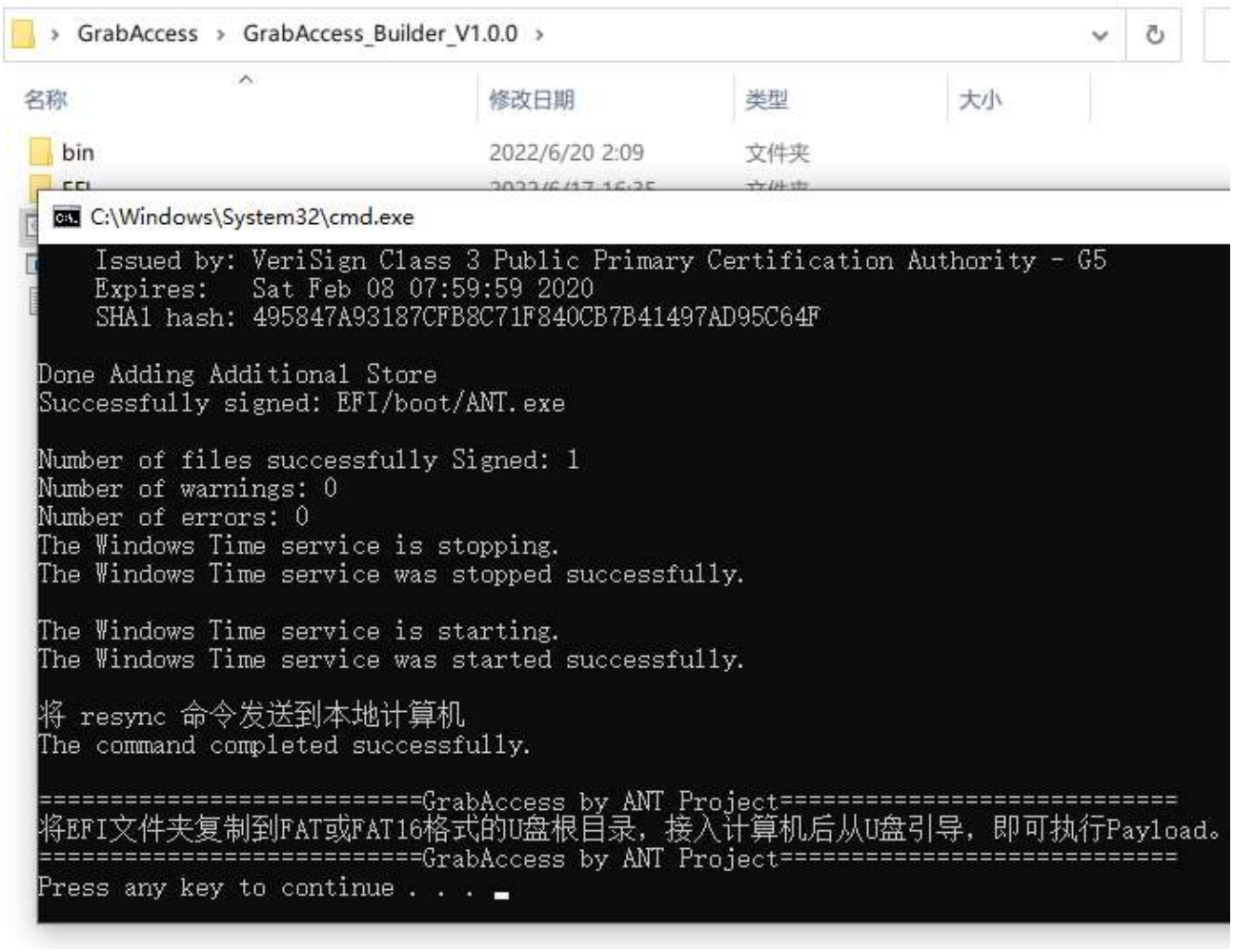
收起

自动化植入木马

GrabAccess可以自动化植入木马。写入指定的程序，并设置自启动。操作过程与上一章节类似，但需提前将GrabAccess与木马程序打包。关键步骤如下：

1. 下载GrabAccess_Builder，解压。

2. 将要植入的木马程序命名为payload.exe，覆盖GrabAccess_Builder目录下的同名文件。
3. 运行build.bat。



4. 将EFI文件夹拷贝到U盘根目录。其后操作与上一章相同。
5. 在Windows启动后，木马就已经完成植入。拔出U盘，跑路即可。（如果目标存在Bitlocker，在出现Bitlocker界面时，就可以拔U盘跑路。但在此之后目标电脑须正常登录，木马才会植入。如果在Bitlocker界面直接关机，GrabAccess会失效）

收起

附件列表：

1. GrabAccess_V1.0.0.zip：最简版本，将EFI文件夹放入U盘即可使用。
2. GrabAccess_Builder_V1.0.0.zip：自动植入指定文件，需要先将文件与GrabAccess打包。
3. GrabAccess_SourecCodeV1.0.0.zip、GrabAccess_SourecCodeV1.0.0.z01：源代码，包含Windows Native Application和Grub2

后记

GrabAccess背后的工作原理，源于Windows一项有趣功能（或者说是合法后门？）。

和Kon-boot篡改Windows内核不同，GrabAccess利用了Windows本身的功能：WPBT（Windows Platform Binary Table）。

WPBT常用于计算机制造商植入驱动软件、防丢软件。类似Bootkit病毒，一旦主板中植入了WPBT条目，无论是重装系统还是更换硬盘，只要使用Windows系统，开机后都会被安装指定程序。因此，该功能多次引发争议，但微软视其为正常功能，不准备修复或添加安全限制。使得我们可以将其当成一个适用范围广泛，并且利用稳定的后门使用。

WPBT的原始设计是，生产商在主板的UEFI固件中插入一个特定的ACPI条目。Windows引导时，会执行该条目指定的程序。但是，通过劫持UEFI的引导过程，攻击者可以插入WPBT条目，而无需修改主板固件。GrabAccess通过Grab2（Linux的bootloader），实现插入WPBT条目。

WPBT加载的程序，并非常见的Win32程序，而是Windows Native Application。该类程序在Windows初始化Win32子系统之前启动。其API和Win32 API不同，需要特殊编写。例如CHKDSK，就是Native APP。

Windows要求加载的Native APP经过签名。但不会对签名的有效性校验，即使签名过期或被吊销，也可执行。攻击者可以通过某些泄露的私钥，对Native APP进行签名。

GrabAccess是对WPBT武器化利用的一个开源实现。开源协议为GPL。读者可以按照需求二次开发，尤其是修改其中的Native APP。目前写入启动项和劫持Shift键的实现，都使用了最基础的手段。如有需要，可以自行编写更高级和隐蔽的后渗透技巧。

源代码包含两个部分。

其一是修改过的Grab2，其中包含一个用于加载WPBT的模块。即源码中的GrabAccess_V1.0.0.tar.xz。需要在Linux环境下编译。

第二部分是一个Windows Native Application，通过其写出文件、添加启动项、劫持Windows粘滞键。即源码中的WindowsNativeAPP。对其编译需要配置Windows Driver Kits环境。

序号	文件名称	下载次数
1	GrabAccess_V1.0.0.zip	15
2	GrabAccess_Builder_V1.0.0.zip	13
3	GrabAccess_SourceCode_V1.0.0.zip	129
4	GrabAccess_SourceCode_V1.0.0.z01	6

Alex Yang

BIOS设置密码、设置仅UEFI开启安全启动

关闭硬盘启动外其他启动项、开启TPM模块

笔记本设BIOS密码会写入EC芯片，抠电池、放电无解

限制硬盘启动外其他启动项可防止加载其它系统/引导

开启TPM并配合BitLocker防止硬盘拆下继续使用或盗用数据

确保万无一失

2022-07-13 00:11:49

点赞 1　回复

开源平台公众号

收起