Windows自启动项的查看和分析

胡正浩 5110369037

一、Windows系统自启动方法

（一）Logon

常规注册表启动项。

1、技术原理

系统启动时，会通过注册表中的常规启动项，如Run，RunOnce，StartupProgram，Shell等键值来加载程序，从而实现自启动。

2、实现细节

HKLM\system\currentcontrol set\control\terminal server\wds\rdpwd\StartupPrograms键的值中包含了启动程序名称，以逗号分隔。

HKLM\software\microsoft\windows nt\currentversion\winlogon\Userinit包含了用户登陆是启动的程序。逗号分隔。

HKLM\software\microsoft\windows nt\currentversion\winlogon\shell 指定了当userinit中的程序调用失败时，用于调用的程序。逗号分隔。

HKLM 以及 HKCU中的各种Run，RunOnce子键，指定了系统启动时调用的程序。

3、隐蔽性

Run和RunOnce子键，名声太响，隐蔽性弱。

Userinit关注度低一点，隐蔽性比较高。

StartupPrograms隐蔽性高，哪儿都搜不到相应的介绍。

Shell 隐蔽性高，只有当userinit中程序调用失败时才会用到shell，有userinit打掩护。

（二）Internet Explorer

IE浏览器BHO对象

1、技术原理

IE浏览器启动时会自动调用BHO对象

2、实现细节

IE的窗口打开时,先寻找HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ Explorer\Browser Helper Objects\里的CLSID,这些CLSID,都对应着相应的BHO插件，然后根据这个CLSID到HKCR下的CLSIDs里找到此插件的信息，包括文件位置等。IE根据找到的CLSID信息创建 BHO 对象,并且查找 IObjectWithSite 接口。IE把IWebBrowser2(浏览器插件)传到 BHO 的 SetSite 方法，在此方法中可挂载自己的事件处理方法。窗口关闭时,IE把 null 传到 BHO 的 SetSite 方法，此方法用来去掉挂载的事件处理方法。

3、隐蔽性

隐蔽性高。其运行时是作为IE的一个子进程运行的，不易被发现。

（三）Service

系统服务

1、技术原理

系统启动时会顺带启动设置成自动的系统服务

2、实现细节

在HKLM\SYSTEM\CurrentControlSet\Services\下添加一个新子键，Displayname为显示的服务名，ImagePath为调用的父进程，parameter子键下的ImagePath为程序的路径，start设为2即自启动。

3、隐蔽性

隐蔽性高。系统服务种类繁多，若不做签名验证无法检测出来。

（四）Drivers

系统驱动程序

1、技术原理

系统启动时需要加载驱动程序，通过搜索注册表找到需要启动的驱动程序。

2、实现细节

在HKLM\SYSTEM\CurrentControlSet\Services\下添加一个新子键，Displayname为显示的服务名，ImagePath为驱动程序的路径，start设为2即自启动。

3、隐蔽性

隐蔽性高。系统服务种类繁多，若不做签名验证无法检测出来。

（五）Scheduled Tasks

计划任务

1、技术原理

通过指定特定时间，特定程序，可以实现程序在指定时间自动运行，从而可以借此运行恶意软件。

2、实现细节

Windows 7以前的计划任务都以xml格式保存在C:\Windows\Tasks\目录下来实现的，访问没有权限要求。

Windows 7以后，计划任务的路径改为C:\Windows\System32\Tasks\，访问需要管理员权限。

3、隐蔽性

隐蔽性较低。计划任务是在用户态进行操作的，因此容易被发现。

（六）Known DLLs

知名动态链接库

1、技术原理

KnownDlls是windows下的一种用来缓存经常用到的DLL文件的机制。KnownDlls必须是在系统目录中，并且是在系统启动的时候，从注册表读取KnownDlls列表。之后，如果加载这个dll，首先搜索系统目录，其次搜索当前目录。

2、实现细节

在HKLM\system\currentcontrolset\control\session manager\knowndlls中添加子键名，将相应的dll放到系统文件夹下。

3、隐蔽性

隐蔽性高。因为KnownDll是系统默认的安全的程序，所以不会对其进行更进一步的检测。

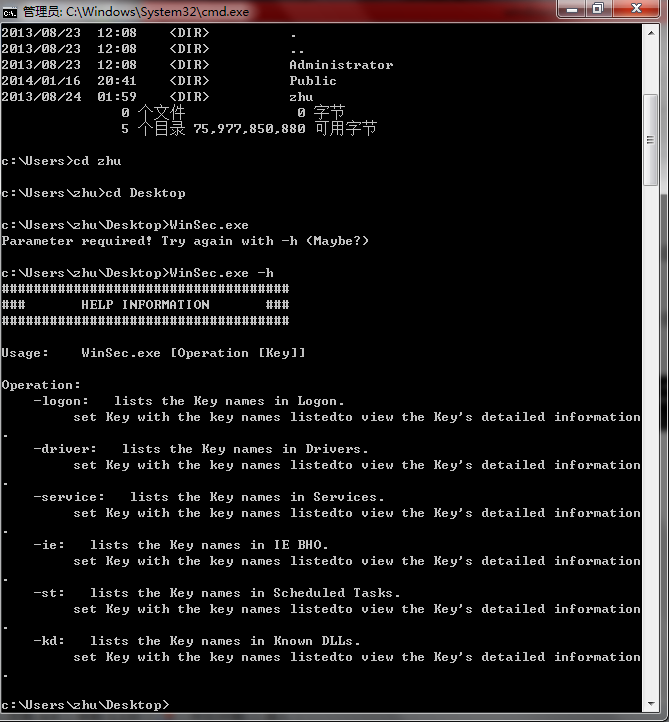
二、Windows 7 （64bit）自启动项查看工具

运行程序通过命令行进行操作。

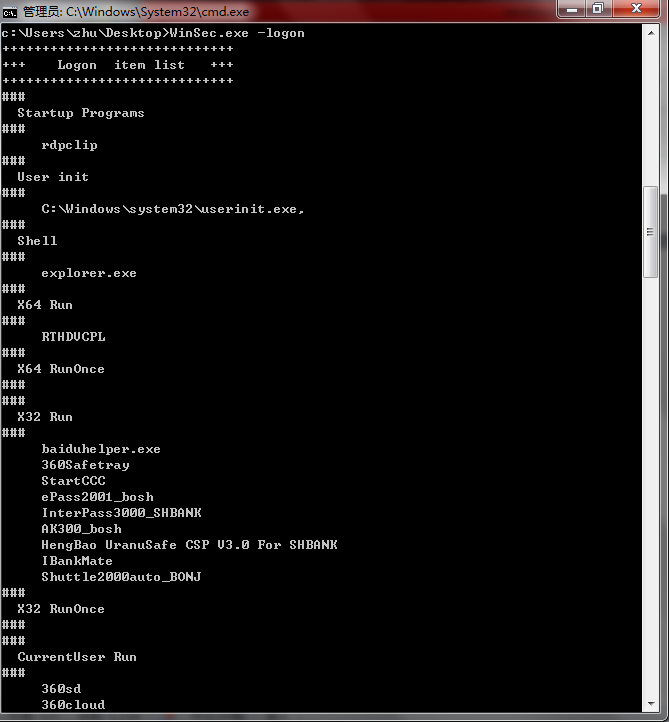
报错信息：



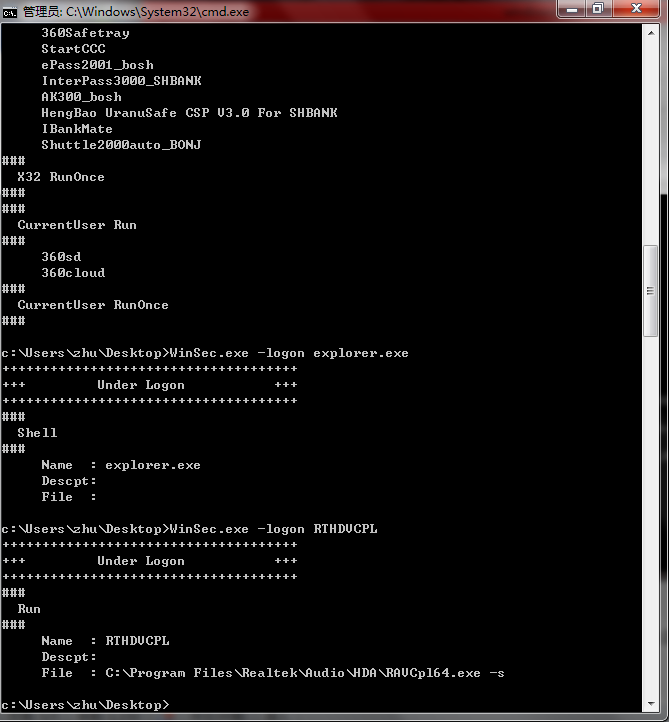
帮助信息：



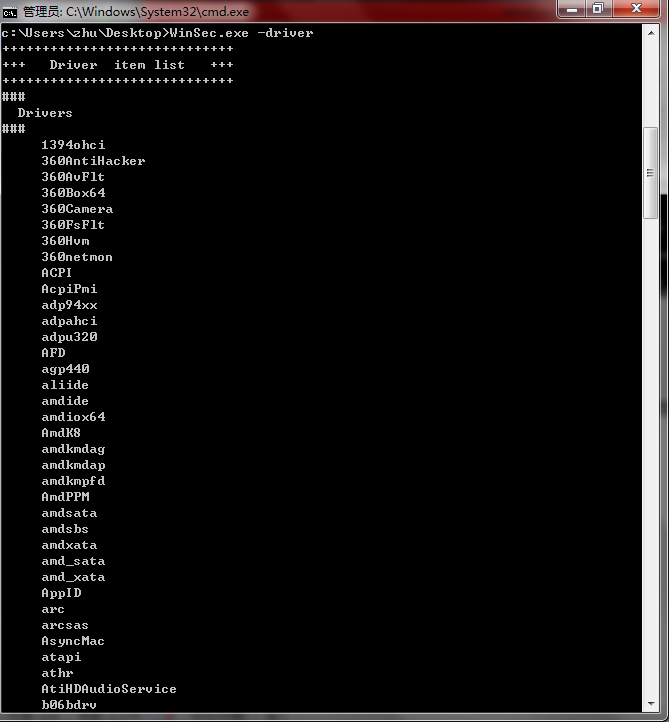
查看Logon：



查看Logon中单条自启动项的详细信息：



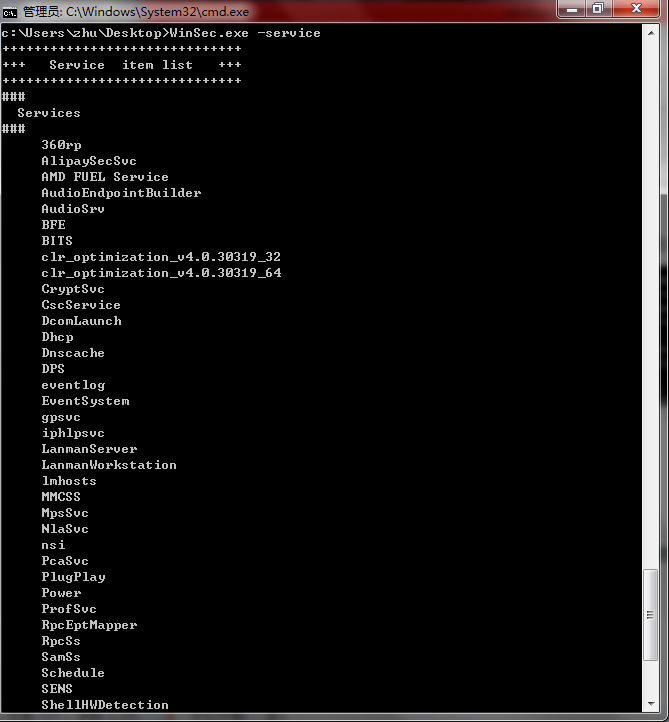
查看Drivers：



查看Drivers中单条自启动项的详细信息：



查看Service：



查看Service中单条自启动项的详细信息：



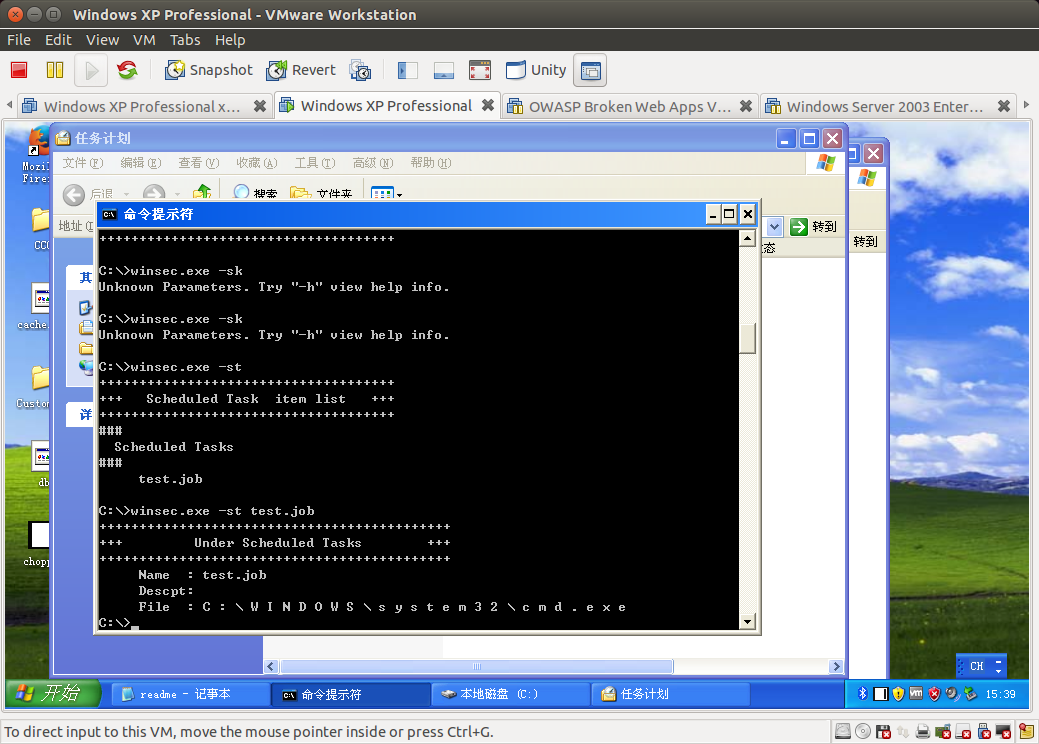
查看IE BHO：



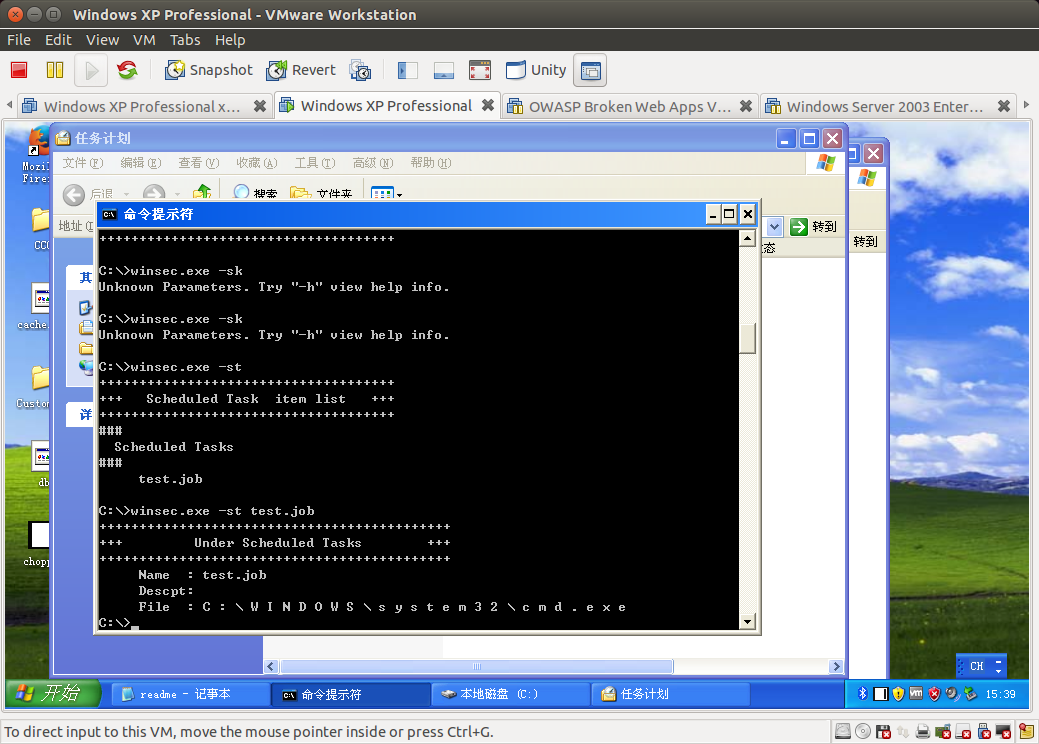
查看IE BHO单条自启动项的详细信息：



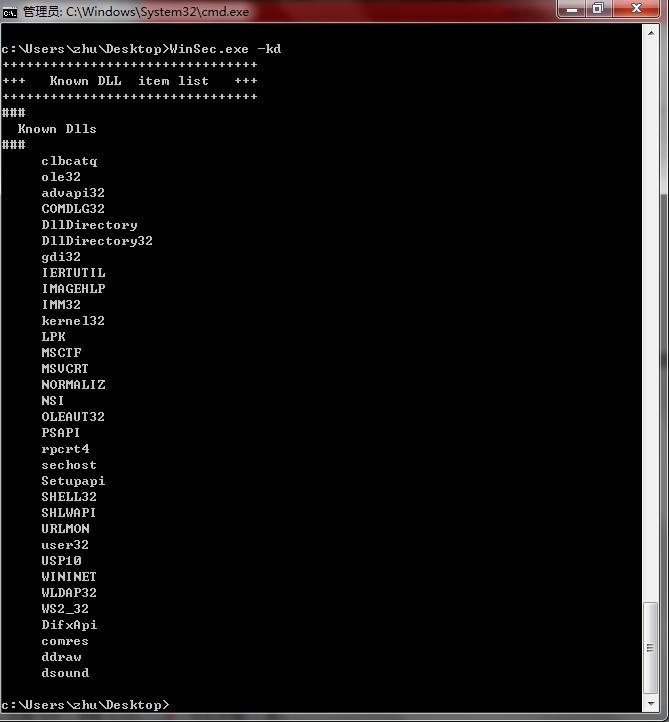
查看计划任务：



查看单条自启动项详细内容：



查看Known Dlls：



查看单条启动项详细信息：

