

Windows 自启动项的查看与分析

姓名：刘浩文 学号：517021911065 邮箱：IssacLiewX@sjtu.edu.cn

Windows 自启动项的查看与分析

Windows 自启动项

[从 Autoruns 软件开始探索](#)

[普通进行自启动项的查看](#)

[“启动”文件夹](#)

[注册表启动项](#)

[Run 键](#)

[RunOnce 键](#)

[RunServicesOnce 键](#)

[RunServices 键](#)

[load 键](#)

[Winlogon 键](#)

[其他注册表位置](#)

Windows 自启动项查看软件的实现

[开发环境](#)

[开发语言与架构](#)

[界面设计](#)

[自启动种类](#)

[Logon](#)

[Services](#)

[Drivers](#)

[Scheduled Tasks](#)

问题与感想

Windows 自启动项

为什么会有 Windows 自启动项？一些系统进程，如一些维护系统安全的进程与一些硬件驱动程序，需要在系统开机时就自动启动，否则会影响系统的启动或损害系统的功能。所以这些进程有必要设置成自启动。还有一些没有必要自启动的进程，但如果将其设置为自启动将会方便一些用户使用计算机功能，所以也可以将它们设置为自启动。

Windows 自动启动功能在给用户带来便捷的同时，也给病毒提供了便利的启动途径。所以无论是出于方便自己使用，还是防范病毒感染电脑，都有必要深挖一下 windows 中所有的启动项。

从 Autoruns 软件开始探索

Autoruns 是一款功能强大的管理开机自启动项目组的软件。

Autonums [691B\hongxing] - Sysinternals: www.sysinternals.com

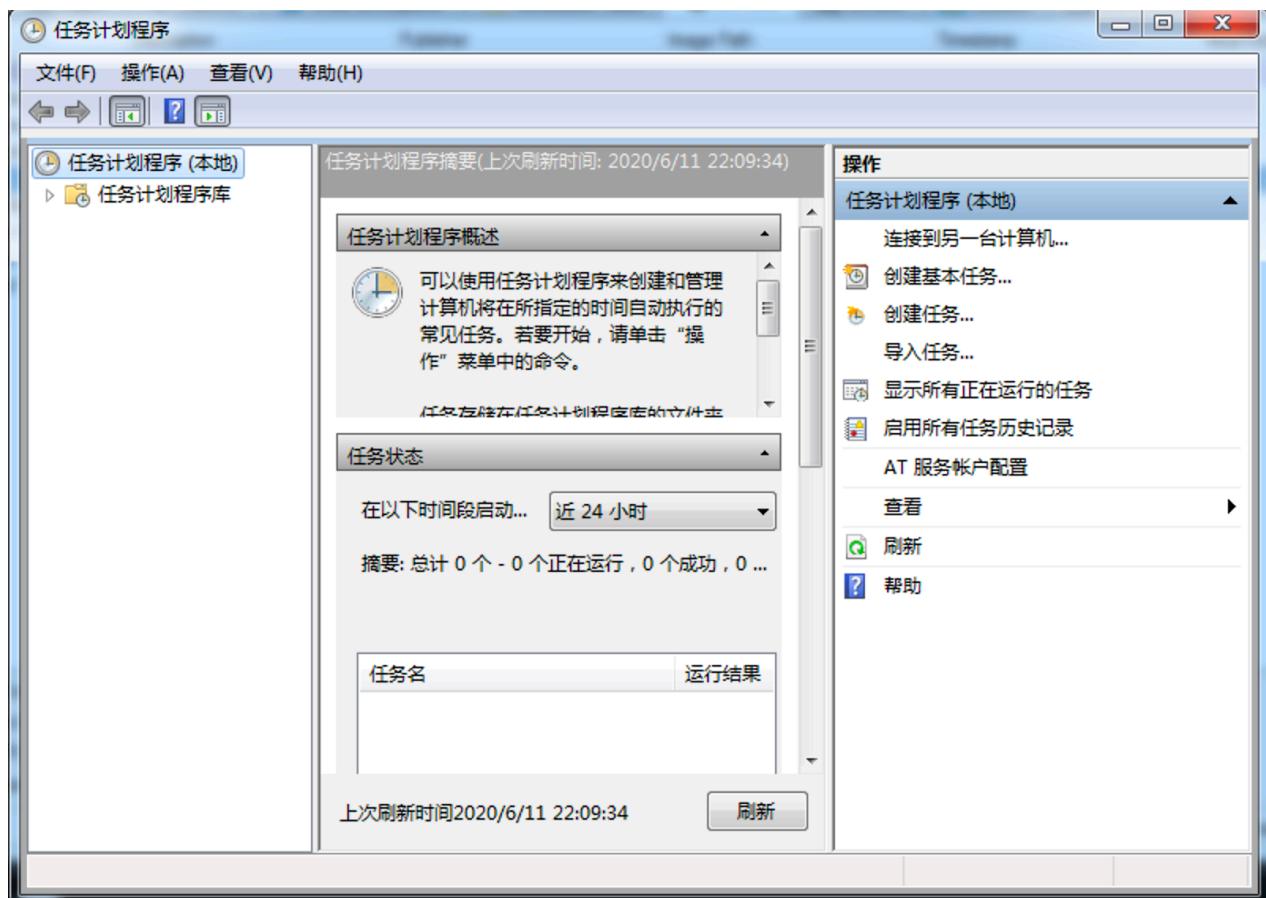
| Category | Description | Publisher | Image Path | Timestamp | VirusTotal |
|---|---|--|--|---|------------------|
| HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell | cmd.exe | Windows 命令处理程序 | (Verified) Microsoft Windows | c:\windows\system32\cmd.exe | 2014/12/28 14:19 |
| HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed Components | n/a | Microsoft IE SECURITY REGISTRATION | (Verified) Microsoft Corporation | c:\windows\system32\mscores.dll | 2019/3/4 20:54 |
| HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Active Setup\Installed Components | n/a | Microsoft .NET IE SECURITY REGISTRATION | (Verified) Microsoft Corporation | c:\windows\syswow64\mscores.dll | 2020/5/30 19:55 |
| HKEY_CURRENT_USER\Software\Classes\shell\shellEx\ContextMenuHandlers | PrToolsShellExt | Parallels Tools Shell Extension | (Verified) Parallels International GmbH | c:\program files (x86)\parallels\parallels tools\shellextensions\pritoolsshell... | 2020/4/13 1:30 |
| HKEY_CURRENT_USER\Software\Classes\Folder\shellEx\ContextMenuHandlers | PrToolsShellExt | Parallels Tools Shell Extension | (Verified) Parallels International GmbH | c:\program files (x86)\parallels\parallels tools\shellextensions\pritoolsshell... | 2020/4/13 1:30 |
| HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlaysIdentifiers | PrToolsShellExt | Parallels Tools Shell Extension | (Verified) Parallels International GmbH | c:\program files (x86)\parallels\parallels tools\shellextensions\pritoolsshell... | 2020/4/13 1:30 |
| Task Scheduler | | | | | |
| Microsoft\Windows\Windows Defender\WindowsDefender\BackgroundDownload | Visual Studio Background Download | (Verified) Microsoft Corporation | c:\program files (x86)\microsoft visual studio\installer\resources\app\servi... | 1908/12/24 14:15 | |
| Microsoft\Windows\Windows Defender\WindowsDefender\MicrosoftMalwareProtection\commandline | Microsoft Malware Protection Command Line Utility | (Not verified) Microsoft Corporation | c:\programdata\microsoft\windows defender\platform\4.18.2005.5-0\imp... | 1912/2/15 10:52 | |
| Microsoft\Windows\Windows Defender\WindowsDefender\MicrosoftMalwareProtection\commandline | Microsoft Malware Protection Command Line Utility | (Not Verified) Microsoft Corporation | c:\programdata\microsoft\windows defender\platform\4.18.2005.5-0\imp... | 1912/2/15 10:52 | |
| Microsoft\Windows\Windows Defender\WindowsDefender\MicrosoftMalwareProtection\commandline | Microsoft Malware Protection Command Line Utility | (Not Verified) Microsoft Corporation | c:\programdata\microsoft\windows defender\platform\4.18.2005.5-0\imp... | 1912/2/15 10:52 | |
| Microsoft\Windows\Windows Defender\WindowsDefender\WindowsDefender\WindowsDefender | Microsoft Malware Protection Command Line Utility | (Not Verified) Microsoft Corporation | c:\programdata\microsoft\windows defender\platform\4.18.2005.5-0\imp... | 1912/2/15 10:52 | |
| Parallels\Parallels Tools consistency check | Parallels Tools Service | (Verified) Parallels International GmbH | c:\program files (x86)\parallels\parallels tools\services\prl_tools_service.e... | 2020/4/13 2:12 | |
| HKLM\System\CurrentControlSet\Control\FontCache | FontCache3.0.0.0 | Windows Presentation Foundation Font Cache 3.0.0.0: 通过... | (Verified) Microsoft Corporation | c:\windows\microsoft.net\framework\64\v3.0\wpresentationfontcache.exe | 2019/1/26 12:17 |
| HKLM\System\CurrentControlSet\Control\FontCache | Parallels Coherence Service | Parallels Coherence Service: Provides support for the Coher... | (Verified) Parallels International GmbH | c:\program files (x86)\parallels\parallels tools\services\coherence.exe | 2020/4/13 2:13 |
| HKLM\System\CurrentControlSet\Control\FontCache | Parallels Tools Service | Parallels Tools Service: Provides support for the integrati... | (Verified) Parallels International GmbH | c:\program files (x86)\parallels\parallels tools\services\prl_tools_service.e... | 2020/4/13 2:12 |
| HKLM\System\CurrentControlSet\Control\FontCache | rpcapd | Remote Packet Capture Protocol v.0 (experimental): Allows ... | (Verified) Riverbed Technology, Inc. | c:\program files (x86)\winpcap\rpcapd.exe | 2013/3/9 2:8 |
| HKLM\System\CurrentControlSet\Control\FontCache | Steam Client Service | Steam Client Service: Steam Client Service monitors and up... | (Verified) Valve | c:\program files (x86)\common files\steam\steam\service.exe | 2020/4/28 5:54 |
| HKLM\System\CurrentControlSet\Control\FontCache | VSSStandardCollectorService150 | Visual Studio Standard Collector Service 15.0: Visual Studio ... | (Verified) Microsoft Corporation | c:\program files (x86)\microsoft visual studio\shared\commondiagnostics... | 2019/5/1 14:11 |
| HKLM\System\CurrentControlSet\Control\FontCache | WinDefnsvc | Windows Defender Antivirus Network Inspection Service: 防... | (Not verified) Microsoft Corporation | c:\programdata\microsoft\windows defender\platform\4.18.2005.5-0\imp... | 1936/4/9 1:55 |
| HKLM\System\CurrentControlSet\Control\FontCache | WinDefend | Windows Defender Antivirus Service: 防助用户防止恶意软件... | (Not Verified) Microsoft Corporation | c:\programdata\microsoft\windows defender\platform\4.18.2005.5-0\imp... | 2020/10/22 23:00 |
| HKLM\System\CurrentControlSet\Control\FontCache | BthA2dp | Microsoft Bluetooth A2dp driver: Bluetooth A2DP Driver | (Not verified) Microsoft Corporation | c:\windows\system32\drivers\btha2dp.sys | 1904/10/18 10:10 |
| HKLM\System\CurrentControlSet\Control\FontCache | iaLPSS1_GPIODriver | Intel(R) 带 I/O GPIO 主机控制驱动程序: Intel(R) Serial IO G... | (Verified) Intel Corporation - Client Components Group | c:\windows\system32\drivers\ialpss1_gpio.sys | 2015/2/2 17:00 |
| HKLM\System\CurrentControlSet\Control\FontCache | NPF | NetGroup Packet Filter Driver: npf.sys (NT5.0 AMD64) Kernel... | (Verified) Riverbed Technology, Inc. | c:\windows\system32\drivers\npf.sys | 2013/3/1 9:31 |
| HKLM\System\CurrentControlSet\Control\FontCache | prt_boot | prt_boot: Parallels Boot Camp Helper | (Verified) Parallels International GmbH | c:\windows\system32\drivers\prt_boot.sys | 2020/4/13 20:13 |
| HKLM\System\CurrentControlSet\Control\FontCache | prt_dd | Parallels Display Adapter (WDDM): Parallels Display Miniport | (Verified) Parallels International GmbH | c:\windows\system32\drivers\prt_kmdd.sys | 2020/4/13 20:12 |
| HKLM\System\CurrentControlSet\Control\FontCache | prt_fs | Parallels Shared Folders: Parallels Shared Folders Network P... | (Verified) Parallels International GmbH | c:\windows\system32\drivers\prt_fs.sys | 2020/4/13 20:12 |
| HKLM\System\CurrentControlSet\Control\FontCache | prt_memdev | prt_memdev: (Verified) Parallels International GmbH | (Verified) Parallels International GmbH | c:\windows\system32\drivers\prt_memdev.sys | 2020/4/13 20:09 |
| HKLM\System\CurrentControlSet\Control\FontCache | prt_mouf | Parallels Mouse Synchronization Device: Parallels Mouse Sy... | (Verified) Parallels International GmbH | c:\windows\system32\drivers\prt_mouf.sys | 2020/4/13 20:09 |

Everything: 全部的开机自启动项都在这个标签下。

Logon: *LOGON* 进程是登录的初始者，也是用户在使用安装有 *NT* 计算机时通常会经历的登录阶段的前台程序。*LOGON*本身是个很特殊的应用程序。名字为登录，但是实际上并不负责登录验证。他仅仅收集用户名、密码、域的信息，进行一些特定的操作。当 *NT* 启动 *LOGON* 时，*LOGON* 会加载一些 *DLL*。恶意攻击者可能将带有恶意代码的 *DLL* 混入其中，使系统遭到破坏。由于攻击在用户登录时发生，且不能直接探测到，需要打开注册表对很多项进行分析，所以攻击隐蔽，危险性高。

Internet Explorer: 对应的是IE所有浏览器帮助对象（*BHO*）、网络 URL 地址搜索钩子、各类 *IE* 工具条以及 *IE* 常用工具栏按钮所对应的注册表子项和注册表值项值。

Scheduled Tasks: 在 *Windows* 中，系统有一项重要的“计划任务”功能，通过设置“计划任务”，可以将每天或某一天的某个时间需要做的事拟成计划，到约定的时间，不管在电脑上进行什么工作，系统都会提醒你或者启动设定好的任务程序。通过“开始->程序->附件->系统工具”可以找到并打开“计划任务”窗口。如果攻击者在“计划任务”中插入恶意程序让其定时自动执行，将使系统遭到破坏。不过由于“计划任务”有图形界面，用户可以打开进行快速检查有无恶意程序，所以隐蔽性低。



Services: 系统服务是一种应用程序类型，它在后台运行。服务应用程序通常可以在本地和通过网络为用户提供一些功能，例如客户端/服务器应用程序、Web服务器、数据库服务器以及其他基于服务器的应用程序。系统服务一般在后台运行。与用户运行的程序相比，服务不会出现程序窗口或对话框，只有在任务管理器中才能观察到它们的身影。Service 程序和普通的应用程序有一个根本的区别：Service 程序可以在无用户登录和用户已经注销的情况下运行，而应用程序在没有用户注销的时候是会被终止的。由于具备开机自启动功能，而且依靠 ROOTKIT 技术可以隐蔽运行，所以是隐蔽性高，危险性高。

Driver: 驱动程序一般指的是设备驱动程序（Device Driver），是一种可以使计算机和设备进行相互通信的特殊程序。相当于硬件的接口，操作系统只有通过这个接口，才能控制硬件设备的工作，假如某设备的驱动程序未能正确安装，便不能正常工作。然而硬件驱动程序属于操作系统内核态进程，权限高，若攻击者将恶意进程冒充硬件驱动程序，将可以造成很大危害，所以隐蔽性高而危害性大。

| File | Entry | Options | Help | Print Monitors | Logon | Explorer | Internet Explorer | Scheduled Tasks | Services | Drivers | Codecs | Boot Execute | Image Hijacks | Sidebar Gadgets | Office |
|--|--|---|--|-----------------|------------|----------|-------------------|-----------------|----------|---------|--------|--------------|---------------|-----------------|--------|
| Auton Entry | | | | | | | | | | | | | | | |
| HKLM\System\CurrentControlSet\Services | Description | Publisher | Image Path | Timestamp | VirusTotal | | | | | | | | | | |
| NPF | NetGroup Packet Filter Driver: npf.sys (NT5/6 AMD64)... | (Verified) CACE Technologies, Inc. | c:\windows\system32\drivers\npf.sys | 2009/10/21 2:00 | | | | | | | | | | | |
| prl_boot | prl_boot: Parallels Boot Camp Helper | (Verified) Parallels International GmbH | c:\windows\system32\drivers\prl_boot.sys | 2020/4/13 20:13 | | | | | | | | | | | |
| prl_dd | Parallels Display Adapter (WDDM): Parallels Display M... | (Verified) Parallels International GmbH | c:\windows\system32\drivers\prl_kmd.sys | 2020/4/13 20:12 | | | | | | | | | | | |
| prl_fs | Parallels Shared Folders: Parallels Shared Folders Netw... | (Verified) Parallels International GmbH | c:\windows\system32\drivers\prl_fs.sys | 2020/4/13 20:12 | | | | | | | | | | | |
| prl_memdev | prl_memdev: | (Verified) Parallels International GmbH | c:\windows\system32\drivers\prl_memdev.sys | 2020/4/13 20:09 | | | | | | | | | | | |
| prl_mouf | Parallels Mouse Synchronization Device: Parallels Mou... | (Verified) Parallels International GmbH | c:\windows\system32\drivers\prl_mouf.sys | 2020/4/13 20:09 | | | | | | | | | | | |
| prl_stg | Parallels paravirt disk filter: Parallels Disk Filter | (Verified) Parallels International GmbH | c:\windows\system32\drivers\prl_stg.sys | 2020/4/13 20:13 | | | | | | | | | | | |
| prl_tg | Parallels Tool Device: Parallels Tool Driver | (Verified) Parallels International GmbH | c:\windows\system32\drivers\prl_tg.sys | 2020/4/13 20:09 | | | | | | | | | | | |
| GPU | VGPU: | | File not found: System32\drivers\vgvkmnd.sys | | | | | | | | | | | | |
| WinDriver6 | WinDriver6: WinDriver Device Driver 10.21 | (Verified) Jungo LTD | c:\windows\system32\drivers\windrv6.sys | 2010/8/31 19:15 | | | | | | | | | | | |
| XilinxPC4Driver | XilinxPC4Driver: Xilinx PC4 Driver | (Verified) Xilinx | c:\windows\system32\drivers\xpc4drv.sys | 2007/5/9 2:54 | | | | | | | | | | | |

Ready. | Signed Windows Entries Hidden.

普通进行自启动项的查看

“启动”文件夹

“开始→程序”，会发现一个“启动”菜单，这就是最经典的Windows启动位置，右击“启动”菜单选择“打开”即可将其打开，如所示，其中的程序和快捷方式都会在系统启动时自动运行。最常见的启动位置如下：

- 1 当前用户: <\documents and settings\用户名\「开始」菜单\程序\启动>
- 2 所有用户: <\documents and settings\allusers\「开始」菜单\程序\启动>

注册表启动项

注册表是启动程序藏身之处最多的地方，主要有以下几项：

Run 键

Run键是病毒最青睐的自启动之所，该键位置是

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run] 、
[HKEY_CURRENT_
USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run] 、 [HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]，其下的所有程序在每次启动登录时都会按顺序自动执行。

RunOnce 键

RunOnce 位于

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce] 和
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce] 键，与 Run
不同的是， RunOnce 下的程序仅会被自动执行一次。

RunServicesOnce 键

`RunServicesOnce` 键位于

`[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]` 和

`[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]`

下，其中的程序会在系统加载时自动启动执行一次。

RunServices 键

`RunServices` 继 `RunServicesOnce` 之后启动的程序，位于注册表

`[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices]` 和

`[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]` 键。

load键

`[HKEY_CURRENT_USER\Software\Microsoft\WindowsNT\CurrentVersion\Windows]` 下的 `load`

键值的程序也可以自启动。

Winlogon键

该键位于位于注册表

`[HKEY_CURRENT_USER\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon]` 和

`[HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon]`，注意下面的 `Notify`、`Userinit`、`Shell` 键值也会有自启动的程序，而且其键值可以用逗号分隔，从而实现登录的时候启动多个程序。

其他注册表位置

还有一些其他键值，经常会有一些程序在这里自动运行，如：

`[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System\Shell1]`

`[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad]`

`[HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System\Scripts]`

`[HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\System\Scripts]`

Windows 自启动项查看软件的实现

开发环境

由于目前只有 *macOS* 机器，因此只能使用虚拟机进行开发。

物理主机系统：*macOS Catalina 10.15.4*

虚拟机系统：*Windows 10 专业版 x64*

计算机名：*691B*

虚拟机软件：*Parallels Desktop 15 for Mac Pro Edition, version 15.1.4 (47270)*

编程环境(IDE)：*Visual Studio 2019*

开发语言与架构

语言: C++

架构: MFC 应用

界面设计

由于没有使用过 C# 语言, 而 C 也只在操作系统进行底层编程时使用过, 所以我在 C/C++/C# 这三种可选的编程语言中选择了使用相对较多的 C++。但由于这学期的其他项目一直都在用 python 进行编程, 对 C++ 已经比较生疏, 且也没有使用 C++ 开发过有图形界面的程序, 所以开发过程可谓充满艰难。

一开始是在网上查找相关资料: 如何使用 C++ 进行图形界面开发, 学着直接使用 windows API 进行图形界面开发。然而花了很多精力也达不到好的效果, 特别是要与 Windows 自启动项查看结合。在与同学进行交流后, 了解了 Visual Studio 自带的 MFC 框架。

MFC (Microsoft Foundation Classes) 是微软基础类库的简称, 是微软公司实现的一个 C++ 类库, 主要封装了大部分的 windows API 函数。MFC 除了是一个类库以外, 还是一个框架, 在 vc++ 里新建一个 MFC 的工程, 开发环境会自动帮你产生许多文件, 同时它使用了 mfcxx.dll。xx是版本, 它封装了 mfc 内核, 所以你在你的代码看不到原本的 SDK 编程中的消息循环等等东西, 因为 MFC 框架帮你封装好了, 这样你就可以专心的考虑你程序的逻辑, 而不是这些每次编程都要重复的东西, 但是由于是通用框架, 没有最好的针对性, 当然也就丧失了一些灵活性和效率。但是 MFC 的封装很浅, 所以效率上损失不大。

由于我在程序前端开发和 MFC 都不熟悉, 所以我前期大量的时间花在学习 C++ MFC 的控件与前端界面的实现。本是想用 Autoruns 程序作为模板, 但最后能力有限未能实现, 于是改为基于 对话框 编程。

自启动种类

Logon

一开始仅查找 Autoruns 软件中显示的我的 Windows7 虚拟机中的几个键: HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell、HKCU\Software\Microsoft\Windows\CurrentVersion\Run、HKLM\Software\Microsoft\Active Setup\Installed Components、HKLM\Software\Wow6432Node\Microsoft\Active Setup\Installed Components。但和同学交流后想起老师说过的 Autoruns 似乎会自动隐藏空键, 所以赶忙把 Autoruns 的设置调为空项也能显示, 果然多出了许多键:

| Autoruns [JD88\hongxing] - Sysinternals: www.sysinternals.com | | | | | | |
|--|---|------------------------------|---|-------------------|------------|-------------------|
| File | Entry | Options | User | Help | | |
| Print Monitors | | LSA Providers | | Network Providers | | WMI |
| Everything | Logon | Explorer | Internet Explorer | Scheduled Tasks | Services | Drivers |
| Codecs | Boot Execute | Image Hijacks | AppInit | KnownDLLs | Winlogon | Winsock Providers |
| Autorun Entry | Description | Publisher | Image Path | Timestamp | VirusTotal | |
| HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Startup | RDP Clip 监视程序 | (Verified) Microsoft Windows | c:\windows\system32\rdpclip.exe | 2010/11/21 11:33 | | |
| HKCU\Software\Policies\Microsoft\Windows\System\Scripts\Startup | | | | 2010/11/20 19:04 | | |
| HKCU\Software\Policies\Microsoft\Windows\System\Scripts\Logon | | | | 2020/6/11 21:54 | | |
| HKLM\Software\Policies\Microsoft\Windows\System\Scripts\Logon | | | | 2020/5/11 21:09 | | |
| HKCU\Environment\UserInitMprLogonScript | | | | 2020/6/11 21:54 | | |
| HKLM\Environment\UserInitMprLogonScript | | | | 2020/6/11 21:54 | | |
| HKLM\Software\Microsoft\Windows\CurrentVersion\Winlogon\Userinit | C:\Windows\system32\userinit.exe 登录应用程序 | (Verified) Microsoft Windows | c:\windows\system32\userinit.exe | 2010/11/20 18:10 | | |
| HKLM\Software\Microsoft\Windows\CurrentVersion\Winlogon\VmApplet | SystemPropertiesPerformance.exe 更改计算机性能设置 | (Verified) Microsoft Windows | c:\windows\system32\systempropertiesperformance.exe | 2020/6/11 21:54 | | |
| HKLM\Software\Policies\Microsoft\Windows\System\Scripts\Shutdown | | | | 2009/7/14 7:56 | | |
| HKCU\Software\Policies\Microsoft\Windows\System\Scripts\Logoff | | | | 2020/6/11 21:54 | | |
| HKLM\Software\Policies\Microsoft\Windows\System\Scripts\Logoff | | | | 2020/6/11 21:54 | | |
| HKCU\Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Startup | | | | 2020/5/10 6:07 | | |
| HKLM\Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Startup | | | | 2020/5/11 20:57 | | |
| HKCU\Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Logon | | | | 2020/5/10 6:09 | | |
| HKLM\Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Logon | | | | 2020/6/11 21:54 | | |
| HKCU\Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Logoff | | | | 2020/6/11 21:54 | | |
| HKLM\Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Logoff | | | | 2020/6/11 21:54 | | |
| HKCU\Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Shutdown | | | | 2020/6/11 21:54 | | |
| HKLM\Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Shutdown | | | | 2020/6/11 21:54 | | |
| HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\Shell | | | | 2020/5/10 6:07 | | |
| HKCU\Software\Microsoft\Windows\NT\CurrentVersion\Winlogon\Shell | | | | 2020/5/11 20:57 | | |
| HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\Shell | | | | 2020/5/10 6:09 | | |
| HKLM\Software\Microsoft\Windows\NT\CurrentVersion\Winlogon\Shell | | | | 2020/6/11 21:54 | | |
| explorer.exe Windows 资源管理器 | (Verified) Microsoft Windows | c:\windows\explorer.exe | 2010/11/20 18:21 | | | |
| HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell | | | | 2009/7/14 12:49 | | |
| cmd.exe Windows 命令处理程序 | (Verified) Microsoft Windows | c:\windows\system32\cmd.exe | 2010/11/20 17:46 | | | |
| HKLM\Software\Microsoft\Windows\CurrentVersion\Winlogon\Taskman | | | | 2020/6/11 21:54 | | |

Ready.

| No Filter.

```

1 "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit",
2 "HKLM\System\CurrentControlSet\Control\Terminal
Server\Wds\rdpwd\StartupPrograms",
3 "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\AppSetup",
4 "HKLM\Software\Policies\Microsoft\Windows\System\Scripts\Startup",
5 "HKCU\Software\Policies\Microsoft\Windows\System\Scripts\Logon",
6 "HKLM\Software\Policies\Microsoft\Windows\System\Scripts\Logon",
7 "HKCU\Environment\UserInitMprLogonScript",
8 "HKLM\Environment\UserInitMprLogonScript",
9 "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit",
10 "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\VmApplet",
11 "HKLM\Software\Policies\Microsoft\Windows\System\Scripts\Shutdown",
12 "HKCU\Software\Policies\Microsoft\Windows\System\Scripts\Logoff",
13 "HKLM\Software\Policies\Microsoft\Windows\System\Scripts\Logoff",
14 "HKCU\Software\Microsoft\Windows\CurrentVersion\Group
Policy\Scripts\Startup",
15 "HKLM\Software\Microsoft\Windows\CurrentVersion\Group
Policy\Scripts\Startup",
16 "HKCU\Software\Microsoft\Windows\CurrentVersion\Group
Policy\Scripts\Logon",
17 "HKLM\Software\Microsoft\Windows\CurrentVersion\Group
Policy\Scripts\Logon",
18 "HKCU\Software\Microsoft\Windows\CurrentVersion\Group
Policy\Scripts\Logoff",
19 "HKLM\Software\Microsoft\Windows\CurrentVersion\Group
Policy\Scripts\Logoff",
20 "HKCU\Software\Microsoft\Windows\CurrentVersion\Group
Policy\Scripts\Shutdown",
21 "HKLM\Software\Microsoft\Windows\CurrentVersion\Group
Policy\Scripts\Shutdown",
22 "HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System\Shell",

```

```
23 "HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell",
24 "HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System\Shell",
25 "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell",
26 "HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell",
27 "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Taskman",
28 "HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Winlogon\AlternateShells\AvailableShells",
29 "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal
Server\Install\Software\Microsoft\Windows\CurrentVersion\Runonce",
30 "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal
Server\Install\Software\Microsoft\Windows\CurrentVersion\RunonceEx",
31 "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal
Server\Install\Software\Microsoft\Windows\CurrentVersion\Run",
32 "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-
Tcp\InitialProgram",
33 "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run",
34 "HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run",
35 "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run",
36 "HKCU\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run",
37 "HKCU\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnceEx",
38 "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce",
39 "HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce",
40 "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce",
41 "HKCU\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce",
42 "HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Load",
43 "HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run",
44 "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run",
45 "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run",
46 "HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components",
47 "HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components",
48 "HKLM\Software\Microsoft\Windows
NT\CurrentVersion\Windows\IconServiceLib",
49 "HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal
Server\Install\Software\Microsoft\Windows\CurrentVersion\Runonce",
50 "HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal
Server\Install\Software\Microsoft\Windows\CurrentVersion\RunonceEx",
51 "HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal
Server\Install\Software\Microsoft\Windows\CurrentVersion\Run",
52 "HKLM\SOFTWARE\Microsoft\Windows CE Services\AutoStartOnConnect",
53 "HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows CE
Services\AutoStartOnConnect",
54 "HKLM\SOFTWARE\Microsoft\Windows CE Services\AutoStartOnDisconnect",
55 "HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows CE
Services\AutoStartOnDisconnect",
```

Services

查看 `Autoruns` 的 `Services` 项发现通过 `Services` 系统服务实现自启动的条目全部在注册表的 `HKLM\System\CurrentControlSet\Services` 这一键下。

| HKLM\System\CurrentControlSet\Services | | | | | | |
|--|--|-----------|---|------------------|------------|--|
| Auton Entry | Description | Publisher | Image Path | Timestamp | VirusTotal | |
| AeLookupSvc | Application Experience: 在应用程序启动时为应用程... (Verified) Microsoft Windows | | c:\windows\system32\aeupsvc.dll | 2009/7/14 9:25 | | |
| ALG | Application Layer Gateway Service: 为 Internet 连接... (Verified) Microsoft Windows | | c:\windows\system32\alg.exe | 2009/7/14 9:08 | | |
| AppIDSvc | Application Identity: 确定并验证应用组件的标识。... (Verified) Microsoft Windows | | c:\windows\system32\appidsvc.dll | 2009/7/14 9:26 | | |
| AppInfo | Application Information: 使用辅助管理权限于交叉... (Verified) Microsoft Windows | | c:\windows\system32\appinfo.dll | 2010/11/20 20:52 | | |
| AppMgmt | Application Management: 通过组策略部署的软件。 (Verified) Microsoft Windows | | c:\windows\system32\appmgmts.dll | 2009/7/14 9:26 | | |
| AudioEndpointBuilder | Windows Audio Endpoint Builder: 管理 Windows 音频。 (Verified) Microsoft Windows | | c:\windows\system32\audiosrv.dll | 2010/11/20 20:51 | | |
| AutoSrv | Windows Audio: 管理基于 Windows 的程序的音频。 (Verified) Microsoft Windows | | c:\windows\system32\audiosrv.dll | 2010/11/20 20:51 | | |
| AxinstSV | ActiveX Installer (AxinstSV) 为从 Internet 安装 Active... (Verified) Microsoft Windows | | c:\windows\system32\axinstsv.dll | 2010/11/20 20:52 | | |
| BDESVC | BitLocker Drive Encryption Service: BDESVC 承载 Et... (Verified) Microsoft Windows | | c:\windows\system32\bdesvc.dll | 2009/7/14 9:25 | | |
| BFE | Base Filtering Engine: 基本端点引擎(BFE)是一种管... (Verified) Microsoft Windows | | c:\windows\system32\bfefw.dll | 2010/11/20 20:54 | | |
| BITS | Background Intelligent Transfer Service: 使用空闲带宽... (Verified) Microsoft Windows | | c:\windows\system32\bginfo.dll | 2010/11/20 21:13 | | |
| Browser | Computer Browser: 维护网络上计算机的更新列表。 ... (Verified) Microsoft Windows | | c:\windows\system32\browse.dll | 2010/11/20 20:55 | | |
| Bthserv | Bluetooth Support Service: 蓝牙服务支持实现。 ... (Verified) Microsoft Windows | | c:\windows\system32\bthserv.dll | 2009/7/14 9:25 | | |
| CertPropSvc | Certificate Propagation: 将用户证书和根证书从智能... (Verified) Microsoft Windows | | c:\windows\system32\certprop.dll | 2010/11/20 20:55 | | |
| cr_optimization_v_2.0.50727_32 | Microsoft .NET Framework NGEN v2.0.50727_X64_M... (Verified) Microsoft Corporation | | c:\windows\microsoft.net\Framework\v2.0.50727\mscorv... 2009/6/4 13:25 | | | |
| cr_optimization_v_2.0.50727_64 | Microsoft .NET Framework NGEN v2.0.50727_X64_M... (Verified) Microsoft Corporation | | c:\windows\microsoft.net\Framework64\v2.0.50727\mscor... 2009/6/4 11:59 | | | |
| COMSysApp | COM+ System Application: 管理基本组件对象模型 (... (Verified) Microsoft Windows | | c:\windows\system32\clifhost.exe | 2009/7/14 9:59 | | |
| CryptSvc | Cryptographic Services: 提供四种安全管理服务: 目录... (Verified) Microsoft Windows | | c:\windows\system32\cryptsvc.dll | 2010/11/20 21:00 | | |
| CscService | Offline Files: 脱机文件服务在脱机文件存储中执行... (Verified) Microsoft Windows | | c:\windows\system32\cscsvc.dll | 2010/11/20 21:00 | | |
| DoomLaunch | DCOM Server Process Launcher: DCOMLAUNCH 服... (Verified) Microsoft Windows | | c:\windows\system32\dcopcs.dll | 2010/11/20 21:13 | | |
| DefragSVC | Disk Defragmenter: 提供磁盘碎片整理功能。 (Verifi... (Verified) Microsoft Windows | | c:\windows\system32\defragsvc.dll | 2009/7/14 9:26 | | |
| Dhcpc | DHCP Client: 为计算机注册并更新 IP 地址。如... (Verified) Microsoft Windows | | c:\windows\system32\dhcpcore.dll | 2010/11/20 20:57 | | |
| DnsCache | DNS Client: DNS 客户端服务(dnscache)缓存域名系... (Verified) Microsoft Windows | | c:\windows\system32\dnssrv.dll | 2010/11/20 20:58 | | |
| dot3svc | Wired AutoConfig: 有线自动配置(DOT3 SVC)服务员... (Verified) Microsoft Windows | | c:\windows\system32\dot3svc.dll | 2010/11/20 20:58 | | |
| DPS | Diagnostic Policy Service: 诊断策略服务启用了 Win... (Verified) Microsoft Windows | | c:\windows\system32\dps.dll | 2010/11/20 20:58 | | |
| EapHost | Extensible Authentication Protocol: 可扩展的身份验... (Verified) Microsoft Windows | | c:\windows\system32\eapsc.dll | 2009/7/14 9:26 | | |
| EFS | Encrypting File System (EFS): 提供使用在 NTFS 文件... (Verified) Microsoft Windows | | c:\windows\system32\eaes.exe | 2009/7/14 7:20 | | |
| ehRecvr | Windows Media Center Receiver Service: 电视或 FM ... (Verified) Microsoft Windows | | c:\windows\ehome\ehrecvr.exe | 2010/11/20 19:19 | | |
| ehSched | Windows Media Center Scheduler Service: 在 Windows... (Verified) Microsoft Windows | | c:\windows\ehome\ehsched.exe | 2009/7/14 9:24 | | |
| eventlog | Windows Event Log: 此服务管理事件和事件日志。 ... (Verified) Microsoft Windows | | c:\windows\system32\wevtsvc.dll | 2010/11/20 21:15 | | |

Drivers

系统驱动程序和Services系统服务在同一个键下，所以只按照可执行文件名是否是以 `.sys` 结尾就可以区分是 Services 还是 Drivers 。

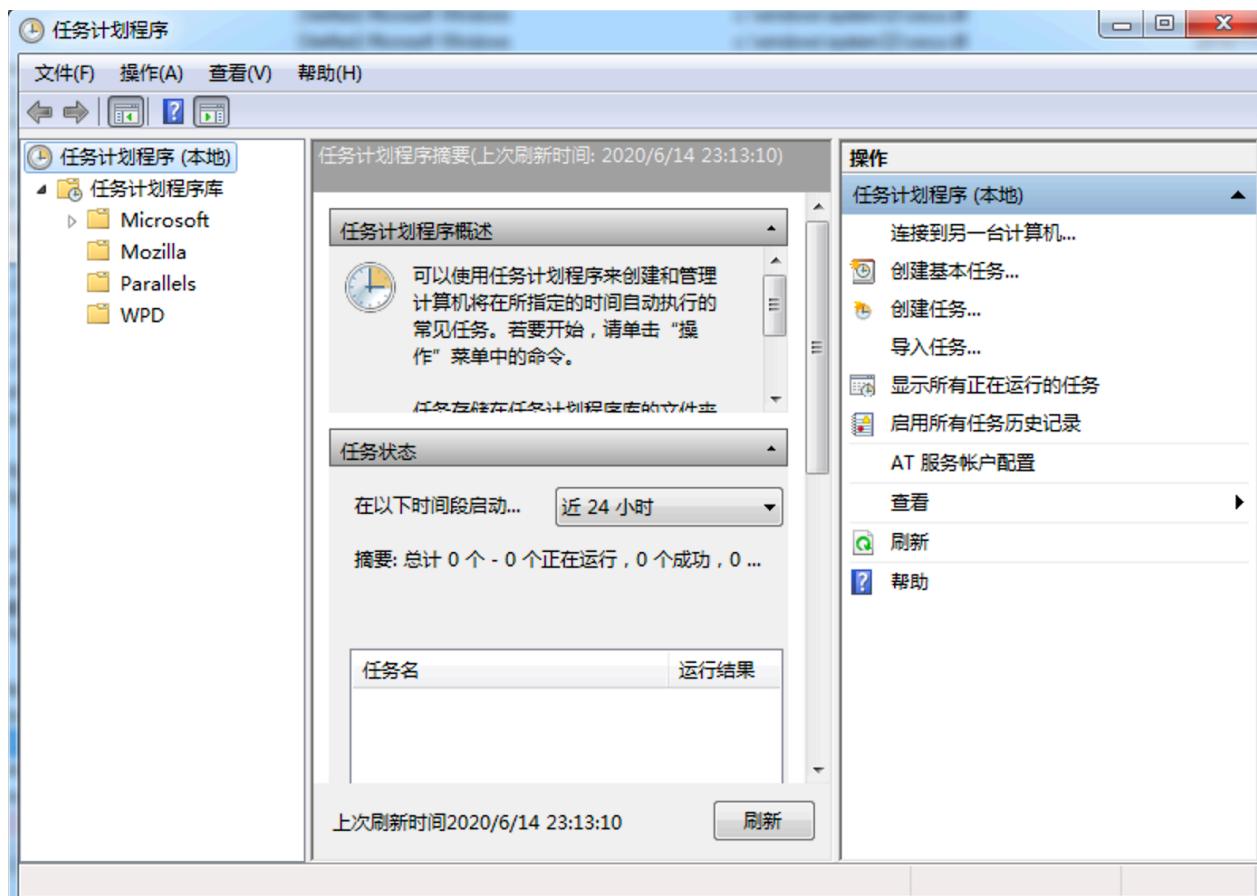
| HKLM\System\CurrentControlSet\Devices | | | | | | |
|---------------------------------------|---|-----------|--|------------------|------------|--|
| Auton Entry | Description | Publisher | Image Path | Timestamp | VirusTotal | |
| 1394hci | 1394 OHCI Compliant Host Controller: 1394 OpenHCI ... (Verified) Microsoft Windows | | c:\windows\system32\drivers\1394ohci.sys | 2010/11/20 18:44 | | |
| ACPI | Microsoft ACPI Driver: 用于 NT 的 ACPI 驱动程序 (Verified) Microsoft Windows | | c:\windows\system32\drivers\acpi.sys | 2010/11/20 17:19 | | |
| AcpiPmi | ACPI Power Meter Driver: ACPI Power Metering Driver (Verified) Microsoft Windows | | c:\windows\system32\drivers\acippmi.sys | 2010/11/20 17:30 | | |
| bdf94xx | adp94xx: Adaptec Windows SAS/SATA Stopport Driver (Verified) Microsoft Windows | | c:\windows\system32\drivers\adp94xx.sys | 2008/12/6 7:54 | | |
| adphaci | adphaci: Adaptec Windows SATA Stopport Driver (Verified) Microsoft Windows | | c:\windows\system32\drivers\adphaci.sys | 2007/5/2 1:30 | | |
| adu320 | adu320: Adaptec StopPort Ultra320 SCSI Driver (X64) (Verified) Microsoft Windows | | c:\windows\system32\drivers\adu320.sys | 2007/2/28 9:04 | | |
| AFD | Ancillary Function Driver for Winsock: Ancillary Function... (Verified) Microsoft Windows | | c:\windows\system32\drivers\afd.sys | 2010/11/20 17:23 | | |
| agp440 | Intel AGP Bus Filter: 440 NT AGP 适配器 (Verified) Microsoft Windows | | c:\windows\system32\drivers\agp440.sys | 2009/7/14 7:38 | | |
| alide | alide: ALI mini IDE Driver (Verified) Microsoft Windows | | c:\windows\system32\drivers\alide.sys | 2009/7/14 7:19 | | |
| amdiude | amdiude: AMD IDE 驱动程序 (Verified) Microsoft Windows | | c:\windows\system32\drivers\amdiude.sys | 2009/7/14 7:19 | | |
| AmDK8 | AMD K8 Processor Driver: Processor Device Driver (Verified) Microsoft Windows | | c:\windows\system32\drivers\amdk8.sys | 2009/7/14 7:19 | | |
| AmPPM | AMD Processor Driver: Processor Device Driver (Verified) Microsoft Windows | | c:\windows\system32\drivers\amppm.sys | 2009/7/14 7:19 | | |
| amdsata | amdsata: AHCI 1.2 Device Driver (Verified) Microsoft Windows | | c:\windows\system32\drivers\amdsata.sys | 2010/3/19 8:45 | | |
| amdsbs | amdsbs: AMD Technology AHCI Compatible Controller ... (Verified) Microsoft Windows | | c:\windows\system32\drivers\amdsbs.sys | 2009/3/21 2:36 | | |
| amdxdata | amdxdata: Storage Filter Driver (Verified) Microsoft Windows | | c:\windows\system32\drivers\amdxdata.sys | 2010/3/20 0:18 | | |
| AppID | AppID 驱动程序: 标识应用程序并强制执行软件限... (Verified) Microsoft Windows | | c:\windows\system32\drivers\appid.sys | 2010/11/20 18:14 | | |
| arc | arc: Adaptec RAID Stopport Driver (Verified) Microsoft Windows | | c:\windows\system32\drivers\arc.sys | 2007/5/25 5:27 | | |
| arcasas | arcasas: Adaptec SAS RAID WS03 Driver (Verified) Microsoft Windows | | c:\windows\system32\drivers\arcasas.sys | 2009/1/15 3:27 | | |
| AsyncMac | RAS 异步媒体驱动程序 - RAS 异步媒体驱动程序 (Verified) Microsoft Windows | | c:\windows\system32\drivers\asyncmac.sys | 2009/7/14 9:10 | | |
| atapi | IDE 适配器: ATAPI IDE Miniport Driver (Verified) Microsoft Windows | | c:\windows\system32\drivers\atapi.sys | 2009/7/14 7:19 | | |
| b190drv | Broadcom NetXtreme II VBD: Broadcom NetXtreme II ... (Verified) Microsoft Windows | | c:\windows\system32\drivers\b190drv.sys | 2009/2/14 6:18 | | |
| b57nd0a | Broadcom NetXtreme Gigabit Ethernet - NDIS 6.0: Bro... (Verified) Microsoft Windows | | c:\windows\system32\drivers\b57nd0a.sys | 2009/4/26 19:14 | | |
| Beep | Beep: BEEP Driver (Verified) Microsoft Windows | | c:\windows\system32\drivers\beep.sys | 2009/7/14 8:00 | | |
| blkdrive | blkdrive: BLK Drive Driver (Verified) Microsoft Windows | | c:\windows\system32\drivers\blkdrive.sys | 2009/7/14 7:35 | | |
| bowner | 浏览器支持驱动程序: 对计算机浏览器执浏览器服务... (Verified) Microsoft Windows | | c:\windows\system32\drivers\bowner.sys | 2009/7/14 7:23 | | |
| bRfL0 | Brother USB Mass-Storage Lower Filter Driver: Window... (Verified) Microsoft Windows | | c:\windows\system32\drivers\brflo.sys | 2006/8/7 9:51 | | |
| bRfUp | Brother USB Mass-Storage Upper Filter Driver: Window... (Verified) Microsoft Windows | | c:\windows\system32\drivers\brfup.sys | 2006/8/7 9:51 | | |
| brend | Brother MFC Serial Port Interface Driver (WDM): Brothe... (Verified) Microsoft Windows | | c:\windows\system32\drivers\brend.sys | 2006/8/7 9:51 | | |
| BSerWdm | Brother WDM Serial driver: Brother Serial driver (WDM ... (Verified) Microsoft Windows | | c:\windows\system32\drivers\bserwdm.sys | 2006/8/7 9:51 | | |
| BrLabMdm | Brother MFC USB Fax Only Modem: Brother MFC MDM... (Verified) Microsoft Windows | | c:\windows\system32\drivers\brlabmdm.sys | 2006/8/7 9:51 | | |

Ready.

| No Filter.

Scheduled Tasks

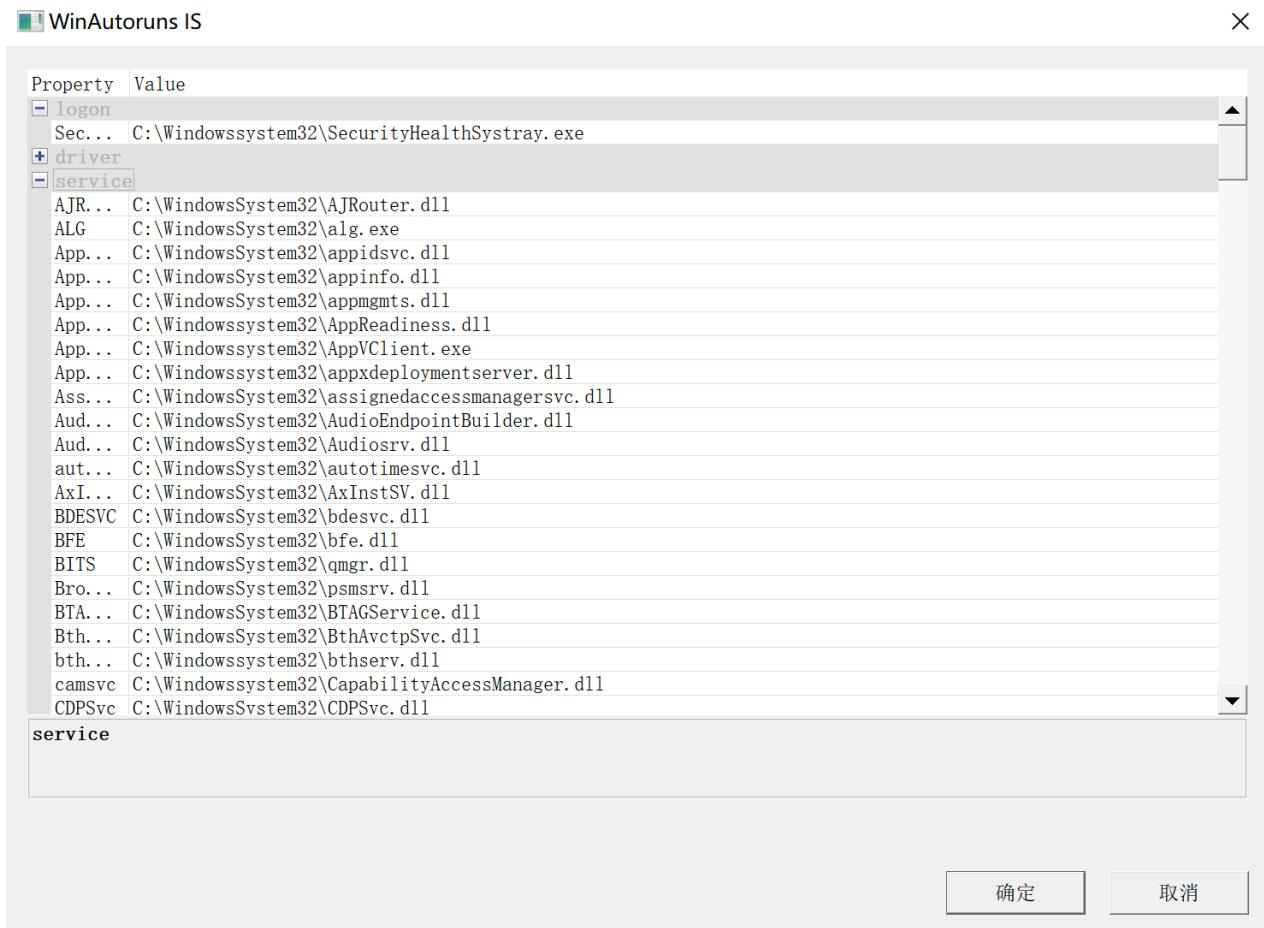
打开“任务计划”界面可以看到本地任务计划程序库，上网查询得知其位置是 `C:\Windows\System32\Tasks`，读取该位置查询即可。



| Autonums [7DB8\hongxing] - Sysinternals: www.sysinternals.com | | | | | | | |
|---|---|------------------------------|--|------------------|------------|------|------|
| File | | Entry | | Options | | User | Help |
| | | | | | | | |
| Autonum Entry | Description | Publisher | Image Path | Timestamp | VirusTotal | | |
| <input checked="" type="checkbox"/> Microsoft\Windows Defender\MP Sched... | Microsoft Malware Protection Command Line Utility | (Verified) Microsoft Windows | c:\program files\windows defender\npcmdrun.exe | 2009/7/14 7:53 | | | |
| <input type="checkbox"/> Microsoft\Windows\Active Directory Right... | Windows 权限管理客户端 | (Verified) Microsoft Windows | c:\windows\system32\msadm.dll | 2010/11/20 21:06 | | | |
| <input checked="" type="checkbox"/> Microsoft\Windows\Active Directory Right... | Windows 权限管理客户端 | (Verified) Microsoft Windows | c:\windows\system32\msadm.dll | 2010/11/20 21:06 | | | |
| <input type="checkbox"/> Microsoft\Windows\ApplID\PolicyConverter... | ApplID Policy Converter Task | (Verified) Microsoft Windows | c:\windows\system32\apppdpolicyconverter.exe | 2009/7/14 7:52 | | | |
| <input type="checkbox"/> Microsoft\Windows\ApplID\VerifierPublic... | ApplID Certificate Store Verification Task | (Verified) Microsoft Windows | c:\windows\system32\apppdcsstorecheck.exe | 2009/7/14 7:52 | | | |
| <input checked="" type="checkbox"/> Microsoft\Windows\Application Experience... | 应用程序经验反馈代理 | (Verified) Microsoft Windows | c:\windows\system32\agengt.exe | 2010/11/20 17:23 | | | |
| <input checked="" type="checkbox"/> Microsoft\Windows\Application Experience... | 应用程序经验反馈代理 | (Verified) Microsoft Windows | c:\windows\system32\sepdwu.dll | 2010/11/20 20:51 | | | |
| <input checked="" type="checkbox"/> Microsoft\Windows\Autochk\Proxy... | Autochk 代理 DLL | (Verified) Microsoft Windows | c:\windows\system32\acproxy.dll | 2009/7/14 9:24 | | | |
| <input checked="" type="checkbox"/> Microsoft\Windows\Bluetooth\Uninstall... | Bluetooth 卸载设备任务 | (Verified) Microsoft Windows | c:\windows\system32\bthudtask.exe | 2009/7/14 8:06 | | | |
| <input checked="" type="checkbox"/> Microsoft\Windows\CertificateServices... | DIMS 作业 DLL | (Verified) Microsoft Windows | c:\windows\system32\dimjob.dll | 2009/7/14 9:26 | | | |
| <input checked="" type="checkbox"/> Microsoft\Windows\CertificateServices... | DIMS 作业 DLL | (Verified) Microsoft Windows | c:\windows\system32\dimjob.dll | 2009/7/14 9:26 | | | |
| <input type="checkbox"/> Microsoft\Windows\DiskDiagnostic\Micro... | Windows 磁盘故障诊断模块 | (Verified) Microsoft Windows | c:\windows\system32\dimjob.dll | 2009/7/14 9:26 | | | |
| <input checked="" type="checkbox"/> Microsoft\Windows\DiskDiagnostic\Micro... | Windows 磁盘故障诊断模块 | (Verified) Microsoft Windows | c:\windows\system32\waspcoms.exe | 2010/11/20 17:53 | | | |
| <input checked="" type="checkbox"/> Microsoft\Windows\Customer Experience... | 内核 CEIP 任务 | (Verified) Microsoft Windows | c:\windows\system32\kernceip.dll | 2009/7/14 9:31 | | | |
| <input checked="" type="checkbox"/> Microsoft\Windows\Customer Experience... | USBCEIP 任务 | (Verified) Microsoft Windows | c:\windows\system32\usbceip.dll | 2009/7/14 9:33 | | | |
| <input checked="" type="checkbox"/> Microsoft\Windows\Defrag\Scheduled... | 磁盘碎片整理程序模块 | (Verified) Microsoft Windows | c:\windows\system32\defrag.exe | 2009/7/14 7:36 | | | |
| <input checked="" type="checkbox"/> Microsoft\Windows\Diagnosis\Schedule... | 脚本诊断计划任务 | (Verified) Microsoft Windows | c:\windows\system32\sdagschd.dll | 2009/7/14 9:33 | | | |
| <input checked="" type="checkbox"/> Microsoft\Windows\DiskDiagnostic\Micro... | Windows 磁盘故障诊断模块 | (Verified) Microsoft Windows | c:\windows\system32\ddfd.dll | 2009/7/14 9:26 | | | |
| <input checked="" type="checkbox"/> Microsoft\Windows\DiskDiagnostic\Micro... | Windows 磁盘诊断工具用户解析程序 | (Verified) Microsoft Windows | c:\windows\system32\ddfviz.exe | 2009/7/14 7:32 | | | |
| <input checked="" type="checkbox"/> Microsoft\Windows\Location\Notifications... | 位置助手 | (Verified) Microsoft Windows | c:\windows\system32\locationnotifications.exe | 2009/7/14 8:00 | | | |
| <input checked="" type="checkbox"/> Microsoft\Windows\Maintenance\WinSAT... | Windows 系统评估工具 API | (Verified) Microsoft Windows | c:\windows\system32\winstatsapi.dll | 2010/11/20 21:16 | | | |
| <input checked="" type="checkbox"/> Microsoft\Windows\Media Center\Activat... | 数字电视调谐器设备注册应用程序。 | (Verified) Microsoft Windows | c:\windows\ehome\ehprivjob.exe | 2010/11/20 19:13 | | | |
| <input checked="" type="checkbox"/> Microsoft\Windows\Media Center\Config... | 数字电视调谐器设备注册应用程序。 | (Verified) Microsoft Windows | c:\windows\ehome\ehprivjob.exe | 2010/11/20 19:13 | | | |
| <input checked="" type="checkbox"/> Microsoft\Windows\Media Center\Depat... | 数字电视调谐器设备注册应用程序。 | (Verified) Microsoft Windows | c:\windows\ehome\ehprivjob.exe | 2010/11/20 19:13 | | | |
| <input checked="" type="checkbox"/> Microsoft\Windows\Media Center\ehDF... | 数字电视调谐器设备注册应用程序。 | (Verified) Microsoft Windows | c:\windows\ehome\ehprivjob.exe | 2010/11/20 19:13 | | | |
| <input checked="" type="checkbox"/> Microsoft\Windows\Media Center\Install... | 数字电视调谐器设备注册应用程序。 | (Verified) Microsoft Windows | c:\windows\ehome\ehprivjob.exe | 2010/11/20 19:13 | | | |
| <input checked="" type="checkbox"/> Microsoft\Windows\Media Center\mcupd... | Windows Media Center 存储更新管理器 | (Verified) Microsoft Windows | c:\windows\ehome\mcupdate.exe | 2010/11/20 19:21 | | | |
| <input checked="" type="checkbox"/> Microsoft\Windows\Media Center\Media... | Windows Media Center 存储更新管理器 | (Verified) Microsoft Windows | c:\windows\ehome\mcupdate.exe | 2010/11/20 19:21 | | | |
| <input checked="" type="checkbox"/> Microsoft\Windows\Media Center\Object... | Windows Media Center 存储更新管理器 | (Verified) Microsoft Windows | c:\windows\ehome\mcupdate.exe | 2010/11/20 19:21 | | | |
| <input checked="" type="checkbox"/> Microsoft\Windows\Media Center\OCUR... | 数字电视调谐器设备注册应用程序。 | (Verified) Microsoft Windows | c:\windows\ehome\ehprivjob.exe | 2010/11/20 19:13 | | | |

Ready. | No Filter.

本来还想实现其他的自启动项查看，但无奈时间不够、能力有限，未能成行。



问题与感想

本门课程的大作业中遇到的最大问题就是对于 C/C++/C# 编程不熟悉，一直用惯了 *python* 方便的编程，对于这类较低层的语言编程便显得力不从心，指针、结构体、类型转换以及 *Visual Studio 2019* 的 C++ 版本等问题弄得我头秃。不过幸好任务本身不难，还有同学进行交流，了解使用 *MFC* 框架后也能较顺利地完成任务，只是最后的页面还是不尽如人意。另外由于一直使用 *macOS* 系统，对 *Windows* 系统已经不是很熟悉，*Visual Studio 2019* 的使用也不熟练，弄崩了好多次。

这个大作业让我有机会深入 *Windows* 的底层，去查看系统中的自启动项，来发现其中的“不法分子”，实际体验了系统安全人员的工作。另外还有机会使用 *SysinternalsSuite* 工具集进行了不少实验，有趣的同时也对 *Windows* 安全的了解更为深入。另外锻炼了 C++ 编程的能力，学习了微软的 MFC 框架。