**IP 监测**

**笔记本：** WEB
**创建时间：** 2019/4/18 16:39 **更新时间：** 2019/4/18 16:43

# IP 监测

使用schtasks /create /TN netstat5303 /sc MINUTE /MO 5 /TR "cmd /c netstat -bn > c:\netstatlog.txt"
命令创建计划任务netstat5303，如下图所示：

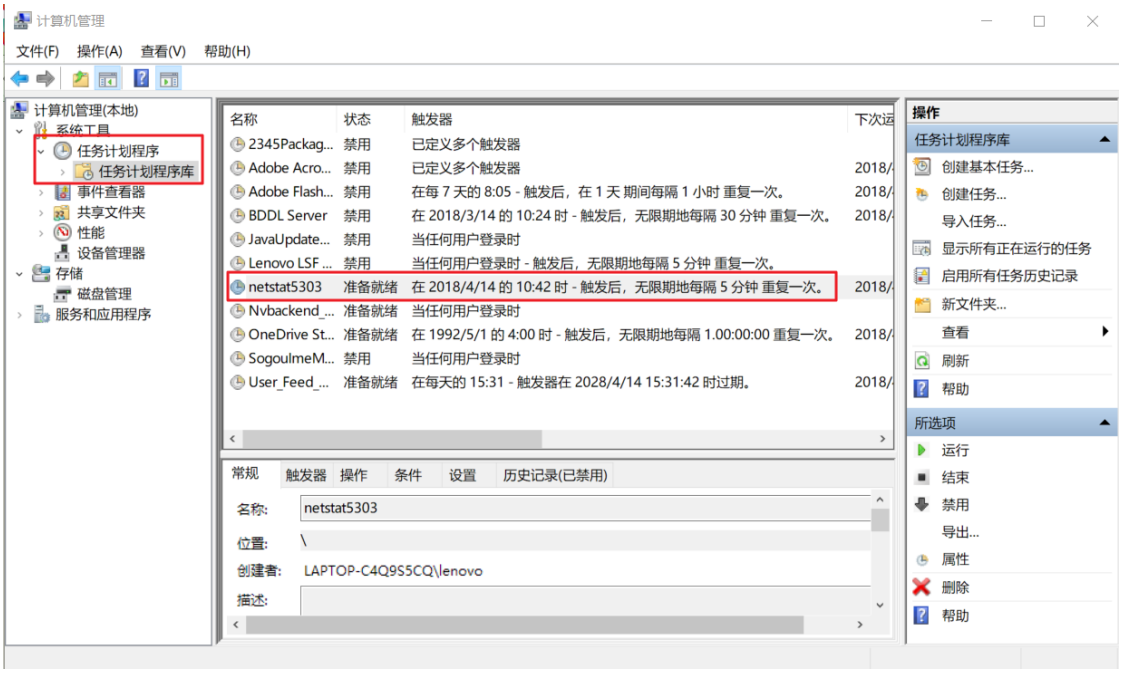
```
C:\WINDOWS\system32>schtasks /create /TN netstat5303 /sc MINUTE /MO 5 /TR "cmd /c netstat -
bn > c:\netstatlog.txt"
成功: 成功创建计划任务 "netstat5303"。

C:\WINDOWS\system32>
```

其中，TN是TaskName的缩写，我们创建的计划任务名是netstat5303；sc表示计时方式，我们以分钟计时填MINUTE；TR=Task Run，要运行的指令是 netstat -bn,b表示显示可执行文件名，n表示以数字来显示IP和端口。在C盘中创建一个netstat5303.bat脚本文件（可先创建txt文本文件，使用记事本写入后通过修改文件名来修改文件格式）

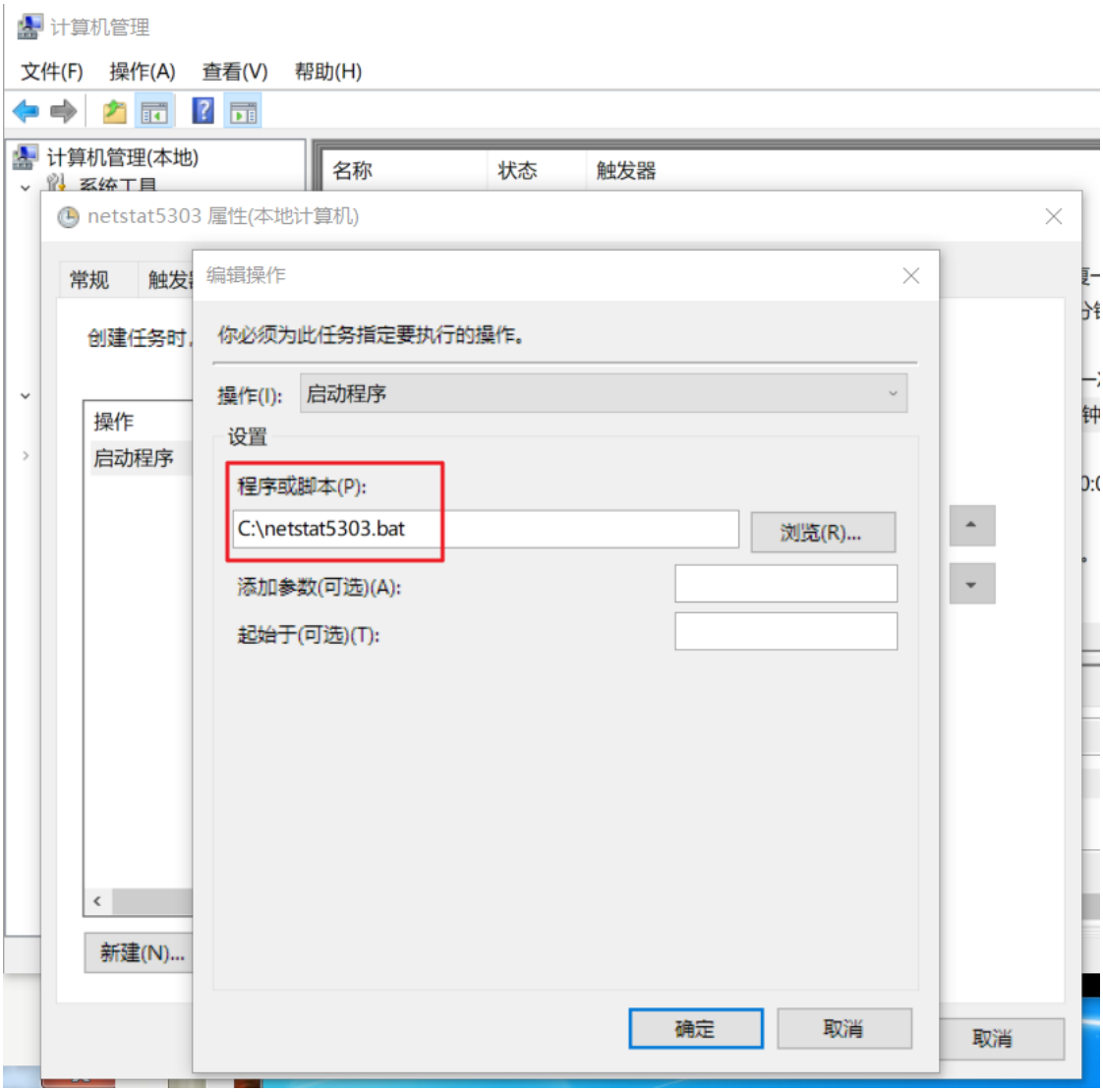

在其中写入以下内容：date /t >> c:\netstat5303.txt
time /t >> c:\netstat5303.txt
netstat -bn >> c:\netstat5303.txt如下图所示：

```
date /t >> c:\netstat5303.txt
time /t >> c:\netstat5303.txt
netstat -bn >> c:\netstat5303.txt
```

打开任务计划程序，可以看到我们新创建的这个任务：

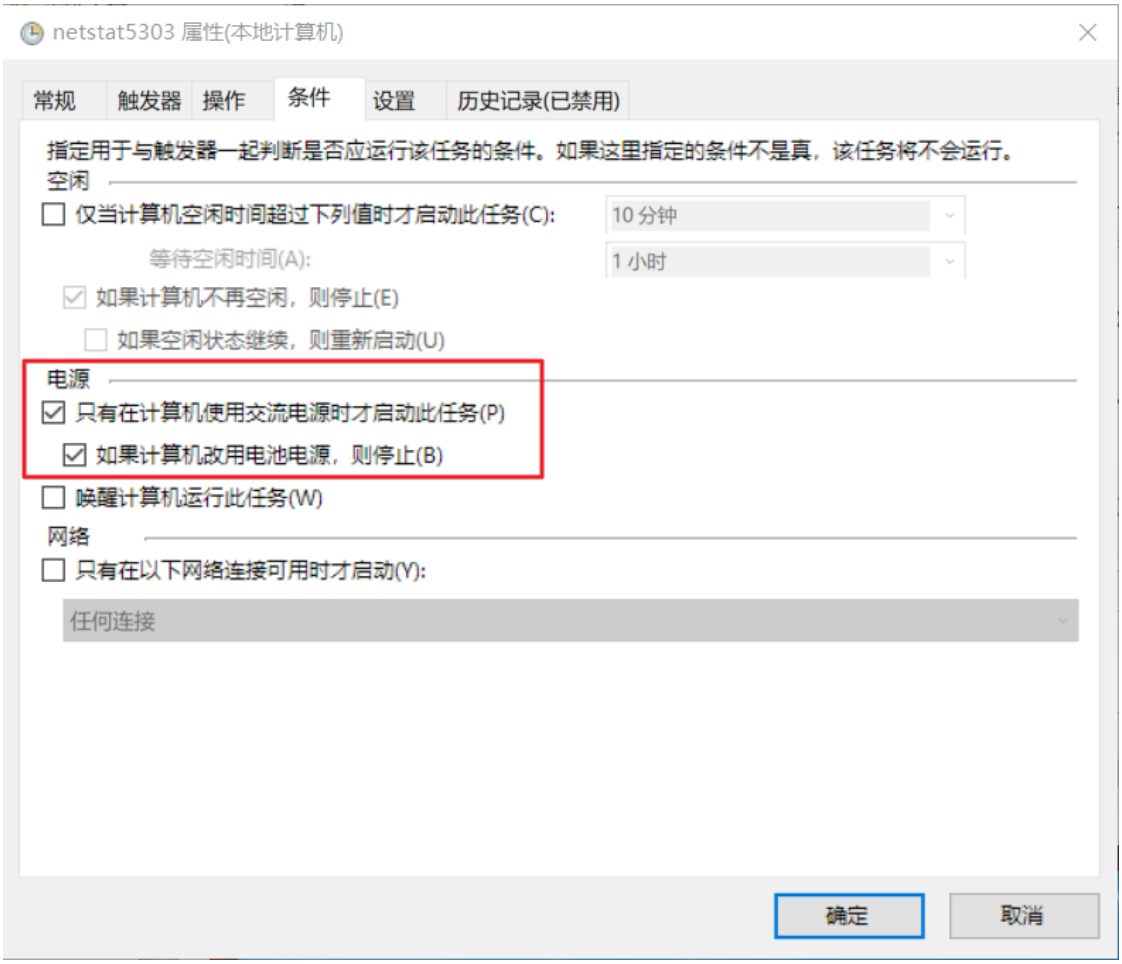



双击这个任务，点击操作并编辑，将“程序或脚本”改为我们创建的netstat5303.bat批处理文件，确定即可。

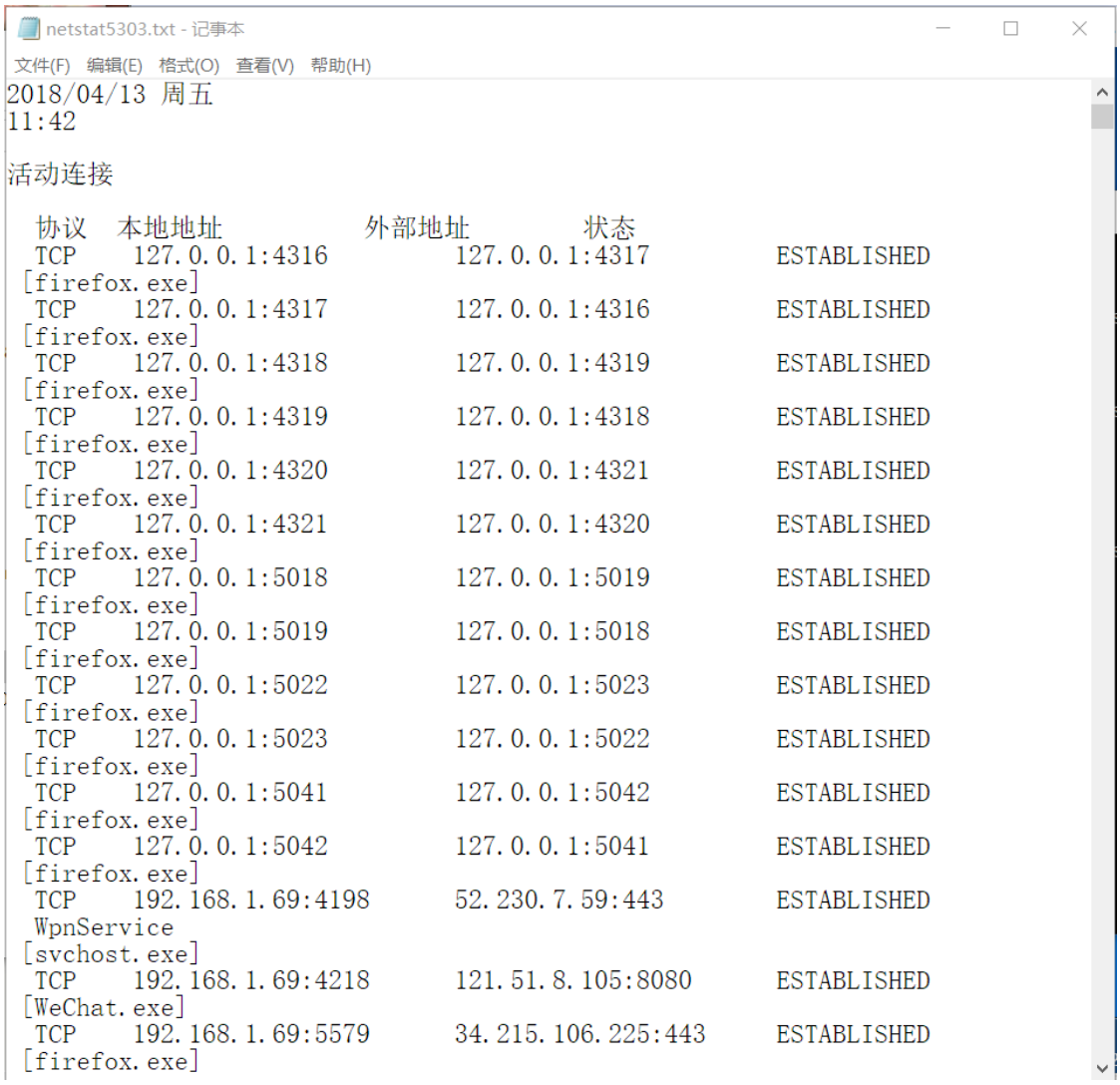



任务还有其他属性，点击“条件”选项卡，可以更改相关的设置。比如默认操作为“只有在计算机使用交流电源时才启动此任务”，那么使用电池电源时就会停止任务。这点需要

格外注意，如果没有修改默认操作，任务无论如何都无法执行可能只是因为拔掉了电源。



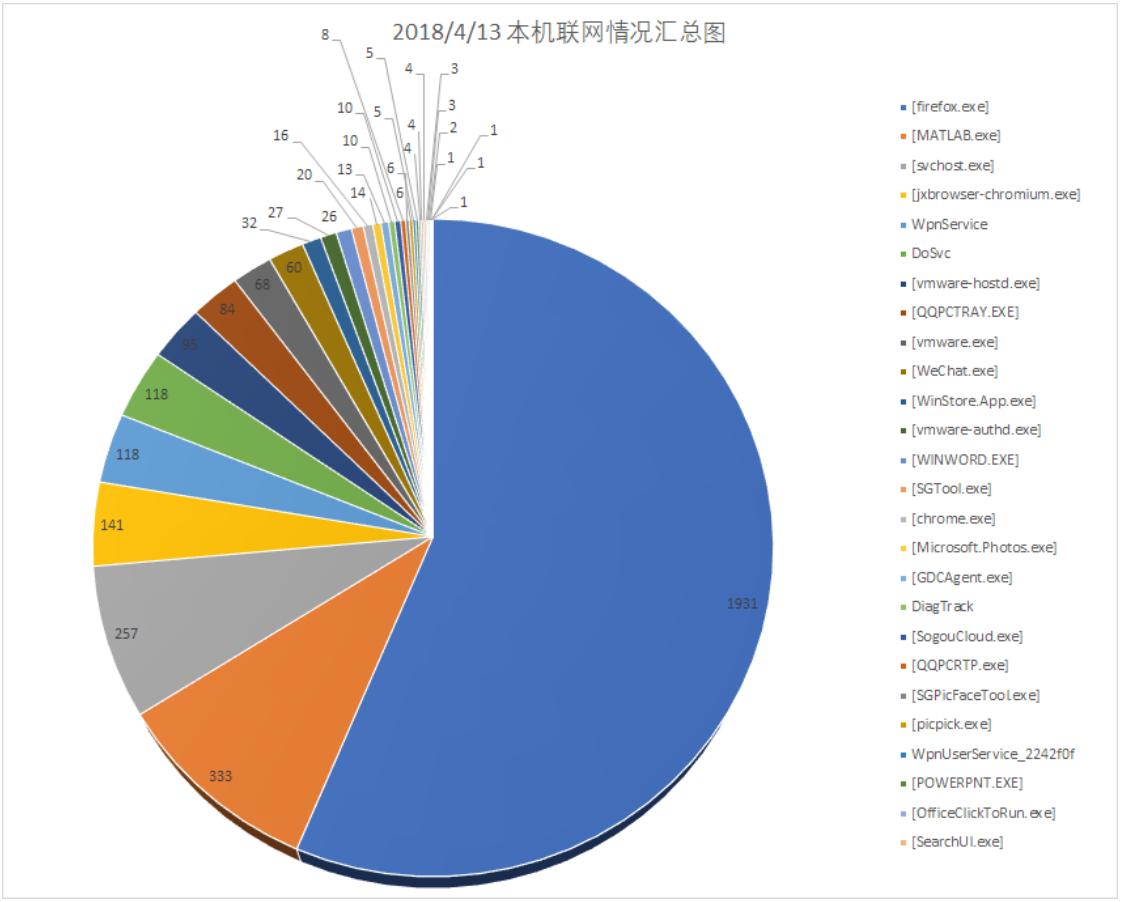

执行此脚本一定时间（如8小时），就可以在netstat5303.txt文件中查看到本机在该时间段内的联网记录：




当记录的数据足够丰富时，停止任务，将所得数据在excel中进行分析（详细操作参考学姐的博客：20144306《网络对抗》MAL_恶意代码分析）。

| | |
|---|---|
| [firefox.exe] | 1931 |
| [MATLAB.exe] | 333 |
| [svchost.exe] | 257 |
| [jxbrowser-chromium.exe | 141 |
| WpnService | 118 |
| DoSvc | 118 |
| [vmware-hostd.exe] | 95 |
| [QQPCTRAY.EXE] | 84 |
| [vmware.exe] | 68 |
| [WeChat.exe] | 60 |
| [WinStore.App.exe] | 32 |
| [vmware-authd.exe] | 27 |
| [WINWORD.EXE] | 26 |
| [SGTool.exe] | 20 |
| [chrome.exe] | 16 |
| [Microsoft.Photos.exe] | 14 |
| [GDCAgent.exe] | 13 |
| DiagTrack | 10 |
| [SogouCloud.exe] | 10 |
| [QQPCRTP.exe] | 8 |
| [SGPicFaceTool.exe] | 6 |
| [picpick.exe] | 6 |
| WpnUserService_2242f0f | 5 |
| [POWERPNT.EXE] | 5 |
| [OfficeClickToRun.exe] | 4 |
| [SearchUI.exe] | 4 |
| [SGDownload.exe] | 4 |
| DcmSvc | 3 |

将每个应用的联网情况做成饼状图，更加清晰直观：




除此之外，还可以将所有的外网地址合并汇总，便于统计分析：

| | A |
|---|---|
| 1 | |
| 2 | |
| 3 | 行标签 |
| 4 | 1.1.1.1:80 |
| 5 | 101.201.169.146:443 |
| 6 | 101.201.170.152:443 |
| 7 | 101.201.173.208:443 |
| 8 | 101.201.174.163:443 |
| 9 | 101.226.154.198:8443 |
| 10 | 101.226.154.30:8443 |
| 11 | 101.26.37.199:443 |
| 12 | 103.235.247.9:443 |
| 13 | 104.127.194.168:443 |
| 14 | 104.127.218.56:443 |
| 15 | 104.18.25.243:80 |
| 16 | 104.20.169.10:443 |
| 17 | 104.24.106.188:80 |
| 18 | 104.28.27.72:80 |
| 19 | 104.75.240.105:80 |
| 20 | 111.13.100.35:80 |
| 21 | 111.13.100.91:443 |
| 22 | 111.13.100.92:443 |
| 23 | 111.13.101.191:443 |
| 24 | 111.13.101.192:443 |
| 25 | 111.13.101.73:80 |
| 26 | 111.13.105.104:443 |
| 27 | 111.13.105.106:443 |
| 28 | 111.13.105.23:443 |
| 29 | 111.13.105.23:80 |
| 30 | 111.13.113.32:443 |

或者，详细显示每一个外网连接时，本机的IP及端口：

| | A |
|---|---|
| 3 | 行标签 |
| 4 | 1.1.1.1:80 |
| 5 | 172.16.8.28:6139 |
| 6 | 172.16.8.28:6164 |
| 7 | 172.16.8.28:6187 |
| 8 | 172.16.8.28:7449 |
| 9 | 172.16.8.28:7489 |
| 10 | 172.16.8.28:7585 |
| 11 | 172.16.8.28:7815 |
| 12 | 172.16.8.28:8081 |
| 13 | 172.16.8.28:8201 |
| 14 | 172.16.8.28:8250 |
| 15 | 172.16.8.28:8375 |
| 16 | 172.16.8.28:8628 |
| 17 | 172.16.8.28:8670 |
| 18 | 172.16.8.28:8743 |
| 19 | 172.30.4.253:12421 |
| 20 | 172.30.4.253:12482 |
| 21 | 172.30.4.253:12525 |
| 22 | 172.30.4.253:12597 |
| 23 | 172.30.4.253:12708 |
| 24 | 172.30.4.253:12735 |
| 25 | 192.168.1.69:5954 |
| 26 | 192.168.1.69:5978 |
| 27 | 192.168.1.69:6008 |
| 28 | 192.168.1.69:6034 |
| 29 | 101.201.169.146:443 |
| 30 | 172.16.8.28:6437 |
| 31 | 172.16.8.28:7860 |
| 32 | 192.168.43.100:10448 |

如有需要，查看这些可疑的外网IP即可。

转自
https://blog.51cto.com/antivirusjo/2054410