内网本机工作组信息收集

不管是在外网中还是在内网中,信息收集都是重要的第一步。对于内网中的一台机器,其所处内网的结构是什么样的、其角色是什么、使用这台机器的人的角色是什么,以及这台机器上安装了什么杀毒软件、这台机器是通过什么方式上网的、这台机器是笔记本电脑还是台式机等问题,都需要通过信息收集来解答。

网络配置信息

获取本机的网络配置信息

```
ipconfig
```

```
C:\>ipconfig

Windows IP 配置


以太网适配器 本地连接:

   连接特定的 DNS 后缀 . . . . . . . :
   本地链接 IPv6 地址. . . . . . . . : fe80::21f5:43d9:d94a:e0bf%11
   IPv4 地址 . . . . . . . . . . . . : 192.168.41.20
   子网掩码  . . . . . . . . . . . . : 255.255.255.0
   默认网关. . . . . . . . . . . . . : 192.168.41.10

隧道适配器 isatap.{B942738B-03AC-4053-9F29-E84AE5F5553E}:

   媒体状态  . . . . . . . . . . . . : 媒体已断开
   连接特定的 DNS 后缀 . . . . . . . :
```

操作系统和软件信息

查询操作系统和版本信息

```
systeminfo | findstr /B /C:"OS Name"/C:"OS Version"
systeminfo| findstr /B /C:"OS 名称" /C:"OS 版本"
```

```
C:\>systeminfo| findstr /B /C:"OS 名称" /C:"OS 版本"
OS 名称:          Microsoft Windows Server 2008 HPC Edition
OS 版本:          6.1.7601 Service Pack 1 Build 7601
```

查看系统体系结构

```
echo %PROCESSOR_ARCHITECTURE%
```

```
C:\>echo %PROCESSOR_ARCHITECTURE%
AMD64
```

查看安装的软件及版本

```
wmic product get name,version
powershell "Get-WmiObject -class win32_product | Select-Object -Property name,version"
```

本机服务信息

```
wmic service list brief
```

```
C:\>wmic service list brief
ExitCode  Name                            ProcessId  StartMode  State    Status
0         AeLookupSvc                     804        Manual     Running  OK
1077      ALG                             0          Manual     Stopped  OK
0         AppHostSvc                      1052       Auto       Running  OK
1077      AppIDSvc                        0          Manual     Stopped  OK
0         Appinfo                         804        Manual     Running  OK
1077      AppMgmt                         0          Manual     Stopped  OK
1077      aspnet_state                    0          Manual     Stopped  OK
1077      AudioEndpointBuilder            0          Manual     Stopped  OK
1077      AudioSrv                        0          Manual     Stopped  OK
0         BFE                             328        Auto       Running  OK
0         BITS                            804        Auto       Running  OK
1077      Browser                         0          Disabled   Stopped  OK
0         CertPropSvc                     804        Manual     Running  OK
1077      clr_optimization_v2.0.50727_32  0          Manual     Stopped  OK
1077      clr_optimization_v2.0.50727_64  0          Manual     Stopped  OK
0         COMSysApp                       1852       Manual     Running  OK
```

进程信息

```
tasklist
wmic process list brief
```

```
C:\>wmic process list brief
HandleCount  Name                       Priority  ProcessId  ThreadCount  WorkingSetSize
0            System Idle Process        0         0          1            24576
563          System                     8         4          87           376832
32           smss.exe                   11        224        2            1077248
547          csrss.exe                  13        320        9            6086656
78           wininit.exe                13        372        3            4812800
255          services.exe               9         476        6            10944512
746          lsass.exe                  9         484        7            13651968
241          lsm.exe                    8         492        10           6250496
357          svchost.exe                8         588        10           9805824
280          svchost.exe                8         652        7            8560640
317          svchost.exe                8         708        13           12984320
1094         svchost.exe                8         804        40           39714816
632          svchost.exe                8         860        16           15036416
239          svchost.exe                8         928        9            10657792
426          svchost.exe                8         976        16           18014208
295          svchost.exe                8         328        16           10838016
268          spoolsv.exe                8         464        13           11051008
97           svchost.exe                8         1052       9            9261056
66           Everything.exe             8         1076       4            4165632
46           svchost.exe                8         1136       3            2711552
130          svchost.exe                8         1296       16           10309632
255          svchost.exe                8         1532       11           7168000
```

启动程序信息

```
wmic startup get command,caption
```

```
C:\>wmic startup get command,caption
Caption                     Command
VMware VM3DService Process  "C:\Windows\system32\vm3dservice.exe" -u
VMware User Process         "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr
```

计划任务信息

如果出现无法加载列资源 输入：chcp 437

```
schtasks /query /fo LIST /v
```

```
C:\>schtasks /query /fo LIST /v

Folder: \
INFO: There are no scheduled tasks presently available at your access level.

Folder: \Microsoft
INFO: There are no scheduled tasks presently available at your access level.

Folder: \Microsoft\Windows
INFO: There are no scheduled tasks presently available at your access level.

Folder: \Microsoft\Windows\Active Directory Rights Management Services Client
HostName:                             PC-2008
TaskName:                             \Microsoft\Windows\Active Directory Rights Management Services
 Client\AD RMS Rights Policy Template Management (Automated)
Next Run Time:                        Disabled
Status:
Logon Mode:                           Interactive/Background
Last Run Time:                        N/A
Last Result:                          1
Author:                               Microsoft Corporation
Task To Run:                          COM handler
Start In:                             N/A
Comment:                              ????? AD RMS ???????????????? Web ????????.????????????????
```

主机开机时间信息

```
net statistics workstation
```

```
C:\>net statistics workstation
\\PC-2008 的工作站统计数据

统计数据开始于 2022/3/30 17:31:21

  接收的字节数                3882
  接收的服务器消息块 (SMB)    20
  传输的字节数                0
  传输的服务器消息块 (SMB)    0
  读取操作                    9
  写入操作                    0
  拒绝原始读取                0
  拒绝原始写入                0
```

用户列表信息

```
net user
wmic useraccount get name ,SID
```

```
C:\>wmic useraccount get name ,SID
Name           SID
Administrator  S-1-5-21-3432382454-1205603526-922924321-500
Guest          S-1-5-21-3432382454-1205603526-922924321-501
Administrator  S-1-5-21-2716900768-72748719-3475352185-500
Guest          S-1-5-21-2716900768-72748719-3475352185-501
krbtgt         S-1-5-21-2716900768-72748719-3475352185-502
bob            S-1-5-21-2716900768-72748719-3475352185-1105
```

列出会话

```
net session
```

```
C:\Windows\system32>net session
列表是空的。
```

查询端口列表

```
netstat -ano
```

```
C:\>netstat -ano

活动连接

  协议  本地地址          外部地址        状态           PID
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       652
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:1688           0.0.0.0:0              LISTENING       2276
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       1532
  TCP    0.0.0.0:47001          0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING       372
```

查看补丁列表

```
systeminfo
wmic qfe get Caption,Description,HotFixID,InstalledOn
```

```
C:\>wmic qfe get Caption,Description,HotFixID,InstalledOn
Caption                                     Description  HotFixID   InstalledOn
http://support.microsoft.com/?kbid=2999226  Update       KB2999226  3/25/2021
http://support.microsoft.com/?kbid=976902   Update       KB976902   11/21/2010
```

查询共享列表

```
net share
wmic share get name,path,status
```

```
C:\>wmic share get name,path,status
Name    Path        Status
ADMIN$  C:\Windows  OK
C$      C:\         OK
IPC$                OK
```

路由信息

```
route print
```

```
C:\>route print
===========================================================================
接口列表
 11...00 0c 29 d4 e2 a4 ......Intel(R) PRO/1000 MT Network Connection
  1...........................Software Loopback Interface 1
 13...00 00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
===========================================================================

IPv4 路由表
===========================================================================
活动路由:
网络目标        网络掩码          网关       接口   跃点数
          0.0.0.0          0.0.0.0    192.168.41.10    192.168.41.20    266
        127.0.0.0        255.0.0.0            在链路上         127.0.0.1    306
        127.0.0.1  255.255.255.255            在链路上         127.0.0.1    306
  127.255.255.255  255.255.255.255            在链路上         127.0.0.1    306
     192.168.41.0    255.255.255.0            在链路上     192.168.41.20    266
    192.168.41.20  255.255.255.255            在链路上     192.168.41.20    266
   192.168.41.255  255.255.255.255            在链路上     192.168.41.20    266
        224.0.0.0        240.0.0.0            在链路上         127.0.0.1    306
        224.0.0.0        240.0.0.0            在链路上     192.168.41.20    266
  255.255.255.255  255.255.255.255            在链路上         127.0.0.1    306
  255.255.255.255  255.255.255.255            在链路上     192.168.41.20    266
===========================================================================
```

防火墙相关操作

1、查看防火墙是否开启

```
netsh firewall show state
```

```
C:\>netsh firewall show state

防火墙状态:
-------------------------------------------------------------------
配置文件                           = 域
操作模式                           = 禁用
例外模式                           = 启用
多播/广播响应模式                  = 启用
通知模式                           = 禁用
组策略版本                         = Windows 防火墙
远程管理模式                       = 禁用

所有网络接口上的端口当前均为打开状态:
端口    协议  版本  程序
-------------------------------------------------------------------
3389    TCP       任何       (null)
```

2、关闭防火墙强

```
Windows server 2003:     netsh firewall set opmode disable
Windows server 2003之后:  netsh firewall set opmode disable 或者netsh advfirewall set
allprofiles state off
```

```
C:\>netsh firewall set opmode disable

重要信息: 已成功执行命令。
但不赞成使用 "netsh firewall";
而应该使用 "netsh advfirewall firewall"。
有关使用 "netsh advfirewall firewall" 命令
而非 "netsh firewall" 的详细信息，请参阅
http://go.microsoft.com/fwlink/?linkid=121488
上的 KB 文章 947709。

确定。
```

3、查看防火墙配置

```
netsh firewall show config
```

```
C:\>netsh firewall show config

域 配置文件配置(当前):
-------------------------------------------------------------------
操作模式                              = 启用
例外模式                              = 启用
多播/广播响应模式                     = 启用
通知模式                              = 禁用

域 配置文件的服务配置文件:
模式     自定义      名称
-------------------------------------------------------------------
启用       否          远程桌面

域 配置文件的允许的程序配置:
模式     流量方向            名称/程序
-------------------------------------------------------------------
```

4、修改防火墙配置

2003及之前的版本,允许指定的程序进行全部的连接:

```
netsh firewall add allowedprogram c:\nc.exe "allownc" enable
```

2003之后的版本，允许指定的程序进行全部的连接

```
netsh advfirewall firewall add rule name="pass nc"dir=in action=allow program="C:\nc.exe"
```

允许指定程序退出,命令如下

```
netsh advfirewall firewall add rule name="Allownc" dir=out action=allow program="C:
\nc.exe"
```

允许3389端口放行,命令如下

```
netsh advfirewall firewall add rule name="RemoteDesktop" protocol=TCP dir=in
localport=3389 action=allow
```

```
netsh advfirewall firewall add rule name=test dir=in action=allow protocol=tcp
localport=4444#允许4444端口进站
netsh advfirewall firewall add rule name=test dir=in action=allow program=c:\a.exe  #允许
a.exe进站
netsh advfirewall firewall add rule name=test dir=out action=allow protocol=tcp
localport=4444#允许4444端口出站  netsh advfirewall firewall add rule name=test dir=out
action=allow program=c:\a.exe#允许a.exe出站
```

开启远程服务

1、在2003机器上

```
wmic path win32_terminalservicesetting where (_CLASS !="") call setallowtsconnections 1
```

2、在server2008和server 2021

```
REG ADD HKLM\SYSTEM\CurrentControlSet\Control\Terminal" "Server /v fDenyTSConnections /t
REG_DWORD /d 00000000 /f  #开启
REG ADD "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t
REG_DWORD /d 11111111 /f  #关闭
```

WIFI密码收集

```
for /f  "skip=9 tokens=1,2 delims=:" %i in ('netsh wlan show profiles')  do  @echo %j |
findstr -i -v echo |  netsh wlan show profiles %j key=clear
```

```
--------------------
    版本                   : 1
    类型                   : 无线局域网
    名称                   : [redacted]
    控制选项               :
        连接模式           : 手动连接
        网络广播           : 只在网络广播时连接
        AutoSwitch         : 请勿切换到其他网络
        MAC 随机化: 禁用

连接设置
---------------------
    SSID 数目              : 1
    SSID 名称              :“涓€鎶婂悓濂园宛鎵€”
    网络类型               : 结构
    无线电类型             : [ 任何无线电类型 ]
    供应商扩展名           : 不存在

安全设置
-----------------
    身份验证         : WPA2 - 个人
    密码                   : CCMP
    身份验证         : WPA2 - 个人
    密码                   : GCMP
    安全密钥               : 存在
    关键内容               : 123456789
```

查询RDP端口

```
reg query "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal
Server\Winstations\RDP-Tcp" /V PortNumber
```

0xd3d即为3389端口

```
C:\>reg query "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Winstations\RDP-T
cp" /V PortNumber

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Winstations\RDP-Tcp
    PortNumber    REG_DWORD    0xd3d
```

查看代理配置信息

```
reg query "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings"
```

```
C:\>reg query "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings"

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
    IE5_UA_Backup_Flag    REG_SZ    5.0
    User Agent    REG_SZ    Mozilla/4.0 (compatible; MSIE 8.0; Win32)
    EmailName    REG_SZ    User@
    PrivDiscUiShown    REG_DWORD    0x1
    EnableHttp1_1    REG_DWORD    0x1
    WarnOnIntranet    REG_DWORD    0x1
    MimeExclusionListForCache    REG_SZ    multipart/mixed multipart/x-mixed-replace multipart/x-byt
eranges
    AutoConfigProxy    REG_SZ    wininet.dll
    UseSchannelDirectly    REG_BINARY    01000000

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Http Filters
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\P3P
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Passport
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones
```

查看当前保存的登陆凭证

```
cmdkey /l
```

Arp信息

```
arp -a
```

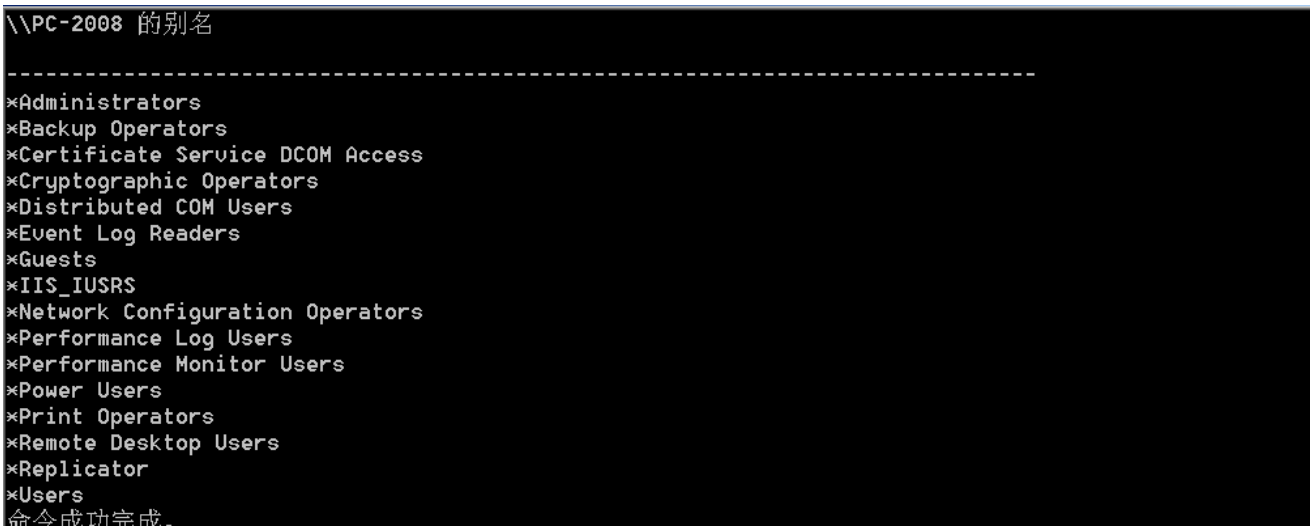
```
C:\>arp -a

接口: 192.168.41.20 --- 0xb
  Internet 地址         物理地址              类型
  192.168.41.10         00-0c-29-58-d6-e0     动态
  192.168.41.255        ff-ff-ff-ff-ff-ff     静态
  224.0.0.22            01-00-5e-00-00-16     静态
  224.0.0.252           01-00-5e-00-00-fc     静态
```

查看最近打开的文档

```
dir %APPDATA%\Microsoft\Windows\Recent
```

查询本机用户组

```
net localgroup
```

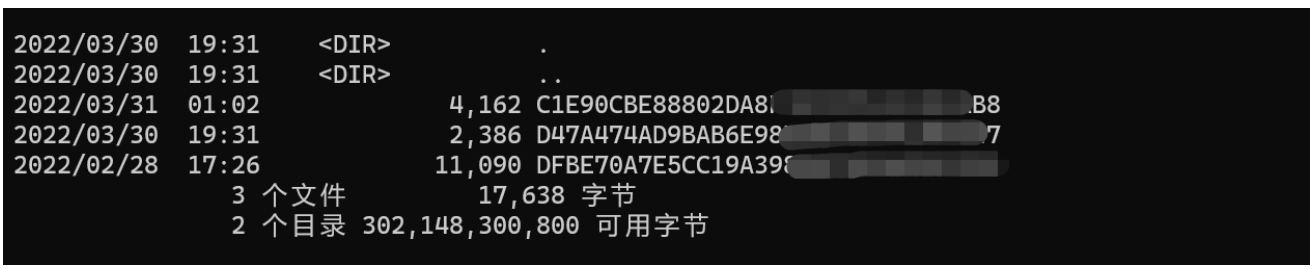


管理员组成员列表

```
net localgroup administrators
```

RDP凭证

```
dir /a %userprofile%\AppData\Local\Microsoft\Credentials\*
```



浏览器密码获取

杀毒软件查询

```
wmic /node:localhost /namespace:\\root\securitycenter2 path antivirusproduct get
displayname /format:list
```

常见杀软程序

```
avList = {
    "360tray.exe": "360安全卫士-实时保护",
    "360safe.exe": "360安全卫士-主程序",
    "ZhuDongFangYu.exe": "360安全卫士-主动防御",
    "360sd.exe": "360杀毒",
    "a2guard.exe": "a-squared杀毒",
    "ad-watch.exe": "Lavasoft杀毒",
    "cleaner8.exe": "The Cleaner杀毒",
    "vba32lder.exe": "vb32杀毒",
    "MongoosaGUI.exe": "Mongoosa杀毒",
    "CorantiControlCenter32.exe": "Coranti2012杀毒",
    "F-PROT.exe": "F-Prot AntiVirus",
    "CMCTrayIcon.exe": "CMC杀毒",
    "K7TSecurity.exe": "K7杀毒",
    "UnThreat.exe": "UnThreat杀毒",
    "CKSoftShiedAntivirus4.exe": "Shield Antivirus杀毒",
    "AVWatchService.exe": "VIRUSfighter杀毒",
    "ArcaTasksService.exe": "ArcaVir杀毒",
    "iptray.exe": "Immunet杀毒",
    "PSafeSysTray.exe": "PSafe杀毒",
    "nspupsvc.exe": "nProtect杀毒",
    "SpywareTerminatorShield.exe": "SpywareTerminator反间谍软件",
    "BKavService.exe": "Bkav杀毒",
    "MsMpEng.exe": "Microsoft Security Essentials",
    "SBAMSvc.exe": "VIPRE",
    "ccSvcHst.exe": "Norton杀毒",
    "f-secure.exe": "冰岛",
    "avp.exe": "Kaspersky",
    "KvMonXP.exe": "江民杀毒",
    "RavMonD.exe": "瑞星杀毒",
    "Mcshield.exe": "McAfee",
    "Tbmon.exe": "McAfee",
    "Frameworkservice.exe": "McAfee",
    "egui.exe": "ESET NOD32",
    "ekrn.exe": "ESET NOD32",
    "eguiProxy.exe": "ESET NOD32",
    "kxetray.exe": "金山毒霸",
    "knsdtray.exe": "可牛杀毒",
    "TMBMSRV.exe": "趋势杀毒",
    "avcenter.exe": "Avira(小红伞)",
    "avguard.exe": "Avira(小红伞)",
    "avgnt.exe": "Avira(小红伞)",
    "sched.exe": "Avira(小红伞)",
    "ashDisp.exe": "Avast网络安全",
    "rtvscan.exe": "诺顿杀毒",
```

```
"ccapp.exe": "SymantecNorton",
"NPFMntor.exe": "Norton杀毒软件",
"ccSetMgr.exe": "赛门铁克",
"ccRegVfy.exe": "Norton杀毒软件",
"ksafe.exe": "金山卫士",
"QQPCRTP.exe": "QQ电脑管家",
"avgwdsvc.exe": "AVG杀毒",
"QUHLPSVC.exe": "QUICK HEAL杀毒",
"mssecess.exe": "微软杀毒",
"SavProgress.exe": "Sophos杀毒",
"SophosUI.exe": "Sophos杀毒",
"SophosFS.exe": "Sophos杀毒",
"SophosHealth.exe": "Sophos杀毒",
"SophosSafestore64.exe": "Sophos杀毒",
"SophosCleanM.exe": "Sophos杀毒",
"fsavgui.exe": "F-Secure杀毒",
"vsserv.exe": "比特梵德",
"remupd.exe": "熊猫卫士",
"FortiTray.exe": "飞塔",
"safedog.exe": "安全狗",
"parmor.exe": "木马克星",
"Iparmor.exe.exe": "木马克星",
"beikesan.exe": "贝壳云安全",
"KSWebShield.exe": "金山网盾",
"TrojanHunter.exe": "木马猎手",
"GG.exe": "巨盾网游安全盾",
"adam.exe": "绿鹰安全精灵",
"AST.exe": "超级巡警",
"ananwidget.exe": "墨者安全专家",
"AVK.exe": "AntiVirusKit",
"avg.exe": "AVG Anti-Virus",
"spidernt.exe": "Dr.web",
"avgaurd.exe": "Avira Antivir",
"vsmon.exe": "Zone Alarm",
"cpf.exe": "Comodo",
"outpost.exe": "Outpost Firewall",
"rfwmain.exe": "瑞星防火墙",
"kpfwtray.exe": "金山网镖",
"FYFireWall.exe": "风云防火墙",
"MPMon.exe": "微点主动防御",
"pfw.exe": "天网防火墙",
"BaiduSdSvc.exe": "百度杀毒-服务进程",
"BaiduSdTray.exe": "百度杀毒-托盘进程",
"BaiduSd.exe": "百度杀毒-主程序",
"SafeDogGuardCenter.exe": "安全狗",
"safedogupdatecenter.exe": "安全狗",
"safedogguardcenter.exe": "安全狗",
"SafeDogSiteIIS.exe": "安全狗",
"SafeDogTray.exe": "安全狗",
"SafeDogServerUI.exe": "安全狗",
"D_Safe_Manage.exe": "D盾",
"d_manage.exe": "D盾",
"yunsuo_agent_service.exe": "云锁",
```

```
"yunsuo_agent_daemon.exe": "云锁",
"HwsPanel.exe": "护卫神",
"hws_ui.exe": "护卫神",
"hws.exe": "护卫神",
"hwsd.exe": "护卫神",
"hipstray.exe": "火绒",
"wsctrl.exe": "火绒",
"usysdiag.exe": "火绒",
"SPHINX.exe": "SPHINX防火墙",
"bddownloader.exe": "百度卫士",
"baiduansvx.exe": "百度卫士-主进程",
"AvastUI.exe": "Avast!5主程序",
"emet_agent.exe": "EMET",
"emet_service.exe": "EMET",
"firesvc.exe": "McAfee",
"firetray.exe": "McAfee",
"hipsvc.exe": "McAfee",
"mfevtps.exe": "McAfee",
"mcafeefire.exe": "McAfee",
"scan32.exe": "McAfee",
"shstat.exe": "McAfee",
"vstskmgr.exe": "McAfee",
"engineserver.exe": "McAfee",
"mfeann.exe": "McAfee",
"mcscript.exe": "McAfee",
"updaterui.exe": "McAfee",
"udaterui.exe": "McAfee",
"naprdmgr.exe": "McAfee",
"cleanup.exe": "McAfee",
"cmdagent.exe": "McAfee",
"frminst.exe": "McAfee",
"mcscript_inuse.exe": "McAfee",
"mctray.exe": "McAfee",
"_avp32.exe": "卡巴斯基",
"_avpcc.exe": "卡巴斯基",
"_avpm.exe": "卡巴斯基",
"aAvgApi.exe": "AVG",
"ackwin32.exe": "已知杀软进程,名称暂未收录",
"alertsvc.exe": "Norton AntiVirus",
"alogserv.exe": "McAfee VirusScan",
"anti-trojan.exe": "Anti-Trojan Elite",
"arr.exe": "Application Request Route",
"atguard.exe": "AntiVir",
"atupdater.exe": "已知杀软进程,名称暂未收录",
"atwatch.exe": "Mustek",
"au.exe": "NSIS",
"aupdate.exe": "Symantec",
"auto-protect.nav80try.exe": "已知杀软进程,名称暂未收录",
"autodown.exe": "AntiVirus AutoUpdater",
"avconsol.exe": "McAfee",
"avgcc32.exe": "AVG",
"avgctrl.exe": "AVG",
"avgemc.exe": "AVG",
```

```
"avgrsx.exe": "AVG",
"avgserv.exe": "AVG",
"avgserv9.exe": "AVG",
"avgw.exe": "AVG",
"avkpop.exe": "G DATA SOFTWARE AG",
"avkserv.exe": "G DATA SOFTWARE AG",
"avkservice.exe": "G DATA SOFTWARE AG",
"avkwctl9.exe": "G DATA SOFTWARE AG",
"avltmain.exe": "Panda Software Aplication",
"avnt.exe": "H+BEDV Datentechnik GmbH",
"avp32.exe": "Kaspersky Anti-Virus",
"avpcc.exe": " Kaspersky AntiVirus",
"avpdos32.exe": " Kaspersky AntiVirus",
"avpm.exe": " Kaspersky AntiVirus",
"avptc32.exe": " Kaspersky AntiVirus",
"avpupd.exe": " Kaspersky AntiVirus",
"avsynmgr.exe": "McAfee",
"avwin.exe": " H+BEDV",
"bargains.exe": "Exact Advertising SpyWare",
"beagle.exe": "Avast",
"blackd.exe": "BlackICE",
"blackice.exe": "BlackICE",
"blink.exe": "micromedia",
"blss.exe": "CBlaster",
"bootwarn.exe": "Symantec",
"bpc.exe": "Grokster",
"brasil.exe": "Exact Advertising",
"ccevtmgr.exe": "Norton Internet Security",
"cdp.exe": "CyberLink Corp.",
"cfd.exe": "Motive Communications",
"cfgwiz.exe": " Norton AntiVirus",
"claw95.exe": "已知杀软进程,名称暂未收录",
"claw95cf.exe": "已知杀软进程,名称暂未收录",
"clean.exe": "windows流氓软件清理大师",
"cleaner.exe": "windows流氓软件清理大师",
"cleaner3.exe": "windows流氓软件清理大师",
"cleanpc.exe": "windows流氓软件清理大师",
"cpd.exe": "McAfee",
"ctrl.exe": "已知杀软进程,名称暂未收录",
"cv.exe": "已知杀软进程,名称暂未收录",
"defalert.exe": "Symantec",
"defscangui.exe": "Symantec",
"defwatch.exe": "Norton Antivirus",
"doors.exe": "已知杀软进程,名称暂未收录",
"dpf.exe": "已知杀软进程,名称暂未收录",
"dpps2.exe": "PanicWare",
"dssagent.exe": "Broderbund",
"ecengine.exe": "已知杀软进程,名称暂未收录",
"emsw.exe": "Alset Inc",
"ent.exe": "已知杀软进程,名称暂未收录",
"espwatch.exe": "已知杀软进程,名称暂未收录",
"ethereal.exe": "RationalClearCase",
"exe.avxw.exe": "已知杀软进程,名称暂未收录",
```

```
"expert.exe": "已知杀软进程,名称暂未收录",
"f-prot95.exe": "已知杀软进程,名称暂未收录",
"fameh32.exe": "F-Secure",
"fast.exe": " FastUsr",
"fch32.exe": "F-Secure",
"fih32.exe": "F-Secure",
"findviru.exe": "F-Secure",
"firewall.exe": "AshampooSoftware",
"fnrb32.exe": "F-Secure",
"fp-win.exe": " F-Prot Antivirus OnDemand",
"fsaa.exe": "F-Secure",
"fsav.exe": "F-Secure",
"fsav32.exe": "F-Secure",
"fsav530stbyb.exe": "F-Secure",
"fsav530wtbyb.exe": "F-Secure",
"fsav95.exe": "F-Secure",
"fsgk32.exe": "F-Secure",
"fsm32.exe": "F-Secure",
"fsma32.exe": "F-Secure",
"fsmb32.exe": "F-Secure",
"gbmenu.exe": "已知杀软进程,名称暂未收录",
"guard.exe": "ewido",
"guarddog.exe": "ewido",
"htlog.exe": "已知杀软进程,名称暂未收录",
"htpatch.exe": "Silicon Integrated Systems Corporation",
"hwpe.exe": "已知杀软进程,名称暂未收录",
"iamapp.exe": "Symantec",
"iamserv.exe": "Symantec",
"iamstats.exe": "Symantec",
"iedriver.exe": " Urlblaze.com",
"iface.exe": "Panda Antivirus Module",
"infus.exe": "Infus Dialer",
"infwin.exe": "Msviewparasite",
"intdel.exe": "Inet Delivery",
"intren.exe": "已知杀软进程,名称暂未收录",
"jammer.exe": "已知杀软进程,名称暂未收录",
"kavpf.exe": "Kapersky",
"kazza.exe": "Kapersky",
"keenvalue.exe": "EUNIVERSE INC",
"launcher.exe": "Intercort Systems",
"ldpro.exe": "已知杀软进程,名称暂未收录",
"ldscan.exe": "Windows Trojans Inspector",
"localnet.exe": "已知杀软进程,名称暂未收录",
"luall.exe": "Symantec",
"luau.exe": "Symantec",
"lucomserver.exe": "Norton",
"mcagent.exe": "McAfee",
"mcmnhdlr.exe": "McAfee",
"mctool.exe": "McAfee",
"mcupdate.exe": "McAfee",
"mcvsrte.exe": "McAfee",
"mcvsshld.exe": "McAfee",
"mfin32.exe": "MyFreeInternetUpdate",
```

```
"mfw2en.exe": "MyFreeInternetUpdate",
"mfweng3.02d30.exe": "MyFreeInternetUpdate",
"mgavrtcl.exe": "McAfee",
"mgavrte.exe": "McAfee",
"mghtml.exe": "McAfee",
"mgui.exe": "BullGuard",
"minilog.exe": "Zone Labs Inc",
"mmod.exe": "EzulaInc",
"mostat.exe": "WurldMediaInc",
"mpfagent.exe": "McAfee",
"mpfservice.exe": "McAfee",
"mpftray.exe": "McAfee",
"mscache.exe": "Integrated Search Technologies Spyware",
"mscman.exe": "OdysseusMarketingInc",
"msmgt.exe": "Total Velocity Spyware",
"msvxd.exe": "W32/Datom-A",
"mwatch.exe": "已知杀软进程,名称暂未收录",
"nav.exe": "Reuters Limited",
"navapsvc.exe": "Norton AntiVirus",
"navapw32.exe": "Norton AntiVirus",
"navw32.exe": "Norton Antivirus",
"ndd32.exe": "诺顿磁盘医生",
"neowatchlog.exe": "已知杀软进程,名称暂未收录",
"netutils.exe": "已知杀软进程,名称暂未收录",
"nisserv.exe": "Norton",
"nisum.exe": "Norton",
"nmain.exe": "Norton",
"nod32.exe": "ESET Smart Security",
"norton_internet_secu_3.0_407.exe": "已知杀软进程,名称暂未收录",
"notstart.exe": "已知杀软进程,名称暂未收录",
"nprotect.exe": "Symantec",
"npscheck.exe": "Norton",
"npssvc.exe": "Norton",
"ntrtscan.exe": "趋势反病毒应用程序",
"nui.exe": "已知杀软进程,名称暂未收录",
"otfix.exe": "已知杀软进程,名称暂未收录",
"outpostinstall.exe": "Outpost",
"patch.exe": "趋势科技",
"pavw.exe": "已知杀软进程,名称暂未收录",
"pcscan.exe": "趋势科技",
"pdsetup.exe": "已知杀软进程,名称暂未收录",
"persfw.exe": "Tiny Personal Firewall",
"pgmonitr.exe": "PromulGate SpyWare",
"pingscan.exe": "已知杀软进程,名称暂未收录",
"platin.exe": "已知杀软进程,名称暂未收录",
"pop3trap.exe": "PC-cillin",
"poproxy.exe": "NortonAntiVirus",
"popscan.exe": "已知杀软进程,名称暂未收录",
"powerscan.exe": "Integrated Search Technologies",
"ppinupdt.exe": "已知杀软进程,名称暂未收录",
"pptbc.exe": "已知杀软进程,名称暂未收录",
"ppvstop.exe": "已知杀软进程,名称暂未收录",
"prizesurfer.exe": "Prizesurfer",
```

```
"prmt.exe": "OpiStat",
"prmvr.exe": "Adtomi",
"processmonitor.exe": "Sysinternals",
"proport.exe": "已知杀软进程,名称暂未收录",
"protectx.exe": "ProtectX",
"pspf.exe": "已知杀软进程,名称暂未收录",
"purge.exe": "已知杀软进程,名称暂未收录",
"qconsole.exe": "Norton AntiVirus Quarantine Console",
"qserver.exe": "Norton Internet Security",
"rapapp.exe": "BlackICE",
"rb32.exe": "RapidBlaster",
"rcsync.exe": "PrizeSurfer",
"realmon.exe": "Realmon ",
"rescue.exe": "已知杀软进程,名称暂未收录",
"rescue32.exe": "卡巴斯基互联网安全套装",
"rshell.exe": "已知杀软进程,名称暂未收录",
"rtvscn95.exe": "Real-time virus scanner ",
"rulaunch.exe": "McAfee User Interface",
"run32dll.exe": "PAL PC Spy",
"safeweb.exe": "PSafe Tecnologia",
"sbserv.exe": "Norton Antivirus",
"scrscan.exe": "360杀毒",
"sfc.exe": "System file checker",
"sh.exe": "MKS Toolkit for Win3",
"showbehind.exe": "MicroSmarts Enterprise Component ",
"soap.exe": "System Soap Pro",
"sofi.exe": "已知杀软进程,名称暂未收录",
"sperm.exe": "已知杀软进程,名称暂未收录",
"supporter5.exe": "eScorcher反病毒",
"symproxysvc.exe": "Symantec",
"symtray.exe": "Symantec",
"tbscan.exe": "ThunderBYTE",
"tc.exe": "TimeCalende",
"titanin.exe": "TitanHide",
"tvmd.exe": "Total Velocity",
"tvtmd.exe": " Total Velocity",
"vettray.exe": "eTrust",
"vir-help.exe": "已知杀软进程,名称暂未收录",
"vnpc3000.exe": "已知杀软进程,名称暂未收录",
"vpc32.exe": "Symantec",
"vpc42.exe": "Symantec",
"vshwin32.exe": "McAfee",
"vsmain.exe": "McAfee",
"vsstat.exe": "McAfee",
"wfindv32.exe": "已知杀软进程,名称暂未收录",
"zapro.exe": "Zone Alarm",
"zonealarm.exe": "Zone Alarm",
"AVPM.exe": "Kaspersky",
"A2CMD.exe": "Emsisoft Anti-Malware",
"A2SERVICE.exe": "a-squared free",
"A2FREE.exe": "a-squared Free",
"ADVCHK.exe": "Norton AntiVirus",
"AGB.exe": "安天防线",
```

```
"AHPROCMONSERVER.exe": "安天防线",
"AIRDEFENSE.exe": "AirDefense",
"ALERTSVC.exe": "Norton AntiVirus",
"AVIRA.exe": "小红伞杀毒",
"AMON.exe": "Tiny Personal Firewall",
"AVZ.exe": "AVZ",
"ANTIVIR.exe": "已知杀软进程,名称暂未收录",
"APVXDWIN.exe": "熊猫卫士",
"ASHMAISV.exe": "Alwil",
"ASHSERV.exe": "Avast Anti-virus",
"ASHSIMPL.exe": "AVAST!VirusCleaner",
"ASHWEBSV.exe": "Avast",
"ASWUPDSV.exe": "Avast",
"ASWSCAN.exe": "Avast",
"AVCIMAN.exe": "熊猫卫士",
"AVCONSOL.exe": "McAfee",
"AVENGINE.exe": "熊猫卫士",
"AVESVC.exe": "Avira AntiVir Security Service",
"AVEVL32.exe": "已知杀软进程,名称暂未收录",
"AVGAM.exe": "AVG",
"AVGCC.exe": "AVG",
"AVGCHSVX.exe": "AVG",
"AVGCSRVX": "AVG",
"AVGNSX.exe": "AVG",
"AVGCC32.exe": "AVG",
"AVGCTRL.exe": "AVG",
"AVGEMC.exe": "AVG",
"AVGFWSRV.exe": "AVG",
"AVGNTMGR.exe": "AVG",
"AVGSERV.exe": "AVG",
"AVGTRAY.exe": "AVG",
"AVGUPSVC.exe": "AVG",
"AVINITNT.exe": "Command AntiVirus for NT Server",
"AVPCC.exe": "Kaspersky",
"AVSERVER.exe": "Kerio MailServer",
"AVSCHED32.exe": "H+BEDV",
"AVSYNMGR.exe": "McAfee",
"AVWUPSRV.exe": "H+BEDV",
"BDSWITCH.exe": "BitDefender Module",
"BLACKD.exe": "BlackICE",
"CCEVTMGR.exe": "Symantec",
"CFP.exe": "COMODO",
"CLAMWIN.exe": "ClamWin Portable",
"CUREIT.exe": "DrWeb CureIT",
"DEFWATCH.exe": "Norton Antivirus",
"DRWADINS.exe": "Dr.Web",
"DRWEB.exe": "Dr.Web",
"DEFENDERDAEMON.exe": "ShadowDefender",
"EWIDOCTRL.exe": "Ewido Security Suite",
"EZANTIVIRUSREGISTRATIONCHECK.exe": "e-Trust Antivirus",
"FIREWALL.exe": "AshampooSoftware",
"FPROTTRAY.exe": "F-PROT Antivirus",
"FPWIN.exe": "Verizon",
```

```
"FRESHCLAM.exe": "ClamAV",
"FSAV32.exe": "F-Secure",
"FSBWSYS.exe": "F-secure",
"FSDFWD.exe": "F-Secure",
"FSGK32.exe": "F-Secure",
"FSGK32ST.exe": "F-Secure",
"FSMA32.exe": "F-Secure",
"FSMB32.exe": "F-Secure",
"FSSM32.exe": "F-Secure",
"GUARDGUI.exe": "网游保镖",
"GUARDNT.exe": "IKARUS",
"IAMAPP.exe": "Symantec",
"INOCIT.exe": "eTrust",
"INORPC.exe": "eTrust",
"INORT.exe": "eTrust",
"INOTASK.exe": "eTrust",
"INOUPTNG.exe": "eTrust",
"ISAFE.exe": "eTrust",
"KAV.exe": "Kaspersky",
"KAVMM.exe": "Kaspersky",
"KAVPF.exe": "Kaspersky",
"KAVPFW.exe": "Kaspersky",
"KAVSTART.exe": "Kaspersky",
"KAVSVC.exe": "Kaspersky",
"KAVSVCUI.exe": "Kaspersky",
"KMAILMON.exe": "金山毒霸",
"MCAGENT.exe": "McAfee",
"MCMNHDLR.exe": "McAfee",
"MCREGWIZ.exe": "McAfee",
"MCUPDATE.exe": "McAfee",
"MCVSSHLD.exe": "McAfee",
"MINILOG.exe": "Zone Alarm",
"MYAGTSVC.exe": "McAfee",
"MYAGTTRY.exe": "McAfee",
"NAVAPSVC.exe": "Norton",
"NAVAPW32.exe": "Norton",
"NAVLU32.exe": "Norton",
"NAVW32.exe": "Norton Antivirus",
"NEOWATCHLOG.exe": "NeoWatch",
"NEOWATCHTRAY.exe": "NeoWatch",
"NISSERV.exe": "Norton",
"NISUM.exe": "Norton",
"NMAIN.exe": "Norton",
"NOD32.exe": "ESET NOD32",
"NPFMSG.exe": "Norman个人防火墙",
"NPROTECT.exe": "Symantec",
"NSMDTR.exe": "Norton",
"NTRTSCAN.exe": "趋势科技",
"OFCPFWSVC.exe": "OfficeScanNT",
"ONLINENT.exe": "已知杀软进程,名称暂未收录",
"OP_MON.exe": " OutpostFirewall",
"PAVFIRES.exe": "熊猫卫士",
"PAVFNSVR.exe": "熊猫卫士",
```

```
"PAVKRE.exe": "熊猫卫士",
"PAVPROT.exe": "熊猫卫士",
"PAVPROXY.exe": "熊猫卫士",
"PAVPRSRV.exe": "熊猫卫士",
"PAVSRV51.exe": "熊猫卫士",
"PAVSS.exe": "熊猫卫士",
"PCCGUIDE.exe": "PC-cillin",
"PCCIOMON.exe": "PC-cillin",
"PCCNTMON.exe": "PC-cillin",
"PCCPFW.exe": "趋势科技",
"PCCTLCOM.exe": "趋势科技",
"PCTAV.exe": "PC Tools AntiVirus",
"PERSFW.exe": "Tiny Personal Firewall",
"PERVAC.exe": "已知杀软进程,名称暂未收录",
"PESTPATROL.exe": "Ikarus",
"PREVSRV.exe": "熊猫卫士",
"RTVSCN95.exe": "Real-time Virus Scanner",
"SAVADMINSERVICE.exe": "SAV",
"SAVMAIN.exe": "SAV",
"SAVSCAN.exe": "SAV",
"SDHELP.exe": "Spyware Doctor",
"SHSTAT.exe": "McAfee",
"SPBBCSVC.exe": "Symantec",
"SPIDERCPL.exe": "Dr.Web",
"SPIDERML.exe": "Dr.Web",
"SPIDERUI.exe": "Dr.Web",
"SPYBOTSD.exe": "Spybot ",
"SWAGENT.exe": "SonicWALL",
"SWDOCTOR.exe": "SonicWALL",
"SWNETSUP.exe": "Sophos",
"SYMLCSVC.exe": "Symantec",
"SYMPROXYSVC.exe": "Symantec",
"SYMSPORT.exe": "Sysmantec",
"SYMWSC.exe": "Sysmantec",
"SYNMGR.exe": "Sysmantec",
"TMLISTEN.exe": "趋势科技",
"TMNTSRV.exe": "趋势科技",
"TMPROXY.exe": "趋势科技",
"TNBUTIL.exe": "Anti-Virus",
"VBA32ECM.exe": "已知杀软进程,名称暂未收录",
"VBA32IFS.exe": "已知杀软进程,名称暂未收录",
"VBA32PP3.exe": "已知杀软进程,名称暂未收录",
"VCRMON.exe": "VirusChaser",
"VRMONNT.exe": "HAURI",
"VRMONSVC.exe": "HAURI",
"VSHWIN32.exe": "McAfee",
"VSSTAT.exe": "McAfee",
"XCOMMSVR.exe": "BitDefender",
"ZONEALARM.exe": "Zone Alarm",
"360rp.exe": "360杀毒",
"afwServ.exe": " Avast Antivirus ",
"safeboxTray.exe": "360杀毒",
"360safebox.exe": "360杀毒",
```

```
    "QQPCTray.exe": "QQ电脑管家",
    "KSafeTray.exe": "金山毒霸",
    "KSafeSvc.exe": "金山毒霸",
    "KWatch.exe": "金山毒霸",
    "gov_defence_service.exe": "云锁",
    "gov_defence_daemon.exe": "云锁",
    "smartscreen.exe": "Windows Defender"
};
```