微软极品工具箱-Sysinternals Suite

工具包由来

Sysinternals Suite是微软发布的一套非常强大的免费工具程序集，一共包括74个windows工具。
Sysinternals是Winternals公司提供的免费工具，Winternals公司原本主力研发系统复原与资料保护，为了解决工程师平常在工作上遇到的各种问题，便开发出许多小工具，之后他们将这些工具集合起来称为Sysinternals。
前段时间很火的3Q大战中用来查看腾讯是否扫描用户硬盘的 **Process Monitor** 就是其中的优秀代表。

工具包简介

本文把这套工具包里的实用软件都整理出来，按照名称首字母排序。

点击每个蓝色标题链接都可以转到微软的对应官方页面，有对这些工具包的直接下载地址和更详尽的用法。
因为每个软件几乎都可以长篇大论的介绍，所以，在此就只做简介和罗列，希望能够对大家有所帮助。
每个软件都可以单独下载，当然更建议直接下载他们的集成版——Sysinternals Suite 系统工具套装

下载地址

微软官网下载： https://technet.microsoft.com/en-us/sysinternals/bb842062
procexp中文版： http://www.xdowns.com/soft/6/56/2006/Soft_32122.html

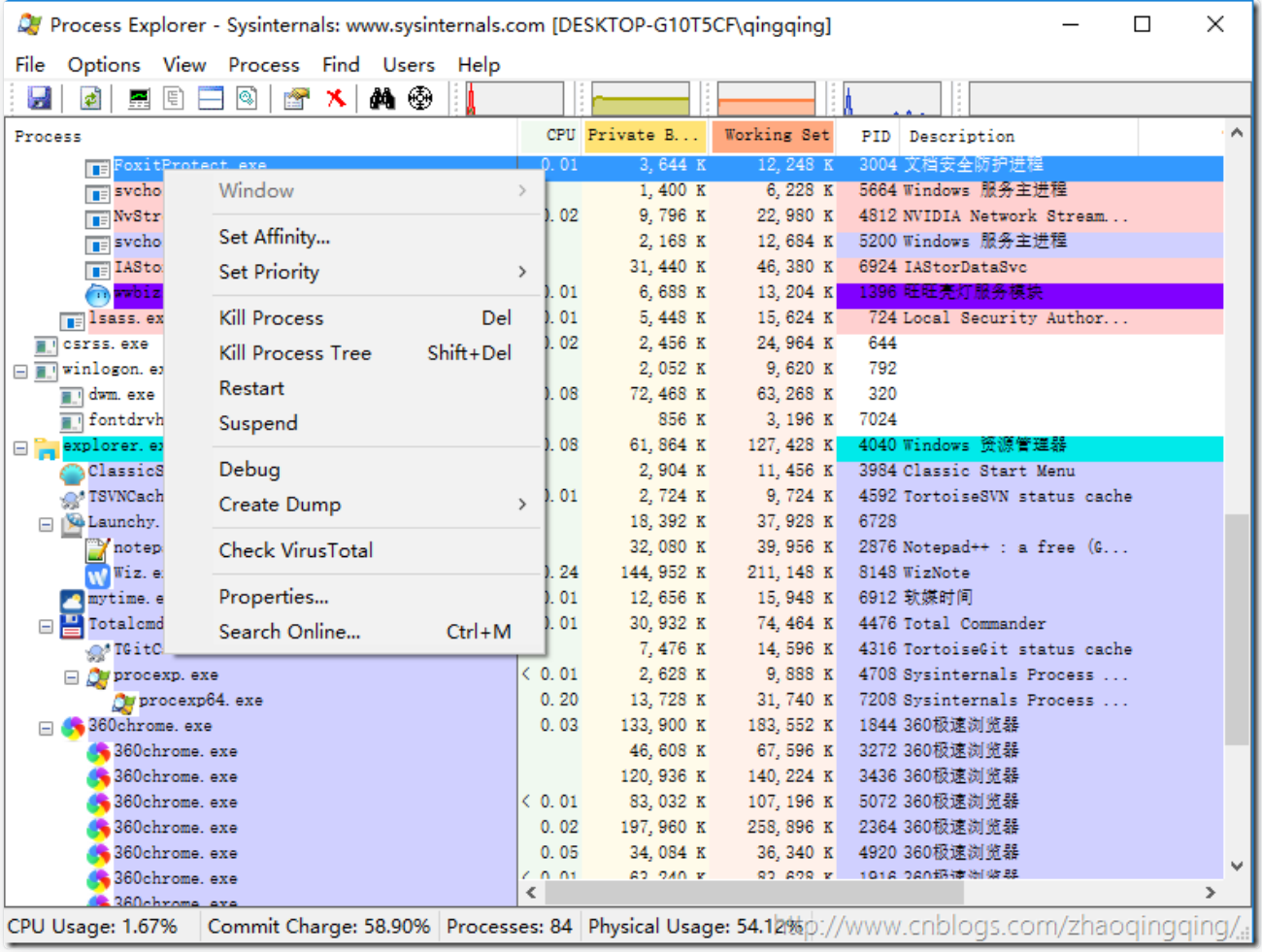
Top 10 Downloads

1. Process Explorer

Process Explorer
进程浏览器，查看进程的详细信息包括CPU，GPU，IO，线程，句柄，内存

中文资料：

iT熊's BloG： Process Explorer使用教程



2. AutoRuns

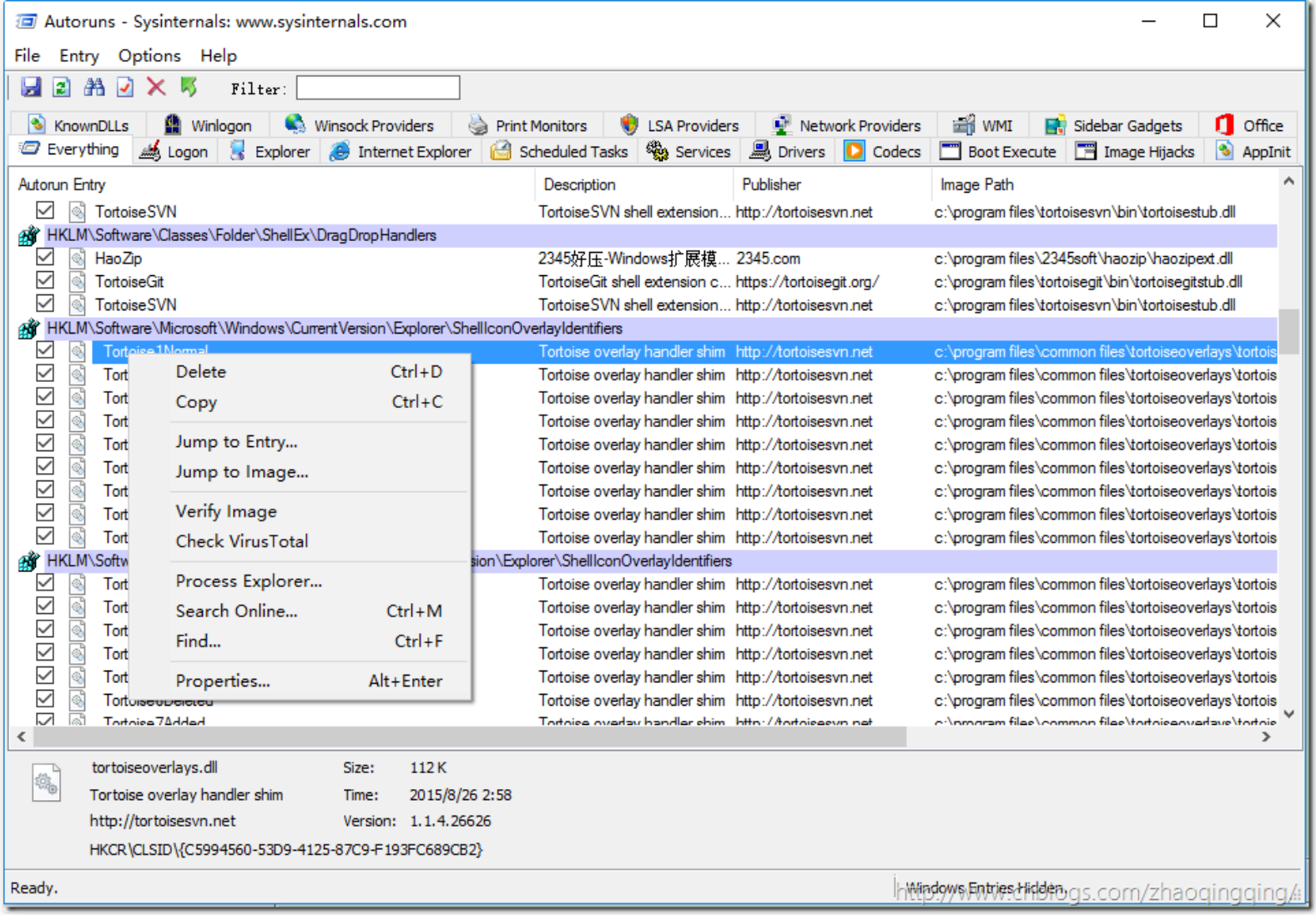
AutoRuns

windows启动程序管理

autoruns拥有最全面的知识，显示系统启动或登录时会自动启动的项目和配置，包括扩展和加载各种Windows进程，其中包括Explorer和Internet Explorer。

它报告可执行文件时间戳的图像，其他文件类型的last - modified时间戳，最后修改时间戳的自动运行的位置。签署"隐藏微软条目"选项帮助你放大第三方自动起动图片已经添加到您的系统。

运行在Windows XP和更高版本，其中包括64位Windows。



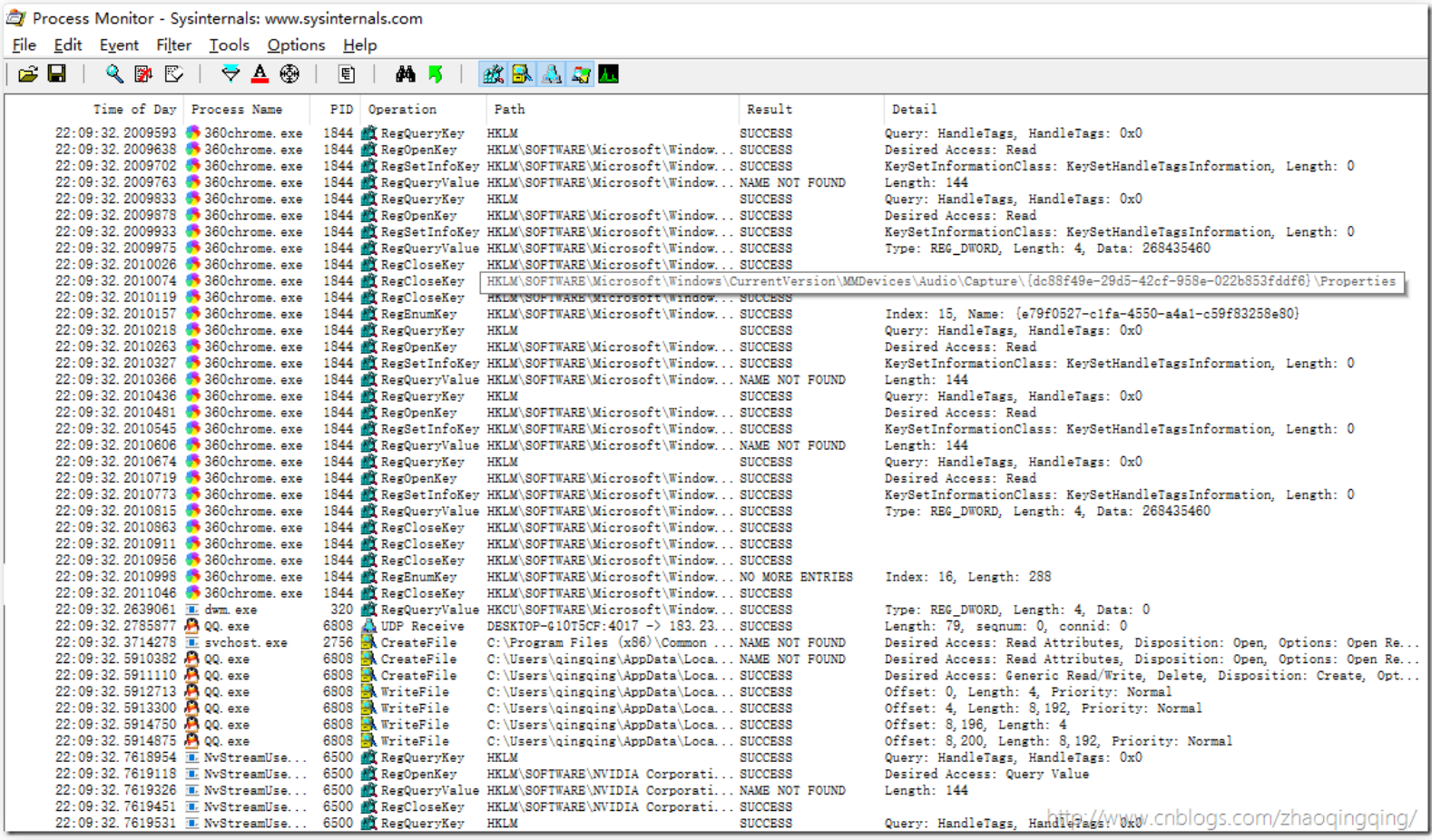
3. Process Monitor

Process Monitor

打开方法：执行 Procmon.exe

一个高级的windows监视器，实时显示文件系统，注册表，网络活动，进程或线程活动，资料收集事件。

Process Monitor是 Filemon + Regmon的整合增强版本



4. PsTools

PsTools

PsTools套件的工具包括:

PsExec——执行远程过程

PsFile——远程显示打开的文件

PsGetSid——显示计算机的SID或一个用户

PsInfo——系统信息列表

PsKill——杀死进程的名字或进程ID

PsList——列表详细信息流程

PsLoggedOn——看谁的本地登录,通过资源共享

PsLogList -倾倒事件日志记录

PsPasswd——更改帐户密码

psp -测试网络性能

PsService——视图和控制服务

PsShutdown——关闭,选择重新启动计算机

PsSuspend——挂起和恢复过程

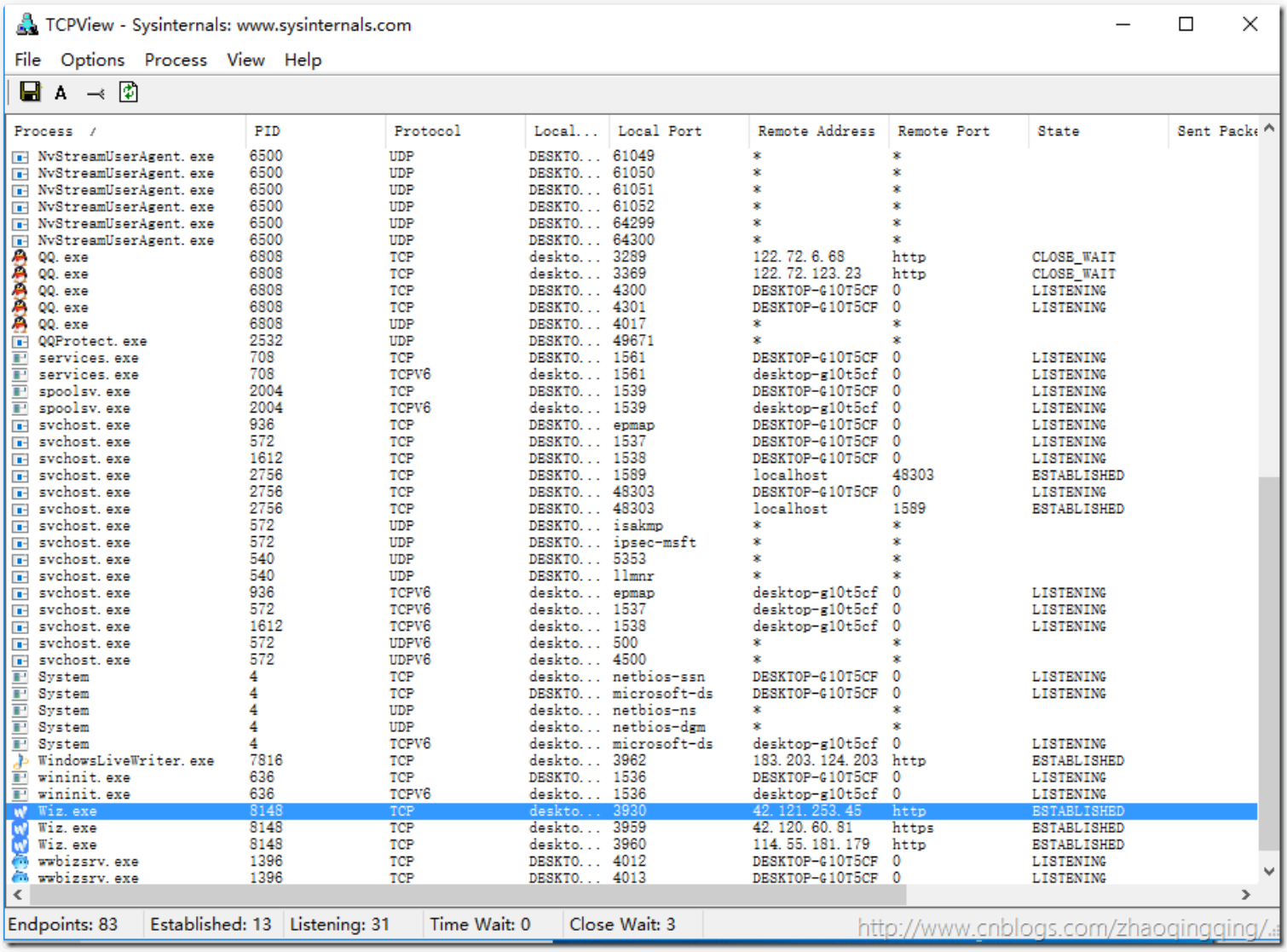
5. TcpView

TcpView

TCPView是一个Windows程序，将告诉你系统上所有TCP和UDP端点的详细清单，包括进程名、远程地址和TCP连接的状态。

TCPView提供了一个方便的查看当前使用网络的子集，适用于Windows NT / 2000 / XP。

TCPView运行在Windows XP或更高系统版本

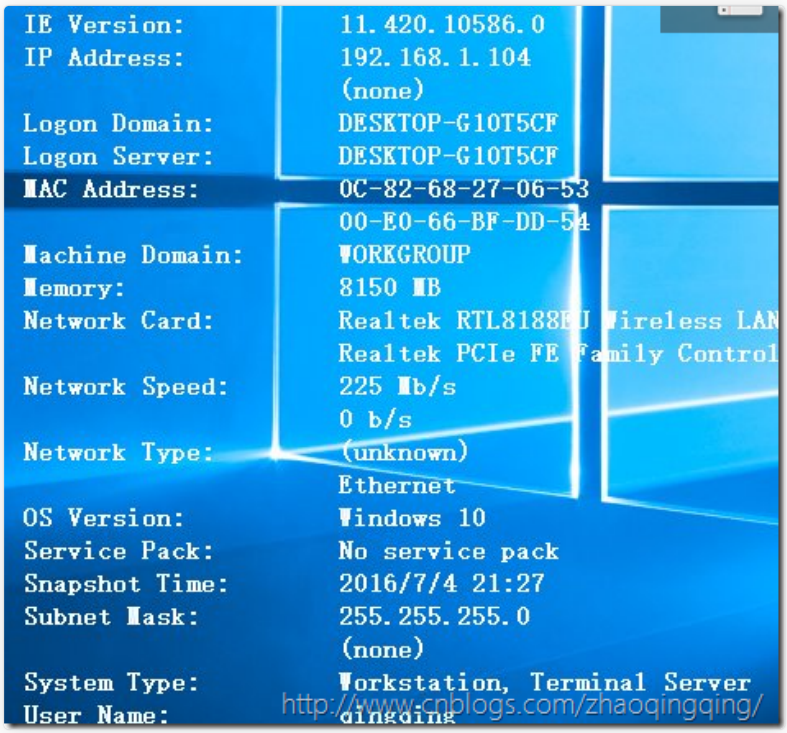


Process	PID	Protocol	Local...	Local Port	Remote Address	Remote Port	State	Sent Packe
NvStreamUserAgent.exe	6500	UDP	DESKTO...	61049	*	*		
NvStreamUserAgent.exe	6500	UDP	DESKTO...	61050	*	*		
NvStreamUserAgent.exe	6500	UDP	DESKTO...	61051	*	*		
NvStreamUserAgent.exe	6500	UDP	DESKTO...	61052	*	*		
NvStreamUserAgent.exe	6500	UDP	DESKTO...	64299	*	*		
NvStreamUserAgent.exe	6500	UDP	DESKTO...	64300	*	*		
QQ.exe	6808	TCP	deskto...	3289	122.72.6.68	http	CLOSE_WAIT	
QQ.exe	6808	TCP	deskto...	3369	122.72.123.23	http	CLOSE_WAIT	
QQ.exe	6808	TCP	DESKTO...	4300	DESKTOP-G10T5CF	0	LISTENING	
QQ.exe	6808	TCP	DESKTO...	4301	DESKTOP-G10T5CF	0	LISTENING	
QQ.exe	6808	UDP	DESKTO...	4017	*	*		
QQProtect.exe	2532	UDP	DESKTO...	49671	*	*		
services.exe	708	TCP	DESKTO...	1561	DESKTOP-G10T5CF	0	LISTENING	
services.exe	708	TCPV6	deskto...	1561	desktop-g10t5cf	0	LISTENING	
spoolsv.exe	2004	TCP	DESKTO...	1539	DESKTOP-G10T5CF	0	LISTENING	
spoolsv.exe	2004	TCPV6	deskto...	1539	desktop-g10t5cf	0	LISTENING	
svchost.exe	936	TCP	DESKTO...	epmap	DESKTOP-G10T5CF	0	LISTENING	
svchost.exe	572	TCP	DESKTO...	1537	DESKTOP-G10T5CF	0	LISTENING	
svchost.exe	1612	TCP	DESKTO...	1538	DESKTOP-G10T5CF	0	LISTENING	
svchost.exe	2756	TCP	DESKTO...	1589	localhost	48303	ESTABLISHED	
svchost.exe	2756	TCP	DESKTO...	48303	DESKTOP-G10T5CF	0	LISTENING	
svchost.exe	2756	TCP	DESKTO...	48303	localhost	1589	ESTABLISHED	
svchost.exe	572	UDP	DESKTO...	isakmp	*	*		
svchost.exe	572	UDP	DESKTO...	ipsec-msft	*	*		
svchost.exe	540	UDP	DESKTO...	5353	*	*		
svchost.exe	540	UDP	DESKTO...	llmnr	*	*		
svchost.exe	936	TCPV6	deskto...	epmap	desktop-g10t5cf	0	LISTENING	
svchost.exe	572	TCPV6	deskto...	1537	desktop-g10t5cf	0	LISTENING	
svchost.exe	1612	TCPV6	deskto...	1538	desktop-g10t5cf	0	LISTENING	
svchost.exe	572	UDPV6	deskto...	500	*	*		
svchost.exe	572	UDPV6	deskto...	4500	*	*		
System	4	TCP	deskto...	netbios-ssn	DESKTOP-G10T5CF	0	LISTENING	
System	4	TCP	DESKTO...	microsoft-ds	DESKTOP-G10T5CF	0	LISTENING	
System	4	UDP	deskto...	netbios-ns	*	*		
System	4	UDP	deskto...	netbios-dgm	*	*		
System	4	TCPV6	deskto...	microsoft-ds	desktop-g10t5cf	0	LISTENING	
WindowsLiveWriter.exe	7816	TCP	deskto...	3962	183.203.124.203	http	ESTABLISHED	
wininit.exe	636	TCP	DESKTO...	1536	DESKTOP-G10T5CF	0	LISTENING	
wininit.exe	636	TCPV6	deskto...	1536	desktop-g10t5cf	0	LISTENING	
Wiz.exe	8148	TCP	deskto...	3930	42.121.253.45	http	ESTABLISHED	
Wiz.exe	8148	TCP	deskto...	3959	42.120.60.81	https	ESTABLISHED	
Wiz.exe	8148	TCP	deskto...	3960	114.55.181.179	http	ESTABLISHED	
wwbizsrv.exe	1396	TCP	DESKTO...	4012	DESKTOP-G10T5CF	0	LISTENING	
wwbizsrv.exe	1396	TCP	DESKTO...	4013	DESKTOP-G10T5CF	0	LISTENING	

6. BgInfo

BgInfo

把系统信息显示在桌面背景图上



7. BlueScreen

BlueScreen

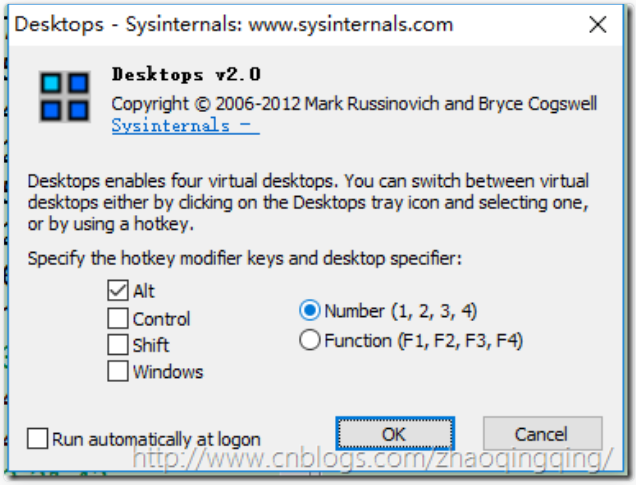
8. Desktops

Desktops

虚拟桌面

默认快捷键：按Alt+1,2,3,4切换不同虚拟桌面；

优点：小巧快速



各工具简介和微软官方网页

AccessChk

为了确保创建安全的环境，Windows 管理员通常需要了解特定用户或用户组对文件、目录、注册表项和 Windows 服务等资源具有哪种访问权限。AccessChk 能够通过直观的界面和输出快速回答这些问题。

AccessEnum

这一简单但强大的安全工具可以向您显示，谁可以用何种访问权限访问您系统中的目录、文件和注册表项。使用此工具可查找权限漏洞。

AdExplorer

Active Directory Explorer 是一个高级的 Active Directory (AD) 查看器和编辑器。

AdInsight

一种 LDAP（轻型目录访问协议）实时监视工具，旨在对 Active Directory 客户端应用程序进行故障排除。

AdRestore

恢复已删除的 Server 2003 Active Directory 对象。

Autologon

登录过程中跳过密码屏幕。

Autoruns

查看哪些程序被配置为在系统启动和您登录时自动启动。Autoruns 还能够完整列出应用程序可以配置自动启动设置的注册表和文件位置。

BgInfo

此完全可配置程序会自动生成桌面背景，其中包含有关系统的 IP 地址、计算机名称、网络适配器及更多内容的重要信息。

BlueScreen

此屏幕保护程序不仅精确模拟"蓝屏"，而且也模拟重新启动（完成 CHKDSK），并可在 Windows NT 4、Windows 2000、Windows XP、Server 2003 和 Windows 9x 上工作。

CacheSet

CacheSet 是一个允许您利用 NT 提供的功能来控制缓存管理器的工作集大小的程序。它与 NT 的所有版本都兼容。

ClockRes

查看系统时钟的分辨率，亦即计时器最大分辨率。

Contig

您是否希望迅速对您频繁使用的文件进行碎片整理？使用 Contig 优化单个的文件，或者创建连续的新文件。

Coreinfo

Coreinfo 是一个新的命令行实用工具，可向您显示逻辑处理器与物理处理器之间的映射、NUMA 节点和它们所处的插槽，以及分配给每个逻辑处理器的缓存。

Ctrl2cap

这是一个内核模式的驱动程序，可在键盘类驱动程序上演示键盘输入过滤，以便将 Caps-Lock 转变为控制键。在此级别过滤允许在 NT 刚好要"看到"键之前变换和隐藏键。Ctrl2cap 还显示如何使用 NtDisplayString() 打印初始化蓝屏的消息。

DebugView

Sysinternals 的另一个优先程序：此程序截取设备驱动程序对 DbgPrint 的调用和 Win32 程序生成的 OutputDebugString。它允许在不使用活动的调试器的情况下，在本地计算机上或通过 Internet 查看和记录调试会话输出。

Desktops

使用这一新的实用工具可以创建最多四个虚拟桌面，使用任务栏界面或热键预览每个桌面上的内容并在这些桌面之间轻松地进行切换。

Disk2vhd

Disk2vhd 可简化从物理系统到虚拟机 (p2v) 的迁移。

DiskExt

显示卷磁盘映射。

Diskmon

此实用工具会捕捉所有硬盘活动，或者在您的系统任务栏中象软件磁盘活动灯一样工作。

DiskView

图形磁盘扇区实用工具。

Disk Usage (DU)

按目录查看磁盘使用情况。

EFSDump

查看加密文件的信息。

Handle

此易用命令行实用工具将显示哪些进程打开了哪些文件，以及更多其他信息。

Hex2dec

将十六进制数字转换为十进制及反向转换。

接合点

创建 Win2K NTFS 符号链接。

LDMDump

转储逻辑磁盘管理器在磁盘上的数据库内容，其中说明了 Windows 2000 动态磁盘的分区情况。

ListDLLs

列出所有当前加载的 DLL，包括加载位置及其版本号。2.0 版将打印已加载模块的完整路径名。

LiveKd

使用 Microsoft 内核调试程序检查真实系统。

LoadOrder

查看设备加载到 WinNT/2K 系统中的顺序。

LogonSessions

列出系统中的活动登录会话。

MoveFile

使您可以安排在系统下一次重新启动时执行移动和删除命令。

NTFSInfo

用 NTFSInfo 可以查看有关 NTFS 卷的详细信息，包括主文件表 (MFT) 和 MFT 区的大小和位置，以及 NTFS 元数据文件的大小。

PageDefrag

对您的分页文件和注册表配置单元进行碎片整理。

PendMoves

枚举在系统下一次启动时所要执行的文件重命名和删除命令的列表。

PipeList

显示系统上的命名管道，包括每个管道的最大实例数和活动实例数。

PortMon

通过高级监视工具监视串行端口和并行端口的活动。它能识别所有的标准串行和并行 IOCTL，甚至可以显示部分正在发送和接收的数据。3.x 版具有强大的新 UI 增强功能和高级筛选功能。

ProcDump

这一新的命令行实用工具旨在捕获其他方式难以隔离和重现 CPU 峰值的进程转储。该工具还可用作用于创建进程转储的一般实用工具，并可以在进程具有挂起的窗口或未处理的异常时监视和生成进程转储。

Process Explorer

找出进程打开了哪些文件、注册表项和其他对象以及已加载哪些 DLL 等信息。这个功能异常强大的实用工具甚至可以显示每个进程的所有者。

Process Monitor

实时监视文件系统、注册表、进程、线程和 DLL 活动。

ProcFeatures

这一小程序会报告处理器和 Windows 对“物理地址扩展”和“无执行”缓冲区溢出保护的支持情况。

PsExec

在远程系统上执行进程。

PsFile

查看远程打开的文件。

PsGetSid

显示计算机或用户的 SID。

PsInfo

获取有关系统的信息。

PsKill

v1.13（2009 年 12 月 1 日）
终止本地或远程进程。

PsList

显示有关进程和线程的信息。

PsLoggedOn

显示登录到某个系统的用户。

PsLogList

转储事件日志记录。

PsPasswd

更改帐户密码。

PsService

查看和控制服务。

PsShutdown

关闭并重新启动（可选）计算机。

PsSuspend

挂起和继续进程。

PsTools

PsTools 套件包括一些命令行程序，可列出本地或远程计算机上运行的进程、远程运行进程、重新启动计算机、转储事件日志，以及执行其他任务。

RegDelNull

扫描并删除包含嵌入空字符的注册表项，标准注册表编辑工具不能删除这种注册表项。

RegJump

跳至 Regedit 中指定的注册表路径。

RootkitRevealer

扫描系统以找出基于 Rootkit 的恶意软件。

SDelete

安全地覆盖敏感文件，并使用此符合 DoD 的安全删除程序清理先前删除文件所在的可用空间。

ShareEnum

扫描网络上的文件共享并查看其安全设置，以关闭安全漏洞。

ShellRunas

通过方便的 shell 上下文菜单项，作为另一个用户启动程序。

Sigcheck

转储文件版本信息并检查系统中的映像是否已进行数字签名。

Streams

显示 NTFS 备用数据流。

Strings

在二进制映像中搜索 ANSI 和 UNICODE 字符串。

Sync

将缓存数据刷新到磁盘。

TCPView

活动套接字命令行查看器。

VMMap

VMMap 是进程虚拟和物理内存分析实用工具。

VolumeId

设置 FAT 或 NTFS 驱动器的卷 ID。

Whois

查看 Internet 地址的所有者。

WinObj

基本对象管理器命名空间查看器。

ZoomIt

在屏幕上进行缩放和绘图的演示实用工具。