

实战——恶意软件监视技术

——郭晋鹏

一、概述

众所周知，恶意软件是一个集合名词，是指非授权情况下在计算机上执行恶意任务的病毒、蠕虫、木马程序。恶意软件的危害也是有目共睹的，感染文件破坏操作系统，攻击服务器，使网络瘫痪，非法窃取用户重要信息等等。

本文将介绍如何用工具来监视和分析恶意软件的行为。

二、恶意软件一般有两大行为特征：

1. 网络行为特征

所谓网络特征，顾名思义，就是恶意软件在网络上表现的行为。常见的有：

- 1) 有些恶意软件会扫描局域网，搜寻有漏洞的主机，伺机传播。
- 2) 特洛伊木马会监听指定的控制端口，和远程控制端进行交互。有些 Bot 工具会发动对远程主机的 DDos 攻击，而有些病毒会疯狂的发送大量带病毒副本的邮件。

2. 系统行为特征

所谓系统行为特征，就是指恶意软件为了达到传播自身，掩饰自己不被发现等目的，而对系统进行修改的种种行为。常见的手法有：

- 1) 修改注册表：某些常见的恶意软件一般通过修改注册表的手法来达到开机随系统自动启动，自动加载等目的。
- 2) 修改系统文件：例如一些恶意软件为了阻止用户使用杀毒软件，提高自身存活率，通过修改系统的 hosts 文件，使得主机不能访问杀毒软件网站，从而不能进行在线杀毒和病毒库更新。
- 3) 杀死对自己有威胁的进程：通过实时监视系统进程，及时杀死某些著名杀毒软件或者监控软件的进程，从而达到保护自己的目的（所谓先下手为强）
- 4) 感染文件：感染系统文件，生成大量副本，传播自身。

三、工具介绍

“工欲善其事，必先利其器”，在开始研究恶意软件的一些行为之前，让我们先来熟悉一下将要用到的工具。

针对恶意软件的两大行为特征，我们需要准备以下几种工具：

1) 网络监控工具。

每种工具都有它的优缺点，所以要学会扬长避短，互相补充。

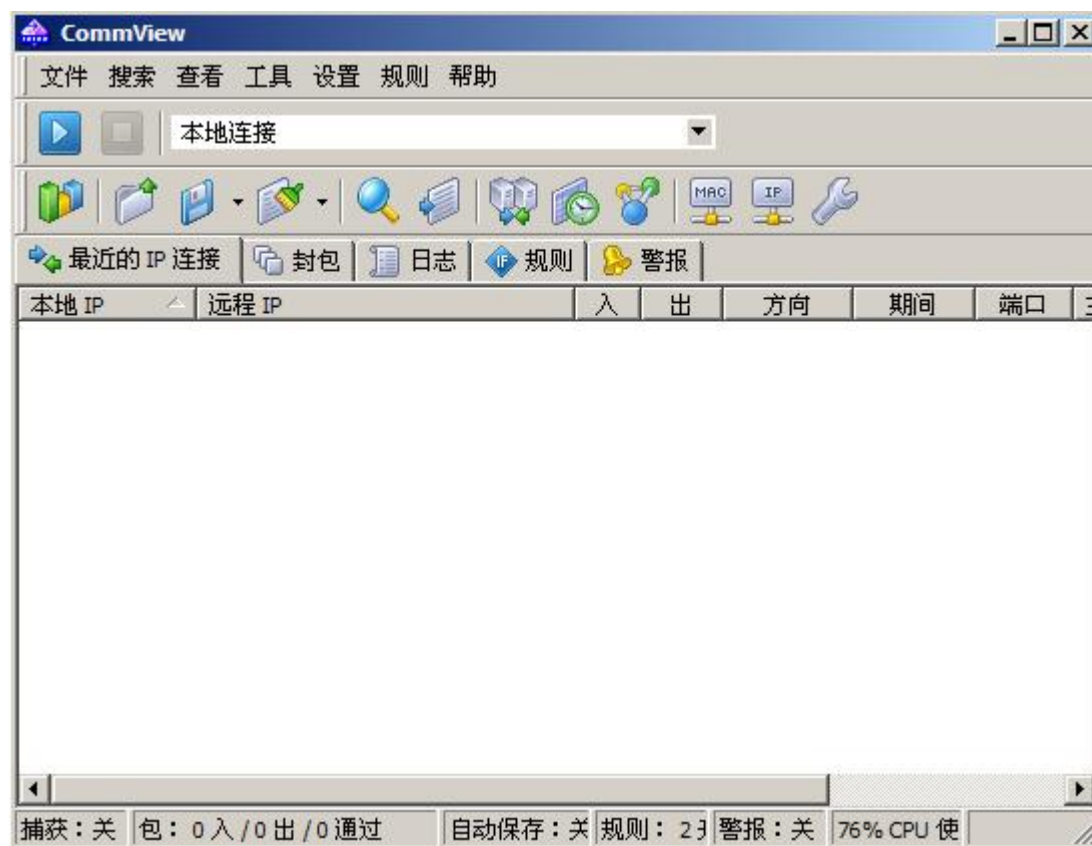
Fport——网络监测首先是监测本地的程序和外界有什么连接，这里较为推崇的是 **Fport**，现在的版本是 2.0。Fport 可以把本机开放的 TCP/UDP 端口同应用程序相关联，并可以显示进程 PID，名称和路径。结合 windows 下的命令“netstat -na”，就可以将本地进程，本地端口，远程主机 IP 及端口都联系起来。对我们分析恶意软件的网络行为很有帮助。由于 Fport 比较使用简单，这里不再赘述。详情见 Fport 帮助。

Sniffer——虽然知道了恶意软件和哪些主机有连接，但是我们更关心的是，这些恶意软件通过网络在做些什么，是在发送病毒副本，还是在发起 DDos（远程拒绝服务）攻击，还是在和控制者进行联系，泄露用户的信用卡帐号密码之类的。这里我们就要对发送和接收的数据包进行窃听，也叫嗅探，用到的工具当然就是嗅探器（sniffer）了。**Sniffer** 是一个强大的网络监视工具，它通过抓取经过本机网卡的所有数据包，监测网络中各种协议、大小的数据包的数量、传播方向、传播速度等等，是网络管理员监测网络性能的得力工具，同时，也

是黑客等进行不法活动的利器。Sniffer 最早出现在 Unix 系统中，例如 Tcpdump，Snoop；后来人们又开发出了 windows 环境下的 Sniffer，例如 Sniffer pro，Commview。由于这次对恶意软件的监控是在 windows 环境下的，所以我们选择了 Commview 这款软件。下面着重介绍一下 Commview 的使用。

1. 下载 Commview 5.0，安装

2. 安装好之后，就可以试运行了。下面是主界面（如图 1）

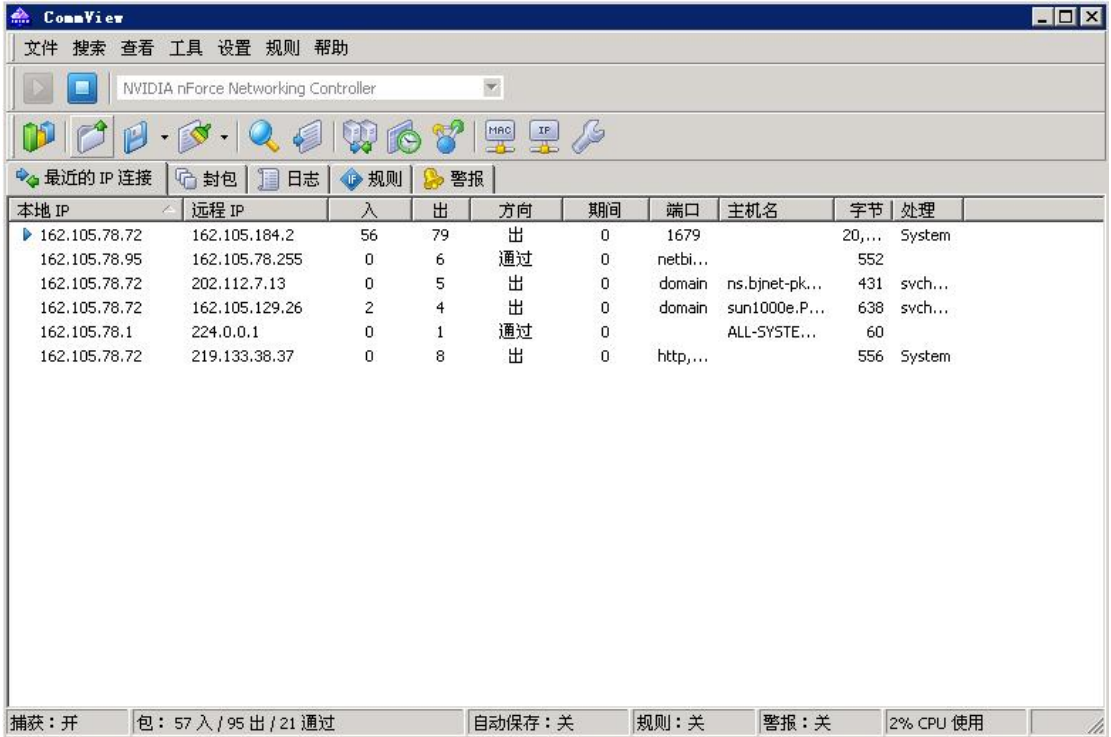


（图 1-Commview_主界面）

这里可以选择要监听的网络适配器（网卡）、可以设置过滤规则，查看当前连接状况、查看捕获到的数据包的内容以及一些复杂的设置。

3. 基本操作

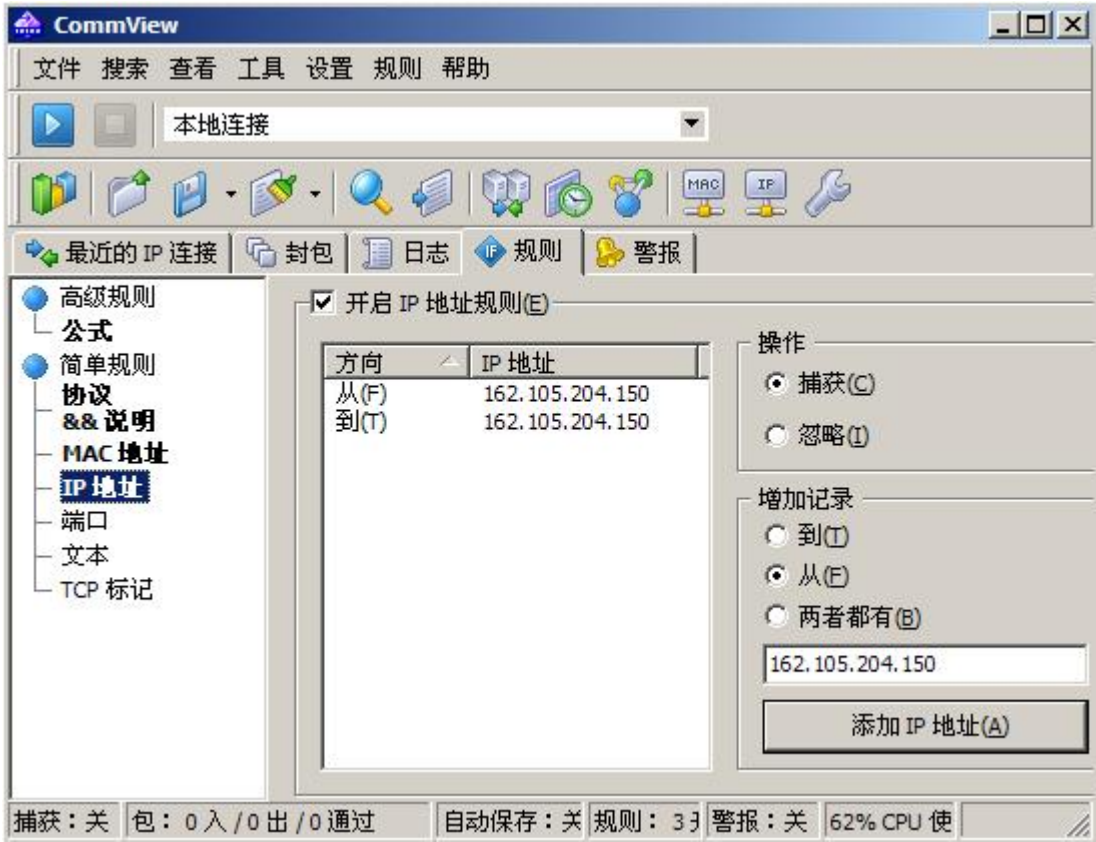
1) 按“开始捕获”开始抓包，如图 2 所示：



(图 2-Commview_开始捕获数据包)

可以看到，输出窗口记录了当前连接的 IP，通过的数据包的数量，以及相关的进程。

2) 为了监视指定的 IP 或者指定的端口的数据包，可以设置过滤规则。如图 3 所示：



(图 3-Commivew_设置过滤规则)

这里可以设置 IP、端口、协议、等等过滤条件，具体按自己的需要而定。

3) 查看数据包内容。可以在“封包”选项里面查看数据包的内容。这里是对刚才 telnet 登陆 162.105.204.150 的纪录, 如图 4 所示:



(图 4-Commview_查看捕获结果)

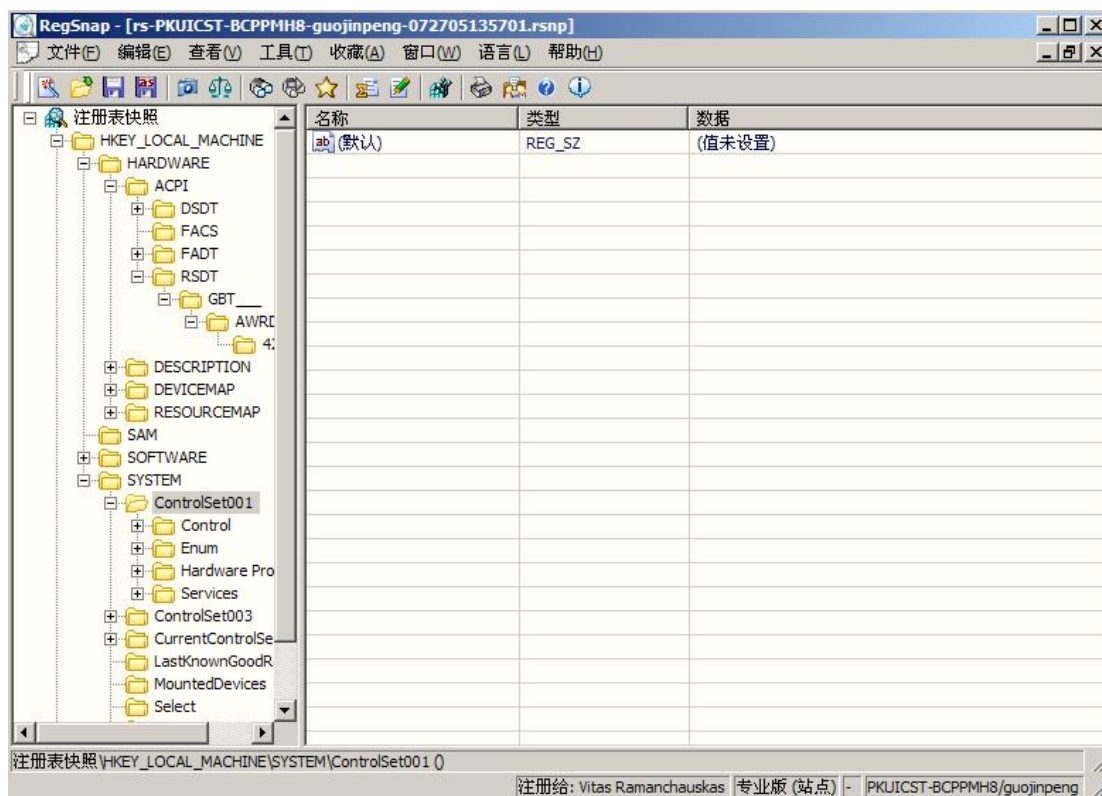
由于 telnet 协议是以明文形式传送的, 所以我们可以直接以 ASCII 形式看到其内容。如果是别的协议, 还需要特殊的解码器。

Commview 的使用就简单介绍到这里, 一会儿我们将用它来监控一个具体的恶意软件。

2) 系统监控工具。

监控系统主要是监控文件系统, 注册表, 以及内存进程。

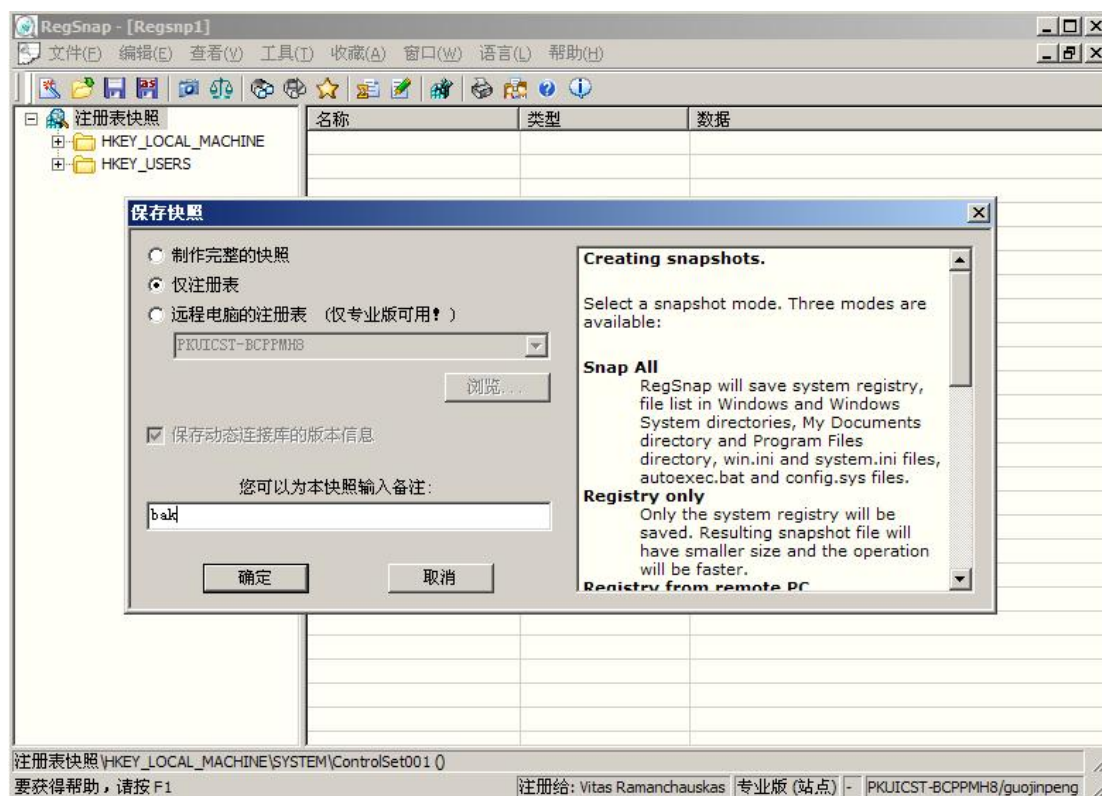
RegSnap——一款很优秀的既可以监视注册表变化, 又可以监视系统文件变化的工具。与别的同类软件不同的是, 它可以对注册表以及系统文件做快照, 并可以对两个快照作比较, 从而发现注册表和系统文件的变化。并且还提供了恢复注册表的功能, 也相当于一个注册表的备份工具。我们看一下软件的主界面 (如图 5 所示):



(图 5-RegSnap_主界面)

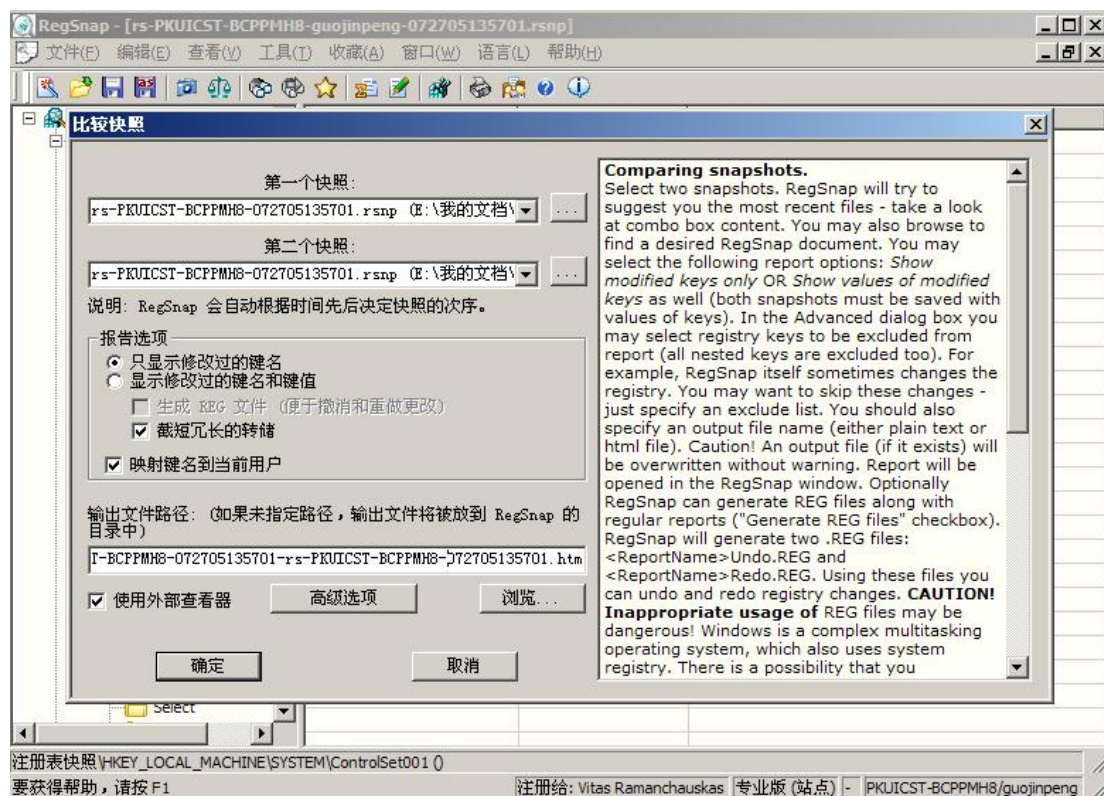
基本操作:

1) 建立快照。为当前注册表以及系统文件信息建立快照。单击工具栏—“新建快照”就可以了 (如图 6 所示):



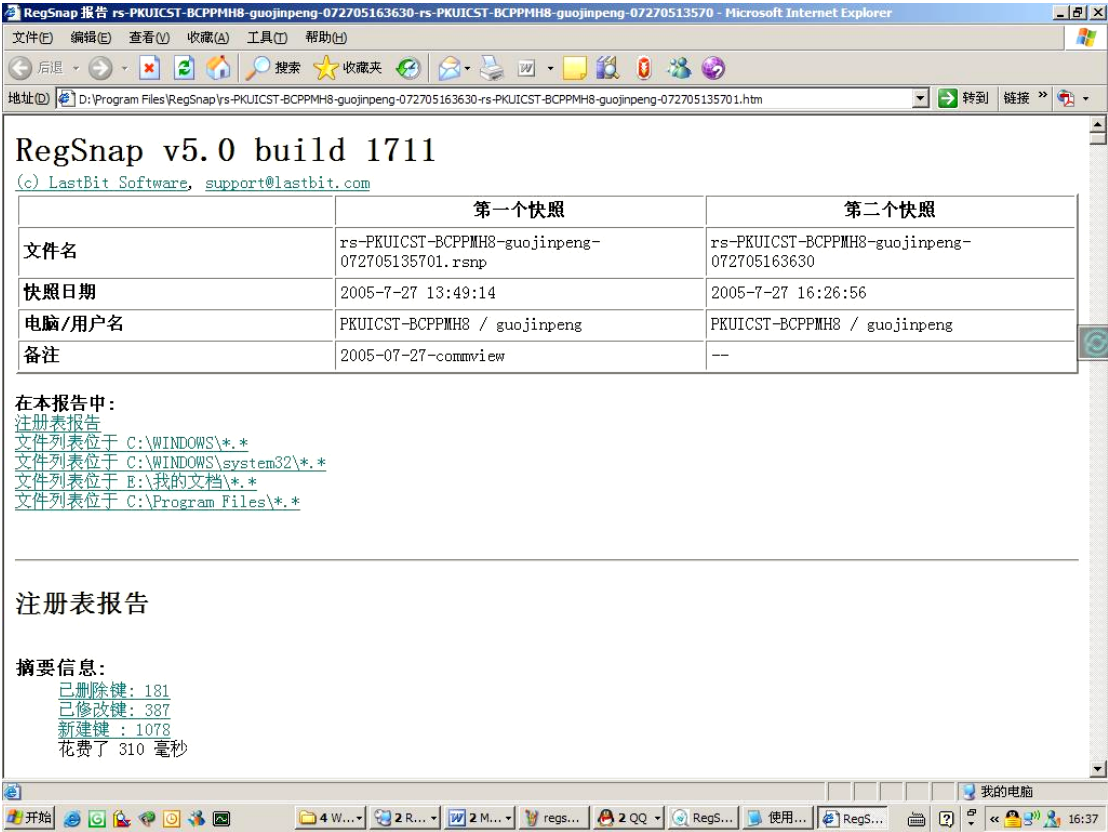
(图 6-RegSnap_建立快照)

2) 经过一些操作以后(例如恶意软件改变了注册表之后),再进行一下快照。然后按“比较”比较前后两次快照的内容,可以得出一个差异报告。如图 7 所示:



(图 7-RegSnap_比较两次内容)

3) 查看报告。这个报告是 html 格式的,方便查阅和分析。不过有很多冗余信息,所以使用的时候,要确定好两个快照的时间间隔,并且中间最好不要做冗余的操作。这样可以较精确的得出结论,而且花的力气也较少。如图 8 显示的是生成的差异报告。



(图 8-RegSnap_差异报告)

可见报告中对各种差异都作了统计，便于我们查看。

PrcView——内存进程监控。PrcView 是一款小巧的进程查看器。他不仅可以完全替代 windows 的任务管理器的进程查看功能，而且有许多自身的优点，例如，可以查看进程的完整路径，可以查看进程的相关启动信息，可以查看进程的模块调用情况，以及内存使用情况。更重要的是，有时候有些恶意软件会杀死任务管理器进程，这时 PrcView 就可以大显身手了。让我们来看一下它的主界面，如图 9 所示

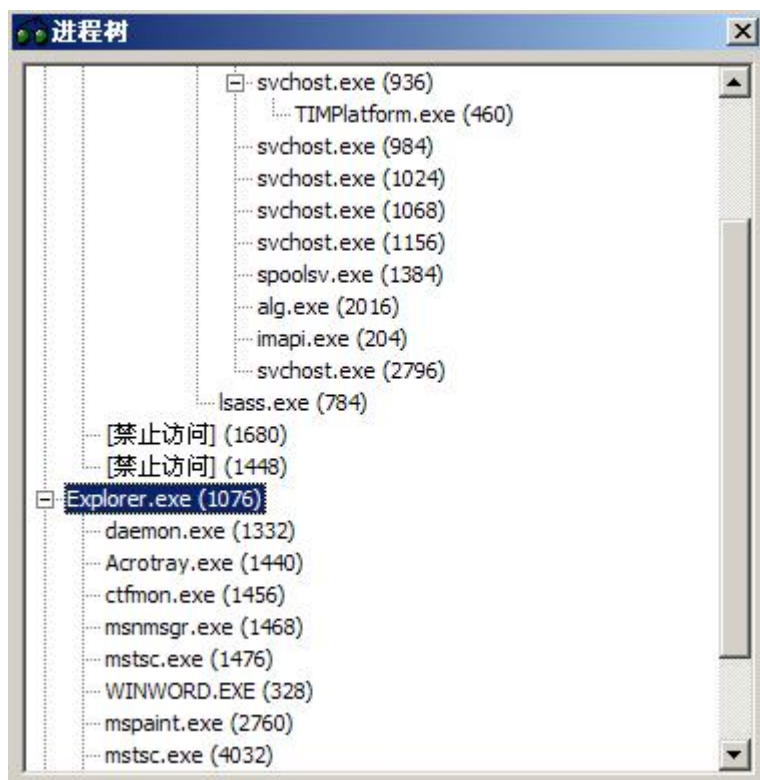


(图 9-PrcView_主界面)

界面简洁明了，很直观的可以看出当前的进程状况。

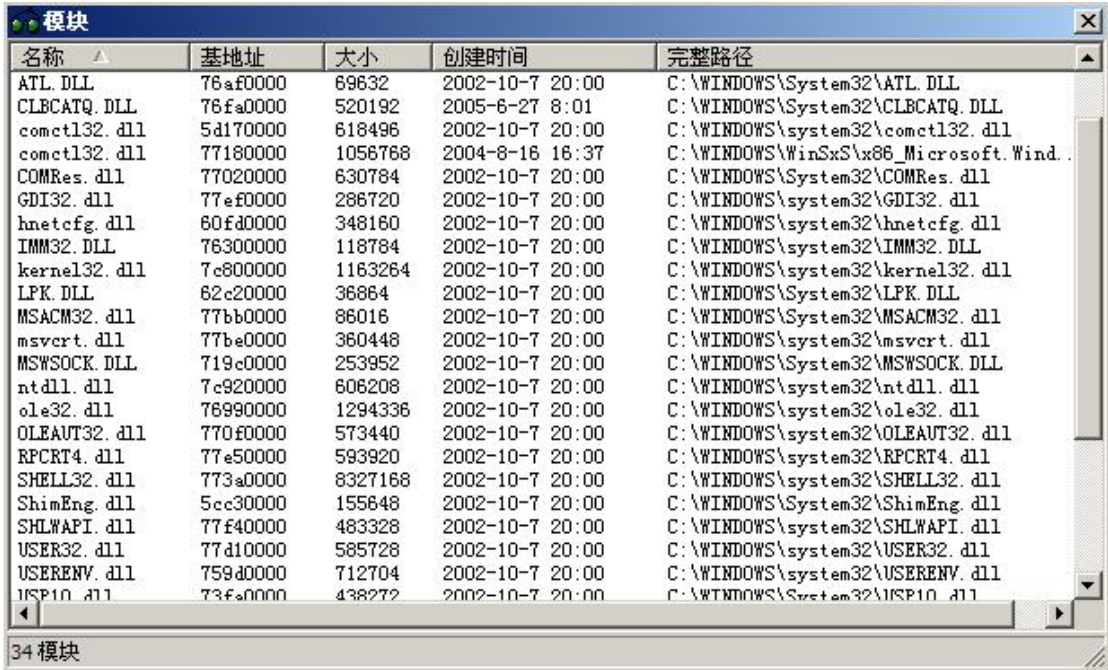
基本操作：

1) 查看进程树：工具栏一查看一进程树，如图 10 所示



(图 10-PrcView_查看进程树)

2) 查看模块使用情况, 如图 11 所示

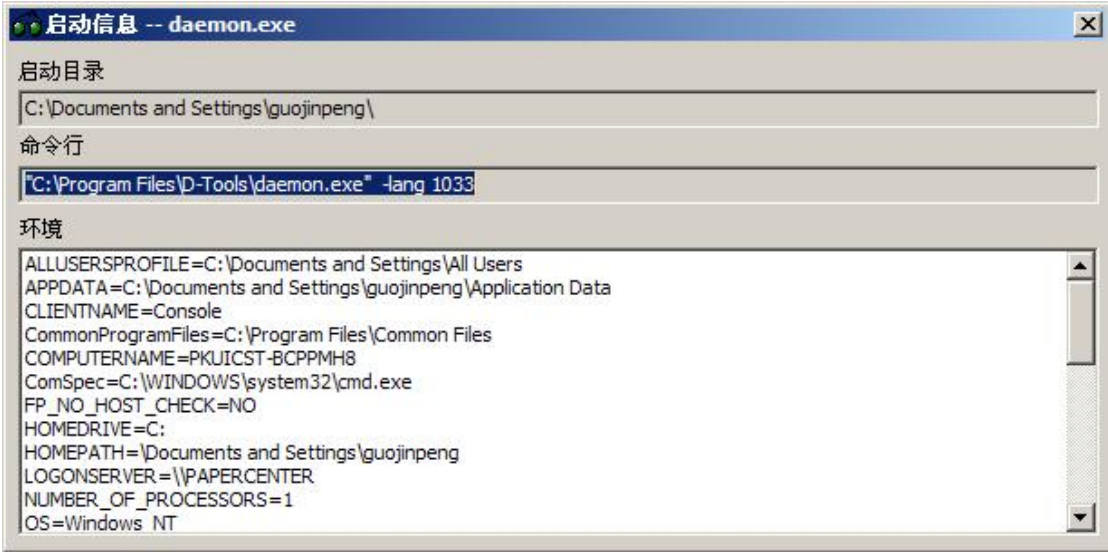


名称	基地址	大小	创建时间	完整路径
ATL.DLL	76af0000	69632	2002-10-7 20:00	C:\WINDOWS\System32\ATL.DLL
CLBCATQ.DLL	76fa0000	520192	2005-6-27 8:01	C:\WINDOWS\System32\CLBCATQ.DLL
comctl32.dll	5d170000	618496	2002-10-7 20:00	C:\WINDOWS\system32\comctl32.dll
comctl32.dll	77180000	1056768	2004-8-16 16:37	C:\WINDOWS\WinSxS\x86_Microsoft.Wind...
COMRes.dll	77020000	630784	2002-10-7 20:00	C:\WINDOWS\System32\COMRes.dll
GDI32.dll	77ef0000	286720	2002-10-7 20:00	C:\WINDOWS\system32\GDI32.dll
hnetcfg.dll	60fd0000	348160	2002-10-7 20:00	C:\WINDOWS\system32\hnetcfg.dll
IMM32.DLL	76300000	118784	2002-10-7 20:00	C:\WINDOWS\system32\IMM32.DLL
kernel32.dll	7c800000	1163264	2002-10-7 20:00	C:\WINDOWS\system32\kernel32.dll
LPK.DLL	62c20000	36864	2002-10-7 20:00	C:\WINDOWS\System32\LPK.DLL
MSACM32.dll	77bb0000	86016	2002-10-7 20:00	C:\WINDOWS\System32\MSACM32.dll
msvcrt.dll	77be0000	360448	2002-10-7 20:00	C:\WINDOWS\system32\msvcrt.dll
MSWSOCK.DLL	719c0000	253952	2002-10-7 20:00	C:\WINDOWS\System32\MSWSOCK.DLL
ntdll.dll	7c920000	606208	2002-10-7 20:00	C:\WINDOWS\system32\ntdll.dll
ole32.dll	76990000	1294336	2002-10-7 20:00	C:\WINDOWS\system32\ole32.dll
OLEAUT32.dll	770f0000	573440	2002-10-7 20:00	C:\WINDOWS\system32\OLEAUT32.dll
RPCRT4.dll	77e50000	593920	2002-10-7 20:00	C:\WINDOWS\system32\RPCRT4.dll
SHELL32.dll	773a0000	8327168	2002-10-7 20:00	C:\WINDOWS\system32\SHELL32.dll
ShimEng.dll	5cc30000	155648	2002-10-7 20:00	C:\WINDOWS\System32\ShimEng.dll
SHLWAPI.dll	77f40000	483328	2002-10-7 20:00	C:\WINDOWS\system32\SHLWAPI.dll
USER32.dll	77d10000	585728	2002-10-7 20:00	C:\WINDOWS\system32\USER32.dll
USERENV.dll	759d0000	712704	2002-10-7 20:00	C:\WINDOWS\system32\USERENV.dll
USP10.dll	73fa0000	438272	2002-10-7 20:00	C:\WINDOWS\System32\USP10.dll

34 模块

(图 11-PrcView_查看模块使用情况)

3) 查看进程启动信息, 如图 12 所示



启动目录
C:\Documents and Settings\guojinpeng\

命令行
"C:\Program Files\D-Tools\daemon.exe" -lang 1033

环境
ALLUSERSPROFILE=C:\Documents and Settings\All Users
APPDATA=C:\Documents and Settings\guojinpeng\Application Data
CLIENTNAME=Console
CommonProgramFiles=C:\Program Files\Common Files
COMPUTERNAME=PKUICST-BCPPMH8
ComSpec=C:\WINDOWS\system32\cmd.exe
FP_NO_HOST_CHECK=NO
HOMEDRIVE=C:
HOMEPATH=\\Documents and Settings\guojinpeng
LOGONSERVER=\\PAPERCENTER
NUMBER_OF_PROCESSORS=1
OS=Windows NT

(图 12-PrcView_查看进程启动信息)

通过查看启动信息, 有时候可以判断它是不是恶意软件

4) 查看进程版本, 如图 13 所示



(图 13-PrcView_查看进程版本)

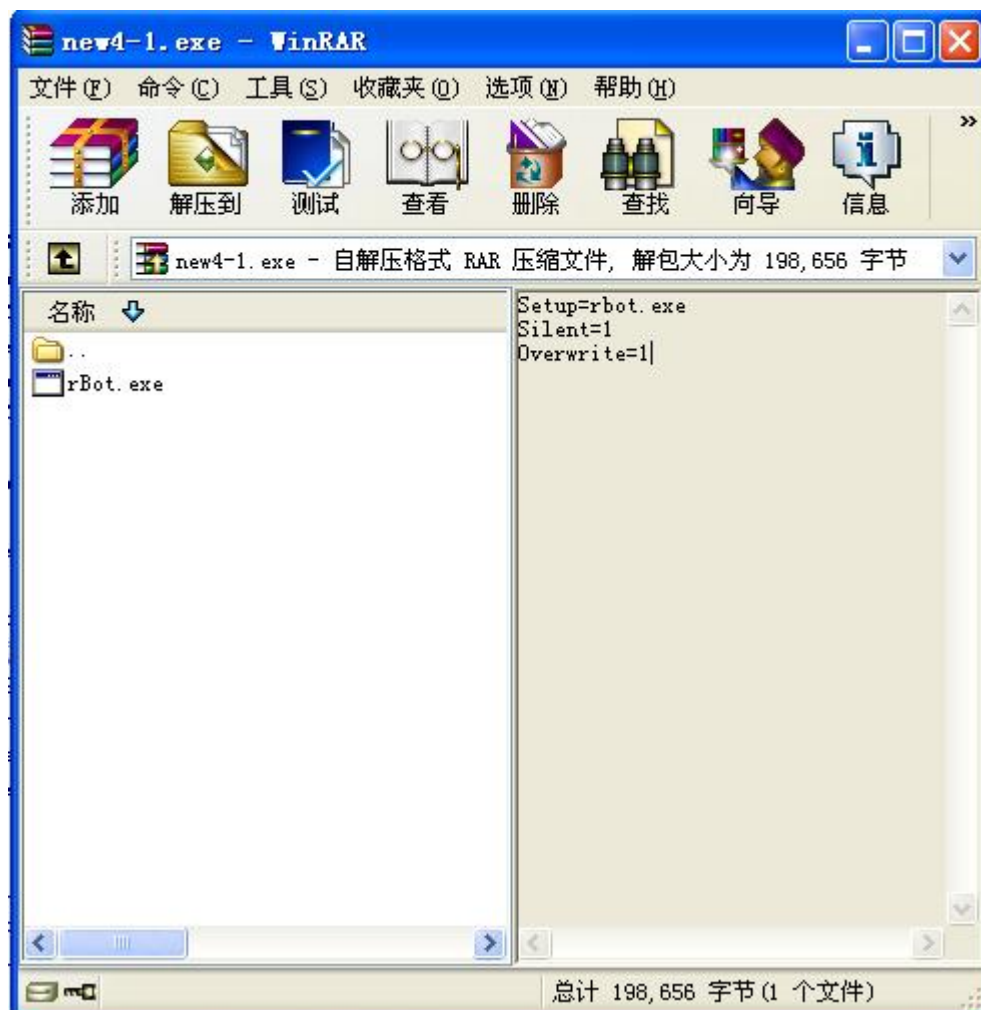
有时候，查看进程的版本可以识别一些名字比较隐蔽的恶意软件进程

工具就介绍到这里，下面就是激动人心的实战了~

四：对 bot 工具 rbot 的监控与分析

我们采用的样本是由我们的恶意软件收集器（mwcollect）收集的。出于对安全性的考虑，实验将在一台虚拟机上进行。因为如果直接在一台主机上跑这些软件的话，很难确保这台实验主机的安全性及其所在网络的安全性。所以，我们的虚拟操作系统安装在虚拟机 VMware 上，并且安装的是没有打 sp1 和 sp2 补丁包的 WindowsXp，以便于恶意软件能够正常运行。

我们的样本是名为 new4.exe 的 WinRAR 自解压程序，仔细观察，自解压的结果是直接运行里面的 rbot.exe（注意右侧的“Setup=rbot.exe”，就是自动运行的意思），如下图所示：



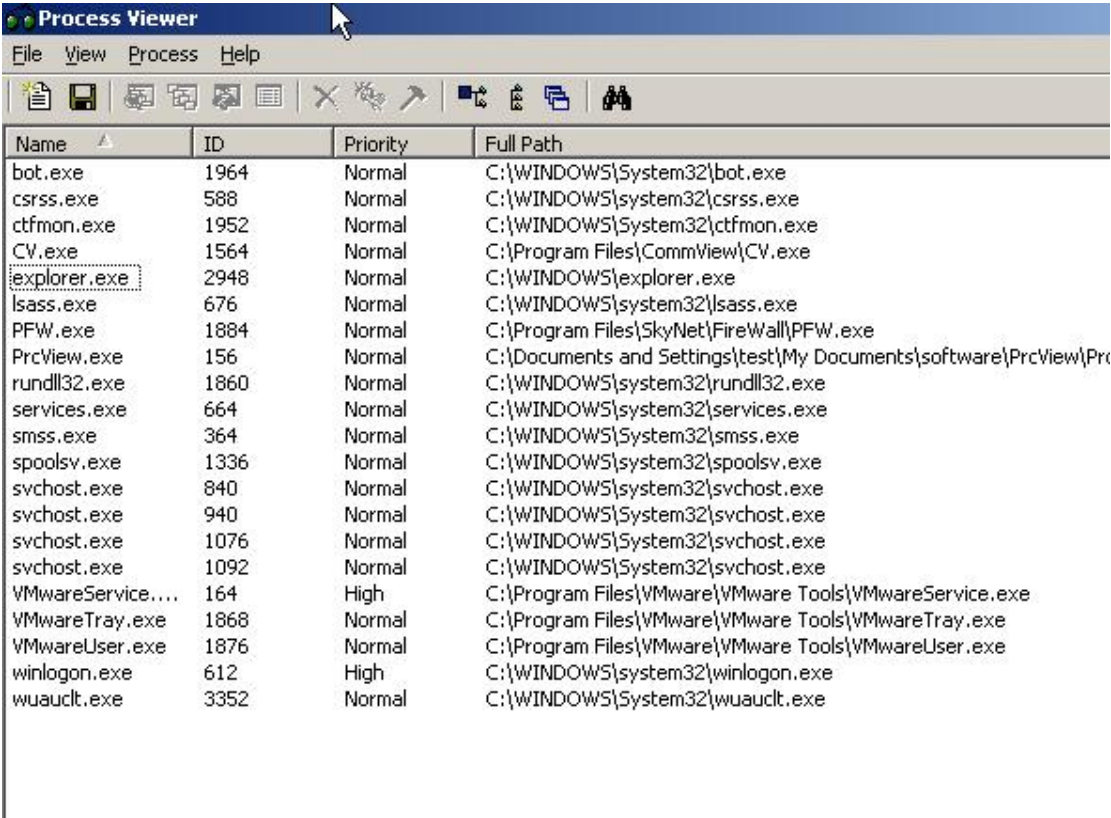
(图 14-rbot_1)

在运行这个 rbot 之前，先要做一些准备工作：

- 1) 开启 XP 的系统还原，并且设置一个还原点，便于及时将系统恢复。
- 2) 打开 RegSnap，做一个注册表和系统文件的镜像，作为原始系统的镜像，以便以后比较。
- 3) 打开 Commview，准备观察连接情况和捕获数据
- 4) 打开 防火墙，观察网络连接状况
- 5) 打开 PrcView，准备监视系统进程

一切准备就绪，然后就可以双击那个自解压的程序了。

运行之后，首先进程中多了一个 bot.exe,如图所示



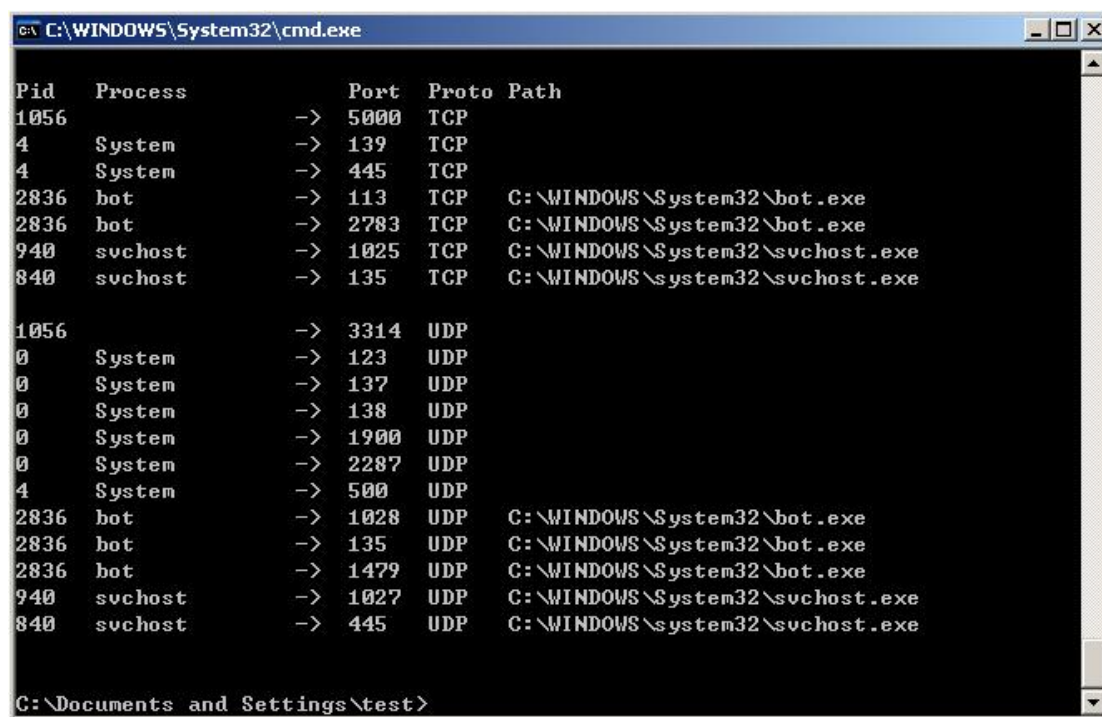
(图 15-bot.exe)

然后，观察 Commview，发现进程 bot.exe 正在向外发送数据包，远程主机的 IP 为 203.151.217.85，端口是 6667，6667 端口一般是登陆 irc 服务器的端口，所以可以断定这个 bot.exe 是一个 bot 工具，而 IP 为 203.151.217.85 的主机就是一台 irc 服务器。不过，在 Commview 观察只有发送出去的包，没有接收到的包，因此基本可以判断，该 irc 服务器是不可达的，可能 down 掉了。来看一下截图：



(图 16-Commview_截图)

用 Fport 来观察（如图 17），可以看到进程 bot.exe 还在监听别的端口，例如 113，135 等等。113 端口也是木马常常利用的端口，而 135 端口主要用于使用 RPC（Remote Procedure Call，远程过程调用）协议并提供 DCOM（分布式组件对象模型）服务，由此可以判断该 bot 工具可能会利用 RPC 缓冲区溢出漏洞进行传播。可见该 bot 工具的利用了多种方式进行传播。



(图 17-Fport_截图)

暂时这个 bot.exe 还没有什么动静，那就先来看一下 rbot 对系统文件和注册表的修改吧。用 RegSnap 再做一个注册表和系统文件的镜像，然后和原来的那个做比较，生成一个报告。先来看对系统文件的修改，因为这个比较直观，容易识别哪些是恶意软件修改的，哪些是系统运行修改的。摘要如下：

文件列表位于 C:\WINDOWS\System32*.*

摘要信息:

已删除文件: 0

已修改文件: 1

新建文件 : 4

已修改文件

catroot2

旧: 大小: 0, 日期/时间: 2005 年 7 月 30 日 21:11:19

新: 大小: 0, 日期/时间: 2005 年 7 月 30 日 23:05:06

位置总数: 1

新建文件

bot.exe 大小: 198,656, 日期/时间: 2002 年 10 月 7 日 20:00:00

jfpzt.msc 大小: 26,624, 日期/时间: 2005 年 7 月 30 日 22:42:20

vv.dat 大小: 26,624, 日期/时间: 2005 年 7 月 30 日 22:42:20

xpdqqg32.dll 大小: 37,888, 日期/时间: 2002 年 10 月 7 日 20:00:00

位置总数: 4

其中，在 system32 目录下面的四个新建的文件最值得怀疑了。仔细观察，其中的 bot.exe 和 xpdqqg32.dll 的文件建立日期居然是 2002 年 10 月 7 日 20:00:00，和大多数系统文件一样，够狡猾的。大胆猜测一下，bot.exe 就是 bot 工具，用来和远程 irc 服务器进行通信，对本机进行控制；xpdqqg32.dll，应该是要注入某个系统进程的 dll，随着那个进程的启动而启动。而 jfpzt.msc 和 vv.dat 的作用暂时还不太清楚，不过在打开 system32 查找这些文件的时候，发现 vv.dat 不见了，由于这两个文件的大小一样，可以判断 vv.dat 是 jfpzt.msc 的一个副本。为了确定这个 jfpzt.msc 文件到底是一个什么文件，我通过如下步骤来确定它的类型。

- 1) 后缀为 msc 的文件应该可以用 Windows 的管理控制台来直接打开，但是双击该文件发现不能运行，提示为该文件不是一个 mmc 文件，不能用 Windows 的管理控制台来打开。
- 2) 猜测该文件将后缀名设置为 msc 只是一个幌子，会让用户误认为是系统文件，实际上应该是病毒的副本，即可执行程序。为了证明这个判断，用软件 eXeScope 打开这个文件，果然是可执行程序。

然后来分析注册表：

日志里面注册表的修改比较多，但是要找到正确的入口也不难，因为我们已经找到了恶意软件的程序，它要开机自动运行，一定会在注册表里面留下痕迹。找出来的关键之处主要有以下几处：

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Reg
键值: 字符串: "bot.exe"

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{30D08AAD-D074-45BE-E0A9-9A5FFB394EC4}\
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{30D08AAD-D074-45BE-E0A9-9A5FFB394EC4}\@
键值: 字符串: ""

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{30D08AAD-D074-45BE-E0A9-9A5FFB394EC4}\InprocServer32\
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{30D08AAD-D074-45BE-E0A9-9A5FFB394EC4}\InprocServer32\@
键值: 字符串: "C:\WINDOWS\System32\xpdqqg32.dll"

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{30D08AAD-D074-45BE-E0A9-9A5FFB394EC4}\InprocServer32\ThreadingModel
键值: 字符串: "Apartment"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DataAccess\Database
键值: 字符串: "hfddfsdhaa"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DataAccess\Paradox
键值: 字符串: "C:\WINDOWS\System32\jfpzt.msc"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DataAccess\SQL
键值: 字符串: "mfuzuhybwi"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Reg
键值: 字符串: "bot.exe"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\Reg
键值: 字符串: "bot.exe"

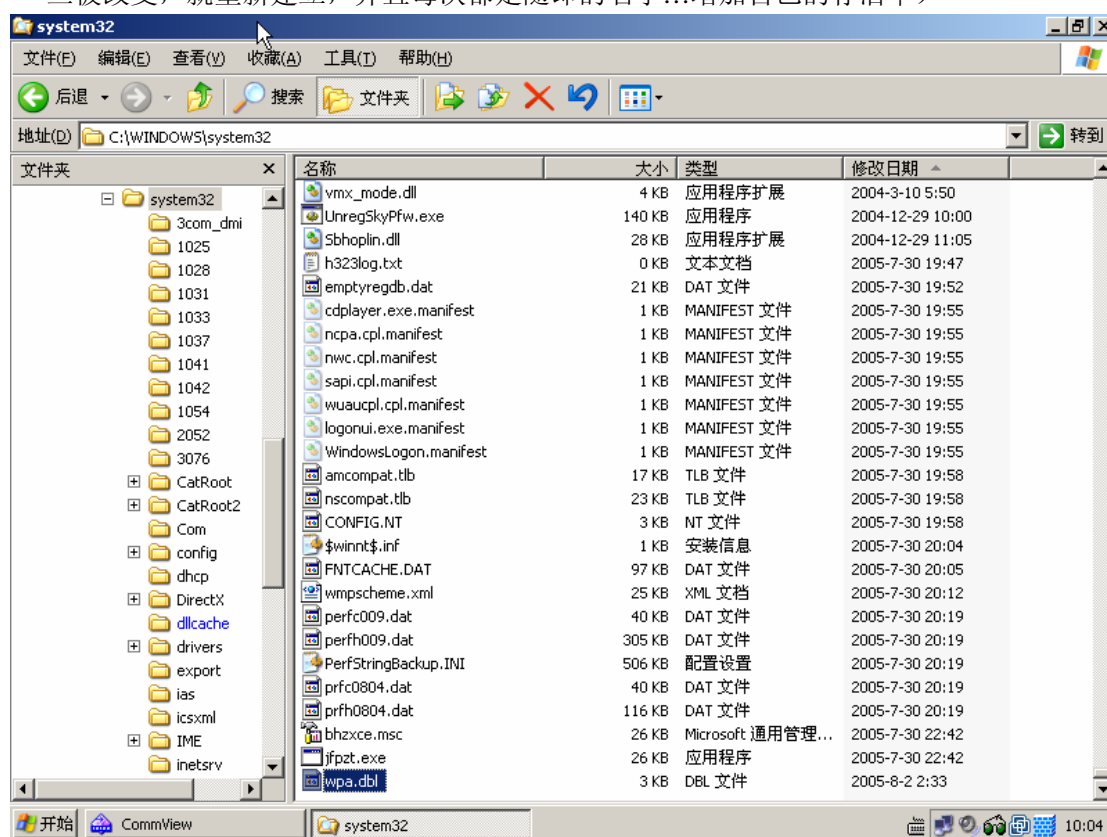
简要的分析一下:

- 1) 包含有"bot.exe"的那几条, 很明显的, 就是在系统启动的时候运行 bot.exe, 这也是大多数恶意软件最惯用的伎俩之一。其实写一处就可以了, 但是它写了好几处, 以防被删除。
- 2) "xpdqqg32.dll", 这个动态链接库将在一会儿的分析中占有很重要的角色。可以看到, 该 rbot 在注册表中将他注册为一个 CLSID 为 30D08AAD-D074-45BE-E0A9-9A5FFB394EC4 的组件, 并且设置了它的线程运行模式。这样程序就可以在外随时调用这个 dll 了。这时可以断定, "xpdqqg32.dll"一定是注册在某个系统进程里面运行的。
- 3) "jfpzt.msc" 注册表中和他相关的是

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DataAccess\Database
键值: 字符串: "hfddsfdsdhaa"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DataAccess\Paradox
键值: 字符串: "C:\WINDOWS\System32\jfpzt.msc"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DataAccess\SQL
键值: 字符串: "mfuzuhybwbi"

随即的那两个字符串“hfddsfdsdhaa”和“mfuzuhybwbi”是没有意义的，目的是为了掩饰，关键的还是“C:\WINDOWS\System32\jfpzt.msc”这一条。写在这里，应该也是为了外部调用的方便。

注册表就暂时分析到这里，概括起来，主要内容是：将 bot.exe 加入系统的启动项中；将“xpdqqg32.dll”注册为系统组件，方便调用；将“jfpzt.msc”写入注册表的隐蔽地方，作为恶意软件的备份。（小插曲：刚才把 jfpzt.msc 的后缀名改为.exe 的时候，过了一会儿去看 system32 文件夹，发现目录下面又有一个新的 msc 文件“bhzxce.msc”，大小和原来的“jfpzt.msc”完全一样（见图），可见该恶意软件的进程在实时监视着自己文件以及注册表的变化，一旦被改变，就重新建立，并且每次都是随即的名字...增加自己的存活率）

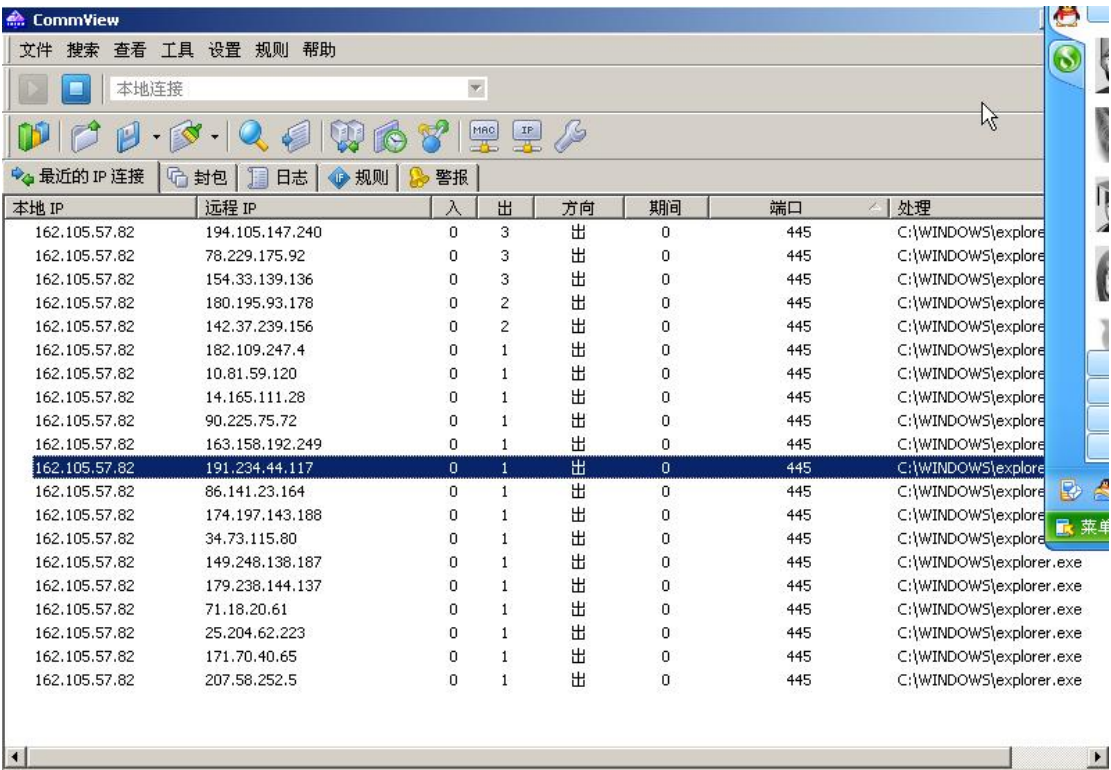


(图 18-两个副本)

下面再回到网络监控上来。

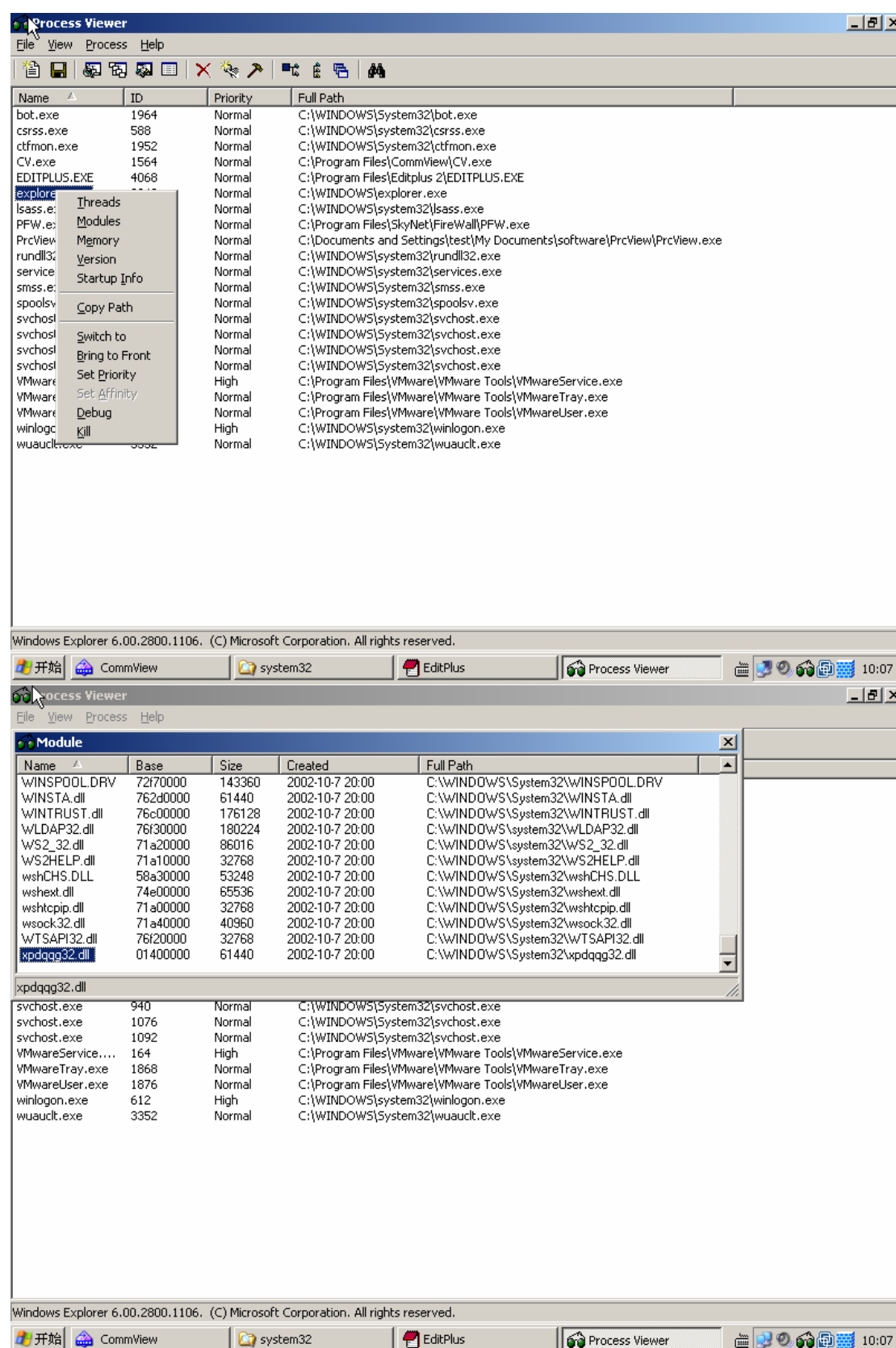
开始的时候，除了发现进程 bot.exe 对外发送一些数据报以外，并没有其他明显的可疑进程。而且，bot.exe 所连接的远程 irc 服务器也总是不响应，但一直在以一定的频率发送大小为 62 字节的数据包。但是过了一小会儿，发现 Commview 里面的数据包突然多起来，而且端口都是 445。大量的这种包发送到随机的 IP 地址，目不暇接，很快系统资源就几乎枯竭了。从 Commview 里面可以看出，发送这些包的进程是 explorer.exe，也就是 Windows 的

资源管理器进程。这时，将 explorer 杀死，就不会再发包了。如图：



(图 19-445 端口，资源管理器)

可以推测出，一定是恶意软件将自己的 DLL 注册到进程 explorer 里面，启动自己的线程来发送这些包的。所以，过了几分钟，当发现 explorer 又开始大量的向外发送数据包的时候，用 PrcView 观察 explorer 的模块调用情况，果然有一个 xpdqqg32.dll，也就是刚才我们提到的恶意软件生成的那几个文件之一。如图所示：



(图 20、21—注册在 explorer 里面的 dll，用来启动扫描线程)

然后将 explorer 杀死以后，explorer 自动重启，再观察其模块使用情况，发现没有了 xpdqgg32.dll，也没有了向外疯狂发送数据包的过程。通过仔细的观察，发现目标的 IP 是随机生成的，但是目标端口都是 445，所以可以判断应该是进行网络扫描，扫描有弱点的机器，

可以很容易的猜想到是扫描有 RPC 漏洞的主机。因为现在 RPC 缓冲区溢出漏洞是恶意软件最常利用的漏洞，其端口又是 445。

结束掉 explorer 之后，偶然打开 FlashFxp 下载点东西，过了一会儿发现 flashfxp 在疯狂的向外发数据包。然后观察其模块调用情况，发现有 **xpdqqg32.dll**...可见，该 dll 不仅可以注册到 explorer 里面，还可以注册到其他进程里面。后来又发现了一次注册到任务管理器进程 taskmgr.exe 里面的情况。

对于什么时候扫描开始，什么情况触发 **xpdqqg32.dll** 进行扫描，在经过较长时间的观察之后，发现如下规律：

- 1) bot.exe 启动与否，都不影响扫描的启动
- 2) 打开新的程序，都会激发 **xpdqqg32.dll** 开始扫描
- 3) 如果有一段时间没有扫描，扫描将在一段随机的时间后重新启动
- 4) 尝试删除 **xpdqqg32.dll** 后，会生成一个新的 dll，名字随机。下面是删除 **xpdqqg32.dll** 的时候用 RegSnap 扫描的结果。

已删除文件	
jfpzt.msc	大小: 26,624, 日期/时间: 2005 年 7 月 30 日 22:42:20
xpdqqg32.dll	大小: 37,888, 日期/时间: 2002 年 10 月 7 日 20:00:00
新建文件	
bhzxce.msc	大小: 26,624, 日期/时间: 2005 年 7 月 30 日 22:42:20
jfpzt.exe	大小: 26,624, 日期/时间: 2005 年 7 月 30 日 22:42:20
jqyhe32.dll	大小: 37,888, 日期/时间: 2002 年 10 月 7 日 20:00:00

然后这个新的 **jqyhe32.dll** 继续扮演原来 dll 的角色，发起无数线程，扫描漏洞主机。

综上，对该 bot 工具的分析总结如下：

- 1) 生成系统文件夹下文件 bot.exe 、 [*****].msc、 [*****].dll，其中括号内是随机的文件名
- 2) 对注册表做如下修改

i: 在下列位置添加键值 bot.exe，使得该程序能随系统启动

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\Reg

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Reg

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\Reg

ii: 新建键值

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{30D08AAD-D074-45BE-E0A9-9A5FFB394EC4}\InprocServer32\@

键值: 字符串: "C:\WINDOWS\System32\xpdqqg32.dll"

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{30D08AAD-D074-45BE-E0A9-9A5FFB394EC4}\InprocServer32\ThreadingModel

键值: 字符串: "Apartment"

作为扫描漏洞主机的主要工具

iii: 新建

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DataAccess\Database

键值: 字符串: "hfddsfshaa"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DataAccess\Paradox

键值: 字符串: "C:\WINDOWS\System32\jfpzt.msc"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DataAccess\SQL

键值: 字符串: "mfuzuhybwi"

作为自身的备份, 或者其它用途。

- 3) 进程 bot.exe 随系统启动, 登陆远程 irc 服务器, 等待命令
- 4) [***].dll 注入系统活跃进程, 随时启动大量的线程, 对随机的主机进行扫描, 以发现漏洞主机, 扩大感染范围。