NOVEMBER 10, 2024

HUNTING IN MEMORY

LAB 03

ANTHONY CAMPBELL (STUDENT)
Professor McCulley
University of Texas at San Antonio IS 3523

Contents

Introduction

This lab focuses on hunting in memory using Volatility, a memory forensics tool, to investigate a memory dump file, KobayashiMaru.vmem, for indications of malicious activities. Our goal is to identify potential signs of compromise by analyzing various aspects of the system memory. This will include examination of the operating system, identifying running processes, and analyzing DLLs, files, and file paths for anything unusual that might indicate unauthorized activity on the system.

Basics of the System

I start by finding some basic information concerning the system this vmem dump came from, and of the vmem itself. Using *volatility -f KobayashiMaru.vmem imageinfo* I can find some information. The output we receive back gives us a suggested profile of Win XP, likely Service Pack 2 or 3 on a 32-bit architecture with Service Pack 2 chosen to instantiate the analysis. We can also determine that since Physical Address Extension (PAE) is not enabled, the system is limited to a maximum of 4GB of RAM or less. (Microsoft, 2021) (see Appendix 1: Volatility imageinfo)

Processes

Next I want to list the processes that were running when this vmem dump was created. With *volatility -f KobayashiMaru.vmem –profile=WinXPSP2x86 pslist* we can list the processes running at the time. We see some standard system services while also unfortunately seeing some usual suspects, in terms of malware and suspicious activities, that make it far from the 'average' or typical box. (see reference Appendix 2: Volatility pslist)

The Expected

An average Windows XP system will contain processes like System, smss.exe, csrss.exe, and several instances of svchost.exe (which also may be worth investigating at times), which handles a lot of essential Windows services. Other expected processes like explorer.exe for the Windows shell and VMware processes like VMwareService.exe also were running, indicating that the system is running within a virtual machine.

Abnormalities

We have a few unusual, potentially malicious, and outright malicious processes running, however. We have hxdef100.exe which is related to Hacker Defender, a known rootkit used to hide processes and files from the operating system. The presence of Hacker Defender could indicate an attempt to conceal further malicious activities on the machine. We also find cryptcat.exe which is suspicious, as Cryptcat is a networking tool used often for covert communication and data transfer, which could indicate data exfiltration or unauthorized remote control. The bircd.exe process appears related to an IRC (Internet Relay Chat) application, which can be used by bad actors to communicate with compromised machines or control botnets. (Gates, 2007) (ScienceDirect, n.d.) (Steendijk, 2002)

We also have an iroffer.exe process which is another IRC file-sharing process, potentially supporting malicious file distribution or coordinating with other malicious processes. We have poisonivy.exe as well, which should raise serious concerns as it is a well-known RAT (remote access trojan) that grants an attacker remote control over a system. We also found winvnc4.exe, a VNC service that is often used for remote desktop control and can suggest unauthorized or malicious access. These processes are concerning as they indicate active command and control components as well as the potential for data theft and further system manipulation. ("dinoex", 2024) (Trend Micro, 2012)

Hidden Abnormalities

To be certain that we have the full picture we also run *volatility -f KobayashiMaru.vmem –profile=WinXPSP2x86 psxview* to view processes that were actively trying to hide, which does reveal some processes trying to be under the radar. We find processes svchost.exe, and explorer.exe which are typical in Windows systems. Because we know we have a process, Hacker Defender, running we must make note of these potentially malicious processes and their PIDs for further investigation as if they are not being run from directories they should be running from, would be a big indication that they are malicious. (see reference Appendix 3: Volatility psxview)

Furthermore, using *volatility -f KobayashiMaru.vmem –profile=WinXPSP2x82 connscan* I scan connections just out of curiosity, and see some coordinated malicious activities between iroffer.exe, bircd.exe, and poisonivy.exe. The former two processes seem to be bypassing any sort of external monitoring systems by communicating with one another internally. Then we have poisonivy.exe confirmed as communicating with an external IP address, so we do have an active backdoor on the machine. (see reference Appendix 4: Volatility connscan)

Accounts

Next, I will see if we are able to find any account names and details. Using *volatility -f KobayashiMaru.vmem ---profile=WinXPSP2x86 hashlist* was not successful. From there I decided to dive a little deeper for a bit and ran *volatility -f KobayashiMaru.vmem –profile=WinXPSP2x86 filescan > filescan_output.txt* and then *grep* for "config" in the new text file. (see reference Appendix 5: Volatility filescan & config grep)

With our new offset values of the system file and SAM file, we confirmed that they were corrupted by the various malicious processes and no accounts were recovered with our *hashdump* or *lsadump* commands from volatility, with *hashdump* returning nothing and our *lsadump* returning a "Unable to read LSA secrets from registry" error.

DLLs, Associated Processes, and Pathways

Next to look at the DLLs (Dynamically Linked Libraries) I use the *volatility -f KobayashiMaru.vmem ---profile=WinXPSP2x86 dlllist* command, followed immediately by the same command again after the amount of output was a lot, but into a text file for easier viewability and searching. My greping isn't fully up to snuff, so I decide to just open the text file and search within the text file itself. The PIDs I was interested and start searching for (not in a particular order):

winlogon.exe 688

various svchost.exe 916, 960, 1028, 1108

hxdef100.exe 1416

cryptcat.exe 1472

bircd.exe 1480

various iroffer.exe 1692, 1728, 1824

explorer.exe 404

poisonivy.exe 480

nc.exe 532 and winvnc4.exe 548

Some PIDS from the psxview list I want to investigate make this list above, and I highlight above to note that they were processes trying to remain hidden from the system. As I begin to go through the items one by one, most typical processes are just as they seem – typical, but with Hacker Defender and poisonivy on the system we know we do have some items of interest to investigate at the very least.

Hacker Defender

We find several DLLs being used by Hacker Defender, but they all reside in the legitimate *C:\Windows\System32* directory. While the DLLs are standard for windows processes, if we were not already aware that Hacker Defender was what it is, its executable running from the non-standard path of *C:\hxdefrootkit\* speaks volumes alone, not to mention the not so subtle 'rootkit' port of its name. The command line also references a config file, hxdef100.ini. (see reference Appendix 6: Hacker Defender)

Cryptcat

Several DLLs from standard windows processes are being used with Cryptcat as well. It was initially questionable if Cryptcat was being used for malicious purposes, but now seeing that it runs from the directory that Hacker Defender resides in it is confirmed malicious. Furthermore, it accesses a DLL located in the *C:\WINDOWS\WinSxS* which is a legitimate folder that can be abused by malware to mask their presence, and have legitimate files bundled with malicious file in the location. The command line tells it to listen on port 666, and to execute a windows command prompt to establish a remote shell access to the machine. (Security Joes, n.d.) (see reference Appendix 7: Cryptcat)

Beware IRCD

We find many standard windows DLLs again, and the executable running from a *C:\hidden* which is suspicious. I feel that with the communications between Beware and iroffer.exe earlier and this strongly suggests that the device was likely compromised and is now part of a botnet. (see reference Appendix 8: Beware IRCD)

IROFFER

The two iroffer.exe processes with PIDs 1692 and 1824 were unable to be read, but 1728 was an also in the suspicious *C:\hidden* directory. While using several common Windows DLLs, it also used two DLLs from its *hidden* directory, a cygcrypt-0.dll and a cygwin1.dll. Cygwin is an open-source Unix-like interface for Windows, offering a software repository and allowing the execution of non-Windows-native code. This machine is absolutely riddled with malware and back doors. (Sheldon, n.d.) (see reference Appendix 9: iroffer)

Poisonivy, Netcat, VNC4

Poisonivy is malware. Truly do not need to look at the DLLs to know that, but the executable runs from inside the *system32* directory which is of course suspicious. Otherwise, the DLLs are all common Windows processes, likely being accessed to alter or manipulate in some way. (Trend Micro, 2012) (see reference Appendix 10: Poisonivy)

Netcat is in a *C:\inetpub* directory, the command line has it listening on port 6666 and to execute the Windows command prompt upon connection, providing another remote shell access to the machine. A cmd.exe process is ongoing at time of the memory dump, with a command line of *C:\WINDOWS\system32\cmd.exe /K C:\Inetpub\ftproot\lock.bat* so it is likely a batch file to lock the system down and launch other malware. (Buckbee, 2022) (see reference Appendix 11: Netcat)

VNC4 is also in the *C:\inetpub* directory, makes use of common system32 and a WinSxS DLL, and otherwise seems to be a backup backdoor. (RealVNC, n.d.) (see reference Appendix 12: VNC4)

Other listed above processes were checked, and did not appear to run from strange pathways, access strange files, etc..

Conclusion

The system was compromised by many pieces of malware, including the rootkit, backdoors, and RATs. Hacker Defender was used to hide malicious processes, while tools like Poison Ivy and Netcat provided remote access to the system. The machine was likely part of a botnet, as it had malicious processes communicating internally and externally. The box is very much compromised, and the bad actors have full control over the machine. Assuming the device would be powered down, it needs to be spun back up offline, and few critical files recovered before a complete reimaging.

Bibliography

"dinoex". (2024, July 15). *iroffer-dinoex IRC "bot" that makes sharing files via DCC extremely easy*. Retrieved from freshports: https://www.freshports.org/irc/iroffer-dinoex/

Buckbee, M. (2022, June 9). *How to Use Netcat Commands: Examples and Cheat Sheets*. (Varonis) Retrieved from https://www.varonis.com/blog/netcat-commands

Gates, C. (2007, n.d. n.d.). *HackerDefender*. Retrieved from carnal0wnage: http://www.carnal0wnage.com/papers/rootkit_for_the_masses.pdf

Microsoft. (2021, January 7). *Physical Address Extension*. Retrieved from Microsoft Learn: https://learn.microsoft.com/en-us/windows/win32/memory/physical-address-extension

RealVNC. (n.d., n.d. n.d.). *RealVNC Connect*. Retrieved from RealVNC: https://www.realvnc.com/en/connect/

ScienceDirect. (n.d., n.d. n.d.). *Cryptcat*. Retrieved from ScienceDirect: https://www.sciencedirect.com/topics/computer-science/cryptcat

Security Joes. (n.d., January 1). *Hide and Seek in Windows' Closet: Unmasking the WinSxS Hijacking Hideout*. Retrieved from SecurityJoes: https://www.securityjoes.com/post/hide-and-seek-in-windows-closet-unmasking-the-winsxs-hijacking-hideout

Sheldon, R. (n.d., n.d. n.d.). *What is Cygwin?* Retrieved from techtarget: https://www.techtarget.com/searchdatacenter/definition/Cygwin

Steendijk, B. (2002, n.d. n.d.). *information about using beware ircd*. Retrieved from ircd.bircd: https://ircd.bircd.org/manual.html

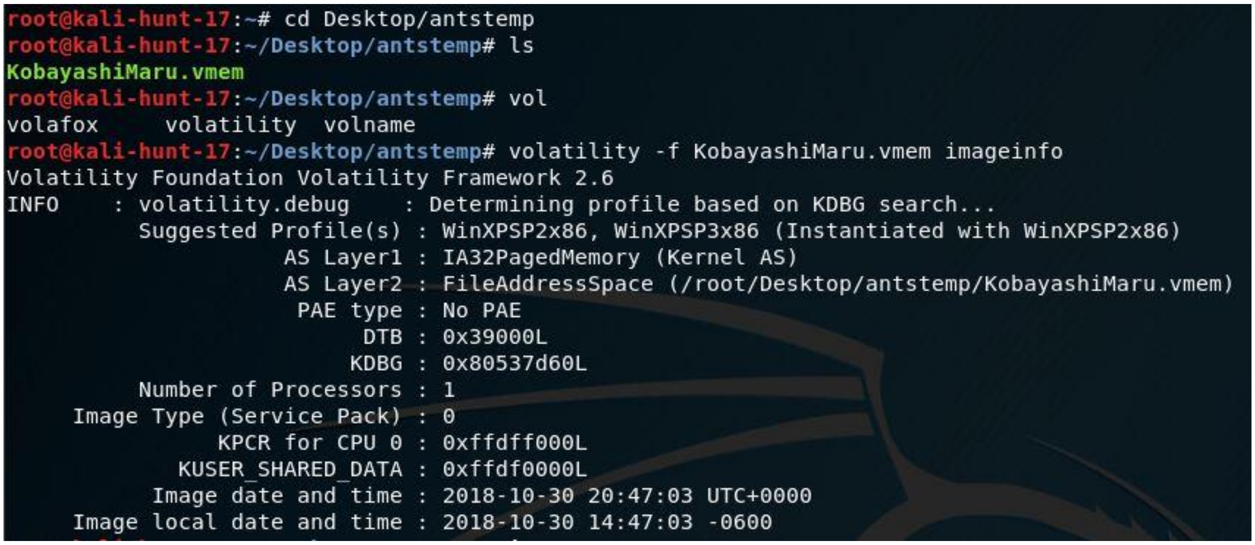
Trend Micro. (2012, October 9). *POISONIVY*. Retrieved from Trendmicro: https://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/poisonivy

"Professor K". (2020, November 18). *Memory Forensics Using the Volatility Framework*. Retrieved from Youtube: https://www.youtube.com/watch?v=4lURQHslmMc

"Volatility Foundation". (2016, December n.d.) *Volatility*. Retrieved from github: https://github.com/volatilityfoundation/volatility

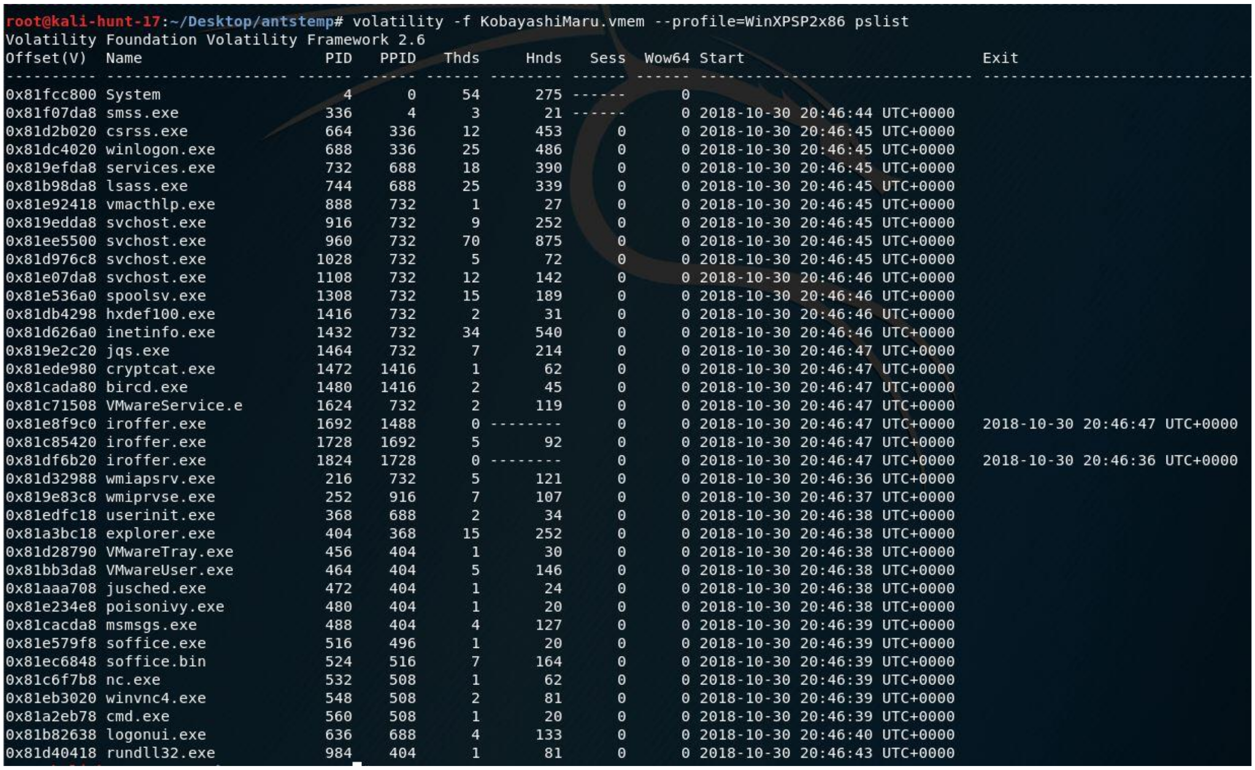
Appendices

Appendix 1: Volatility imageinfo



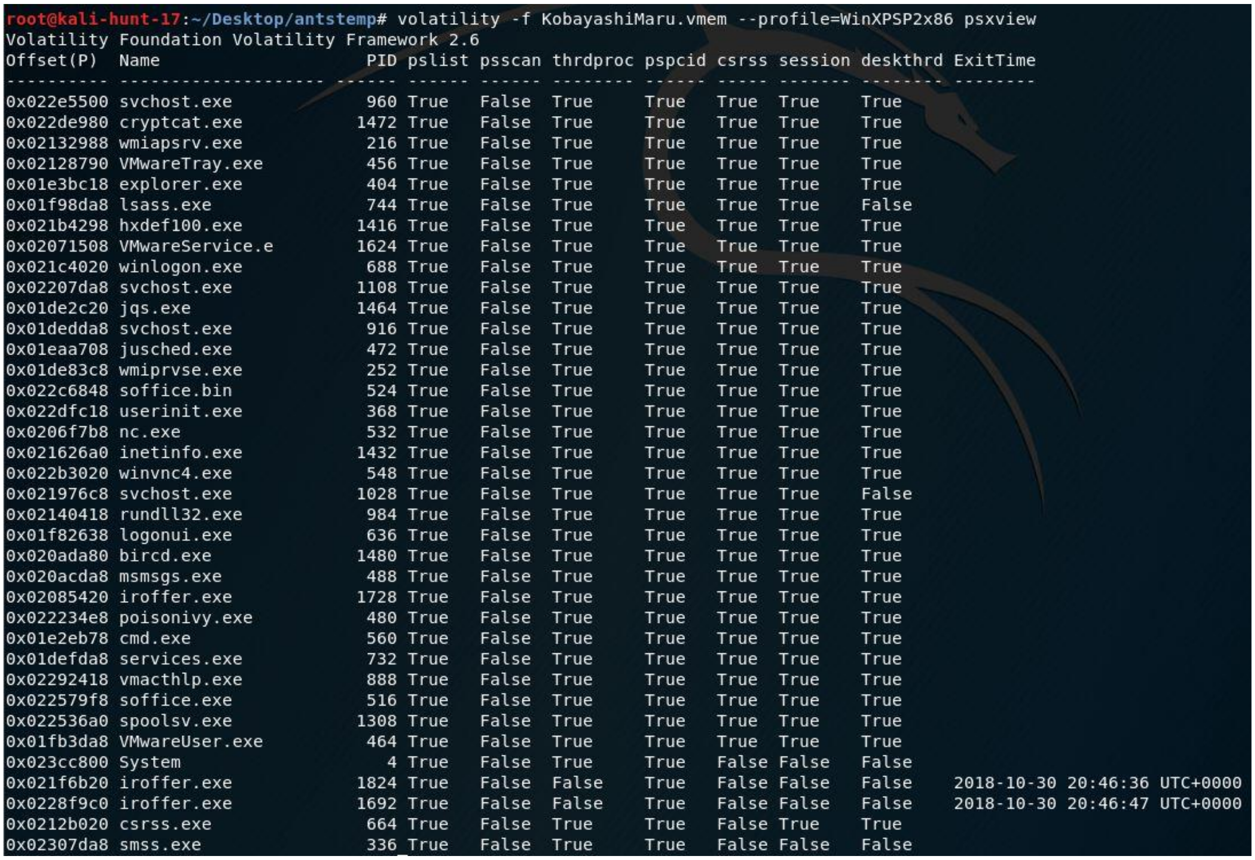
```
root@kali-hunt-17:~# cd Desktop/antstemp
root@kali-hunt-17:~/Desktop/antstemp# ls
KobayashiMaru.vmem
root@kali-hunt-17:~/Desktop/antstemp# vol
volafox     volatility  volname
root@kali-hunt-17:~/Desktop/antstemp# volatility -f KobayashiMaru.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/root/Desktop/antstemp/KobayashiMaru.vmem)
                      PAE type : No PAE
                           DTB : 0x39000L
                          KDBG : 0x80537d60L
          Number of Processors : 1
     Image Type (Service Pack) : 0
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2018-10-30 20:47:03 UTC+0000
     Image local date and time : 2018-10-30 14:47:03 -0600
```

Appendix 2: Volatility pslist



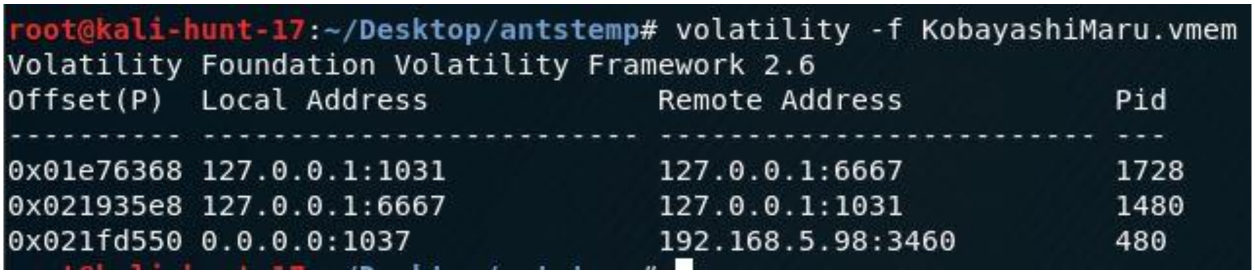
```
root@kali-hunt-17:~/Desktop/antstemp# volatility -f KobayashiMaru.vmem --profile=WinXPSP2x86 pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x81fcc800 System                    4      0     54      275 ------      0
0x81f07da8 smss.exe                336      4      3       21 ------      0 2018-10-30 20:46:44 UTC+0000
0x81d2b020 csrss.exe               664    336     12      453      0      0 2018-10-30 20:46:45 UTC+0000
0x81dc4020 winlogon.exe            688    336     25      486      0      0 2018-10-30 20:46:45 UTC+0000
0x819efda8 services.exe            732    688     18      390      0      0 2018-10-30 20:46:45 UTC+0000
0x81b98da8 lsass.exe               744    688     25      339      0      0 2018-10-30 20:46:45 UTC+0000
0x81e92418 vmacthlp.exe            888    732      1       27      0      0 2018-10-30 20:46:45 UTC+0000
0x819edda8 svchost.exe             916    732      9      252      0      0 2018-10-30 20:46:45 UTC+0000
0x81ee5500 svchost.exe             960    732     70      875      0      0 2018-10-30 20:46:45 UTC+0000
0x81d976c8 svchost.exe            1028    732      5       72      0      0 2018-10-30 20:46:45 UTC+0000
0x81e07da8 svchost.exe            1108    732     12      142      0      0 2018-10-30 20:46:46 UTC+0000
0x81e536a0 spoolsv.exe            1308    732     15      189      0      0 2018-10-30 20:46:46 UTC+0000
0x81db4298 hxdef100.exe           1416    732      2       31      0      0 2018-10-30 20:46:46 UTC+0000
0x81d626a0 inetinfo.exe           1432    732     34      540      0      0 2018-10-30 20:46:46 UTC+0000
0x819e2c20 jqs.exe                1464    732      7      214      0      0 2018-10-30 20:46:47 UTC+0000
0x81ede980 cryptcat.exe           1472   1416      1       62      0      0 2018-10-30 20:46:47 UTC+0000
0x81cada80 bircd.exe              1480   1416      2       45      0      0 2018-10-30 20:46:47 UTC+0000
0x81c71508 VMwareService.e        1624    732      2      119      0      0 2018-10-30 20:46:47 UTC+0000
0x81e8f9c0 iroffer.exe            1692   1488      0 --------      0      0 2018-10-30 20:46:47 UTC+0000   2018-10-30 20:46:47 UTC+0000
0x81c85420 iroffer.exe            1728   1692      5       92      0      0 2018-10-30 20:46:47 UTC+0000
0x81df6b20 iroffer.exe            1824   1728      0 --------      0      0 2018-10-30 20:46:47 UTC+0000   2018-10-30 20:46:36 UTC+0000
0x81d32988 wmiapsrv.exe            216    732      5      121      0      0 2018-10-30 20:46:36 UTC+0000
0x819e83c8 wmiprvse.exe            252    916      7      107      0      0 2018-10-30 20:46:37 UTC+0000
0x81edfc18 userinit.exe            368    688      2       34      0      0 2018-10-30 20:46:38 UTC+0000
0x81a3bc18 explorer.exe            404    368     15      252      0      0 2018-10-30 20:46:38 UTC+0000
0x81d28790 VMwareTray.exe          456    404      1       30      0      0 2018-10-30 20:46:38 UTC+0000
0x81bb3da8 VMwareUser.exe          464    404      5      146      0      0 2018-10-30 20:46:38 UTC+0000
0x81aaa708 jusched.exe             472    404      1       24      0      0 2018-10-30 20:46:38 UTC+0000
0x81e234e8 poisonivy.exe           480    404      1       20      0      0 2018-10-30 20:46:38 UTC+0000
0x81cacda8 msmsgs.exe              488    404      4      127      0      0 2018-10-30 20:46:39 UTC+0000
0x81e579f8 soffice.exe             516    496      1       20      0      0 2018-10-30 20:46:39 UTC+0000
0x81ec6848 soffice.bin             524    516      7      164      0      0 2018-10-30 20:46:39 UTC+0000
0x81c6f7b8 nc.exe                  532    508      1       62      0      0 2018-10-30 20:46:39 UTC+0000
0x81eb3020 winvnc4.exe             548    508      2       81      0      0 2018-10-30 20:46:39 UTC+0000
0x81a2eb78 cmd.exe                 560    508      1       20      0      0 2018-10-30 20:46:39 UTC+0000
0x81b82638 logonui.exe             636    688      4      133      0      0 2018-10-30 20:46:40 UTC+0000
0x81d40418 rundll32.exe            984    404      1       81      0      0 2018-10-30 20:46:43 UTC+0000
```

Appendix 3: Volatility psxview



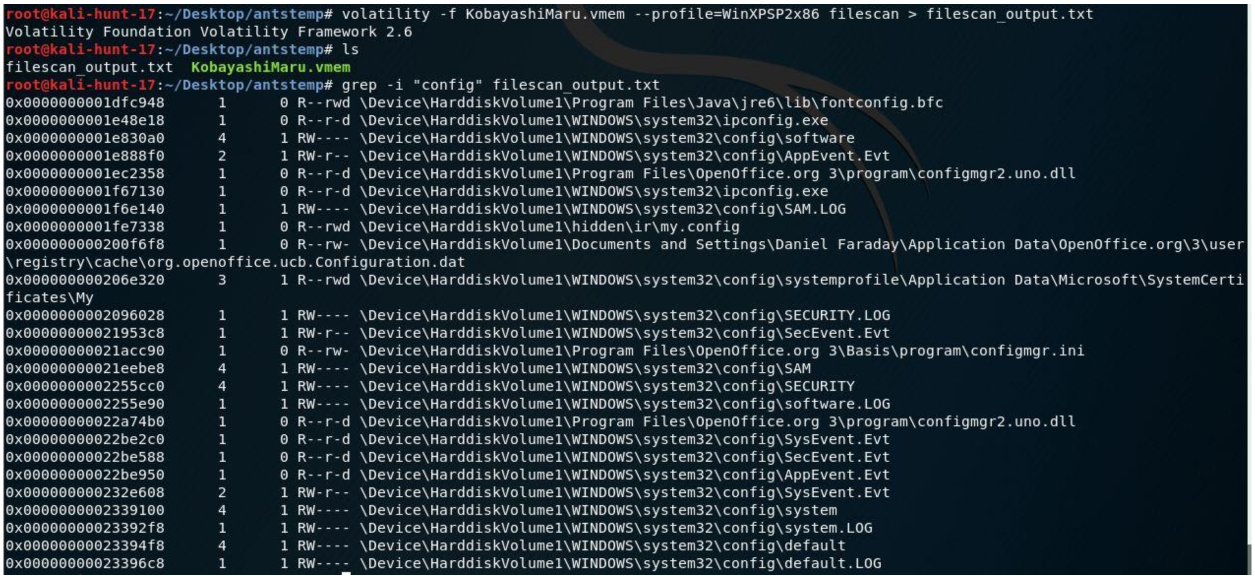
```
root@kali-hunt-17:~/Desktop/antstemp# volatility -f KobayashiMaru.vmem --profile=WinXPSP2x86 psxview
Volatility Foundation Volatility Framework 2.6
Offset(P)  Name                    PID pslist psscan thrdproc pspcid csrss session deskthrd ExitTime
---------- -------------------- ------ ------ ------ -------- ------ ----- ------- -------- --------
0x022e5500 svchost.exe             960 True   False  True     True   True  True    True
0x022de980 cryptcat.exe           1472 True   False  True     True   True  True    True
0x02132988 wmiapsrv.exe            216 True   False  True     True   True  True    True
0x02128790 VMwareTray.exe          456 True   False  True     True   True  True    True
0x01e3bc18 explorer.exe            404 True   False  True     True   True  True    True
0x01f98da8 lsass.exe               744 True   False  True     True   True  True    False
0x021b4298 hxdef100.exe           1416 True   False  True     True   True  True    True
0x02071508 VMwareService.e        1624 True   False  True     True   True  True    True
0x021c4020 winlogon.exe            688 True   False  True     True   True  True    True
0x02207da8 svchost.exe            1108 True   False  True     True   True  True    True
0x01de2c20 jqs.exe                1464 True   False  True     True   True  True    True
0x01dedda8 svchost.exe             916 True   False  True     True   True  True    True
0x01eaa708 jusched.exe             472 True   False  True     True   True  True    True
0x01de83c8 wmiprvse.exe            252 True   False  True     True   True  True    True
0x022c6848 soffice.bin             524 True   False  True     True   True  True    True
0x022dfc18 userinit.exe            368 True   False  True     True   True  True    True
0x0206f7b8 nc.exe                  532 True   False  True     True   True  True    True
0x021626a0 inetinfo.exe           1432 True   False  True     True   True  True    True
0x022b3020 winvnc4.exe             548 True   False  True     True   True  True    True
0x021976c8 svchost.exe            1028 True   False  True     True   True  True    False
0x02140418 rundll32.exe            984 True   False  True     True   True  True    True
0x01f82638 logonui.exe             636 True   False  True     True   True  True    True
0x020ada80 bircd.exe              1480 True   False  True     True   True  True    True
0x020acda8 msmsgs.exe              488 True   False  True     True   True  True    True
0x02085420 iroffer.exe            1728 True   False  True     True   True  True    True
0x022234e8 poisonivy.exe           480 True   False  True     True   True  True    True
0x01e2eb78 cmd.exe                 560 True   False  True     True   True  True    True
0x01defda8 services.exe            732 True   False  True     True   True  True    True
0x02292418 vmacthlp.exe            888 True   False  True     True   True  True    True
0x022579f8 soffice.exe             516 True   False  True     True   True  True    True
0x022536a0 spoolsv.exe            1308 True   False  True     True   True  True    True
0x01fb3da8 VMwareUser.exe          464 True   False  True     True   True  True    True
0x023cc800 System                    4 True   False  True     True   False False   False
0x021f6b20 iroffer.exe            1824 True   False  False    True   False False   False    2018-10-30 20:46:36 UTC+0000
0x0228f9c0 iroffer.exe            1692 True   False  False    True   False False   False    2018-10-30 20:46:47 UTC+0000
0x0212b020 csrss.exe               664 True   False  True     True   False True    True
0x02307da8 smss.exe                336 True   False  True     True   False False   False
```

Appendix 4: Volatility connscan



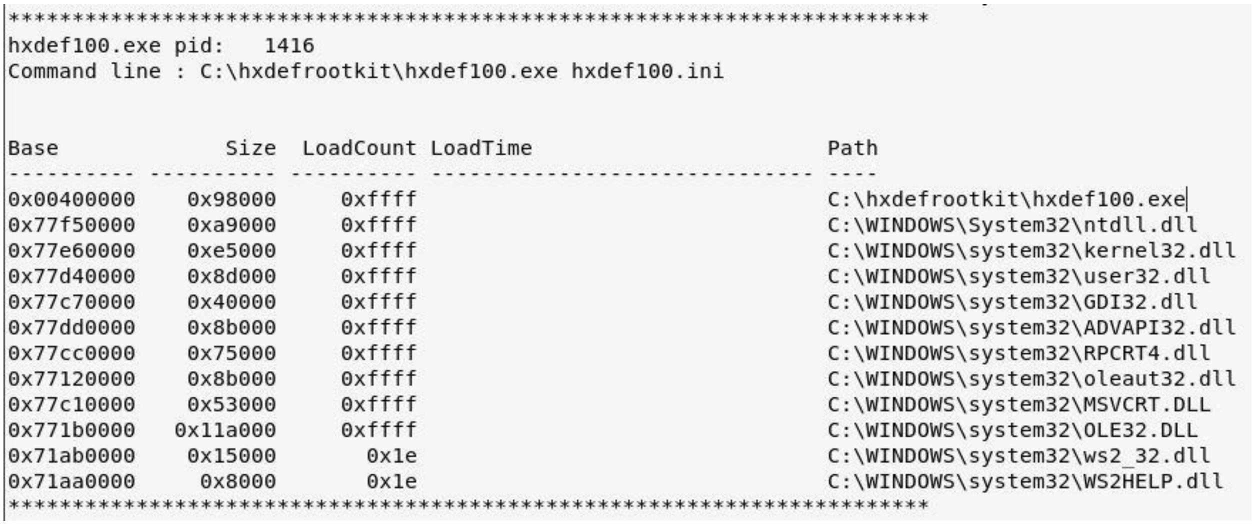
```
root@kali-hunt-17:~/Desktop/antstemp# volatility -f KobayashiMaru.vmem
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0x01e76368 127.0.0.1:1031            127.0.0.1:6667            1728
0x021935e8 127.0.0.1:6667            127.0.0.1:1031            1480
0x021fd550 0.0.0.0:1037              192.168.5.98:3460         480
```

Appendix 5: Volatility filescan & config grep



```
root@kali-hunt-17:~/Desktop/antstemp# volatility -f KobayashiMaru.vmem --profile=WinXPSP2x86 filescan > filescan_output.txt
Volatility Foundation Volatility Framework 2.6
root@kali-hunt-17:~/Desktop/antstemp# ls
filescan_output.txt  KobayashiMaru.vmem
root@kali-hunt-17:~/Desktop/antstemp# grep -i "config" filescan_output.txt
0x0000000001dfc948      1      0 R--rwd \Device\HarddiskVolume1\Program Files\Java\jre6\lib\fontconfig.bfc
0x0000000001e48e18      1      0 R--r-d \Device\HarddiskVolume1\WINDOWS\system32\ipconfig.exe
0x0000000001e830a0      4      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\software
0x0000000001e888f0      2      1 RW-r-- \Device\HarddiskVolume1\WINDOWS\system32\config\AppEvent.Evt
0x0000000001ec2358      1      0 R--r-d \Device\HarddiskVolume1\Program Files\OpenOffice.org 3\program\configmgr2.uno.dll
0x0000000001f67130      1      0 R--r-d \Device\HarddiskVolume1\WINDOWS\system32\ipconfig.exe
0x0000000001f6e140      1      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\SAM.LOG
0x0000000001fe7338      1      0 R--rwd \Device\HarddiskVolume1\hidden\ir\my.config
0x000000000200f6f8      1      0 R--rw- \Device\HarddiskVolume1\Documents and Settings\Daniel Faraday\Application Data\OpenOffice.org\3\user
\registry\cache\org.openoffice.ucb.Configuration.dat
0x000000000206e320      3      1 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\config\systemprofile\Application Data\Microsoft\SystemCerti
ficates\My
0x0000000002096028      1      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY.LOG
0x00000000021953c8      1      1 RW-r-- \Device\HarddiskVolume1\WINDOWS\system32\config\SecEvent.Evt
0x00000000021acc90      1      0 R--rw- \Device\HarddiskVolume1\Program Files\OpenOffice.org 3\Basis\program\configmgr.ini
0x00000000021eebe8      4      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
0x0000000002255cc0      4      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
0x0000000002255e90      1      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\software.LOG
0x00000000022a74b0      1      0 R--r-d \Device\HarddiskVolume1\Program Files\OpenOffice.org 3\program\configmgr2.uno.dll
0x00000000022be2c0      1      0 R--r-d \Device\HarddiskVolume1\WINDOWS\system32\config\SysEvent.Evt
0x00000000022be588      1      0 R--r-d \Device\HarddiskVolume1\WINDOWS\system32\config\SecEvent.Evt
0x00000000022be950      1      0 R--r-d \Device\HarddiskVolume1\WINDOWS\system32\config\AppEvent.Evt
0x000000000232e608      2      1 RW-r-- \Device\HarddiskVolume1\WINDOWS\system32\config\SysEvent.Evt
0x0000000002339100      4      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\system
0x00000000023392f8      1      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\system.LOG
0x00000000023394f8      4      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\default
0x00000000023396c8      1      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\default.LOG
```

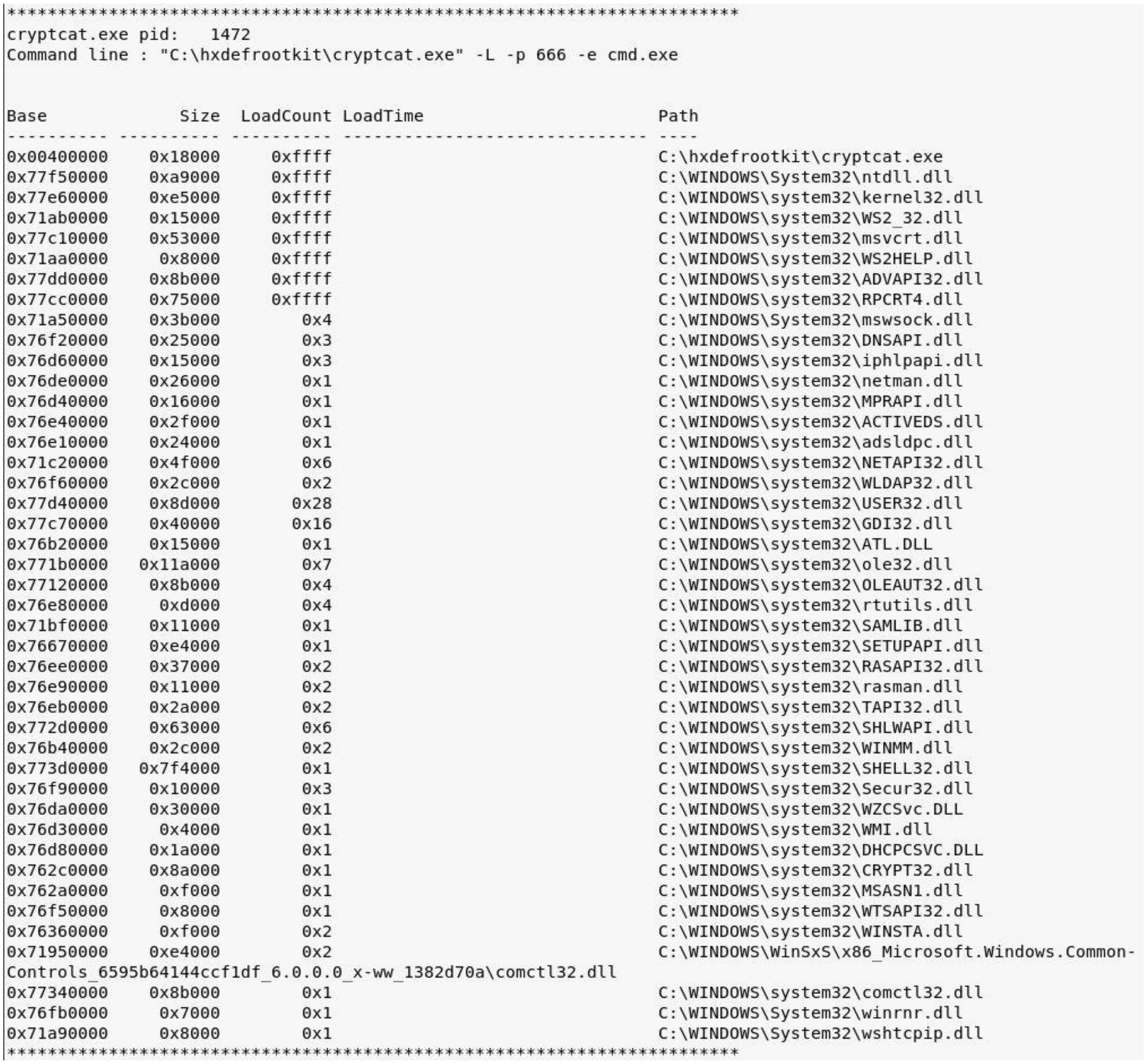
Appendix 6: Hacker Defender



```
************************************************************************
hxdef100.exe pid:   1416
Command line : C:\hxdefrootkit\hxdef100.exe hxdef100.ini


Base             Size  LoadCount LoadTime                       Path
---------- ---------- ---------- ------------------------------ ----
0x00400000    0x98000     0xffff                                C:\hxdefrootkit\hxdef100.exe
0x77f50000    0xa9000     0xffff                                C:\WINDOWS\System32\ntdll.dll
0x77e60000    0xe5000     0xffff                                C:\WINDOWS\system32\kernel32.dll
0x77d40000    0x8d000     0xffff                                C:\WINDOWS\system32\user32.dll
0x77c70000    0x40000     0xffff                                C:\WINDOWS\system32\GDI32.dll
0x77dd0000    0x8b000     0xffff                                C:\WINDOWS\system32\ADVAPI32.dll
0x77cc0000    0x75000     0xffff                                C:\WINDOWS\system32\RPCRT4.dll
0x77120000    0x8b000     0xffff                                C:\WINDOWS\system32\oleaut32.dll
0x77c10000    0x53000     0xffff                                C:\WINDOWS\system32\MSVCRT.DLL
0x771b0000   0x11a000     0xffff                                C:\WINDOWS\system32\OLE32.DLL
0x71ab0000    0x15000       0x1e                                C:\WINDOWS\system32\ws2_32.dll
0x71aa0000     0x8000       0x1e                                C:\WINDOWS\system32\WS2HELP.dll
************************************************************************
```

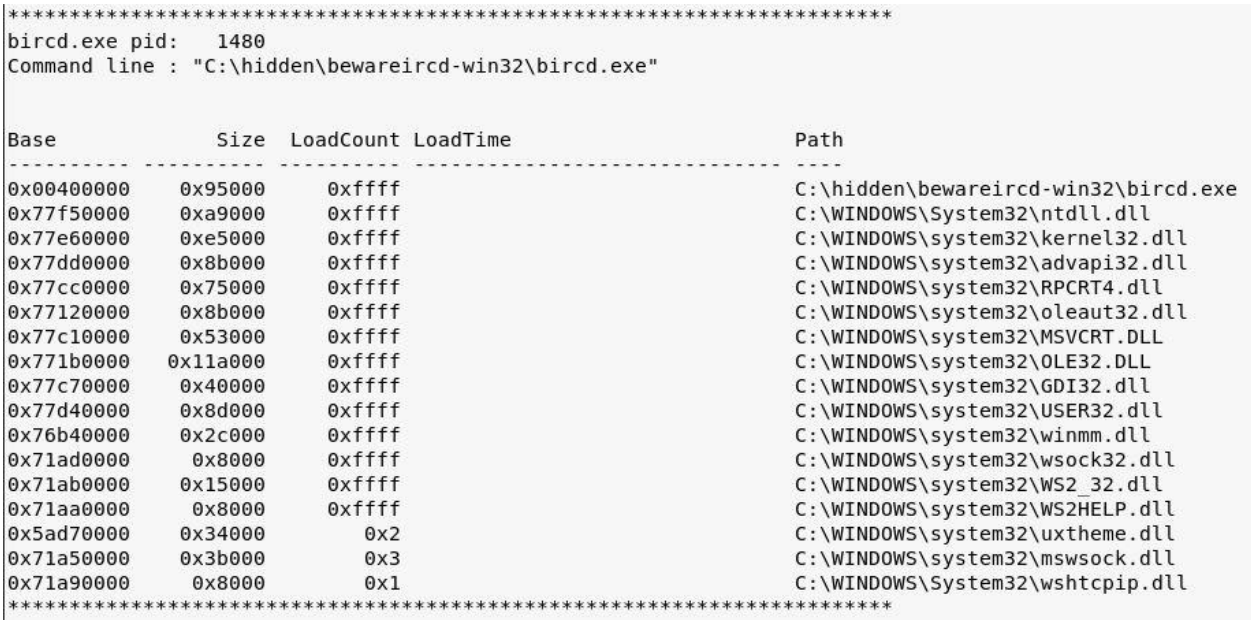
Appendix 7: Cryptcat



```
************************************************************************
cryptcat.exe pid:   1472
Command line : "C:\hxdefrootkit\cryptcat.exe" -L -p 666 -e cmd.exe


Base             Size  LoadCount LoadTime                       Path
---------- ---------- ---------- ------------------------------ ----
0x00400000    0x18000     0xffff                                C:\hxdefrootkit\cryptcat.exe
0x77f50000    0xa9000     0xffff                                C:\WINDOWS\System32\ntdll.dll
0x77e60000    0xe5000     0xffff                                C:\WINDOWS\system32\kernel32.dll
0x71ab0000    0x15000     0xffff                                C:\WINDOWS\system32\WS2_32.dll
0x77c10000    0x53000     0xffff                                C:\WINDOWS\system32\msvcrt.dll
0x71aa0000     0x8000     0xffff                                C:\WINDOWS\system32\WS2HELP.dll
0x77dd0000    0x8b000     0xffff                                C:\WINDOWS\system32\ADVAPI32.dll
0x77cc0000    0x75000     0xffff                                C:\WINDOWS\system32\RPCRT4.dll
0x71a50000    0x3b000        0x4                                C:\WINDOWS\System32\mswsock.dll
0x76f20000    0x25000        0x3                                C:\WINDOWS\system32\DNSAPI.dll
0x76d60000    0x15000        0x3                                C:\WINDOWS\system32\iphlpapi.dll
0x76de0000    0x26000        0x1                                C:\WINDOWS\system32\netman.dll
0x76d40000    0x16000        0x1                                C:\WINDOWS\system32\MPRAPI.dll
0x76e40000    0x2f000        0x1                                C:\WINDOWS\system32\ACTIVEDS.dll
0x76e10000    0x24000        0x1                                C:\WINDOWS\system32\adsldpc.dll
0x71c20000    0x4f000        0x6                                C:\WINDOWS\system32\NETAPI32.dll
0x76f60000    0x2c000        0x2                                C:\WINDOWS\system32\WLDAP32.dll
0x77d40000    0x8d000       0x28                                C:\WINDOWS\system32\USER32.dll
0x77c70000    0x40000       0x16                                C:\WINDOWS\system32\GDI32.dll
0x76b20000    0x15000        0x1                                C:\WINDOWS\system32\ATL.DLL
0x771b0000   0x11a000        0x7                                C:\WINDOWS\system32\ole32.dll
0x77120000    0x8b000        0x4                                C:\WINDOWS\system32\OLEAUT32.dll
0x76e80000     0xd000        0x4                                C:\WINDOWS\system32\rtutils.dll
0x71bf0000    0x11000        0x1                                C:\WINDOWS\system32\SAMLIB.dll
0x76670000    0xe4000        0x1                                C:\WINDOWS\system32\SETUPAPI.dll
0x76ee0000    0x37000        0x2                                C:\WINDOWS\system32\RASAPI32.dll
0x76e90000    0x11000        0x2                                C:\WINDOWS\system32\rasman.dll
0x76eb0000    0x2a000        0x2                                C:\WINDOWS\system32\TAPI32.dll
0x772d0000    0x63000        0x6                                C:\WINDOWS\system32\SHLWAPI.dll
0x76b40000    0x2c000        0x2                                C:\WINDOWS\system32\WINMM.dll
0x773d0000   0x7f4000        0x1                                C:\WINDOWS\system32\SHELL32.dll
0x76f90000    0x10000        0x3                                C:\WINDOWS\system32\Secur32.dll
0x76da0000    0x30000        0x1                                C:\WINDOWS\system32\WZCSvc.DLL
0x76d30000     0x4000        0x1                                C:\WINDOWS\system32\WMI.dll
0x76d80000    0x1a000        0x1                                C:\WINDOWS\system32\DHCPCSVC.DLL
0x762c0000    0x8a000        0x1                                C:\WINDOWS\system32\CRYPT32.dll
0x762a0000     0xf000        0x1                                C:\WINDOWS\system32\MSASN1.dll
0x76f50000     0x8000        0x1                                C:\WINDOWS\system32\WTSAPI32.dll
0x76360000     0xf000        0x2                                C:\WINDOWS\system32\WINSTA.dll
0x71950000    0xe4000        0x2                                C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.0.0_x-ww_1382d70a\comctl32.dll
0x77340000    0x8b000        0x1                                C:\WINDOWS\system32\comctl32.dll
0x76fb0000     0x7000        0x1                                C:\WINDOWS\System32\winrnr.dll
0x71a90000     0x8000        0x1                                C:\WINDOWS\System32\wshtcpip.dll
************************************************************************
```

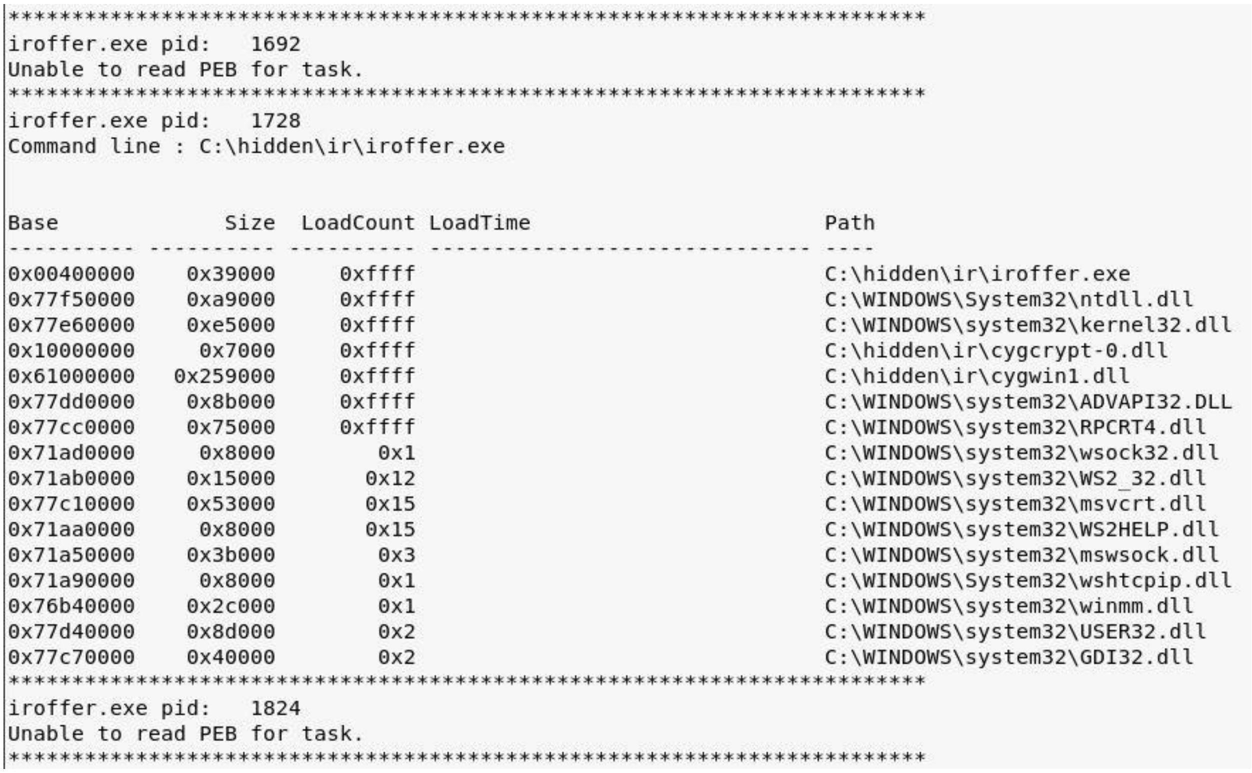
Appendix 8: Beware IRCD



```
************************************************************************
bircd.exe pid:   1480
Command line : "C:\hidden\bewareircd-win32\bircd.exe"


Base             Size  LoadCount LoadTime                       Path
---------- ---------- ---------- ------------------------------ ----
0x00400000    0x95000     0xffff                                C:\hidden\bewareircd-win32\bircd.exe
0x77f50000    0xa9000     0xffff                                C:\WINDOWS\System32\ntdll.dll
0x77e60000    0xe5000     0xffff                                C:\WINDOWS\system32\kernel32.dll
0x77dd0000    0x8b000     0xffff                                C:\WINDOWS\system32\advapi32.dll
0x77cc0000    0x75000     0xffff                                C:\WINDOWS\system32\RPCRT4.dll
0x77120000    0x8b000     0xffff                                C:\WINDOWS\system32\oleaut32.dll
0x77c10000    0x53000     0xffff                                C:\WINDOWS\system32\MSVCRT.DLL
0x771b0000   0x11a000     0xffff                                C:\WINDOWS\system32\OLE32.DLL
0x77c70000    0x40000     0xffff                                C:\WINDOWS\system32\GDI32.dll
0x77d40000    0x8d000     0xffff                                C:\WINDOWS\system32\USER32.dll
0x76b40000    0x2c000     0xffff                                C:\WINDOWS\system32\winmm.dll
0x71ad0000     0x8000     0xffff                                C:\WINDOWS\system32\wsock32.dll
0x71ab0000    0x15000     0xffff                                C:\WINDOWS\system32\WS2_32.dll
0x71aa0000     0x8000     0xffff                                C:\WINDOWS\system32\WS2HELP.dll
0x5ad70000    0x34000        0x2                                C:\WINDOWS\system32\uxtheme.dll
0x71a50000    0x3b000        0x3                                C:\WINDOWS\system32\mswsock.dll
0x71a90000     0x8000        0x1                                C:\WINDOWS\System32\wshtcpip.dll
************************************************************************
```

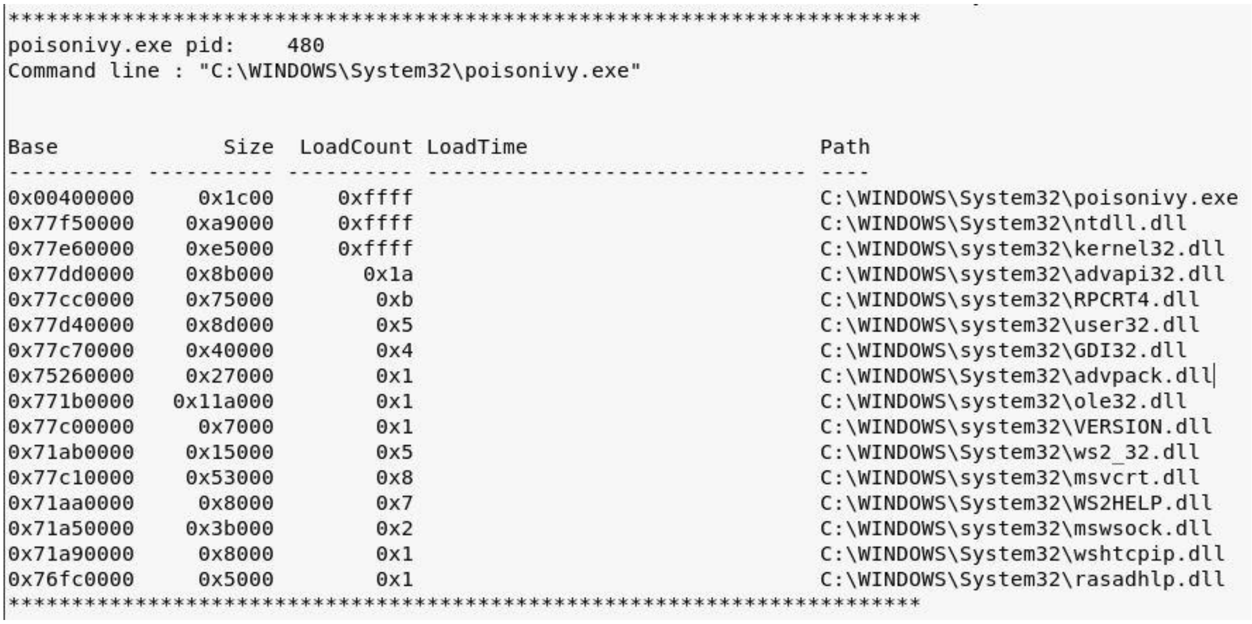
Appendix 9: iroffer



```
************************************************************************
iroffer.exe pid:   1692
Unable to read PEB for task.
************************************************************************
iroffer.exe pid:   1728
Command line : C:\hidden\ir\iroffer.exe


Base             Size  LoadCount LoadTime                       Path
---------- ---------- ---------- ------------------------------ ----
0x00400000    0x39000     0xffff                                C:\hidden\ir\iroffer.exe
0x77f50000    0xa9000     0xffff                                C:\WINDOWS\System32\ntdll.dll
0x77e60000    0xe5000     0xffff                                C:\WINDOWS\system32\kernel32.dll
0x10000000     0x7000     0xffff                                C:\hidden\ir\cygcrypt-0.dll
0x61000000   0x259000     0xffff                                C:\hidden\ir\cygwin1.dll
0x77dd0000    0x8b000     0xffff                                C:\WINDOWS\system32\ADVAPI32.DLL
0x77cc0000    0x75000     0xffff                                C:\WINDOWS\system32\RPCRT4.dll
0x71ad0000     0x8000        0x1                                C:\WINDOWS\system32\wsock32.dll
0x71ab0000    0x15000       0x12                                C:\WINDOWS\system32\WS2_32.dll
0x77c10000    0x53000       0x15                                C:\WINDOWS\system32\msvcrt.dll
0x71aa0000     0x8000       0x15                                C:\WINDOWS\system32\WS2HELP.dll
0x71a50000    0x3b000        0x3                                C:\WINDOWS\system32\mswsock.dll
0x71a90000     0x8000        0x1                                C:\WINDOWS\System32\wshtcpip.dll
0x76b40000    0x2c000        0x1                                C:\WINDOWS\system32\winmm.dll
0x77d40000    0x8d000        0x2                                C:\WINDOWS\system32\USER32.dll
0x77c70000    0x40000        0x2                                C:\WINDOWS\system32\GDI32.dll
************************************************************************
iroffer.exe pid:   1824
Unable to read PEB for task.
************************************************************************
```

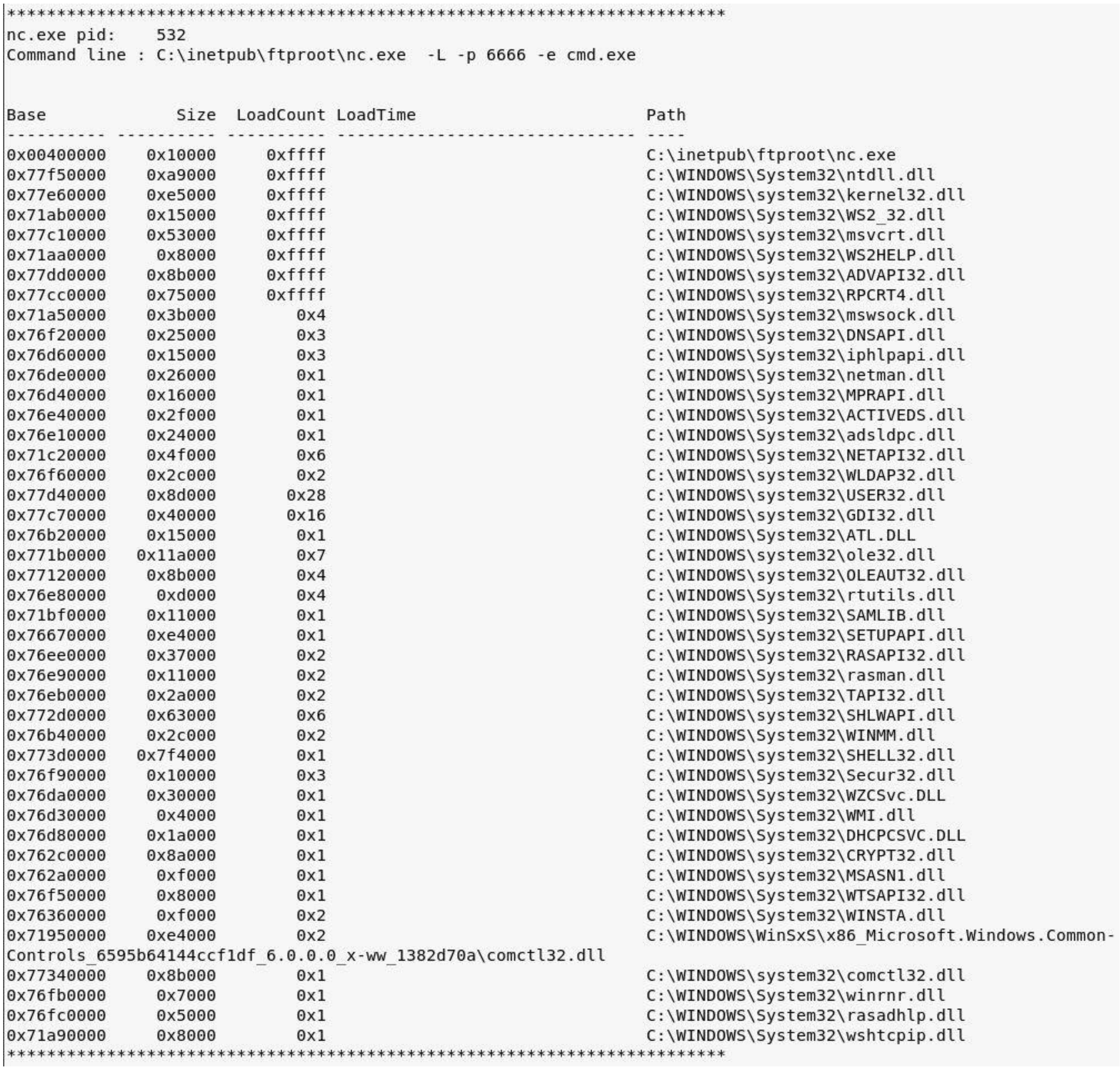
Appendix 10: Poisonivy



```
************************************************************************
poisonivy.exe pid:    480
Command line : "C:\WINDOWS\System32\poisonivy.exe"


Base             Size  LoadCount LoadTime                       Path
---------- ---------- ---------- ------------------------------ ----
0x00400000     0x1c00     0xffff                                C:\WINDOWS\System32\poisonivy.exe
0x77f50000    0xa9000     0xffff                                C:\WINDOWS\System32\ntdll.dll
0x77e60000    0xe5000     0xffff                                C:\WINDOWS\system32\kernel32.dll
0x77dd0000    0x8b000       0x1a                                C:\WINDOWS\system32\advapi32.dll
0x77cc0000    0x75000        0xb                                C:\WINDOWS\system32\RPCRT4.dll
0x77d40000    0x8d000        0x5                                C:\WINDOWS\system32\user32.dll
0x77c70000    0x40000        0x4                                C:\WINDOWS\system32\GDI32.dll
0x75260000    0x27000        0x1                                C:\WINDOWS\System32\advpack.dll
0x771b0000   0x11a000        0x1                                C:\WINDOWS\system32\ole32.dll
0x77c00000     0x7000        0x1                                C:\WINDOWS\system32\VERSION.dll
0x71ab0000    0x15000        0x5                                C:\WINDOWS\System32\ws2_32.dll
0x77c10000    0x53000        0x8                                C:\WINDOWS\system32\msvcrt.dll
0x71aa0000     0x8000        0x7                                C:\WINDOWS\System32\WS2HELP.dll
0x71a50000    0x3b000        0x2                                C:\WINDOWS\system32\mswsock.dll
0x71a90000     0x8000        0x1                                C:\WINDOWS\System32\wshtcpip.dll
0x76fc0000     0x5000        0x1                                C:\WINDOWS\System32\rasadhlp.dll
************************************************************************
```

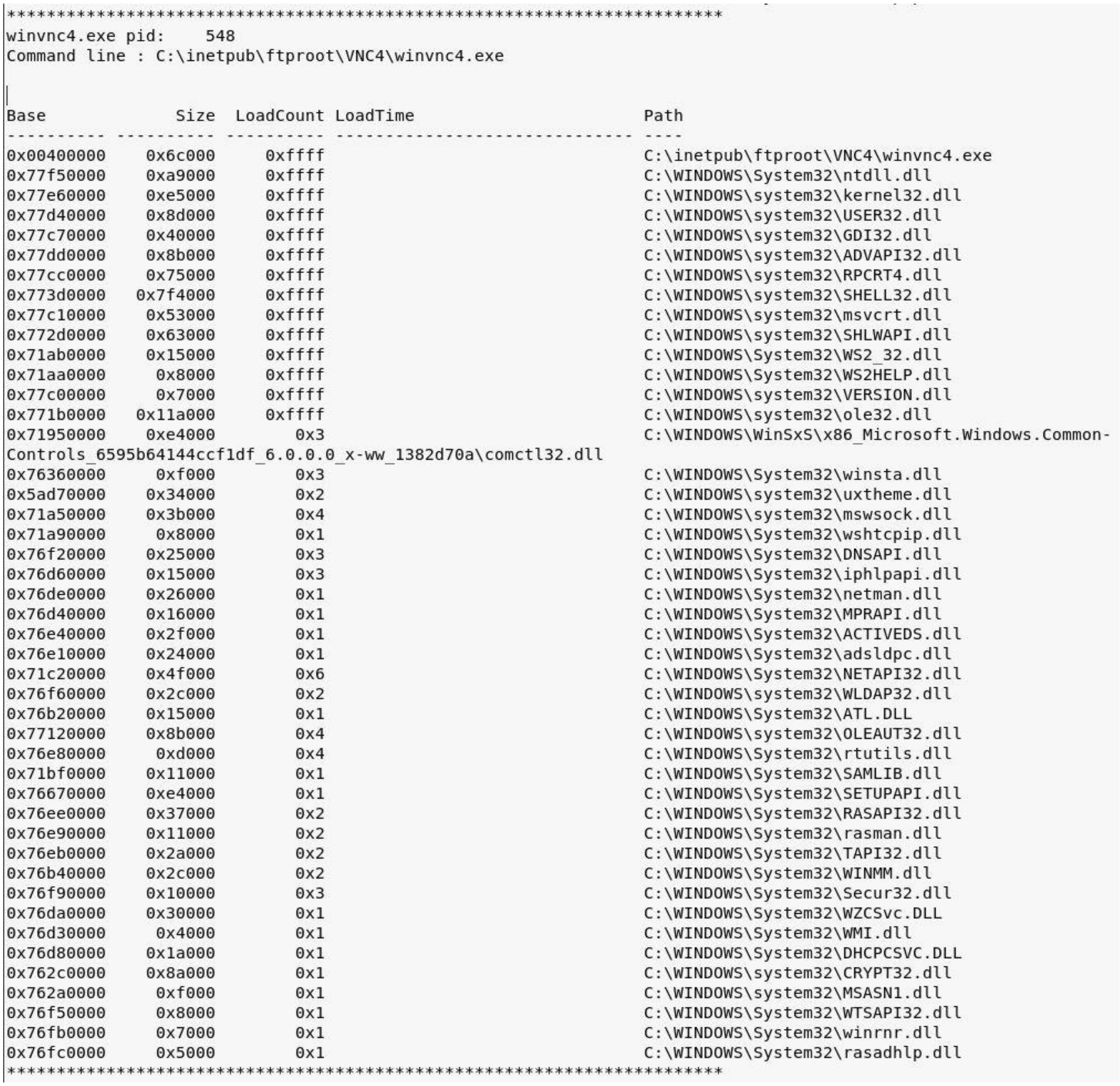
Appendix 11: Netcat



```
************************************************************************
nc.exe pid:    532
Command line : C:\inetpub\ftproot\nc.exe  -L -p 6666 -e cmd.exe


Base             Size  LoadCount LoadTime                       Path
---------- ---------- ---------- ------------------------------ ----
0x00400000    0x10000     0xffff                                C:\inetpub\ftproot\nc.exe
0x77f50000    0xa9000     0xffff                                C:\WINDOWS\System32\ntdll.dll
0x77e60000    0xe5000     0xffff                                C:\WINDOWS\system32\kernel32.dll
0x71ab0000    0x15000     0xffff                                C:\WINDOWS\System32\WS2_32.dll
0x77c10000    0x53000     0xffff                                C:\WINDOWS\system32\msvcrt.dll
0x71aa0000     0x8000     0xffff                                C:\WINDOWS\System32\WS2HELP.dll
0x77dd0000    0x8b000     0xffff                                C:\WINDOWS\system32\ADVAPI32.dll
0x77cc0000    0x75000     0xffff                                C:\WINDOWS\system32\RPCRT4.dll
0x71a50000    0x3b000        0x4                                C:\WINDOWS\System32\mswsock.dll
0x76f20000    0x25000        0x3                                C:\WINDOWS\System32\DNSAPI.dll
0x76d60000    0x15000        0x3                                C:\WINDOWS\System32\iphlpapi.dll
0x76de0000    0x26000        0x1                                C:\WINDOWS\System32\netman.dll
0x76d40000    0x16000        0x1                                C:\WINDOWS\System32\MPRAPI.dll
0x76e40000    0x2f000        0x1                                C:\WINDOWS\System32\ACTIVEDS.dll
0x76e10000    0x24000        0x1                                C:\WINDOWS\System32\adsldpc.dll
0x71c20000    0x4f000        0x6                                C:\WINDOWS\System32\NETAPI32.dll
0x76f60000    0x2c000        0x2                                C:\WINDOWS\system32\WLDAP32.dll
0x77d40000    0x8d000       0x28                                C:\WINDOWS\system32\USER32.dll
0x77c70000    0x40000       0x16                                C:\WINDOWS\system32\GDI32.dll
0x76b20000    0x15000        0x1                                C:\WINDOWS\System32\ATL.DLL
0x771b0000   0x11a000        0x7                                C:\WINDOWS\system32\ole32.dll
0x77120000    0x8b000        0x4                                C:\WINDOWS\system32\OLEAUT32.dll
0x76e80000     0xd000        0x4                                C:\WINDOWS\System32\rtutils.dll
0x71bf0000    0x11000        0x1                                C:\WINDOWS\System32\SAMLIB.dll
0x76670000    0xe4000        0x1                                C:\WINDOWS\System32\SETUPAPI.dll
0x76ee0000    0x37000        0x2                                C:\WINDOWS\System32\RASAPI32.dll
0x76e90000    0x11000        0x2                                C:\WINDOWS\System32\rasman.dll
0x76eb0000    0x2a000        0x2                                C:\WINDOWS\System32\TAPI32.dll
0x772d0000    0x63000        0x6                                C:\WINDOWS\system32\SHLWAPI.dll
0x76b40000    0x2c000        0x2                                C:\WINDOWS\System32\WINMM.dll
0x773d0000   0x7f4000        0x1                                C:\WINDOWS\system32\SHELL32.dll
0x76f90000    0x10000        0x3                                C:\WINDOWS\System32\Secur32.dll
0x76da0000    0x30000        0x1                                C:\WINDOWS\System32\WZCSvc.DLL
0x76d30000     0x4000        0x1                                C:\WINDOWS\System32\WMI.dll
0x76d80000    0x1a000        0x1                                C:\WINDOWS\System32\DHCPCSVC.DLL
0x762c0000    0x8a000        0x1                                C:\WINDOWS\system32\CRYPT32.dll
0x762a0000     0xf000        0x1                                C:\WINDOWS\system32\MSASN1.dll
0x76f50000     0x8000        0x1                                C:\WINDOWS\System32\WTSAPI32.dll
0x76360000     0xf000        0x2                                C:\WINDOWS\System32\WINSTA.dll
0x71950000    0xe4000        0x2                                C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.0.0_x-ww_1382d70a\comctl32.dll
0x77340000    0x8b000        0x1                                C:\WINDOWS\system32\comctl32.dll
0x76fb0000     0x7000        0x1                                C:\WINDOWS\System32\winrnr.dll
0x76fc0000     0x5000        0x1                                C:\WINDOWS\System32\rasadhlp.dll
0x71a90000     0x8000        0x1                                C:\WINDOWS\System32\wshtcpip.dll
************************************************************************
```

Appendix 12: VNC4



```
************************************************************************
winvnc4.exe pid:    548
Command line : C:\inetpub\ftproot\VNC4\winvnc4.exe


Base             Size  LoadCount LoadTime                       Path
---------- ---------- ---------- ------------------------------ ----
0x00400000    0x6c000     0xffff                                C:\inetpub\ftproot\VNC4\winvnc4.exe
0x77f50000    0xa9000     0xffff                                C:\WINDOWS\System32\ntdll.dll
0x77e60000    0xe5000     0xffff                                C:\WINDOWS\system32\kernel32.dll
0x77d40000    0x8d000     0xffff                                C:\WINDOWS\system32\USER32.dll
0x77c70000    0x40000     0xffff                                C:\WINDOWS\system32\GDI32.dll
0x77dd0000    0x8b000     0xffff                                C:\WINDOWS\system32\ADVAPI32.dll
0x77cc0000    0x75000     0xffff                                C:\WINDOWS\system32\RPCRT4.dll
0x773d0000   0x7f4000     0xffff                                C:\WINDOWS\system32\SHELL32.dll
0x77c10000    0x53000     0xffff                                C:\WINDOWS\system32\msvcrt.dll
0x772d0000    0x63000     0xffff                                C:\WINDOWS\system32\SHLWAPI.dll
0x71ab0000    0x15000     0xffff                                C:\WINDOWS\System32\WS2_32.dll
0x71aa0000     0x8000     0xffff                                C:\WINDOWS\System32\WS2HELP.dll
0x77c00000     0x7000     0xffff                                C:\WINDOWS\system32\VERSION.dll
0x771b0000   0x11a000     0xffff                                C:\WINDOWS\system32\ole32.dll
0x71950000    0xe4000        0x3                                C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-
Controls_6595b64144ccf1df_6.0.0.0_x-ww_1382d70a\comctl32.dll
0x76360000     0xf000        0x3                                C:\WINDOWS\System32\winsta.dll
0x5ad70000    0x34000        0x2                                C:\WINDOWS\system32\uxtheme.dll
0x71a50000    0x3b000        0x4                                C:\WINDOWS\system32\mswsock.dll
0x71a90000     0x8000        0x1                                C:\WINDOWS\System32\wshtcpip.dll
0x76f20000    0x25000        0x3                                C:\WINDOWS\System32\DNSAPI.dll
0x76d60000    0x15000        0x3                                C:\WINDOWS\System32\iphlpapi.dll
0x76de0000    0x26000        0x1                                C:\WINDOWS\System32\netman.dll
0x76d40000    0x16000        0x1                                C:\WINDOWS\System32\MPRAPI.dll
0x76e40000    0x2f000        0x1                                C:\WINDOWS\System32\ACTIVEDS.dll
0x76e10000    0x24000        0x1                                C:\WINDOWS\System32\adsldpc.dll
0x71c20000    0x4f000        0x6                                C:\WINDOWS\System32\NETAPI32.dll
0x76f60000    0x2c000        0x2                                C:\WINDOWS\system32\WLDAP32.dll
0x76b20000    0x15000        0x1                                C:\WINDOWS\System32\ATL.DLL
0x77120000    0x8b000        0x4                                C:\WINDOWS\system32\OLEAUT32.dll
0x76e80000     0xd000        0x4                                C:\WINDOWS\System32\rtutils.dll
0x71bf0000    0x11000        0x1                                C:\WINDOWS\System32\SAMLIB.dll
0x76670000    0xe4000        0x1                                C:\WINDOWS\System32\SETUPAPI.dll
0x76ee0000    0x37000        0x2                                C:\WINDOWS\System32\RASAPI32.dll
0x76e90000    0x11000        0x2                                C:\WINDOWS\System32\rasman.dll
0x76eb0000    0x2a000        0x2                                C:\WINDOWS\System32\TAPI32.dll
0x76b40000    0x2c000        0x2                                C:\WINDOWS\System32\WINMM.dll
0x76f90000    0x10000        0x3                                C:\WINDOWS\System32\Secur32.dll
0x76da0000    0x30000        0x1                                C:\WINDOWS\System32\WZCSvc.DLL
0x76d30000     0x4000        0x1                                C:\WINDOWS\System32\WMI.dll
0x76d80000    0x1a000        0x1                                C:\WINDOWS\System32\DHCPCSVC.DLL
0x762c0000    0x8a000        0x1                                C:\WINDOWS\system32\CRYPT32.dll
0x762a0000     0xf000        0x1                                C:\WINDOWS\system32\MSASN1.dll
0x76f50000     0x8000        0x1                                C:\WINDOWS\System32\WTSAPI32.dll
0x76fb0000     0x7000        0x1                                C:\WINDOWS\System32\winrnr.dll
0x76fc0000     0x5000        0x1                                C:\WINDOWS\System32\rasadhlp.dll
************************************************************************
```