Global Information Assurance Certification Paper

GREM Practical
(GIAC Reverse Engineering Malware)

Sven Olensky

SANS Online Course 2004
Practical Version 1.0

Contents

1. Preface

This is my submission to fulfill the requirements for the practical assignment part of the GREM / Reverse Engineering Malware. It consists of a detailed analysis of an unknown, possibly malicious binary.

Thanks to my wife Jamie and our kids (Neo and Kiki [DOGS]) for loving me like they do.

Sven Olensky
August/September 2004

2. Introduction

This paper consists of 7 sections plus an appendix.

2.1. Legend

- commands that are getting executed, comments and the output of these commands in the assignments are typed in Courier New
- words in brackets [WORD] indicates a reference that can be found in the appendix
- '$' in front of the command means user-level access, '#' means root-level access
- '//' means comment

Examples

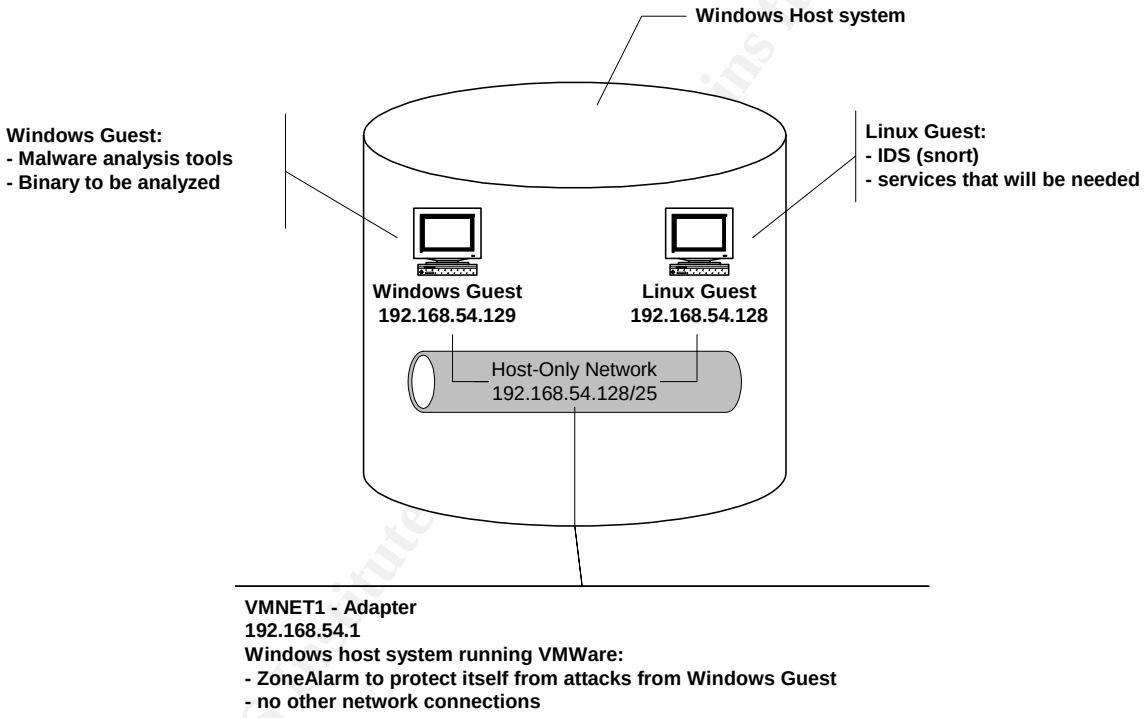
```
$ ls –l
// list contents in long form, user-level access

# rm –rf *
// delete everything, starting in this directory, as root
```

3. Laboratory Setup

Laboratory Setup - 10 points

Describe in detail your laboratory setup. We suggest using the setup described in the course material, or you may use your own set up as long as it meets the reverse-engineering needs of this practical assignment. Describe the hardware, networking, and software resources you used for your analysis. Explain laboratory isolation precautions that you implemented to protect your production environment from infection. Make sure to include a detailed description of each resource, its purpose, how, and where how you used it during the analysis.

3.1. Lab setup



The lab is based on a VMware- setup. The host system running VMware is a laptop running Windows 2000 Professional with all the latest security patches. The guest operating systems that are installed within the VMware environment are one RedHat Linux system and one Windows 2000 Professional system. The RedHat Linux system will run the Intrusion Detection System Snort and emulate any services that might be requested by the Guest- Windows 2000 System, on which the malware analysis will take place and on which the actual malicious application will be executed.

The network that is shared between the guests and the host system is a VMware host-only network which is only accessible by those systems. It is closed off to the outside. In addition to that, the laptop's real network connection is unplugged to protect the surrounding networks in case the trojan finds its way out of the protected VMware environment.

3.2. Tools used

The Windows 2000 guest system has the following tools installed that will aid in the analysis of the malicious executable:

- IDA Pro disassembler [IDAPRO]
- OllyDbg debugger [OLLYDBG]
- Various SysInternals tools: RegMon (monitoring of registry), FileMon (monitoring of file accesses), TDIMon (monitoring of network access), ProcExp to show active processes [SYSINTERNALS]
- BinText to analyse string contents of files [BINTEXT]
- RegShot to compare registry snapshots [REGSHOT]
- WinZip to unpack any required archives [WINZIP]
- PEInfo to analyse file type and other file details [SANSCLASS]
- file for file type analysis [FILE]

The laptop (the host system that is running VMware) is also running Zonelabs ZoneAlarm to protect itself from any potential malicious traffic that could be initiated by the binary.

4. Properties of the Malware Specimen

Properties of the Malware Specimen - 5 points

List the following properties of the malware. Make sure to include a detailed explanation of your steps, and an interpretation of your findings.

- Type of file (e.g. executable, compressed, data, etc.)
- Size of the file
- MD5 hash of the file
- Operating system(s) it runs on
- Strings embedded into it

4.1. Type of file

This seems to be an executable, either MS-DOS or Windows.

4.2. Size of file

PEInfo states 41984 Bytes, 41.0 KB.

```
Path: C:\download\sanspractical\msrll.exe
     File size:   41984
    Image size:   1179648
File Alignment:   512
Resources account for 0.00% of the executable
41.0 KB (41,984 bytes)
```

4.3. MD5 hashes of the file

```
C:\download\sanspractical>md5sum msrll.zip
696c78651244b1ad0363a400a23d48ef *msrll.zip

C:\download\sanspractical>md5sum msrll.exe
84acfe96a98590813413122c12c11aaa *msrll.exe
```

4.4. Operating Systems it runs on

The string `'!This program cannot be run in DOS mode.'` below indicates that this is a Windows executable. The file tool is more precise:

```
C:\Program Files\GnuWin32\bin>file c:\download\sanspractical\msrll.exe
c:\download\sanspractical\msrll.exe: MS Windows PE Intel 80386 GUI executable no
t relocatable
```

This seems to be a MS-Windows executable for Intel-386-based systems.

4.5. Strings embedded in the binary

From PEInfo:

```
File pos   Mem pos      ID   Text
========   =======      ==   ====

0000004D   0040004D      0   !This program cannot be run in DOS mode.
00000178   00400178      0   .text
000001A0   004001A0      0   .data
000001F0   004001F0      0   .idata
00000218   00400218      0   .aspack
00000240   00400240      0   .adata
00000427   00401027      0   6>HBId
00000572   00401172      0   (l]Ol
000006AA   004012AA      0   S'tt@
00000702   00401302      0   ~MMhx
000007F0   004013F0      0   Xp,Yd
000008FD   004014FD      0   TPVTR
00000927   00401527      0   0&rgt
00000D1A   0040191A      0   Y8EoM,
00000E94   00401A94      0   gPtL7S
00000F17   00401B17      0   #u1DY
00000F8F   00401B8F      0   Syv,l
00000FCC   00401BCC      0   YQ(W;n
00000FFF   00401BFF      0   @\X~K
0000106F   00401C6F      0   , gMF
000010CE   00401CCE      0   1d%.A
00001149   00401D49      0   wmfe)
000011BC   00401DBC      0   wn*-(
0000139E   00401F9E      0   <)Ii>
0000152A   0040212A      0   )<)H1
00001646   00402246      0   Hq '7
00001678   00402278      0   : d'V
000016CD   004022CD      0   h=#tD
00001729   00402329      0   Ul=.Z
000017BC   004023BC      0   3#b5pHo
000019BF   004025BF      0   iWw+V
00001A37   00402637      0   w3i5Y-
00001C58   00402858      0   [u)aH=
00001D09   00402909      0   /0mo0
00001D1A   0040291A      0   Bj3K7%(
00001D85   00402985      0    yb>qO
00001E76   00402A76      0   h=&PO
00001E7E   00402A7E      0   O7IsL
00001F7A   00402B7A      0   s7xI:
00002222   00402E22      0   TN9x0
00002361   00402F61      0   U[{*\4
000023FB   00402FFB      0   k3VgD
000024B4   004030B4      0   m&8NRM
000026D8   004032D8      0   k;Px,
0000286F   0040346F      0   8e47xW
00002947   00403547      0   x[D.-
00002B4C   0040374C      0   H&,0d
00002B59   00403759      0   W'A=j
00002BC7   004037C7      0   EAe4xIpO
00002E2D   00403A2D      0   r8cy!/
00002EB9   00403AB9      0   127$9v
00002F5A   00403B5A      0   zYX[[T
00002FBA   00403BBA      0   } {e}
00003336   00403F36      0   PS=,sdVQ
000033A2   00403FA2      0   UZKSU,
00003414   00404014      0   5OUS</
000034C4   004040C4      0   %XjBZnu
000034DC   004040DC      0   sX_,G
000035D4   004041D4      0   9QBDW
00003613   00404213      0   :|gs3~3
0000367C   0040427C      0   WN      7g
000036FB   004042FB      0   A7Od-
```

```
000038B0   004044B0      0   cJ =H
0000397B   0040457B      0   G-~+f
00003AB6   004046B6      0   s&+*uX
00003C96   00404896      0   L,HvCy
00003F2A   00404B2A      0   h~RX<
00004164   00404D64      0   wZMFN_
00004242   00404E42      0   u}>|y
000042E3   00404EE3      0   $+z_l
0000437C   00404F7C      0   T_6F+
00004394   00404F94      0   jlR=N
000043BA   00404FBA      0   55R[M
0000442A   0040502A      0   y!]zqZ
00004494   00405094      0   s$ILIEK
000044F9   004050F9      0   pr}#
00004544   00405144      0   '.gcH(
00004555   00405155      0   # dNZ
00004599   00405199      0   PQiqGt
000046C7   004052C7      0   P[{'R
00004729   00405329      0   ?Q~)Qv
00004767   00405367      0   Y|5S(K
00004934   00405534      0   ?v'Tz
0000498B   0040558B      0   0]2%I
00004BA7   004057A7      0   >~g[f!Unl
00004E54   00405A54      0   xaa11K
00004E8D   00405A8D      0   fOjv.
0000515E   00405D5E      0   G       /a}
00005172   00405D72      0   M1QF;
000052D5   00405ED5      0   d{fB0d
000054F8   004060F8      0   <?nxt
00005514   00406114      0   s$OY5-
00005534   00406134      0   ]ruy~
0000560E   0040620E      0   h9pPE
0000564E   0040624E      0   .@g5d
0000566C   0040626C      0   s*9r\sN
00005729   00406329      0   ca7%D
00005803   00406403      0   ?d]aH
00005925   00406525      0   Z3O-,;
00005A4A   0040664A      0   0X/\@
00005C56   00406856      0   fOq2f
00005CF7   004068F7      0   kvK@~G
00005E65   00406A65      0   GHWWa
00005F1E   00406B1E      0   {[3aM
00005F78   00406B78      0   /xzKX
00006253   00406E53      0   PAPD;-
00006504   00407104      0   m#]+d
00006575   00407175      0   E2#fW
000066B3   004072B3      0   icBLM
00006816   00407416      0   E'>*)
00006C1F   0040781F      0   3N@G:
00006D47   00407947      0   ~/WDE
00006E3A   00407A3A      0   xCd4!c
00006E99   00407A99      0   6n|O+
00006ECA   00407ACA      0   Sn)b/
000070D2   00407CD2      0   /&*Qr
00007216   00407E16      0   gmRx[
0000723E   00407E3E      0   fuQal
000073A4   00407FA4      0    M'L s
00007536   00408136      0   xq,p:j
00007604   00408204      0   bn;&%y
00007664   00408264      0   }NHvl
0000769A   0040829A      0   ,UQ &
000077D3   004083D3      0   y[:BaV_
00007918   00408518      0   ]zI(3
000079BF   004085BF      0   E               G2
00007A2A   0040862A      0   8qA9;
00007B41   00408741      0   aZ!zU
00007B99   00408799      0   ?u%\Y
00007D57   00408957      0   dqiV*
00007D88   00408988      0   ~a0FG
00007D9E   0040899E      0   Yqc*Jam
00007E14   00408A14      0   q6*\
```

```
00007F18   00408B18      0   I.zxx
00008011   00408C11      0   ~a|Yh
000081F4   00408DF4      0   >+0ac
00008440   00413040      0   GMZid+K
00008519   00413119      0   XFt##
00008540   00413140      0   90K.P
000085CA   004131CA      0   5 RBd
00008655   00413255      0   /af=V
00008A73   0051B073      0   'Uazu
00008B6F   0051B16F      0   \%Ap2
00008E7D   0051B47D      0   bI4x+Za
00008EDD   0051B4DD      0   Z/rA'
00008F72   0051B572      0   ga1YAx
00009094   0051B694      0   kN2$6|[x
000090A3   0051B6A3      0   .yw_|
000090D1   0051B6D1      0   p[3bg
00009271   0051D071      0   VirtualAlloc
0000927E   0051D07E      0   VirtualFree
00009641   0051D441      0   kernel32.dll
0000964E   0051D44E      0   ExitProcess
0000965A   0051D45A      0   user32.dll
00009665   0051D465      0   MessageBoxA
00009671   0051D471      0   wsprintfA
0000967B   0051D47B      0   LOADER ERROR
00009688   0051D488      0   The procedure entry point %s could not be located in the
dynamic link library %s
000096D9   0051D4D9      0   The ordinal %u could not be located in the dynamic link
library %s
000098E6   0051D6E6      0    (08@P
00009A74   0051D874      0   D4l|M
00009BC0   0051D9C0      0   ;;F,s
00009BCF   0051D9CF      0   ,;F0s
00009BDB   0051D9DB      0    ;F4s
00009EB5   0051DCB5      0   D$$W3
0000A16C   0051DF6C      0   kernel32.dll
0000A17B   0051DF7B      0   GetProcAddress
0000A18C   0051DF8C      0   GetModuleHandleA
0000A19F   0051DF9F      0   LoadLibraryA
0000A274   0051E074      0   advapi32.dll
0000A281   0051E081      0   msvcrt.dll
0000A28C   0051E08C      0   msvcrt.dll
0000A297   0051E097      0   shell32.dll
0000A2A3   0051E0A3      0   user32.dll
0000A2AE   0051E0AE      0   version.dll
0000A2BA   0051E0BA      0   wininet.dll
0000A2C6   0051E0C6      0   ws2_32.dll
0000A313   0051E113      0   AdjustTokenPrivileges
0000A32B   0051E12B      0   _itoa
0000A333   0051E133      0   __getmainargs
0000A343   0051E143      0   ShellExecuteA
0000A353   0051E153      0   DispatchMessageA
0000A366   0051E166      0   GetFileVersionInfoA
0000A37C   0051E17C      0   InternetCloseHandle
0000A392   0051E192      0   WSAGetLastError
```

Aside from Windows function calls in the last part of the string output, no useful information can be extracted from the character strings. It appears to be that the file is somehow packed or encrypted. The first lines indicate the section names.

```
00000178   00400178      0   .text
000001A0   004001A0      0   .data
000001F0   004001F0      0   .idata
00000218   00400218      0   .aspack
00000240   00400240      0   .adata
```

`.aspack` indicates that the file was packed using ASPack [ASPACK]

5. Behavioural Analysis

Behavioural Analysis - 35 points

Use your laboratory setup to perform a behavioural analysis of the unknown malware specimen infecting a system in the laboratory, with the malicious program under controlled conditions. Describe the analysis in detail. Describe your actions and your use of your the analysis tools in detail. Explain the implications of the behaviour of the malware specimen.

Example procedures:

- Monitoring file system access
- Monitoring registry / configuration access
- Monitoring / redirecting network connections
- Monitoring processes on the system

5.1. Preparations

Before the binary gets executed, all the monitors have to be in place and started:

- RegMon (monitoring of registry)
- FileMon (monitoring of file accesses)
- TDIMon (monitoring of network access)
- RegShot: take a snapshot of the registry before the binary gets executed so that the registry modifications can be seen later on
- ProcExp to monitor running processes

This section is split into two parts: the behaviour of the binary on the local machine and the behaviour of the machine on the network.

5.2. Behaviour of the Binary on the local machine

5.2.1. RegShot

Lets look at the comparison of the registry snapshots before and after the execution of msrll.exe, created by RegShot:

```
REGSHOT LOG 1.61e5
Comments:
Datetime:2004/8/16 19:59:09  ,  2004/8/16 20:33:56
Computer:COMPUTER , COMPUTER
Username: ,

----------------------------------
Keys added:8
----------------------------------
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY_FILEMON\0000\Control
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY_REGMON\0000\Control
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\mfm
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\mfm\Security
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_FILEMON\0000\Control
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_REGMON\0000\Control
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\mfm
```

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\mfm\Security

---------------------------------
Values added:29
---------------------------------
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY_FILEMON\0000\Control\ActiveServi
ce: "FILEMON"
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY_REGMON\0000\Control\ActiveServic
e: "REGMON"
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY_TDIMSYS\0000\Control\ActiveServi
ce: "TDIMSYS"
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\SW\{b7eafdc0-a680-11d0-96d8-
00aa0051e51d}\{9B365890-165F-11D0-A195-0020AFD156E4}\Control\DeviceReference: 0x811F7B10
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\kmixer\Enum\0: "SW\{b7eafdc0-a680-11d0-
96d8-00aa0051e51d}\{9B365890-165F-11D0-A195-0020AFD156E4}"
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\mfm\Security\Security: 01 00 14 80 A0 00
00 00 AC 00 00 00 14 00 00 00 30 00 00 00 02 00 1C 00 01 00 00 00 02 80 14 00 FF 01 0F 00
01 01 00 00 00 00 00 01 00 00 00 00 02 00 70 00 04 00 00 00 00 00 18 00 FD 01 02 00 01 01
00 00 00 00 00 05 12 00 00 00 49 00 4D 00 00 00 1C 00 FF 01 0F 00 01 02 00 00 00 00 00 05
20 00 00 00 20 02 00 00 53 00 59 00 00 00 18 00 8D 01 02 00 01 01 00 00 00 00 00 05 0B 00
00 00 20 02 00 00 00 00 1C 00 FD 01 02 00 01 02 00 00 00 00 00 05 20 00 00 00 23 02 00 00
53 00 59 00 01 01 00 00 00 00 00 05 12 00 00 00 01 01 00 00 00 00 00 05 12 00 00 00
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\mfm\Type: 0x00000120
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\mfm\Start: 0x00000002
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\mfm\ErrorControl: 0x00000002
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\mfm\ImagePath:
"C:\WINNT\system32\mfm\msrll.exe"
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\mfm\DisplayName: "Rll enhanced drive"
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\mfm\ObjectName: "LocalSystem"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_FILEMON\0000\Control\ActiveS
ervice: "FILEMON"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_REGMON\0000\Control\ActiveSe
rvice: "REGMON"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_TDIMSYS\0000\Control\ActiveS
ervice: "TDIMSYS"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\SW\{b7eafdc0-a680-11d0-96d8-
00aa0051e51d}\{9B365890-165F-11D0-A195-0020AFD156E4}\Control\DeviceReference: 0x811F7B10
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kmixer\Enum\0: "SW\{b7eafdc0-a680-
11d0-96d8-00aa0051e51d}\{9B365890-165F-11D0-A195-0020AFD156E4}"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\mfm\Security\Security: 01 00 14 80
A0 00 00 00 AC 00 00 00 14 00 00 00 30 00 00 00 02 00 1C 00 01 00 00 00 02 80 14 00 FF 01
0F 00 01 01 00 00 00 00 00 01 00 00 00 00 02 00 70 00 04 00 00 00 00 00 18 00 FD 01 02 00
01 01 00 00 00 00 00 05 12 00 00 00 49 00 4D 00 00 00 1C 00 FF 01 0F 00 01 02 00 00 00 00
00 05 20 00 00 00 20 02 00 00 53 00 59 00 00 00 18 00 8D 01 02 00 01 01 00 00 00 00 00 05
0B 00 00 00 20 02 00 00 00 00 1C 00 FD 01 02 00 01 02 00 00 00 00 00 05 20 00 00 00 23 02
00 00 53 00 59 00 01 01 00 00 00 00 00 05 12 00 00 00 01 01 00 00 00 00 00 05 12 00 00 00
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\mfm\Type: 0x00000120
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\mfm\Start: 0x00000002
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\mfm\ErrorControl: 0x00000002
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\mfm\ImagePath:
"C:\WINNT\system32\mfm\msrll.exe"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\mfm\DisplayName: "Rll enhanced
drive"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\mfm\ObjectName: "LocalSystem"
HKEY_USERS\S-1-5-21-823518204-1326574676-725345543-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU\h: 46 00
69 00 6C 00 65 00 6D 00 6F 00 6E 00 2E 00 65 00 78 00 65 00 00 00 43 00 3A 00 5C 00 44 00
6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 73 00 20 00 61 00 6E 00 64 00 20 00 53 00 65 00
74 00 74 00 69 00 6E 00 67 00 73 00 5C 00 41 00 64 00 6D 00 69 00 6E 00 69 00 73 00 74 00
72 00 61 00 74 00 6F 00 72 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 00 00
HKEY_USERS\S-1-5-21-823518204-1326574676-725345543-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\log\c:
"C:\Documents and Settings\Administrator\Desktop\Filemon.LOG"
HKEY_USERS\S-1-5-21-823518204-1326574676-725345543-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.log\OpenWithList\d:
"Filemon.exe"
HKEY_USERS\S-1-5-21-823518204-1326574676-725345543-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.log\c: 46 00 69 00 6C
00 65 00 6D 00 6F 00 6E 00 2E 00 4C 00 4F 00 47 00 00 00 1F 00 32 00 00 00 00 00 00 00 00
00 00 00 46 69 6C 65 6D 6F 6E 2E 4C 4F 47 2E 6C 6E 6B 00 00 00 00
```

HKEY_USERS\S-1-5-21-823518204-1326574676-725345543-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-
9888-006097DEACF9}\Count\HRZR_EHACNGU:P:\qbjaybnq\fnafcenpgvpny\zfeyy.rkr: 06 00 00 00 06
00 00 00 30 5A 66 C7 CB 83 C4 01

Values modified:46

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\RNG\Seed: 1F 3A D2 83 29 AF 2A EB E3
75 B7 C1 F4 67 55 30 DD 34 22 17 61 32 2E 49 5D 1E 7D 05 2A CC EA 96 5F 6A 7A 0C A2 34 5C
B7 84 E2 5C 48 61 4C 2D 9F 85 38 5B F3 DF 1E B8 40 66 87 25 4E 19 C9 83 11 10 46 5E 2B 81
88 67 3F A3 5B DE 09 93 34 EC 14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\RNG\Seed: 6C B0 A2 25 AF A8 66 C8 AB
04 C4 8F D7 A7 2A 89 AE 9C 64 05 F6 C7 30 FE C9 EB 24 8E 10 1E 2D 0A A4 F4 EF 33 36 6A 69
45 D8 2D 25 9D 28 91 BC 71 80 95 58 AE BF 03 FE B0 84 C0 55 89 CB 79 DC 5B 4E 97 AA C0 EA
90 CD 67 5E 37 4E 14 26 18 38 77
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet
Settings\Cache\Paths\Directory: "C:\Documents and Settings\Default User\Local
Settings\Temporary Internet Files\Content.IE5"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet
Settings\Cache\Paths\Directory: "C:\Documents and Settings\Administrator\Local
Settings\Temporary Internet Files\Content.IE5"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet
Settings\Cache\Paths\path1\CachePath: "C:\Documents and Settings\Default User\Local
Settings\Temporary Internet Files\Content.IE5\Cache1"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet
Settings\Cache\Paths\path1\CachePath: "C:\Documents and Settings\Administrator\Local
Settings\Temporary Internet Files\Content.IE5\Cache1"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet
Settings\Cache\Paths\path2\CachePath: "C:\Documents and Settings\Default User\Local
Settings\Temporary Internet Files\Content.IE5\Cache2"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet
Settings\Cache\Paths\path2\CachePath: "C:\Documents and Settings\Administrator\Local
Settings\Temporary Internet Files\Content.IE5\Cache2"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet
Settings\Cache\Paths\path3\CachePath: "C:\Documents and Settings\Default User\Local
Settings\Temporary Internet Files\Content.IE5\Cache3"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet
Settings\Cache\Paths\path3\CachePath: "C:\Documents and Settings\Administrator\Local
Settings\Temporary Internet Files\Content.IE5\Cache3"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet
Settings\Cache\Paths\path4\CachePath: "C:\Documents and Settings\Default User\Local
Settings\Temporary Internet Files\Content.IE5\Cache4"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet
Settings\Cache\Paths\path4\CachePath: "C:\Documents and Settings\Administrator\Local
Settings\Temporary Internet Files\Content.IE5\Cache4"
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Dhcp\Parameters\{9C57D580-0CCB-4A39-
AE24-881CDD481145}: 06 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 77 18 21 41 C0 A8 3A
01 0F 00 00 00 00 00 00 00 0B 00 00 00 00 00 00 00 77 18 21 41 6C 6F 63 61 6C 64 6F 6D 61
69 6E 00 01 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 77 18 21 41 FF FF FF 00 33 00 00
00 00 00 00 00 04 00 00 00 00 00 00 00 77 18 21 41 00 00 07 08 36 00 00 00 00 00 00 00 04
00 00 00 00 00 00 00 00 77 18 21 41 C0 A8 3A FE 35 00 00 00 00 00 00 00 01 00 00 00 00 00 00
00 77 18 21 41 05 00 00 00
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Dhcp\Parameters\{9C57D580-0CCB-4A39-
AE24-881CDD481145}: 06 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 7F 1F 21 41 C0 A8 3A
01 0F 00 00 00 00 00 00 00 0B 00 00 00 00 00 00 00 7F 1F 21 41 6C 6F 63 61 6C 64 6F 6D 61
69 6E 00 01 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 7F 1F 21 41 FF FF FF 00 33 00 00
00 00 00 00 00 04 00 00 00 00 00 00 00 7F 1F 21 41 00 00 07 08 36 00 00 00 00 00 00 00 04
00 00 00 00 00 00 00 00 7F 1F 21 41 C0 A8 3A FE 35 00 00 00 00 00 00 00 01 00 00 00 00 00 00
00 7F 1F 21 41 05 00 00 00
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\kmixer\Enum\Count: 0x00000000
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\kmixer\Enum\Count: 0x00000001
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\kmixer\Enum\NextInstance: 0x00000000
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\kmixer\Enum\NextInstance: 0x00000001
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{9C57D580-
0CCB-4A39-AE24-881CDD481145}\LeaseObtainedTime: 0x4121116F
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{9C57D580-
0CCB-4A39-AE24-881CDD481145}\LeaseObtainedTime: 0x41211877
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{9C57D580-
0CCB-4A39-AE24-881CDD481145}\T1: 0x412114F3

```
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{9C57D580-
0CCB-4A39-AE24-881CDD481145}\T1: 0x41211BFB
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{9C57D580-
0CCB-4A39-AE24-881CDD481145}\T2: 0x41211796
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{9C57D580-
0CCB-4A39-AE24-881CDD481145}\T2: 0x41211E9E
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{9C57D580-
0CCB-4A39-AE24-881CDD481145}\LeaseTerminatesTime: 0x41211877
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{9C57D580-
0CCB-4A39-AE24-881CDD481145}\LeaseTerminatesTime: 0x41211F7F
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\TDIMSYS\Security\Security: 01 00 14 80
A0 00 00 00 AC 00 00 00 14 00 00 00 30 00 00 00 02 00 1C 00 01 00 00 00 02 80 14 00 FF 01
0F 00 01 01 00 00 00 00 00 01 00 00 00 00 02 00 70 00 04 00 00 00 00 00 18 00 FD 01 02 00
01 01 00 00 00 00 00 05 12 00 00 00 00 00 00 00 00 00 1C 00 FF 01 0F 00 01 02 00 00 00 00
00 05 20 00 00 00 20 02 00 00 00 00 00 00 00 00 18 00 8D 01 02 00 01 01 00 00 00 00 00 05
0B 00 00 00 20 02 00 00 00 00 1C 00 FD 01 02 00 01 02 00 00 00 00 00 05 20 00 00 00 23 02
00 00 00 00 00 00 01 01 00 00 00 00 00 05 12 00 00 00 01 01 00 00 00 00 00 05 12 00 00 00
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\TDIMSYS\Security\Security: 01 00 14 80
A0 00 00 00 AC 00 00 00 14 00 00 00 30 00 00 00 02 00 1C 00 01 00 00 00 02 80 14 00 FF 01
0F 00 01 01 00 00 00 00 00 01 00 00 00 00 02 00 70 00 04 00 00 00 00 00 18 00 FD 01 02 00
01 01 00 00 00 00 00 05 12 00 00 00 03 00 00 00 00 00 1C 00 FF 01 0F 00 01 02 00 00 00 00
00 05 20 00 00 00 20 02 00 00 80 01 A0 01 00 00 18 00 8D 01 02 00 01 01 00 00 00 00 00 05
0B 00 00 00 20 02 00 00 00 00 1C 00 FD 01 02 00 01 02 00 00 00 00 00 05 20 00 00 00 23 02
00 00 80 01 A0 01 01 01 00 00 00 00 00 05 12 00 00 00 01 01 00 00 00 00 00 05 12 00 00 00
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\{9C57D580-0CCB-4A39-AE24-
881CDD481145}\Parameters\Tcpip\LeaseObtainedTime: 0x4121116F
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\{9C57D580-0CCB-4A39-AE24-
881CDD481145}\Parameters\Tcpip\LeaseObtainedTime: 0x41211877
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\{9C57D580-0CCB-4A39-AE24-
881CDD481145}\Parameters\Tcpip\T1: 0x412114F3
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\{9C57D580-0CCB-4A39-AE24-
881CDD481145}\Parameters\Tcpip\T1: 0x41211BFB
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\{9C57D580-0CCB-4A39-AE24-
881CDD481145}\Parameters\Tcpip\T2: 0x41211796
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\{9C57D580-0CCB-4A39-AE24-
881CDD481145}\Parameters\Tcpip\T2: 0x41211E9E
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\{9C57D580-0CCB-4A39-AE24-
881CDD481145}\Parameters\Tcpip\LeaseTerminatesTime: 0x41211877
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\{9C57D580-0CCB-4A39-AE24-
881CDD481145}\Parameters\Tcpip\LeaseTerminatesTime: 0x41211F7F
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dhcp\Parameters\{9C57D580-0CCB-4A39-
AE24-881CDD481145}: 06 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 77 18 21 41 C0 A8 3A
01 0F 00 00 00 00 00 00 00 0B 00 00 00 00 00 00 00 77 18 21 41 6C 6F 63 61 6C 64 6F 6D 61
69 6E 00 01 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 77 18 21 41 FF FF FF 00 33 00 00
00 00 00 00 00 04 00 00 00 00 00 00 00 00 77 18 21 41 00 00 07 08 36 00 00 00 00 00 00 04
00 00 00 00 00 00 00 77 18 21 41 C0 A8 3A FE 35 00 00 00 00 00 00 01 00 00 00 00 00 00 00
00 77 18 21 41 05 00 00 00
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dhcp\Parameters\{9C57D580-0CCB-4A39-
AE24-881CDD481145}: 06 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 7F 1F 21 41 C0 A8 3A
01 0F 00 00 00 00 00 00 00 0B 00 00 00 00 00 00 00 7F 1F 21 41 6C 6F 63 61 6C 64 6F 6D 61
69 6E 00 01 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 7F 1F 21 41 FF FF FF 00 33 00 00
00 00 00 00 00 04 00 00 00 00 00 00 00 00 7F 1F 21 41 00 00 07 08 36 00 00 00 00 00 00 04
00 00 00 00 00 00 00 7F 1F 21 41 C0 A8 3A FE 35 00 00 00 00 00 00 01 00 00 00 00 00 00 00
00 7F 1F 21 41 05 00 00 00
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kmixer\Enum\Count: 0x00000000
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kmixer\Enum\Count: 0x00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kmixer\Enum\NextInstance: 0x00000000
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\kmixer\Enum\NextInstance: 0x00000001
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{9C57D58
0-0CCB-4A39-AE24-881CDD481145}\LeaseObtainedTime: 0x4121116F
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{9C57D58
0-0CCB-4A39-AE24-881CDD481145}\LeaseObtainedTime: 0x41211877
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{9C57D58
0-0CCB-4A39-AE24-881CDD481145}\T1: 0x412114F3
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{9C57D58
0-0CCB-4A39-AE24-881CDD481145}\T1: 0x41211BFB
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{9C57D58
0-0CCB-4A39-AE24-881CDD481145}\T2: 0x41211796
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{9C57D58
0-0CCB-4A39-AE24-881CDD481145}\T2: 0x41211E9E
```

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{9C57D58
0-0CCB-4A39-AE24-881CDD481145}\LeaseTerminatesTime: 0x41211877
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{9C57D58
0-0CCB-4A39-AE24-881CDD481145}\LeaseTerminatesTime: 0x41211F7F
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TDIMSYS\Security\Security: 01 00 14
80 A0 00 00 00 AC 00 00 00 14 00 00 00 30 00 00 00 02 00 1C 00 01 00 00 00 02 80 14 00 FF
01 0F 00 01 01 00 00 00 00 00 01 00 00 00 00 02 00 70 00 04 00 00 00 00 00 18 00 FD 01 02
00 01 01 00 00 00 00 00 05 12 00 00 00 00 00 00 00 00 00 00 1C 00 FF 01 0F 00 01 02 00 00 00
00 00 05 20 00 00 00 00 20 02 00 00 00 00 00 00 00 00 18 00 8D 01 02 00 01 01 00 00 00 00
05 0B 00 00 00 20 02 00 00 00 00 1C 00 FD 01 02 00 01 02 00 00 00 00 00 05 20 00 00 00 23
02 00 00 00 00 00 00 01 01 00 00 00 00 00 05 12 00 00 00 01 01 00 00 00 00 00 05 12 00 00
00
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TDIMSYS\Security\Security: 01 00 14
80 A0 00 00 00 AC 00 00 00 14 00 00 00 30 00 00 00 02 00 1C 00 01 00 00 00 02 80 14 00 FF
01 0F 00 01 01 00 00 00 00 00 01 00 00 00 00 02 00 70 00 04 00 00 00 00 00 18 00 FD 01 02
00 01 01 00 00 00 00 00 05 12 00 00 00 03 00 00 00 00 00 00 1C 00 FF 01 0F 00 01 02 00 00 00
00 00 05 20 00 00 00 00 20 02 00 00 80 01 A0 01 00 00 18 00 8D 01 02 00 01 01 00 00 00 00
05 0B 00 00 00 20 02 00 00 00 00 1C 00 FD 01 02 00 01 02 00 00 00 00 00 05 20 00 00 00 23
02 00 00 80 01 A0 01 01 01 00 00 00 00 00 05 12 00 00 00 01 01 00 00 00 00 00 05 12 00 00
00
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\{9C57D580-0CCB-4A39-AE24-
881CDD481145}\Parameters\Tcpip\LeaseObtainedTime: 0x4121116F
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\{9C57D580-0CCB-4A39-AE24-
881CDD481145}\Parameters\Tcpip\LeaseObtainedTime: 0x41211877
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\{9C57D580-0CCB-4A39-AE24-
881CDD481145}\Parameters\Tcpip\T1: 0x412114F3
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\{9C57D580-0CCB-4A39-AE24-
881CDD481145}\Parameters\Tcpip\T1: 0x41211BFB
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\{9C57D580-0CCB-4A39-AE24-
881CDD481145}\Parameters\Tcpip\T2: 0x41211796
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\{9C57D580-0CCB-4A39-AE24-
881CDD481145}\Parameters\Tcpip\T2: 0x41211E9E
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\{9C57D580-0CCB-4A39-AE24-
881CDD481145}\Parameters\Tcpip\LeaseTerminatesTime: 0x41211877
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\{9C57D580-0CCB-4A39-AE24-
881CDD481145}\Parameters\Tcpip\LeaseTerminatesTime: 0x41211F7F
HKEY_USERS\S-1-5-21-823518204-1326574676-725345543-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU\MRUList:
"agefdcb"
HKEY_USERS\S-1-5-21-823518204-1326574676-725345543-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU\MRUList:
"cdhagefb"
HKEY_USERS\S-1-5-21-823518204-1326574676-725345543-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU*\MRUList:
"fedbcjahgi"
HKEY_USERS\S-1-5-21-823518204-1326574676-725345543-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU*\MRUList:
"ghifedbcja"
HKEY_USERS\S-1-5-21-823518204-1326574676-725345543-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU*\i:
"C:\download\Hanuman.exe"
HKEY_USERS\S-1-5-21-823518204-1326574676-725345543-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU*\i:
"C:\Documents and Settings\Administrator\Desktop\Filemon.LOG"
HKEY_USERS\S-1-5-21-823518204-1326574676-725345543-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\log\MRUList:
"ba"
HKEY_USERS\S-1-5-21-823518204-1326574676-725345543-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU\log\MRUList:
"abc"
HKEY_USERS\S-1-5-21-823518204-1326574676-725345543-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.log\OpenWithList\MRUList
: "cba"
HKEY_USERS\S-1-5-21-823518204-1326574676-725345543-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.log\OpenWithList\MRUList
: "abdc"
HKEY_USERS\S-1-5-21-823518204-1326574676-725345543-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\MRUList:
"kutcewxbsmrqpjnohalfi{}d|gyv"

HKEY_USERS\S-1-5-21-823518204-1326574676-725345543-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\MRUList:
"i{zkutcewxbsmrqpjnohalf}d|gyv"
HKEY_USERS\S-1-5-21-823518204-1326574676-725345543-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\z: 4E 00 54 00 46 00 49
00 4C 00 4D 00 4F 00 4E 00 2E 00 7A 00 69 00 70 00 00 00 20 00 32 00 00 00 00 00 00 00 00
00 00 00 4E 54 46 49 4C 4D 4F 4E 2E 7A 69 70 2E 6C 6E 6B 00 00 00 00
HKEY_USERS\S-1-5-21-823518204-1326574676-725345543-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\z: 46 00 69 00 6C 00 65
00 6D 00 6F 00 6E 00 2E 00 4C 00 4F 00 47 00 00 00 1F 00 32 00 00 00 00 00 00 00 00 00 00
00 46 69 6C 65 6D 6F 6E 2E 4C 4F 47 2E 6C 6E 6B 00 00 00 00
HKEY_USERS\S-1-5-21-823518204-1326574676-725345543-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.log\MRUList: "ab"
HKEY_USERS\S-1-5-21-823518204-1326574676-725345543-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.log\MRUList: "abc"
HKEY_USERS\S-1-5-21-823518204-1326574676-725345543-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-
9888-006097DEACF9}\Count\HRZR_EHACNGU: 06 00 00 00 F5 00 00 00 C0 0C 4F 79 CB 83 C4 01
HKEY_USERS\S-1-5-21-823518204-1326574676-725345543-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-
9888-006097DEACF9}\Count\HRZR_EHACNGU: 06 00 00 00 F9 00 00 00 30 5A 66 C7 CB 83 C4 01
HKEY_USERS\S-1-5-21-823518204-1326574676-725345543-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-
9888-006097DEACF9}\Count\HRZR_EHACNGU:P:\Cebtenz Svyrf\flfvagreanyf\Svyrzba.rkr: 05 00 00
00 15 00 00 00 A0 1C E6 86 44 6C C4 01
HKEY_USERS\S-1-5-21-823518204-1326574676-725345543-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-
9888-006097DEACF9}\Count\HRZR_EHACNGU:P:\Cebtenz Svyrf\flfvagreanyf\Svyrzba.rkr: 06 00 00
00 16 00 00 00 20 EC D6 89 CB 83 C4 01
HKEY_USERS\S-1-5-21-823518204-1326574676-725345543-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-
9888-006097DEACF9}\Count\HRZR_EHACNGU:P:\Cebtenz Svyrf\flfvagreanyf\Ertzba.rkr: 04 00 00
00 0C 00 00 00 B0 FB D7 E3 E0 69 C4 01
HKEY_USERS\S-1-5-21-823518204-1326574676-725345543-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-
9888-006097DEACF9}\Count\HRZR_EHACNGU:P:\Cebtenz Svyrf\flfvagreanyf\Ertzba.rkr: 06 00 00
00 0D 00 00 00 B0 E9 47 81 CB 83 C4 01
HKEY_USERS\S-1-5-21-823518204-1326574676-725345543-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-
9888-006097DEACF9}\Count\HRZR_EHACNGU:P:\Cebtenz Svyrf\flfvagreanyf\GQVZBA.RKR: 04 00 00
00 0A 00 00 00 B0 A0 94 09 E1 69 C4 01
HKEY_USERS\S-1-5-21-823518204-1326574676-725345543-
500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-
9888-006097DEACF9}\Count\HRZR_EHACNGU:P:\Cebtenz Svyrf\flfvagreanyf\GQVZBA.RKR: 06 00 00
00 0B 00 00 00 B0 8B 31 AA CB 83 C4 01
HKEY_USERS\S-1-5-21-823518204-1326574676-725345543-
500\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\Connections\SavedLegacySettings: 3C 00 00 00 8B 00 00 00 01 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00
HKEY_USERS\S-1-5-21-823518204-1326574676-725345543-
500\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\Connections\SavedLegacySettings: 3C 00 00 00 8C 00 00 00 01 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00
HKEY_USERS\S-1-5-21-823518204-1326574676-725345543-
500\Software\Sysinternals\Filemon\Settings: B4 01 00 00 00 00 00 00 00 00 00 58 02 00
00 9B 01 00 00 23 00 00 00 5A 00 00 00 5A 00 00 00 82 00 00 00 58 01 00 00 46 00 00 00 96
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 01 00 00 00 01 01 01 00
00 00 01 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 90 01 00 00 00 00 00 00 01
02 02 22 4D 53 20 53 61 6E 73 20 53 65 72 69 66 00 13 00 78 01 13 00 D3 00 00 00 03 C6 FC
77 C9 C4 FC 77 FF FF FF 00 FF 00 00 00 00 01 00 00
HKEY_USERS\S-1-5-21-823518204-1326574676-725345543-
500\Software\Sysinternals\Filemon\Settings: B4 01 00 00 00 00 00 00 00 00 00 A6 03 00
00 80 01 00 00 23 00 00 00 5A 00 00 00 5A 00 00 00 82 00 00 00 58 01 00 00 46 00 00 00 96
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 01 01 00
00 00 01 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 90 01 00 00 00 00 00 00 01
02 02 22 4D 53 20 53 61 6E 73 20 53 65 72 69 66 00 13 00 78 01 13 00 D3 00 00 00 03 C6 FC
77 C9 C4 FC 77 FF FF FF 00 FF 00 00 00 00 01 00 00
HKEY_USERS\S-1-5-21-823518204-1326574676-725345543-
500\Software\Sysinternals\Regmon\Settings: AE 01 00 00 64 00 00 00 64 00 00 00 58 02 00

```
00 2C 01 00 00 23 00 00 00 5A 00 00 00 46 00 00 00 46 00 00 00 BE 00 00 00 47 00 00 00 DB
01 00 00 00 00 00 00 01 00 00 00 FF FF FF 00 FF 00 00 00 01 01 01 01 01 00 00 00 08 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 90 01 00 00 00 00 00 00 01 02 02 22 4D 53 20 53 61
6E 73 20 53 65 72 69 66 00 12 00 22 00 00 00 8C 2A F8 77 00 00 13 00 E8 0C 13 00
HKEY_USERS\S-1-5-21-823518204-1326574676-725345543-
500\Software\Sysinternals\Regmon\Settings: AE 01 00 00 04 00 00 00 3F 01 00 00 E2 03 00
00 42 01 00 00 23 00 00 00 5A 00 00 00 F7 00 00 00 46 00 00 00 60 01 00 00 47 00 00 00 DB
01 00 00 00 00 00 00 00 00 00 00 FF FF FF 00 FF 00 00 00 01 01 01 01 01 00 00 00 08 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 90 01 00 00 00 00 00 00 01 02 02 22 4D 53 20 53 61
6E 73 20 53 65 72 69 66 00 12 00 22 00 00 00 8C 2A F8 77 00 00 13 00 E8 0C 13 00
HKEY_USERS\S-1-5-21-823518204-1326574676-725345543-500\Software\Systems
Internals\Tdimon\Settings: 2C 01 00 00 17 00 00 00 D8 00 00 00 CF 03 00 00 99 01 00 00 23
00 00 00 28 00 00 00 74 00 00 00 5A 00 00 00 96 00 00 00 82 00 00 00 15 00 00 00 64 00 00
00 F4 00 00 00 00 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 90
01 00 00 00 00 00 00 01 02 02 22 4D 53 20 53 61 6E 73 20 53 65 72 69 66 00 CB 00 CC 00 CD
00 CE 00 CF 00 D0 00 D1 00 D2 00 D3 00 00 01 01 01 01 00 00 00 FF FF FF 00 FF 00 00 00 00
00 00 00 00 43 3A 5C 44 6F 63 75 6D 65 6E 74 73 20 61 6E 64 20 53 65 74 74 69 6E 67 73 5C
41 64 6D 69 6E 69 73 74 72 61 74 6F 72 5C 44 65 73 6B 74 6F 70 5C 54 64 69 6D 6F 6E 2E 6C
6F 67 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 01 01 01 00 00
00
HKEY_USERS\S-1-5-21-823518204-1326574676-725345543-500\Software\Systems
Internals\Tdimon\Settings: 2C 01 00 00 97 00 00 00 F6 00 00 00 CF 03 00 00 99 01 00 00 23
00 00 00 28 00 00 00 74 00 00 00 5A 00 00 00 96 00 00 00 82 00 00 00 15 00 00 00 64 00 00
00 F4 00 00 00 00 00 00 00 00 00 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 90
01 00 00 00 00 00 00 01 02 02 22 4D 53 20 53 61 6E 73 20 53 65 72 69 66 00 CB 00 CC 00 CD
00 CE 00 CF 00 D0 00 D1 00 D2 00 D3 00 00 01 01 01 01 00 00 00 FF FF FF 00 FF 00 00 00 00
00 00 00 00 43 3A 5C 44 6F 63 75 6D 65 6E 74 73 20 61 6E 64 20 53 65 74 74 69 6E 67 73 5C
41 64 6D 69 6E 69 73 74 72 61 74 6F 72 5C 44 65 73 6B 74 6F 70 5C 54 64 69 6D 6F 6E 2E 6C
6F 67 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 01 01 01 00 00
00

----------------------------------
Files added:4
----------------------------------
C:\Documents and Settings\Administrator\Desktop\Filemon.LOG
C:\Documents and Settings\Administrator\Recent\Filemon.LOG.lnk
C:\WINNT\system32\mfm\jtram.conf
C:\WINNT\system32\mfm\msrll.exe

----------------------------------
Files deleted:1
----------------------------------
C:\download\sanspractical\msrll.exe

----------------------------------
Files [attributes?] modified:14
----------------------------------
C:\Documents and Settings\Administrator\Cookies\index.dat
C:\Documents and Settings\Administrator\Desktop\Regmon.LOG
C:\Documents and Settings\Administrator\Desktop\Tdimon.log
C:\Documents and Settings\Administrator\Local Settings\History\History.IE5\index.dat
C:\Documents and Settings\Administrator\Local
Settings\History\History.IE5\MSHist012004081620040817\index.dat
C:\Documents and Settings\Administrator\Local Settings\Temporary Internet
Files\Content.IE5\index.dat
C:\Documents and Settings\Administrator\NTUSER.DAT
C:\Documents and Settings\Administrator\ntuser.dat.LOG
C:\Documents and Settings\Administrator\Recent\Regmon.LOG.lnk
C:\Documents and Settings\Administrator\Recent\Tdimon.log.lnk
```

```
C:\WINNT\system32\config\software
C:\WINNT\system32\config\software.LOG
C:\WINNT\system32\config\system
C:\WINNT\system32\config\SYSTEM.ALT

---------------------------------
Folders added:3
---------------------------------
C:\WINNT\system32\mfm
C:\WINNT\system32\mfm\.
C:\WINNT\system32\mfm\..

---------------------------------
Total changes:105
```

5.2.2. FileMon

Lets look at what FileMon logged during the execution of the binary. Only the interesting parts of the log file are listed.

These are the files that were read by the binary:

```
167     4:01:12 PM     msrll.exe:788  READ    C:\download\sanspractical\msrll.exe   SUCCESS
        Offset: 35328 Length: 2048

294     4:01:12 PM     msrll.exe:788  READ    C:\WINNT\System32\shell32.dll SUCCESS Offset:
0 Length: 12

408     4:01:12 PM     msrll.exe:1032 READ    C:\WINNT\system32\mfm\msrll.exe       SUCCESS
        Offset: 37376 Length: 4608

736     4:01:27 PM     msrll.exe:1032 READ    C:\WINNT\system32\msafd.dll   SUCCESS Offset:
0 Length: 32768

747     4:01:27 PM     msrll.exe:1032 READ    C:\WINNT\System32\wshtcpip.dll        SUCCESS
        Offset: 0 Length: 20480

854     4:01:28 PM     msrll.exe:1032 READ    C:\Documents and
Settings\Administrator\Local Settings\History\History.IE5\index.dat SUCCESS Offset: 4096
Length: 12288

981     4:01:28 PM     msrll.exe:1032 READ    C:\autoexec.bat        SUCCESS Offset: 0
Length: 0

1993    4:01:48 PM     msrll.exe:1032 READ    C:\WINNT\system32\rsabase.dll SUCCESS Offset:
0 Length: 32768
```

These are the files that were created by the binary:

```
168     4:01:12 PM     msrll.exe:788  CREATE  C:\WINNT\system32\mfm  SUCCESS Options:
Create Directory  Access: All
245     4:01:12 PM     msrll.exe:788  CREATE  C:\WINNT\system32\mfm\msrll.exe       SUCCESS
        Options: OverwriteIf Sequential  Access: All
521     4:01:12 PM     msrll.exe:1032 CREATE  C:\WINNT\system32\mfm  NAME COLLISION
        Options: Create Directory  Access: All
1984    4:01:48 PM     msrll.exe:1032 CREATE  C:\WINNT\system32\mfm\jtram.conf      SUCCESS
        Options: OverwriteIf  Access: All
```

These are the files that were deleted by the binary:

```
480     4:01:12 PM     msrll.exe:1032 DELETE  C:\download\sanspractical\msrll.exe   SUCCESS
```

These are the files that were opened by the binary:

```
118     4:01:11 PM     explorer.exe:540       OPEN    C:\download\sanspractical\msrll.exe
        SUCCESS Options: Open  Access: All
127     4:01:11 PM     explorer.exe:540       OPEN    C:\download\sanspractical\msrll.exe
        SUCCESS Options: Open  Access: Execute
133     4:01:12 PM     explorer.exe:540       OPEN    C:\download\sanspractical\msrll.exe
        SUCCESS Options: Open  Access: Execute
141     4:01:12 PM     msrll.exe:788  OPEN    C:\download\sanspractical     SUCCESS
        Options: Open Directory  Access: Traverse
149     4:01:12 PM     msrll.exe:788  OPEN    C:\WINNT\system32\ws2_32.dll  SUCCESS
        Options: Open  Access: Execute
154     4:01:12 PM     msrll.exe:788  OPEN    C:\WINNT\system32\WS2HELP.DLL SUCCESS
        Options: Open  Access: Execute
171     4:01:12 PM     msrll.exe:788  OPEN    C:\WINNT\system32\mfm  SUCCESS Options: Open
Directory  Access: Traverse
238     4:01:12 PM     msrll.exe:788  OPEN    C:\download\sanspractical\msrll.exe   SUCCESS
        Options: Open Sequential  Access: All
253     4:01:12 PM     msrll.exe:788  OPEN    C:\WINNT\system32\rpcss.dll   SUCCESS
        Options: Open  Access: Execute
257     4:01:12 PM     msrll.exe:788  OPEN    C:\     SUCCESS Options: Open Directory
Access: All
264     4:01:12 PM     msrll.exe:788  OPEN    C:\     SUCCESS Options: Open Directory
Access: All
277     4:01:12 PM     msrll.exe:788  OPEN    C:\WINNT\system32\CLBCATQ.DLL SUCCESS
        Options: Open  Access: Execute
282     4:01:12 PM     msrll.exe:788  OPEN    C:\WINNT\system32\cscui.dll   SUCCESS
        Options: Open  Access: Execute
287     4:01:12 PM     msrll.exe:788  OPEN    C:\WINNT\system32\CSCDLL.DLL  SUCCESS
        Options: Open  Access: Execute
291     4:01:12 PM     msrll.exe:788  OPEN    C:\WINNT\System32\shell32.dll SUCCESS
        Options: Open  Access: All
298     4:01:12 PM     msrll.exe:788  OPEN    C:\WINNT\      SUCCESS Options: Open
Directory  Access: All
301     4:01:12 PM     msrll.exe:788  OPEN    C:\WINNT\system32\     SUCCESS Options: Open
Directory  Access: All
305     4:01:12 PM     msrll.exe:788  OPEN    C:\WINNT\system32\mfm\ SUCCESS Options: Open
Directory  Access: All
309     4:01:12 PM     msrll.exe:788  OPEN    C:\     SUCCESS Options: Open Directory
Access: All
312     4:01:12 PM     msrll.exe:788  OPEN    C:\WINNT\      SUCCESS Options: Open
Directory  Access: All
315     4:01:12 PM     msrll.exe:788  OPEN    C:\WINNT\system32\     SUCCESS Options: Open
Directory  Access: All
318     4:01:12 PM     msrll.exe:788  OPEN    C:\WINNT\system32\mfm\ SUCCESS Options: Open
Directory  Access: All
324     4:01:12 PM     msrll.exe:788  OPEN    C:\WINNT\system32\MSI.DLL     SUCCESS
        Options: Open  Access: Execute
392     4:01:12 PM     msrll.exe:788  OPEN    C:\WINNT\system32\mfm\msrll.exe       SUCCESS
        Options: Open  Access: All
402     4:01:12 PM     msrll.exe:788  OPEN    C:\WINNT\system32\mfm\msrll.exe       SUCCESS
        Options: Open  Access: Execute
407     4:01:12 PM     msrll.exe:1032 OPEN    C:\WINNT\system32\mfm  SUCCESS Options: Open
Directory  Access: Traverse
412     4:01:12 PM     msrll.exe:1032 OPEN    C:\WINNT\system32\ws2_32.dll  SUCCESS
        Options: Open  Access: Execute
417     4:01:12 PM     msrll.exe:1032 OPEN    C:\WINNT\system32\WS2HELP.DLL SUCCESS
        Options: Open  Access: Execute
431     4:01:12 PM     Regmon.exe:988 OPEN    C:\download\sanspractical\msrll.exe   SUCCESS
        Options: Open  Access: All
520     4:01:12 PM     msrll.exe:1032 OPEN    C:\download\sanspractical\msrll.exe   FILE
NOT FOUND      Options: Open  Access: All
544     4:01:13 PM     procexp.exe:504        OPEN    C:\WINNT\system32\mfm\msrll.exe
        SUCCESS Options: Open  Access: Execute
548     4:01:13 PM     procexp.exe:504        OPEN    C:\WINNT\system32\mfm\msrll.exe
        SUCCESS Options: Open  Access: All
731     4:01:27 PM     msrll.exe:1032 OPEN    C:\WINNT\system32\mfm\jtram.conf      FILE
NOT FOUND      Options: Open  Access: All
733     4:01:27 PM     msrll.exe:1032 OPEN    C:\WINNT\system32\msafd.dll   SUCCESS
        Options: Open  Access: Execute
```

```
738     4:01:27 PM     msrll.exe:1032 OPEN    C:\WINNT\system32\msafd.dll   SUCCESS
        Options: Open  Access: Execute
744     4:01:27 PM     msrll.exe:1032 OPEN    C:\WINNT\System32\wshtcpip.dll        SUCCESS
        Options: Open  Access: Execute
749     4:01:27 PM     msrll.exe:1032 OPEN    C:\WINNT\System32\wshtcpip.dll        SUCCESS
        Options: Open  Access: Execute
783     4:01:28 PM     msrll.exe:1032 OPEN    C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files      SUCCESS Options: Open
Access: All
800     4:01:28 PM     msrll.exe:1032 OPEN    C:\Documents and
Settings\Administrator\Local Settings\History        SUCCESS Options: Open  Access: All
804     4:01:28 PM     msrll.exe:1032 OPEN    C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\        SUCCESS
        Options: Open Directory  Access: All
807     4:01:28 PM     msrll.exe:1032 OPEN    C:\     SUCCESS Options: Open Directory
Access: All
812     4:01:28 PM     msrll.exe:1032 OPEN    C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\        SUCCESS
        Options: Open  Access: All
815     4:01:28 PM     msrll.exe:1032 OPEN    C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\index.dat
        SUCCESS Options: OpenIf  Access: All
819     4:01:28 PM     msrll.exe:1032 OPEN    C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\index.dat
        SUCCESS Options: OpenIf  Access: All
821     4:01:28 PM     msrll.exe:1032 OPEN    C:\Documents and
Settings\Administrator\Cookies\       SUCCESS Options: Open Directory  Access: All
824     4:01:28 PM     msrll.exe:1032 OPEN    C:\     SUCCESS Options: Open Directory
Access: All
829     4:01:28 PM     msrll.exe:1032 OPEN    C:\Documents and
Settings\Administrator\Cookies\       SUCCESS Options: Open  Access: All
832     4:01:28 PM     msrll.exe:1032 OPEN    C:\Documents and
Settings\Administrator\Cookies\index.dat     SUCCESS Options: OpenIf  Access: All
836     4:01:28 PM     msrll.exe:1032 OPEN    C:\Documents and
Settings\Administrator\Cookies\index.dat     SUCCESS Options: OpenIf  Access: All
838     4:01:28 PM     msrll.exe:1032 OPEN    C:\Documents and
Settings\Administrator\Local Settings\History\History.IE5\  SUCCESS Options: Open
Directory  Access: All
841     4:01:28 PM     msrll.exe:1032 OPEN    C:\     SUCCESS Options: Open Directory
Access: All
846     4:01:28 PM     msrll.exe:1032 OPEN    C:\Documents and
Settings\Administrator\Local Settings\History\History.IE5\  SUCCESS Options: Open  Access:
All
849     4:01:28 PM     msrll.exe:1032 OPEN    C:\Documents and
Settings\Administrator\Local Settings\History\History.IE5\index.dat SUCCESS Options:
OpenIf  Access: All
853     4:01:28 PM     msrll.exe:1032 OPEN    C:\Documents and
Settings\Administrator\Local Settings\History\History.IE5\index.dat SUCCESS Options:
OpenIf  Access: All
856     4:01:28 PM     msrll.exe:1032 OPEN    C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\        SUCCESS
        Options: Open  Access: All
861     4:01:28 PM     msrll.exe:1032 OPEN    C:\Documents and
Settings\Administrator\Local Settings\History\History.IE5\  SUCCESS Options: Open  Access:
All
875     4:01:28 PM     msrll.exe:1032 OPEN    C:\WINNT\system32\RASAPI32.DLL        SUCCESS
        Options: Open  Access: Execute
880     4:01:28 PM     msrll.exe:1032 OPEN    C:\WINNT\system32\RASMAN.DLL  SUCCESS
        Options: Open  Access: Execute
885     4:01:28 PM     msrll.exe:1032 OPEN    C:\WINNT\system32\TAPI32.DLL  SUCCESS
        Options: Open  Access: Execute
890     4:01:28 PM     msrll.exe:1032 OPEN    C:\WINNT\system32\RTUTILS.DLL SUCCESS
        Options: Open  Access: Execute
896     4:01:28 PM     msrll.exe:1032 OPEN    C:\WINNT\system32\sensapi.dll SUCCESS
        Options: Open  Access: Execute
906     4:01:28 PM     msrll.exe:1032 OPEN    C:\WINNT\system32\USERENV.DLL SUCCESS
        Options: Open  Access: Execute
913     4:01:28 PM     msrll.exe:1032 OPEN    C:\WINNT\system32\netapi32.dll        SUCCESS
        Options: Open  Access: Execute
918     4:01:28 PM     msrll.exe:1032 OPEN    C:\WINNT\system32\Secur32.dll SUCCESS
        Options: Open  Access: Execute
```

```
923     4:01:28 PM     msrll.exe:1032 OPEN    C:\WINNT\system32\NTDSAPI.dll SUCCESS
        Options: Open  Access: Execute
928     4:01:28 PM     msrll.exe:1032 OPEN    C:\WINNT\system32\DNSAPI.DLL  SUCCESS
        Options: Open  Access: Execute
933     4:01:28 PM     msrll.exe:1032 OPEN    C:\WINNT\system32\WSOCK32.DLL SUCCESS
        Options: Open  Access: Execute
938     4:01:28 PM     msrll.exe:1032 OPEN    C:\WINNT\system32\NETRAP.dll  SUCCESS
        Options: Open  Access: Execute
943     4:01:28 PM     msrll.exe:1032 OPEN    C:\WINNT\system32\SAMLIB.dll  SUCCESS
        Options: Open  Access: Execute
979     4:01:28 PM     msrll.exe:1032 OPEN    C:\autoexec.bat       SUCCESS Options: Open
Access: All
984     4:01:28 PM     msrll.exe:1032 OPEN    C:\     SUCCESS Options: Open Directory
Access: All
987     4:01:28 PM     msrll.exe:1032 OPEN    C:\Documents and Settings\    SUCCESS
        Options: Open Directory  Access: All
990     4:01:28 PM     msrll.exe:1032 OPEN    C:\Documents and Settings\Administrator\
        SUCCESS Options: Open Directory  Access: All
994     4:01:28 PM     msrll.exe:1032 OPEN    C:\     SUCCESS Options: Open Directory
Access: All
997     4:01:28 PM     msrll.exe:1032 OPEN    C:\Documents and Settings\    SUCCESS
        Options: Open Directory  Access: All
1000    4:01:28 PM     msrll.exe:1032 OPEN    C:\Documents and Settings\Administrator\
        SUCCESS Options: Open Directory  Access: All
1004    4:01:28 PM     msrll.exe:1032 OPEN    C:\Documents and Settings\All
Users\Application Data\Microsoft\Network\Connections\Pbk\   SUCCESS Options: Open
Directory  Access: All
1007    4:01:28 PM     msrll.exe:1032 OPEN    C:\WINNT\system32\Ras\ SUCCESS Options: Open
Directory  Access: All
1012    4:01:28 PM     msrll.exe:1032 OPEN    C:\autoexec.bat       SUCCESS Options: Open
Access: All
1017    4:01:28 PM     msrll.exe:1032 OPEN    C:\     SUCCESS Options: Open Directory
Access: All
1020    4:01:28 PM     msrll.exe:1032 OPEN    C:\Documents and Settings\    SUCCESS
        Options: Open Directory  Access: All
1023    4:01:28 PM     msrll.exe:1032 OPEN    C:\Documents and Settings\Administrator\
        SUCCESS Options: Open Directory  Access: All
1027    4:01:28 PM     msrll.exe:1032 OPEN    C:\     SUCCESS Options: Open Directory
Access: All
1030    4:01:28 PM     msrll.exe:1032 OPEN    C:\Documents and Settings\    SUCCESS
        Options: Open Directory  Access: All
1033    4:01:28 PM     msrll.exe:1032 OPEN    C:\Documents and Settings\Administrator\
        SUCCESS Options: Open Directory  Access: All
1037    4:01:28 PM     msrll.exe:1032 OPEN    C:\Documents and
Settings\Administrator\Application Data\Microsoft\Network\Connections\Pbk\ PATH NOT FOUND
        Options: Open Directory  Access: All
1043    4:01:28 PM     msrll.exe:1032 OPEN    C:\WINNT\System32\rnr20.dll   SUCCESS
        Options: Open  Access: Execute
1047    4:01:28 PM     msrll.exe:1032 OPEN    C:\WINNT\System32\rnr20.dll   SUCCESS
        Options: Open  Access: Execute
1052    4:01:28 PM     msrll.exe:1032 OPEN    C:\WINNT\system32\iphlpapi.dll       SUCCESS
        Options: Open  Access: Execute
1057    4:01:28 PM     msrll.exe:1032 OPEN    C:\WINNT\system32\ICMP.DLL    SUCCESS
        Options: Open  Access: Execute
1062    4:01:28 PM     msrll.exe:1032 OPEN    C:\WINNT\system32\MPRAPI.DLL  SUCCESS
        Options: Open  Access: Execute
1067    4:01:28 PM     msrll.exe:1032 OPEN    C:\WINNT\system32\ACTIVEDS.DLL       SUCCESS
        Options: Open  Access: Execute
1072    4:01:28 PM     msrll.exe:1032 OPEN    C:\WINNT\system32\ADSLDPC.DLL SUCCESS
        Options: Open  Access: Execute
1077    4:01:28 PM     msrll.exe:1032 OPEN    C:\WINNT\system32\SETUPAPI.DLL       SUCCESS
        Options: Open  Access: Execute
1082    4:01:28 PM     msrll.exe:1032 OPEN    C:\WINNT\system32\DHCPCSVC.DLL       SUCCESS
        Options: Open  Access: Execute
1085    4:01:28 PM     msrll.exe:1032 OPEN    C:\WINNT\System32\winrnr.dll  SUCCESS
        Options: Open  Access: Execute
1089    4:01:28 PM     msrll.exe:1032 OPEN    C:\WINNT\System32\winrnr.dll  SUCCESS
        Options: Open  Access: Execute
1979    4:01:48 PM     msrll.exe:1032 OPEN    C:\WINNT\system32\rasadhlp.dll       SUCCESS
        Options: Open  Access: Execute
```

```
1983    4:01:48 PM     msrll.exe:1032 OPEN    C:\WINNT\system32\mfm\jtram.conf      FILE
NOT FOUND      Options: Open  Access: All
1985    4:01:48 PM     msrll.exe:1032 OPEN    C:\dev\random  PATH NOT FOUND Options: Open
Access: All
1986    4:01:48 PM     msrll.exe:1032 OPEN    C:\WINNT\system32\mfm\rsabase.dll     FILE
NOT FOUND      Options: Open  Access: All
1991    4:01:48 PM     msrll.exe:1032 OPEN    C:\WINNT\system32\rsabase.dll SUCCESS
        Options: Open  Access: All
2104    4:01:49 PM     msrll.exe:1032 OPEN    C:\dev\random  PATH NOT FOUND Options: Open
Access: All
```

These are the files that were written to by the binary:

```
245     4:01:12 PM     msrll.exe:788  CREATE  C:\WINNT\system32\mfm\msrll.exe       SUCCESS
        Options: OverwriteIf Sequential  Access: All
248     4:01:12 PM     msrll.exe:788  WRITE   C:\WINNT\system32\mfm\msrll.exe       SUCCESS
        Offset: 0 Length: 41984
1984    4:01:48 PM     msrll.exe:1032 CREATE  C:\WINNT\system32\mfm\jtram.conf      SUCCESS
        Options: OverwriteIf  Access: All
```

5.2.3. TDIMon

Looking at the TDIMon output, the following ports are being opened on the local machine:

```
7  47.29260898  msrll.exe:1032  811E2E88  IRP_MJ_CREATE  TCP:0.0.0.0:2200  Address Open

122  68.64820976  msrll.exe:1032  81316A88  IRP_MJ_CREATE  TCP:0.0.0.0:113  Address Open
```

The TCP ports 113 and 2200 are opened and listening for incoming connections.

5.2.4. Summary

The following changes stand out:

- a directory gets created, `C:\WINNT\system32\mfm`
- the binary gets copied over into the newly created directory
- the binary is identical with the original EXE file, as md5sum proves:

original file:

```
C:\download\sanspractical>md5sum msrll.zip
696c78651244b1ad0363a400a23d48ef *msrll.zip

C:\download\sanspractical>md5sum msrll.exe
84acfe96a98590813413122c12c11aaa *msrll.exe
```

created file in `C:\WINNT\system32\mfm:`

MD5 hashes match for the EXE files.

- a system service gets added, “RLL enhanced drive”, which loads up the binary automatically at each system boot, from its new location
- a configuration file gets created, “jtram.conf” in the directory `C:\WINNT\system32\mfm`
- the old binary gets deleted
- 2 ports are opened up on the local machine itself, TCP 113 and TCP 2200

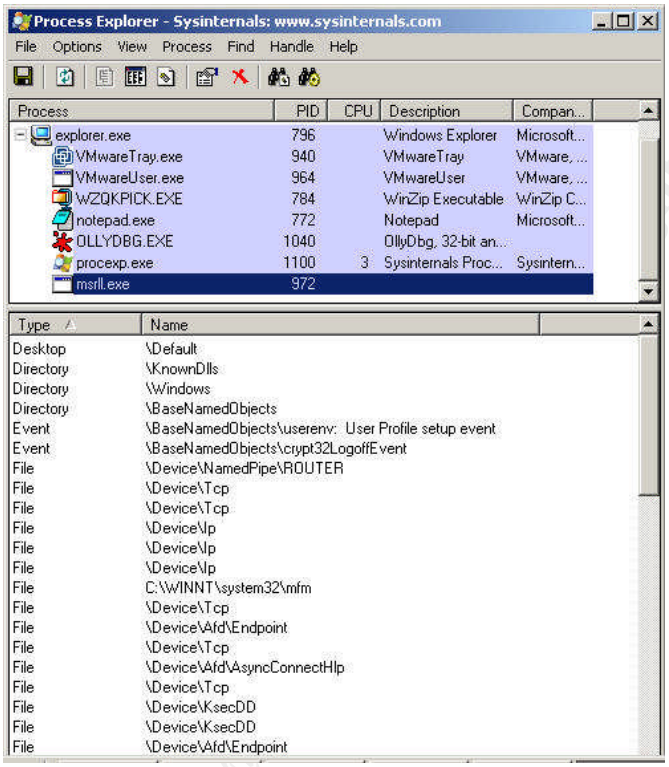
Something else stands out when inspecting the FileMon output: msrll.exe queries the file index.dat [INDEXDAT] in the Temporary Internet Files-Folder of the Administrator:

```
23381   6:31:16 PM     msrll.exe:1108 QUERY INFORMATION     C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\index.dat
        SUCCESS Length: 212992
23382   6:31:47 PM     msrll.exe:1108 QUERY INFORMATION     C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\index.dat
        SUCCESS Length: 212992
23383   6:31:47 PM     msrll.exe:1108 QUERY INFORMATION     C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\index.dat
        SUCCESS Length: 212992
23384   6:32:18 PM     msrll.exe:1108 QUERY INFORMATION     C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\index.dat
        SUCCESS Length: 212992
23385   6:32:18 PM     msrll.exe:1108 QUERY INFORMATION     C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\index.dat
        SUCCESS Length: 212992
23386   6:32:49 PM     msrll.exe:1108 QUERY INFORMATION     C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\index.dat
        SUCCESS Length: 212992
23387   6:32:49 PM     msrll.exe:1108 QUERY INFORMATION     C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\index.dat
        SUCCESS Length: 212992
23388   6:33:20 PM     msrll.exe:1108 QUERY INFORMATION     C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\index.dat
        SUCCESS Length: 212992
23389   6:33:20 PM     msrll.exe:1108 QUERY INFORMATION     C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\index.dat
        SUCCESS Length: 212992
23390   6:33:51 PM     msrll.exe:1108 QUERY INFORMATION     C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\index.dat
        SUCCESS Length: 212992
23391   6:33:51 PM     msrll.exe:1108 QUERY INFORMATION     C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\index.dat
        SUCCESS Length: 212992
23392   6:34:22 PM     msrll.exe:1108 QUERY INFORMATION     C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\index.dat
        SUCCESS Length: 212992
[…]
23396   6:35:24 PM     msrll.exe:1108 QUERY INFORMATION     C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\index.dat
        SUCCESS Length: 212992
23397   6:35:24 PM     msrll.exe:1108 QUERY INFORMATION     C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\index.dat
        SUCCESS Length: 212992
23398   6:35:55 PM     msrll.exe:1108 QUERY INFORMATION     C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\index.dat
        SUCCESS Length: 212992
23399   6:35:55 PM     msrll.exe:1108 QUERY INFORMATION     C:\Documents and
Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\index.dat
        SUCCESS Length: 212992
```

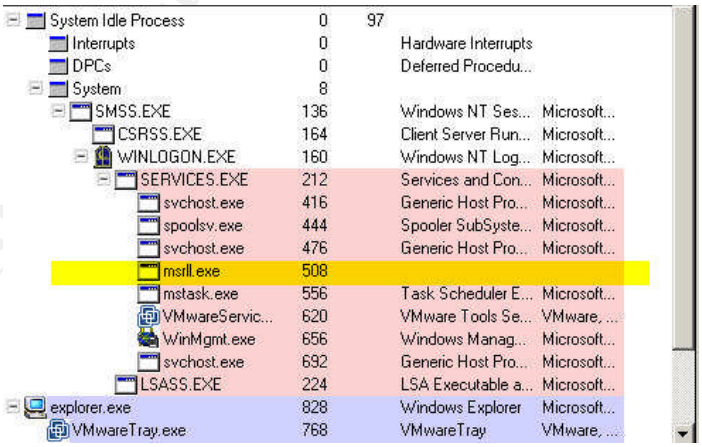
This seems to happen about every 30 seconds while the binary is running.

5.2.5. Processes

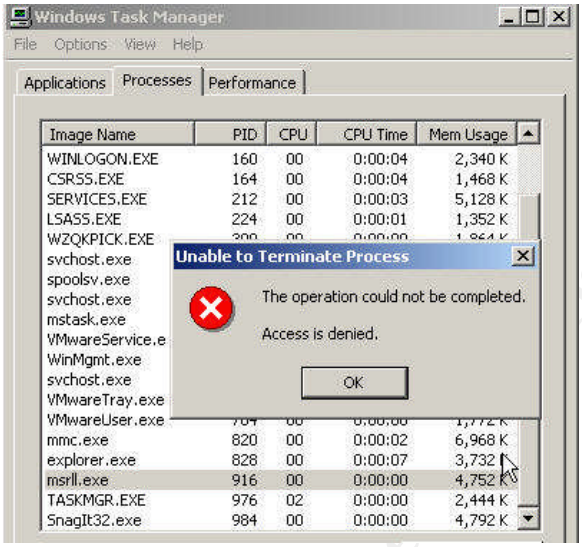
Whether the binary is executed by itself or within OllyDbg, the process ‘msrll.exe’ shows up in the process list.



Once it has installed itself as a system service and the system has been rebooted, it shows up in the list of running services:



The ‘service’ can be killed using the process explorer, but not by using the standard Windows Taskmanager.



At any rate, hiding the process would have increased the stealthiness. Maybe the supplied specimen was less advanced then later versions that actually would hide the process, or it was desired by the author to show the process as running.

5.2.6. jtram.conf

Lets look at the string contents of jtram.conf, the file that gets created when msrll.exe is executed for the first time.

```
File pos   Mem pos      ID   Text
========   =======      ==   ====
00000000   00000000      0   YwERACWWtLmMJ1BGq7OafIjzfhtrOxAnI/gkYkxNEDKmYu6qYA==
eP8RAAnm4N9SN3W34KwIOuq5u4y9jMeXfPFm+Va+715NSfdQmw==
tP4RALAs5s7ZiwjH/QWkDrAIw04yvOL7DazoPVXXgltgM9Vv2g==
000000A0   000000A0      0   Wv8RAIW6pQGDE/ZsHFuPMAW85AWttWajSl8yCia7Gk4l1Rfy8A==
qQARAAxCnuiXUXrefF+26NK1g0iHzipKp7s/bbXNZV5kBZ9ZPA==
qvwRAPZWhZSXtZQ0jvGNbZX1Jb46ga0l2NWg2h2jBWdliTZpzQ==
00000140   00000140      0   VQARADaYGT1fO5/MHN76Akp23C8bym1NZiSlh+iWJLSfXOSjLQ==
yf8RALKhz4WqyWJQv7FqRN53/ZhGT8NpDPZe3IQpolNf92qG/w==
FQBKABuIsNFPEBkWP/dLu/NyH5vxCjbk/9jVHxCBlaRovHbGvkYOqdF66nfgb6ggxjnxWuOpXwG44XCdZvF/R+/RQ
PLaRtFJxaZb2lvJlq9fdY6do4YIOF/QCCBW8w==
0000022C   0000022C      0   cAARAEit4e27m/HVY/Q8L6rWc1JucDrLdVKG97Ze3xDIMxGVrg==
T/8RAAF1GAhw1IeKWCOU7qofjq2r91TCBGcvM5isRhzWHEwA6Q==
Mv4RAFSdMBo0o4C3DoebJKNDjgZKuz9iyACC8Q8xwFPSBdBE6w==
000002CC   000002CC      0   QgERAA80I6khdJu1Ns7H5BxGj7Jvn1YYbhwOTkQMGznacx/5gA==
h/4RAMm7qZUb6r3l/s3NjFAMQjtdpk5w+zUwhWv1ksWyfaRDnQ==
VQIjAHaiyUg7lpGGd4I3VHpsDDGVGwpcYEOMR/SVeiMMcnc1JlkKa49+qqiQmnUbM665RzWb4A==
00000384   00000384      0   ZwARAKFwO9ssrjZEqr5zvKCmbZvRV0POehvdRtEOjYI2fSd3xg==
8P4RABYSiGPlZyqA+2kmc5ROOQUeAhbC3kaKlKdMmy0Us5WA6A==
pP8jALz70I4nSAWuDJdC2JWCO65p+ykra6EvhDayFN4MNweHPVEGuz842Dx+V7Sy5HS9FgJ1tA==
```

The content looks encrypted. That might explain why msrll.exe made use of the RSABASE.DLL, the encryption library.

5.3. Behaviour of the Binary on the network

As mentioned in the lab setup section, the Windows virtual machine that is executing the binary, the Linux host and the VMWare host system share one host-only private network that is separated from everything else. The Linux machine is running snort to monitor the network traffic that is being generated by the infected Windows system.

For clarification:

- 192.168.58.129 is the Windows guest system executing the malicious binary
- 192.168.58.128 is the Linux guest system running snort and other services we may run
- 192.168.58.1 is the VMWare host system

5.3.1. First network trace

```
07/20-08:16:49.479663 ARP who-has 192.168.58.1 tell 192.168.58.129

07/20-08:16:49.479695 ARP reply 192.168.58.1 is-at 0:50:56:C0:0:1

07/20-08:16:49.479713 192.168.58.1 -> 192.168.58.129
ICMP TTL:128 TOS:0x0 ID:27166 IpLen:20 DgmLen:56
Type:3  Code:3  DESTINATION UNREACHABLE: PORT UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
192.168.58.129:1703 -> 192.168.58.1:53
UDP TTL:128 TOS:0x0 ID:3999 IpLen:20 DgmLen:66
Len: 38
** END OF DUMP
00 00 00 00 45 00 00 42 0F 9F 00 00 80 11 35 39  ....E..B......59
C0 A8 3A 81 C0 A8 3A 01 06 A7 00 35 00 2E B3 A0  ..:...:....5....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-08:16:49.479720 192.168.58.129:1703 -> 192.168.58.1:53
UDP TTL:128 TOS:0x0 ID:3999 IpLen:20 DgmLen:66
Len: 38
B7 81 01 00 00 01 00 00 00 00 00 0B 63 6F 6C  ............col
6C 65 63 74 69 76 65 37 04 7A 78 79 30 03 63 6F  lective7.zxy0.co
6D 00 00 01 00 01                               m.....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-08:16:49.479727 192.168.58.1 -> 192.168.58.129
ICMP TTL:128 TOS:0x0 ID:27167 IpLen:20 DgmLen:56
Type:3  Code:3  DESTINATION UNREACHABLE: PORT UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
192.168.58.129:1703 -> 192.168.58.1:53
UDP TTL:128 TOS:0x0 ID:4000 IpLen:20 DgmLen:66
Len: 38
** END OF DUMP
00 00 00 00 45 00 00 42 0F A0 00 00 80 11 35 38  ....E..B......58
C0 A8 3A 81 C0 A8 3A 01 06 A7 00 35 00 2E B3 A0  ..:...:....5....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-08:16:49.479735 192.168.58.129:1703 -> 192.168.58.1:53
UDP TTL:128 TOS:0x0 ID:4000 IpLen:20 DgmLen:66
Len: 38
B7 81 01 00 00 01 00 00 00 00 00 0B 63 6F 6C  ............col
6C 65 63 74 69 76 65 37 04 7A 78 79 30 03 63 6F  lective7.zxy0.co
6D 00 00 01 00 01                               m.....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-08:16:49.479741 192.168.58.1 -> 192.168.58.129
ICMP TTL:128 TOS:0x0 ID:27168 IpLen:20 DgmLen:56
```

```
Type:3  Code:3  DESTINATION UNREACHABLE: PORT UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
192.168.58.129:1703 -> 192.168.58.1:53
UDP TTL:128 TOS:0x0 ID:4001 IpLen:20 DgmLen:66
Len: 38
** END OF DUMP
00 00 00 00 45 00 00 42 0F A1 00 00 80 11 35 37  ....E..B......57
C0 A8 3A 81 C0 A8 3A 01 06 A7 00 35 00 2E B3 A0  ..:...:....5....
```

The infected Windows machine tries to do a DNS lookup for collective7.zxy0.com, using its gateway (the VMWare host system) as DNS server. Of course, no DNS service is running on that machine, so the DNS query fails.

5.3.2. Fixing DNS

In order to see what the infected system does when DNS succeeds, we will need to make sure that it assumes that collective7.zxy0.com resolves to a reachable, yet secure, host. Hence we will add a hosts entry on the infected system to point collective7.zxy0.com to 192.168.58.128, the Linux guest system that resides in the same protected network.

Steps to undertake:

- terminate the msrll.exe process
- modify the hosts file
- restart the msrll.exe process
- monitor the network

5.3.2.1. Modifying the hosts file

The hosts file resides in C:\WINNT\system32\drivers\etc. It will be modified to look like this:

```
[…]
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

127.0.0.1       localhost
192.168.58.128  collective7.zxy0.com

[…]
```

5.3.2.2. Testing the changes

After restarting the msrll.exe from C:\WINNT\system32\mfm (since the original binary was deleted when it was first executed), the network traces show the following:

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-14:53:21.992961 192.168.58.129:2757 -> 192.168.58.128:6667
TCP TTL:128 TOS:0x0 ID:8260 IpLen:20 DgmLen:48
******S* Seq: 0x982813AE  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

```
07/20-14:53:21.993091 192.168.58.128:6667 -> 192.168.58.129:2757
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:40 DF
***A*R** Seq: 0x0  Ack: 0x982813AF  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-14:53:22.534478 192.168.58.129:2757 -> 192.168.58.128:6667
TCP TTL:128 TOS:0x0 ID:8261 IpLen:20 DgmLen:48
******S* Seq: 0x982813AE  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[...]


=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-14:53:53.159226 192.168.58.129:2758 -> 192.168.58.128:9999
TCP TTL:128 TOS:0x0 ID:8263 IpLen:20 DgmLen:48
******S* Seq: 0x9895ED4D  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-14:53:53.159429 192.168.58.128:9999 -> 192.168.58.129:2758
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:40 DF
***A*R** Seq: 0x0  Ack: 0x9895ED4E  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

[...]

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-14:54:24.126226 192.168.58.129:2759 -> 192.168.58.128:8080
TCP TTL:128 TOS:0x0 ID:8266 IpLen:20 DgmLen:48
******S* Seq: 0x9902CF04  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-14:54:24.126414 192.168.58.128:8080 -> 192.168.58.129:2759
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:40 DF
***A*R** Seq: 0x0  Ack: 0x9902CF05  Win: 0x0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

msrll.exe obviously accepts ‘our’ IP for collective7.zxy0.com and tries to connect to the ports 6667, 9999 and 8080 on the machine. No services are running on those ports of course, so we will start netcat in listen mode to listen on those ports, in order to see what kind of data is transmitted.

5.3.2.3. Running Netcat

We will start netcat (nc) as following, each one in a separate console on the Linux system:

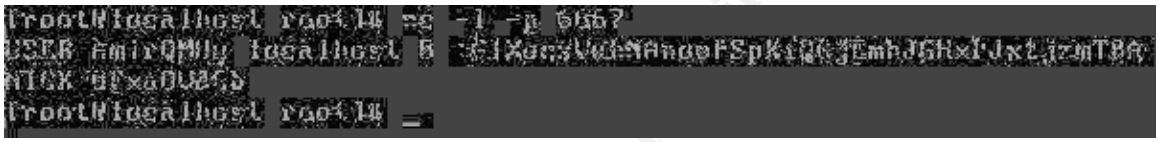
Console 2:
nc –l –p 6667

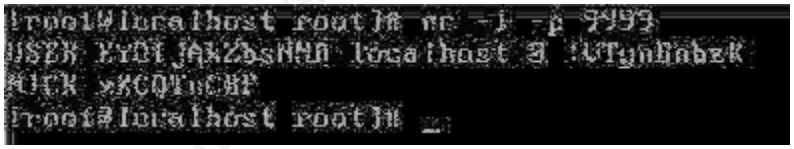
Console 3:
nc –l –p 8080

Console 4:
nc –l –p 9999

We now restart msrll.exe and see what data will be transmitted when connected to those ports.

The consoles show the following:





This is a typical IRC server connection attempt. Msrll.exe tries to connect to external IRC servers.

To see whether this assumption is true or not, we will start an IRC daemon on port 6667. At the same time, the binary will be monitored to see if it still tries to establish connections to the other ports above, 8080 and 9999. We achieve this by letting nc listen on those ports.

IRC server running on port 6667, netcat listening on ports 8080 and 9999

After msrll.exe was restarted, we see different traffic patterns:

```
07/20-16:49:06.202784 192.168.58.129:2827 -> 192.168.58.128:6667
TCP TTL:128 TOS:0x0 ID:8492 IpLen:20 DgmLen:48
******S* Seq: 0xF706FF59  Ack: 0x0  Win: 0x4000  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-16:49:06.202902 192.168.58.128:6667 -> 192.168.58.129:2827
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:48 DF
***A**S* Seq: 0xC42BB5A4  Ack: 0xF706FF5A  Win: 0x16D0  TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

```
07/20-16:49:06.206272 192.168.58.129:2827 -> 192.168.58.128:6667
TCP TTL:128 TOS:0x0 ID:8493 IpLen:20 DgmLen:40
***A**** Seq: 0xF706FF5A  Ack: 0xC42BB5A5  Win: 0x4470  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-16:49:06.207006 192.168.58.128:6667 -> 192.168.58.129:2827
TCP TTL:64 TOS:0x0 ID:54878 IpLen:20 DgmLen:86 DF
***AP*** Seq: 0xC42BB5A5  Ack: 0xF706FF5A  Win: 0x16D0  TcpLen: 20
4E 4F 54 49 43 45 20 41 55 54 48 20 3A 2A 2A 2A  NOTICE AUTH :***
20 4C 6F 6F 6B 69 6E 67 20 75 70 20 79 6F 75 72   Looking up your
20 68 6F 73 74 6E 61 6D 65 2E 2E 2E 0D 0A         hostname.....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-16:49:06.207668 192.168.58.128:1025 -> 192.168.58.1:53
UDP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:73 DF
Len: 45
31 20 01 00 00 01 00 00 00 00 00 00 03 31 32 39  1 ...........129
02 35 38 03 31 36 38 03 31 39 32 07 69 6E 2D 61  .58.168.192.in-a
64 64 72 04 61 72 70 61 00 00 0C 00 01           ddr.arpa.....

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-16:49:06.207818 ARP reply 192.168.58.128 is-at 0:C:29:56:36:3F

07/20-16:49:06.207859 192.168.58.1 -> 192.168.58.128
ICMP TTL:128 TOS:0x0 ID:30021 IpLen:20 DgmLen:56
Type:3  Code:3  DESTINATION UNREACHABLE: PORT UNREACHABLE
** ORIGINAL DATAGRAM DUMP:
192.168.58.128:1025 -> 192.168.58.1:53
UDP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:73 DF
Len: 45
** END OF DUMP
00 00 00 00 45 00 00 49 00 00 40 00 40 11 44 D2  ....E..I..@.@.D.
C0 A8 3A 80 C0 A8 3A 01 04 01 00 35 00 35 4B 32  ..:...:....5.5K2

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-16:49:06.221702 192.168.58.128:1165 -> 192.168.58.129:113
TCP TTL:64 TOS:0x0 ID:43904 IpLen:20 DgmLen:60 DF
******S* Seq: 0xC41FC87C  Ack: 0x0  Win: 0x16D0  TcpLen: 40
TCP Options (5) => MSS: 1460 SackOK TS: 14443516 0 NOP WS: 0

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-16:49:06.231330 192.168.58.129:113 -> 192.168.58.128:1165
TCP TTL:128 TOS:0x0 ID:8494 IpLen:20 DgmLen:64
***A**S* Seq: 0xF7085004  Ack: 0xC41FC87D  Win: 0x4470  TcpLen: 44
TCP Options (9) => MSS: 1460 NOP WS: 0 NOP NOP TS: 0 0 NOP NOP SackOK

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-16:49:06.271008 192.168.58.128:6667 -> 192.168.58.129:2827
TCP TTL:64 TOS:0x0 ID:54879 IpLen:20 DgmLen:73 DF
***AP*** Seq: 0xC42BB5D3  Ack: 0xF706FF5A  Win: 0x16D0  TcpLen: 20
4E 4F 54 49 43 45 20 41 55 54 48 20 3A 2A 2A 2A  NOTICE AUTH :***
20 43 68 65 63 6B 69 6E 67 20 49 64 65 6E 74 0D   Checking Ident.
0A                                               .
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-16:49:06.430678 192.168.58.129:2827 -> 192.168.58.128:6667
TCP TTL:128 TOS:0x0 ID:8497 IpLen:20 DgmLen:40
***A**** Seq: 0xF706FF5A  Ack: 0xC42BB5F4  Win: 0x4421  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-16:49:06.808935 192.168.58.129:2827 -> 192.168.58.128:6667
```

```
TCP TTL:128 TOS:0x0 ID:8498 IpLen:20 DgmLen:129
***AP*** Seq: 0xF706FF5A  Ack: 0xC42BB5F4  Win: 0x4421  TcpLen: 20
55 53 45 52 20 4C 49 6B 6C 69 70 74 63 20 6C 6F  USER LIkliptc lo
63 61 6C 68 6F 73 74 20 30 20 3A 57 52 61 6D 79  calhost 0 :WRamy
71 75 53 72 55 58 41 64 4C 72 6A 58 53 68 4F 66  quSrUXAdLrjXShOf
5A 68 53 47 55 7A 4E 5A 53 47 66 61 74 67 73 44  ZhSGUzNZSGfatgsD
63 49 52 69 6E 46 0A 4E 49 43 4B 20 78 54 63 5A  cIRinF.NICK xTcZ
57 42 6A 4A 53 64 7A 79 0A                       WBjJSdzy.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-16:49:06.809043 192.168.58.128:6667 -> 192.168.58.129:2827
TCP TTL:64 TOS:0x0 ID:54880 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xC42BB5F4  Ack: 0xF706FFB3  Win: 0x16D0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-16:49:06.810790 192.168.58.129:113 -> 192.168.58.128:1165
TCP TTL:128 TOS:0x0 ID:8499 IpLen:20 DgmLen:86
***AP*** Seq: 0xF7085005  Ack: 0xC41FC88A  Win: 0x4463  TcpLen: 32
TCP Options (3) => NOP NOP TS: 1031949 14443517
32 38 32 37 20 2C 20 36 36 36 37 20 3A 20 55 53  2827 , 6667 : US
45 52 49 44 20 3A 20 55 4E 49 58 20 3A 20 78 64  ERID : UNIX : xd
43 0A                                            C.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-16:49:06.810822 192.168.58.128:1165 -> 192.168.58.129:113
TCP TTL:64 TOS:0x0 ID:43907 IpLen:20 DgmLen:52 DF
***A**** Seq: 0xC41FC88A  Ack: 0xF7085027  Win: 0x16D0  TcpLen: 32
TCP Options (3) => NOP NOP TS: 14443575 1031949

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-16:49:06.811633 192.168.58.128:1165 -> 192.168.58.129:113
TCP TTL:64 TOS:0x0 ID:43908 IpLen:20 DgmLen:52 DF
***A***F Seq: 0xC41FC88A  Ack: 0xF7085027  Win: 0x16D0  TcpLen: 32
TCP Options (3) => NOP NOP TS: 14443575 1031949

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-16:49:06.811717 192.168.58.128:6667 -> 192.168.58.129:2827
TCP TTL:64 TOS:0x0 ID:54881 IpLen:20 DgmLen:77 DF
***AP*** Seq: 0xC42BB5F4  Ack: 0xF706FFB3  Win: 0x16D0  TcpLen: 20
4E 4F 54 49 43 45 20 41 55 54 48 20 3A 2A 2A 2A  NOTICE AUTH :***
20 47 6F 74 20 49 64 65 6E 74 20 72 65 73 70 6F   Got Ident respo
6E 73 65 0D 0A                                   nse..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+


=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-16:49:32.887074 192.168.58.128:6667 -> 192.168.58.129:2827
TCP TTL:64 TOS:0x0 ID:54882 IpLen:20 DgmLen:89 DF
***AP*** Seq: 0xC42BB619  Ack: 0xF706FFB3  Win: 0x16D0  TcpLen: 20
4E 4F 54 49 43 45 20 41 55 54 48 20 3A 2A 2A 2A  NOTICE AUTH :***
20 43 6F 75 6C 64 6E 27 74 20 6C 6F 6F 6B 20 75   Couldn't look u
70 20 79 6F 75 72 20 68 6F 73 74 6E 61 6D 65 0D  p your hostname.
0A                                               .

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-16:49:33.023192 192.168.58.129:2827 -> 192.168.58.128:6667
TCP TTL:128 TOS:0x0 ID:8503 IpLen:20 DgmLen:40
***A**** Seq: 0xF706FFB3  Ack: 0xC42BB64A  Win: 0x43CB  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-16:49:33.519327 192.168.58.128:6667 -> 192.168.58.129:2827
TCP TTL:64 TOS:0x0 ID:54883 IpLen:20 DgmLen:1064 DF
```

```
***AP*** Seq: 0xC42BB64A  Ack: 0xF706FFB3  Win: 0x16D0  TcpLen: 20
3A 6C 6F 63 61 6C 68 6F 73 74 2E 6C 6F 63 61 6C  :localhost.local
64 6F 6D 61 69 6E 20 30 30 31 20 78 54 63 5A 57  domain 001 xTcZW
42 6A 4A 53 20 3A 57 65 6C 63 6F 6D 65 20 74 6F  BjJS :Welcome to
20 74 68 65 20 49 6E 74 65 72 6E 65 74 20 52 65   the Internet Re
6C 61 79 20 4E 65 74 77 6F 72 6B 20 78 54 63 5A  lay Network xTcZ
57 42 6A 4A 53 0D 0A 3A 6C 6F 63 61 6C 68 6F 73  WBjJS..:localhos
74 2E 6C 6F 63 61 6C 64 6F 6D 61 69 6E 20 30 30  t.localdomain 00
32 20 78 54 63 5A 57 42 6A 4A 53 20 3A 59 6F 75  2 xTcZWBjJS :You
72 20 68 6F 73 74 20 69 73 20 6C 6F 63 61 6C 68  r host is localh
6F 73 74 2E 6C 6F 63 61 6C 64 6F 6D 61 69 6E 5B  ost.localdomain[
6C 6F 63 61 6C 68 6F 73 74 2E 6C 6F 63 61 6C 64  localhost.locald
6F 6D 61 69 6E 2F 36 36 36 37 5D 2C 20 72 75 6E  omain/6667], run
6E 69 6E 67 20 76 65 72 73 69 6F 6E 20 32 2E 38  ning version 2.8
2F 68 79 62 72 69 64 2D 36 2E 33 2E 31 0D 0A 4E  /hybrid-6.3.1..N
4F 54 49 43 45 20 78 54 63 5A 57 42 6A 4A 53 20  OTICE xTcZWBjJS
3A 2A 2A 2A 20 59 6F 75 72 20 68 6F 73 74 20 69  :*** Your host i
73 20 6C 6F 63 61 6C 68 6F 73 74 2E 6C 6F 63 61  s localhost.loca
6C 64 6F 6D 61 69 6E 5B 6C 6F 63 61 6C 68 6F 73  ldomain[localhos
74 2E 6C 6F 63 61 6C 64 6F 6D 61 69 6E 2F 36 36  t.localdomain/66
36 37 5D 2C 20 72 75 6E 6E 69 6E 67 20 76 65 72  67], running ver
73 69 6F 6E 20 32 2E 38 2F 68 79 62 72 69 64 2D  sion 2.8/hybrid-
36 2E 33 2E 31 0D 0A 3A 6C 6F 63 61 6C 68 6F 73  6.3.1..:localhos
74 2E 6C 6F 63 61 6C 64 6F 6D 61 69 6E 20 30 30  t.localdomain 00
33 20 78 54 63 5A 57 42 6A 4A 53 20 3A 54 68 69  3 xTcZWBjJS :Thi
73 20 73 65 72 76 65 72 20 77 61 73 20 63 72 65  s server was cre
61 74 65 64 20 54 75 65 20 4A 75 6E 20 34 20 32  ated Tue Jun 4 2
30 30 32 20 61 74 20 31 36 3A 35 39 3A 34 35 20  002 at 16:59:45
45 44 54 0D 0A 3A 6C 6F 63 61 6C 68 6F 73 74 2E  EDT..:localhost.
6C 6F 63 61 6C 64 6F 6D 61 69 6E 20 30 30 34 20  localdomain 004
78 54 63 5A 57 42 6A 4A 53 20 6C 6F 63 61 6C 68  xTcZWBjJS localh
6F 73 74 2E 6C 6F 63 61 6C 64 6F 6D 61 69 6E 20  ost.localdomain
32 2E 38 2F 68 79 62 72 69 64 2D 36 2E 33 2E 31  2.8/hybrid-6.3.1
20 6F 4F 69 77 73 7A 63 72 6B 66 79 64 6E 78 62   oOiwszcrkfydnxb
20 62 69 6B 6C 6D 6E 6F 70 73 74 76 65 0D 0A 3A   biklmnopstve..:
6C 6F 63 61 6C 68 6F 73 74 2E 6C 6F 63 61 6C 64  localhost.locald
6F 6D 61 69 6E 20 30 30 35 20 78 54 63 5A 57 42  omain 005 xTcZWB
6A 4A 53 20 57 41 4C 4C 43 48 4F 50 53 20 50 52  jJS WALLCHOPS PR
45 46 49 58 3D 28 6F 76 29 40 2B 20 43 48 41 4E  EFIX=(ov)@+ CHAN
54 59 50 45 53 3D 23 26 20 4D 41 58 43 48 41 4E  TYPES=#& MAXCHAN
4E 45 4C 53 3D 32 30 20 4D 41 58 42 41 4E 53 3D  NELS=20 MAXBANS=
32 35 20 4E 49 43 4B 4C 45 4E 3D 39 20 54 4F 50  25 NICKLEN=9 TOP
49 43 4C 45 4E 3D 31 32 30 20 4B 49 43 4B 4C 45  ICLEN=120 KICKLE
4E 3D 39 30 20 4E 45 54 57 4F 52 4B 3D 45 46 6E  N=90 NETWORK=EFn
65 74 20 43 48 41 4E 4D 4F 44 45 53 3D 62 2C 6B  et CHANMODES=b,k
2C 6C 2C 69 6D 6E 70 73 74 20 4D 4F 44 45 53 3D  ,l,imnpst MODES=
34 20 3A 61 72 65 20 73 75 70 70 6F 72 74 65 64  4 :are supported
20 62 79 20 74 68 69 73 20 73 65 72 76 65 72 0D   by this server.
0A 3A 6C 6F 63 61 6C 68 6F 73 74 2E 6C 6F 63 61  .:localhost.loca
6C 64 6F 6D 61 69 6E 20 32 35 31 20 78 54 63 5A  ldomain 251 xTcZ
57 42 6A 4A 53 20 3A 54 68 65 72 65 20 61 72 65  WBjJS :There are
20 30 20 75 73 65 72 73 20 61 6E 64 20 32 20 69   0 users and 2 i
6E 76 69 73 69 62 6C 65 20 6F 6E 20 31 20 73 65  nvisible on 1 se
72 76 65 72 73 0D 0A 3A 6C 6F 63 61 6C 68 6F 73  rvers..:localhos
74 2E 6C 6F 63 61 6C 64 6F 6D 61 69 6E 20 32 35  t.localdomain 25
35 20 78 54 63 5A 57 42 6A 4A 53 20 3A 49 20 68  5 xTcZWBjJS :I h
61 76 65 20 32 20 63 6C 69 65 6E 74 73 20 61 6E  ave 2 clients an
64 20 30 20 73 65 72 76 65 72 73 0D 0A 3A 6C 6F  d 0 servers..:lo
63 61 6C 68 6F 73 74 2E 6C 6F 63 61 6C 64 6F 6D  calhost.localdom
61 69 6E 20 32 36 35 20 78 54 63 5A 57 42 6A 4A  ain 265 xTcZWBjJ
53 20 3A 43 75 72 72 65 6E 74 20 6C 6F 63 61 6C  S :Current local
20 20 75 73 65 72 73 3A 20 32 20 20 4D 61 78 3A    users: 2  Max:
20 32 0D 0A 3A 6C 6F 63 61 6C 68 6F 73 74 2E 6C   2..:localhost.l
6F 63 61 6C 64 6F 6D 61 69 6E 20 32 36 36 20 78  ocaldomain 266 x
54 63 5A 57 42 6A 4A 53 20 3A 43 75 72 72 65 6E  TcZWBjJS :Curren

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-16:49:33.523499 192.168.58.129:2827 -> 192.168.58.128:6667
TCP TTL:128 TOS:0x0 ID:8504 IpLen:20 DgmLen:59
***AP*** Seq: 0xF706FFB3  Ack: 0xC42BBA4A  Win: 0x3FCB  TcpLen: 20
```

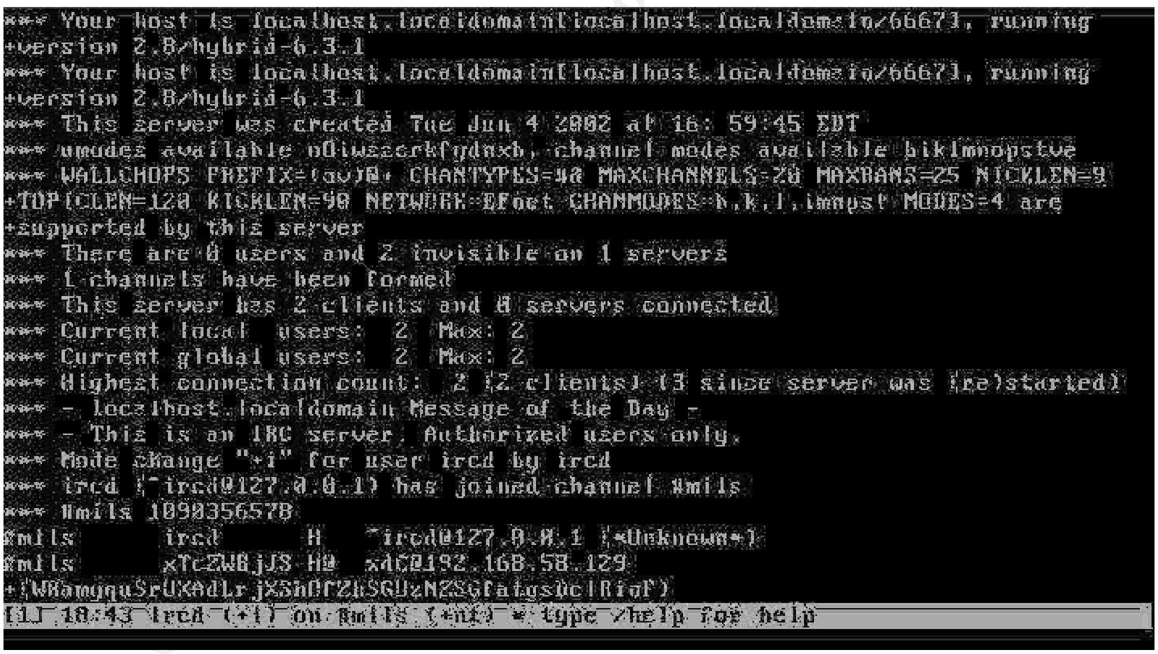
```
55 53 45 52 48 4F 53 54 20 78 54 63 5A 57 42 6A  USERHOST xTcZWBj
4A 53 0A                                         JS.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-16:49:33.523610 192.168.58.128:6667 -> 192.168.58.129:2827
TCP TTL:64 TOS:0x0 ID:54884 IpLen:20 DgmLen:443 DF
***AP*** Seq: 0xC42BBA4A  Ack: 0xF706FFC6  Win: 0x16D0  TcpLen: 20
74 20 67 6C 6F 62 61 6C 20 75 73 65 72 73 3A 20  t global users:
32 20 20 4D 61 78 3A 20 32 0D 0A 3A 6C 6F 63 61  2  Max: 2..:loca
6C 68 6F 73 74 2E 6C 6F 63 61 6C 64 6F 6D 61 69  lhost.localdomai
6E 20 32 35 30 20 78 54 63 5A 57 42 6A 4A 53 20  n 250 xTcZWBjJS
3A 48 69 67 68 65 73 74 20 63 6F 6E 6E 65 63 74  :Highest connect
69 6F 6E 20 63 6F 75 6E 74 3A 20 31 20 28 31 20  ion count: 1 (1
63 6C 69 65 6E 74 73 29 20 28 32 20 73 69 6E 63  clients) (2 sinc
65 20 73 65 72 76 65 72 20 77 61 73 20 28 72 65  e server was (re
29 73 74 61 72 74 65 64 29 0D 0A 3A 6C 6F 63 61  )started)..:loca
6C 68 6F 73 74 2E 6C 6F 63 61 6C 64 6F 6D 61 69  lhost.localdomai
6E 20 33 37 35 20 78 54 63 5A 57 42 6A 4A 53 20  n 375 xTcZWBjJS
3A 2D 20 6C 6F 63 61 6C 68 6F 73 74 2E 6C 6F 63  :- localhost.loc
61 6C 64 6F 6D 61 69 6E 20 4D 65 73 73 61 67 65  aldomain Message
20 6F 66 20 74 68 65 20 44 61 79 20 2D 20 0D 0A   of the Day - ..
3A 6C 6F 63 61 6C 68 6F 73 74 2E 6C 6F 63 61 6C  :localhost.local
64 6F 6D 61 69 6E 20 33 37 32 20 78 54 63 5A 57  domain 372 xTcZW
42 6A 4A 53 20 3A 2D 20 54 68 69 73 20 69 73 20  BjJS :- This is
61 6E 20 49 52 43 20 73 65 72 76 65 72 2E 20 41  an IRC server. A
75 74 68 6F 72 69 7A 65 64 20 75 73 65 72 73 20  uthorized users
6F 6E 6C 79 2E 0D 0A 3A 6C 6F 63 61 6C 68 6F 73  only...:localhos
74 2E 6C 6F 63 61 6C 64 6F 6D 61 69 6E 20 33 37  t.localdomain 37
36 20 78 54 63 5A 57 42 6A 4A 53 20 3A 45 6E 64  6 xTcZWBjJS :End
20 6F 66 20 2F 4D 4F 54 44 20 63 6F 6D 6D 61 6E   of /MOTD comman
64 2E 0D 0A 3A 78 54 63 5A 57 42 6A 4A 53 20 4D  d...:xTcZWBjJS M
4F 44 45 20 78 54 63 5A 57 42 6A 4A 53 20 3A 2B  ODE xTcZWBjJS :+
69 0D 0A                                         i..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-16:49:33.679274 192.168.58.129:2827 -> 192.168.58.128:6667
TCP TTL:128 TOS:0x0 ID:8505 IpLen:20 DgmLen:40
***A**** Seq: 0xF706FFC6  Ack: 0xC42BBBDD  Win: 0x4470  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-16:49:33.887148 192.168.58.128:6667 -> 192.168.58.129:2827
TCP TTL:64 TOS:0x0 ID:54885 IpLen:20 DgmLen:110 DF
***AP*** Seq: 0xC42BBBDD  Ack: 0xF706FFC6  Win: 0x16D0  TcpLen: 20
3A 6C 6F 63 61 6C 68 6F 73 74 2E 6C 6F 63 61 6C  :localhost.local
64 6F 6D 61 69 6E 20 33 30 32 20 78 54 63 5A 57  domain 302 xTcZW
42 6A 4A 53 20 3A 78 54 63 5A 57 42 6A 4A 53 3D  BjJS :xTcZWBjJS=
2B 78 64 43 40 31 39 32 2E 31 36 38 2E 35 38 2E  +xdC@192.168.58.
31 32 39 20 0D 0A                                129 ..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-16:49:34.007289 192.168.58.129:2827 -> 192.168.58.128:6667
TCP TTL:128 TOS:0x0 ID:8506 IpLen:20 DgmLen:40
***A**** Seq: 0xF706FFC6  Ack: 0xC42BBC23  Win: 0x442A  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-16:49:38.895750 192.168.58.129:2827 -> 192.168.58.128:6667
TCP TTL:128 TOS:0x0 ID:8511 IpLen:20 DgmLen:53
***AP*** Seq: 0xF706FFC6  Ack: 0xC42BBC23  Win: 0x442A  TcpLen: 20
4A 4F 49 4E 20 23 6D 69 6C 73 20 3A 0A           JOIN #mils :.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-16:49:38.927274 192.168.58.128:6667 -> 192.168.58.129:2827
TCP TTL:64 TOS:0x0 ID:54886 IpLen:20 DgmLen:246 DF
***AP*** Seq: 0xC42BBC23  Ack: 0xF706FFD3  Win: 0x16D0  TcpLen: 20
3A 78 54 63 5A 57 42 6A 4A 53 21 78 64 43 40 31  :xTcZWBjJS!xdC@1
```

```
39 32 2E 31 36 38 2E 35 38 2E 31 32 39 20 4A 4F  92.168.58.129 JO
49 4E 20 3A 23 6D 69 6C 73 0D 0A 3A 6C 6F 63 61  IN :#mils..:loca
6C 68 6F 73 74 2E 6C 6F 63 61 6C 64 6F 6D 61 69  lhost.localdomai
6E 20 4D 4F 44 45 20 23 6D 69 6C 73 20 2B 6E 74  n MODE #mils +nt
0D 0A 3A 6C 6F 63 61 6C 68 6F 73 74 2E 6C 6F 63  ..:localhost.loc
61 6C 64 6F 6D 61 69 6E 20 33 35 33 20 78 54 63  aldomain 353 xTc
5A 57 42 6A 4A 53 20 3D 20 23 6D 69 6C 73 20 3A  ZWBjJS = #mils :
40 78 54 63 5A 57 42 6A 4A 53 20 0D 0A 3A 6C 6F  @xTcZWBjJS ..:lo
63 61 6C 68 6F 73 74 2E 6C 6F 63 61 6C 64 6F 6D  calhost.localdom
61 69 6E 20 33 36 36 20 78 54 63 5A 57 42 6A 4A  ain 366 xTcZWBjJ
53 20 23 6D 69 6C 73 20 3A 45 6E 64 20 6F 66 20  S #mils :End of
2F 4E 41 4D 45 53 20 6C 69 73 74 2E 0D 0A        /NAMES list...

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-16:49:39.041875 192.168.58.129:2827 -> 192.168.58.128:6667
TCP TTL:128 TOS:0x0 ID:8512 IpLen:20 DgmLen:40
***A**** Seq: 0xF706FFD3  Ack: 0xC42BBCF1  Win: 0x435C  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-16:49:41.911235 192.168.58.129:2827 -> 192.168.58.128:6667
TCP TTL:128 TOS:0x0 ID:8513 IpLen:20 DgmLen:61
***AP*** Seq: 0xF706FFD3  Ack: 0xC42BBCF1  Win: 0x435C  TcpLen: 20
4D 4F 44 45 20 23 6D 69 6C 73 0A 57 48 4F 20 23  MODE #mils.WHO #
6D 69 6C 73 0A                                   mils.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-16:49:41.946159 192.168.58.128:6667 -> 192.168.58.129:2827
TCP TTL:64 TOS:0x0 ID:54887 IpLen:20 DgmLen:40 DF
***A**** Seq: 0xC42BBCF1  Ack: 0xF706FFE8  Win: 0x16D0  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-16:49:41.975044 192.168.58.128:6667 -> 192.168.58.129:2827
TCP TTL:64 TOS:0x0 ID:54888 IpLen:20 DgmLen:352 DF
***AP*** Seq: 0xC42BBCF1  Ack: 0xF706FFE8  Win: 0x16D0  TcpLen: 20
3A 6C 6F 63 61 6C 68 6F 73 74 2E 6C 6F 63 61 6C  :localhost.local
64 6F 6D 61 69 6E 20 33 32 34 20 78 54 63 5A 57  domain 324 xTcZW
42 6A 4A 53 20 23 6D 69 6C 73 20 2B 74 6E 20 0D  BjJS #mils +tn .
0A 3A 6C 6F 63 61 6C 68 6F 73 74 2E 6C 6F 63 61  .:localhost.loca
6C 64 6F 6D 61 69 6E 20 33 32 39 20 78 54 63 5A  ldomain 329 xTcZ
57 42 6A 4A 53 20 23 6D 69 6C 73 20 31 30 39 30  WBjJS #mils 1090
33 35 36 35 37 38 0D 0A 3A 6C 6F 63 61 6C 68 6F  356578..:localho
73 74 2E 6C 6F 63 61 6C 64 6F 6D 61 69 6E 20 33  st.localdomain 3
35 32 20 78 54 63 5A 57 42 6A 4A 53 20 23 6D 69  52 xTcZWBjJS #mi
6C 73 20 78 64 43 20 31 39 32 2E 31 36 38 2E 35  ls xdC 192.168.5
38 2E 31 32 39 20 6C 6F 63 61 6C 68 6F 73 74 2E  8.129 localhost.
6C 6F 63 61 6C 64 6F 6D 61 69 6E 20 78 54 63 5A  localdomain xTcZ
57 42 6A 4A 53 20 48 40 20 3A 30 20 57 52 61 6D  WBjJS H@ :0 WRam
79 71 75 53 72 55 58 41 64 4C 72 6A 58 53 68 4F  yquSrUXAdLrjXShO
66 5A 68 53 47 55 7A 4E 5A 53 47 66 61 74 67 73  fZhSGUzNZSGfatgs
44 63 49 52 69 6E 46 0D 0A 3A 6C 6F 63 61 6C 68  DcIRinF..:localh
6F 73 74 2E 6C 6F 63 61 6C 64 6F 6D 61 69 6E 20  ost.localdomain
33 31 35 20 78 54 63 5A 57 42 6A 4A 53 20 23 6D  315 xTcZWBjJS #m
69 6C 73 20 3A 45 6E 64 20 6F 66 20 2F 57 48 4F  ils :End of /WHO
20 6C 69 73 74 2E 0D 0A                           list...

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-16:49:42.098742 192.168.58.129:2827 -> 192.168.58.128:6667
TCP TTL:128 TOS:0x0 ID:8514 IpLen:20 DgmLen:40
***A**** Seq: 0xF706FFE8  Ack: 0xC42BBE29  Win: 0x4224  TcpLen: 20

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-16:52:20.146876 192.168.58.128:6667 -> 192.168.58.129:2827
TCP TTL:64 TOS:0x0 ID:54889 IpLen:20 DgmLen:69 DF
***AP*** Seq: 0xC42BBE29  Ack: 0xF706FFE8  Win: 0x16D0  TcpLen: 20
50 49 4E 47 20 3A 6C 6F 63 61 6C 68 6F 73 74 2E  PING :localhost.
```

```
6C 6F 63 61 6C 64 6F 6D 61 69 6E 0D 0A           localdomain..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

07/20-16:52:20.148801 ARP who-has 192.168.58.128 tell 192.168.58.129

07/20-16:52:20.148855 ARP reply 192.168.58.128 is-at 0:C:29:56:36:3F

07/20-16:52:20.149015 192.168.58.129:2827 -> 192.168.58.128:6667
TCP TTL:128 TOS:0x0 ID:8515 IpLen:20 DgmLen:68
***AP*** Seq: 0xF706FFE8  Ack: 0xC42BBE46  Win: 0x4207  TcpLen: 20
50 4F 4E 47 20 3A 6C 6F 63 61 6C 68 6F 73 74 2E  PONG :localhost.
6C 6F 63 61 6C 64 6F 6D 61 69 6E 0A              localdomain.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

5.3.3. Conclusions so far

- o msrll.exe connected to the IRC server port 6667 on the Linux machine
- o msrll.exe provided the ident service on the infected Windows machine on port 113, in order to be able to respond to incoming ident-requests
- o it chooses the nick `xTcZWBjJS` to use in IRC. Randomly generated characters, the chosen nick changes every time the application connects to the server
- o it then joins the channel #mils
- o also, when the bot gets kicked off the channel, it joins back in automatically



This screenshot shows the perspective from another IRC client that I used on the Linux machine itself to connect to the IRC server, join channel #mils and list the users that are in the channel. Ircd is me, `xTcZWBjJS` is the 'user', the msrll.exe application on the infected Windows machine.

5.3.4. Conversation with the IRCBot

At this point it seems that the binary msrll.exe launches an IRC client to connect to a certain IRC server. An automated IRC client (i.e. connecting to a server and joining of a channel automatically, as well as sitting in a channel and waiting for commands) is also called an IRCBot.

Since we could not determine the commands that we can use by simply looking at the string output of the binary, we will issue some standard commands that may be common in some IRCBot implementations.

The only command we found working was the CTCP VERSION command that queries a user for the version information of the IRC client he/she is using:

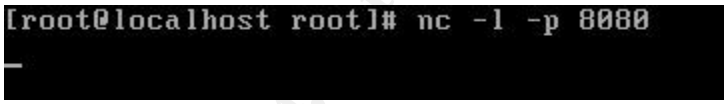
```
/ctcp xTcZWBjJS version
```

Response:

```
*** CTCP VERSION reply from xTcZWBjJS : mIRC v6.12 Khaled Mardam-Bey
```

This means the IRCBot pretends to be a mIRC version 6.12 client. A very common IRC client on the Windows platform.

The other ports Netcat was listening on (8080 and 9999) do not show any activity. This indicates that msrll.exe only tries to connect to those ports if the previous port is not available, some kind of 'fallback' to ensure irc server connectivity. This was also verified by testing: the IRC server was configured to listen on 8080 and 9999 subsequently; msrll.exe rotated through the port numbers until it found a server listening on one of the ports. Then it stopped trying to connect to any other port.



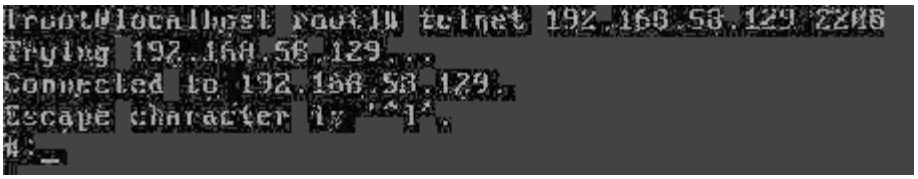
No activity on the other ports.

Shells on the infected Windows system?

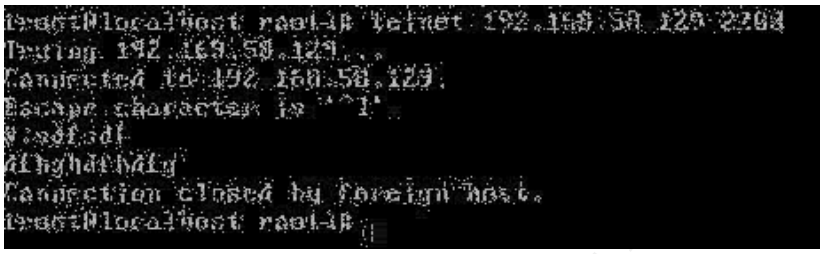
A netstat –an shows TCP ports 2200 and 2827 listening on the infected Windows system:

```
 Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1026           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2200           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2827           0.0.0.0:0              LISTENING
  TCP    192.168.58.129:139     0.0.0.0:0              LISTENING
  TCP    192.168.58.129:2827    192.168.58.128:6667    ESTABLISHED
  UDP    0.0.0.0:445            *:*
  UDP    192.168.58.129:137     *:*
  UDP    192.168.58.129:138     *:*
  UDP    192.168.58.129:500     *:*
```

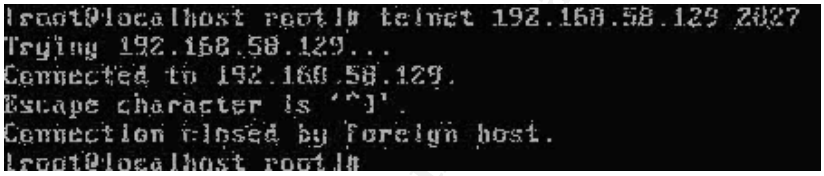
Connecting to port 2200 from the Linux machine results in a prompt:



Typing in random characters closes the connection after two lines of input (hitting 'Return' after each line):

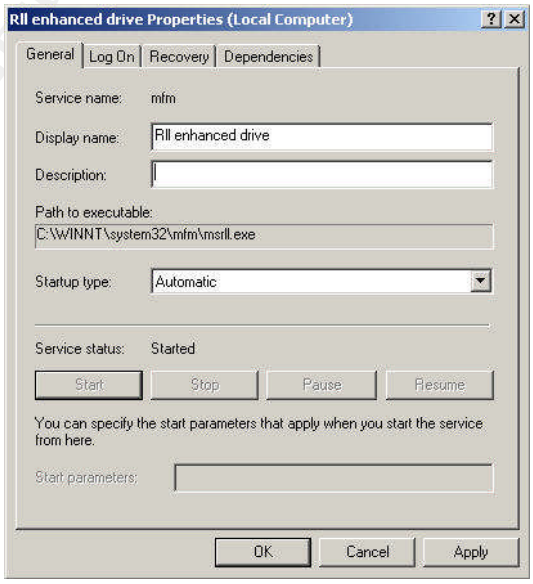


Connecting to port 2827 from the Linux machine results in a connection reset:



Whether it is possible or not to access a backdoor shell over these ports cannot be found out this way. The correct commands to access the shells – as well as the commands available to converse with the IRCBot – need to be determined through code analysis.

As stated before, msrll installs itself as a system service. An interesting property of it is that once an infected system was restarted and the 'service' has been started, not even the Administrator can stop it via the Settings - Control Panel – Administrative Tools – Services console: the control buttons are greyed out:



The only way to disable the service is to change the startup type to Manual or Disabled and reboot the machine.

6. Code Analysis

Code Analysis - 35 points

Use your laboratory setup to perform a code analysis of the unknown malware specimen. Describe the analysis in detail. Describe your steps and your use of your tools in detail. Explain the implications of the behavior of the malware.

Example procedures:

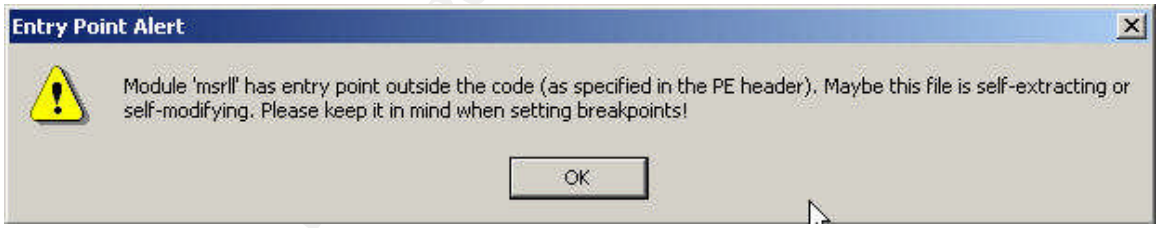
- Unpacking / Unencrypting
- Program code disassembly
- Debugging

6.1. Unpacking the file

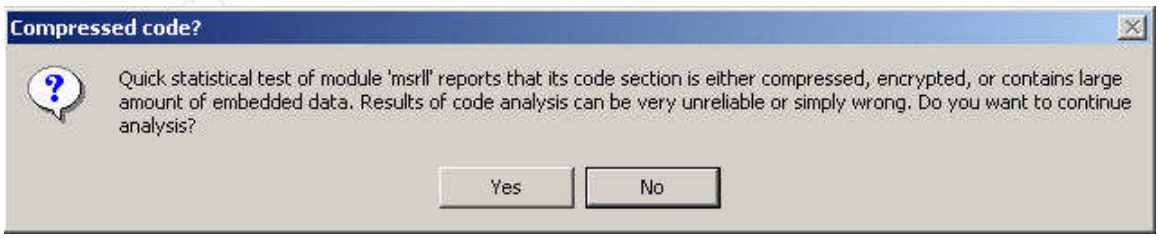
As already stated in the section “Properties of the Malware System”, these are the section headers in the msrll.exe binary:

```
00000178   00400178      0   .text
000001A0   004001A0      0   .data
000001F0   004001F0      0   .idata
00000218   00400218      0   .aspack
00000240   00400240      0   .adata
```

`.aspack` indicates that the file was packed using ASPack [ASPACK]



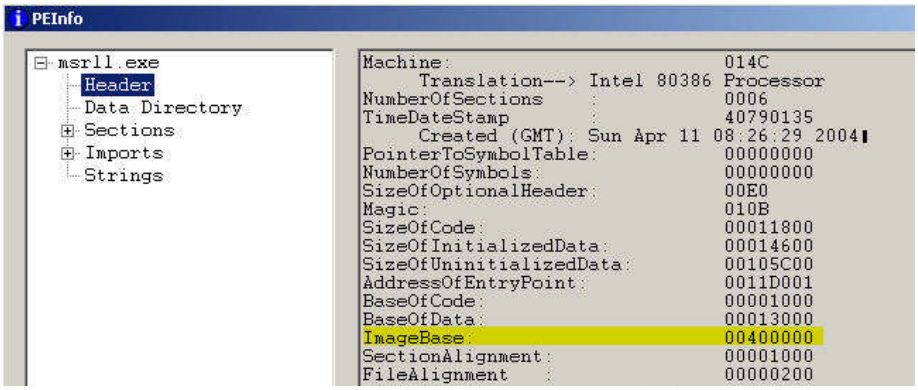
Since the binary might be self-modifying, it might be impossible to set correct breakpoints for debugging.



Also, the analysis can be unreliable and/or wrong, because of the compressed code. We need to unpack the binary.

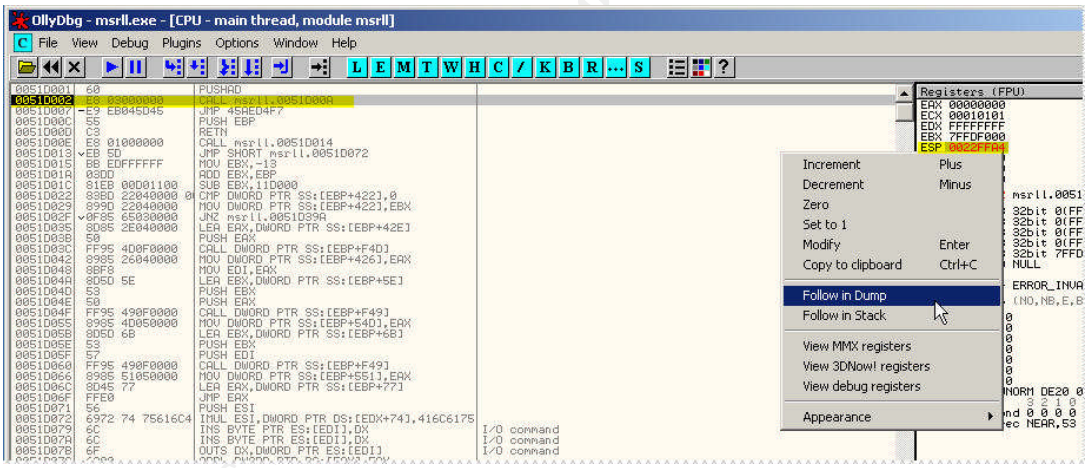
I found a walkthrough on how to unpack ASP-packed binaries with OllyDbg. [ASPACKUNPACK]

- since the file is packed, we need to find out what the original entry point is of the unpacked binary

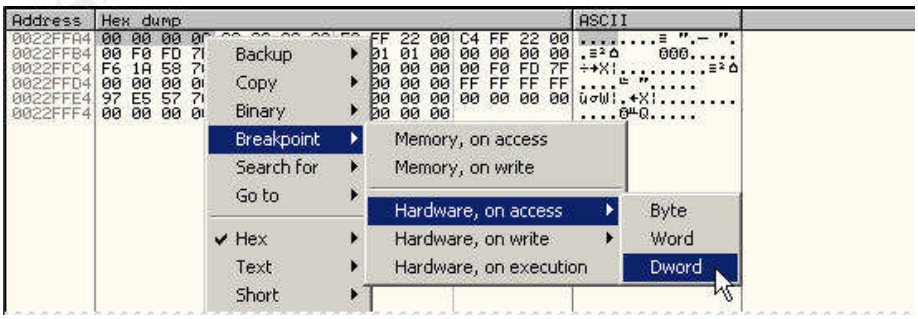


See highlighted above the image base (the base addresse) of the binary. We need this later to determine the offset of the original entry point.

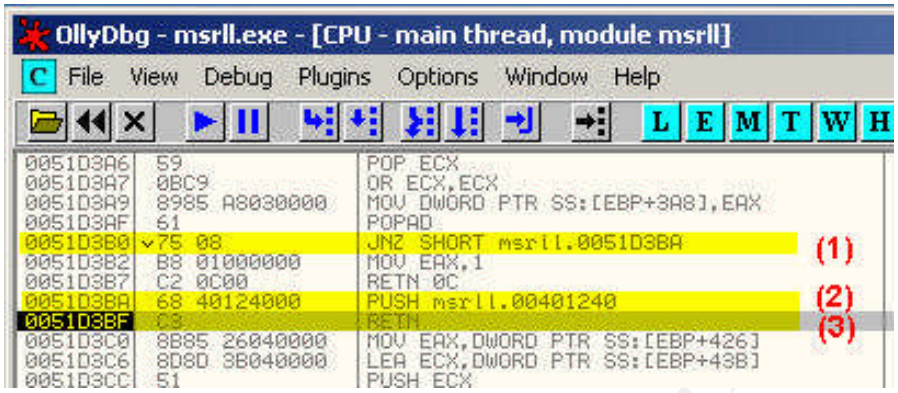
- open up the file in OllyDbg and press F8 to step to the CALL function
- right-click on the ESP register on the right and select 'Follow in Dump'



- in the dump window in the lower left of OllyDbg, mark the first four bytes, right-click and select 'Breakpoint – Hardware, on access – Dword'

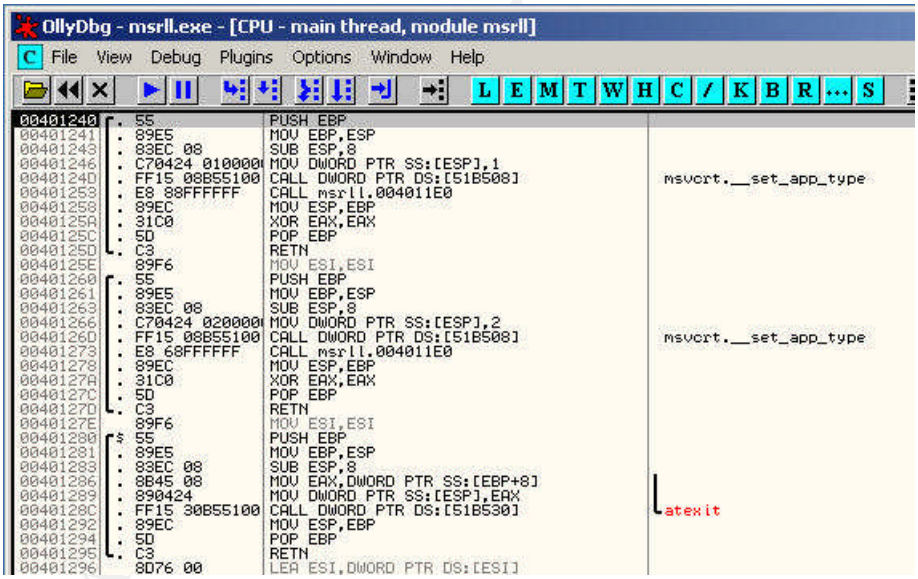


- hit F9 to start executing the binary, it will hit the breakpoint soon after

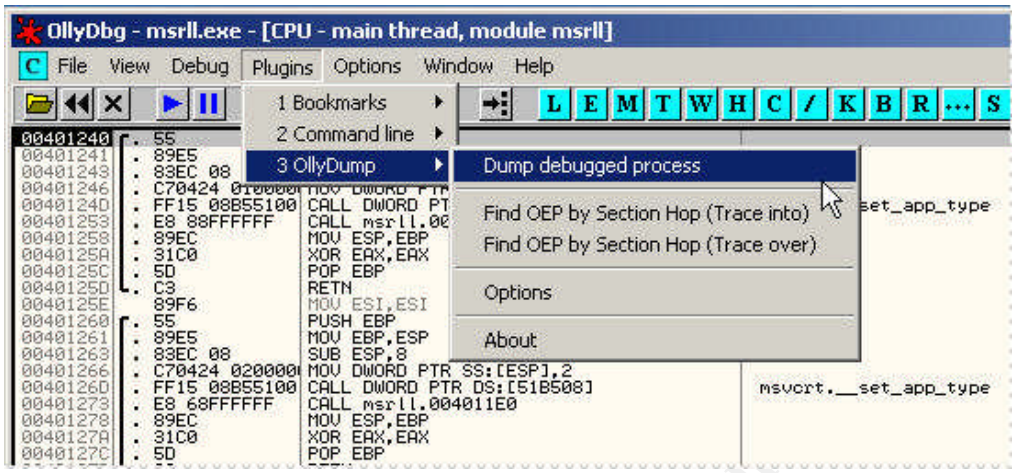


(1) denotes where the breakpoint was hit
(2) shows the address that will be pushed on the stack and
(3) will then return to that address, 0x00401240

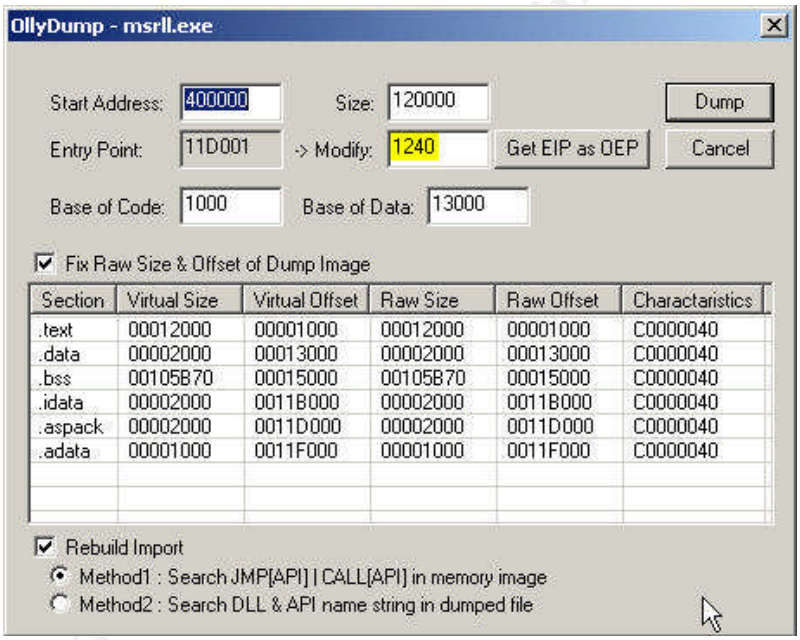
- hit F7 to trace into the code that resides at that address. This is the original entry point of the code
- Right-click on the code, select 'Analyse – Analyse code' to see the real code



- The address of the original entry point is 0x00401240. The imagebase of the code is 0x00400000. The offset of the original entry point is 0x00401240 - 0x00400000 = 1240.
- Select Plugins – OllyDump – Dump debugged process



- Modify the offset to show 1240, OllyDump may have already calculated that. Check 'Rebuild Import – Method1'



- dump the data into a new file, e.g. 'dumped_msrll.exe'

- close out the packed msrll.exe and load the newly created file into OllyDbg, then execute it. The binary works and the application connects to the IRC server the same way the packed original file did.

6.2. Analysing the unpacked file

Now that the file is unpacked, we can run it through Bintext to see if we find any useful information. Below you can find the interesting parts of the strings found.

```
File pos   Mem pos      ID   Text
========   =======      ==   ====

0000004D   0040004D      0   !This program cannot be run in DOS mode.
00000178   00400178      0   .text
000001A0   004001A0      0   .data
000001F0   004001F0      0   .idata
00000218   00400218      0   .aspack
00000240   00400240      0   .adata
00000268   00400268      0   .newIID
00001326   00401326      0   ?insmod
0000132E   0040132E      0   ?rmmod
00001335   00401335      0   ?lsmod
00001399   00401399      0   %s: <mod name>
000013A8   004013A8      0   %s: mod list full
000013BA   004013BA      0   %s: err: %u
000013C6   004013C6      0   mod_init
000013CF   004013CF      0   mod_free
000013D8   004013D8      0   %s: cannot init %s
000013EB   004013EB      0   %s: %s loaded (%u)
000013FE   004013FE      0   %s: mod allready loaded
00001416   00401416      0   %s:%s err %u
000015B5   004015B5      0   %s:%s not found
000015C5   004015C5      0   %s: unloading %s
000016AE   004016AE      0   [%u]: %s hinst:%x
00001712   00401712      0   unloading %s
000017A0   004017A0      0   %s: invalid_addr: %s
000017B5   004017B5      0   %s%s [port]
000018E8   004018E8      0   finished %s
00001A40   00401A40      0   %s <ip> <port> <t_time> <delay>
00001B32   00401B32      0   sockopt: %u
00001B3E   00401B3E      0   sendto err: %u
00001B4D   00401B4D      0   sockraw: %u
00001B59   00401B59      0   syn: done
00001FBC   00401FBC      0   %s <ip> <duration> <delay>
00002096   00402096      0   sendto: %u
000020A2   004020A2      0   jolt2: done
00002260   00402260      0   %s <ip> <p size> <duration> <delay>
00002356   00402356      0   Err: %u
0000235E   0040235E      0   smurf done
00002567   00402567      0   PhV#@
000025DE   004025DE      0   &err: %u
00002753   00402753      0   ?ping
00002763   00402763      0   ?smurf
0000276A   0040276A      0   ?jolt
00002820   00402820      0   PONG :%s
0000283A   0040283A      0   0h (@
0000299D   0040299D      0   %s!%s@%s
00002B3D   00402B3D      0   %s!%s
00002BB6   00402BB6      0   SVh=+@
00002BD7   00402BD7      0   irc.nick
00002BE0   00402BE0      0   NICK %s
00002EEA   00402EEA      0   NETWORK=
00002FF8   00402FF8      0   irc.pre
000032CC   004032CC      0   _%s__
000032D2   004032D2      0   __%s__
000032D9   004032D9      0   __%s___
000032E1   004032E1      0   NICK %s
000032F0   004032F0      0   %s %s
000036B0   004036B0      0   irc.chan
00003775   00403775      0   %s %s
0000377B   0040377B      0   WHO %s
00003A45   00403A45      0   USERHOST %s
```

```
00003A52   00403A52      0   logged into %s(%s) as %s
00003A97   00403A97      0   <$hE:@
00003ABB   00403ABB      0   PhR:@
00003B99   00403B99      0   nick.pre
00003BA2   00403BA2      0   %s-%04u
00003BAA   00403BAA      0   irc.user
00003BB3   00403BB3      0   irc.usereal
00003BBF   00403BBF      0   irc.real
00003BC8   00403BC8      0   irc.pass
00003BE0   00403BE0      0   tsend(): connection to %s:%u failed
00003C20   00403C20      0   USER %s localhost 0 :%s
00003C38   00403C38      0   NICK %s
00003DF5   00403DF5      0   Ph <@
000040BF   004040BF      0   PRIVMSG
00004100   00404100      0   trecv(): Disconnected from %s err:%u
0000446B   0040446B      0   NOTICE
00004472   00404472      0   %s %s :%s
00004615   00404615      0   Ph}D@
00004711   00404711      0   MODE %s -o+b %s *@%s
00004798   00404798      0   C'PSWh
000047B4   004047B4      0   Sh'G@
000047E7   004047E7      0   MODE %s -bo %s %s
0000487B   0040487B      0   Sh'G@
00004924   00404924      0   %s.key
00004A63   00404A63      0   Ph'G@
00004AA8   00404AA8      0   sk#%u %s is dead!
00004ABA   00404ABA      0   s_check: %s dead? pinging...
00004AD7   00404AD7      0   PING :ok
00004B00   00404B00      0   s_check: send error to %s disconnecting
00004B28   00404B28      0   expect the worst
00004B39   00404B39      0   s_check: killing socket %s
00004B54   00404B54      0   irc.knick
00004B5E   00404B5E      0   jtr.%u%s.iso
00004B6B   00404B6B      0   ison %s
00004B74   00404B74      0   servers
00004B7C   00404B7C      0   s_check: trying %s
00004DAA   00404DAA      0   Ph9K@
00004ED5   00404ED5      0   PhkK@
00004F41   00404F41      0   ShtK@
00004FD8   00404FD8      0   uYVh|K@
00005052   00405052      0   %s.mode
0000505A   0040505A      0   MODE %s %s
00005078   00405078      0   ShRP@
000050DA   004050DA      0   Sh$I@
000051A8   004051A8      0   PShZP@
000055A3   004055A3      0   mode %s +o %s
000055B2   004055B2      0   akick
000055B8   004055B8      0   mode %s +b %s %s
000055CA   004055CA      0   KICK %s %s
00005760   00405760      0   irc.pre
00005781   00405781      0   Set an irc sock to preform %s command on
000057AB   004057AB      0     Type
000057B3   004057B3      0   %csklist
000057BC   004057BC      0    to view current sockets, then
000057DC   004057DC      0   %cdccsk
000057E4   004057E4      0    <#>
000058B4   004058B4      0   %s: dll loaded
000058C3   004058C3      0   %s: %d
000059E1   004059E1      0   said %s to %s
000059EF   004059EF      0   usage: %s <target> "text"
00005A74   00405A74      0   %s not on %s
00005A81   00405A81      0   usage: %s <nick> <chan>
00005B20   00405B20      0   %s logged in
00005B87   00405B87      0   Sh [@
00005BA2   00405BA2      0   sys: %s bot: %s
00005BB2   00405BB2      0   preformance counter not avail
00005C2B   00405C2B      0   usage: %s <cmd>
00005C3B   00405C3B      0   %s free'd
00005C45   00405C45      0   unable to free %s
00005C6F   00405C6F      0   0h+\@
00005CAD   00405CAD      0   later!
```

```
00005CB4   00405CB4      0   unable to %s errno:%u
00005D40   00405D40      0   service:%c user:%s inet connection:%c contype:%s reboot
privs:%c
00005E23   00405E23      0    %-5u %s
00005F8F   00405F8F      0   %s: %s
00005F96   00405F96      0   %s: somefile
0000603F   0040603F      0   PhHY@
000060D4   004060D4      0   host: %s ip: %s
00006269   00406269      0   capGetDriverDescriptionA
00006292   00406292      0   cpus:%u
000062A0   004062A0      0   WIN%s (u:%s)%s%s mem:(%u/%u) %u%% %s %s
000065CB   004065CB      0   %s: %s (%u)
00006708   00406708      0   %s %s
00006754   00406754      0   %s bad args
000067DA   004067DA      0   akick
000067E8   004067E8      0   %s[%u] %s
000067F2   004067F2      0   %s removed
000067FD   004067FD      0   couldnt find %s
0000680D   0040680D      0   %s added
00006816   00406816      0   %s allready in list
0000682A   0040682A      0   usage: %s +/- <host>
0000696F   0040696F      0   7h*h@
000069EB   004069EB      0   jtram.conf
000069F6   004069F6      0   %s /t %s
000069FF   004069FF      0   jtr.home
00006A08   00406A08      0   %s\%s
00006A0E   00406A0E      0   %s: possibly failed: code %u
00006A2B   00406A2B      0   %s: possibly failed
00006A3F   00406A3F      0   %s: exec of %s failed err: %u
00006A90   00406A90      0   u.exf
00006C2D   00406C2D      0   Ph+j@
00006C82   00406C82      0   Ph?j@
00006CBC   00406CBC      0   jtr.id
00006CC3   00406CC3      0   %s: <url> <id>
00006ED7   00406ED7      0   IREG
00006EDD   00406EDD      0   CLON
00006EE3   00406EE3      0   ICON
00006EF8   00406EF8      0   WCON
00006F40   00406F40      0     #%u [fd:%u] %s:%u [%s%s] last:%u
00006F63   00406F63      0      |\=> [n:%s fh:%s] (%s)
00006F82   00406F82      0      |---[%s] (%u) %s
00006F96   00406F96      0      |     |-[%s%s] [%s]
00006FAD   00406FAD      0      |=> (%s) (%.8x)
0000716E   0040716E      0   B$PRhco@
00007360   00407360      0   %s <pass> <salt>
000073C8   004073C8      0   %s <nick> <chan>
0000748B   0040748B      0   PING %s
000074C9   004074C9      0   mIRC v6.12 Khaled Mardam-Bey
000074E7   004074E7      0   VERSION %s
0000751C   0040751C      0   dcc.pass
00007525   00407525      0   temp add %s
000075BD   004075BD      0   $h%u@
0000766A   0040766A      0   %s%u-%s
00007675   00407675      0   %s opened (%u)
000076A0   004076A0      0   %u bytes from %s in %u seconds saved to %s
000076CB   004076CB      0   (%s %s): incomplete! %u bytes
000076E9   004076E9      0   couldnt open %s err:%u
00007700   00407700      0   (%s) %s: %s
0000770C   0040770C      0   (%s) urlopen failed
00007720   00407720      0   (%s): inetopen failed
00007798   00407798      0   Whjv@
00007B9D   00407B9D      0   Ph w@
00007BE4   00407BE4      0   no file name in %s
00007DDB   00407DDB      0   %s created
00007E49   00407E49      0   %s %s to %s Ok
00007E8F   00407E8F      0   3hI~@
00007EE0   00407EE0      0   %0.2u/%0.2u/%0.2u  %0.2u:%0.2u  %15s  %s
00007F09   00407F09      0   %s (err: %u)
0000806B   0040806B      0   ShHY@
00008085   00408085      0   err: %u
000080F8   004080F8      0   %s %s :ok
```

```
00008165   00408165      0   unable to %s %s (err: %u)
000081C3   004081C3      0   ShHY@
000081F5   004081F5      0   %-16s %s
00008200   00408200      0   %-16s (%u.%u.%u.%u)
00008489   00408489      0   [%s][%s] %s
00008595   00408595      0   closing %u [%s:%u]
000085A8   004085A8      0   unable to close socket %u
000087E2   004087E2      0   using sock #%u %s:%u (%s)
000087FD   004087FD      0   Invalid sock
0000880B   0040880B      0   usage %s <socks #>
000088D7   004088D7      0   leaves %s
000088E1   004088E1      0   :0 * * :%s
00008A96   00408A96      0   joins: %s
00008B82   00408B82      0   ACCEPT
00008B89   00408B89      0   resume
00008B90   00408B90      0   err: %u00008B99   00408B99      0   DCC ACCEPT %s %s %s
00008BAE   00408BAE      0   dcc_resume: cant find port %s
00008BD1   00408BD1      0   dcc.dir
00008BD9   00408BD9      0   %s\%s\%s\%s
00008BE5   00408BE5      0   unable to open (%s): %u
00008BFD   00408BFD      0   resuming dcc from %s to %s
00008C19   00408C19      0   DCC RESUME %s %s %u
0000934E   0040934E      0   ?clone
00009355   00409355      0   ?clones
0000935D   0040935D      0   ?login
00009364   00409364      0   ?uptime
0000936C   0040936C      0   ?reboot
00009374   00409374      0   ?status
0000937C   0040937C      0   ?jump
00009382   00409382      0   ?nick
00009388   00409388      0   ?echo
0000938E   0040938E      0   ?hush
00009394   00409394      0   ?wget
0000939A   0040939A      0   ?join
000093A9   004093A9      0   ?akick
000093B0   004093B0      0   ?part
000093B6   004093B6      0   ?dump
000093C6   004093C6      0   ?md5p
000093CC   004093CC      0   ?free
000093D7   004093D7      0   ?update
000093DF   004093DF      0   ?hostname
000093EE   004093EE      0   ?!fif
000093FE   004093FE      0   ?play
00009404   00409404      0   ?copy
0000940A   0040940A      0   ?move
00009415   00409415      0   ?sums
00009423   00409423      0   ?rmdir
0000942A   0040942A      0   ?mkdir
00009436   00409436      0   ?exec
00009440   00409440      0   ?kill
00009446   00409446      0   ?killall
0000944F   0040944F      0   ?crash
0000946E   0040946E      0   ?sklist
00009476   00409476      0   ?unset
0000947D   0040947D      0   ?uattr
00009484   00409484      0   ?dccsk
00009490   00409490      0   ?killsk
00009499   00409499      0   VERSION*
000094AE   004094AE      0   IDENT
000096BE   004096BE      0   %ud %02uh %02um %02us
000096D4   004096D4      0   %02uh %02um %02us
000096E6   004096E6      0   %um %02us
000099E0   004099E0      0   jtram.conf
000099EB   004099EB      0   jtr.*
000099F5   004099F5      0   DiCHFc2ioiVmb3cb4zZ7zWZH1oM=
00009A16   00409A16      0   conf_dump: wrote %u lines
0000A270   0040A270      0   get of %s incomplete at %u bytes
0000A2B0   0040A2B0      0   get of %s completed (%u bytes), %u seconds %u cps
0000A2F0   0040A2F0      0   error while writing to %s (%u)
0000A65C   0040A65C      0   chdir: %s -> %s (%u)
0000A750   0040A750      0   dcc_wait: get of %s from %s timed out
```

```
0000A790   0040A790      0   dcc_wait: closing [#%u] %s:%u (%s)
0000A9F0   0040A9F0      0   %4s #%.2u %s %ucps %u%% [sk#%u] %s
0000AA30   0040AA30      0   %u Send(s) %u Get(s) (%u transfer(s) total) UP:%ucps
DOWN:%ucps Total:%ucps
0000ACD0   0040ACD0      0   send of %s incomplete at %u bytes
0000AD10   0040AD10      0   send of %s completed (%u bytes), %u seconds %u cps
0000AF50   0040AF50      0   cant open %s (err:%u) pwd:{%s}
0000AF70   0040AF70      0   DCC SEND %s %u %u %u
0000B751   0040B751      0   %s %s
0000B757   0040B757      0   %s exited with code %u
0000B76E   0040B76E      0   %s\%s
0000B774   0040B774      0   %s: %s
0000B77B   0040B77B      0   exec: Error:%u pwd:%s cmd:%s
0000BB40   0040BB40      0   dcc.pass
0000BB49   0040BB49      0   bot.port
0000BB52   0040BB52      0   %s bad pass from "%s"@%s
0000BCC9   0040BCC9      0   %s: connect from %s
0000BD33   0040BD33      0   jtr.bin
0000BD3B   0040BD3B      0   msrll.exe
0000BD45   0040BD45      0   jtr.home
0000BD57   0040BD57      0   jtr.id
0000BD63   0040BD63      0   irc.quit
0000BD6E   0040BD6E      0   servers
0000BD80   0040BD80      0
collective7.zxy0.com,collective7.zxy0.com:9999!,collective7.zxy0.com:8080
0000BDCA   0040BDCA      0   irc.chan
0000BDD3   0040BDD3      0   #mils
0000BDE0   0040BDE0      0   $1$KZLPLKDf$W8kl8Jr1X8DOHZsmIp9qq0
0000BE20   0040BE20      0   $1$KZLPLKDf$55isA1ITvamR7bjAdBziX.
0000C02F   0040C02F      0   SSL_get_error
0000C03D   0040C03D      0   SSL_load_error_strings
0000C054   0040C054      0   SSL_library_init
0000C065   0040C065      0   SSLv3_client_method
0000C079   0040C079      0   SSL_set_connect_state
0000C08F   0040C08F      0   SSL_CTX_new
0000C09B   0040C09B      0   SSL_new
0000C0A3   0040C0A3      0   SSL_set_fd
0000C0AE   0040C0AE      0   SSL_connect
0000C0BA   0040C0BA      0   SSL_write
0000C0C4   0040C0C4      0   SSL_read
0000C0CD   0040C0CD      0   SSL_shutdown
0000C0DA   0040C0DA      0   SSL_free
0000C0E3   0040C0E3      0   SSL_CTX_free
0000C263   0040C263      0   kernel32.dll
0000C270   0040C270      0   QueryPerformanceCounter
0000C288   0040C288      0   QueryPerformanceFrequency
0000C2A2   0040C2A2      0   RegisterServiceProcess
0000C2B9   0040C2B9      0   jtram.conf
0000C5B1   0040C5B1      0   irc.user
0000C5BA   0040C5BA      0   %s : USERID : UNIX : %s
0000C6A4   0040C6A4      0   QUIT :FUCK %u
0000C742   0040C742      0   Killed!? Arrg! [%u]
0000C756   0040C756      0   QUIT :%s
0000C7E8   0040C7E8      0   SeShutdownPrivilege
0000C888   0040C888      0   %s\%s
0000C88E   0040C88E      0   %s\%s\%s
0000C897   0040C897      0   Rll enhanced drive
0000C8C0   0040C8C0      0   software\microsoft\windows\currentversion\run
0000C8EE   0040C8EE      0   /d "%s"
0000CE3D   0040CE3D      0    < u&
0000D010   0040D010      0
./0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz
0000EA60   0040EA60      0   usage %s: server[:port] amount
0000EB33   0040EB33      0   %s: %s
0000EB3E   0040EB3E      0   %s %s %s <PARAM>
0000EB80   0040EB80      0   %s: [NETWORK|all] %s <"parm"> ...
0000EE20   0040EE20      0   USER %s localhost 0 :%s
0000EE38   0040EE38      0   NICK %s
0000EEE4   0040EEE4      0   PSVh
0000F140   0040F140      0   md5.c
0000F146   0040F146      0   md != NULL
```

```
0000F8F1   0040F8F1      0   buf != NULL
0000F99F   0040F99F      0   hash != NULL
0000FAC5   0040FAC5      0   message digest
0000FAD4   0040FAD4      0   abcdefghijklmnopqrstuvwxyz
0000FB00   0040FB00      0
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789
0000FB40   0040FB40      0
12345678901234567890123456789012345678901234567890123456789012345678901234567890
0000FCE0   0040FCE0      0   sprng
0000FD11   0040FD11      0   sprng.c
0000FD19   0040FD19      0   buf != NULL
0000FDBC   0040FDBC      0   rc6.c
0000FDC2   0040FDC2      0   skey != NULL
0000FDCF   0040FDCF      0   key != NULL
0000FFD1   0040FFD1      0   ct != NULL
0000FFDC   0040FFDC      0   pt != NULL
000103C3   004103C3      0   desired_keysize != NULL
00010430   00410430      0   ctr.c
00010436   00410436      0   ctr != NULL
00010442   00410442      0   key != NULL
0001044E   0041044E      0   count != NULL
00010546   00410546      0   ct != NULL
00010551   00410551      0   pt != NULL
000106F0   004106F0      0
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
0001077F   0041077F      0   ?456789:;<=
000107B7   004107B7      0    !"#$%&'()*+,-./0123
```

There is a lot more useful information we can now see.

- apparent IRCBot commands

```
00001326   00401326      0   ?insmod
0000132E   0040132E      0   ?rmmod
00001335   00401335      0   ?lsmod
00002753   00402753      0   ?ping
00002763   00402763      0   ?smurf
0000276A   0040276A      0   ?jolt
0000934E   0040934E      0   ?clone
00009355   00409355      0   ?clones
0000935D   0040935D      0   ?login
00009364   00409364      0   ?uptime
0000936C   0040936C      0   ?reboot
00009374   00409374      0   ?status
0000937C   0040937C      0   ?jump
00009382   00409382      0   ?nick
00009388   00409388      0   ?echo
0000938E   0040938E      0   ?hush
00009394   00409394      0   ?wget
0000939A   0040939A      0   ?join
000093A9   004093A9      0   ?akick
000093B0   004093B0      0   ?part
000093B6   004093B6      0   ?dump
000093C6   004093C6      0   ?md5p
000093CC   004093CC      0   ?free
000093D7   004093D7      0   ?update
000093DF   004093DF      0   ?hostname
000093EE   004093EE      0   ?!fif
000093FE   004093FE      0   ?play
00009404   00409404      0   ?copy
0000940A   0040940A      0   ?move
00009415   00409415      0   ?sums
00009423   00409423      0   ?rmdir
0000942A   0040942A      0   ?mkdir
00009436   00409436      0   ?exec
00009440   00409440      0   ?kill
00009446   00409446      0   ?killall
0000944F   0040944F      0   ?crash
0000946E   0040946E      0   ?sklist
00009476   00409476      0   ?unset
```

```
0000947D   0040947D      0   ?uattr
00009484   00409484      0   ?dccsk
00009490   00409490      0   ?killsk
```

- IRCBot and application messages

```
00001399   00401399      0   %s: <mod name>
000013A8   004013A8      0   %s: mod list full
000013BA   004013BA      0   %s: err: %u
000013C6   004013C6      0   mod_init
000013CF   004013CF      0   mod_free
000013D8   004013D8      0   %s: cannot init %s
000013EB   004013EB      0   %s: %s loaded (%u)
000013FE   004013FE      0   %s: mod allready loaded
00001416   00401416      0   %s:%s err %u
000015B5   004015B5      0   %s:%s not found
000015C5   004015C5      0   %s: unloading %s
000016AE   004016AE      0   [%u]: %s hinst:%x
00001712   00401712      0   unloading %s
000017A0   004017A0      0   %s: invalid_addr: %s
000017B5   004017B5      0   %s%s [port]
000018E8   004018E8      0   finished %s
00001A40   00401A40      0   %s <ip> <port> <t_time> <delay>
00001B59   00401B59      0   syn: done
00001FBC   00401FBC      0   %s <ip> <duration> <delay>
00002096   00402096      0   sendto: %u
000020A2   004020A2      0   jolt2: done
00002260   00402260      0   %s <ip> <p size> <duration> <delay>
00002356   00402356      0   Err: %u
0000235E   0040235E      0   smurf done
00002820   00402820      0   PONG :%s
00002BD7   00402BD7      0   irc.nick
00002BE0   00402BE0      0   NICK %s
00002EEA   00402EEA      0   NETWORK=
00002FF8   00402FF8      0   irc.pre
000032E1   004032E1      0   NICK %s
000036B0   004036B0      0   irc.chan
0000377B   0040377B      0   WHO %s
00003A45   00403A45      0   USERHOST %s
00003A52   00403A52      0   logged into %s(%s) as %s
00003B99   00403B99      0   nick.pre
00003BAA   00403BAA      0   irc.user
00003BB3   00403BB3      0   irc.usereal
00003BBF   00403BBF      0   irc.real
00003BC8   00403BC8      0   irc.pass
00003BE0   00403BE0      0   tsend(): connection to %s:%u failed
00003C20   00403C20      0   USER %s localhost 0 :%s
00003C38   00403C38      0   NICK %s
000040BF   004040BF      0   PRIVMSG
00004100   00404100      0   trecv(): Disconnected from %s err:%u
0000446B   0040446B      0   NOTICE
00004711   00404711      0   MODE %s -o+b %s *@%s
000047E7   004047E7      0   MODE %s -bo %s %s
00004924   00404924      0   %s.key
00004AA8   00404AA8      0   sk#%u %s is dead!
00004ABA   00404ABA      0   s_check: %s dead? pinging...
00004AD7   00404AD7      0   PING :ok
00004B00   00404B00      0   s_check: send error to %s disconnecting
00004B28   00404B28      0   expect the worst
00004B39   00404B39      0   s_check: killing socket %s
00004B54   00404B54      0   irc.knick
00004B5E   00404B5E      0   jtr.%u%s.iso
00004B6B   00404B6B      0   ison %s
00004B74   00404B74      0   servers
00004B7C   00404B7C      0   s_check: trying %s
00005052   00405052      0   %s.mode
0000505A   0040505A      0   MODE %s %s
000055A3   004055A3      0   mode %s +o %s
000055B2   004055B2      0   akick
000055B8   004055B8      0   mode %s +b %s %s
```

```
000055CA   004055CA      0   KICK %s %s
00005760   00405760      0   irc.pre
00005781   00405781      0   Set an irc sock to preform %s command on
000057AB   004057AB      0     Type
000057B3   004057B3      0   %csklist
000057BC   004057BC      0    to view current sockets, then
000057DC   004057DC      0   %cdccsk
000058B4   004058B4      0   %s: dll loaded
000058C3   004058C3      0   %s: %d
000059E1   004059E1      0   said %s to %s
000059EF   004059EF      0   usage: %s <target> "text"
00005A74   00405A74      0   %s not on %s
00005A81   00405A81      0   usage: %s <nick> <chan>
00005B20   00405B20      0   %s logged in
00005BA2   00405BA2      0   sys: %s bot: %s
00005BB2   00405BB2      0   preformance counter not avail
00005C2B   00405C2B      0   usage: %s <cmd>
00005C3B   00405C3B      0   %s free'd
00005C45   00405C45      0   unable to free %s
00005CAD   00405CAD      0   later!
00005CB4   00405CB4      0   unable to %s errno:%u
00005D40   00405D40      0   service:%c user:%s inet connection:%c contype:%s reboot
privs:%c
00005F96   00405F96      0   %s: somefile
000060D4   004060D4      0   host: %s ip: %s
00006292   00406292      0   cpus:%u
000062A0   004062A0      0   WIN%s (u:%s)%s%s mem:(%u/%u) %u%% %s %s
00006754   00406754      0   %s bad args
000067DA   004067DA      0   akick
000067F2   004067F2      0   %s removed
000067FD   004067FD      0   couldnt find %s
0000680D   0040680D      0   %s added
00006816   00406816      0   %s allready in list
0000682A   0040682A      0   usage: %s +/- <host>
000069EB   004069EB      0   jtram.conf
000069FF   004069FF      0   jtr.home
00006A0E   00406A0E      0   %s: possibly failed: code %u
00006A2B   00406A2B      0   %s: possibly failed
00006A3F   00406A3F      0   %s: exec of %s failed err: %u
00006CBC   00406CBC      0   jtr.id
00006CC3   00406CC3      0   %s: <url> <id>
00006ED7   00406ED7      0   IREG
00006EDD   00406EDD      0   CLON
00006EE3   00406EE3      0   ICON
00006EF8   00406EF8      0   WCON
00006F40   00406F40      0     #%u [fd:%u] %s:%u [%s%s] last:%u
00006F63   00406F63      0      |\=> [n:%s fh:%s] (%s)
00006F82   00406F82      0      |---[%s] (%u) %s
00006F96   00406F96      0      |     |-[%s%s] [%s]
00006FAD   00406FAD      0      |=> (%s) (%.8x)
00007360   00407360      0   %s <pass> <salt>
000073C8   004073C8      0   %s <nick> <chan>
0000748B   0040748B      0   PING %s
000074C9   004074C9      0   mIRC v6.12 Khaled Mardam-Bey
000074E7   004074E7      0   VERSION %s
0000751C   0040751C      0   dcc.pass
00007525   00407525      0   temp add %s
000075BD   004075BD      0   $h%u@
0000766A   0040766A      0   %s%u-%s
00007675   00407675      0   %s opened (%u)
000076A0   004076A0      0   %u bytes from %s in %u seconds saved to %s
000076CB   004076CB      0   (%s %s): incomplete! %u bytes
000076E9   004076E9      0   couldnt open %s err:%u
00007700   00407700      0   (%s) %s: %s
0000770C   0040770C      0   (%s) urlopen failed
00007720   00407720      0   (%s): inetopen failed
00007BE4   00407BE4      0   no file name in %s
00007DDB   00407DDB      0   %s created
00008085   00408085      0   err: %u
00008165   00408165      0   unable to %s %s (err: %u)
00008595   00408595      0   closing %u [%s:%u]
```

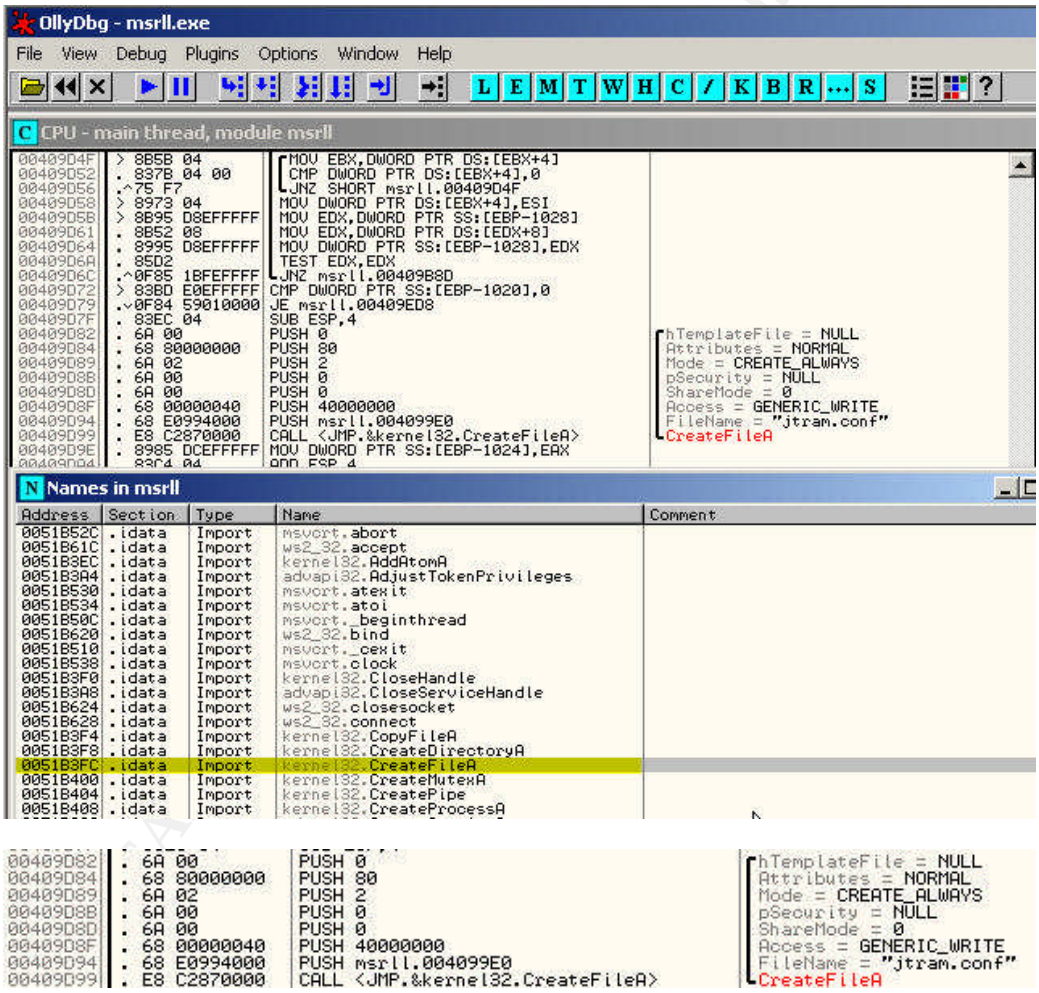
```
000085A8   004085A8      0   unable to close socket %u
000087E2   004087E2      0   using sock #%u %s:%u (%s)
000087FD   004087FD      0   Invalid sock
0000880B   0040880B      0   usage %s <socks #>
000088D7   004088D7      0   leaves %s
00008A96   00408A96      0   joins: %s
00008B82   00408B82      0   ACCEPT
00008B89   00408B89      0   resume
00008B90   00408B90      0   err: %u
00008B99   00408B99      0   DCC ACCEPT %s %s %s
00008BAE   00408BAE      0   dcc_resume: cant find port %s
00008BD1   00408BD1      0   dcc.dir
00008BE5   00408BE5      0   unable to open (%s): %u
00008BFD   00408BFD      0   resuming dcc from %s to %s
00008C19   00408C19      0   DCC RESUME %s %s %u

00009499   00409499      0   VERSION*
000094AE   004094AE      0   IDENT
000099E0   004099E0      0   jtram.conf
000099EB   004099EB      0   jtr.*
00009A16   00409A16      0   conf_dump: wrote %u lines
0000A270   0040A270      0   get of %s incomplete at %u bytes
0000A2B0   0040A2B0      0   get of %s completed (%u bytes), %u seconds %u cps
0000A2F0   0040A2F0      0   error while writing to %s (%u)
0000A65C   0040A65C      0   chdir: %s -> %s (%u)
0000A750   0040A750      0   dcc_wait: get of %s from %s timed out
0000A790   0040A790      0   dcc_wait: closing [#%u] %s:%u (%s)
0000AA30   0040AA30      0   %u Send(s) %u Get(s) (%u transfer(s) total) UP:%ucps
DOWN:%ucps Total:%ucps
0000ACD0   0040ACD0      0   send of %s incomplete at %u bytes
0000AD10   0040AD10      0   send of %s completed (%u bytes), %u seconds %u cps
0000AF50   0040AF50      0   cant open %s (err:%u) pwd:{%s}
0000AF70   0040AF70      0   DCC SEND %s %u %u %u
0000B757   0040B757      0   %s exited with code %u
0000B77B   0040B77B      0   exec: Error:%u pwd:%s cmd:%s
0000BB40   0040BB40      0   dcc.pass
0000BB49   0040BB49      0   bot.port
0000BB52   0040BB52      0   %s bad pass from "%s"@%s
0000BCC9   0040BCC9      0   %s: connect from %s
0000BD33   0040BD33      0   jtr.bin
0000BD3B   0040BD3B      0   msrll.exe
0000BD45   0040BD45      0   jtr.home
0000BD57   0040BD57      0   jtr.id
0000BD63   0040BD63      0   irc.quit
0000BD6E   0040BD6E      0   servers
collective7.zxy0.com,collective7.zxy0.com:9999!,collective7.zxy0.com:8080
0000BDCA   0040BDCA      0   irc.chan
0000BDD3   0040BDD3      0   #mils
0000C2B9   0040C2B9      0   jtram.conf
0000C5B1   0040C5B1      0   irc.user
0000C5BA   0040C5BA      0   %s : USERID : UNIX : %s
0000C6A4   0040C6A4      0   QUIT :FUCK %u
0000C742   0040C742      0   Killed!? Arrg! [%u]
0000C756   0040C756      0   QUIT :%s
0000C897   0040C897      0   Rll enhanced drive
0000C8C0   0040C8C0      0   software\microsoft\windows\currentversion\run
0000EA60   0040EA60      0   usage %s: server[:port] amount
0000EB3E   0040EB3E      0   %s %s %s <PARAM>
0000EB80   0040EB80      0   %s: [NETWORK|all] %s <"parm"> ...
0000EE20   0040EE20      0   USER %s localhost 0 :%s
0000EE38   0040EE38      0   NICK %s
```

6.2.1. jtram.conf

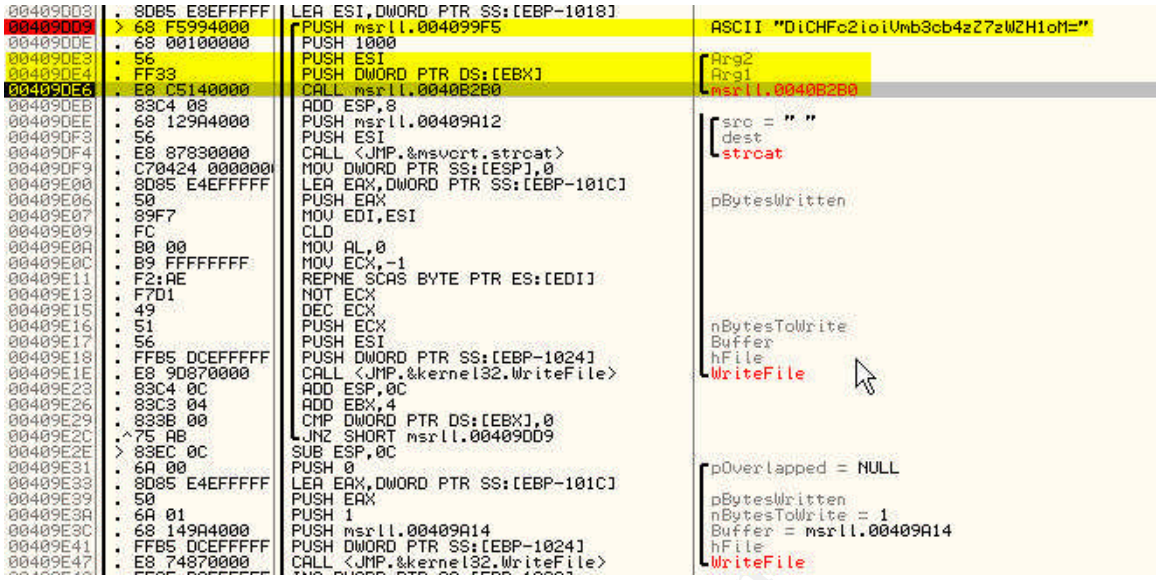
The file jtram.conf contains encrypted content. The file gets read and re-written every time the binary is executed. If we would be able to prevent the binary from encrypting the contents before the file gets written, the contents would be saved in clear text.

CreateFileA is a function responsible for creating files. CTRL-M in OllyDbg brings up all the symbolic names used in a module, so we use this to show the location of the function calls.

It occurs multiple times in the main module, however, the function that gets called at address 0x00409D99 refers to jtram.conf, as can be seen below.

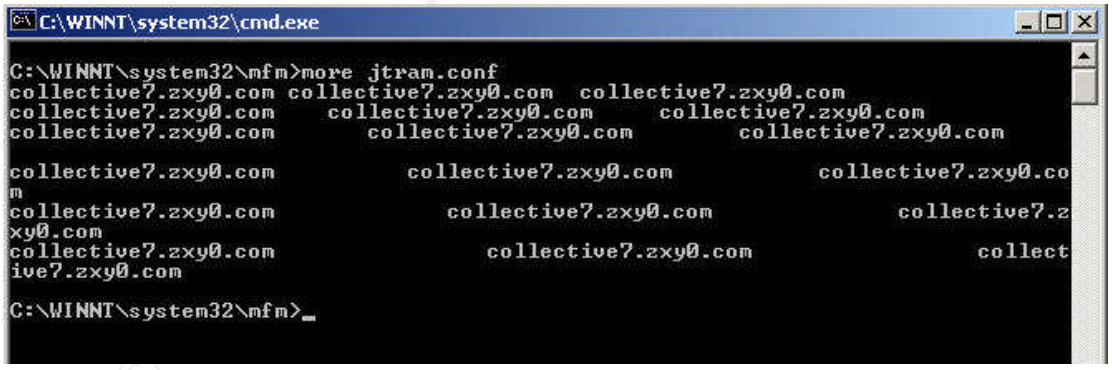


Immediately thereafter, we see a string that seems to be randomly generated, a function call and a string operation, strcat(), to concatenate strings. A breakpoint was set at the 'push' to stop the program at that point.



The function call at 0x00409DE6 XORs the random string and the string that should be 'encrypted'. Putting NOPs where the function call is prevents this from taking place.

Continuing the program, the file jtram.conf gets rewritten, with the content in cleartext.



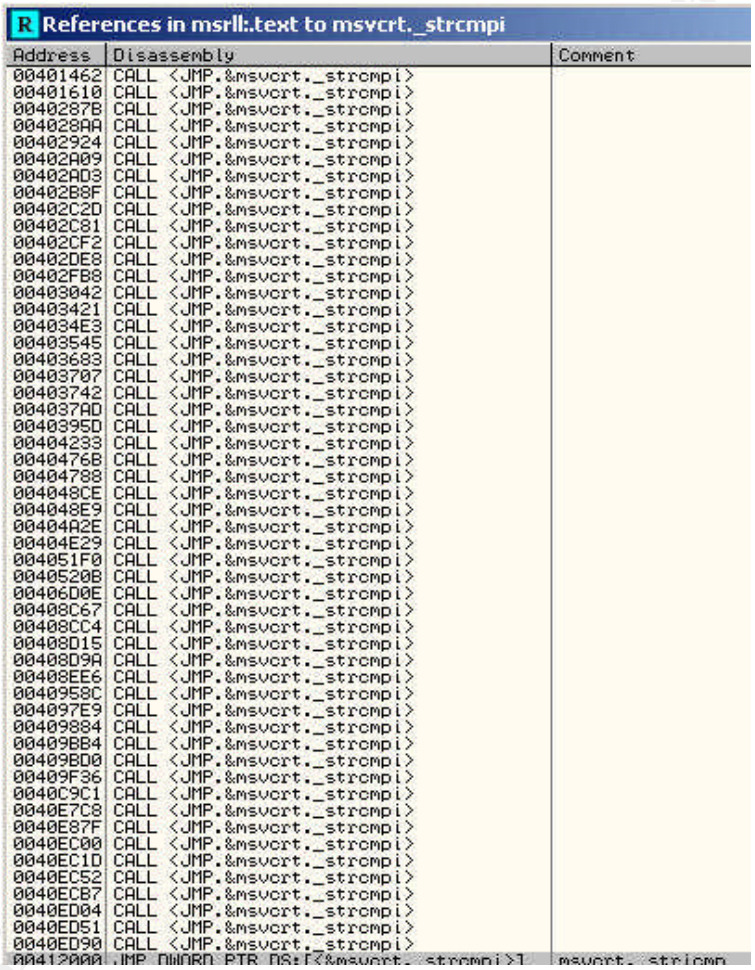
It is unclear why the file gets rewritten every time the binary gets executed. The content (collective7.zxy0.com) gets read out and written back every time the program is run.

6.2.2. Control of the IRCBot

To see how the IRCBot is controlled, we will check for the occurrence where string comparison functions are being used in the module, as it will be there where the input of the IRC channel will be processed.

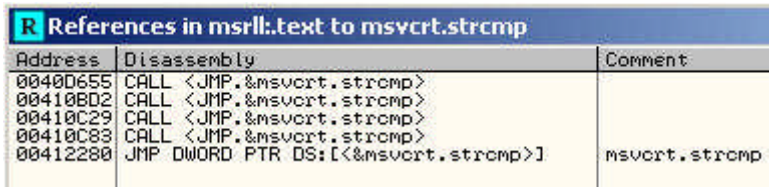
strcmpi() compares two strings, regardless of case.

Occurrences of strcmpi():



strcmp() compares two strings, however, it is case-sensitive.

Occurrences of strcmp():



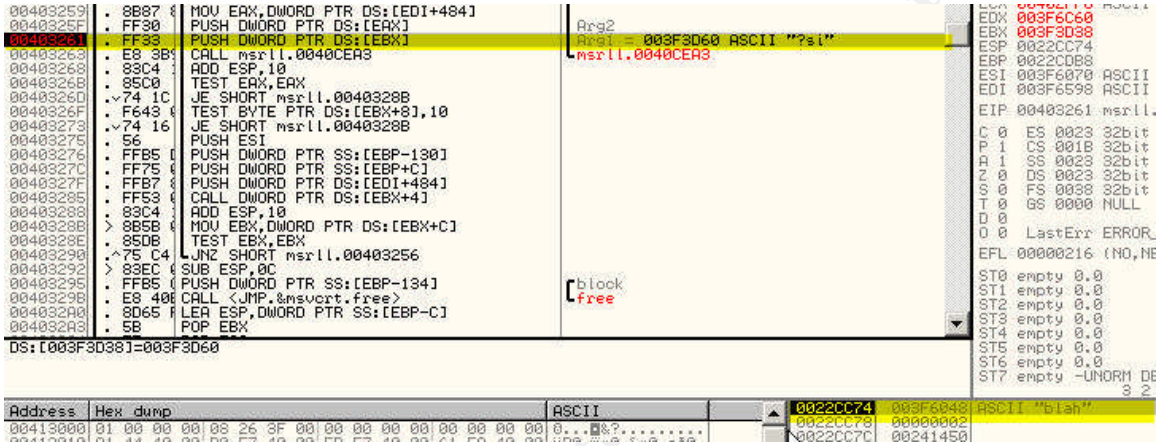
We will work our way through all these function calls, starting with the strcmpi calls.

This is done on a ‘clean’ – unpatched, yet unpacked, version of the msrll.exe.

The string comparison commands are narrowed down to the ones that get executed whenever something is input on the IRC channel.

6.2.2.1. IRCBot commands

There is a function call at 0x00403263 that has 2 arguments as parameters: the input from the IRC channel and whatever commands are allowed.



The push at 0x00403261 points to a memory address, 0x003F3D60 (containing ASCII “?si”). Looking at the memory region 0x003F0000 via the Memory Map – “Dump in CPU”, we can see the commands. I saved the dump into a file and parsed it with a Perl script [PERLSCRIPT] I wrote for all occurrences of “?<command>” with the following results, sorted by alphabet:

```
?!fif           ?exec           ?lsmod          ?run
?akick          ?fif            ?md5p           ?say
?aop            ?free           ?mkdir          ?set
?cd             ?get            ?move           ?si
?clone          ?hostname       ?msg            ?sklist
?clones         ?hush           ?nick           ?smurf
?con            ?insmod         ?op             ?ssl
?copy           ?join           ?part           ?status
?crash          ?jolt           ?ping           ?sums
?dcc            ?jump           ?play           ?syn
?dccsk          ?kb             ?ps             ?uattr
?del            ?kill           ?pwd            ?udp
?die            ?killall        ?raw            ?unset
?dir            ?killsk         ?reboot         ?update
?dump           ?login          ?rmdir          ?uptime
?echo           ?ls             ?rmmod          ?wget
```

This looks like a relative complete list of probably valid commands to control the IRCBot.

6.2.2.2. Finding an authentication section

Looking through the code sections, one stands out: it talks about ‘PASS’ and ‘logged in’. The section starts at address 0x00415B1B.

I am not sure when the program jumps to this section. Checking the call trace (CTRL-K in OllyDbg) for every reasonable command in this section does not reveal anything. I am guessing that the command that jumps to this section gets its jump address dynamically, by pointing at register content rather than fixed addresses. If the program can be tricked to jump to this section, we may be able to gain control over the bot.

The place where the authentication has been successfully verified might be at around 0x00405B87. That is the location in the code where arguments are getting supplied to the function call at 0x00405B93 that then jumps over to 0x00404481.

I am lacking the assembler knowledge to accomplish the jump to this authentication section or to 00x00404481 without crashing the program (I tried modifying calls to point to that location instead, but got access violations), so this is where I stop the code analysis section of this paper.

7. Analysis Wrap-Up

Analysis Wrap-Up - 15 points

Based on your analysis, what is the malware specimen's capabilities? What does it do? Who would use the program? What defensive measures can you derive from your analysis to prevent future attacks by this specimen and eliminate current infections? What other information can be deduced about the program?

7.1. Capabilities of the Specimen

- installs itself as system service under fake name ('RLL System Drive') that starts automatically on system start-up
- features an integrated IRCBot that connects to an external IRC server, joins a predefined channel and waits for orders
- cycles through different ports on the IRC server in case a port is not reachable
- when kicked off channel, joins back in automatically
- opens a shell on the infected machine on port 2200
- vast list of commands enable in-depth control of the IRCBot
    - IRC-typical commands such as DCC support, commands for maintaining channel control
    - Remote control of the infected system: show contents of directories, remote download files, crash/reboot the system, modify filesystem (mkdir etc), execute commands on system (run)
    - Clone
    - ability to launch syn-, smurf- and jolt-based Denial-Of-Service attacks [SMURF], [JOLT2]

Note: regarding the comments about the list of commands above: since I was not able to gain control over the IRCBot in the previous section, I assume that the commands that were found in memory are valid commands. I interpreted the functionality of those commands by the names of those (i.e. ?jolt launching a jolt attack, ?mkdir creating a directory on the infected host etc).

7.2. Behaviour

Summary of behaviour: upon execution, the binary

- creates a directory in Winnt\System32 called mfm
- copies itself over
- executes itself from the new location
- tries to read in a configuration file, jtram.conf in that directory and re-writes that file. If the file does not exist, it uses its default configuration (the IRC server it connects to is set to collective7.zxy0.com)
- deletes the original file
- installs itself as a system-service, using a description of 'RLL enhanced drive', set to start automatically at system start-up
- opens listening ports on the infected machine, TCP 113 for Ident service to supply information to querying IRC server/s, TCP2200 for a backdoor shell
- connects to an IRC server, trying pre-set ports until successful. Uses randomly created nick name and user identification string
- logs into channel #mils and waits for input

7.3. Audience that would use this Malware

The target audience that would use this malware would be people desiring to gain control over Windows-based host systems. The program can be used to control and modify an infected system, provide support in controlling IRC channels, host files for (illegal) distribution (files would be accessible on the infected system per IRC DCC sessions) and to launch Denial-Of-Service-based attacks on other systems.

7.4. Defensive Measures

The following measures should always be implemented:

- users must be educated about the risks involved with accessing (local and remote) sites in the Intranet and the Internet; the dangers of visiting untrusted sites; the use of untrusted applications; the risks involved with e-mail (opening attachments for example)
- systems must always be patched up to the latest revisions to make sure that the operating system or installed applications do not facilitate a local or remote compromise
- hosts need to be locked down according to strict security standards, locally as well as on the network-level. Defense-in-Depth should always be employed: the securing of devices, systems, applications, networks, access on multiple levels to enable a maximum level of protection
- local protective and defensive measures should include the use of anti-virus scanners, host-based firewalls, strict security policies that are applied locally and on the network as a whole
- network-based defensive measures should include intrusion detection and –prevention systems, firewalls, router/switch-based access lists
- applications that can be used by users and that access untrusted destinations should be restricted to an absolute minimum (e.g. only use internal instant messaging if at all, prohibit the use of other instant messengers, chat applications like IRC etc, restrict website access to a limited number of sites – at least communicate what kind of websites are not approved to be accessed)

7.5. Other information

Using the name of the configuration file, jtram.conf, as keyword with Google, I found out that "Troj/Tometa-A - BKDR_TOMETA.A" is the real name of the program. It is classified as a Trojan.

Excerpts from the information page [TRENDMICRO]:

```
[…]
Details:

Installation and Autostart

Upon execution, this memory-resident backdoor program creates the folder mfm in the
Windows system directory. It then drops the following files in the said folder:

MSRLL.EXE – main malware executable
JTRAM.CONF – non-malicious data file used by the malware
It creates the following autostart entry on Windows 95, 98, and ME to ensure its
execution at every system startup:

HKEY_LOCAL_MACHINE\Software\Microsoft\
Windows\CurrentVersion\Run
Rll enhanced drive = "%System%\mfm\msrll.exe"

(Note: %System% is the Windows system folder, which is usually C:\Windows\System on
Windows 95, 98 and ME, C:\WINNT\System32 on Windows NT and 2000, and C:\Windows\System32
on Windows XP.)

On Windows NT, 2000, and XP systems, it attempts to add itself as a service using the
name Rll enhanced drive by adding the following registry key:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\mfm

Backdoor Capability

This backdoor program attempts to connect to the Internet Relay Chat (IRC) server of
collective7.zxy0.com. It cycles through remote ports 6667 (default IRC port), 9999, and
8080 when attempting to connect to the server.

Once connected, it then joins a channel, where it awaits for commands from a remote user.
It also listens for commands from the TCP port 2200.

Other Details

It arrives Aspack-compressed.
[…]
```

Since I am running Windows 2000, as mentioned in the first section of this paper, the trojan did not create a key under `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\ CurrentVersion\Run`, it only installed itself as a service.

8. Appendix

8.1. References

[DOGS]
http://www.campsitstay.com/Kiki_Neo.jpg
- my kids, Kiki and Neo (left to right)

[IDAPRO]
http://www.datarescue.com/

[OLLYDBG]
http://home.t-online.de/home/Ollydbg/

[SYSINTERNALS]
http://www.sysinternals.com/ntw2k/utilities.shtml

[BINTEXT]
http://www.foundstone.com/

[REGSHOT]
http://www.snapfiles.com/get/regshot.html

[WINZIP]
http://www.winzip.com/

[SANSCLASS]
This file was obtained through the SANS GREM course

[FILE]
http://gnuwin32.sourceforge.net/packages/file.htm

[ASPACK]
http://www.aspack.com/

[INDEXDAT]
http://www.exits.ro/index-dat-files.html

[ASPACKUNPACK]
http://biw.rult.at/tuts/mupaspack.rar

[JOLT2]
http://downloads.securityfocus.com/vulnerabilities/exploits/jolt2.c

[SMURF]
http://www.sans.org/resources/idfaq/smurf.doc

[TRENDMICRO]
http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=BKDR_TOMETA.A

8.2. Perl script to extract commands

[PERLSCRIPT]

```
#!/usr/bin/perl
$MEMFILE=$ARGV[0];
chomp ($MEMFILE);

print ("MEMFILE is $ARGV[0]\n");

open(INPUT,"$MEMFILE")||die("cant open $MEMFILE.\n");
@memfile=<INPUT>;
close(INPUT);

foreach $line (0..$#memfile)
{
    chomp ($memfile[$line]);
    if($memfile[$line]=~/(\?\w+)/)
    {
        $cmd=$1;
        print("$cmd\n");
    }
    elsif ($memfile[$line]=~/(\?\!\w+)/)
    {
        $cmd=$1;
        print("$cmd\n");
    }
}
```