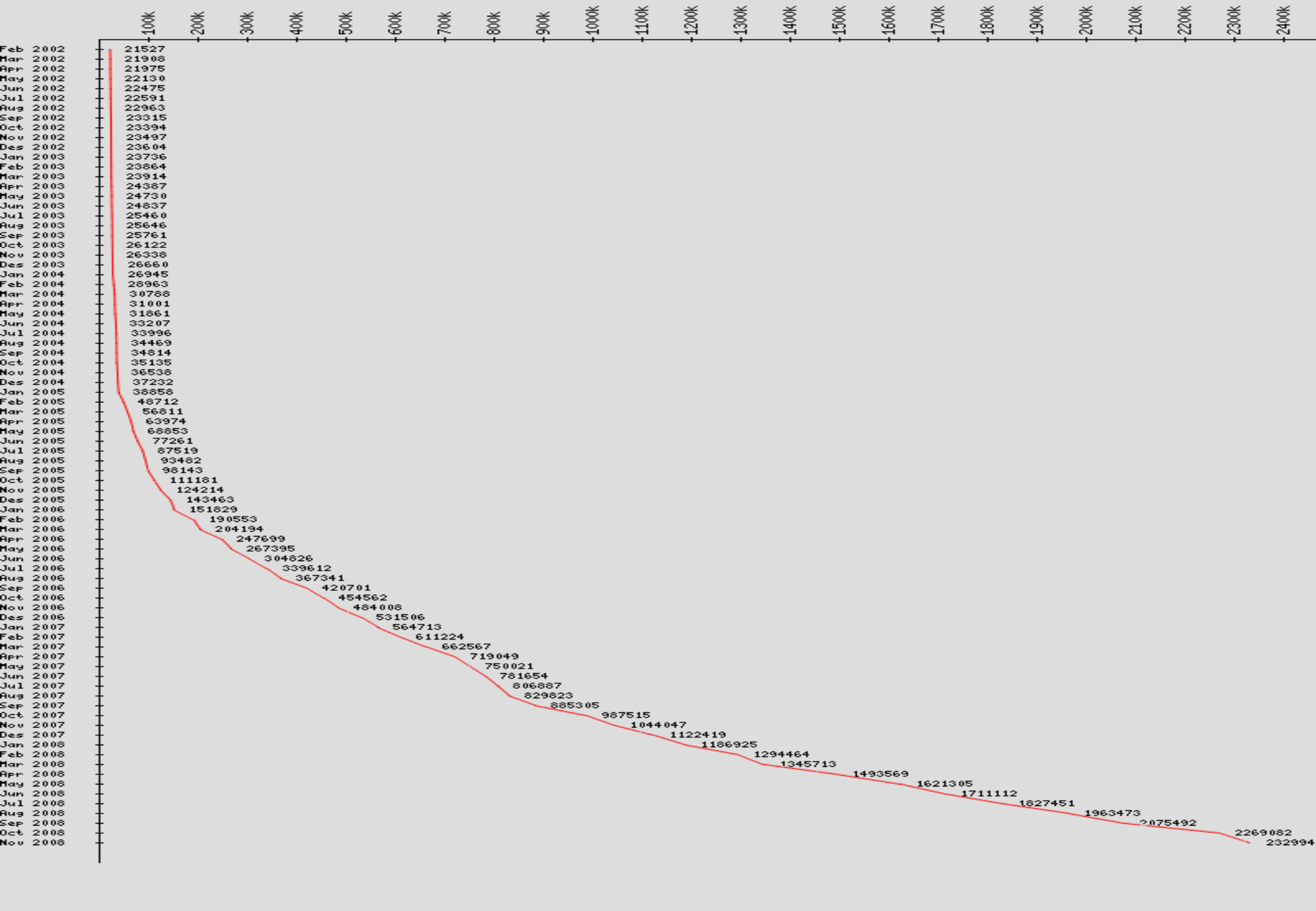

NORMAN®
Enter
PgDn
End
PgUp
Home
Back Space
Scroll Lock
Pause Break
Display
A flood of malware
A view from the antivirus lab
Snorre Fagerland, senior virus analyst

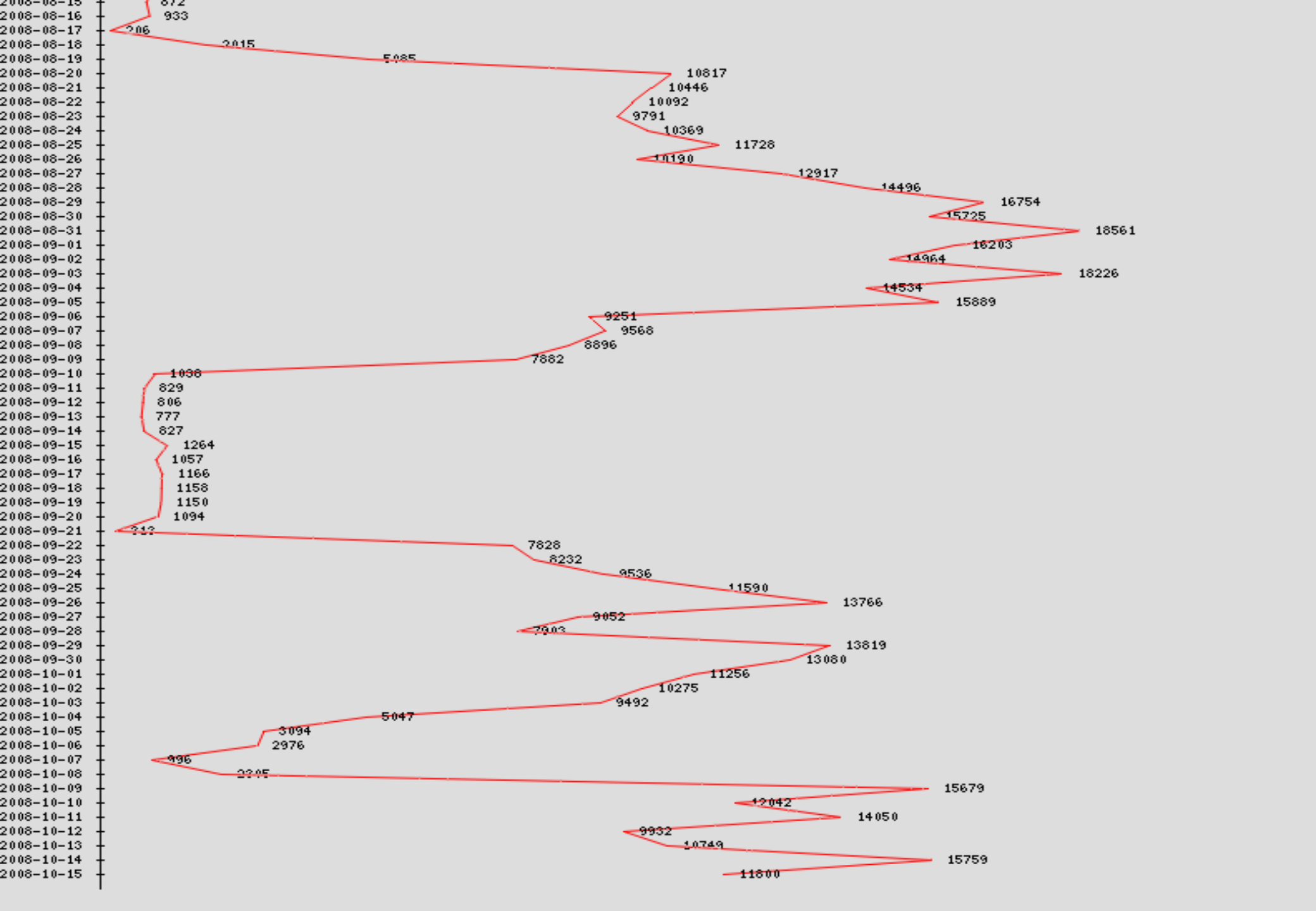
In 1988

- A new virus was a major event
- Would trigger a flurry of analysis activity worldwide
- Analysis could take days
- Detailed descriptions would be made for all new viruses

In 2008

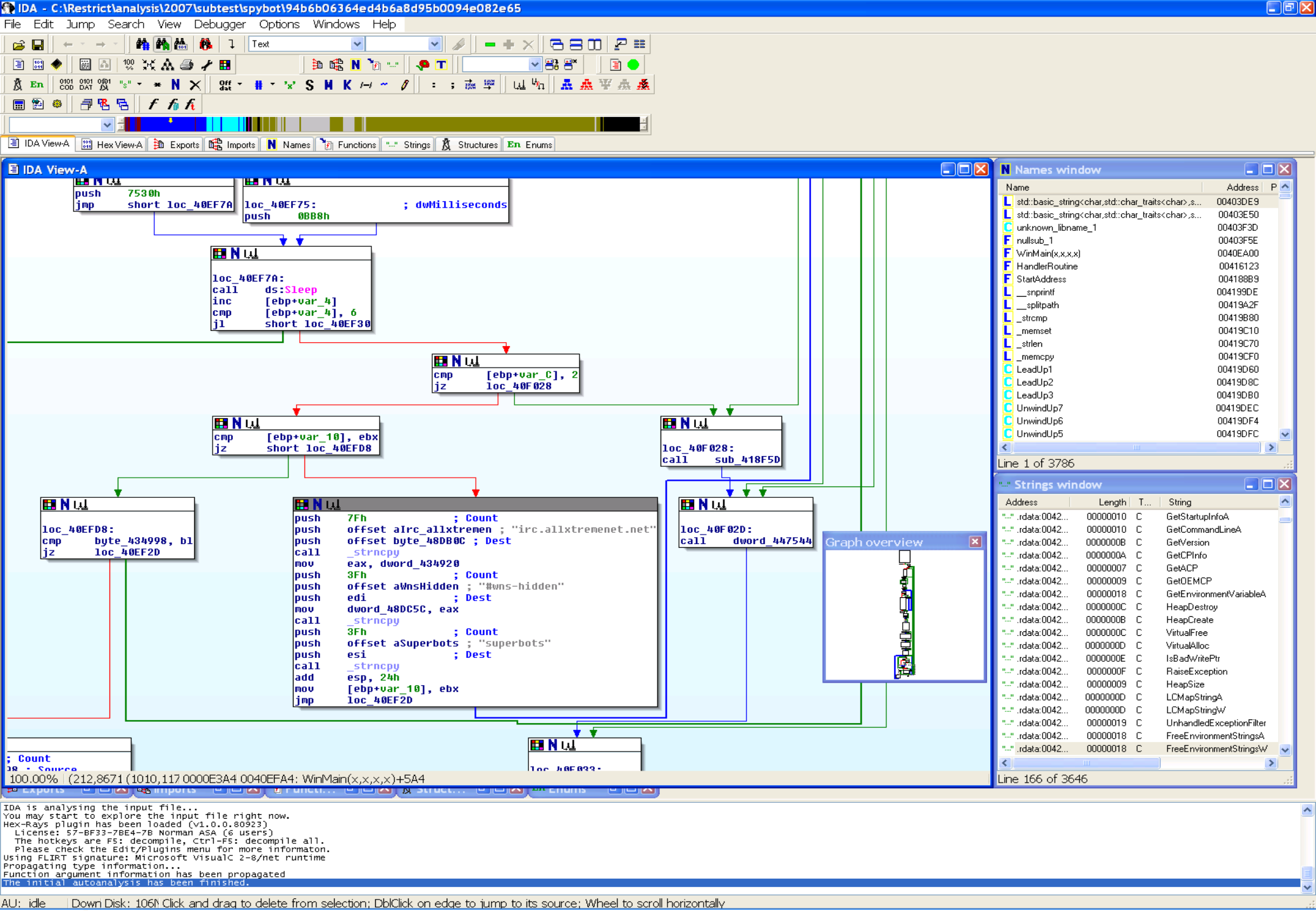
- A new malware is usually almost a negligible event
- Will trigger a small movement of electrons in automatic systems
- Analysis takes seconds or at most minutes
- Detailed descriptions are very few. Usually descriptions are made for whole families, covering hundreds of malwares.

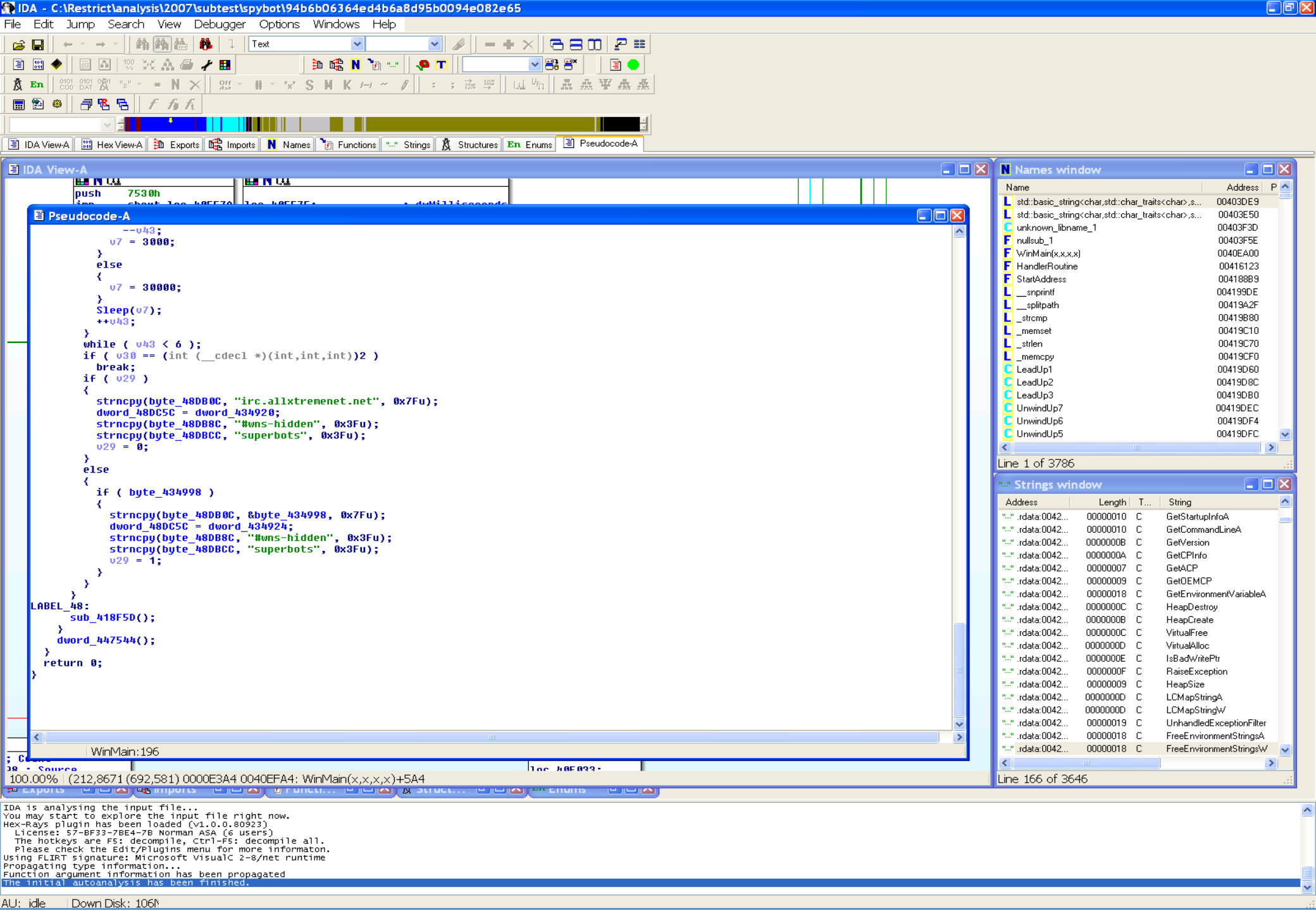

100k
200k
300k
400k
500k
600k
700k
800k
900k
1000k
1100k
1200k
1300k
1400k
1500k
1600k
1700k
1800k
1900k
2000k
2100k
2200k
2300k
2400k
Feb 2002 21527
Mar 2002 21908
Apr 2002 21975
May 2002 22130
Jun 2002 22475
Jul 2002 22591
Aug 2002 22963
Sep 2002 23315
Oct 2002 23394
Nov 2002 23497
Des 2002 23604
Jan 2003 23736
Feb 2003 23864
Mar 2003 23914
Apr 2003 24387
May 2003 24730
Jun 2003 24837
Jul 2003 25460
Aug 2003 25646
Sep 2003 25761
Oct 2003 26122
Nov 2003 26338
Des 2003 26660
Jan 2004 26945
Feb 2004 28963
Mar 2004 30788
Apr 2004 31001
May 2004 31861
Jun 2004 33207
Jul 2004 33996
Aug 2004 34469
Sep 2004 34814
Oct 2004 35135
Nov 2004 36538
Des 2004 37232
Jan 2005 38858
Feb 2005 48712
Mar 2005 56811
Apr 2005 63974
May 2005 68853
Jun 2005 77261
Jul 2005 87519
Aug 2005 93482
Sep 2005 98143
Oct 2005 111181
Nov 2005 124214
Des 2005 143463
Jan 2006 151829
Feb 2006 190553
Mar 2006 204194
Apr 2006 247699
May 2006 267395
Jun 2006 304826
Jul 2006 339612
Aug 2006 367341
Sep 2006 420701
Oct 2006 454562
Nov 2006 484008
Des 2006 531506
Jan 2007 564713
Feb 2007 611224
Mar 2007 662567
Apr 2007 719049
May 2007 750021
Jun 2007 781654
Jul 2007 806887
Aug 2007 829823
Sep 2007 885305
Oct 2007 987515
Nov 2007 1044047
Des 2007 1122419
Jan 2008 1186925
Feb 2008 1294464
Mar 2008 1345713
Apr 2008 1493569
May 2008 1621305
Jun 2008 1711112
Jul 2008 1827451
Aug 2008 1963473
Sep 2008 2075492
Oct 2008 2269082
Nov 2008 2329941

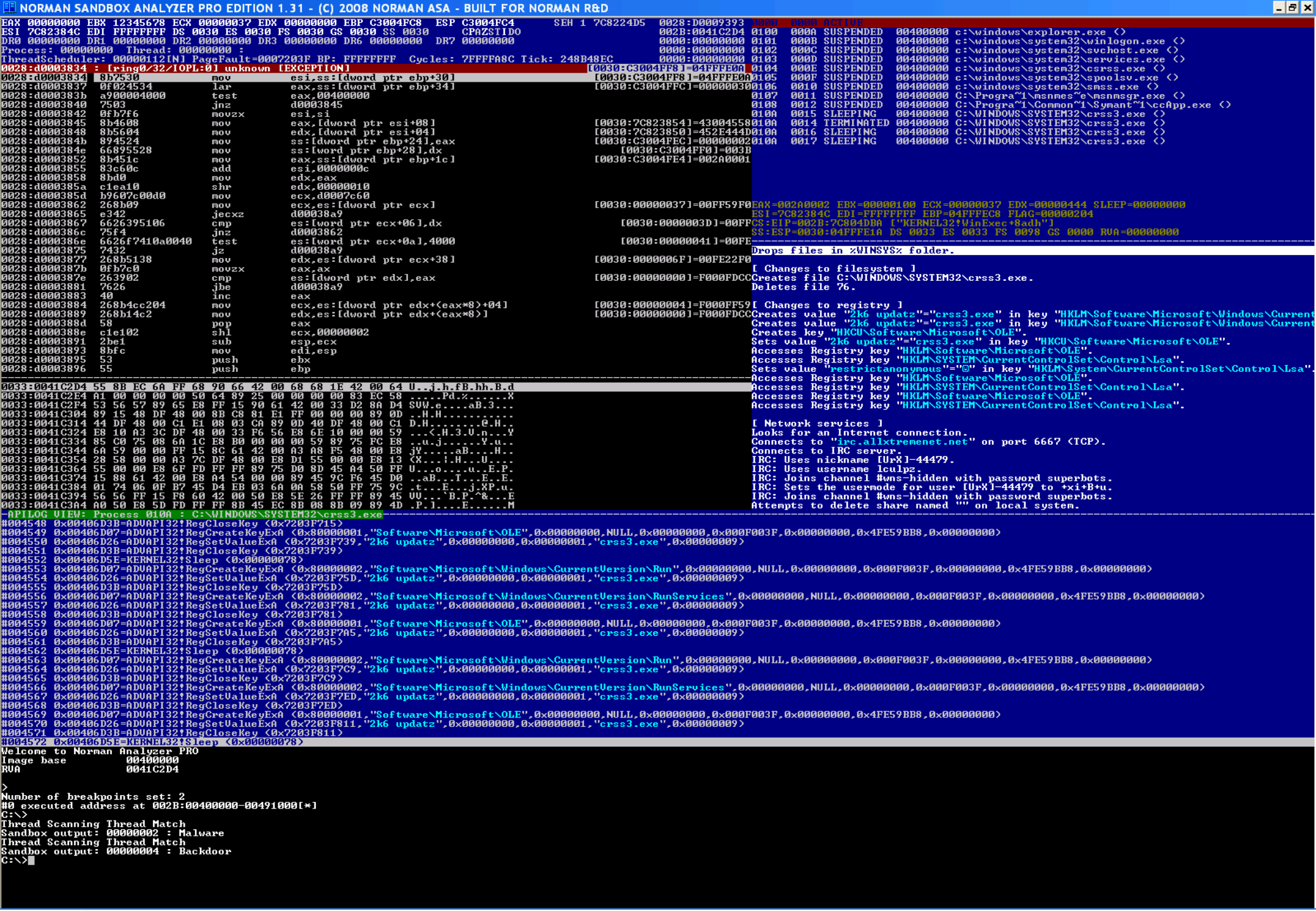

2008-08-15
2008-08-16
2008-08-17
2008-08-18
2008-08-19
2008-08-20
2008-08-21
2008-08-22
2008-08-23
2008-08-24
2008-08-25
2008-08-26
2008-08-27
2008-08-28
2008-08-29
2008-08-30
2008-08-31
2008-09-01
2008-09-02
2008-09-03
2008-09-04
2008-09-05
2008-09-06
2008-09-07
2008-09-08
2008-09-09
2008-09-10
2008-09-11
2008-09-12
2008-09-13
2008-09-14
2008-09-15
2008-09-16
2008-09-17
2008-09-18
2008-09-19
2008-09-20
2008-09-21
2008-09-22
2008-09-23
2008-09-24
2008-09-25
2008-09-26
2008-09-27
2008-09-28
2008-09-29
2008-09-30
2008-10-01
2008-10-02
2008-10-03
2008-10-04
2008-10-05
2008-10-06
2008-10-07
2008-10-08
2008-10-09
2008-10-10
2008-10-11
2008-10-12
2008-10-13
2008-10-14
2008-10-15
872
933
206
2015
5085
10817
10446
10092
9791
10369
11728
10190
12917
14496
16754
15725
18561
16203
14964
18226
14534
15889
9251
9568
8896
7882
1036
829
806
777
827
1264
1057
1166
1158
1150
1094
212
7828
8232
9536
11590
13766
9052
7903
13819
13080
11256
10275
9492
5047
3094
2976
996
2205
15679
12042
14050
9932
10749
15759
11800

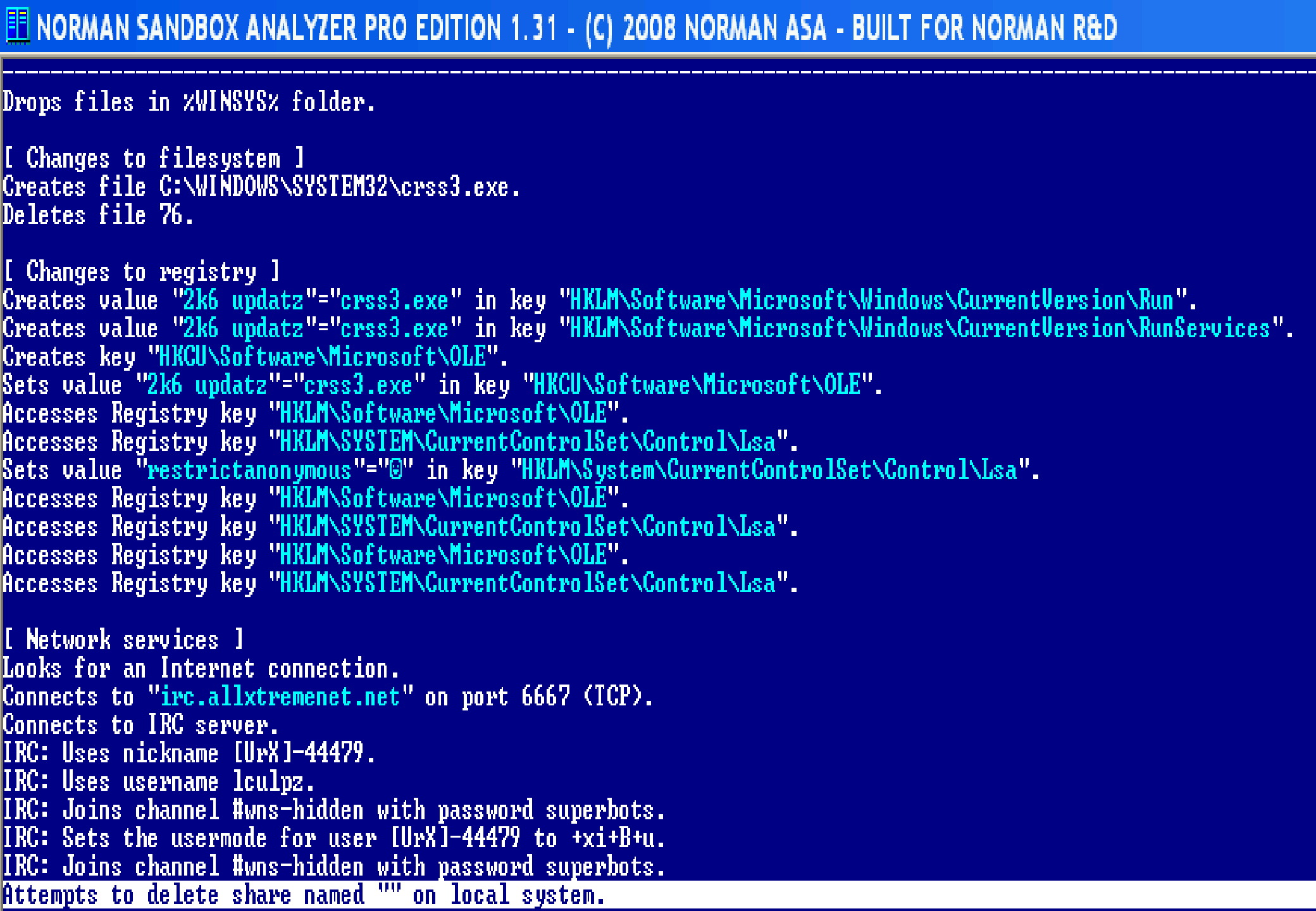
Analysis work

- Oldfashioned code analysis still used.
- Tools have improved greatly since old days
- A LOT of work done by automatic systems.


IDA - C:\Restrict\analysis\2007\subtest\spybot\94b6b06364ed4b6a8d95b0094e082e65
File Edit Jump Search View Debugger Options Windows Help
IDA View-A
Hex View-A
Exports
Imports
Names
Functions
Strings
Structures
Enums
push 7530h
jmp short loc_40EF7A
loc_40EF75: ; dwMilliseconds
push 0BB8h
loc_40EF7A:
call ds:Sleep
inc [ebp+var_4]
cmp [ebp+var_4], 6
jl short loc_40EF30
cmp [ebp+var_C], 2
jz loc_40F028
cmp [ebp+var_10], ebx
jz short loc_40EFD8
loc_40F028:
call sub_418F5D
loc_40EFD8:
cmp byte_434998, bl
jz loc_40EF2D
push 7Fh ; Count
push offset aIrc_allxtremen ; "irc.allxtremenet.net"
push offset byte_48DB0C ; Dest
call _strncpy
mov eax, dword_434920
push 3Fh ; Count
push offset aWnsHidden ; "#wns-hidden"
push edi ; Dest
mov dword_48DC5C, eax
call _strncpy
push 3Fh ; Count
push offset aSuperbots ; "superbots"
push esi ; Dest
call _strncpy
add esp, 24h
mov [ebp+var_10], ebx
jmp loc_40EF2D
loc_40F02D:
call dword_447544
Graph overview
100.00% (212,8671 (1010,117 0000E3A4 0040EFA4: WinMain(x,x,x,x)+5A4
Names window
Name Address
std::basic_string<char,std::char_traits<char>,s... 00403DE9
std::basic_string<char,std::char_traits<char>,s... 00403E50
unknown_libname_1 00403F3D
nullsub_1 00403F5E
WinMain(x,x,x,x) 0040EA00
HandlerRoutine 00416123
StartAddress 004188B9
__snprintf 004199DE
__splitpath 00419A2F
_strcmp 00419B80
_memset 00419C10
_strlen 00419C70
_memcpy 00419CF0
LeadUp1 00419D60
LeadUp2 00419D8C
LeadUp3 00419DB0
UnwindUp7 00419DEC
UnwindUp6 00419DF4
UnwindUp5 00419DFC
Line 1 of 3786
Strings window
Address Length T... String
.rdata:0042... 00000010 C GetStartupInfoA
.rdata:0042... 00000010 C GetCommandLineA
.rdata:0042... 0000000B C GetVersion
.rdata:0042... 0000000A C GetCPInfo
.rdata:0042... 00000007 C GetACP
.rdata:0042... 00000009 C GetOEMCP
.rdata:0042... 00000018 C GetEnvironmentVariableA
.rdata:0042... 0000000C C HeapDestroy
.rdata:0042... 0000000B C HeapCreate
.rdata:0042... 0000000C C VirtualFree
.rdata:0042... 0000000D C VirtualAlloc
.rdata:0042... 0000000E C IsBadWritePtr
.rdata:0042... 0000000F C RaiseException
.rdata:0042... 00000009 C HeapSize
.rdata:0042... 0000000D C LCMapStringA
.rdata:0042... 0000000D C LCMapStringW
.rdata:0042... 00000019 C UnhandledExceptionFilter
.rdata:0042... 00000018 C FreeEnvironmentStringsA
.rdata:0042... 00000018 C FreeEnvironmentStringsW
Line 166 of 3646
IDA is analysing the input file...
You may start to explore the input file right now.
Hex-Rays plugin has been loaded (v1.0.0.80923)
License: 57-BF33-7BE4-7B Norman ASA (6 users)
The hotkeys are F5: decompile, Ctrl-F5: decompile all.
Please check the Edit/Plugins menu for more informaton.
Using FLIRT signature: Microsoft VisualC 2-8/net runtime
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished.
AU: idle Down Disk: 106\ Click and drag to delete from selection; DblClick on edge to jump to its source; Wheel to scroll horizontally


IDA - C:\Restrict\analysis\2007\subtest\spybot\94b6b06364ed4b6a8d95b0094e082e65
File Edit Jump Search View Debugger Options Windows Help
IDA View-A
Hex View-A
Exports
Imports
Names
Functions
Strings
Structures
Enums
Pseudocode-A
Pseudocode-A
--v43;
v7 = 3000;
}
else
{
v7 = 30000;
}
Sleep(v7);
++v43;
}
while (v43 < 6);
if (v30 == (int (__cdecl *)(int,int,int))2)
break;
if (v29)
{
strncpy(byte_48DB0C, "irc.allxtremenet.net", 0x7Fu);
dword_48DC5C = dword_434920;
strncpy(byte_48DB8C, "#wns-hidden", 0x3Fu);
strncpy(byte_48DBCC, "superbots", 0x3Fu);
v29 = 0;
}
else
{
if (byte_434998)
{
strncpy(byte_48DB0C, &byte_434998, 0x7Fu);
dword_48DC5C = dword_434924;
strncpy(byte_48DB8C, "#wns-hidden", 0x3Fu);
strncpy(byte_48DBCC, "superbots", 0x3Fu);
v29 = 1;
}
}
}
LABEL_48:
sub_418F5D();
}
dword_447544();
}
return 0;
}
WinMain:196
Names window
Name
Address
std::basic_string<char,std::char_traits<char>,s... 00403DE9
std::basic_string<char,std::char_traits<char>,s... 00403E50
unknown_libname_1 00403F3D
nullsub_1 00403F5E
WinMain(x,x,x,x) 0040EA00
HandlerRoutine 00416123
StartAddress 004188B9
__snprintf 004199DE
__splitpath 00419A2F
_strcmp 00419B80
_memset 00419C10
_strlen 00419C70
_memcpy 00419CF0
LeadUp1 00419D60
LeadUp2 00419D8C
LeadUp3 00419DB0
UnwindUp7 00419DEC
UnwindUp6 00419DF4
UnwindUp5 00419DFC
Line 1 of 3786
Strings window
Address
Length
T...
String
.rdata:0042... 00000010 C GetStartupInfoA
.rdata:0042... 00000010 C GetCommandLineA
.rdata:0042... 0000000B C GetVersion
.rdata:0042... 0000000A C GetCPInfo
.rdata:0042... 00000007 C GetACP
.rdata:0042... 00000009 C GetOEMCP
.rdata:0042... 00000018 C GetEnvironmentVariableA
.rdata:0042... 0000000C C HeapDestroy
.rdata:0042... 0000000B C HeapCreate
.rdata:0042... 0000000C C VirtualFree
.rdata:0042... 0000000D C VirtualAlloc
.rdata:0042... 0000000E C IsBadWritePtr
.rdata:0042... 0000000F C RaiseException
.rdata:0042... 00000009 C HeapSize
.rdata:0042... 0000000D C LCMapStringA
.rdata:0042... 0000000D C LCMapStringW
.rdata:0042... 00000019 C UnhandledExceptionFilter
.rdata:0042... 00000018 C FreeEnvironmentStringsA
.rdata:0042... 00000018 C FreeEnvironmentStringsW
Line 166 of 3646
100.00% (212,8671 (692,581) 0000E3A4 0040EFA4: WinMain(x,x,x,x)+5A4
IDA is analysing the input file...
You may start to explore the input file right now.
Hex-Rays plugin has been loaded (v1.0.0.80923)
License: 57-BF33-7BE4-7B Norman ASA (6 users)
The hotkeys are F5: decompile, Ctrl-F5: decompile all.
Please check the Edit/Plugins menu for more informaton.
Using FLIRT signature: Microsoft VisualC 2-8/net runtime
Propagating type information...
Function argument information has been propagated
The initial autoanalysis has been finished.
AU: idle
Down Disk: 106


NORMAN SANDBOX ANALYZER PRO EDITION 1.31 - (C) 2008 NORMAN ASA - BUILT FOR NORMAN R&D
EAX 00000000 EBX 12345678 ECX 00000037 EDX 00000000 EBP C3004FC8 ESP C3004FC4 SEH 1 7C8224D5 0028:D0009393
ESI 7C82384C EDI FFFFFFFF DS 0030 ES 0030 FS 0030 GS 0030 SS 0030 CPAZSTIDO 002B:0041C2D4
DR0 00000000 DR1 00000000 DR2 00000000 DR3 00000000 DR6 00000000 DR7 00000000 0000:00000000
Process: 00000000 Thread: 00000000 : 0000:00000000
ThreadScheduler: 00000112[N] PageFault=0007203F BP: FFFFFFFF Cycles: 7FFFFA8C Tick: 248B48EC 0000:00000000
0028:d0003834 : [ring0/32/IOPL:0] unknown [EXCEPTION] [0030:C3004FF8]=04FFFE0A
0028:d0003834 8b7530 mov esi,ss:[dword ptr ebp+30] [0030:C3004FF8]=04FFFE0A
0028:d0003837 0f024534 lar eax,ss:[dword ptr ebp+34] [0030:C3004FFC]=00000030
0028:d000383b a900004000 test eax,00400000
0028:d0003840 7503 jnz d0003845
0028:d0003842 0fb7f6 movzx esi,si
0028:d0003845 8b4608 mov eax,[dword ptr esi+08] [0030:7C823854]=43004558
0028:d0003848 8b5604 mov edx,[dword ptr esi+04] [0030:7C823850]=452E444D
0028:d000384b 894524 mov ss:[dword ptr ebp+24],eax [0030:C3004FEC]=00000002
0028:d000384e 66895528 mov ss:[word ptr ebp+28],dx [0030:C3004FF0]=003B
0028:d0003852 8b451c mov eax,ss:[dword ptr ebp+1c] [0030:C3004FE4]=002A0001
0028:d0003855 83c60c add esi,0000000c
0028:d0003858 8bd0 mov edx,eax
0028:d000385a c1ea10 shr edx,00000010
0028:d000385d b9607c00d0 mov ecx,d0007c60
0028:d0003862 268b09 mov ecx,es:[dword ptr ecx] [0030:00000037]=00FF59F0
0028:d0003865 e342 jecxz d00038a9
0028:d0003867 6626395106 cmp es:[word ptr ecx+06],dx [0030:0000003D]=00FF
0028:d000386c 75f4 jnz d0003862
0028:d000386e 6626f7410a0040 test es:[word ptr ecx+0a],4000 [0030:00000041]=00FE
0028:d0003875 7432 jz d00038a9
0028:d0003877 268b5138 mov edx,es:[dword ptr ecx+38] [0030:0000006F]=00FE22F0
0028:d000387b 0fb7c0 movzx eax,ax
0028:d000387e 263902 cmp es:[dword ptr edx],eax [0030:00000000]=F000FDCC
0028:d0003881 7626 jbe d00038a9
0028:d0003883 40 inc eax
0028:d0003884 268b4cc204 mov ecx,es:[dword ptr edx+(eax*8)+04] [0030:00000004]=F000FF59
0028:d0003889 268b14c2 mov edx,es:[dword ptr edx+(eax*8)] [0030:00000000]=F000FDCC
0028:d000388d 58 pop eax
0028:d000388e c1e102 shl ecx,00000002
0028:d0003891 2be1 sub esp,ecx
0028:d0003893 8bfc mov edi,esp
0028:d0003895 53 push ebx
0028:d0003896 55 push ebp
0033:0041C2D4 55 8B EC 6A FF 68 90 66 42 00 68 68 1E 42 00 64 U..j.h.fB.hh.B.d
0033:0041C2E4 A1 00 00 00 00 50 64 89 25 00 00 00 00 83 EC 58 .....Pd.%......X
0033:0041C2F4 53 56 57 89 65 E8 FF 15 90 61 42 00 33 D2 8A D4 SVW.e....aB.3...
0033:0041C304 89 15 48 DF 48 00 8B C8 81 E1 FF 00 00 00 89 0D ..H.H...........
0033:0041C314 44 DF 48 00 C1 E1 08 03 CA 89 0D 40 DF 48 00 C1 D.H........@.H..
0033:0041C324 E8 10 A3 3C DF 48 00 33 F6 56 E8 6E 10 00 00 59 ...<.H.3.V.n...Y
0033:0041C334 85 C0 75 08 6A 1C E8 B0 00 00 00 59 89 75 FC E8 ..u.j......Y.u..
0033:0041C344 6A 59 00 00 FF 15 8C 61 42 00 A3 A8 F5 48 00 E8 jY.....aB....H..
0033:0041C354 28 58 00 00 A3 7C DF 48 00 E8 D1 55 00 00 E8 13 (X...|.H...U....
0033:0041C364 55 00 00 E8 6F FD FF FF 89 75 D0 8D 45 A4 50 FF U...o....u..E.P.
0033:0041C374 15 88 61 42 00 E8 A4 54 00 00 89 45 9C F6 45 D0 ..aB...T...E..E.
0033:0041C384 01 74 06 0F B7 45 D4 EB 03 6A 0A 58 50 FF 75 9C .t...E...j.XP.u.
0033:0041C394 56 56 FF 15 F8 60 42 00 50 E8 5E 26 FF FF 89 45 VV...`B.P.^&...E
0033:0041C3A4 A0 50 E8 5D FD FF FF 8B 45 EC 8B 08 8B 09 89 4D .P.]....E......M
-APILOG VIEW: Process 010A : C:\WINDOWS\SYSTEM32\crss3.exe
#004548 0x00406D3B=ADVAPI32!RegCloseKey (0x7203F715)
#004549 0x00406D07=ADVAPI32!RegCreateKeyExA (0x80000001,"Software\Microsoft\OLE",0x00000000,NULL,0x00000000,0x000F003F,0x00000000,0x4FE59BB8,0x00000000)
#004550 0x00406D26=ADVAPI32!RegSetValueExA (0x7203F739,"2k6 updatz",0x00000000,0x00000001,"crss3.exe",0x00000009)
#004551 0x00406D3B=ADVAPI32!RegCloseKey (0x7203F739)
#004552 0x00406D5E=KERNEL32!Sleep (0x00000078)
#004553 0x00406D07=ADVAPI32!RegCreateKeyExA (0x80000002,"Software\Microsoft\Windows\CurrentVersion\Run",0x00000000,NULL,0x00000000,0x000F003F,0x00000000,0x4FE59BB8,0x00000000)
#004554 0x00406D26=ADVAPI32!RegSetValueExA (0x7203F75D,"2k6 updatz",0x00000000,0x00000001,"crss3.exe",0x00000009)
#004555 0x00406D3B=ADVAPI32!RegCloseKey (0x7203F75D)
#004556 0x00406D07=ADVAPI32!RegCreateKeyExA (0x80000002,"Software\Microsoft\Windows\CurrentVersion\RunServices",0x00000000,NULL,0x00000000,0x000F003F,0x00000000,0x4FE59BB8,0x00000000)
#004557 0x00406D26=ADVAPI32!RegSetValueExA (0x7203F781,"2k6 updatz",0x00000000,0x00000001,"crss3.exe",0x00000009)
#004558 0x00406D3B=ADVAPI32!RegCloseKey (0x7203F781)
#004559 0x00406D07=ADVAPI32!RegCreateKeyExA (0x80000001,"Software\Microsoft\OLE",0x00000000,NULL,0x00000000,0x000F003F,0x00000000,0x4FE59BB8,0x00000000)
#004560 0x00406D26=ADVAPI32!RegSetValueExA (0x7203F7A5,"2k6 updatz",0x00000000,0x00000001,"crss3.exe",0x00000009)
#004561 0x00406D3B=ADVAPI32!RegCloseKey (0x7203F7A5)
#004562 0x00406D5E=KERNEL32!Sleep (0x00000078)
#004563 0x00406D07=ADVAPI32!RegCreateKeyExA (0x80000002,"Software\Microsoft\Windows\CurrentVersion\Run",0x00000000,NULL,0x00000000,0x000F003F,0x00000000,0x4FE59BB8,0x00000000)
#004564 0x00406D26=ADVAPI32!RegSetValueExA (0x7203F7C9,"2k6 updatz",0x00000000,0x00000001,"crss3.exe",0x00000009)
#004565 0x00406D3B=ADVAPI32!RegCloseKey (0x7203F7C9)
#004566 0x00406D07=ADVAPI32!RegCreateKeyExA (0x80000002,"Software\Microsoft\Windows\CurrentVersion\RunServices",0x00000000,NULL,0x00000000,0x000F003F,0x00000000,0x4FE59BB8,0x00000000)
#004567 0x00406D26=ADVAPI32!RegSetValueExA (0x7203F7ED,"2k6 updatz",0x00000000,0x00000001,"crss3.exe",0x00000009)
#004568 0x00406D3B=ADVAPI32!RegCloseKey (0x7203F7ED)
#004569 0x00406D07=ADVAPI32!RegCreateKeyExA (0x80000001,"Software\Microsoft\OLE",0x00000000,NULL,0x00000000,0x000F003F,0x00000000,0x4FE59BB8,0x00000000)
#004570 0x00406D26=ADVAPI32!RegSetValueExA (0x7203F811,"2k6 updatz",0x00000000,0x00000001,"crss3.exe",0x00000009)
#004571 0x00406D3B=ADVAPI32!RegCloseKey (0x7203F811)
#004572 0x00406D5E=KERNEL32!Sleep (0x00000078)
Welcome to Norman Analyzer PRO
Image base 00400000
RVA 0041C2D4
>
Number of breakpoints set: 2
#0 executed address at 002B:00400000-00491000[*]
C:\>
Thread Scanning Thread Match
Sandbox output: 00000002 : Malware
Thread Scanning Thread Match
Sandbox output: 00000004 : Backdoor
C:\>
0000 0000 ACTIVE
0100 000A SUSPENDED 00400000 c:\windows\explorer.exe ()
0101 000B SUSPENDED 00400000 c:\windows\system32\winlogon.exe ()
0102 000C SUSPENDED 00400000 c:\windows\system32\svchost.exe ()
0103 000D SUSPENDED 00400000 c:\windows\system32\services.exe ()
0104 000E SUSPENDED 00400000 c:\windows\system32\csrss.exe ()
0105 000F SUSPENDED 00400000 c:\windows\system32\spoolsv.exe ()
0106 0010 SUSPENDED 00400000 c:\windows\system32\smss.exe ()
0107 0011 SUSPENDED 00400000 C:\Progra~1\msnmes~1\msnmsgr.exe ()
0108 0012 SUSPENDED 00400000 C:\Progra~1\Common~1\Symant~1\ccApp.exe ()
010A 0015 SLEEPING 00400000 C:\WINDOWS\SYSTEM32\crss3.exe ()
010A 0014 TERMINATED 00400000 C:\WINDOWS\SYSTEM32\crss3.exe ()
010A 0016 SLEEPING 00400000 C:\WINDOWS\SYSTEM32\crss3.exe ()
010A 0017 SLEEPING 00400000 C:\WINDOWS\SYSTEM32\crss3.exe ()
EAX=002A0002 EBX=00000100 ECX=00000037 EDX=00000444 SLEEP=00000000
ESI=?C82384C EDI=FFFFFFFF EBP=04FFFEC8 FLAG=00000204
CS:EIP=002B:?C804DBA ["KERNEL32!WinExec+8adh"]
SS:ESP=0030:04FFFE1A DS 0033 ES 0033 FS 0098 GS 0000 RVA=00000000
Drops files in %WINSYS% folder.
[Changes to filesystem]
Creates file C:\WINDOWS\SYSTEM32\crss3.exe.
Deletes file 76.
[Changes to registry]
Creates value "2k6 updatz"="crss3.exe" in key "HKLM\Software\Microsoft\Windows\Current
Creates value "2k6 updatz"="crss3.exe" in key "HKLM\Software\Microsoft\Windows\Current
Creates key "HKCU\Software\Microsoft\OLE".
Sets value "2k6 updatz"="crss3.exe" in key "HKCU\Software\Microsoft\OLE".
Accesses Registry key "HKLM\Software\Microsoft\OLE".
Accesses Registry key "HKLM\SYSTEM\CurrentControlSet\Control\Lsa".
Sets value "restrictanonymous"="0" in key "HKLM\System\CurrentControlSet\Control\Lsa".
Accesses Registry key "HKLM\Software\Microsoft\OLE".
Accesses Registry key "HKLM\SYSTEM\CurrentControlSet\Control\Lsa".
Accesses Registry key "HKLM\Software\Microsoft\OLE".
Accesses Registry key "HKLM\SYSTEM\CurrentControlSet\Control\Lsa".
[Network services]
Looks for an Internet connection.
Connects to "irc.allxtremenet.net" on port 6667 (TCP).
Connects to IRC server.
IRC: Uses nickname [UrX]-44479.
IRC: Uses username lculpz.
IRC: Joins channel #wns-hidden with password superbots.
IRC: Sets the usermode for user [UrX]-44479 to +xi+B+u.
IRC: Joins channel #wns-hidden with password superbots.
Attempts to delete share named "" on local system.


NORMAN SANDBOX ANALYZER PRO EDITION 1.31 - (C) 2008 NORMAN ASA - BUILT FOR NORMAN R&D
Drops files in %WINSYS% folder.
[Changes to filesystem]
Creates file C:\WINDOWS\SYSTEM32\crss3.exe.
Deletes file 76.
[Changes to registry]
Creates value "2k6 updatz"="crss3.exe" in key "HKLM\Software\Microsoft\Windows\CurrentVersion\Run".
Creates value "2k6 updatz"="crss3.exe" in key "HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices".
Creates key "HKCU\Software\Microsoft\OLE".
Sets value "2k6 updatz"="crss3.exe" in key "HKCU\Software\Microsoft\OLE".
Accesses Registry key "HKLM\Software\Microsoft\OLE".
Accesses Registry key "HKLM\SYSTEM\CurrentControlSet\Control\Lsa".
Sets value "restrictanonymous"="0" in key "HKLM\System\CurrentControlSet\Control\Lsa".
Accesses Registry key "HKLM\Software\Microsoft\OLE".
Accesses Registry key "HKLM\SYSTEM\CurrentControlSet\Control\Lsa".
Accesses Registry key "HKLM\Software\Microsoft\OLE".
Accesses Registry key "HKLM\SYSTEM\CurrentControlSet\Control\Lsa".
[Network services]
Looks for an Internet connection.
Connects to "irc.allxtremenet.net" on port 6667 (TCP).
Connects to IRC server.
IRC: Uses nickname [UrX]-44479.
IRC: Uses username lculpz.
IRC: Joins channel #wns-hidden with password superbots.
IRC: Sets the usermode for user [UrX]-44479 to +xi+B+u.
IRC: Joins channel #wns-hidden with password superbots.
Attempts to delete share named "" on local system.

NORMAN

Norman Analysis Desktop v2.0

- Home
- Manage Users
- Sample Queue
- Cases (+63)
- Requests
- Sigbase
- Tools
- FP Network
- Statistics
- Search
- Search_New
- Defs & Fixes
- Submit a case
- Sample Groups
- Scheduler
- Settings
- Mailbox (3 new mail)
- Bugreports (+20)
- Knowledge Base
- Nbash
- Logout

General info:
Logged in as: snf
Access level: Super Analyst

Current issues:

- Opera 9.5 users will need a new certificate. Send a mail to tbr@norman.no to get one.

News:

- NAD v2.0 released!
  If you encounter any errors,

Main

Norman Analysis Desktop

Use the menu to the left to navigate

Display all stats

NAD Agent:
server.exe:

MONKEY1
MONKEY2
MONKEY3
MONKEY4
MONKEY5
MONKEY6
MONKEY7
MONKEY8
MONKEY9
MONKEY10
MONKEY11
MONKEY12
MONKEY13
MONKEY14
MONKEY15
MONKEY16
MONKEY17
MONKEY18
MONKEY19
MONKEY20
MONKEY21
MONKEY22
MONKEY23
Virtual Monkey 1
Virtual Monkey 2
Virtual Monkey 3
Virtual Monkey 4
Virtual Monkey 5
Virtual Monkey 6
Virtual Monkey 7
Virtual Monkey 8
Virtual Monkey 9
Virtual Monkey 10
Virtual Monkey 11
Virtual Monkey 12