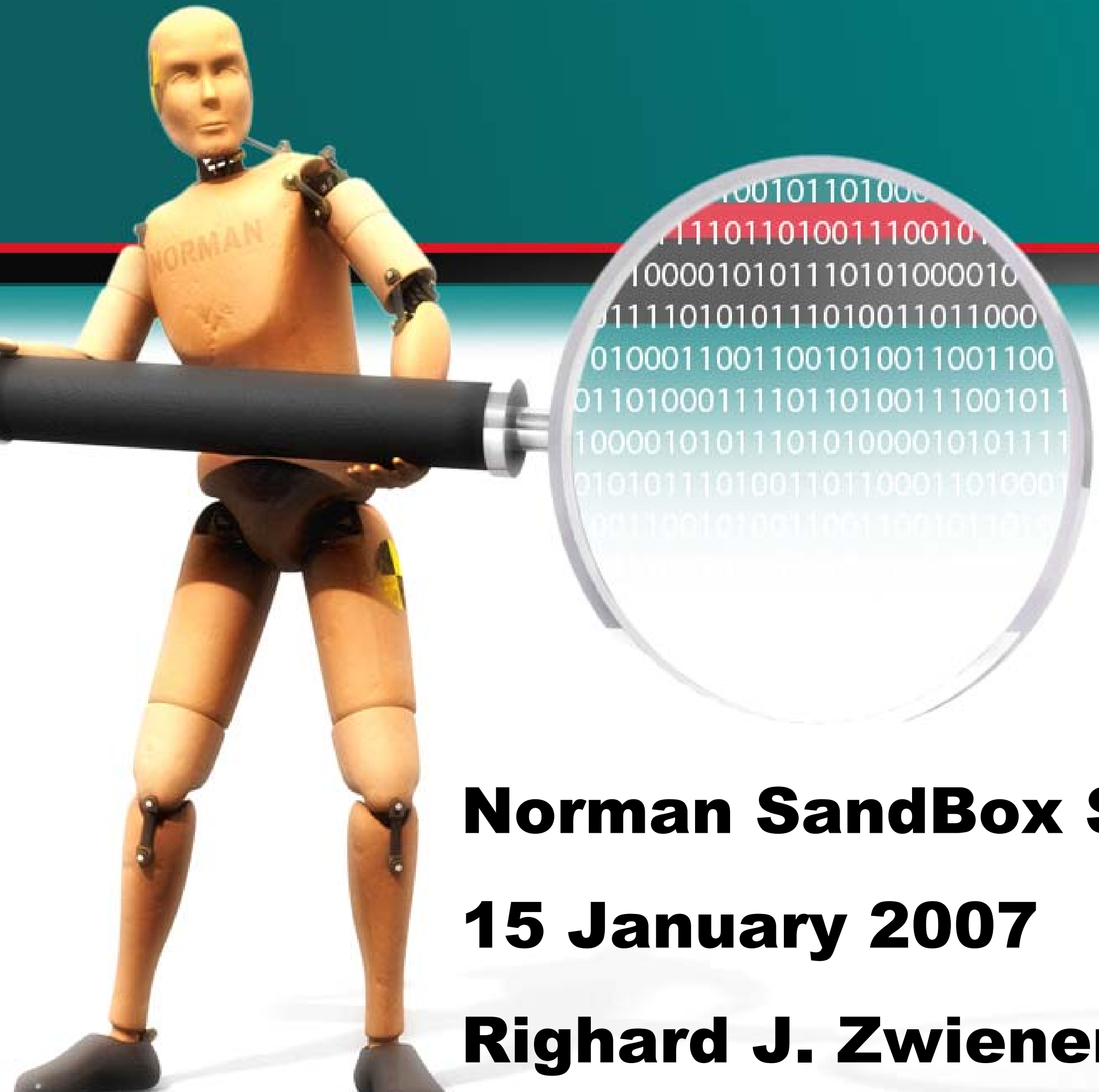
NORMA

Proactive IT securi

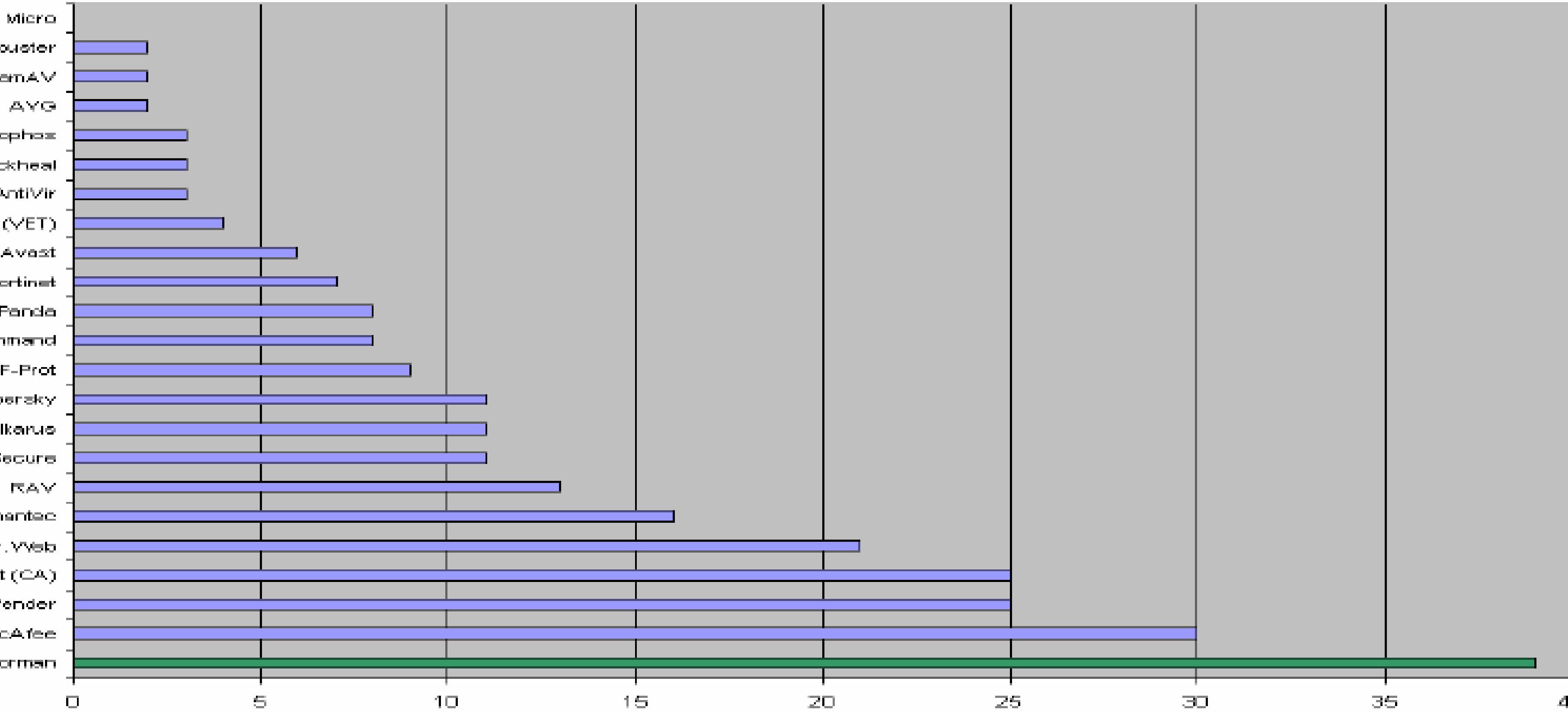


Cortina
14 avenue J-B Clemen
92100 Boulogne-Billa
Tel : +33 (0)1 41 10 26
Email : info@cortina.f

Norman SandBox Solutions

15 January 2007

Righard J. Zwienenberg



Source ; AV-Test, Andreas Marx, 2

Agenda

- Introduction
- The Norman SandBox
- Demonstration
- Q&A

Introduction: Righard J. Zwienenberg

- 1976: First experience computers (9 years old)
- 1977: Actively working working with computers
- 1982: Teaching my first classes (15 years old)
- 1988: Technical University Delft, Technical Informatics (first virus, Jerusalem.1808.B-A204)
- 1988-1991: Freelance consultant, VirScan.Dat (TBScan/HTScan)
- 1991: Member of CARO
- 1990-1996: The Hague High School, Sector Informatics
- 1991-1995: Founded Computer Security Engineers, Ltd.
- 1995-1998: Research & Development at ThunderBYTE
- 1998-now: Norman
- 2000: Co-founded AVED, Board Member on AVED
- 2003: Technical Overview Board Member of the WildList Organization
- 2005: Technical Board Member of CME (Common Malware Enumeration)
- 2005: Vice-President AVAR, European Operations
- 2005: Chief Research Officer at Norman

Introduction: Righard Zwienenberg in Norman

- Virus Research
- Scanner Engine Development
- Security Research
- Liaison for Norman to Virus Bulletin, EICAR, ICSA Labs, AVAR, Certification Organizations (eg Checkmark), Microsoft, Testers, Reviewers, etc.
- Presentations, Seminars, Workshops, Conferences
- Talking to journalists
- Flying over the world for Norman

Introduction: Righard Zwienenberg privately

- Married for 9.5 years
- 1 boy (almost 18 months) Matthew
- Drummer
- Magician
- Modelling
- Stand-up Comedy

Commodore Pet-2001

- 4KB Memory
- Video memory: 1KB
- Starts up with Basic

The next code made the Pet 2001 went up in fire!!!

```
10 motor 1
20 motor 0
30 goto 10
```

Sandbox: a quick introduction

- Why was it created?
- Why do we make the technology publicly available?
- How do we make it available?

Norman SandBox Solutions Overview

- **Norman SandBox Reporter**
  - Malware information sent by email
  - Subscription based

- **Norman SandBox Analyzer**
  - Application to perform fast and efficient analysis of suspicious files

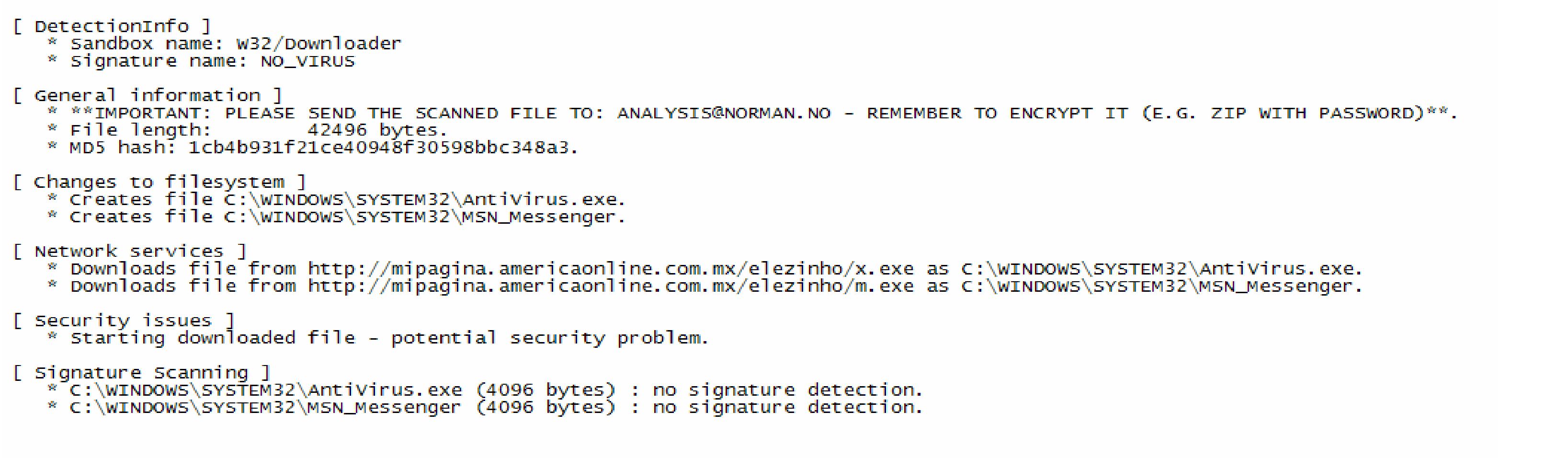
- **Norman SandBox Analyzer Pro**
  - Application to perform in-depth analysis of malware

Norman SandBox Reporter

- Information gathered by Norman SandBox Information Center (http://sandbox.norman.com) in the past 24 hours
- SandBox summary
- List of URL’s with possible malicious content
- List of IRC servers including login details found in the analyzed files
- Provided as .txt and .xml file

SandBox Reporter Sample of SandBox Summar

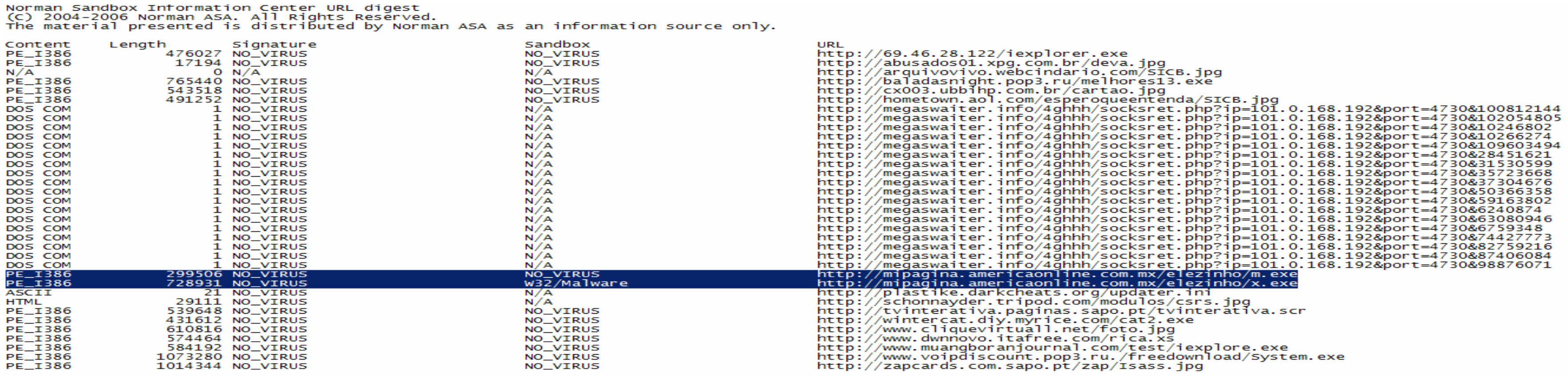
- **Detection Info**
  - Display SandBox classification like, W32/Downloader
  - If the scanned file are known to Norman, the name of the malicious file will be displayed here like Bagle, Sober etc.
- **General Information**
  - Gives you file length and MD5 hash information
- **Changes to Filesystem, Registry etc.**
  - Here you will find information about files created and deleted as well as new registry keys and deleted registry keys.
- **Network services**
  - Will show information about network services the file are using like, downloading/uploading files from/to a specific location. IRC networks it will connect to with login details, SMTP server details etc.
- **Security issues**
  - We will describe why this would be a possible security issue
- **Signature Scanning**
  - In this case we will scan the created files and if they are know the name will be shown here.
- **More information are available depending of kind of malicious file.**



```
[ DetectionInfo ]
   * Sandbox name: W32/Downloader
   * Signature name: NO_VIRUS

[ General information ]
   * **IMPORTANT: PLEASE SEND THE SCANNED FILE TO: ANALYSIS@NORMAN.NO - REMEMBER TO ENCRYPT IT (E.G. ZIP WITH PASSWORD)**.
   * File length:        42496 bytes.
   * MD5 hash: 1cb4b931f21ce40948f30598bbc348a3.

[ Changes to filesystem ]
   * Creates file C:\WINDOWS\SYSTEM32\AntiVirus.exe.
   * Creates file C:\WINDOWS\SYSTEM32\MSN_Messenger.

[ Network services ]
   * Downloads file from http://mipagina.americaonline.com.mx/elezinho/x.exe as C:\WINDOWS\SYSTEM32\AntiVirus.exe.
   * Downloads file from http://mipagina.americaonline.com.mx/elezinho/m.exe as C:\WINDOWS\SYSTEM32\MSN_Messenger.

[ Security issues ]
   * Starting downloaded file - potential security problem.

[ Signature Scanning ]
   * C:\WINDOWS\SYSTEM32\AntiVirus.exe (4096 bytes) : no signature detection.
   * C:\WINDOWS\SYSTEM32\MSN_Messenger (4096 bytes) : no signature detection.
```

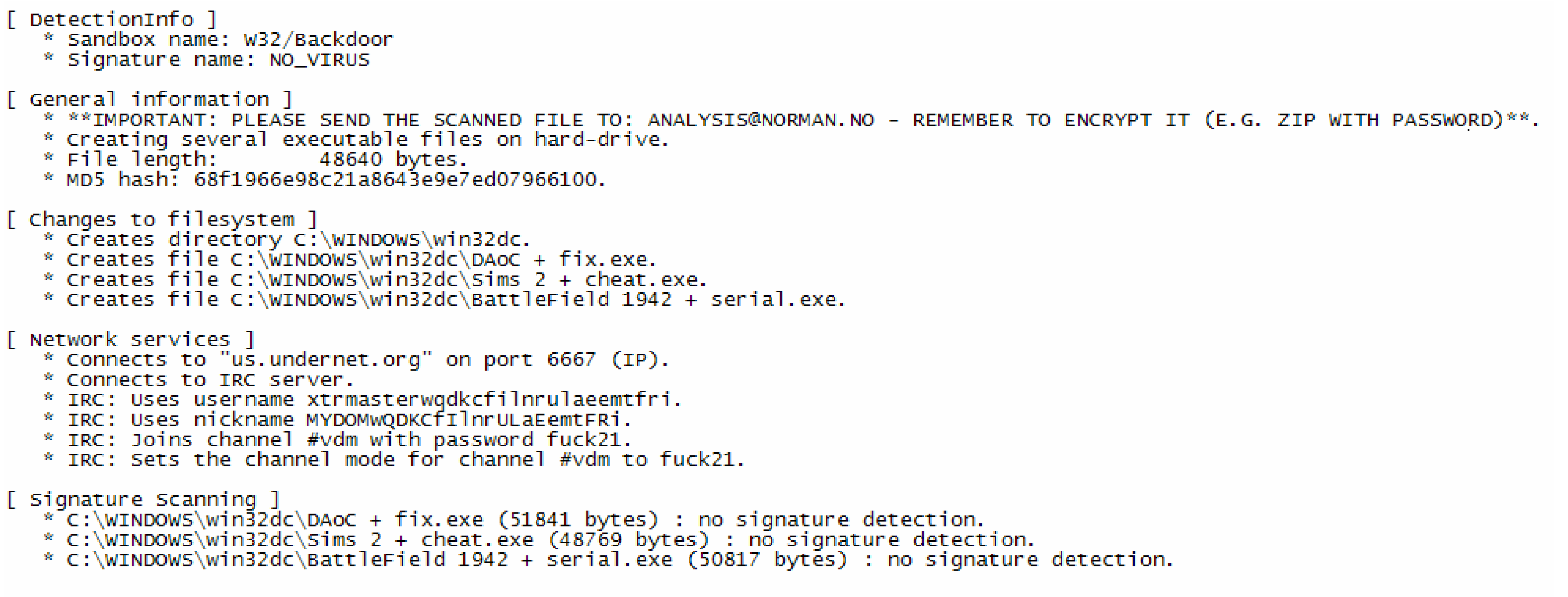
SandBox Reporter - URL List

- Contains exact paths to where files are connecting to download files, as these URL's are fou malware they most likely to be malicious even if we report "no virus" as long as the file conte PE_I386 and there is a value in the length column.
- Signature means name of malware as reported Norman Virus Control
- SandBox means SandBox classification of malware in the URL
- The example below have 2 lines in blue and are found in the SandBox summary on the previ slide (show the link between the 2 reports).



```
Norman Sandbox Information Center URL digest
(C) 2004-2006 Norman ASA. All Rights Reserved.
The material presented is distributed by Norman ASA as an information source only.

Content    Length       Signature                      Sandbox                        URL
PE_I386          476027 NO_VIRUS                       NO_VIRUS                       http://69.46.28.122/iexplorer.exe
PE_I386           17194 NO_VIRUS                       NO_VIRUS                       http://abusados01.xpg.com.br/deva.jpg
N/A                   0 N/A                            N/A                            http://arquivovivo.webcindario.com/SICB.jpg
PE_I386          765440 NO_VIRUS                       NO_VIRUS                       http://baladasnight.pop3.ru/melhores13.exe
PE_I386          543518 NO_VIRUS                       NO_VIRUS                       http://cx003.ubbihp.com.br/cartao.jpg
PE_I386          491252 NO_VIRUS                       NO_VIRUS                       http://hometown.aol.com/esperoqueeentenda/SICB.jpg
DOS COM               1 NO_VIRUS                       N/A                            http://megaswaiter.info/4ghhh/socksret.php?ip=101.0.168.192&port=4730&100812144
DOS COM               1 NO_VIRUS                       N/A                            http://megaswaiter.info/4ghhh/socksret.php?ip=101.0.168.192&port=4730&102054805
DOS COM               1 NO_VIRUS                       N/A                            http://megaswaiter.info/4ghhh/socksret.php?ip=101.0.168.192&port=4730&10246802
DOS COM               1 NO_VIRUS                       N/A                            http://megaswaiter.info/4ghhh/socksret.php?ip=101.0.168.192&port=4730&10266274
DOS COM               1 NO_VIRUS                       N/A                            http://megaswaiter.info/4ghhh/socksret.php?ip=101.0.168.192&port=4730&109603494
DOS COM               1 NO_VIRUS                       N/A                            http://megaswaiter.info/4ghhh/socksret.php?ip=101.0.168.192&port=4730&28451621
DOS COM               1 NO_VIRUS                       N/A                            http://megaswaiter.info/4ghhh/socksret.php?ip=101.0.168.192&port=4730&31530599
DOS COM               1 NO_VIRUS                       N/A                            http://megaswaiter.info/4ghhh/socksret.php?ip=101.0.168.192&port=4730&35723668
DOS COM               1 NO_VIRUS                       N/A                            http://megaswaiter.info/4ghhh/socksret.php?ip=101.0.168.192&port=4730&37304676
DOS COM               1 NO_VIRUS                       N/A                            http://megaswaiter.info/4ghhh/socksret.php?ip=101.0.168.192&port=4730&50366358
DOS COM               1 NO_VIRUS                       N/A                            http://megaswaiter.info/4ghhh/socksret.php?ip=101.0.168.192&port=4730&59163802
DOS COM               1 NO_VIRUS                       N/A                            http://megaswaiter.info/4ghhh/socksret.php?ip=101.0.168.192&port=4730&6240874
DOS COM               1 NO_VIRUS                       N/A                            http://megaswaiter.info/4ghhh/socksret.php?ip=101.0.168.192&port=4730&63080946
DOS COM               1 NO_VIRUS                       N/A                            http://megaswaiter.info/4ghhh/socksret.php?ip=101.0.168.192&port=4730&6759348
DOS COM               1 NO_VIRUS                       N/A                            http://megaswaiter.info/4ghhh/socksret.php?ip=101.0.168.192&port=4730&74427773
DOS COM               1 NO_VIRUS                       N/A                            http://megaswaiter.info/4ghhh/socksret.php?ip=101.0.168.192&port=4730&82759216
DOS COM               1 NO_VIRUS                       N/A                            http://megaswaiter.info/4ghhh/socksret.php?ip=101.0.168.192&port=4730&87406084
DOS COM               1 NO_VIRUS                       N/A                            http://megaswaiter.info/4ghhh/socksret.php?ip=101.0.168.192&port=4730&98876071
PE_I386          299506 NO_VIRUS                       NO_VIRUS                       http://mipagina.americaonline.com.mx/elezinho/m.exe
PE_I386          728931 NO_VIRUS                       W32/Malware                    http://mipagina.americaonline.com.mx/elezinho/x.exe
ASCII                21 NO_VIRUS                       N/A                            http://plastike.darkcheats.org/updater.ini
HTML              29111 NO_VIRUS                       N/A                            http://schonnayder.tripod.com/modulos/csrs.jpg
PE_I386          539648 NO_VIRUS                       NO_VIRUS                       http://tvinterativa.paginas.sapo.pt/tvinterativa.scr
PE_I386          431612 NO_VIRUS                       NO_VIRUS                       http://wintercat.diy.myrice.com/cat2.exe
PE_I386          610816 NO_VIRUS                       NO_VIRUS                       http://www.cliquevirtuall.net/foto.jpg
PE_I386          574464 NO_VIRUS                       NO_VIRUS                       http://www.dwnnovo.itafree.com/rica.xs
PE_I386          584192 NO_VIRUS                       NO_VIRUS                       http://www.muangboranjournal.com/test/iexplore.exe
PE_I386         1073280 NO_VIRUS                       NO_VIRUS                       http://www.voipdiscount.pop3.ru./freedownload/System.exe
PE_I386         1014344 NO_VIRUS                       NO_VIRUS                       http://zapcards.com.sapo.pt/zap/Isass.jpg
```

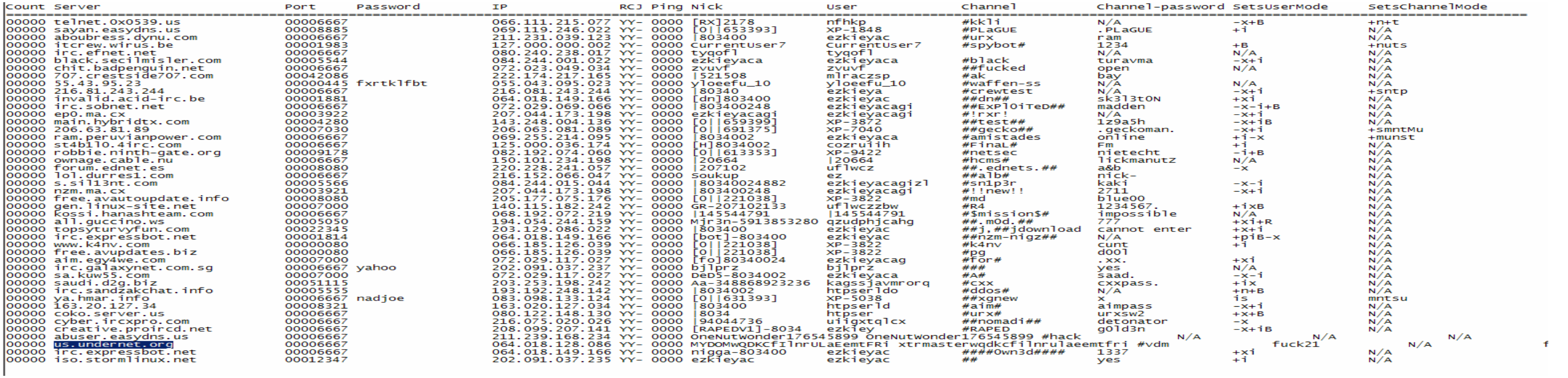
SandBox Reporter - Summary



```
[ DetectionInfo ]
   * Sandbox name: W32/Backdoor
   * Signature name: NO_VIRUS

[ General information ]
   * **IMPORTANT: PLEASE SEND THE SCANNED FILE TO: ANALYSIS@NORMAN.NO - REMEMBER TO ENCRYPT IT (E.G. ZIP WITH PASSWORD)**.
   * Creating several executable files on hard-drive.
   * File length:        48640 bytes.
   * MD5 hash: 68f1966e98c21a8643e9e7ed07966100.

[ Changes to filesystem ]
   * Creates directory C:\WINDOWS\win32dc.
   * Creates file C:\WINDOWS\win32dc\DAoC + fix.exe.
   * Creates file C:\WINDOWS\win32dc\Sims 2 + cheat.exe.
   * Creates file C:\WINDOWS\win32dc\BattleField 1942 + serial.exe.

[ Network services ]
   * Connects to "us.undernet.org" on port 6667 (IP).
   * Connects to IRC server.
   * IRC: Uses username xtrmasterwgdkcfilnrulaeemtfri.
   * IRC: Uses nickname MYDOMwQDKCfIlnrULaEemtFRi.
   * IRC: Joins channel #vdm with password fuck21.
   * IRC: Sets the channel mode for channel #vdm to fuck21.

[ Signature Scanning ]
   * C:\WINDOWS\win32dc\DAoC + fix.exe (51841 bytes) : no signature detection.
   * C:\WINDOWS\win32dc\Sims 2 + cheat.exe (48769 bytes) : no signature detection.
   * C:\WINDOWS\win32dc\BattleField 1942 + serial.exe (50817 bytes) : no signature detection.
```

SandBox Reporter - IRC List

- **Contains information about IRC servers found in the analyzed malware**
- **Information provided includes**
  - Server name, port connects on, password used, IP address, active or not
  - Nickname, username, channel password, user mode
  - Etc.
- **These IRC networks are likely to be Botnets as they are found in malware**



```
Count Server                          Port     Password        IP              RCJ Ping Nick              User           Channel          Channel-password SetsUserMode     SetsChannelMode
=========================================================================================================================================================================================
00000 telnet.0x0539.us                00006667                 066.111.215.077 YY- 0000 [RX]2178          nfhkp          #kkli            N/A              -x+B             +n+t
00000 sayan.easydns.us                00008885                 069.119.246.022 YY- 0000 [0||653393]       XP-1848        #PLaGUE          .PLaGUE          +i               N/A
00000 aboubress.dynu.com              00006667                 211.231.039.123 YY- 0000 |803400           ezkieyac       #urx             ram                               N/A
00000 itcrew.wirus.be                 00001983                 127.000.000.002 YY- 0000 CurrentUser7      CurrentUser7   #spybot#         1234             +B               +nuts
00000 irc.efnet.net                   00006667                 080.240.238.017 YY- 0000 tyqofl            tyqofl                          N/A              N/A              N/A
00000 black.secilmisler.com           00005544                 084.244.001.022 YY- 0000 ezkieyaca         ezkieyaca      #black           turavma          -x+i             N/A
00000 chit.badpenguin.net             00006667                 072.023.049.034 YY- 0000 zvuvf             zvuvf          ##fucked         open             N/A              N/A
00000 707.crestside707.com            00042086                 222.174.217.165 YY- 0000 |521508           mlraczsp       #ak              bay                               N/A
00000 55.43.95.23                     00000445 fxrtklfbt       055.043.095.023 YY- 0000 yloeefu_10        yloeefu_10     #waffen-ss       N/A              N/A              N/A
00000 216.81.243.244                  00006667                 216.081.243.244 YY- 0000 |80340            ezkieya        #crewtest        N/A              -x+i             +sntp
00000 invalid.acid-irc.be             00001881                 064.018.149.166 YY- 0000 [dn]803400        ezkieyac       ##dn##           sk3l3tON         +xi              N/A
00000 irc.sobnet.net                  00006667                 072.029.069.066 YY- 0000 |803400248        ezkieyacagi    ##ExPl0iTeD##    madden           -x-i+B           N/A
00000 ep0.ma.cx                       00003922                 207.044.173.198 YY- 0000 ezkieyacagi       ezkieyacagi    #!rxr!           N/A              -x+i             N/A
00000 main.hybridtx.com               00004280                 143.248.004.136 YY- 0000 [0||659399]       XP-3872        ##test##         1z9a5h           -x+iB            N/A
00000 206.63.81.89                    00007030                 206.063.081.089 YY- 0000 [0||691375]       XP-7040        ##gecko##        .geckoman.       -x+i             +smntMu
00000 ram.peruvianpower.com           00006667                 069.255.214.095 YY- 0000 |8034002          ezkieyaca      #amistades       online           +i-x             +munst
00000 st4b1l0.4irc.com                00006667                 125.000.036.174 YY- 0000 [H]8034002        cozruiih       #FinaL#          Fm               +i               N/A
00000 robbie.ninth-gate.org           00009178                 082.192.074.060 YY- 0000 [0||613353]       XP-9422        #netsec          nietecht         -i+B             N/A
00000 ownage.cable.nu                 00006667                 150.101.234.198 YY- 0000 |20664            |20664         #hcms#           lickmanutZ       N/A              N/A
00000 forum.ednet.es                  00008080                 220.228.241.057 YY- 0000 |207102           uflwcz         ##.ednets.##     a&b              -x               N/A
00000 lol.durres1.com                 00006667                 216.152.066.047 YY- 0000 Soukup            ez             ##alb#           nick-                             N/A
00000 s.sil13nt.com                   00005566                 084.244.015.044 YY- 0000 |80340024882      ezkieyacagizl  #sn1p3r          kaki             -x-i             N/A
00000 nzm.ma.cx                       00003921                 207.044.173.198 YY- 0000 |803400248        ezkieyacagi    #!!new!!         2711             -x+i             N/A
00000 free.avautoupdate.info          00008080                 205.177.075.176 YY- 0000 [0||221038]       XP-3822        #md              blue00                            N/A
00000 gen.linux-site.net              00007000                 140.115.182.242 YY- 0000 GR-207102133      uflwczzbw      #R4              1234567.         +ixB             N/A
00000 kossi.hanashteam.com            00006667                 068.192.072.219 YY- 0000 |145544791        |145544791     #$mission$#      impossible       N/A              N/A
00000 all.guccino.ws                  00005050                 194.054.244.159 YY- 0000 Mjr3n-5913853280  qzudphjcahg    ##.m0d.##        777              +xi+R            N/A
00000 topsyturvyfun.com               00022345                 203.129.086.022 YY- 0000 |803400           ezkieyac       ##j,##jdownload  cannot enter     +x+i             N/A
00000 irc.expressbot.net              00001814                 064.018.149.166 YY- 0000 [bot]-803400      ezkieyac       ##nzm-nigz##     N/A              +piB-x           N/A
00000 www.k4nv.com                    00000080                 066.185.126.039 YY- 0000 [0||221038]       XP-3822        #k4nv            cunt             +i               N/A
00000 free.avupdates.biz              00000080                 066.185.126.039 YY- 0000 [0||221038]       XP-3822        #pg              d00l                              N/A
00000 aim.egy4we.com                  00007000                 072.029.117.027 YY- 0000 [fo]80340024      ezkieyacag     #for#            .xx.             +xi              N/A
00000 irc.galaxynet.com.sg            00006667 yahoo           202.091.037.237 YY- 0000 bjlprz            bjlprz         ###              yes              N/A              N/A
00000 sa.kuw55.com                    00007000                 072.029.117.027 YY- 0000 DeD5-8034002      ezkieyaca      #A#              saad.            -x-i             N/A
00000 saudi.d2g.biz                   00051115                 203.253.198.242 YY- 0000 Aa-348868923236   kagssjavmrorq  #cxx             cxxpass.         +ix              N/A
00000 irc.sandzakchat.info            00005555                 193.192.248.142 YY- 0000 |8034002          htpserldo      #ddos#           N/A              +n+B             N/A
00000 ya.hmar.info                    00006667 nadjoe          083.098.133.124 YY- 0000 [0||631393]       XP-5038        ##xgnew          x                is               mntsu
00000 163.20.127.34                   00008321                 163.020.127.034 YY- 0000 |803400           htpserld       #aim#            aimpass          -x+i             N/A
00000 coko.server.us                  00006667                 080.122.148.130 YY- 0000 |8034             htpser         #urx#            urxsw2           +x+B             N/A
00000 cyber.ircxpro.com               00006667                 216.075.020.026 YY- 0000 |94044736         uiigxtqlcx     ##nomadi##       detonator        -x               N/A
00000 creative.proircd.net            00006667                 208.099.207.141 YY- 0000 [RAPEDV1]-8034    ezkiey         #RAPED           g0ld3n           -x+iB            N/A
00000 abuser.easydns.us               00006667                 211.239.168.234 YY- 0000 OneNutWonder176545899 OneNutWonder176545899 #hack               N/A              N/A              N/A
00000 us.undernet.org                 00006667                 064.018.128.086 YY- 0000 MYDOMwQDKCfIlnrULaEemtFRi xtrmasterwqdkcfilnrulaeemtfri #vdm                 fuck21          N/A              f
00000 irc.expressbot.net              00006667                 064.018.149.166 YY- 0000 nigga-803400      ezkieyac       ####0wn3d####    1337             +xi              N/A
00000 iso.stormlinux.net              00012347                 202.091.037.235 YY- 0000 ezkieyac          ezkieyac       ##               yes              +i               N/A
```

SandBox Reporter: where to use...

- In (Personal) Firewalls…
- In Filters…
- Etc…

Norman SandBox Analyzer

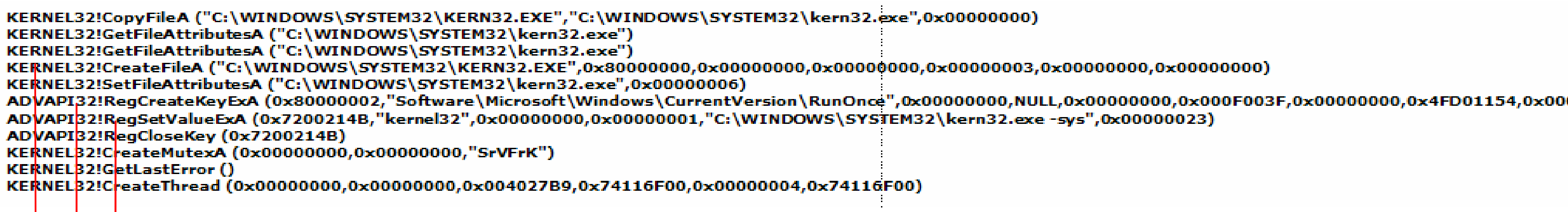
- An applications for analyzing files, deeper, faster and more efficient than previously seen
- Analyze files one by one or in batch jobs to increase efficiency
- Ability to set number of emulation cycles to increase detection rate
- Get SandBox summary of files analyzed for fast evaluation of file action like type of malware, changes to filesystem, registry, network services used, signature name if existing and more
- Get the complete API log of the analyzed file actions
- Analyze further dropper files from analyzed files.

Norman SandBox Analyzer

- **Designed for organizations dealing with suspicious files**
  - Security organizations
  - Malware researchers
  - Network security application and appliance vendors etc.
  - ISP’s
  - Large corporate
  - Helpdesks

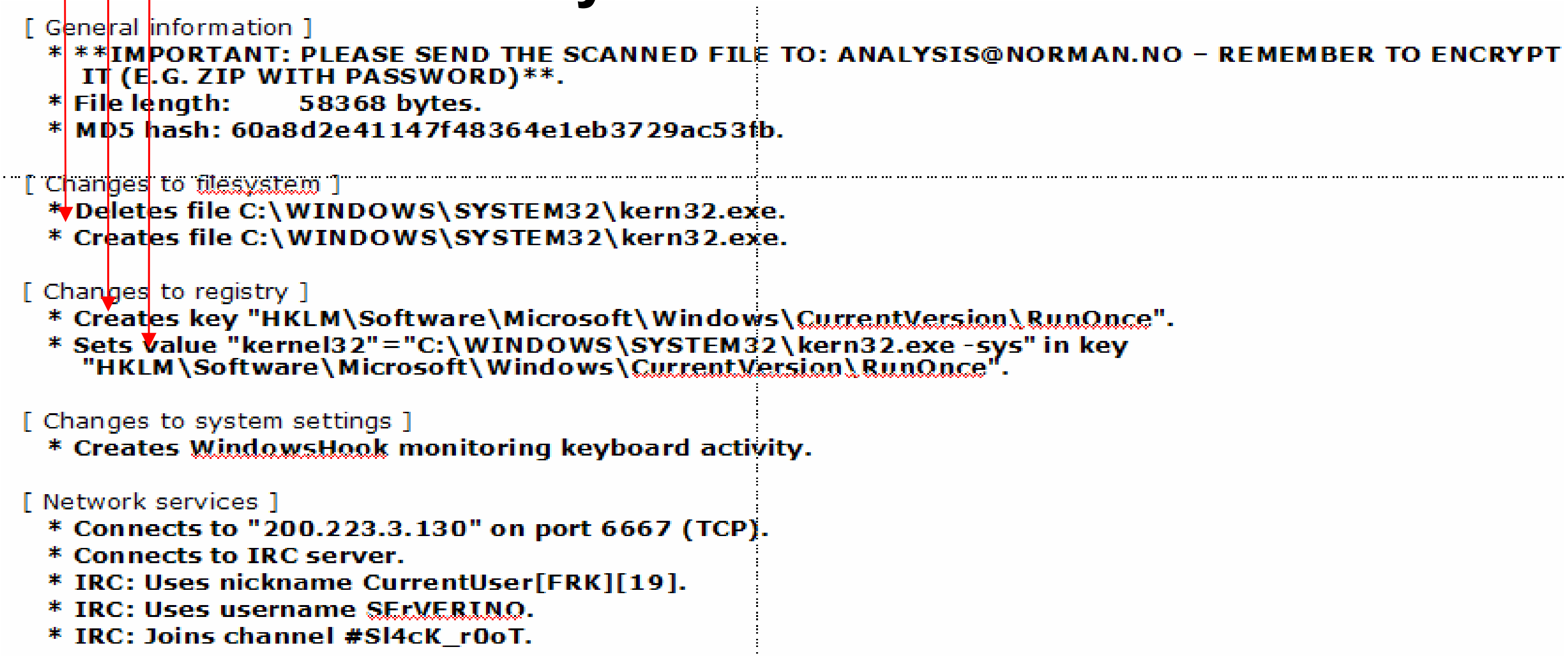
SandBox Relations Between API Log & Summa

- ## API Log



```
KERNEL32!CopyFileA ("C:\WINDOWS\SYSTEM32\KERN32.EXE","C:\WINDOWS\SYSTEM32\kern32.exe",0x00000000)
KERNEL32!GetFileAttributesA ("C:\WINDOWS\SYSTEM32\kern32.exe")
KERNEL32!GetFileAttributesA ("C:\WINDOWS\SYSTEM32\kern32.exe")
KERNEL32!CreateFileA ("C:\WINDOWS\SYSTEM32\KERN32.EXE",0x80000000,0x00000000,0x00000000,0x00000003,0x00000000,0x00000000)
KERNEL32!SetFileAttributesA ("C:\WINDOWS\SYSTEM32\kern32.exe",0x00000006)
ADVAPI32!RegCreateKeyExA (0x80000002,"Software\Microsoft\Windows\CurrentVersion\RunOnce",0x00000000,NULL,0x00000000,0x000F003F,0x00000000,0x4FD01154,0x000
ADVAPI32!RegSetValueExA (0x7200214B,"kernel32",0x00000000,0x00000001,"C:\WINDOWS\SYSTEM32\kern32.exe -sys",0x00000023)
ADVAPI32!RegCloseKey (0x7200214B)
KERNEL32!CreateMutexA (0x00000000,0x00000000,"SrVFrK")
KERNEL32!GetLastError ()
KERNEL32!CreateThread (0x00000000,0x00000000,0x004027B9,0x74116F00,0x00000004,0x74116F00)
```

- ## SandBox Summary

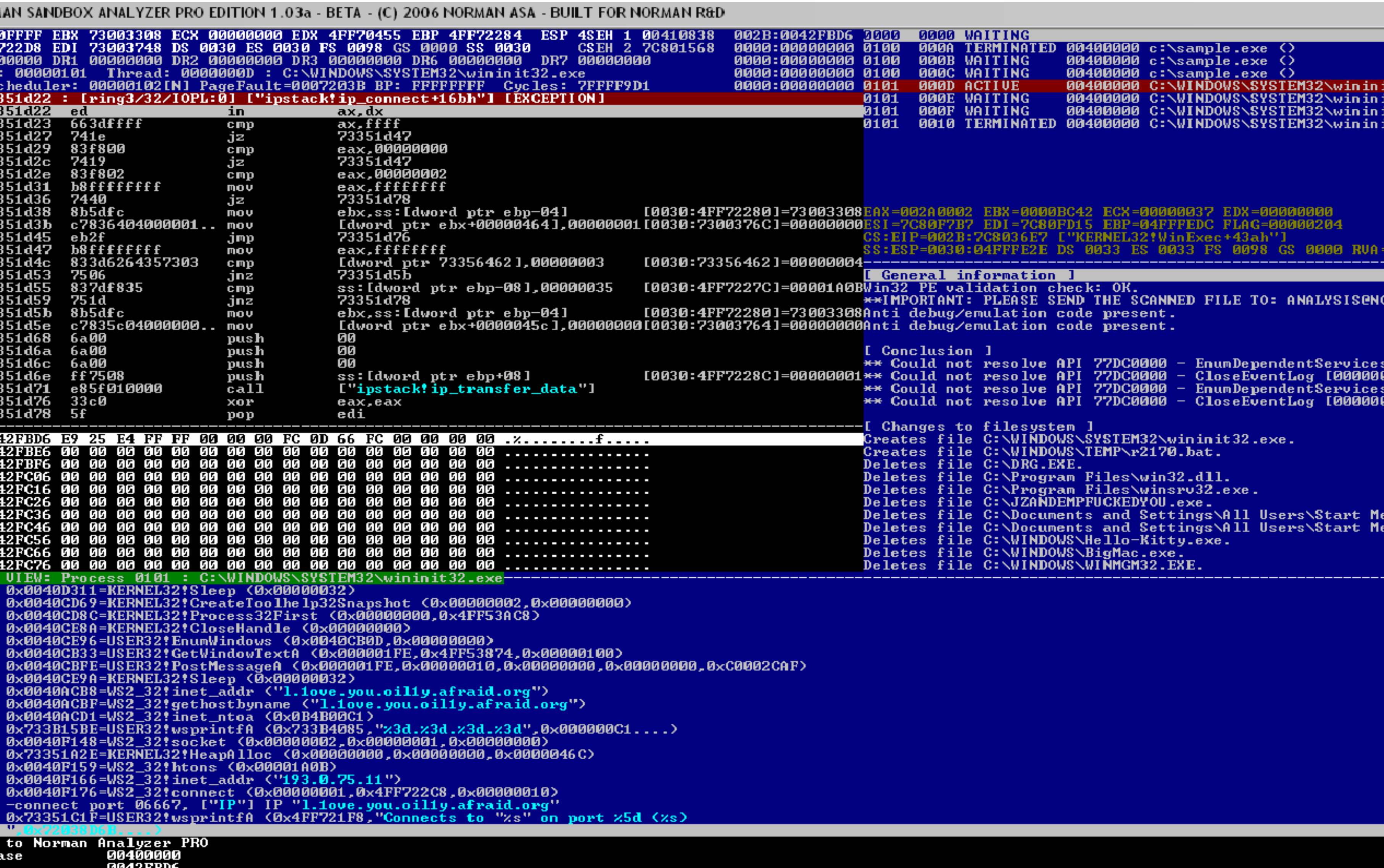


```
[ General information ]
  * **IMPORTANT: PLEASE SEND THE SCANNED FILE TO: ANALYSIS@NORMAN.NO - REMEMBER TO ENCRYPT
    IT (E.G. ZIP WITH PASSWORD)**.
  * File length:       58368 bytes.
  * MD5 hash: 60a8d2e41147f48364e1eb3729ac53fb.

[ Changes to filesystem ]
  * Deletes file C:\WINDOWS\SYSTEM32\kern32.exe.
  * Creates file C:\WINDOWS\SYSTEM32\kern32.exe.

[ Changes to registry ]
  * Creates key "HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce".
  * Sets value "kernel32"="C:\WINDOWS\SYSTEM32\kern32.exe -sys" in key
    "HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce".

[ Changes to system settings ]
  * Creates WindowsHook monitoring keyboard activity.

[ Network services ]
  * Connects to "200.223.3.130" on port 6667 (TCP).
  * Connects to IRC server.
  * IRC: Uses nickname CurrentUser[FRK][19].
  * IRC: Uses username SErVERINO.
  * IRC: Joins channel #Sl4cK_r0oT.
```

SandBox Analyzer Pro

- **Norman SandBox Analyzer Pro**
  - Target market, security organizations, security companies needing to do deep analysis of file behavior
  - Since deep analysis is not time critical you can set it to run a higher number of emulation cycles
  - By the use of a large set of parameters you are able to monitor various sections of the code as it runs and after it have been running
    - See the changes to the OS as the file is running
    - Set breakpoint's and insert additional code to see the reaction
    - Watch library being loaded
    - See Threads running
    - See Sockets created
  - All in all you will get the full picture of the actions done by the file that is being analyzed

SandBox Analyzer Pro



```
AN SANDBOX ANALYZER PRO EDITION 1.03a - BETA - (C) 2006 NORMAN ASA - BUILT FOR NORMAN R&D
```

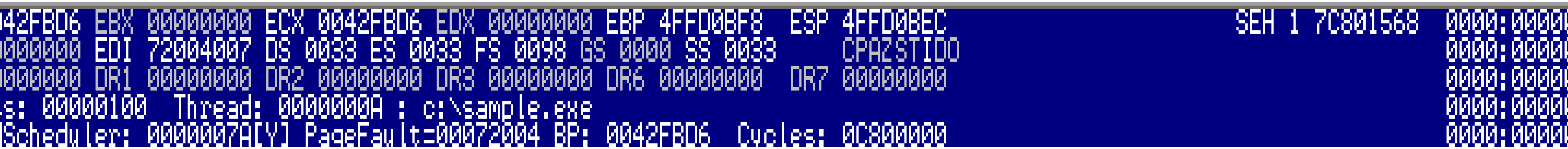
```
0FFFF EBX 73003308 ECX 00000000 EDX 4FF70455 EBP 4FF72284  ESP 4SEH 1 00410838  002B:0042FBD6
722D8 EDI 73003748 DS 0030 ES 0030 FS 0098 GS 0000 SS 0030     CSEH 2 7C801568  0000:00000000
00000 DR1 00000000 DR2 00000000 DR3 00000000 DR6 00000000  DR7 00000000         0000:00000000
: 00000101  Thread: 0000000D : C:\WINDOWS\SYSTEM32\wininit32.exe                0000:00000000
cheduler: 00000102[N] PageFault=0007203B BP: FFFFFFFF  Cycles: 7FFFF9D1        0000:00000000
351d22 : [ring3/32/IOPL:0] ["ipstack!ip_connect+16bh"] [EXCEPTION]
351d22  ed                 in         ax,dx
351d23  663dffff           cmp        ax,ffff
351d27  741e               jz         73351d47
351d29  83f800             cmp        eax,00000000
351d2c  7419               jz         73351d47
351d2e  83f802             cmp        eax,00000002
351d31  b8ffffffff         mov        eax,ffffffff
351d36  7440               jz         73351d78
351d38  8b5dfc             mov        ebx,ss:[dword ptr ebp-04]        [0030:4FF72280]=73003308
351d3b  c7836404000001..   mov        [dword ptr ebx+00000464],00000001[0030:7300376C]=00000000
351d45  eb2f               jmp        73351d76
351d47  b8ffffffff         mov        eax,ffffffff
351d4c  833d6264357303     cmp        [dword ptr 73356462],00000003    [0030:73356462]=00000004
351d53  7506               jnz        73351d5b
351d55  837df835           cmp        ss:[dword ptr ebp-08],00000035   [0030:4FF7227C]=00001A0B
351d59  751d               jnz        73351d78
351d5b  8b5dfc             mov        ebx,ss:[dword ptr ebp-04]        [0030:4FF72280]=73003308
351d5e  c7835c04000000..   mov        [dword ptr ebx+0000045c],00000000[0030:73003764]=00000000
351d68  6a00               push       00
351d6a  6a00               push       00
351d6c  6a00               push       00
351d6e  ff7508             push       ss:[dword ptr ebp+08]            [0030:4FF7228C]=00000001
351d71  e85f010000         call       ["ipstack!ip_transfer_data"]
351d76  33c0               xor        eax,eax
351d78  5f                 pop        edi
------------------------------------------------------------------------------------------
42FBD6 E9 25 E4 FF FF 00 00 00 FC 0D 66 FC 00 00 00 00 .%........f.....
42FBE6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
42FBF6 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
42FC06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
42FC16 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
42FC26 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
42FC36 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
42FC46 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
42FC56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
42FC66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
42FC76 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
```

```
0000   0000 WAITING
0100   000A TERMINATED 00400000 c:\sample.exe ()
0100   000B WAITING    00400000 c:\sample.exe ()
0100   000C WAITING    00400000 c:\sample.exe ()
0101   000D ACTIVE     00400000 C:\WINDOWS\SYSTEM32\winin
0101   000E WAITING    00400000 C:\WINDOWS\SYSTEM32\winin
0101   000F WAITING    00400000 C:\WINDOWS\SYSTEM32\winin
0101   0010 TERMINATED 00400000 C:\WINDOWS\SYSTEM32\winin

EAX=002A0002 EBX=0000BC42 ECX=00000037 EDX=00000000
ESI=7C80F7B7 EDI=7C80FD15 EBP=04FFFEDC FLAG=00000204
CS:EIP=002B:7C8036E7 ["KERNEL32!WinExec+43ah"]
SS:ESP=0030:04FFFE2E DS 0033 ES 0033 FS 0098 GS 0000 RVA=
------------------------------------------------------------
[ General information ]
Win32 PE validation check: OK.
**IMPORTANT: PLEASE SEND THE SCANNED FILE TO: ANALYSIS@NO
Anti debug/emulation code present.
Anti debug/emulation code present.

[ Conclusion ]
** Could not resolve API 77DC0000 - EnumDependentServices
** Could not resolve API 77DC0000 - CloseEventLog [000000
** Could not resolve API 77DC0000 - EnumDependentServices
** Could not resolve API 77DC0000 - CloseEventLog [000000

[ Changes to filesystem ]
Creates file C:\WINDOWS\SYSTEM32\wininit32.exe.
Creates file C:\WINDOWS\TEMP\r2170.bat.
Deletes file C:\DRG.EXE.
Deletes file C:\Program Files\win32.dll.
Deletes file C:\Program Files\winsrv32.exe.
Deletes file C:\JZANDEMPFUCKEDYOU.exe.
Deletes file C:\Documents and Settings\All Users\Start Me
Deletes file C:\Documents and Settings\All Users\Start Me
Deletes file C:\WINDOWS\Hello-Kitty.exe.
Deletes file C:\WINDOWS\BigMac.exe.
Deletes file C:\WINDOWS\WINMGM32.EXE.
```

```
VIEW: Process 0101 : C:\WINDOWS\SYSTEM32\wininit32.exe----------------------------------------
0x0040D311=KERNEL32!Sleep (0x00000032)
0x0040CD69=KERNEL32!CreateToolhelp32Snapshot (0x00000002,0x00000000)
0x0040CD8C=KERNEL32!Process32First (0x00000000,0x4FF53AC8)
0x0040CE8A=KERNEL32!CloseHandle (0x00000000)
0x0040CE96=USER32!EnumWindows (0x0040CB0D,0x00000000)
0x0040CB33=USER32!GetWindowTextA (0x000001FE,0x4FF53874,0x00000100)
0x0040CBFE=USER32!PostMessageA (0x000001FE,0x00000010,0x00000000,0x00000000,0xC0002CAF)
0x0040CE9A=KERNEL32!Sleep (0x00000032)
0x0040ACB8=WS2_32!inet_addr ("l.1ove.you.oil1y.afraid.org")
0x0040ACBF=WS2_32!gethostbyname ("l.1ove.you.oil1y.afraid.org")
0x0040ACD1=WS2_32!inet_ntoa (0x0B4B00C1)
0x733B15BE=USER32!wsprintfA (0x733B4085,"%3d.%3d.%3d.%3d",0x000000C1....)
0x0040F148=WS2_32!socket (0x00000002,0x00000001,0x00000000)
0x73351A2E=KERNEL32!HeapAlloc (0x00000000,0x00000000,0x0000046C)
0x0040F159=WS2_32!htons (0x00001A0B)
0x0040F166=WS2_32!inet_addr ("193.0.75.11")
0x0040F176=WS2_32!connect (0x00000001,0x4FF722C8,0x00000010)
-connect port 06667, ["IP"] IP "l.1ove.you.oil1y.afraid.org"
0x73351C1F=USER32!wsprintfA (0x4FF721F8,"Connects to "%s" on port %5d (%s)
",0x72038D6B....)
 to Norman Analyzer PRO
ase             00400000
                0042FBD6
```

SandBox Analyzer Pro

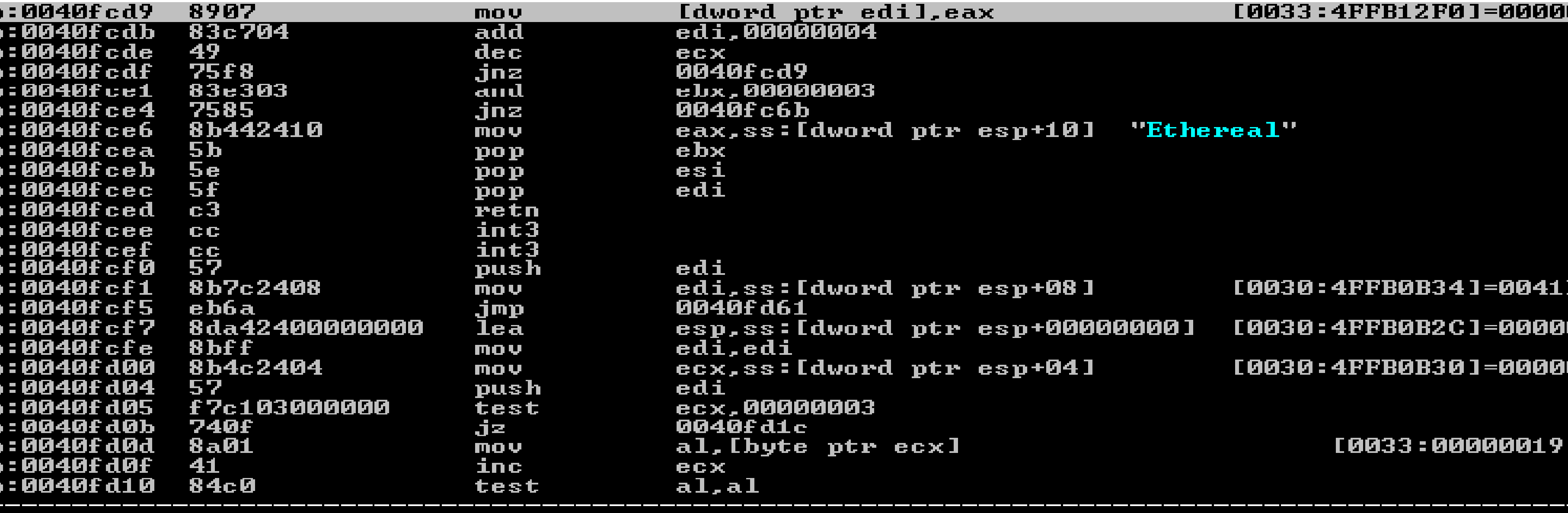
- **Register view**
  - Shows the emulator “CPU” status.
    - The normal registers, including some debug registers and “CPU” flags.
    - ThreadScheduler
    - PageFault
    - Breakpoints
    - Emulation cycles
    - Status Line



```
)42FBD6 EBX 00000000 ECX 0042FBD6 EDX 00000000 EBP 4FFD0BF8  ESP 4FFD0BEC           SEH 1 7C801568  0000:0000
)000000 EDI 72004007 DS 0033 ES 0033 FS 0098 GS 0000 SS 0033     CPAZSTIDO                            0000:0000
)000000 DR1 00000000 DR2 00000000 DR3 00000000 DR6 00000000  DR7 00000000                             0000:0000
:s: 00000100  Thread: 0000000A : c:\sample.exe                                                        0000:0000
)Scheduler: 0000007A[Y] PageFault=00072004 BP: 0042FBD6  Cycles: 0C800000                             0000:0000
```

SandBox Analyzer Pro

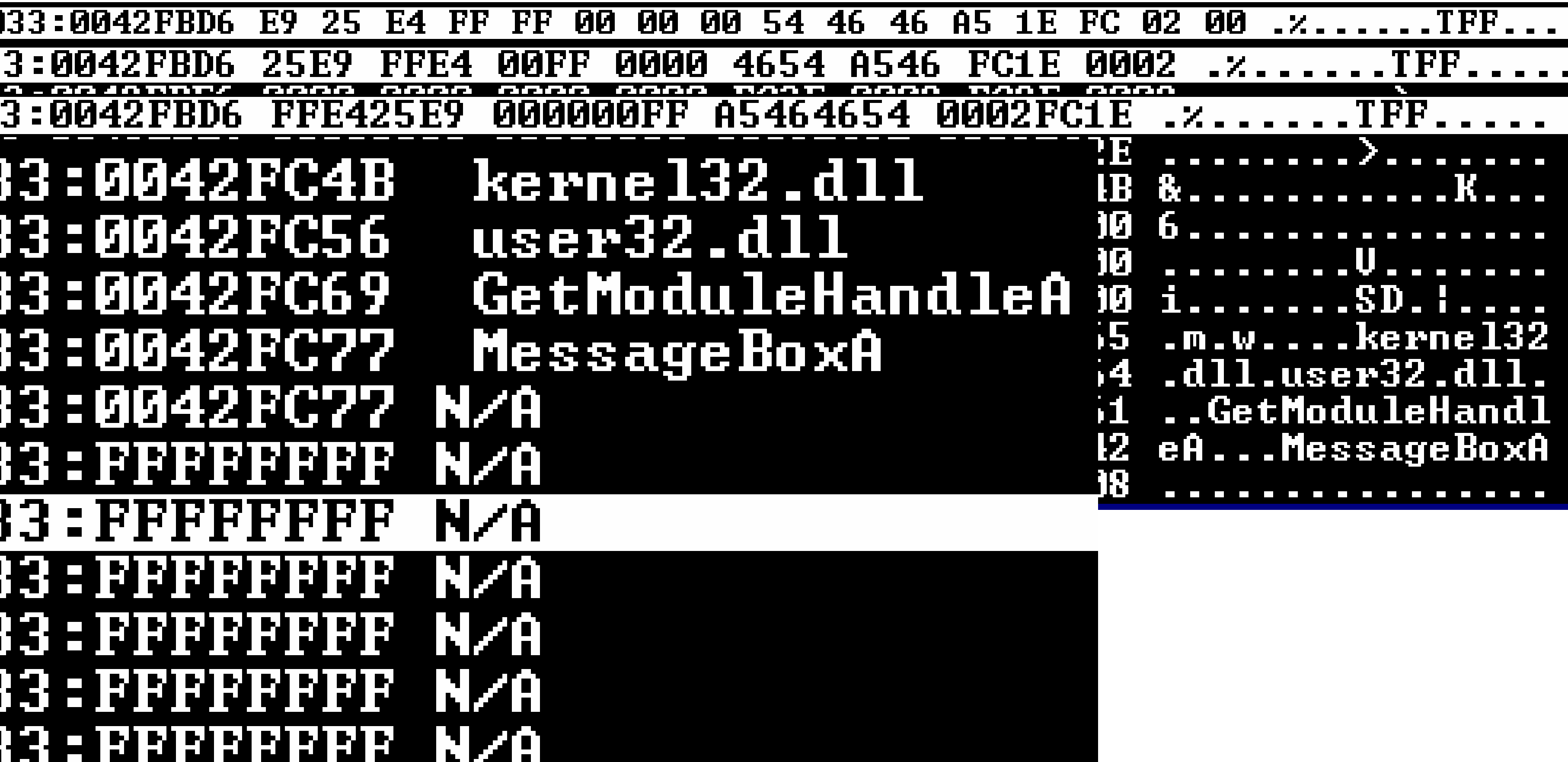
- **Disassembler view**
  - This view will disassemble the instruction at CS:EIP, or any given memory address.
  - Arrow keys can be used to move up and down.
  - The view will update, together with the “Register View” to show the state of the emulator.
  - The disassembler will try to resolve addresses against imported functions



```
:0040fcd9  8907            mov    [dword ptr edi],eax            [0033:4FFB12F0]=0000
:0040fcdb  83c704          add    edi,00000004
:0040fcde  49              dec    ecx
:0040fcdf  75f8            jnz    0040fcd9
:0040fce1  83e303          and    ebx,00000003
:0040fce4  7585            jnz    0040fc6b
:0040fce6  8b442410        mov    eax,ss:[dword ptr esp+10]  "Ethereal"
:0040fcea  5b              pop    ebx
:0040fceb  5e              pop    esi
:0040fcec  5f              pop    edi
:0040fced  c3              retn
:0040fcee  cc              int3
:0040fcef  cc              int3
:0040fcf0  57              push   edi
:0040fcf1  8b7c2408        mov    edi,ss:[dword ptr esp+08]      [0030:4FFB0B34]=0041
:0040fcf5  eb6a            jmp    0040fd61
:0040fcf7  8da42400000000  lea    esp,ss:[dword ptr esp+00000000] [0030:4FFB0B2C]=0000
:0040fcfe  8bff            mov    edi,edi
:0040fd00  8b4c2404        mov    ecx,ss:[dword ptr esp+04]      [0030:4FFB0B30]=0000
:0040fd04  57              push   edi
:0040fd05  f7c103000000    test   ecx,00000003
:0040fd0b  740f            jz     0040fd1c
:0040fd0d  8a01            mov    al,[byte ptr ecx]                  [0033:00000019
:0040fd0f  41              inc    ecx
:0040fd10  84c0            test   al,al
```

SandBox Analyzer Pro

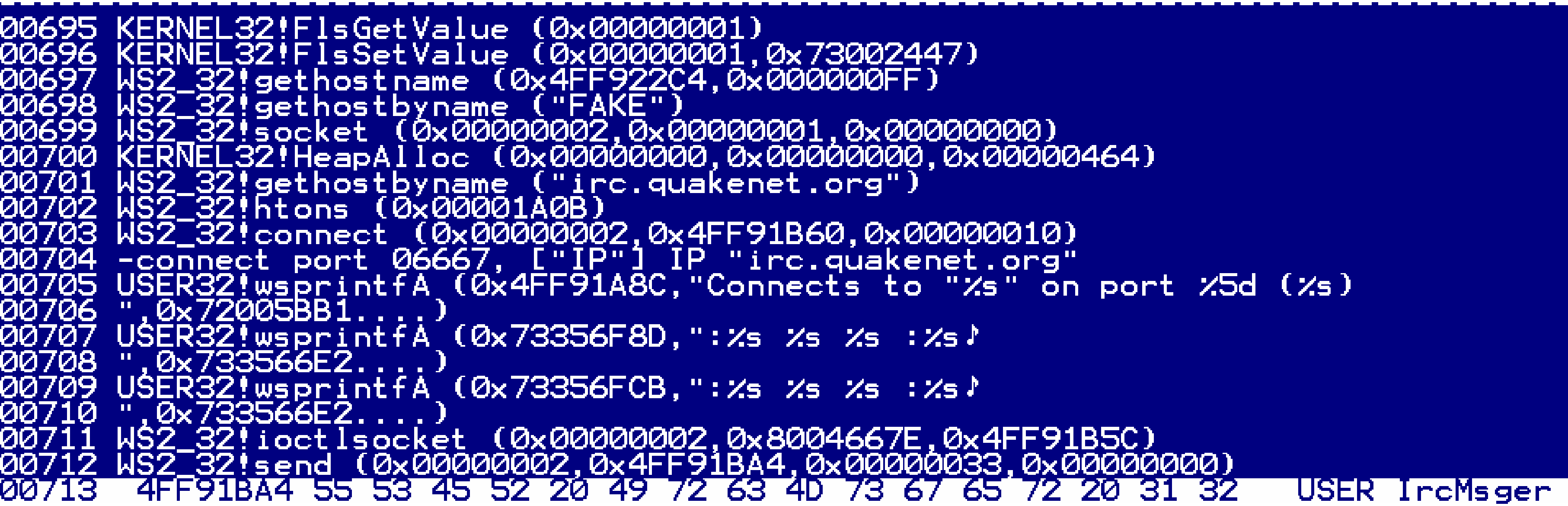
- **Memory dump view**
  - This view can dump any memory area.



```
33:0042FBD6  E9 25 E4 FF FF 00 00 00 54 46 46 A5 1E FC 02 00  .%......TFF...
3:0042FBD6  25E9  FFE4  00FF  0000  4654  A546  FC1E  0002  .%......TFF.....
3:0042FBD6  FFE425E9  000000FF  A5464654  0002FC1E  .%......TFF.....
                                                  E  ........>.......
33:0042FC4B   kernel32.dll                        4B &...........K...
33:0042FC56   user32.dll                          00 6...............
33:0042FC69   GetModuleHandleA                    00 .........V.......
33:0042FC77   MessageBoxA                         00 i........SD.¦....
33:0042FC77  N/A                                   5 .m.w....kernel32
33:FFFFFFFF  N/A                                   4 .dll.user32.dll.
33:FFFFFFFF  N/A                                   1 ..GetModuleHandl
33:FFFFFFFF  N/A                                   2 eA...MessageBoxA
33:FFFFFFFF  N/A                                  08 ................
33:FFFFFFFF  N/A
33:FFFFFFFF  N/A
```

SandBox Analyzer Pro

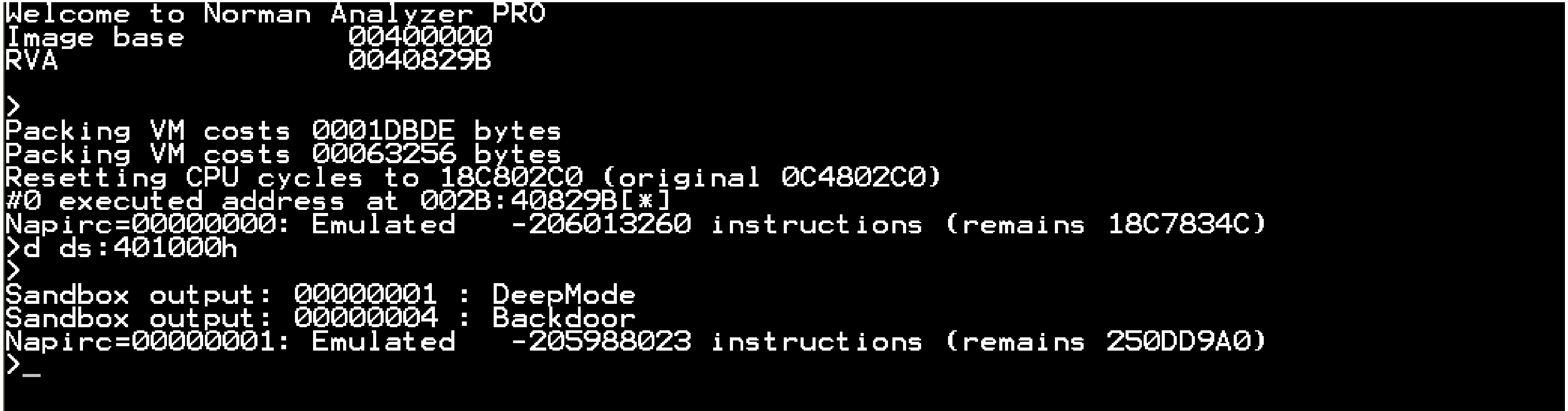
- **API Log view**
  - As the program being emulated interacts with the sandbox operating system, the details of supported APIs are showed in this window.
  - This memory buffer is predefined to be 64MB.
  - API log can be saved to disk



```
00695 KERNEL32!FlsGetValue (0x00000001)
00696 KERNEL32!FlsSetValue (0x00000001,0x73002447)
00697 WS2_32!gethostname (0x4FF922C4,0x000000FF)
00698 WS2_32!gethostbyname ("FAKE")
00699 WS2_32!socket (0x00000002,0x00000001,0x00000000)
00700 KERNEL32!HeapAlloc (0x00000000,0x00000000,0x00000464)
00701 WS2_32!gethostbyname ("irc.quakenet.org")
00702 WS2_32!htons (0x00001A0B)
00703 WS2_32!connect (0x00000002,0x4FF91B60,0x00000010)
00704 -connect port 06667, ["IP"] IP "irc.quakenet.org"
00705 USER32!wsprintfA (0x4FF91A8C,"Connects to "%s" on port %5d (%s)
00706 ",0x72005BB1....)
00707 USER32!wsprintfA (0x73356F8D,":%s %s %s :%s♪
00708 ",0x733566E2....)
00709 USER32!wsprintfA (0x73356FCB,":%s %s %s :%s♪
00710 ",0x733566E2....)
00711 WS2_32!ioctlsocket (0x00000002,0x8004667E,0x4FF91B5C)
00712 WS2_32!send (0x00000002,0x4FF91BA4,0x00000033,0x00000000)
00713  4FF91BA4 55 53 45 52 20 49 72 63 4D 73 67 65 72 20 31 32   USER IrcMsger
```

SandBox Analyzer Pro

- **Command input view**
  - This view will receive information from the sandbox regarding detection, emulation cycles done etc
  - You are able to give specific command to the SandBox
  - Currently 30 commands are available, including;
    - Set a breakpoint on a given interrupt
    - Set a breakpoint on a memory write on the given selector:offset
    - Will display stack trace
    - Show the MMX registers
    - Show page table.
    - +25 more

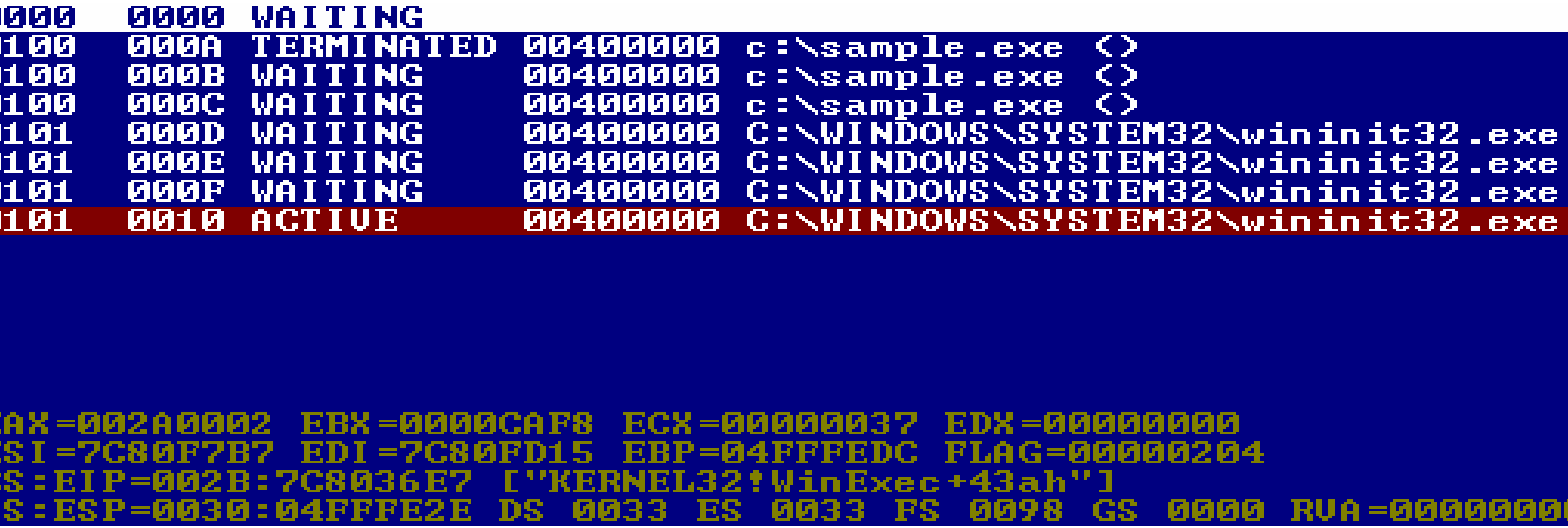


```
Welcome to Norman Analyzer PRO
Image base         00400000
RVA                0040829B

>
Packing VM costs 0001DBDE bytes
Packing VM costs 00063256 bytes
Resetting CPU cycles to 18C802C0 (original 0C4802C0)
#0 executed address at 002B:40829B[*]
Napirc=00000000: Emulated   -206013260 instructions (remains 18C7834C)
>d ds:401000h
>
Sandbox output: 00000001 : DeepMode
Sandbox output: 00000004 : Backdoor
Napirc=00000001: Emulated   -205988023 instructions (remains 250DD9A0)
>_
```

SandBox Analyzer Pro

•Thread view

- Shows information on all created threads
  - thread ID
  - thread status
  - Information regarding active threads
- Possibility to navigate the different threads

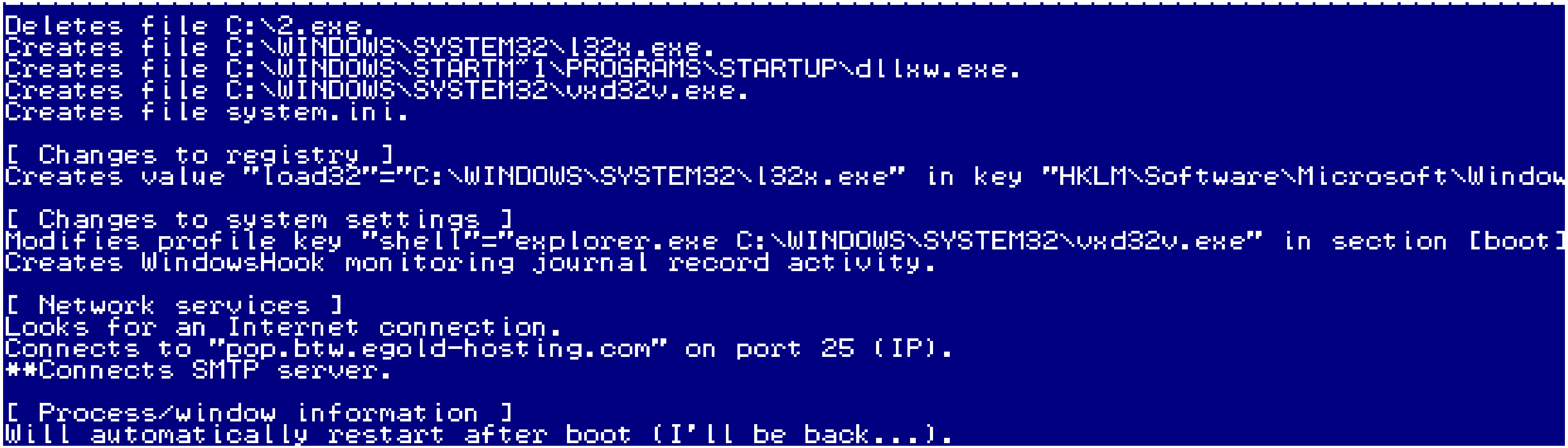


```
000   0000 WAITING
100   000A TERMINATED 00400000 c:\sample.exe ()
100   000B WAITING    00400000 c:\sample.exe ()
100   000C WAITING    00400000 c:\sample.exe ()
101   000D WAITING    00400000 C:\WINDOWS\SYSTEM32\wininit32.exe
101   000E WAITING    00400000 C:\WINDOWS\SYSTEM32\wininit32.exe
101   000F WAITING    00400000 C:\WINDOWS\SYSTEM32\wininit32.exe
101   0010 ACTIVE     00400000 C:\WINDOWS\SYSTEM32\wininit32.exe




AX=002A0002 EBX=0000CAF8 ECX=00000037 EDX=00000000
SI=7C80F7B7 EDI=7C80FD15 EBP=04FFFEDC FLAG=00000204
S:EIP=002B:7C8036E7 ["KERNEL32!WinExec+43ah"]
S:ESP=0030:04FFFE2E DS 0033 ES 0033 FS 0098 GS 0000 RVA=0000000
```

SandBox Analyzer Pro

•SandBox Summary View

- A view summarizing the findings of the emulation
- Grouping them into different categories like
  - Changes to file system
  - Changes to registry
  - Changes to system settings
  - Network services used by the analyzed file
  - Process/Window information created

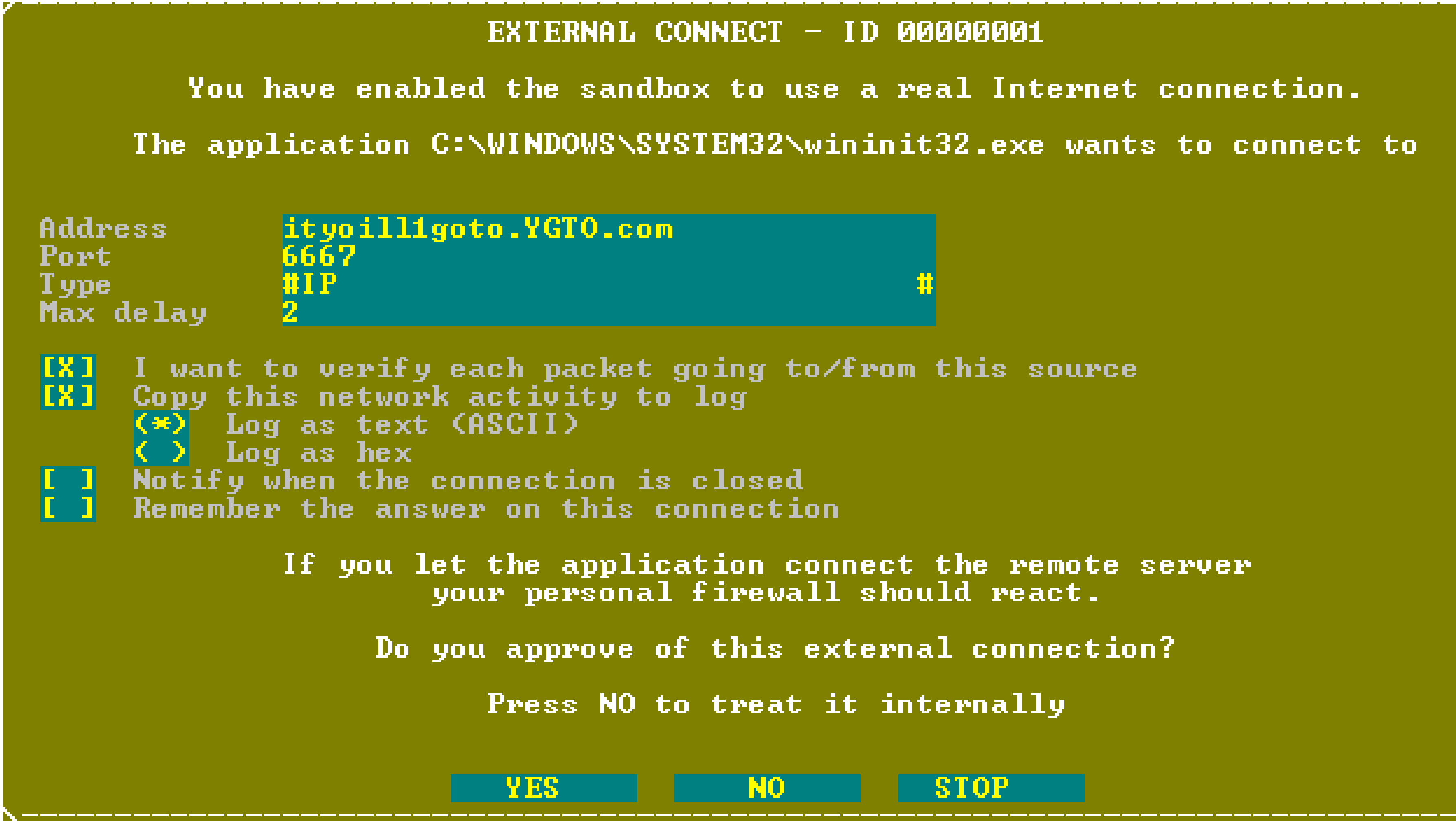


```
Deletes file C:\2.exe.
Creates file C:\WINDOWS\SYSTEM32\l32x.exe.
Creates file C:\WINDOWS\STARTM~1\PROGRAMS\STARTUP\dllxw.exe.
Creates file C:\WINDOWS\SYSTEM32\vxd32v.exe.
Creates file system.ini.

[ Changes to registry ]
Creates value "load32"="C:\WINDOWS\SYSTEM32\l32x.exe" in key "HKLM\Software\Microsoft\Window

[ Changes to system settings ]
Modifies profile key "shell"="explorer.exe C:\WINDOWS\SYSTEM32\vxd32v.exe" in section [boot]
Creates WindowsHook monitoring journal record activity.

[ Network services ]
Looks for an Internet connection.
Connects to "pop.btw.egold-hosting.com" on port 25 (IP).
**Connects SMTP server.

[ Process/window information ]
Will automatically restart after boot (I'll be back...).
```

Connecting to the real internet

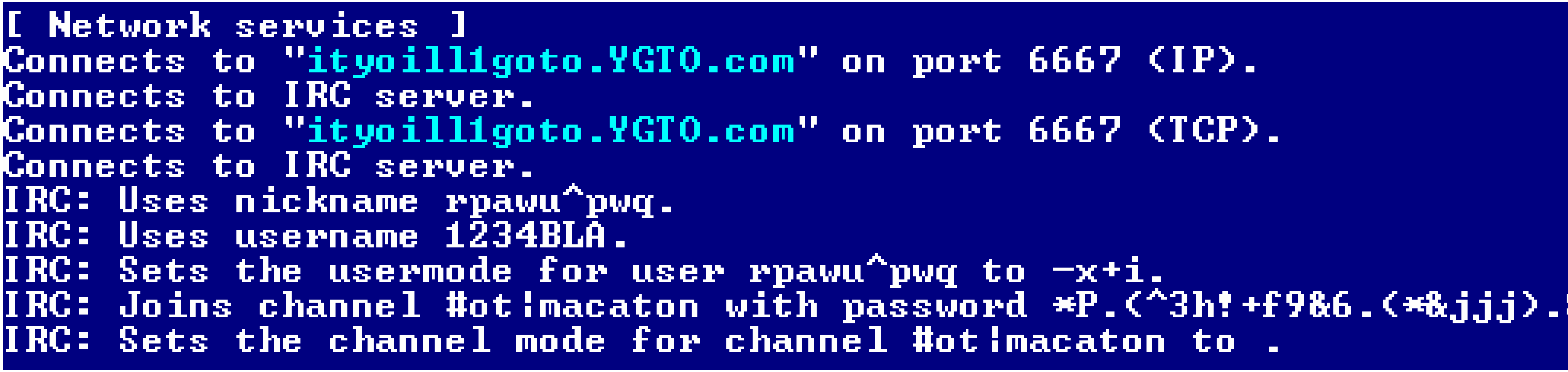
- Why would you want to connect to the real internet?

Connecting to the real internet

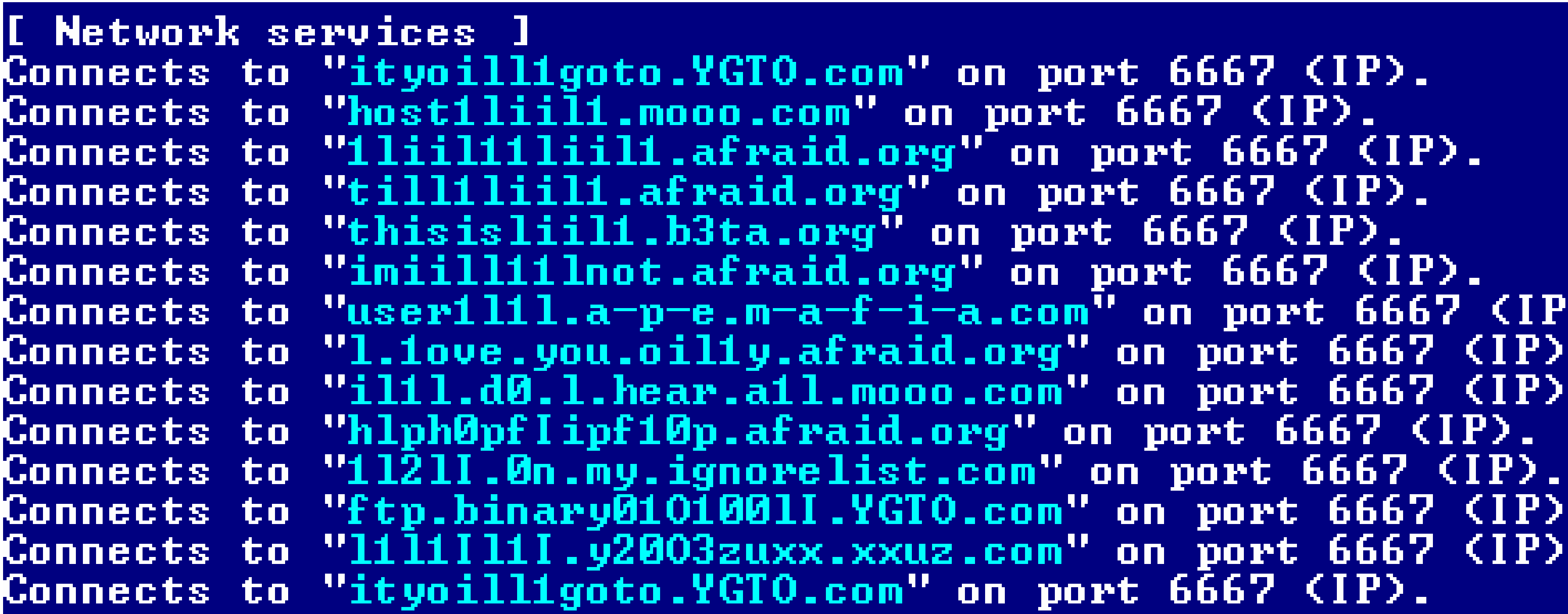


```
                    EXTERNAL CONNECT - ID 00000001

     You have enabled the sandbox to use a real Internet connection.

   The application C:\WINDOWS\SYSTEM32\wininit32.exe wants to connect to


Address        ityoill1goto.YGTO.com
Port           6667
Type           #IP                                    #
Max delay      2

[X]  I want to verify each packet going to/from this source
[X]  Copy this network activity to log
     (*)  Log as text (ASCII)
     ( )  Log as hex
[ ]  Notify when the connection is closed
[ ]  Remember the answer on this connection

           If you let the application connect the remote server
                   your personal firewall should react.

               Do you approve of this external connection?

                      Press NO to treat it internally
```

Internal and/or external



```
[ Network services ]
Connects to "ityoill1goto.YGTO.com" on port 6667 (IP).
Connects to IRC server.
Connects to "ityoill1goto.YGTO.com" on port 6667 (TCP).
Connects to IRC server.
IRC: Uses nickname rpawu^pwq.
IRC: Uses username 1234BLA.
IRC: Sets the usermode for user rpawu^pwq to -x+i.
IRC: Joins channel #ot¦macaton with password *P.(^3h!+f9&6.(*&jjj).
IRC: Sets the channel mode for channel #ot¦macaton to .
```



```
[ Network services ]
Connects to "ityoill1goto.YGTO.com" on port 6667 (IP).
Connects to "host1liil1.mooo.com" on port 6667 (IP).
Connects to "1liil11liil1.afraid.org" on port 6667 (IP).
Connects to "till1liil1.afraid.org" on port 6667 (IP).
Connects to "thisisliil1.b3ta.org" on port 6667 (IP).
Connects to "imiill11lnot.afraid.org" on port 6667 (IP).
Connects to "user1l1l.a-p-e.m-a-f-i-a.com" on port 6667 (IP
Connects to "l.1ove.you.oil1y.afraid.org" on port 6667 (IP)
Connects to "il1l.d0.l.hear.a1l.mooo.com" on port 6667 (IP)
Connects to "hlph0pfIipf10p.afraid.org" on port 6667 (IP).
Connects to "1l2lI.0n.my.ignorelist.com" on port 6667 (IP).
Connects to "ftp.binary0101001I.YGTO.com" on port 6667 (IP)
Connects to "1l1lIl1I.y2003zuxx.xxuz.com" on port 6667 (IP)
Connects to "ityoill1goto.YGTO.com" on port 6667 (IP).
```

What can Norman Sandbox do for you?

- Save time
  - The average response time to a new threat is 6 – 24 hours.
  - Start with knowledge of what the sample is trying to do.
- Save money
  - Growing number of viruses to analyze, growing number of analyst needed to respond to these threats.
- Save the day
  - You’ve been in the situation where something needed to be analyzed yesterday and now you have access to the tools to make it happen.

Demo-time...

Questions and Answers

Righard J. Zwienenberg
Chief Research Officer
Righard.Zwienenberg@norman.no

http://www.norman.com/fr

Norman France
8 Rue de Berri
75008 Paris
Tel: +33-1-42 99 94 14
E-mail: info@norman.fr

Cortina
14 avenue J-B Clement
92100 Boulogne-Billanco
Tel : +33 (0)1 41 10 26 10
Email : info@cortina.fr