Malware Sandbox Analysis

Monnappa KA

www.SecurityXploded.com

Disclaimer

The Content, Demonstration, Source Code and Programs presented here is "AS IS" without any warranty or conditions of any kind. Also the views/ideas/knowledge expressed here are solely of the trainer's only and nothing to do with the company or the organization in which the trainer is currently working.

However in no circumstances neither the Trainer nor SecurityXploded is responsible for any damage or loss caused due to use or misuse of the information presented here.

Acknowledgement

- Special thanks to **Null** community for their extended support and co-operation.
- Special thanks to **ThoughtWorks** for the beautiful venue.
- Thanks to all the trainers who have devoted their precious time and countless hours to make it happen.

Advanced Malware Analysis Training

This presentation is part of our **Advanced Malware Analysis** Training program. Currently it is delivered only during our local meets for FREE of cost.

For complete details of this course, visit our Security Training page.

Who am I?

Monnappa

- Member, SecurityXploded
- Info Security Investigator @ Cisco
- Reversing, Malware Analysis, Memory Forensics.
- Email: monnappa22@gmail.com
- Twitter: @monnappa22
- LinkedIn: http://www.linkedin.com/pub/monnappa-ka-grem-ceh/42/45a/1b8

Content

- Sandbox Overview
- Why Sandbox Analysis
- Sandbox Architecture
- Online Sandboxes
- Custom Sandbox (Sandbox.py)
- Sandbox.py working
- Sandbox.py report
- Demo 1&2 (Sandbox Analysis)

Sandbox Overview

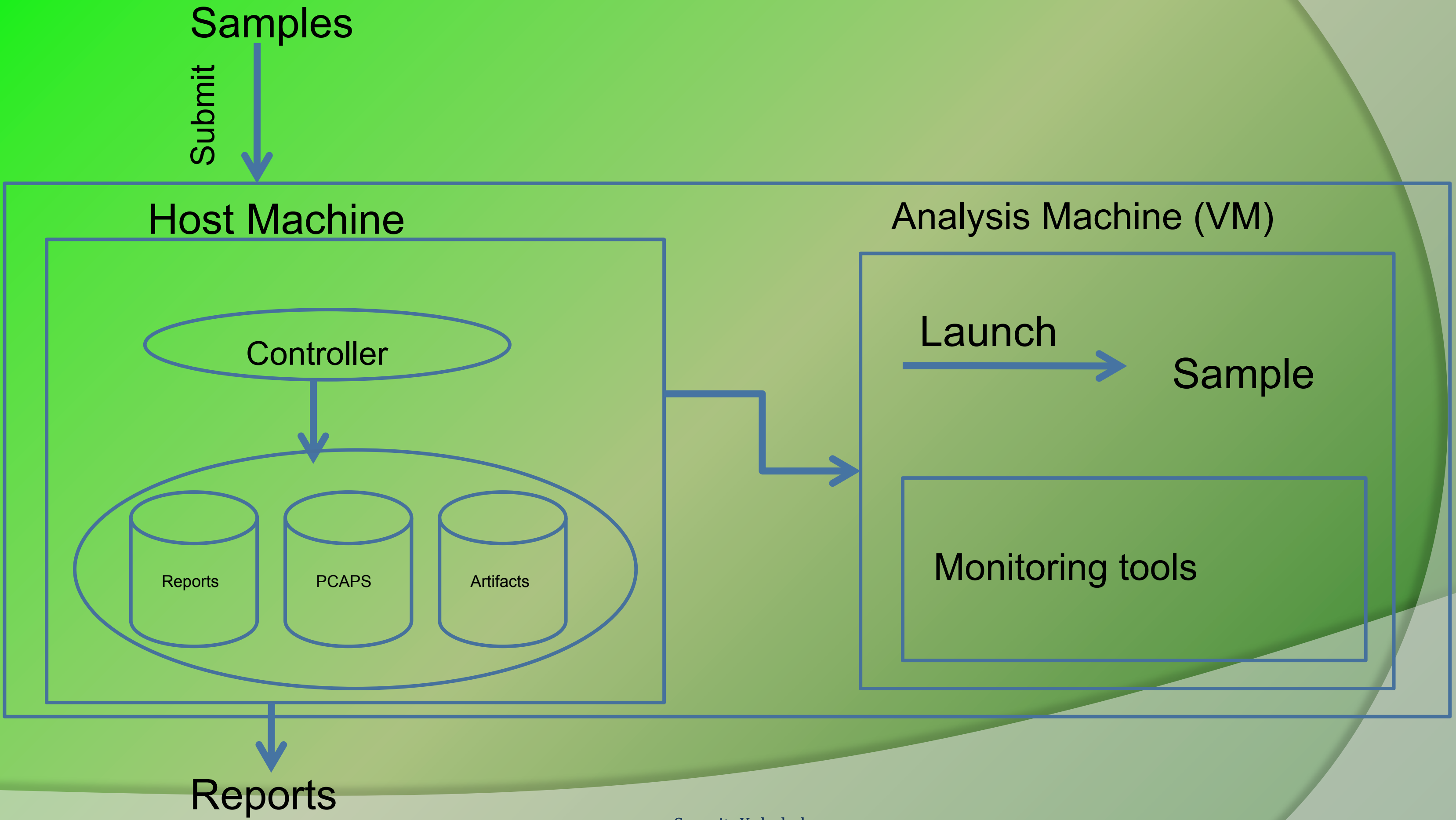
- Execute malware in a controlled/monitored environment
- Monitors file system, registry, process and network activity
- Outputs the results in multiple formats
- Examples of Sandboxes
  - Cuckoo Sandbox
  - ThreatExpert
  - Anubis
  - CWSandbox

Why Sandbox Analysis?

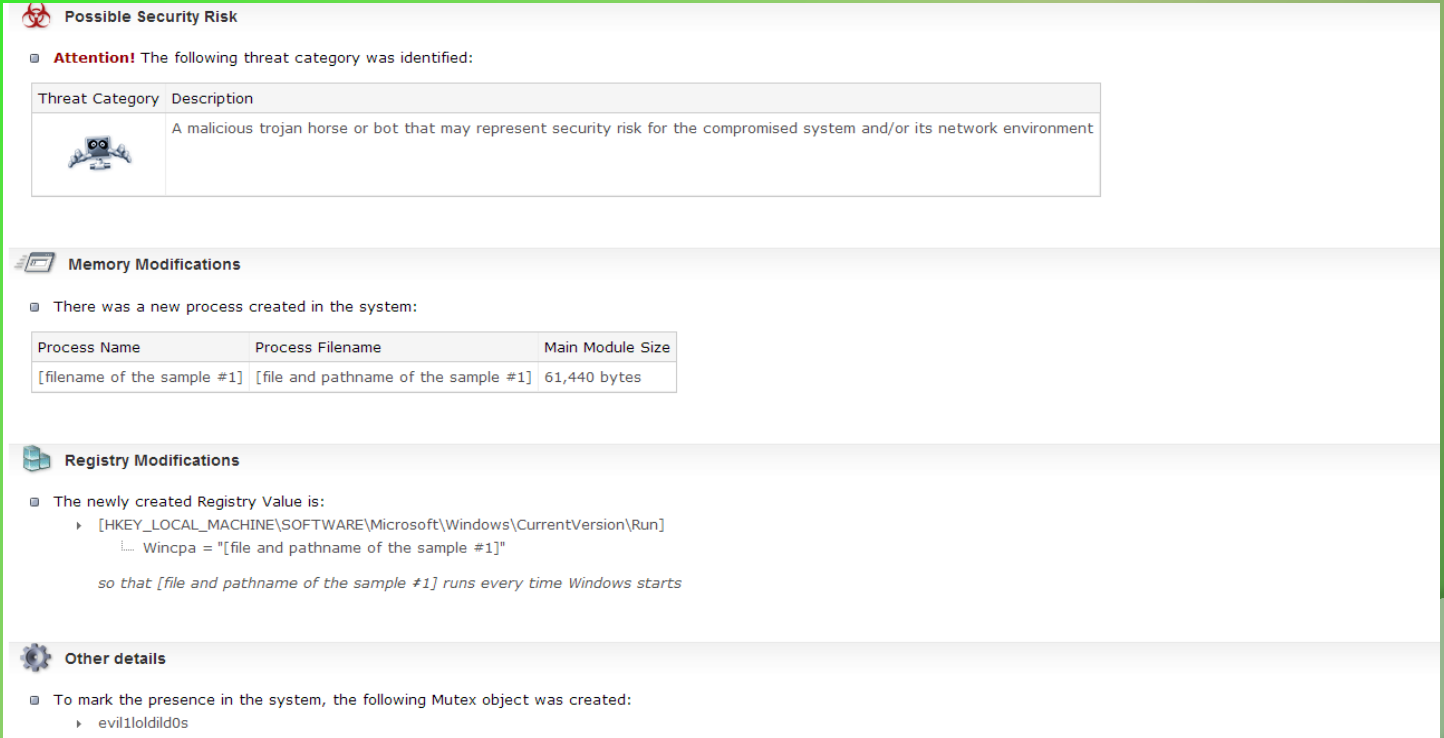
To determine:

- The nature and purpose of the malware
- Interaction with the file system
- Interaction with the registry
- Interaction with the network
- To determine identifiable patterns

Sandbox Architecture



Online Sandbox –ThreatExpert results



Possible Security Risk

- **Attention!** The following threat category was identified:

Threat Category	Description
	A malicious trojan horse or bot that may represent security risk for the compromised system and/or its network environment

Memory Modifications

- There was a new process created in the system:

Process Name	Process Filename	Main Module Size
[filename of the sample #1]	[file and pathname of the sample #1]	61,440 bytes

Registry Modifications

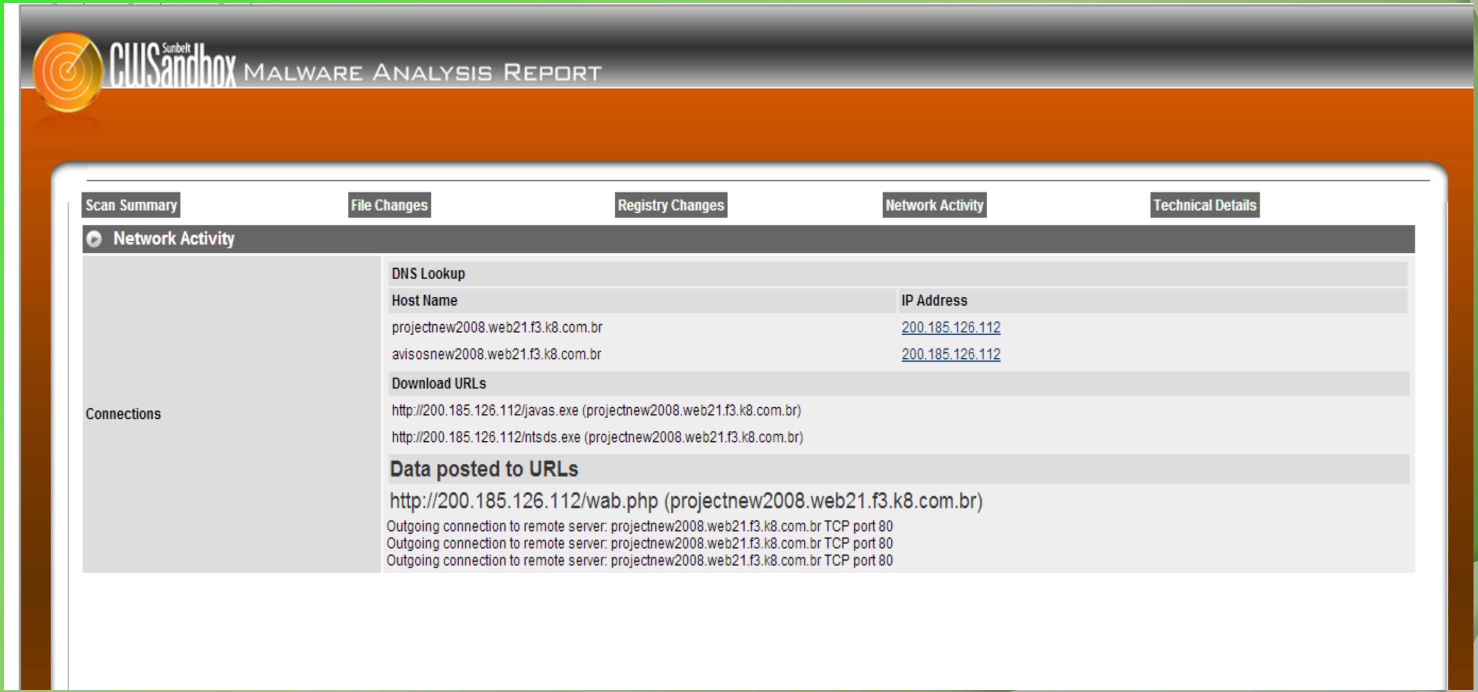
- The newly created Registry Value is:
  - [HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
    - Wincpa = "[file and pathname of the sample #1]"

  so that [file and pathname of the sample #1] runs every time Windows starts

Other details

- To mark the presence in the system, the following Mutex object was created:
  - evil1loldild0s

Online Sandbox –CWSandbox results



Network Activity

Connections

DNS Lookup

Host Name	IP Address
projectnew2008.web21.f3.k8.com.br	200.185.126.112
avisosnew2008.web21.f3.k8.com.br	200.185.126.112

Download URLs

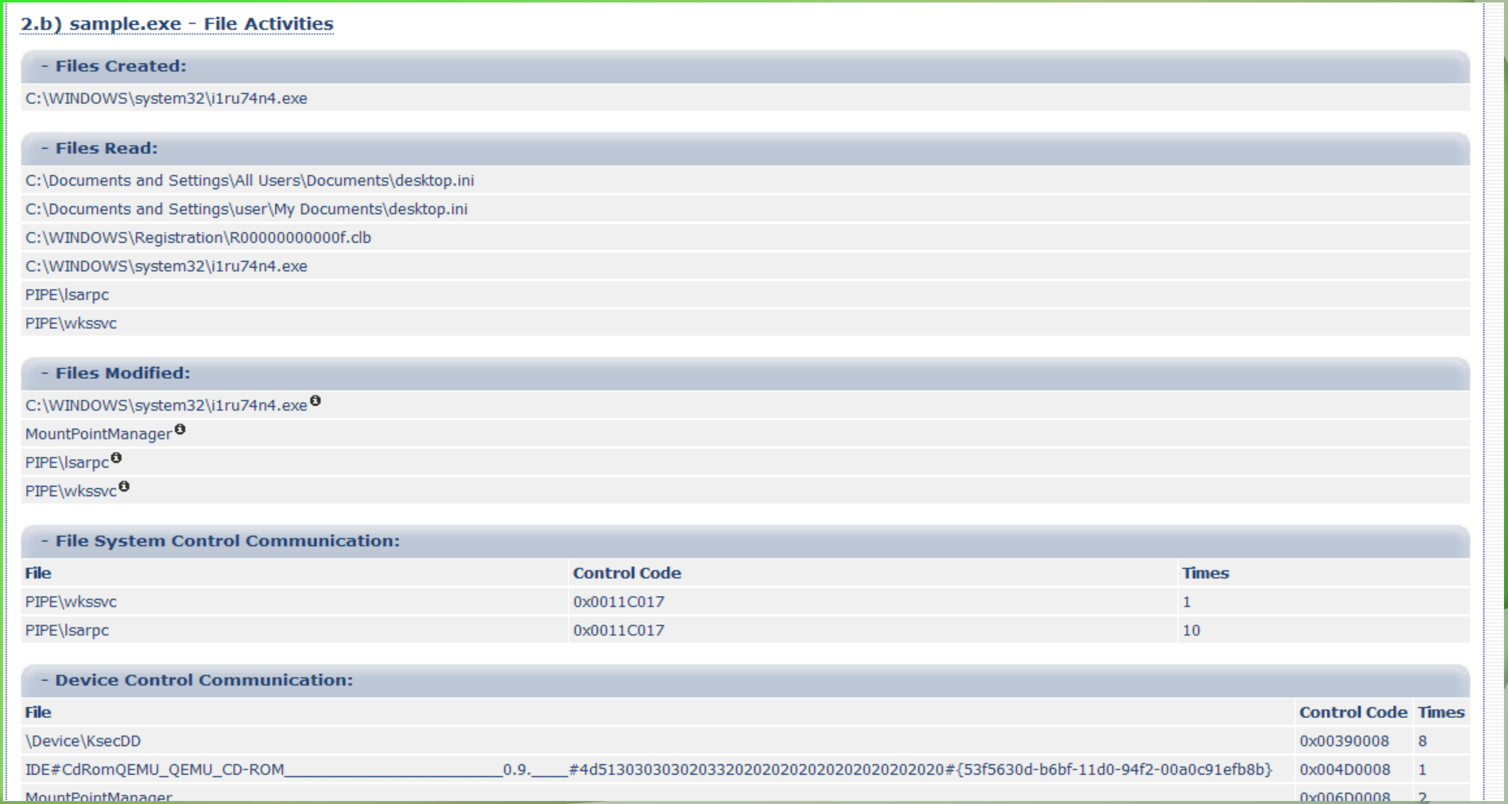
http://200.185.126.112/javas.exe (projectnew2008.web21.f3.k8.com.br)
http://200.185.126.112/ntsds.exe (projectnew2008.web21.f3.k8.com.br)

Data posted to URLs

http://200.185.126.112/wab.php (projectnew2008.web21.f3.k8.com.br)

```
Outgoing connection to remote server: projectnew2008.web21.f3.k8.com.br TCP port 80
Outgoing connection to remote server: projectnew2008.web21.f3.k8.com.br TCP port 80
Outgoing connection to remote server: projectnew2008.web21.f3.k8.com.br TCP port 80
```

Online Sandbox –Anubis results



2.b) sample.exe - File Activities

- Files Created:

C:\WINDOWS\system32\i1ru74n4.exe

- Files Read:

C:\Documents and Settings\All Users\Documents\desktop.ini

C:\Documents and Settings\user\My Documents\desktop.ini

C:\WINDOWS\Registration\R00000000000f.clb

C:\WINDOWS\system32\i1ru74n4.exe

PIPE\lsarpc

PIPE\wkssvc

- Files Modified:

C:\WINDOWS\system32\i1ru74n4.exe

MountPointManager

PIPE\lsarpc

PIPE\wkssvc

- File System Control Communication:

File	Control Code	Times
PIPE\wkssvc	0x0011C017	1
PIPE\lsarpc	0x0011C017	10

- Device Control Communication:

File	Control Code	Times
\Device\KsecDD	0x00390008	8
IDE#CdRomQEMU_QEMU_CD-ROM________________________0.9.____#4d51303030303320202020202020202020202020#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}	0x004D0008	1
MountPointManager	0x006D0008	2

Custom Sandbox – sandbox.py

- Automates static, dynamic and Memory analysis using open source tools
- Written in python
- Can be run in sandbox mode or internet mode
- In sandbox mode it can simulate internet services (this is the default mode)
- Allows you to set the timeout for the malware to run (default is 60 seconds)
- Stores final reports, pcaps, desktop screeshot , and malicious artifacts for later analysis

Sandbox.py (working)

- Takes sample as input
- Performs static analysis
- Reverts VM to clean snapshot
- Starts the VM
- Transfers the malware to VM
- Runs the monitoring tools (to monitor process, registry, file system, network activity)
- Executes the malware for the specified time

Sandbox.py (working contd)

- Stops the monitoring tools
- Suspends the VM
- Acquires the memory image
- Performs memory analysis using Volatility framework
- Stores the results (Final reports, destkop screenshot, pcaps and malicious artifacts for later analysis)

Sandbox.py Report

Static analysis results:

- File type (uses magic python module)
- Cryptographic hash (md5sum – uses hashlib python module)
- VirusTotal results (python script using VirusTotal's public api)
- Determines packers used by malware (uses yara-python)
- Determines the capabilities of the malware like IRC, P2P etc etc (uses yara-python module)

Sandbox.py report

Dynamic analysis results:

- Determines File system activity
- Determines Process activity
- Determines Registry activity
- Monitor Network activity
- Displays DNS summary
- Shows TCP conversations
- Displays HTTP requests & HTTP request tree

Sandbox.py report

Memory analysis results:

- uses Volatility advanced memory forensics framework
- displays process, hidden process in memory
- displays network connections, terminated network connections
- displays listening sockets
- determines api hooks, code injection and embedded executable in memory
- displays DLL's loaded by the process memory
- displays services in memory
- displays the registry keys (like run registry key)

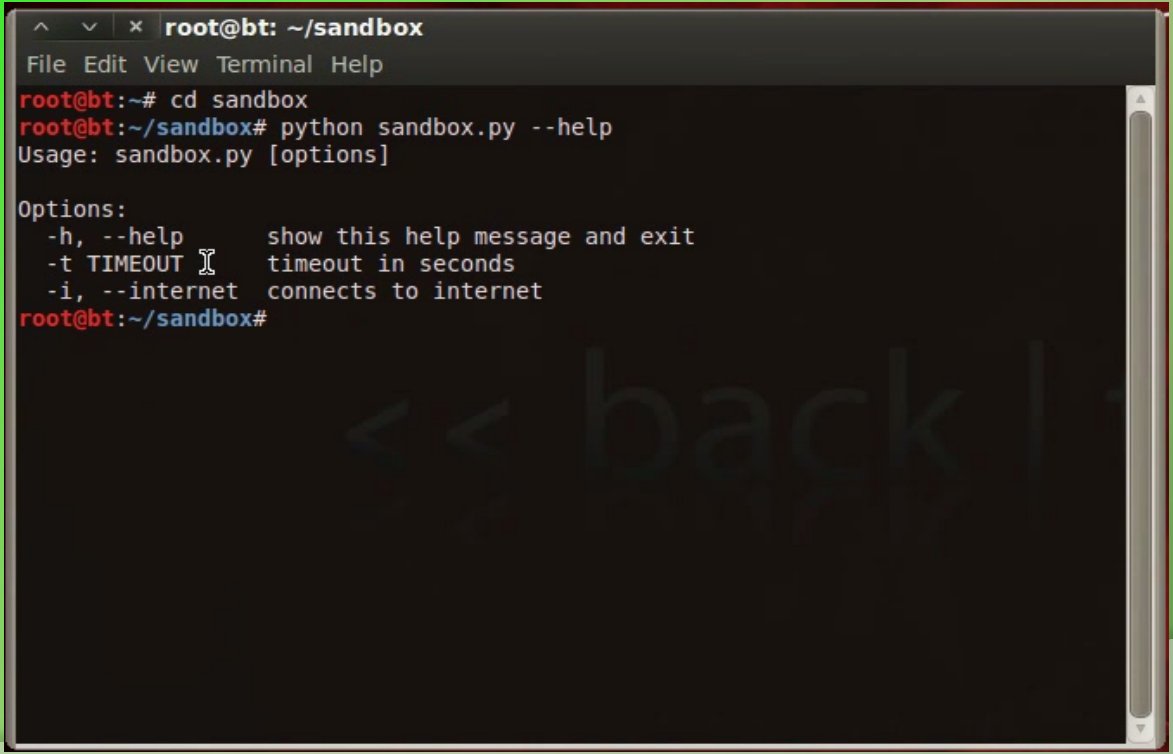
DEMO 1, 2 & 3

(SANDBOX ANALYSIS)

All Training Demo Videos are available at
http://securityxploded.com/security-training-videos.php

Sandbox.py – Help option

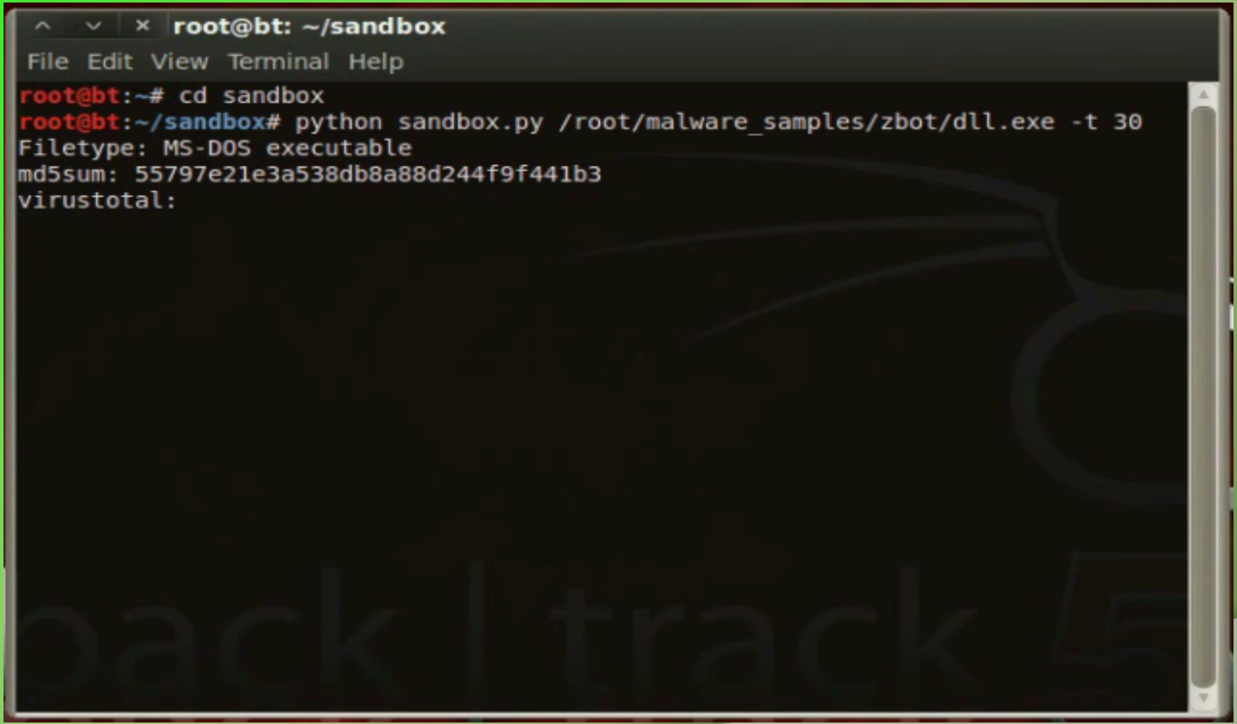
The below screenshot shows the sandbox.py help option



```
root@bt:~# cd sandbox
root@bt:~/sandbox# python sandbox.py --help
Usage: sandbox.py [options]

Options:
  -h, --help      show this help message and exit
  -t TIMEOUT      timeout in seconds
  -i, --internet  connects to internet
root@bt:~/sandbox#
```

Sandbox.py – Input

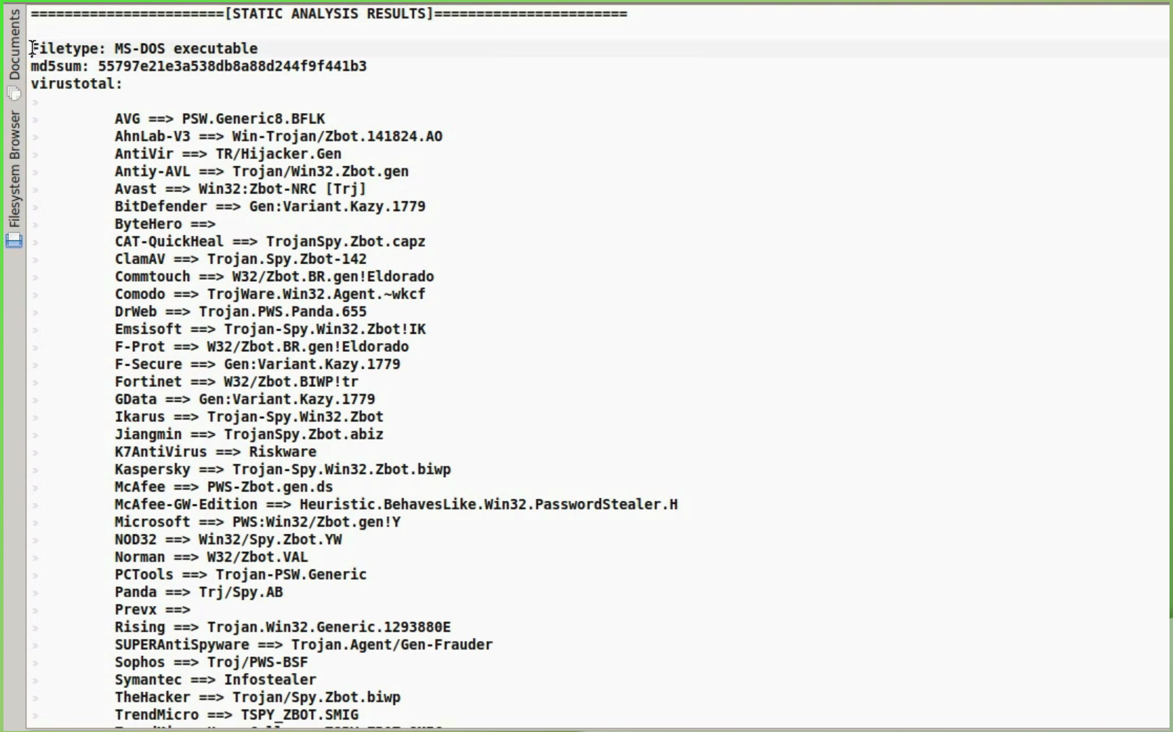
The below screenshot shows the sandbox.py taking sample as input to run it for 30 seconds



```
root@bt:~# cd sandbox
root@bt:~/sandbox# python sandbox.py /root/malware_samples/zbot/dll.exe -t 30
Filetype: MS-DOS executable
md5sum: 55797e21e3a538db8a88d244f9f441b3
virustotal:
```

Sandbox.py – Static Analysis

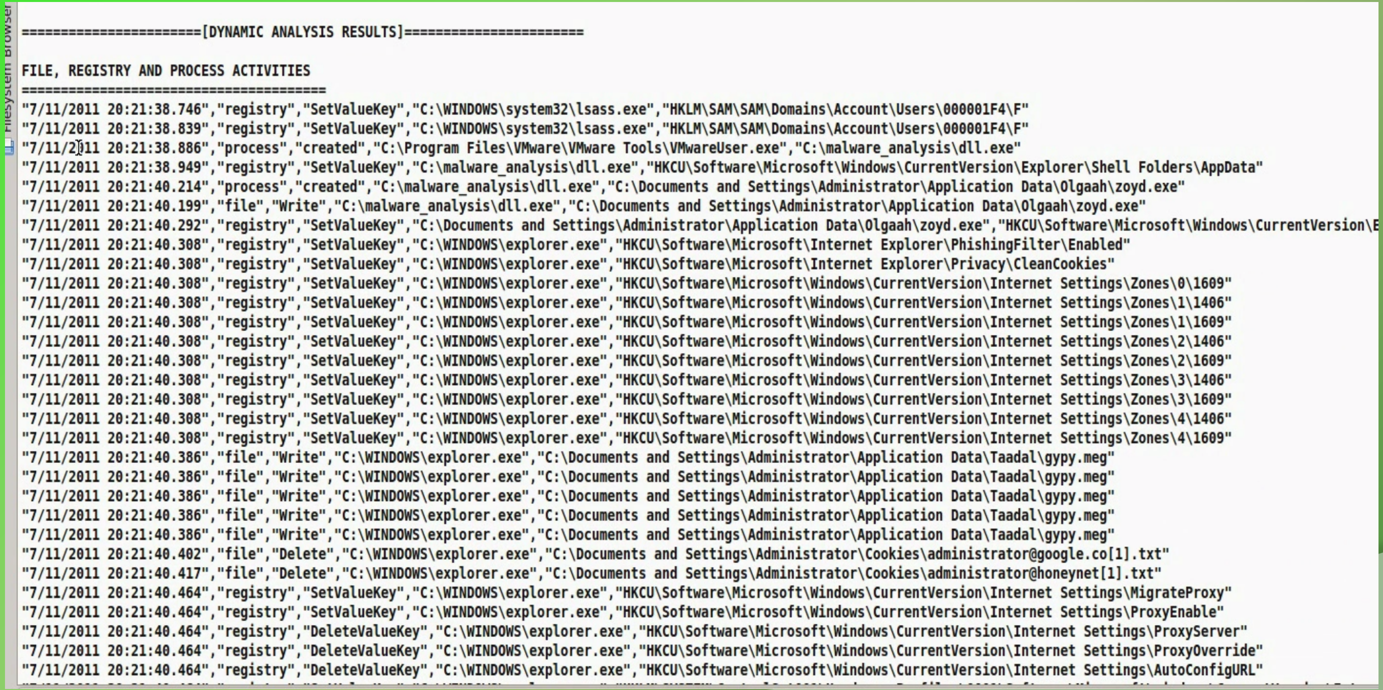
The below screenshot shows the static analysis results after executing the sample



```
=======================[STATIC ANALYSIS RESULTS]=======================

Filetype: MS-DOS executable
md5sum: 55797e21e3a538db8a88d244f9f441b3
virustotal:

          AVG ==> PSW.Generic8.BFLK
          AhnLab-V3 ==> Win-Trojan/Zbot.141824.AO
          AntiVir ==> TR/Hijacker.Gen
          Antiy-AVL ==> Trojan/Win32.Zbot.gen
          Avast ==> Win32:Zbot-NRC [Trj]
          BitDefender ==> Gen:Variant.Kazy.1779
          ByteHero ==>
          CAT-QuickHeal ==> TrojanSpy.Zbot.capz
          ClamAV ==> Trojan.Spy.Zbot-142
          Commtouch ==> W32/Zbot.BR.gen!Eldorado
          Comodo ==> TrojWare.Win32.Agent.~wkcf
          DrWeb ==> Trojan.PWS.Panda.655
          Emsisoft ==> Trojan-Spy.Win32.Zbot!IK
          F-Prot ==> W32/Zbot.BR.gen!Eldorado
          F-Secure ==> Gen:Variant.Kazy.1779
          Fortinet ==> W32/Zbot.BIWP!tr
          GData ==> Gen:Variant.Kazy.1779
          Ikarus ==> Trojan-Spy.Win32.Zbot
          Jiangmin ==> TrojanSpy.Zbot.abiz
          K7AntiVirus ==> Riskware
          Kaspersky ==> Trojan-Spy.Win32.Zbot.biwp
          McAfee ==> PWS-Zbot.gen.ds
          McAfee-GW-Edition ==> Heuristic.BehavesLike.Win32.PasswordStealer.H
          Microsoft ==> PWS:Win32/Zbot.gen!Y
          NOD32 ==> Win32/Spy.Zbot.YW
          Norman ==> W32/Zbot.VAL
          PCTools ==> Trojan-PSW.Generic
          Panda ==> Trj/Spy.AB
          Prevx ==>
          Rising ==> Trojan.Win32.Generic.1293880E
          SUPERAntiSpyware ==> Trojan.Agent/Gen-Frauder
          Sophos ==> Troj/PWS-BSF
          Symantec ==> Infostealer
          TheHacker ==> Trojan/Spy.Zbot.biwp
          TrendMicro ==> TSPY_ZBOT.SMIG
```

Sandbox.py – Dynamic Analysis

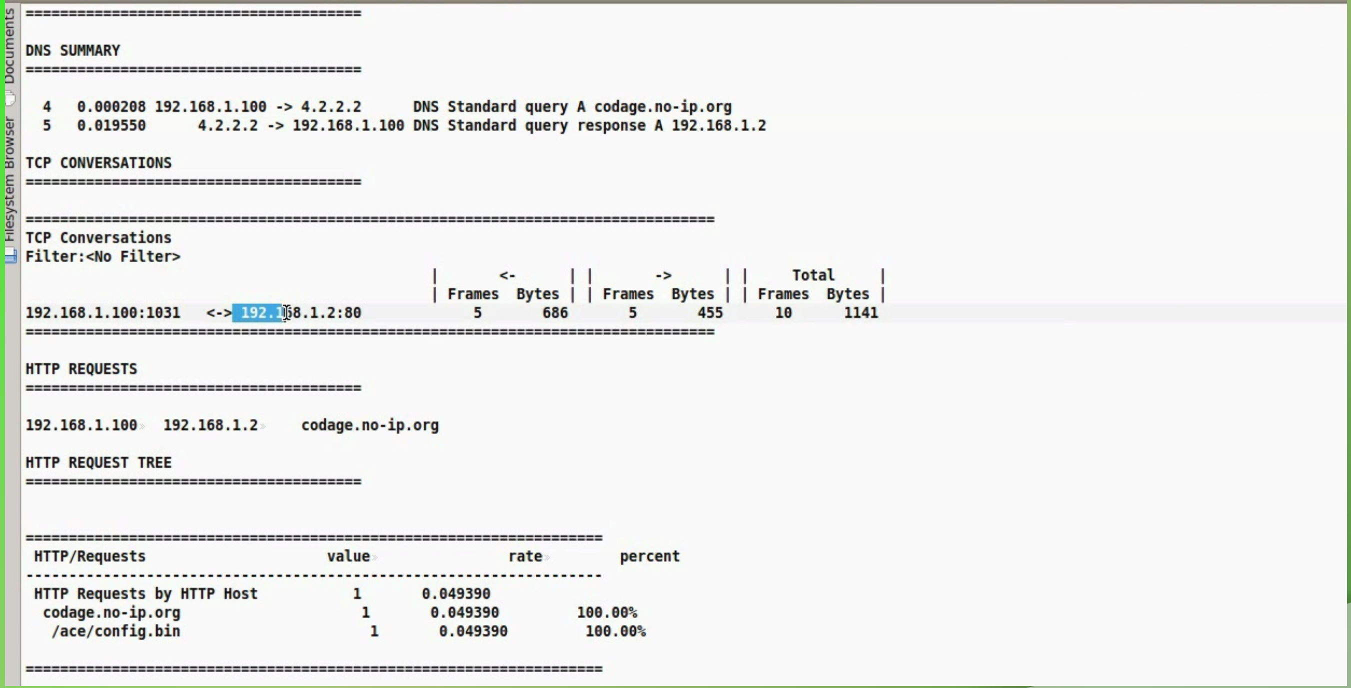
The below screenshot shows the dynamic analysis results after executing the sample



```
=======================[DYNAMIC ANALYSIS RESULTS]=======================

FILE, REGISTRY AND PROCESS ACTIVITIES
=======================================
"7/11/2011 20:21:38.746","registry","SetValueKey","C:\WINDOWS\system32\lsass.exe","HKLM\SAM\SAM\Domains\Account\Users\000001F4\F"
"7/11/2011 20:21:38.839","registry","SetValueKey","C:\WINDOWS\system32\lsass.exe","HKLM\SAM\SAM\Domains\Account\Users\000001F4\F"
"7/11/2011 20:21:38.886","process","created","C:\Program Files\VMware\VMware Tools\VMwareUser.exe","C:\malware_analysis\dll.exe"
"7/11/2011 20:21:38.949","registry","SetValueKey","C:\malware_analysis\dll.exe","HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\AppData"
"7/11/2011 20:21:40.214","process","created","C:\malware_analysis\dll.exe","C:\Documents and Settings\Administrator\Application Data\Olgaah\zoyd.exe"
"7/11/2011 20:21:40.199","file","Write","C:\malware_analysis\dll.exe","C:\Documents and Settings\Administrator\Application Data\Olgaah\zoyd.exe"
"7/11/2011 20:21:40.292","registry","SetValueKey","C:\Documents and Settings\Administrator\Application Data\Olgaah\zoyd.exe","HKCU\Software\Microsoft\Windows\CurrentVersion\E
"7/11/2011 20:21:40.308","registry","SetValueKey","C:\WINDOWS\explorer.exe","HKCU\Software\Microsoft\Internet Explorer\PhishingFilter\Enabled"
"7/11/2011 20:21:40.308","registry","SetValueKey","C:\WINDOWS\explorer.exe","HKCU\Software\Microsoft\Internet Explorer\Privacy\CleanCookies"
"7/11/2011 20:21:40.308","registry","SetValueKey","C:\WINDOWS\explorer.exe","HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0\1609"
"7/11/2011 20:21:40.308","registry","SetValueKey","C:\WINDOWS\explorer.exe","HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1\1406"
"7/11/2011 20:21:40.308","registry","SetValueKey","C:\WINDOWS\explorer.exe","HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1\1609"
"7/11/2011 20:21:40.308","registry","SetValueKey","C:\WINDOWS\explorer.exe","HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2\1406"
"7/11/2011 20:21:40.308","registry","SetValueKey","C:\WINDOWS\explorer.exe","HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2\1609"
"7/11/2011 20:21:40.308","registry","SetValueKey","C:\WINDOWS\explorer.exe","HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\1406"
"7/11/2011 20:21:40.308","registry","SetValueKey","C:\WINDOWS\explorer.exe","HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\1609"
"7/11/2011 20:21:40.308","registry","SetValueKey","C:\WINDOWS\explorer.exe","HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\1406"
"7/11/2011 20:21:40.308","registry","SetValueKey","C:\WINDOWS\explorer.exe","HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4\1609"
"7/11/2011 20:21:40.386","file","Write","C:\WINDOWS\explorer.exe","C:\Documents and Settings\Administrator\Application Data\Taadal\gypy.meg"
"7/11/2011 20:21:40.386","file","Write","C:\WINDOWS\explorer.exe","C:\Documents and Settings\Administrator\Application Data\Taadal\gypy.meg"
"7/11/2011 20:21:40.386","file","Write","C:\WINDOWS\explorer.exe","C:\Documents and Settings\Administrator\Application Data\Taadal\gypy.meg"
"7/11/2011 20:21:40.386","file","Write","C:\WINDOWS\explorer.exe","C:\Documents and Settings\Administrator\Application Data\Taadal\gypy.meg"
"7/11/2011 20:21:40.386","file","Write","C:\WINDOWS\explorer.exe","C:\Documents and Settings\Administrator\Application Data\Taadal\gypy.meg"
"7/11/2011 20:21:40.402","file","Delete","C:\WINDOWS\explorer.exe","C:\Documents and Settings\Administrator\Cookies\administrator@google.co[1].txt"
"7/11/2011 20:21:40.417","file","Delete","C:\WINDOWS\explorer.exe","C:\Documents and Settings\Administrator\Cookies\administrator@honeynet[1].txt"
"7/11/2011 20:21:40.464","registry","SetValueKey","C:\WINDOWS\explorer.exe","HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\MigrateProxy"
"7/11/2011 20:21:40.464","registry","SetValueKey","C:\WINDOWS\explorer.exe","HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable"
"7/11/2011 20:21:40.464","registry","DeleteValueKey","C:\WINDOWS\explorer.exe","HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer"
"7/11/2011 20:21:40.464","registry","DeleteValueKey","C:\WINDOWS\explorer.exe","HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyOverride"
"7/11/2011 20:21:40.464","registry","DeleteValueKey","C:\WINDOWS\explorer.exe","HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\AutoConfigURL"
```

Sandbox.py – Network Activity

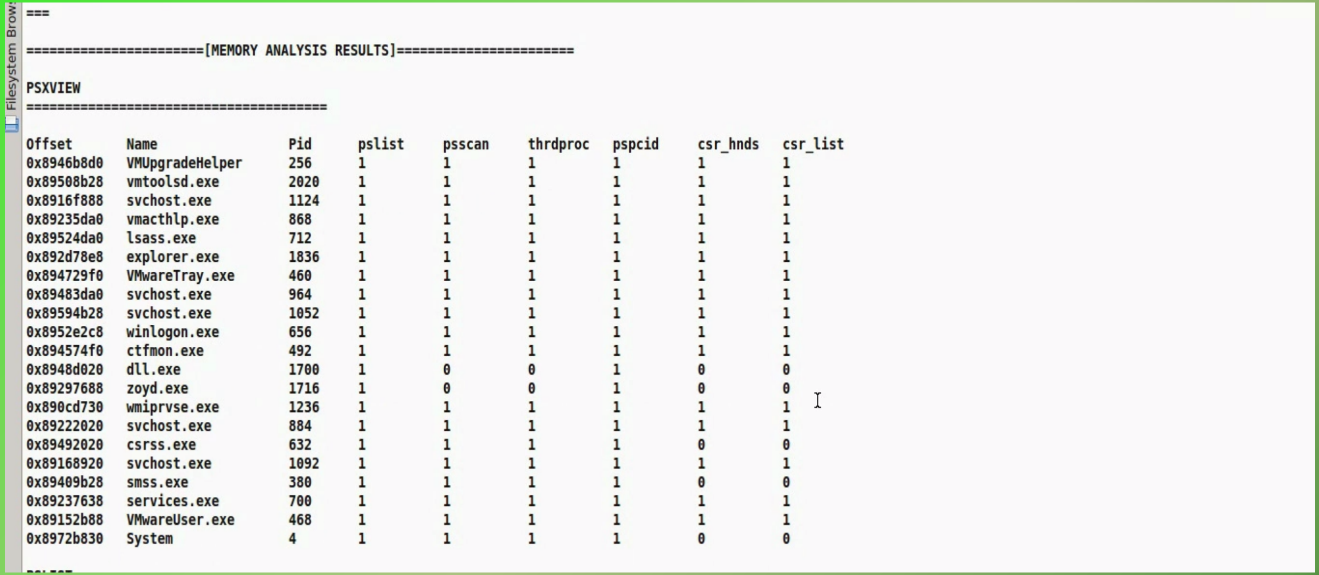
The below screenshot shows the network activity after executing the sample



```
=======================================

DNS SUMMARY
=======================================

  4   0.000208 192.168.1.100 -> 4.2.2.2      DNS Standard query A codage.no-ip.org
  5   0.019550      4.2.2.2 -> 192.168.1.100 DNS Standard query response A 192.168.1.2

TCP CONVERSATIONS
=======================================

================================================================================
TCP Conversations
Filter:<No Filter>
                                               |       <-      | |       ->      | |     Total     |
                                               | Frames  Bytes | | Frames  Bytes | | Frames  Bytes |
192.168.1.100:1031    <-> 192.168.1.2:80            5       686       5       455      10      1141
================================================================================

HTTP REQUESTS
=======================================

192.168.1.100   192.168.1.2     codage.no-ip.org

HTTP REQUEST TREE
=======================================


===================================================================
 HTTP/Requests                    value                rate         percent
-------------------------------------------------------------------
 HTTP Requests by HTTP Host          1       0.049390
  codage.no-ip.org                    1       0.049390         100.00%
   /ace/config.bin                     1       0.049390         100.00%

===================================================================
```

Sandbox.py – Memory Analysis

The below screenshot shows the memory analysis results after executing the sample



```
===

=====================[MEMORY ANALYSIS RESULTS]=====================

PSXVIEW
=======================================

Offset      Name              Pid     pslist    psscan    thrdproc  pspcid    csr_hnds  csr_list
0x8946b8d0  VMUpgradeHelper   256     1         1         1         1         1         1
0x89508b28  vmtoolsd.exe      2020    1         1         1         1         1         1
0x8916f888  svchost.exe       1124    1         1         1         1         1         1
0x89235da0  vmacthlp.exe      868     1         1         1         1         1         1
0x89524da0  lsass.exe         712     1         1         1         1         1         1
0x892d78e8  explorer.exe      1836    1         1         1         1         1         1
0x894729f0  VMwareTray.exe    460     1         1         1         1         1         1
0x89483da0  svchost.exe       964     1         1         1         1         1         1
0x89594b28  svchost.exe       1052    1         1         1         1         1         1
0x8952e2c8  winlogon.exe      656     1         1         1         1         1         1
0x894574f0  ctfmon.exe        492     1         1         1         1         1         1
0x8948d020  dll.exe           1700    1         0         0         1         0         0
0x89297688  zoyd.exe          1716    1         0         0         1         0         0
0x890cd730  wmiprvse.exe      1236    1         1         1         1         1         1
0x89222020  svchost.exe       884     1         1         1         1         1         1
0x89492020  csrss.exe         632     1         1         1         1         0         0
0x89168920  svchost.exe       1092    1         1         1         1         1         1
0x89409b28  smss.exe          380     1         1         1         1         0         0
0x89237638  services.exe      700     1         1         1         1         1         1
0x89152b88  VMwareUser.exe    468     1         1         1         1         1         1
0x8972b830  System            4       1         1         1         1         0         0
```

Reference

Complete Reference Guide for Advanced Malware Analysis Training

[Include links for all the Demos & Tools]

Thank You !

www.SecurityXploded.com