

Financial Malware Analysis- Secrets of ZeuS

Rushita Dave¹,Anisetti Anjaneyulu²

¹Forensics Analyst eSF Labs Ltd.

Abstract- Malware becomes one of the internet's major security threats these days. Malware is the most widespread threat towards IT now. Because of the huge quantity of new malware samples, researchers rely on dynamic malware analysis. Malware analysis is an important part of understanding the objectives of the malware and how to defend against this threat. To be able to defend against the threat imposed by malware we need to understand both how and why the malware exists.

I. INTRODUCTION

Malware is a general term for a piece of software inserted into an information system to cause harm to the system. Malware can gain remote access to system, record and send data to a third party without the user's permission or knowledge. Malware are commonly described as viruses, worms, trojan horses, backdoors, keystroke loggers, rootkits or spyware. Software may contain vulnerabilities, in its structure caused by imperfect coding. Once this type of vulnerabilities is revealed, malware can be developed to exploit them for malicious purposes.

Zeus refers to an entire family of trojans and their respective botnets. Zeus installs a rootkit component to stay hidden on infected systems. To bypass firewalls and to remain active on infected systems, Zeus inserts itself in the address space of other running processes typically Windows Explorer.

Features of Zeus: Capture credentials over HTTP and HTTPS, Steals HTTP and flash cookies, encrypted configuration file, modifies local host files, unique bot identification string.

II. MEMORY FORENSICS FOR MALWARE ANALYSIS

RAM contains critical information about the runtime state of the system while the system is active. By capturing an entire RAM and analyzing it on a separate computer, it is possible to reconstruct the state of the original system, including what applications were running, which files those applications were accessing, which network connections were active, and many other artifacts. For these reasons, memory forensics is extremely important to incident response. Memory forensics helps with unpacking, rootkit detection, and reverse engineering.

A. Tools to capture memory

ManTech Memory DD
Mandiant Memoryze
FTK Imager

DumpIt

Virtual Machine Files (vmem):

Virtual machines provide a useful environment for dynamic analysis of malware. Acquire RAM from guest machines by just suspending or pausing the VM, and guest's RAM will be written to a file on the host's disk. Then grab the ".vmem" file for analysis. The default location of the vmem file for VMware is %My Documents%\My Virtual Machines\<VM Name>*.vmem

B. Tool to analyze the memory

Volatility

The Volatility Framework is an open collection of tools for the extraction of digital artifacts from volatile memory samples. Whether your memory dump is in raw format, a Microsoft crash dump, hibernation file, or virtual machine snapshot, Volatility is able to work with it. It is a very good tool used for malware analysis as malware runs in the memory.

III. MALWARE ANALYSIS USING VOLATILITY

A. Image information (imageinfo)

```
python vol.py -f Zeus_Final.vmem imageinfo
```

Set a profile to tell Volatility what operating system the dump came from. The "imageinfo" output suggests profile that should be passed as the parameter to --profile=PROFILE

B. Scan for the ZeuS Malware (zbotscan)

```
python vol.py --profile=WinXPSP2x86 -f Zeus_2_Final.vmem
zbotscan
```

This will show the version of the ZeuS - ZEUS 2.1.0.1, malware infected process with pid - 1512, registry key - HKCU\SOFTWARE\Microsoft\Irpao and executable - ixmo.exe

Fig 1. zbot command to check for the infected process

C. Checking the process list (psscan)

```
python vol.py --profile=WinXPSP2x86 -f Zeus_2_Final.vmem
psscan
```

This is used for analysis of malware and rootkit activities. It scans for inactive, hidden and unlinked processes by a malware or rootkit.

Check for the process that was shown in the zbotscan command.

Fig.2 List of the process running in the system at the time the dump was taken

Here it shows the detail about the "explorer.exe" which was found before.

D. Handles of the Process (handles)

```
python vol.py --profile=WinXPSP2x86 -f Zeus_2_Final.vmem
handles -p 1512 -t Process
```

Fig.3 Process handles of the "explorer.exe"

Here it shows that explorer.exe is communicating with 2 processes. One is itself explorer.exe and other is ixmo.exe which is executable shown before.

E. Check for the hooks (apihooks)

It is used to find API hooks in user mode or kernel mode. This finds IAT, EAT, Inline style hooks. . For Inline hooks, it detects CALLs and JMPs to direct and indirect locations.

```
python vol.py --profile=WinXPSP2x86 -f Zeus_2_Final.vmem
handles
```

It show the hook type - Inline hook, Process - explorer.exe, victim module - ntdll.dll, kernel32.dll, user32.dll.

F. Check for the modules (ldrmodules)

It is also possible for malware to hide a DLL by simply overwriting the path. Tools that only look for unlinked entries may miss the fact that malware overwrite C:\malicious.dll to show C:\windows\system32\kernel32.dll.

```
python vol.py --profile=WinXPSP2x86 -f Zeus_2_Final.vmem
ldrmodules
```

Fig.4 modules of explorer.exe

It shows the base address of process that can be further use for analyzing the process for finding the injected code in it.

G. Volatility Shell (volshell)

Volshell is the teminal of the volatility itself.

```
python vol.py --profile=WinXPSP2x86 -f Zeus_2_Final.vmem
volshell
```

```
cc(pid=1512)
```

```
db(offset)
```

offset - found from the result of the ldrmodules.

```
C:\Users\ESP\Desktop\Volatility\python vol.py --profile=WinXPSP2x86 -f Zeus_Final.vmem volshell
Volatility Foundation Volatility Framework 2.5.1
Current context: process System, pid=4, ppid=0 DIB=0x334000
Welcome to volshell! Current memory image is:
File:///C:/Users/ESP/Desktop/Volatility/Zeus_Final.vmem
>>> !process 1 1512
Current context: process explorer.exe, pid=1512, ppid=1496 DIB=0x400c00
>>> db(0x7e0000)
0x7e000000 4d 5a 90 00 03 00 00 00 04 ff ff 00 00 MZ.....
0x7e000100 b0 00 00 00 00 00 00 00 00 00 00 00 .....P.....
0x7e000200 00 00 00 00 00 00 00 00 00 00 00 00 .....E.....
0x7e000300 00 00 00 00 00 00 00 00 00 00 00 00 .....F.....
0x7e000400 00 1f 00 00 00 00 00 00 00 00 00 00 .....L.Th
0x7e000500 69 73 20 70 72 6f 67 72 61 64 28 63 61 6e 6f is.program.canno
0x7e000600 74 20 62 65 28 22 75 6e 28 69 6e 28 44 4f 53 28 t.be.run.in.DOS.
0x7e000700 6d 6f 64 65 2e 0d 0d 0s 24 08 00 00 00 00 00 mode...$.....
>>>
```

Fig.5 volatility shell

H. Finding malicious code (malfind)

The malfind is used to find hidden or injected code/DLLs in user mode memory. It is also used to locate sequence of bytes, regular expressions, ANSI strings, or Unicode strings in user mode or kernel memory. The purpose of malfind is to locate DLLs that standard methods/tools do not see.

```
python vol.py --profile=WinXPSP2x86 -f Zeus_2_Final.vmem
malfind
```

```
Process: explorer.exe Pid: 1512 Address: 0xc10000
Vad Tag: Vad_Protection_PPAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6
0x0c100000 b8 35 00 00 00 e9 8b d1 cf 7b 6b 6c 02 00 00 e9 .5.....ch...
0x0c100100 94 63 d0 7b 8b ff 55 8b ec e9 6c 11 c8 7b 8b ff .c.<.0...1.<.
0x0c100200 55 8b ec e9 22 9e 60 76 8b ff 55 8b ec e9 74 60 0.....v.u.t;
0x0c100300 55 8b 88 ff 55 8b ec e9 5b 76 8b ff 55 8b .....v.u.
0xc10000 b835000000 MOU EBX, 0x35
0xc10005 e98hd1cf7b JMP 0x7c9bd195
0xc1000a 686c020000 PUSH DWORD 0x26c
0xc1000f e97463d07b JMP 0x7c9163a8
0xc10014 8fff MOU EDI, EDI
0xc10016 55 PUSH EBP
0xc10017 b8ec MOU EBP, ESP
0xc10019 e96c11c07b JMP 0x7c81118a
0xc1001e 55 MOU EDI, EDI
0xc10020 8b4f PUSH EBP
0xc10021 b8ec MOU EBP, ESP
0xc10023 e9922e6076 JMP 0x772212c1
0xc10028 8bfff MOU EDI, EDI
0xc1002a 55 PUSH EBP
0xc1002b b8ec MOU EBP, ESP
0xc1002d e97465b76 JMP 0x771c60a6
0xc10030 55 MOU EDI, EDI
0xc10034 55 PUSH EBP
0xc10035 b8ec MOU EBP, ESP
0xc10037 e98a95b76 JMP 0x771cc9c6
0xc1003c 55 MOU EDI, EDI
0xc1003e 55 PUSH EBP
0xc1003f 8b DB 0x8b
```

Fig.6 malfind command for hidden or injected code

detect the presence of Zeus. The first memory segment was detected because its executable and has meaning that there is memory mapped file already occupying the space.

I. Yara File Scan (yarascan)

Yara file is a set of rules to identify the behavior of the malware. It contains the list of the strings that is needed to be searched in the memory image for analyzing the behavior of the malware.

```
C:\Users\ESP\Desktop\Volatility\python vol.py --profile=WinXPSP2x86 -f Zeus_Final.vmem yarascan -y "C:/Users/ESP/Desktop/Volatility/yara.rules\zeus_v1_OldZeus.dev"
Volatility Foundation Volatility Framework 2.5.1
[0] : crime_01Zeus
[0] : crime_01Zeus.dev
[0] : crime_01Zeus.exe
[0] : crime_01Zeus.fid 1512
0x00001614 68 5a 90 00 03 00 00 00 04 ff ff 00 00 MZ.....
0x00001615 65 2a 63 00 64 21 77 85 62 83 79 00 63 00 http://www.google.com/webhp.h...
0x00001616 65 2a 63 00 64 21 77 85 62 83 79 00 63 00 .....
0x00001617 65 2a 63 00 64 21 77 85 62 83 79 00 63 00 .....
0x00001618 65 2a 63 00 64 21 77 85 62 83 79 00 63 00 .....
0x00001619 24 00 65 00 66 00 68 00 73 61 63 00 71 00 66 00
[0] : crime_01Zeus.dev
[0] : crime_01Zeus.exe
[0] : crime_01Zeus.fid 1512
0x00001720 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 http://www.google.com/webhp.h...
0x00001721 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IP.Clar...
0x00001722 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 Pk.Read.Fs.Write...
0x00001723 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...http://www.google.com...
0x00001724 55 61 64 00 58 52 5f 57 72 63 74 00 68 00 68 00
0x00001725 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001726 73 00 65 00 66 00 68 00 73 00 74 00 68 00 65 00 ...IPB...003...
0x00001727 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001728 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001729 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000172a 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000172b 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000172c 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000172d 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000172e 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000172f 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001730 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001731 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001732 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001733 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001734 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001735 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001736 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001737 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001738 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001739 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000173a 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000173b 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000173c 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000173d 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000173e 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000173f 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001740 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001741 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001742 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001743 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001744 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001745 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001746 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001747 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001748 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001749 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000174a 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000174b 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000174c 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000174d 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000174e 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000174f 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001750 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001751 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001752 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001753 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001754 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001755 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001756 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001757 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001758 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001759 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000175a 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000175b 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000175c 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000175d 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000175e 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000175f 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001760 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001761 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001762 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001763 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001764 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001765 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001766 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001767 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001768 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001769 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000176a 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000176b 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000176c 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000176d 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000176e 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000176f 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001770 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001771 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001772 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001773 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001774 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001775 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001776 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001777 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001778 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001779 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000177a 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000177b 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000177c 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000177d 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000177e 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000177f 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001780 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001781 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001782 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001783 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001784 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001785 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001786 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001787 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001788 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001789 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000178a 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000178b 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000178c 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000178d 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000178e 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000178f 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001790 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001791 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001792 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001793 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001794 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001795 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001796 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001797 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001798 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x00001799 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000179a 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000179b 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000179c 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000179d 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000179e 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x0000179f 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x000017a0 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x000017a1 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x000017a2 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x000017a3 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x000017a4 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x000017a5 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x000017a6 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x000017a7 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x000017a8 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x000017a9 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x000017aa 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x000017ab 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x000017ac 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x000017ad 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x000017ae 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x000017af 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x000017b0 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x000017b1 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x000017b2 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x000017b3 5b 52 5f 00 70 65 6e 54 53 63 6f 63 65 64 ...IPB...003...
0x000017b4 5b 
```

K. Checking event logs (evtlogs)

```
python vol.py --profile=WinXPSP2x86 -f Zeus_2_Final.vmem
evtlogs -D C:\Users\ESF\Desktop\Dump
```

The "sysevent.txt" file is the important file to be analyzed from the four files that is acquired by this command.

It shows that a socket operation was attempted to unreachable host. It means that some process of the system has tried to connect to the remote server. It also shows that the computer browser is stopped. It means that at some point of time the computer browser was stared.

VI. CONCLUSION

Volatility tool gives the detailed result of the malware behavior. It shows the infected process among the all running processes in the system, the malware information, the infected executable. It also shows the string of the malware. It states that the malware tries to hide itself behind the legitimate process of the system and infect the system.

REFERENCES

- [1] Malware Analyst's cookbook and DVD:Tools and Techniques for Fighting Malicious Code Paperback by Michael Ligh (Author), Steven Adair (Author), Blake Hartstein (Author),Matthew Richard (Author)
- [2] Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software Paperback by Michael Sikorski (Author), Andrew Honig (Author)
- [3] Mandiant Practical Malware Analysis by Kris Kendall
- [4] https://code.google.com/p/volatility/wiki/CommandReference#Image_Identification
- [5] <https://code.google.com/p/volatility/wiki/LinuxMemoryForensics>
- [6] <http://msdn.microsoft.com/en-US>
- [7] Symantec : ZeuS: King of the bots by Nicolas Falliere and Eric Chien
- [8] www.secarma.co.uk/blog/2013/04/03/how-to-installing-volatility-on-windows-7-64-bit/
- [9] SANS CheetSheet v2.3
- [10] Reversing and Malware Analysis Training [2012]
- [11] Malware Analysis: An Introduction, SANS Institute InfoSec Reading Room, by Author: Dennis Distler