Harsimran Kaur V00879358
Maninder Singh V00879900

Elec 570 Project I: Investigating an Infected Machine

(Weight: 15%; Due June 8, 2017)

Case Description

One of the managers of a company fell for a spearphishing scam, which was delivered through a spam email containing a file attachment. After opening the file, the manager did not notice anything; however, recently they have started experiencing unusual activity in the company's accounts. This triggered an investigation, where first responders were able to collect a memory image of the suspected infected machine.

As a forensics investigator, your mission is to analyze the memory image and report on any suspected activities found.

Task

Provide a report analysing suspicious activities by answering the following questions:

1. **Identify running processes, and determine which ones look suspicious and justify why. Process is most likely responsible for the initial exploit. [4%]**

Solution:

To identify running processes first we need to start Volatility as follows:

Forensics Tools>Memory Forensics>Volatility

Then we need to find the image information so that we can extract the running processes as follows:

python vol.py -f /home/caine/Desktop/caineshared/project1-c/project1-c.vmem imageinfo

```
caine@Caine:/usr/share/caine/pacchetti/volatility$ python vol.py -f /home/caine/
Desktop/CaineShared/project1-c/project1-c.vmem imageinfo
Volatility Foundation Volatility Framework 2.4
Determining profile based on KDBG search...

          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with Win
XPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/caine/Desktop/CaineShar
ed/project1-c/project1-c.vmem)
                      PAE type : PAE
                           DTB : 0x2fe000L
                          KDBG : 0x80545ae0
          Number of Processors : 1
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000
             KUSER_SHARED_DATA : 0xffdf0000
           Image date and time : 2012-07-22 02:45:08 UTC+0000
     Image local date and time : 2012-07-21 22:45:08 -0400
caine@Caine:/usr/share/caine/pacchetti/volatility$
```

Here we can see that Image type is service pack 3, which points to WinXPSP2x86 as profile. Now we can see identify running processes.

For this we will export profile and location by setting environment variables, so that we don't have to give the folder location again and again.

export VOLATILITY_LOCATION=file:///home/caine/Desktop/caineshared/project1-c/project1-c.vmem
export VOLATILITY_PROFILE=WinXPSP3x86

Now identifying rogue processes by following command:
python vol.py pslist

```
caine@Caine:/usr/share/caine/pacchetti/volatility$ export VOLATILITY_LOCATION=file:///home/caine/Desktop/CaineShared/project1-c/project
1-c.vmem
caine@Caine:/usr/share/caine/pacchetti/volatility$ export VOLATILITY_PROFILE=WinXPSP2x86
caine@Caine:/usr/share/caine/pacchetti/volatility$ python vol.py pslist
Volatility Foundation Volatility Framework 2.4
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                         Exit
--
0x823c89c8 System                    4      0     53      240 ------      0
0x822f1020 smss.exe                368      4      3       19 ------      0 2012-07-22 02:42:31 UTC+0000
0x822a0598 csrss.exe               584    368      9      326      0      0 2012-07-22 02:42:32 UTC+0000
0x82298700 winlogon.exe            608    368     23      519      0      0 2012-07-22 02:42:32 UTC+0000
0x81e2ab28 services.exe            652    608     16      243      0      0 2012-07-22 02:42:32 UTC+0000
0x81e2a3b8 lsass.exe               664    608     24      330      0      0 2012-07-22 02:42:32 UTC+0000
0x82311360 svchost.exe             824    652     20      194      0      0 2012-07-22 02:42:33 UTC+0000
0x81e29ab8 svchost.exe             908    652      9      226      0      0 2012-07-22 02:42:33 UTC+0000
0x823001d0 svchost.exe            1004    652     64     1118      0      0 2012-07-22 02:42:33 UTC+0000
```

```
0x821dfda0 svchost.exe            1056    652      5       60      0      0 2012-07-22 02:42:33 UTC+0000
0x82295650 svchost.exe            1220    652     15      197      0      0 2012-07-22 02:42:35 UTC+0000
0x821dea70 explorer.exe           1484   1464     17      415      0      0 2012-07-22 02:42:36 UTC+0000
0x81eb17b8 spoolsv.exe            1512    652     14      113      0      0 2012-07-22 02:42:36 UTC+0000
0x81e7bda0 reader_sl.exe          1640   1484      5       39      0      0 2012-07-22 02:42:36 UTC+0000
0x820e8da0 alg.exe                 788    652      7      104      0      0 2012-07-22 02:43:01 UTC+0000
0x821fcda0 wuauclt.exe            1136   1004      8      173      0      0 2012-07-22 02:43:46 UTC+0000
0x8205bda0 wuauclt.exe            1588   1004      5      132      0      0 2012-07-22 02:44:01 UTC+0000
caine@Caine:/usr/share/caine/pacchetti/volatility$
```

The columns display the offset, process name, process ID, the parent process ID, number of threads, number of handles, and date/time when the process started. If there is a process with 0 handle and 0 offset then that process is not alive. The **offset is a virtual address** by default, but the **physical offset** can be obtained with the -P switch:

python vol.py pslist –P

```
caine@Caine:/usr/share/caine/pacchetti/volatility$ python vol.py pslist -P
Volatility Foundation Volatility Framework 2.4
Offset(P)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- ------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ----
--
0x025c89c8 System                    4      0     53      240 ------      0
0x024f1020 smss.exe                368      4      3       19 ------      0 2012-07-22 02:42:31 UTC+0000
0x024a0598 csrss.exe               584    368      9      326      0      0 2012-07-22 02:42:32 UTC+0000
0x02498700 winlogon.exe            608    368     23      519      0      0 2012-07-22 02:42:32 UTC+0000
0x0202ab28 services.exe            652    608     16      243      0      0 2012-07-22 02:42:32 UTC+0000
0x0202a3b8 lsass.exe               664    608     24      330      0      0 2012-07-22 02:42:32 UTC+0000
0x02511360 svchost.exe             824    652     20      194      0      0 2012-07-22 02:42:33 UTC+0000
0x02029ab8 svchost.exe             908    652      9      226      0      0 2012-07-22 02:42:33 UTC+0000
0x025001d0 svchost.exe            1004    652     64     1118      0      0 2012-07-22 02:42:33 UTC+0000
0x023dfda0 svchost.exe            1056    652      5       60      0      0 2012-07-22 02:42:33 UTC+0000
0x02495650 svchost.exe            1220    652     15      197      0      0 2012-07-22 02:42:35 UTC+0000
0x023dea70 explorer.exe           1484   1464     17      415      0      0 2012-07-22 02:42:36 UTC+0000
0x020b17b8 spoolsv.exe            1512    652     14      113      0      0 2012-07-22 02:42:36 UTC+0000
0x0207bda0 reader_sl.exe          1640   1484      5       39      0      0 2012-07-22 02:42:36 UTC+0000
0x022e8da0 alg.exe                 788    652      7      104      0      0 2012-07-22 02:43:01 UTC+0000
0x023fcda0 wuauclt.exe            1136   1004      8      173      0      0 2012-07-22 02:43:46 UTC+0000
0x0225bda0 wuauclt.exe            1588   1004      5      132      0      0 2012-07-22 02:44:01 UTC+0000
caine@Caine:/usr/share/caine/pacchetti/volatility$
```

The processes are represented in the form of doubly linked list. Here in these figures locating parent process is difficult so we will display in tree format using **pstree** plugin.

python vol.py pstree

```
caine@Caine:/usr/share/caine/pacchetti/volatility$ python vol.py pstree
Volatility Foundation Volatility Framework 2.4
Name                                                  Pid   PPid   Thds   Hnds Time
..................................................... ...... ...... ...... ...... ....
 0x823c89c8:System                                      4      0     53    240 1970-01-01 00:00:00 UTC+0000
. 0x822f1020:smss.exe                                 368      4      3     19 2012-07-22 02:42:31 UTC+0000
.. 0x82298700:winlogon.exe                            608    368     23    519 2012-07-22 02:42:32 UTC+0000
... 0x81e2ab28:services.exe                           652    608     16    243 2012-07-22 02:42:32 UTC+0000
.... 0x821dfda0:svchost.exe                          1056    652      5     60 2012-07-22 02:42:33 UTC+0000
.... 0x81eb17b8:spoolsv.exe                          1512    652     14    113 2012-07-22 02:42:36 UTC+0000
.... 0x81e29ab8:svchost.exe                           908    652      9    226 2012-07-22 02:42:33 UTC+0000
.... 0x823001d0:svchost.exe                          1004    652     64   1118 2012-07-22 02:42:33 UTC+0000
..... 0x8205bda0:wuauclt.exe                         1588   1004      5    132 2012-07-22 02:44:01 UTC+0000
..... 0x821fcda0:wuauclt.exe                         1136   1004      8    173 2012-07-22 02:43:46 UTC+0000
.... 0x82311360:svchost.exe                           824    652     20    194 2012-07-22 02:42:33 UTC+0000
.... 0x820e8da0:alg.exe                               788    652      7    104 2012-07-22 02:43:01 UTC+0000
.... 0x82295650:svchost.exe                          1220    652     15    197 2012-07-22 02:42:35 UTC+0000
... 0x81e2a3b8:lsass.exe                              664    608     24    330 2012-07-22 02:42:32 UTC+0000
.. 0x822a0598:csrss.exe                               584    368      9    326 2012-07-22 02:42:32 UTC+0000
 0x821dea70:explorer.exe                              1484   1464     17    415 2012-07-22 02:42:36 UTC+0000
. 0x81e7bda0:reader_sl.exe                            1640   1484      5     39 2012-07-22 02:42:36 UTC+0000
caine@Caine:/usr/share/caine/pacchetti/volatility$
```

Using pstree plugin we can find the suspicious processes. But nothing is exactly suspicious here. The only process which looks suspicious is explorer.exe and

reader_sl.exe because these both processes do not have any parent process ID which executes these processes from the system.

File: **explorer.exe**

It can be a suspicious process as its parent ID is 1464 which is not of svchost. It might be possible that the machine is remotely operated and tried to install malicious software.

File: **reader_sl.exe**

Its parent id is 1484 which is that of explorer.exe, if that is a suspicious process then this is also a suspicious process as it is child of that process.

2. Identify suspicious network connections from/to the victim machine, and determine which process(es) is(are) most likely responsible for the initial exploit, by refining the previous list of suspicious processes. [4%]

Answer:

To investigate further about suspicious connections we have to execute connections plugin

Python vol.py connections

```
caine@Caine:/usr/share/caine/pacchetti/volatility$ python vol.py connections
Volatility Foundation Volatility Framework 2.4
Offset(V)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0x81e87620 172.16.112.128:1038       41.168.5.140:8080         1484
caine@Caine:/usr/share/caine/pacchetti/volatility$
```

This shows one active remote connection that is using **8080 port and its PID is 1484** which is the **parent ID of explorer.exe and reader_sl.exe.** It means **explorer.exe and reader_sl.exe** are suspicious processes because explorer cannot open web browser.

To list recent network connections using the connscan plugin as follows:

Python vol.py connscan

```
caine@Caine:/usr/share/caine/pacchetti/volatility$ python vol.py connscan
Volatility Foundation Volatility Framework 2.4
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0x02087620 172.16.112.128:1038       41.168.5.140:8080         1484
0x023a8008 172.16.112.128:1037       125.19.103.198:8080       1484
```

This shows 2 connections established by the machine to remote IP address 41.168.5.140 and 125.19.103.198.

Both connections were made by a process with PID=1484. Since this process is connecting to port 8080.

Using connscan plugin again it is confirmed **that explorer.exe and reader_sl.exe are** most likely responsible for the initial exploit, by refining the previous list of suspicious processes.

Now, we have a service connecting to port 8080; which is abnormal. This means that there is a great chance that the process 1484 is malicious.

3. Identify the IP addresses and locations of the suspicious machines involved. [1%]

Answer: IP addresses are found using connscan and are: **41.168.5.140 and 125.19.103.198.**

Locations can be found using

https://www.iplocation.net/

here we can see that location is south africa and company name is Neotel Pty Ltd for 41.168.5.140.

Geolocation data from EurekAPI (Product: API, real-time)

IP Address	Country	Region	City
41.168.5.140	South Africa	Gauteng	Midrand
ISP	**Organization**	**Latitude**	**Longitude**
Neotel Pty Ltd	Neotel Pty Ltd	-25.9636	28.1378

The second IP address is 125.19.103.198 which is located either in New Delhi or Rajasthan in INDIA with the owner name Shriram general insurance company and internet service provider is Bharti Airtel.

Geolocation data from ipinfo.io (Product: API, real-time)

IP Address	Country	Region	City
125.19.103.198	India	National Capital Territory of Delhi	New Delhi
ISP	**Organization**	**Latitude**	**Longitude**
Bharti Airtel Ltd.	SHRIRAM GENERAL INSURANCE COMPANY LTD	28.6000	77.2000

To check if the IP address is blocked or not we can use www.ipvoid.com

www.ipvoid.com/ip-blacklist-check/

How Hacking Works: Raj Kapoor Instrumen Antivirus Software an Create installation me

IP Reputatic

Analysis Date	2017-06-12 01:04:59
Blacklist Status	BLACKLISTED 1/85
IP Address	41.168.5.140 (Find Websites)
Reverse DNS	Unknown
ASN	AS36937
ASN Owner	Neotel Pty Ltd
ISP	Neotel Pty Ltd
Continent	Africa
Country Code	(ZA) South Africa

And the website address is **support.tray-international.com**

IP ADDRESS: 41.168.5.140

We have found in our database of already analyzed websites that there **is only 1 website** hosted in the same web server with IP address **41.168.5.140**. Remember that it is not good to have too many websites located in the same web server because if a website gets infected by malware, it can easily affect the online reputation of the IP address and also of all the other websites.

Browse a list of websites hosted in **41.168.5.140** IP address:

#	Website
1	support.tray-international.com

The second IP address is also blacklisted which is 125.19.103.198. and the website address is **poluicenotgo.ru**

Analysis Date	2017-06-12 01:10:44
Blacklist Status	BLACKLISTED 2/85
IP Address	**125.19.103.198** (Find Websites)
Reverse DNS	Unknown
ASN	AS9498
ASN Owner	BHARTI Airtel Ltd.
ISP	Bharti Broadband
Continent	Asia
Country Code	(IN) India

IP ADDRESS: 125.19.103.198

We have found in our database of already analyzed websites that there **is only 1 website** hosted in the same web server with IP address **125.19.103.198**. Remember that it is not good to have too many websites located in the same web server because if a website gets infected by malware, it can easily affect the online reputation of the IP address and also of all the other websites.

Browse a list of websites hosted in **125.19.103.198** IP address:

#	Website
1	poluicenotgo.ru

4. **List the sockets involved, and identify suspicious ones by analyzing the timeline (i.e. created around incident timeline) [3%]**

   Answer:

   To find the sockets involved sockscan plugin is used: **python vol.py sockscan**

   By carefully analzing, we can say that process ID 908 is suspicious. Because it is created at the same time. As in the pstree and sockscan. And after that connection is established between the machine and internet.exe is executed.

```
caine@Caine:/usr/share/caine/pacchetti/volatility$ python vol.py sockscan
Volatility Foundation Volatility Framework 2.4
Offset(P)          PID   Port  Proto Protocol        Address         Create Time
---------- -------- ------ ------ ---------- ---------- ----------
0x01fd7618     1220   1900     17 UDP        172.16.112.128  2012-07-22 02:43:01 UTC+0000
0x01fdb780      664    500     17 UDP        0.0.0.0         2012-07-22 02:42:53 UTC+0000
0x0203f460        4    138     17 UDP        172.16.112.128  2012-07-22 02:42:38 UTC+0000
0x02076620     1004    123     17 UDP        127.0.0.1       2012-07-22 02:43:01 UTC+0000
0x020c23b0      908    135      6 TCP        0.0.0.0         2012-07-22 02:42:33 UTC+0000
0x02325610      788   1028      6 TCP        127.0.0.1       2012-07-22 02:43:01 UTC+0000
0x02372808      664      0    255 Reserved   0.0.0.0         2012-07-22 02:42:53 UTC+0000
0x02372c50      664   4500     17 UDP        0.0.0.0         2012-07-22 02:42:53 UTC+0000
0x0239cc08        4    445      6 TCP        0.0.0.0         2012-07-22 02:42:31 UTC+0000
0x023f0630     1004    123     17 UDP        172.16.112.128  2012-07-22 02:43:01 UTC+0000
0x023f0d00        4    445     17 UDP        0.0.0.0         2012-07-22 02:42:31 UTC+0000
0x02440d08     1484   1038      6 TCP        0.0.0.0         2012-07-22 02:44:45 UTC+0000
0x02476878        4    139      6 TCP        172.16.112.128  2012-07-22 02:42:38 UTC+0000
0x02477460        4    137     17 UDP        172.16.112.128  2012-07-22 02:42:38 UTC+0000
0x024cd2b0     1220   1900     17 UDP        127.0.0.1       2012-07-22 02:43:01 UTC+0000
caine@Caine:/usr/share/caine/pacchetti/volatility$
```

```
caine@Caine:/usr/share/caine/pacchetti/volatility$ python vol.py pstree
Volatility Foundation Volatility Framework 2.4
Name                                                 Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x823c89c8:System                                    4      0     53    240 1970-01-01 00:00:00 UTC+0000
. 0x822f1020:smss.exe                               368      4      3     19 2012-07-22 02:42:31 UTC+0000
.. 0x82298700:winlogon.exe                          608    368     23    519 2012-07-22 02:42:32 UTC+0000
... 0x81e2ab28:services.exe                         652    608     16    243 2012-07-22 02:42:32 UTC+0000
.... 0x821dfda0:svchost.exe                        1056    652      5     60 2012-07-22 02:42:33 UTC+0000
.... 0x81eb17b8:spoolsv.exe                        1512    652     14    113 2012-07-22 02:42:36 UTC+0000
.... 0x81e29ab8:svchost.exe                         908    652      9    226 2012-07-22 02:42:33 UTC+0000
.... 0x823001d0:svchost.exe                        1004    652     64   1118 2012-07-22 02:42:33 UTC+0000
..... 0x8205bda0:wuauclt.exe                       1588   1004      5    132 2012-07-22 02:44:01 UTC+0000
..... 0x821fcda0:wuauclt.exe                       1136   1004      8    173 2012-07-22 02:43:46 UTC+0000
.... 0x82311360:svchost.exe                         824    652     20    194 2012-07-22 02:42:33 UTC+0000
.... 0x820e8da0:alg.exe                             788    652      7    104 2012-07-22 02:43:01 UTC+0000
.... 0x82295650:svchost.exe                        1220    652     15    197 2012-07-22 02:42:35 UTC+0000
... 0x81e2a3b8:lsass.exe                            664    608     24    330 2012-07-22 02:42:32 UTC+0000
.. 0x822a0598:csrss.exe                             584    368      9    326 2012-07-22 02:42:32 UTC+0000
 0x821dea70:explorer.exe                           1484   1464     17    415 2012-07-22 02:42:36 UTC+0000
. 0x81e7bda0:reader_sl.exe                         1640   1484      5     39 2012-07-22 02:42:36 UTC+0000
caine@Caine:/usr/share/caine/pacchetti/volatility$
```

5. **Extract all executable (files) from the suspicious processes running on the victim's machine (as determined in question 2), and check whether some of these files are malicious using an online virus scanner. [1%]**

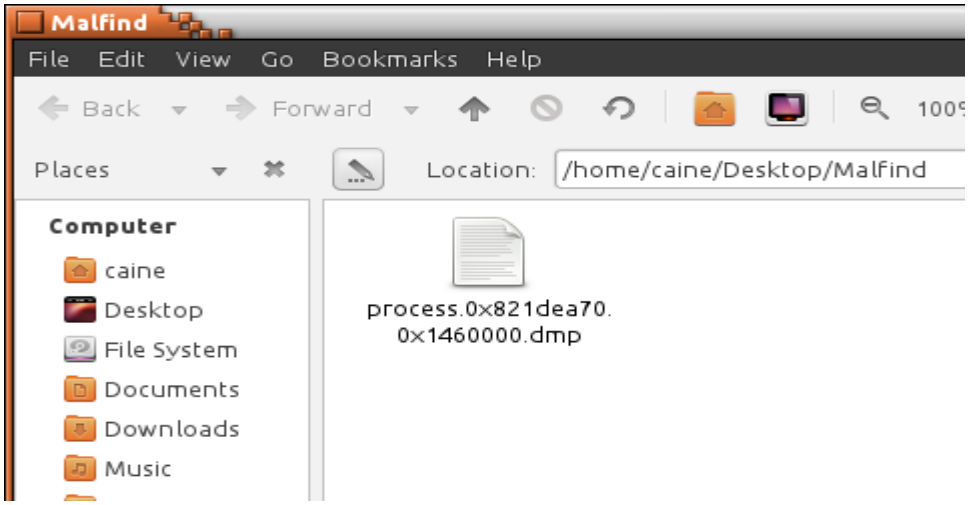
   Answer:

   To extract all suspicious processes from the files we have to use malfind plugin

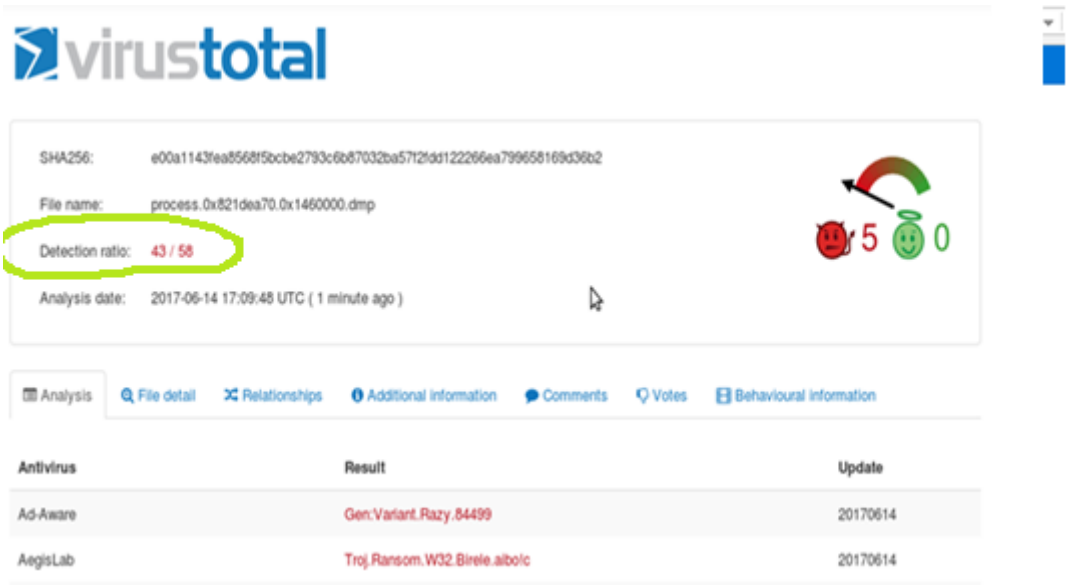
   python vol.py malfind -p 1484 --dump-dir /home/caine/Desktop/Malfind

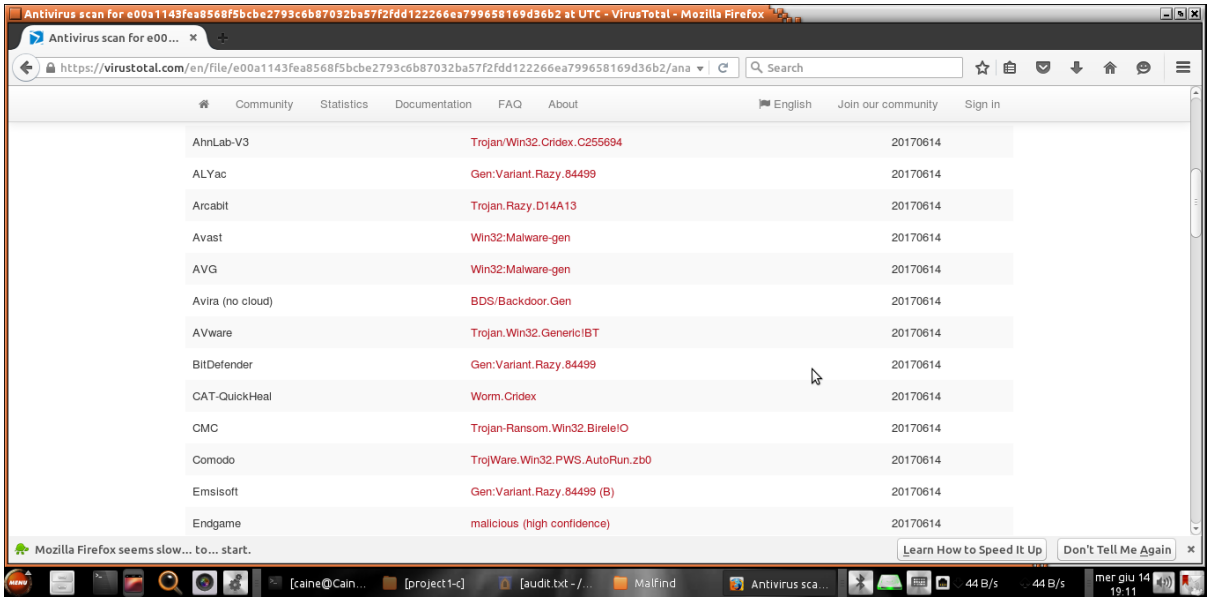
```
caine@Caine:/usr/share/caine/pacchetti/volatility$ python vol.py malfind -p 1484 --dump-dir /home/caine/Deskt
op/Malfind
Volatility Foundation Volatility Framework 2.4
Process: explorer.exe Pid: 1484 Address: 0x1460000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 33, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x01460000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00   MZ..............
0x01460010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ........@.......
0x01460020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x01460030  00 00 00 00 00 00 00 00 00 00 00 00 e0 00 00 00   ................

0x1460000 4d              DEC EBP
0x1460001 5a              POP EDX
0x1460002 90              NOP
0x1460003 0003            ADD [EBX], AL
0x1460005 0000            ADD [EAX], AL
0x1460007 000400          ADD [EAX+EAX], AL
0x146000a 0000            ADD [EAX], AL
0x146000c ff              DB 0xff
0x146000d ff00            INC DWORD [EAX]
```

The extracted file will be stored in the specified directory.

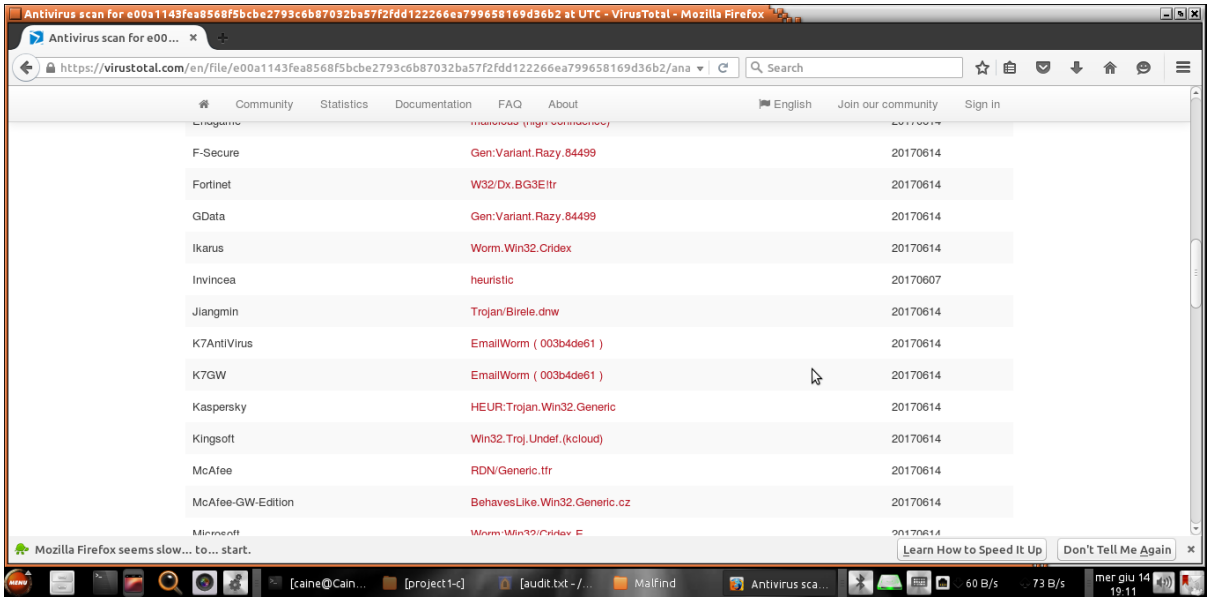


In this case, one file is generated. We can check this file by uploading on online virus scanner, e.g., virustotal.com

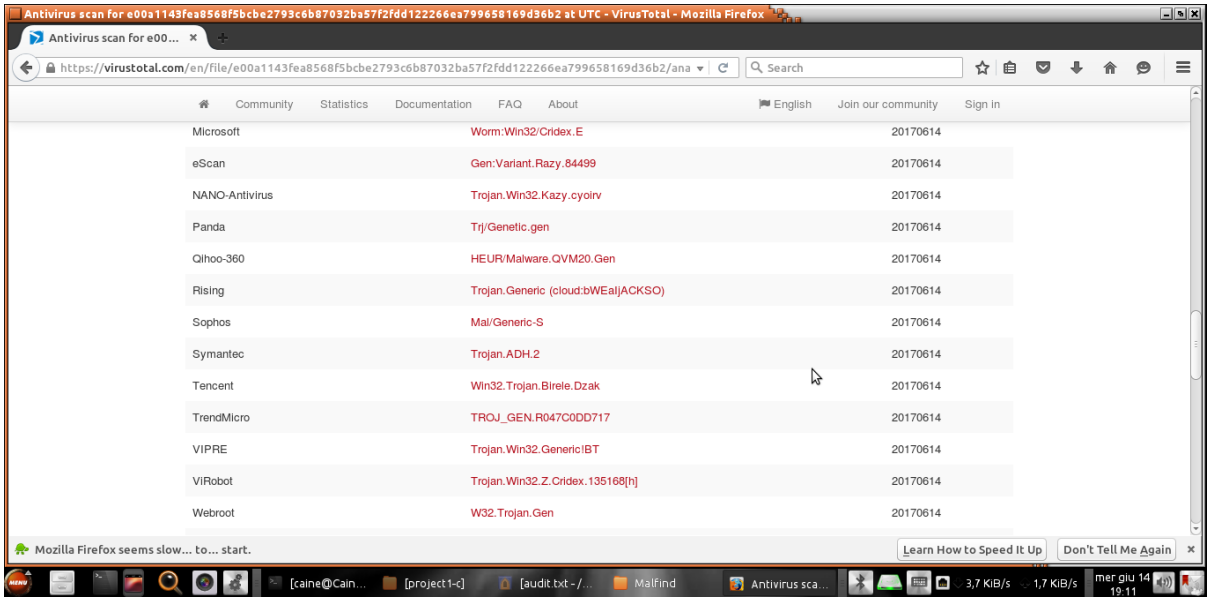




AhnLab-V3	Trojan/Win32.Cridex.C255694	20170614
ALYac	Gen:Variant.Razy.84499	20170614
Arcabit	Trojan.Razy.D14A13	20170614
Avast	Win32:Malware-gen	20170614
AVG	Win32:Malware-gen	20170614
Avira (no cloud)	BDS/Backdoor.Gen	20170614
AVware	Trojan.Win32.Generic!BT	20170614
BitDefender	Gen:Variant.Razy.84499	20170614
CAT-QuickHeal	Worm.Cridex	20170614
CMC	Trojan-Ransom.Win32.Birele!O	20170614
Comodo	TrojWare.Win32.PWS.AutoRun.zb0	20170614
Emsisoft	Gen:Variant.Razy.84499 (B)	20170614
Endgame	malicious (high confidence)	20170614



F-Secure	Gen:Variant.Razy.84499	20170614
Fortinet	W32/Dx.BG3E!tr	20170614
GData	Gen:Variant.Razy.84499	20170614
Ikarus	Worm.Win32.Cridex	20170614
Invincea	heuristic	20170607
Jiangmin	Trojan/Birele.dnw	20170614
K7AntiVirus	EmailWorm (003b4de61)	20170614
K7GW	EmailWorm (003b4de61)	20170614
Kaspersky	HEUR:Trojan.Win32.Generic	20170614
Kingsoft	Win32.Troj.Undef.(kcloud)	20170614
McAfee	RDN/Generic.tfr	20170614
McAfee-GW-Edition	BehavesLike.Win32.Generic.cz	20170614



Microsoft	Worm:Win32/Cridex.E	20170614
eScan	Gen:Variant.Razy.84499	20170614
NANO-Antivirus	Trojan.Win32.Kazy.cyoirv	20170614
Panda	Trj/Genetic.gen	20170614
Qihoo-360	HEUR/Malware.QVM20.Gen	20170614
Rising	Trojan.Generic (cloud:bWEaIjACKSO)	20170614
Sophos	Mal/Generic-S	20170614
Symantec	Trojan.ADH.2	20170614
Tencent	Win32.Trojan.Birele.Dzak	20170614
TrendMicro	TROJ_GEN.R047C0DD717	20170614
VIPRE	Trojan.Win32.Generic!BT	20170614
ViRobot	Trojan.Win32.Z.Cridex.135168[h]	20170614
Webroot	W32.Trojan.Gen	20170614

The results indicate that 43/58 scanners have classified this file as malware.

6. **Identify the URL for one of the financial institutions that may be in the suspected process(es) memory space. [1%]**

   Answer:

   strings /home/caine/desktop/1484.dmp | grep “http://”

```
caine@Caine:/usr/share/caine/pacchetti/volatility$ strings /home/caine/Desktop/1484.dmp | grep "http://"
$http://www.trustcenter.de/guidelines0
'http://www.certplus.com/CRL/class3P.crl0
$http://crl.verisign.com/pca1.1.1.crl0G
http://www.usertrust.com1
http://www.usertrust.com1
3http://crl.usertrust.com/UTN-USERFirst-Hardware.crl01
http://www.valicert.com/1 0
http://www.valicert.com/1 0
(http://www.certplus.com/CRL/class3TS.crl0
*http://ca.sia.it/seccli/repository/CRL.der0J
http://www.usertrust.com1
http://www.usertrust.com1
,http://crl.usertrust.com/UTN-DATACorpSGC.crl0*
http://www.usertrust.com1+0)
http://www.usertrust.com1+0)
>http://crl.usertrust.com/UTN-USERFirst-NetworkApplications.crl0
*http://ca.sia.it/secsrv/repository/CRL.der0J
$http://crl.verisign.com/pca2.1.1.crl0G
http://www.valicert.com/1 0
http://www.valicert.com/1 0
&http://www.certplus.com/CRL/class1.crl0
$http://www.trustcenter.de/guidelines0
&http://www.certplus.com/CRL/class2.crl0
$http://www.trustcenter.de/guidelines0
```

```
3http://crl.usertrust.com/UTN-USERFirst-Hardware.crl01
http://188.40.0.138:8080/zb/v_01_a/in/cp.php
<!-- BEGIN Global Navigation table --><table cellspacing="0" cellpadding="0" border="0" class="fullwi
dth" summary="global navigation"><tr><td><a href="http://www.chase.com/" id="siteLogo"><img src="http
s://chaseonline.chase.com/images//ChaseNew.gif" alt="Chase Online Logo" style="margin: 17px 17px 17px
 17px;"/></a></td><td class="globalnav"><a id="homelink" href="JavaScript:document.location.href='htt
p://www.chase.com/';" class="globalnavlinks">Chase.com</a>  </td>
<!--Footer--><table border="0" cellspacing="0" cellpadding="0" class="fullwidth" summary="terms of us
e link and copyright"><tr><td class="spacerh10" colspan="3"> </td></tr><tr><td style="width:30%; vert
ical-align:top"> </td><td align="center" width="40%" valign="top"><span class="footertext"><a id="Sec
urityLink" href="JavaScript:document.location.href='http://www.chase.com//ccp/index.jsp?pg_name=ccpma
pp/shared/assets/page/security_measures';" onBlur="window.status='';return true" onMouseOver="window.
status='';return true" onFocus="window.status='';return true" onMouseOut="window.status='';return tru
e">Security</a> | <!-- mp_trans_remove_start --><a id="TermsLink" href="JavaScript:document.location.
href='http://www.chase.com//ccp/index.jsp?pg_name=ccpmapp/shared/assets/page/terms';" onBlur="window.
status='';return true" onMouseOver="window.status='';return true" onFocus="window.status='';return t
ue" onMouseOut="window.status='';return true">Terms of Use</a> <!-- mp_trans_remove_end --><!-- mp_t
ans_add<a id="TermsLink" href="JavaScript:document.location.href='https://www.chase.com/index.jsp?pg
name=ccpmapp/spanish/resources/page/terms';" onBlur="window.status='';return true" onMouseOver="windo
w.status='';return true" onFocus="window.status='';return true" onMouseOut="window.status='';return t
rue">Terms of Use</a> --></span></td><td style="text-align:center; width:30%; vertical-align:top"> </
td></tr></table><div class="printable"><table border="0" cellspacing="0" cellpadding="0" class="fullw
idth"><tr><td class="spacerh10"> </td></tr><tr><td align="center" class="footertext">
http://*:2869/
http://www.microsoft.com/provisioning/Master
http://www.microsoft.com/provisioning/Register
http://www.microsoft.com/provisioning/SSID
http://www.microsoft.com/provisioning/BaseEapUserPropertiesV1
http://www.microsoft.com/provisioning/EapUserPropertiesV1
http://www.microsoft.com/provisioning/MsChapV2UserPropertiesV1
```

We can see here that www.chase.com is the financial institution involved after doing google all the URL's shown above.

7. Identify at least one related IP address and corresponding location (in addition to the ones found earlier) that may be in the suspected process(es) memory space. [1%]

Answer:

The associated URL with this suspected process memory space is: 188.40.0.38 and location is **GERMANY**

```
http://www.usertrust.com1
http://www.usertrust.com1
,http://crl.usertrust.com/UTN-DATACorpSGC.crl0*
*http://ca.sia.it/seccli/repository/CRL.der0J
'http://www.certplus.com/CRL/class3P.crl0
http://www.usertrust.com1
http://www.usertrust.com1
3http://crl.usertrust.com/UTN-USERFirst-Hardware.crl01
http://188.40.0.138:8080/zb/v_01_a/in/cp.php
```

Upon further investigation it is seen that this URL is safe but this suspicious process has been attached to it

www.ipvoid.com/ip-blacklist-check/

IP Reputation Feeds»

Analysis Date	2017-06-14 13:58:04
Blacklist Status	POSSIBLY SAFE 0/85
IP Address	188.40.0.138 (Find Websites)
Reverse DNS	restorewww1.flk1.host-h.net
ASN	AS24940
ASN Owner	Hetzner Online GmbH
ISP	Hetzner Online GmbH
Continent	Europe
Country Code	(DE) Germany
Latitude / Longitude	51.2993 / 9.491

Following are the websites hosted using this IP address

Browse a list of websites hosted in **188.40.0.138** IP address:

#	Website
1	✔ campsbayaccommodation.info
2	✔ aubergealouette.com
3	✔ africantouchtours.com
4	✔ wind-rose.co.za
5	✔ capescape.co.za

Further the locations can be found at www.iplocation.net

Organization name is hetzner online GmbH

Geolocation data from ipinfo.io (Product: API, real-time)

IP Address	Country	Region	City
188.40.0.38	Germany	Not Available	Not Available
ISP	**Organization**	**Latitude**	**Longitude**
Hetzner Online GmbH	hetzner Africa	51.2993	9.4910