PV204 Security Technologies

6th assignment – Part1 – Memory analysis

Supervisor: Dr. Václav Lorenc

Student: Pedro Gomes, 490830

User and Malware story

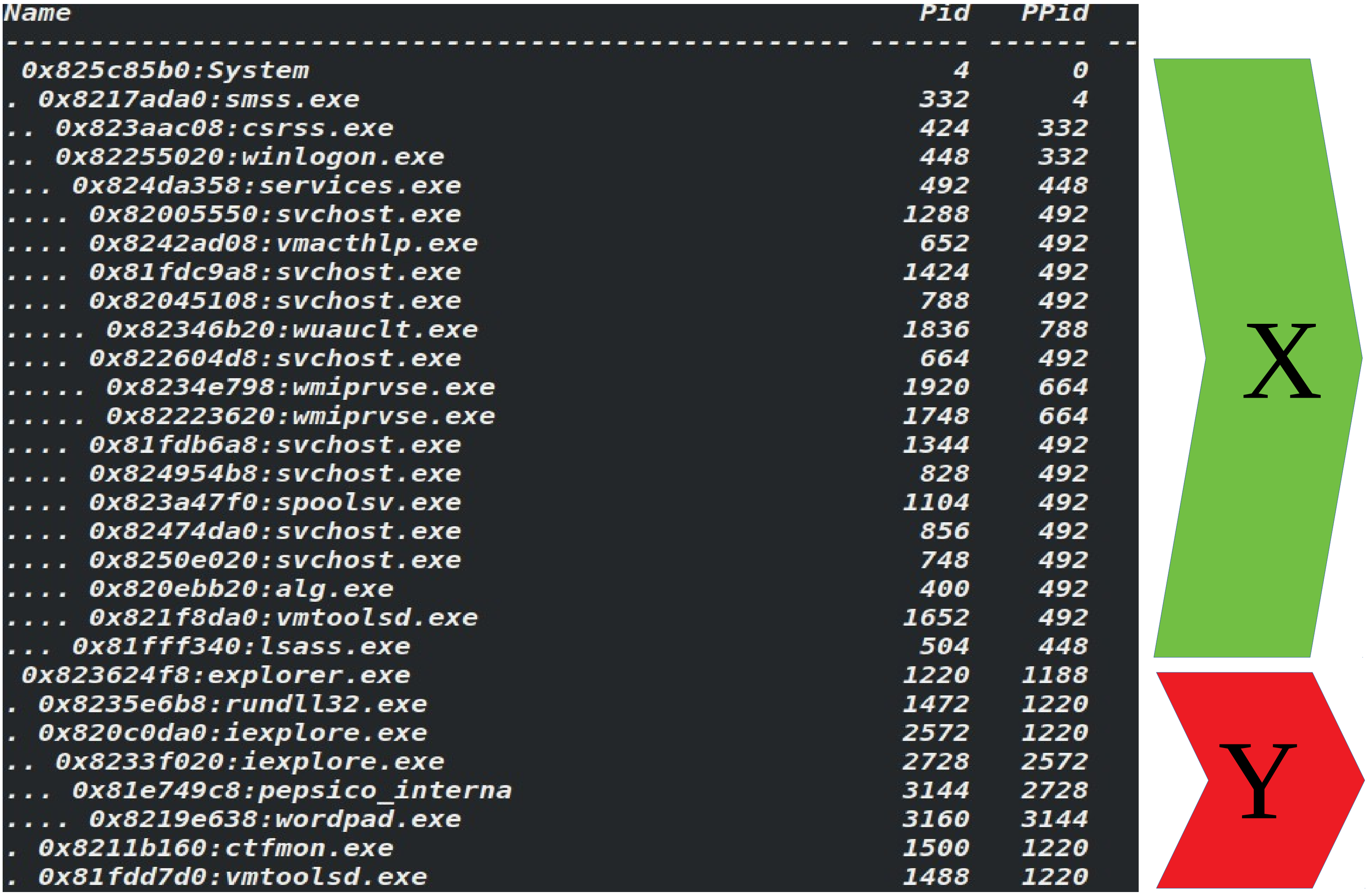
The first thing I did was to detect the type of the image that I had with the following command:

volatility -f homework-2019.vmem imageinfo

The output clearly showed it was an image of a windowsXP machine. After that I decided to see the processes that were launched, ordered in a tree, for that I issued the following command:

volatility -f homework-2019.vmem --profile WinXPSP2x86 pstree

which gave the following output:



```
Name                                                  Pid   PPid
-------------------------------------------------- ------ ------ --
 0x825c85b0:System                                      4      0
. 0x8217ada0:smss.exe                                 332      4
.. 0x823aac08:csrss.exe                               424    332
.. 0x82255020:winlogon.exe                            448    332
... 0x824da358:services.exe                           492    448
.... 0x82005550:svchost.exe                          1288    492
.... 0x8242ad08:vmacthlp.exe                          652    492
.... 0x81fdc9a8:svchost.exe                          1424    492
.... 0x82045108:svchost.exe                           788    492
..... 0x82346b20:wuauclt.exe                         1836    788
.... 0x822604d8:svchost.exe                           664    492
..... 0x8234e798:wmiprvse.exe                        1920    664
..... 0x82223620:wmiprvse.exe                        1748    664
.... 0x81fdb6a8:svchost.exe                          1344    492
.... 0x824954b8:svchost.exe                           828    492
.... 0x823a47f0:spoolsv.exe                          1104    492
.... 0x82474da0:svchost.exe                           856    492
.... 0x8250e020:svchost.exe                           748    492
.... 0x820ebb20:alg.exe                               400    492
.... 0x821f8da0:vmtoolsd.exe                         1652    492
... 0x81fff340:lsass.exe                              504    448
 0x823624f8:explorer.exe                             1220   1188
. 0x8235e6b8:rundll32.exe                            1472   1220
. 0x820c0da0:iexplore.exe                            2572   1220
.. 0x8233f020:iexplore.exe                           2728   2572
... 0x81e749c8:pepsico_interna                       3144   2728
.... 0x8219e638:wordpad.exe                          3160   3144
. 0x8211b160:ctfmon.exe                              1500   1220
. 0x81fdd7d0:vmtoolsd.exe                            1488   1220
```

If we see the processes near X, I believe that the operating system is booting up. The process *smss.exe* is the first user-mode process started by the kernel[1] . I was a little bit suspicious about the fact that there are so many svchost.exe instances, but apparently it is not unusual[2]

At the beginning of Y, the explorer.exe is launched, which is the process responsible for several things, including the windows interface, which is one of the few things being launched at the boot.

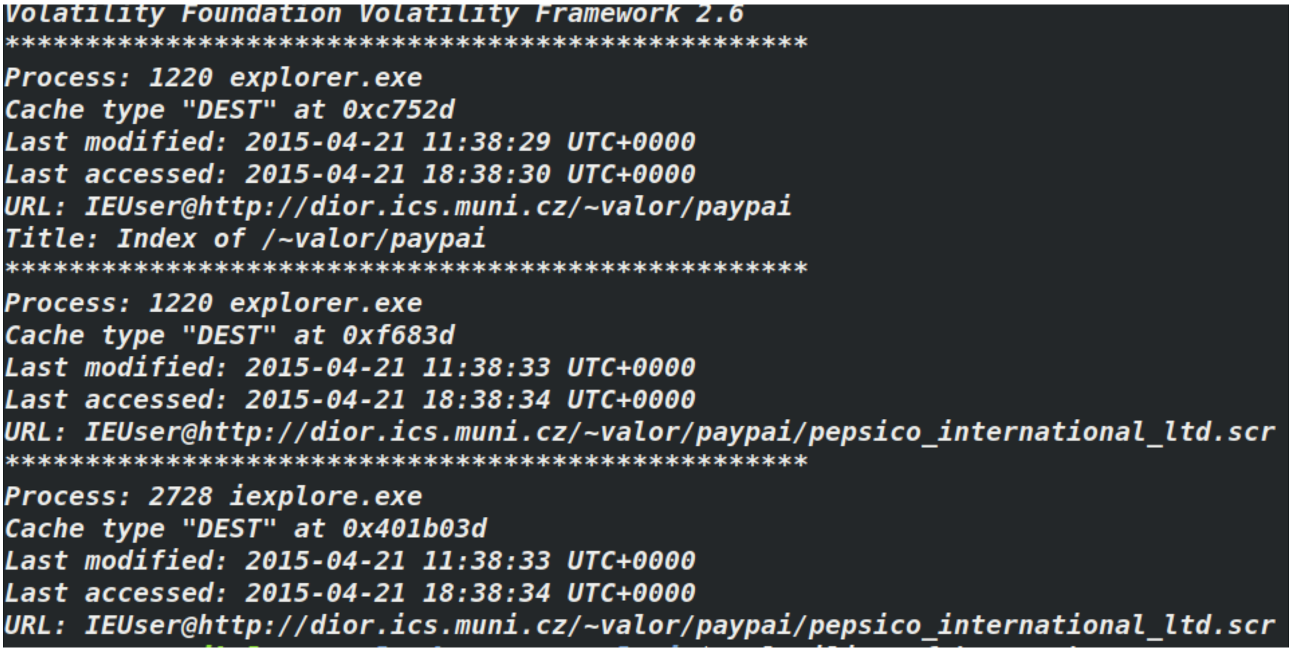
It seems to me that the user did not interact yet with his machine(since the boot), because the process rundll32.exe is automatically launched right after the explorer, without having some program that triggers it. After some investigation[3] I concluded that rundll32.exe is a malicious process that allows remote access to some system, it can maybe be categorized as a RAT.

In order to install rundll32.exe some other program must have triggered it, and we cannot see it, because as it was already mentioned, the process that launches it is a reliable windows process explorer.exe. Perhaps, this means that rundll32.exe has already **gained persistence** somehow and it is being normally launched at startup.

Rundll32.exe launches internet explorer, and that internet explorer instance launches another one, for some reason that I cannot understand. We can also see that the 2nd internet explorer instance(PID: 2728) accesses some resource named: **“pepsico interna”** . This leaded me to check the IE history, using the following command:

volatility -f homework-2019.vmem --profile WinXPSP2x86 iehistory

The above command yielded the following output:



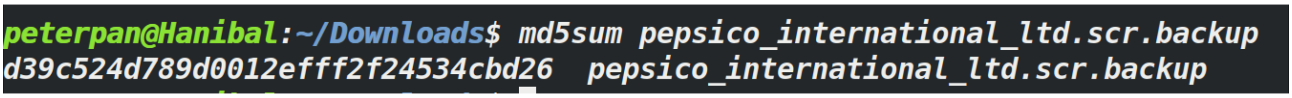
```
Volatility Foundation Volatility Framework 2.6
**************************************************
Process: 1220 explorer.exe
Cache type "DEST" at 0xc752d
Last modified: 2015-04-21 11:38:29 UTC+0000
Last accessed: 2015-04-21 18:38:30 UTC+0000
URL: IEUser@http://dior.ics.muni.cz/~valor/paypai
Title: Index of /~valor/paypai
**************************************************
Process: 1220 explorer.exe
Cache type "DEST" at 0xf683d
Last modified: 2015-04-21 11:38:33 UTC+0000
Last accessed: 2015-04-21 18:38:34 UTC+0000
URL: IEUser@http://dior.ics.muni.cz/~valor/paypai/pepsico_international_ltd.scr
**************************************************
Process: 2728 iexplore.exe
Cache type "DEST" at 0x401b03d
Last modified: 2015-04-21 11:38:33 UTC+0000
Last accessed: 2015-04-21 18:38:34 UTC+0000
URL: IEUser@http://dior.ics.muni.cz/~valor/paypai/pepsico_international_ltd.scr
```

Illustration 1: Internet Explorer history of the image

We can clearly see that both internet explorer instances access some resource that has a file of the src format. Usually, src format stands for any kind of code. It could be C, C++, java, etc.

After accessing the link in a none windows operating system, I was surprised to see a message from the “hacker” Dr.Vaclav

As instructed, the MD5 of the malware: d39c524d789d0012efff2f24534cbd26 , I confirmed it with:



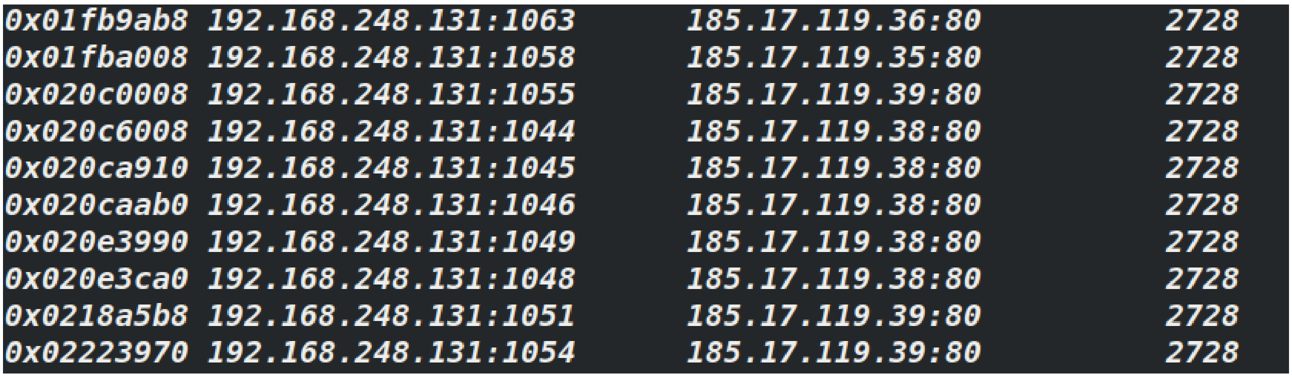
```
peterpan@Hanibal:~/Downloads$ md5sum pepsico_international_ltd.scr.backup
d39c524d789d0012efff2f24534cbd26  pepsico_international_ltd.scr.backup
```

Illustration 2: MD5 confirmation of malware

It is also worth mentioning that the PID: 2728, which is the 2nd internet explorer instance was also heavily interacting with some IP within Czech Republic(Prague) , I inspected the connections of the OS with the following command:

volatility -f homework-2019.vmem --profile WinXPSP2x86 connscan

Which yielded:
…



```
0x01fb9ab8 192.168.248.131:1063      185.17.119.36:80           2728
0x01fba008 192.168.248.131:1058      185.17.119.35:80           2728
0x020c0008 192.168.248.131:1055      185.17.119.39:80           2728
0x020c6008 192.168.248.131:1044      185.17.119.38:80           2728
0x020ca910 192.168.248.131:1045      185.17.119.38:80           2728
0x020caab0 192.168.248.131:1046      185.17.119.38:80           2728
0x020e3990 192.168.248.131:1049      185.17.119.38:80           2728
0x020e3ca0 192.168.248.131:1048      185.17.119.38:80           2728
0x0218a5b8 192.168.248.131:1051      185.17.119.39:80           2728
0x02223970 192.168.248.131:1054      185.17.119.39:80           2728
```

…

I tried to ping the domain and access it in port 80, but both were unsuccessful.

To sum up I would say that the user previously installed some program that contained the rundll32.exe file. The vulnerability that the latter provides allowed some attacked to download a src file, that was opened with wordpad. Fortunately, the file only had a nice message from Dr.Vaclav

References

[1]: https://en.wikipedia.org/wiki/Session_Manager_Subsystem, explanation about smss
[2]: Bleepin' Gumshoe, https://www.bleepingcomputer.com/forums/t/125879/is-having-multiple-svchostexe-normal/, what is svchost.exe and what it does
[3]:https://www.processlibrary.com/en/directory/files/rundll32/25747/ , explanation of what rundll32.exe is.