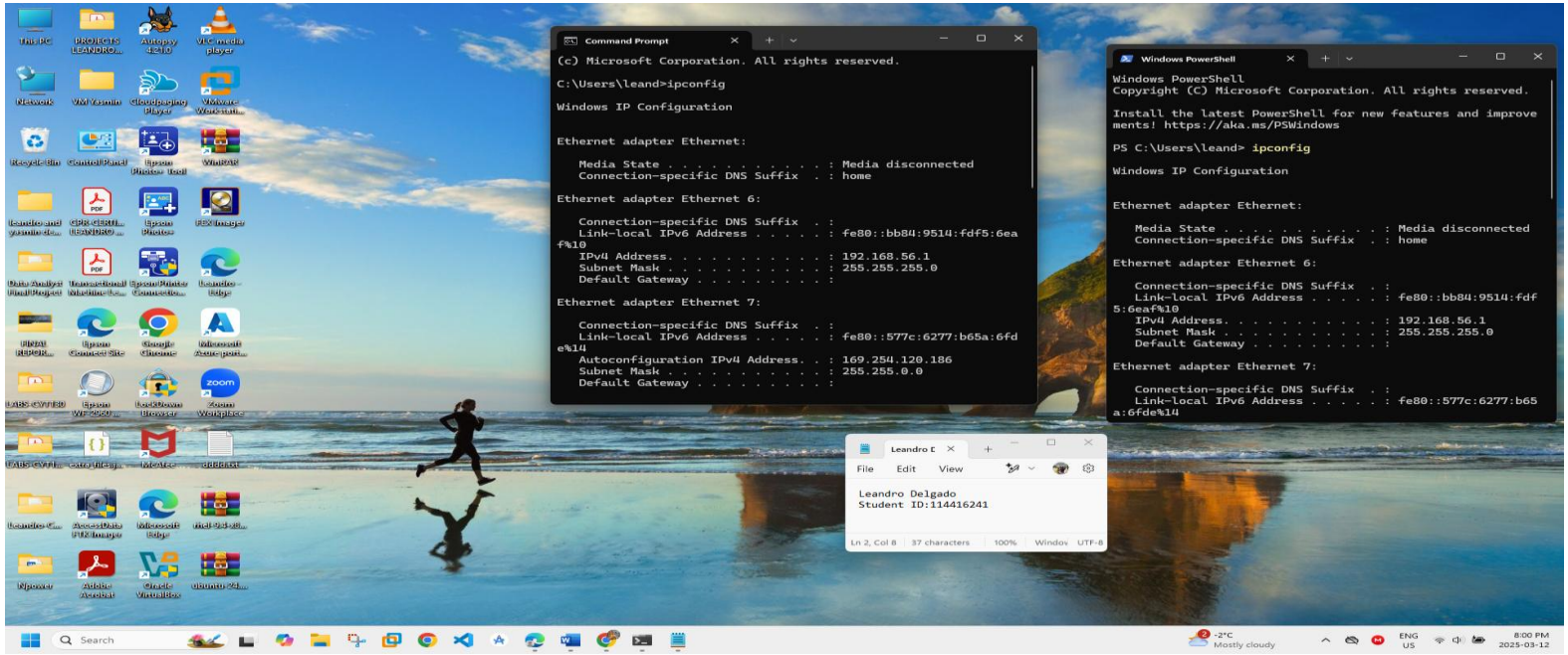
Put Student Name(s) ↓	Put Student IDs ↓	Due Date	Grade Weight
Leandro Delgado	114416241	As Posted	6%

Name	Lab8: RedLine Endpoint Forensics Challenge
Instructions	• It is an Individual assignment. Put your name + Student ID in the empty spaces above. • Show your genuine signs of your work is done on your machine. This includes: ○ Screenshots that show your desktop background with Date/Time. ○ Show a pop-up bx that shows "your name + IP". ○ Show your logged account when applicable. Optional: Your photo. • Submit your report name: CYT215-Lab8-Student Name & ID
Challenge Scenario	As a member of the Security Blue team: Your assignment is to analyze a memory dump using Redline and Volatility tools. Your goal is to trace the steps taken by the attacker on the compromised machine and determine how they managed to bypass the Network Intrusion Detection System "NIDS". Your investigation will involve identifying the specific malware family employed in the attack, along with its characteristics. Additionally, your task is to identify and mitigate any traces or footprints left by the attacker.
Challenge Questions To be Answered	 *Figure 1. 0 Screen*

1. What is the name of the suspicious process?

```
┌──(venv)─(kali㉿kali)-[~/volatility3]
└─$ python3 vol.py -f ~/Desktop/MemoryDump.mem windows.malfind.Malfind

Volatility 3 Framework 2.23.0
Progress:  100.00               PDB scanning finished
PID     Process Start VPN       End VPN Tag     Protection      CommitCharge    PrivateMemory   File output     Notes   Hexdump Disasm
WARNING  volatility3.plugins.windows.malfind: [proc_id 5704] Found suspicious DIRTY + PAGE_EXECUTE_READ page at 0x21ddbca0000

5704    RuntimeBroker.  0x21ddbca0000   0x21ddbcaffff   VadS    PAGE_EXECUTE_READ       16      1       Disabled        N/A
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0x21ddbca0000:  add     byte ptr [rax], al
0x21ddbca0002:  add     byte ptr [rax], al
0x21ddbca0004:  add     byte ptr [rax], al
0x21ddbca0006:  add     byte ptr [rax], al
0x21ddbca0008:  add     byte ptr [rax], al
0x21ddbca000a:  add     byte ptr [rax], al
0x21ddbca000c:  add     byte ptr [rax], al
0x21ddbca000e:  add     byte ptr [rax], al
0x21ddbca0010:  add     byte ptr [rax], al
0x21ddbca0012:  add     byte ptr [rax], al
0x21ddbca0014:  add     byte ptr [rax], al
0x21ddbca0016:  add     byte ptr [rax], al
0x21ddbca0018:  add     byte ptr [rax], al
0x21ddbca001a:  add     byte ptr [rax], al
0x21ddbca001c:  add     byte ptr [rax], al
0x21ddbca001e:  add     byte ptr [rax], al
0x21ddbca0020:  add     byte ptr [rax], al
0x21ddbca0022:  add     byte ptr [rax], al
0x21ddbca0024:  add     byte ptr [rax], al
0x21ddbca0026:  add     byte ptr [rax], al
0x21ddbca0028:  add     byte ptr [rax], al
0x21ddbca002a:  add     byte ptr [rax], al
0x21ddbca002c:  add     byte ptr [rax], al
0x21ddbca002e:  add     byte ptr [rax], al
0x21ddbca0030:  add     byte ptr [rax], al
0x21ddbca0032:  add     byte ptr [rax], al
0x21ddbca0034:  add     byte ptr [rax], al
0x21ddbca0036:  add     byte ptr [rax], al
0x21ddbca0038:  add     byte ptr [rax], al
0x21ddbca003a:  add     byte ptr [rax], al
0x21ddbca003c:  add     byte ptr [rax], al
0x21ddbca003e:  add     byte ptr [rax], al
5896    oneetx.exe      0x400000        0x437fff        VadS    PAGE_EXECUTE_READWRITE  56      1       Disabled        MZ header
4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ..............
b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ........@.......
```

```
Leandro Delgado
Student number:114416241
```

Figure 2. Names of suspicious Process

2. What is the child process name of the suspicious process?

```
b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ........@.......
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 ................
0x400000:       dec     ebp
0x400001:       pop     edx
0x400002:       nop
0x400003:       add     byte ptr [ebx], al
0x400005:       add     byte ptr [eax], al
0x400007:       add     byte ptr [eax + eax], al
0x40000a:       add     byte ptr [eax], al
7540    smartscreen.ex  0x2505c140000   0x2505c15ffff   VadS    PAGE_EXECUTE_READWRITE  1       1       Disabled        N/A
48 89 54 24 10 48 89 4c 24 08 4c 89 44 24 18 4c H.T$.H.L$.L.D$.L
89 4c 24 20 48 8b 41 28 48 8b 48 08 48 8b 51 50 .L$ H.A(H.H.H.QP
48 83 e2 f8 48 8b ca 48 b8 60 00 14 5c 50 02 00 H...H..H.`..\P..
00 48 2b c8 48 81 f9 70 0f 00 00 76 09 48 c7 c1 .H+.H..p...v.H..
0x2505c140000:  mov     qword ptr [rsp + 0x10], rdx
0x2505c140005:  mov     qword ptr [rsp + 8], rcx
0x2505c14000a:  mov     qword ptr [rsp + 0x18], r8
0x2505c14000f:  mov     qword ptr [rsp + 0x20], r9
0x2505c140014:  mov     rax, qword ptr [rcx + 0x28]
0x2505c140018:  mov     rcx, qword ptr [rax + 8]
0x2505c14001c:  mov     rdx, qword ptr [rcx + 0x50]
0x2505c140020:  and     rdx, 0xfffffffffffffff8
0x2505c140024:  mov     rcx, rdx
0x2505c140027:  movabs  rax, 0x2505c140060
0x2505c140031:  sub     rcx, rax
0x2505c140034:  cmp     rcx, 0xf70
0x2505c14003b:  jbe     0x2505c140046

┌──(venv)─(kali㉿kali)-[~/volatility3]
└─$ vol.py -f MemoryDump.mem windows.pslist | grep -E "5704|5896"
vol.py: command not found

┌──(venv)─(kali㉿kali)-[~/volatility3]
└─$ vol.py -f MemoryDump.mem windows.pslist | grep -E "5896|7540"
vol.py: command not found

┌──(venv)─(kali㉿kali)-[~/volatility3]
└─$ python3 vol.py -f ~/Desktop/MemoryDump.mem windows.pslist.PsList | grep -E "5896"

5896    8844    oneetx.exe      0xad8189b41080  5       -       1       True    2023-05-21 22:30:56.000000 UTC  N/A     Disabled
7732    5896    rundll32.exe    0xad818d1912c0  1       -       1       True    2023-05-21 22:31:53.000000 UTC  N/A     Disabled

┌──(venv)─(kali㉿kali)-[~/volatility3]
└─$ python3 vol.py -f ~/Desktop/MemoryDump.mem windows.pstree.PsTree | grep -E "5896"

5896    8844    oneetx.exe      0xad8189b41080  5       -       1       True    2023-05-21 22:30:56.000000 UTC  N/A     \Device\HarddiskVolume3\Users\Tammam\AppData\Local\Temp\c3912af058\oneetx.e
xe      -       -
* 7732  5896    rundll32.exe    0xad818d1912c0  1       -       1       True    2023-05-21 22:31:53.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\SysWOW64\rundll32.exe   -       -
```

```
Leandro Delgado
Student number:114416241
```

Figure 3 Child process name of the suspicious process

3. What is the memory protection applied to the suspicious process memory region?

```
┌──(venv)─(kali㉿kali)-[~/volatility3]
└─$ python3 vol.py -f ~/Desktop/MemoryDump.mem windows.malfind.Malfind

Volatility 3 Framework 2.23.0
Progress:  100.00               PDB scanning finished
PID     Process Start VPN       End VPN Tag     Protection      CommitCharge    PrivateMemory   File output     Notes   Hexdump Disasm
WARNING  volatility3.plugins.windows.malfind: [proc_id 5704] Found suspicious DIRTY + PAGE_EXECUTE_READ page at 0x21ddbca0000

5704    RuntimeBroker.  0x21ddbca0000   0x21ddbcaffff   VadS    PAGE_EXECUTE_READ       16      1       Disabled        N/A
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0x21ddbca0000:  add     byte ptr [rax], al
0x21ddbca0002:  add     byte ptr [rax], al
0x21ddbca0004:  add     byte ptr [rax], al
0x21ddbca0006:  add     byte ptr [rax], al
0x21ddbca0008:  add     byte ptr [rax], al
0x21ddbca000a:  add     byte ptr [rax], al
0x21ddbca000c:  add     byte ptr [rax], al
0x21ddbca000e:  add     byte ptr [rax], al
0x21ddbca0010:  add     byte ptr [rax], al
0x21ddbca0012:  add     byte ptr [rax], al
0x21ddbca0014:  add     byte ptr [rax], al
0x21ddbca0016:  add     byte ptr [rax], al
0x21ddbca0018:  add     byte ptr [rax], al
0x21ddbca001a:  add     byte ptr [rax], al
0x21ddbca001c:  add     byte ptr [rax], al
0x21ddbca001e:  add     byte ptr [rax], al
0x21ddbca0020:  add     byte ptr [rax], al
0x21ddbca0022:  add     byte ptr [rax], al
0x21ddbca0024:  add     byte ptr [rax], al
0x21ddbca0026:  add     byte ptr [rax], al
0x21ddbca0028:  add     byte ptr [rax], al
0x21ddbca002a:  add     byte ptr [rax], al
0x21ddbca002c:  add     byte ptr [rax], al
0x21ddbca002e:  add     byte ptr [rax], al
0x21ddbca0030:  add     byte ptr [rax], al
0x21ddbca0032:  add     byte ptr [rax], al
0x21ddbca0034:  add     byte ptr [rax], al
0x21ddbca0036:  add     byte ptr [rax], al
0x21ddbca0038:  add     byte ptr [rax], al
0x21ddbca003a:  add     byte ptr [rax], al
0x21ddbca003c:  add     byte ptr [rax], al
0x21ddbca003e:  add     byte ptr [rax], al
5896    oneetx.exe      0x400000        0x437fff        VadS    PAGE_EXECUTE_READWRITE  56      1       Disabled        MZ header
4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ..............
b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ........@.......
```

Leandro Delgado
Student number:114416241

Figure 4 Memory protection applied to the suspicious process memory region

4. What is the name of the process responsible for the VPN connection?

```
(venv)-(kali@kali)-[~/volatility3]
$ python3 vol.py -f ~/Desktop/MemoryDump.mem windows.pstree.PsTree

Volatility 3 Framework 2.23.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        Audit   Cmd     Path

4       0       System  0xad8185883180  157     -       N/A     False   2023-05-21 22:27:10.000000 UTC  N/A     -       -       -
* 1280  4       MemCompression  0xad8187835080  62      -       N/A     False   2023-05-21 22:27:49.000000 UTC  N/A     MemCompression  -       -
* 108   4       Registry        0xad81858f2080  4       -       N/A     False   2023-05-21 22:26:54.000000 UTC  N/A     Registry        -       -
* 332   4       smss.exe        0xad81860dc040  2       -       N/A     False   2023-05-21 22:27:10.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\smss.exe       -       -
452     444     csrss.exe       0xad81861cd080  12      -       0       False   2023-05-21 22:27:22.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\csrss.exe      -       -
528     520     csrss.exe       0xad8186f1b140  14      -       1       False   2023-05-21 22:27:25.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\csrss.exe
552     444     wininit.exe     0xad8186f2b080  1       -       0       False   2023-05-21 22:27:25.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\wininit.exe    -       -
* 696   552     lsass.exe       0xad8186fc6080  10      -       0       False   2023-05-21 22:27:29.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\lsass.exe      C:\Windows\system32
\lsass.exe      C:\Windows\system32\lsass.exe
* 676   552     services.exe    0xad8186f4d080  7       -       0       False   2023-05-21 22:27:29.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\services.exe   C:\Windows\system32
\services.exe   C:\Windows\system32\services.exe
** 4228 676     SearchIndexer.  0xad818ce06240  15      -       0       False   2023-05-21 22:31:27.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\SearchIndexer.exe      C:\Windows\
system32\SearchIndexer.exe /Embedding   C:\Windows\system32\SearchIndexer.exe
** 8708 676     svchost.exe     0xad818d431080  5       -       0       False   2023-05-21 22:57:33.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\svchost.exe    -       -
** 5136 676     SecurityHealth  0xad818d374280  7       -       0       False   2023-05-21 22:32:01.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\SecurityHealthService.exe      - -
** 2200 676     VGAuthService.  0xad81896b3300  2       -       0       False   2023-05-21 22:28:19.000000 UTC  N/A     \Device\HarddiskVolume3\Pro[illegible]\VGAuth\VGA
uthService.exe  -       -
** 3608 676     svchost.exe     0xad818d07a080  3       -       0       False   2023-05-21 22:41:28.000000 UTC  N/A     \Device\HarddiskVolume3\Wir[illegible]
** 2076 676     svchost.exe     0xad8187b94080  10      -       0       False   2023-05-21 22:28:19.000000 UTC  N/A     \Device\HarddiskVolume3\Wir[illegible]System32
\svchost.exe -k utcsvc -p       C:\Windows\System32\svchost.exe
** 1448 676     svchost.exe     0xad818796c2c0  30      -       0       False   2023-05-21 22:27:52.000000 UTC  N/A     \Device\HarddiskVolume3\Wir[illegible]System32
\svchost.exe -k NetworkService -p       C:\Windows\System32\svchost.exe
** 1064 676     svchost.exe     0xad8189d7c2c0  15      -       1       False   2023-05-21 22:30:09.000000 UTC  N/A     \Device\HarddiskVolume3\Wir[illegible]system32
\svchost.exe -k UnistackSvcGroup        C:\Windows\system32\svchost.exe
** 6696 676     svchost.exe     0xad818c532080  8       -       0       False   2023-05-21 22:34:07.000000 UTC  N/A     \Device\HarddiskVolume3\Wir[illegible]
** 1196 676     svchost.exe     0xad81877972c0  34      -       0       False   2023-05-21 22:27:46.000000 UTC  N/A     \Device\HarddiskVolume3\Wir[illegible]system32
\svchost.exe -k LocalService -p C:\Windows\system32\svchost.exe
** 1840 676     spoolsv.exe     0xad8187acb200  10      -       0       False   2023-05-21 22:28:03.000000 UTC  N/A     \Device\HarddiskVolume3\Wind[illegible]
** 952  676     svchost.exe     0xad81876802c0  12      -       0       False   2023-05-21 22:27:36.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\svchost.exe    C:\Windows\system32
\svchost.exe -k RPCSS -p        C:\Windows\system32\svchost.exe
** 824  676     svchost.exe     0xad818761d240  22      -       0       False   2023-05-21 22:27:32.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\svchost.exe    C:\Windows\system32
\svchost.exe -k DcomLaunch -p   C:\Windows\system32\svchost.exe
*** 7312        824     ApplicationFra  0xad818e84f300  10      -       1       False   2023-05-21 22:35:44.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\ApplicationFrameHost.exe C
:\Windows\system32\ApplicationFrameHost.exe -Embedding  C:\Windows\system32\ApplicationFrameHost.exe
*** 4116        824     RuntimeBroker.  0xad818cd93300  3       -       1       False   2023-05-21 22:31:24.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\RuntimeBroker.exe      - -
*** 5656        824     RuntimeBroker.  0xad81876e8080  0       -       1       False   2023-05-21 21:58:19.000000 UTC  2023-05-21 22:02:01.000000 UTC  \Device\HarddiskVolume3\Windows\System32\Ru
ntimeBroker.exe -       -
*** 2332        824     TiWorker.exe    0xad818e780080  4       -       0       False   2023-05-21 22:58:13.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\WinSxS\amd64_microsoft-windows-serv
icingstack_31bf3856ad364e35_10.0.19041.1940_none_7dd80d767cb5c7b0\TiWorker.exe  -       -
*** 7336        824     RuntimeBroker.  0xad818e8bb080  2       -       1       False   2023-05-21 22:11:39.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\RuntimeBroker.exe      - -
*** 5808        824     HxTsr.exe       0xad818de5d080  0       -       1       False   2023-05-21 21:59:58.000000 UTC  2023-05-21 22:07:45.000000 UTC  \Device\HarddiskVolume3\Program Files\Windo
wsApps\microsoft.windowscommunicationsapps_16005.11629.20316.0_x64__8wekyb3d8bbwe\HxTsr.exe     -       -
```

Leandro Delgado
Student number:114416241

Figure 5 Command Windows. pstree

```
(venv)kali@kali: ~/volatility3
File  Actions  Edit  View  Help
(venv)kali@kali: ~/volatility3 ×   kali@kali: ~/Desktop ×
588     520     winlogon.exe    0xad8186f450c0  5       -       1       False   2023-05-21 22:27:25.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\winlogon.exe   -       -
* 1016  588     dwm.exe 0xad81876e4340  15      -       1       False   2023-05-21 22:27:38.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\dwm.exe        "dwm.exe"       C:\Windows\
system32\dwm.exe
* 3556  588     userinit.exe    0xad818c02f340  0       -       1       False   2023-05-21 22:30:28.000000 UTC  2023-05-21 22:30:43.000000 UTC  \Device\HarddiskVolume3\Windows\System32\userinit.e
xe      -       -
** 3580 3556    explorer.exe    0xad818c047340  76      -       1       False   2023-05-21 22:30:28.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\explorer.exe    C:\Windows\Explorer.EXE C:\
Windows\Explorer.EXE
*** 6724        3580    Outline.exe     0xad818e578080  0       -       1       True    2023-05-21 22:36:09.000000 UTC  2023-05-21 23:01:24.000000 UTC  \Device\HarddiskVolume3\Program Files (x86)
\Outline\Outline.exe    -       -
**** 4224       6724    Outline.exe     0xad818e88b080  0       -       1       True    2023-05-21 22:36:23.000000 UTC  2023-05-21 23:01:24.000000 UTC  \Device\HarddiskVolume3\Program Files (x86)
\Outline\Outline.exe
**** 4628       6724    tun2socks.exe   0xad818de82340  0       -       1       True    2023-05-21 22:40:10.000000 UTC  2023-05-21 23:01:24.000000 UTC  \Device\HarddiskVolume3\Program Files (x86)
\Outline\resources\app.asar.unpacked\third_party\outline-go-tun2socks\win32\tun2socks.exe       -       -
*** 5636        3580    notepad.exe     0xad818db45080  1       -       1       False   2023-05-21 22:46:50.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\notepad.exe    -       -
*** 464 3580    SecurityHealth  0xad818979d080  3       -       1       False   2023-05-21 22:31:59.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\SecurityHealthSystray.exe      - -
*** 5328        3580    msedge.exe      0xad818d0980c0  54      -       1       False   2023-05-21 22:32:02.000000 UTC  N/A     \Device\HarddiskVolume3\Program Files (x86)\Microsoft\Edge\Applicat
ion\msedge.exe  "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --no-startup-window --win-session-start /prefetch:5      C:\Program Files (x86)\Microsoft\Edge\Application\msedge.ex
e
**** 4544       5328    msedge.exe      0xad818d75b080  14      -       1       False   2023-05-21 22:32:39.000000 UTC  N/A     \Device\HarddiskVolume3\Program Files (x86)\Microsoft\Edge\Applicat
ion\msedge.exe  -       -
**** 8896       5328    msedge.exe      0xad8187a39080  18      -       1       False   2023-05-21 22:28:21.000000 UTC  N/A     \Device\HarddiskVolume3\Program Files (x86)\Microsoft\Edge\Applicat
ion\msedge.exe  -       -
**** 5156       5328    msedge.exe      0xad818c553080  14      -       1       False   2023-05-21 22:28:22.000000 UTC  N/A     \Device\HarddiskVol                                     Applicat
ion\msedge.exe  -       -
**** 7964       5328    msedge.exe      0xad818dee5080  19      -       1       False   2023-05-21 22:22:09.000000 UTC  N/A     \Device\HarddiskVol                                     Applicat
ion\msedge.exe  -       -
**** 4396       5328    msedge.exe      0xad818d515080  7       -       1       False   2023-05-21 22:32:19.000000 UTC  N/A     \Device\HarddiskVol                                     Applicat
ion\msedge.exe  -       -
**** 6544       5328    msedge.exe      0xad818c0ea080  18      -       1       False   2023-05-21 22:22:35.000000 UTC  N/A     \Device\HarddiskVol                                     Applicat
ion\msedge.exe  -       -
**** 2388       5328    msedge.exe      0xad818e54c340  18      -       1       False   2023-05-21 22:05:35.000000 UTC  N/A     \Device\HarddiskVol                                     Applicat
ion\msedge.exe  -       -
**** 6292       5328    msedge.exe      0xad818d7a1080  20      -       1       False   2023-05-21 22:06:15.000000 UTC  N/A     \Device\HarddiskVol                                     Applicat
ion\msedge.exe  -       -
**** 1144       5328    msedge.exe      0xad818d75f080  18      -       1       False   2023-05-21 22:32:38.000000 UTC  N/A     \Device\HarddiskVol                                     Applicat
ion\msedge.exe  -       -
**** 5340       5328    msedge.exe      0xad818d7b3080  10      -       1       False   2023-05-21 22:32:39.000000 UTC  N/A     \Device\HarddiskVolume3\Program Files (x86)\Microsoft\Edge\Applicat
ion\msedge.exe  -       -
*** 3252        3580    vmtoolsd.exe    0xad8189796300  8       -       1       False   2023-05-21 22:31:59.000000 UTC  N/A     \Device\HarddiskVolume3\Program Files\VMware\VMware Tools\vmtoolsd.
exe     "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr    C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
*** 2228        3580    FTK Imager.exe  0xad818d143080  10      -       1       False   2023-05-21 22:43:56.000000 UTC  N/A     \Device\HarddiskVolume3\Program Files\AccessData\FTK Imager\FTK Ima
ger.exe -       -
*** 8920        3580    FTK Imager.exe  0xad818ef81080  20      -       1       False   2023-05-21 23:02:28.000000 UTC  N/A     \Device\HarddiskVolume3\Program Files\AccessData\FTK Imager\FTK Ima
ger.exe "C:\Program Files\AccessData\FTK Imager\FTK Imager.exe"         C:\Program Files\AccessData\FTK Imager\FTK Imager.exe
* 860   588     fontdrvhost.ex  0xad818761f140  5       -       1       False   2023-05-21 22:27:33.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\System32\fontdrvhost.exe        -       -
5896    8844    oneetx.exe      0xad8189b41080  5       -       1       True    2023-05-21 22:30:56.000000 UTC  N/A     \Device\HarddiskVolume3\Users\Tammam\AppData\Local\Temp\c3912af058\oneetx.e
xe      -       -
* 7732  5896    rundll32.exe    0xad818d1912c0  1       -       1       True    2023-05-21 22:31:53.000000 UTC  N/A     \Device\HarddiskVolume3\Windows\SysWOW64\rundll32.exe   -       -

File  Edit  View
Leandro Delgado
Student number:114416241
Ln 2, Col 25  40 characters  100%  Windov  UTF-8
```

Figure 6 Command Windows. pstree-part

5. What is the attacker's IP address?

```
(venv)kali@kali: ~/volatility3
File  Actions  Edit  View  Help
(venv)kali@kali: ~/volatility3 ×   kali@kali: ~/Desktop ×

┌──(venv)─(kali㉿kali)-[~/volatility3]
└─$ python3 vol.py -f ~/Desktop/MemoryDump.mem windows.netscan.NetScan | sort | uniq

Progress:  100.00               PDB scanning finished
0×ad81861e2310  TCPv4   0.0.0.0 49668   0.0.0.0 0       LISTENING       1840    spoolsv.exe     2023-05-21 22:28:09.000000 UTC
0×ad81861e2310  TCPv6   ::      49668   ::      0       LISTENING       1840    spoolsv.exe     2023-05-21 22:28:09.000000 UTC
0×ad81861e2470  TCPv4   0.0.0.0 5040    0.0.0.0 0       LISTENING       1196    svchost.exe     2023-05-21 22:30:31.000000 UTC
0×ad81861e2730  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       952     svchost.exe     2023-05-21 22:27:36.000000 UTC
0×ad81861e2b50  TCPv4   0.0.0.0 49665   0.0.0.0 0       LISTENING       552     wininit.exe     2023-05-21 22:27:36.000000 UTC
0×ad81861e2b50  TCPv6   ::      49665   ::      0       LISTENING       552     wininit.exe     2023-05-21 22:27:36.000000 UTC
0×ad81861e2e10  TCPv4   0.0.0.0 49665   0.0.0.0 0       LISTENING       552     wininit.exe     2023-05-21 22:27:36.000000 UTC
0×ad81861e3230  TCPv4   0.0.0.0 49664   0.0.0.0 0       LISTENING       696     lsass.exe       2023-05-21 22:27:36.000000 UTC
0×ad81861e3390  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       952     svchost.exe     2023-05-21 22:27:36.000000 UTC
0×ad81861e3390  TCPv6   ::      135     ::      0       LISTENING       952     svchost.exe     2023-05-21 22:27:36.000000 UTC
0×ad81861e34f0  TCPv4   0.0.0.0 49664   0.0.0.0 0       LISTENING       696     lsass.exe       2023-05-21 22:27:36.000000 UTC
0×ad81861e34f0  TCPv6   ::      49664   ::      0       LISTENING       696     lsass.exe       2023-05-21 22:27:36.000000 UTC
0×ad81861e37b0  TCPv4   0.0.0.0 49666   0.0.0.0 0       LISTENING       1012    svchost.exe     2023-05-21 22:27:49.000000 UTC
0×ad81861e37b0  TCPv6   ::      49666   ::      0       LISTENING       1012    svchost.exe     2023-05-21 22:27:49.000000 UTC
0×ad81861e3910  TCPv4   0.0.0.0 49667   0.0.0.0 0       LISTENING       448     svchost.exe     2023-05-21 22:27:58.000000 UTC
0×ad81861e3910  TCPv6   ::      49667   ::      0       LISTENING       448     svchost.exe     2023-05-21 22:27:58.000000 UTC
0×ad81861e3a70  TCPv4   0.0.0.0 49668   0.0.0.0 0       LISTENING       1840    spoolsv.exe     2023-05-21 22:28:09.000000 UTC
0×ad81861e3bd0  TCPv4   0.0.0.0 49666   0.0.0.0 0       LISTENING       1012    svchost.exe     2023-05-21 22:27:49.000000 UTC
0×ad81861e3e90  TCPv4   0.0.0.0 49667   0.0.0.0 0       LISTENING       448     svchost.exe     2023-05-21 22:27:58.000000 UTC
0×ad818662ecb0  TCPv4   0.0.0.0 445     0.0.0.0 0       LISTENING       4       System  2023-05-21 22:29:04.000000 UTC
0×ad818662ecb0  TCPv6   ::      445     ::      0       LISTENING       4       System  2023-05-21 22:29:04.000000 UTC
0×ad818662f390  TCPv4   0.0.0.0 7680    0.0.0.0 0       LISTENING       5476    svchost.exe     2023-05-21 22:58:09.000000 UTC
0×ad818662f390  TCPv6   ::      7680    ::      0       LISTENING       5476    svchost.exe     2023-05-21 22:58:09.000000 UTC
0×ad81878518f0  UDPv4   192.168.190.141 138     *       0               4       System  2023-05-21 22:27:56.000000 UTC
0×ad8187852250  UDPv4   192.168.190.141 137     *       0               4       System  2023-05-21 22:27:56.000000 UTC
0×ad818902a5d0  TCPv4   192.168.190.141 139     0.0.0.0 0       LISTENING       4       System  2023-05-21 22:27:56.000000 UTC
0×ad818971f870  UDPv4   0.0.0.0 56250   *       0               6644    SkypeApp.exe    2023-05-21 22:58:07.000000 UTC
0×ad818971f870  UDPv6   ::      56250   *       0               6644    SkypeApp.exe    2023-05-21 22:58:07.000000 UTC
0×ad81897eb010  TCPv4   10.0.85.2       55439   20.22.207.36    443     CLOSED  448     svchost.exe     2023-05-21 23:00:40.000000 UTC
0×ad81898a6d10  UDPv4   127.0.0.1       57787   *       0               448     svchost.exe     2023-05-21 22:28:54.000000 UTC
0×ad81898bc7f0  UDPv4   0.0.0.0 5355    *       0               1448    svchost.exe     2023-05-21 22:57:37.000000 UTC
0×ad81898bc7f0  UDPv6   ::      5355    *       0               1448    svchost.exe     2023-05-21 22:57:37.000000 UTC
0×ad8189a291b0  TCPv4   0.0.0.0 55972   0.0.0.0 0       LISTENING       5964    svchost.exe     2023-05-21 22:27:57.000000 UTC
0×ad8189a291b0  TCPv6   ::      55972   ::      0       LISTENING       5964    svchost.exe     2023-05-21 22:27:57.000000 UTC
0×ad8189a29470  TCPv4   0.0.0.0 55972   0.0.0.0 0       LISTENING       5964    svchost.exe     2023-05-21 22:27:57.000000 UTC
0×ad8189a2a7b0  TCPv4   0.0.0.0 49669   0.0.0.0 0       LISTENING       676     services.exe    2023-05-21 22:29:08.000000 UTC
0×ad8189a2a910  TCPv4   0.0.0.0 49669   0.0.0.0 0       LISTENING       676     services.exe    2023-05-21 22:29:08.000000 UTC
0×ad8189a2a910  TCPv6   ::      49669   ::      0       LISTENING       676     services.exe    2023-05-21 22:29:08.000000 UTC
0×ad8189a30a20  TCPv4   192.168.190.141 53660   38.121.43.65    443     CLOSED  4628    tun2socks.exe   2023-05-21 22:00:25.000000 UTC
0×ad8189a844e0  UDPv4   10.0.85.2       58844   *       0               5328    msedge.exe      2023-05-21 22:51:53.000000 UTC
0×ad8189cea350  UDPv4   0.0.0.0 5050    *       0               1196    svchost.exe     2023-05-21 22:30:27.000000 UTC
0×ad818c17ada0  UDPv4   0.0.0.0 52051   *       0               4628    tun2socks.exe   2023-05-21 22:24:14.000000 UTC
0×ad818c367b30  TCPv4   192.168.190.141 49710   204.79.197.203  443     CLOSE_WAIT      1916    SearchApp.exe   2023-05-21 22:33:09.000000 UTC
0×ad818c3b22e0  UDPv4   0.0.0.0 63218   *       0               1448    svchost.exe     2023-05-21 22:39:15.000000 UTC
0×ad818c3b22e0  UDPv6   ::      63218   *       0               1448    svchost.exe     2023-05-21 22:39:15.000000 UTC
```

```
File  Edit  View
Leandro Delgado
Student number:114416241
Ln 2, Col 25   40 characters   100%   Windov   UTF-8
```

Figure 7 Attacker IP address

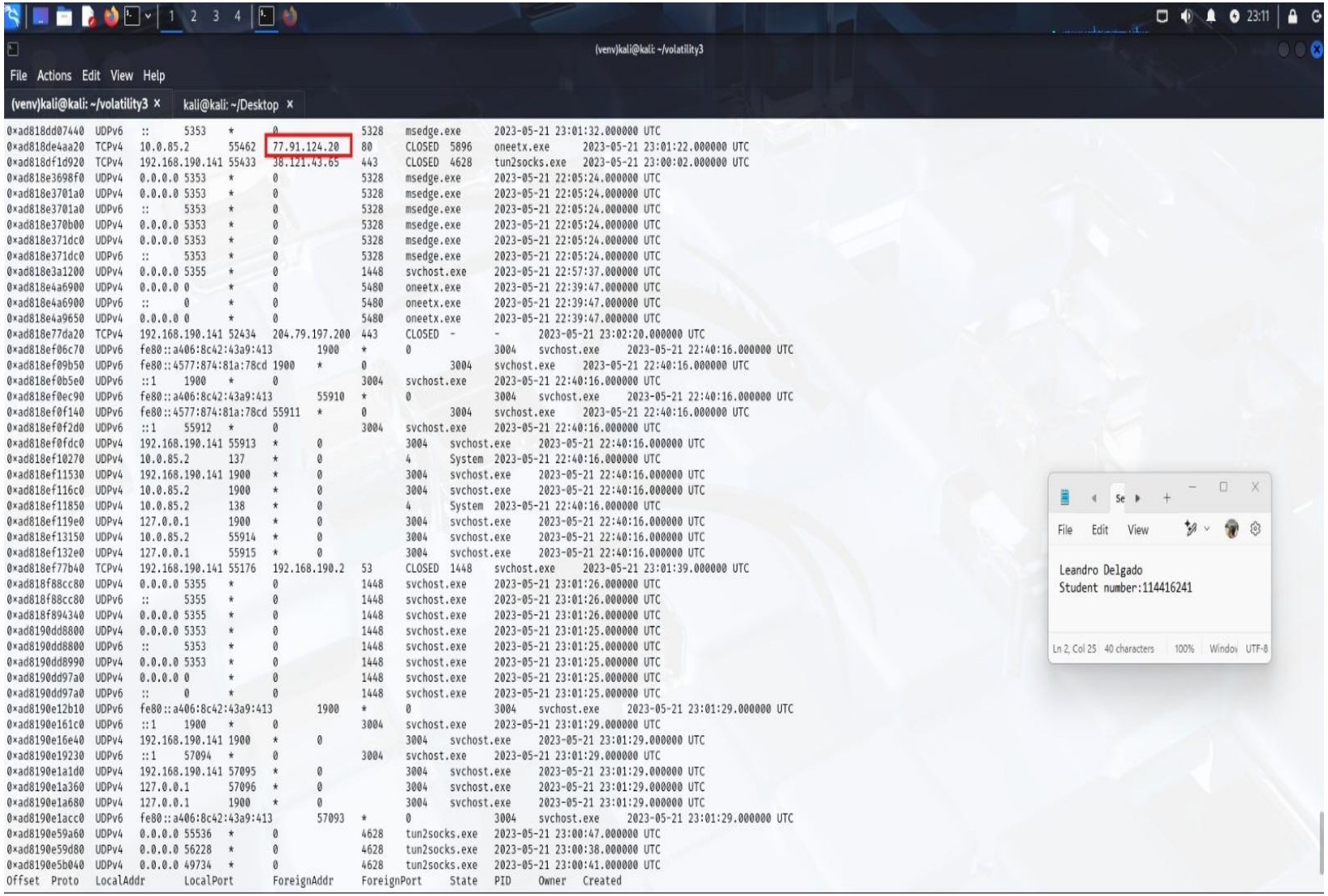


Figure 8 Attacker Ip address part 2

6. Based on the previous artifacts. What is the name of the malware family?

```
9.9.9.9

┌──(venv)─(kali㉿kali)-[~/volatility3]
└─$ strings ~/Desktop/MemoryDump.mem | grep -i "redline\|stealer"

!Redline.YUQ!
+dStealer.D!MTB
Stealer!mcl@P
32/ArkeiStealer.A
!RedLineStealer
Redline.N
!RedLineStealer.
!Redline.GDL
lStealer
RedLineStealer
Redline.K
!Redline.GH
PSWStealer.XE
!RedlineS
!InfoStealer-
Spy:AndroidOS/InfoStealer.AB2
RedLineSteal`
ArkeiStealer.M
!RedLineStealer.MEn
32/Stealer.C
RedLineS├MD
IsUsingLevelTriggeredLineInterrupt
IsUsingEdgeTriggeredLineInterrupt
Redline.NEJF
RedLine!atmn
!Redline.GEO>
!Redline.LL
Redline.GCW
!Stealerium.
Stealer.PF
!RedlineSteaq7
ff3.5.x stealer\stub\
Stealerc.GJ
RedLine
!Redline.ZLZ>
RedLineStealer.EBn
DarkStealer.AD
!Redline.GJA
Stealerc
neStealer.MTA~
RedLine.RDI!Mw
LngStealers
!Redline.BT
RedLine.M
```

Leandro Delgado
Student number:114416241

Figure 9 Name of the Malware family

7. What is the full URL of the PHP file that the attacker visited?

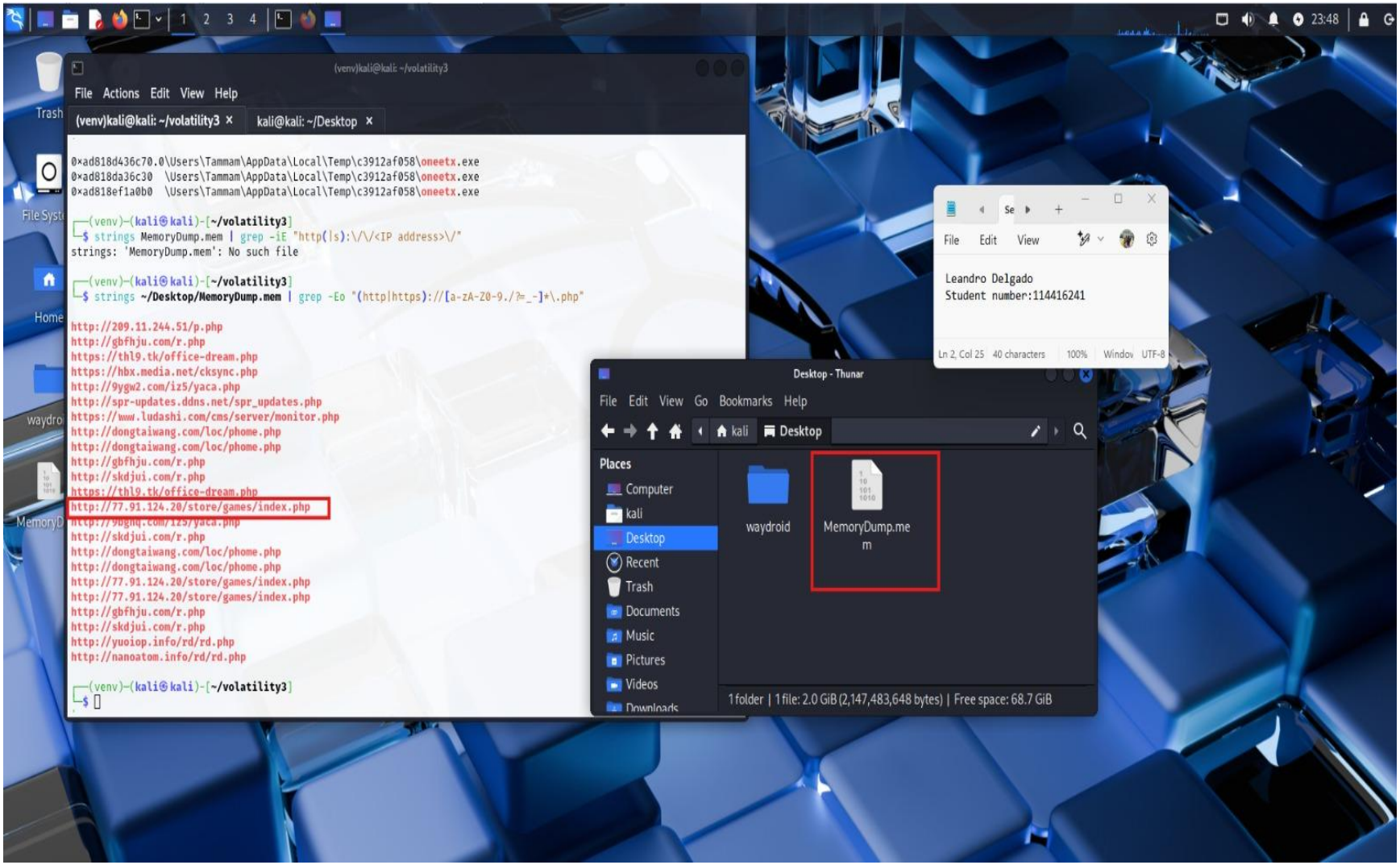


Figure 10 Url of the PHP file the attacker

8. What is the full path of the malicious executable?

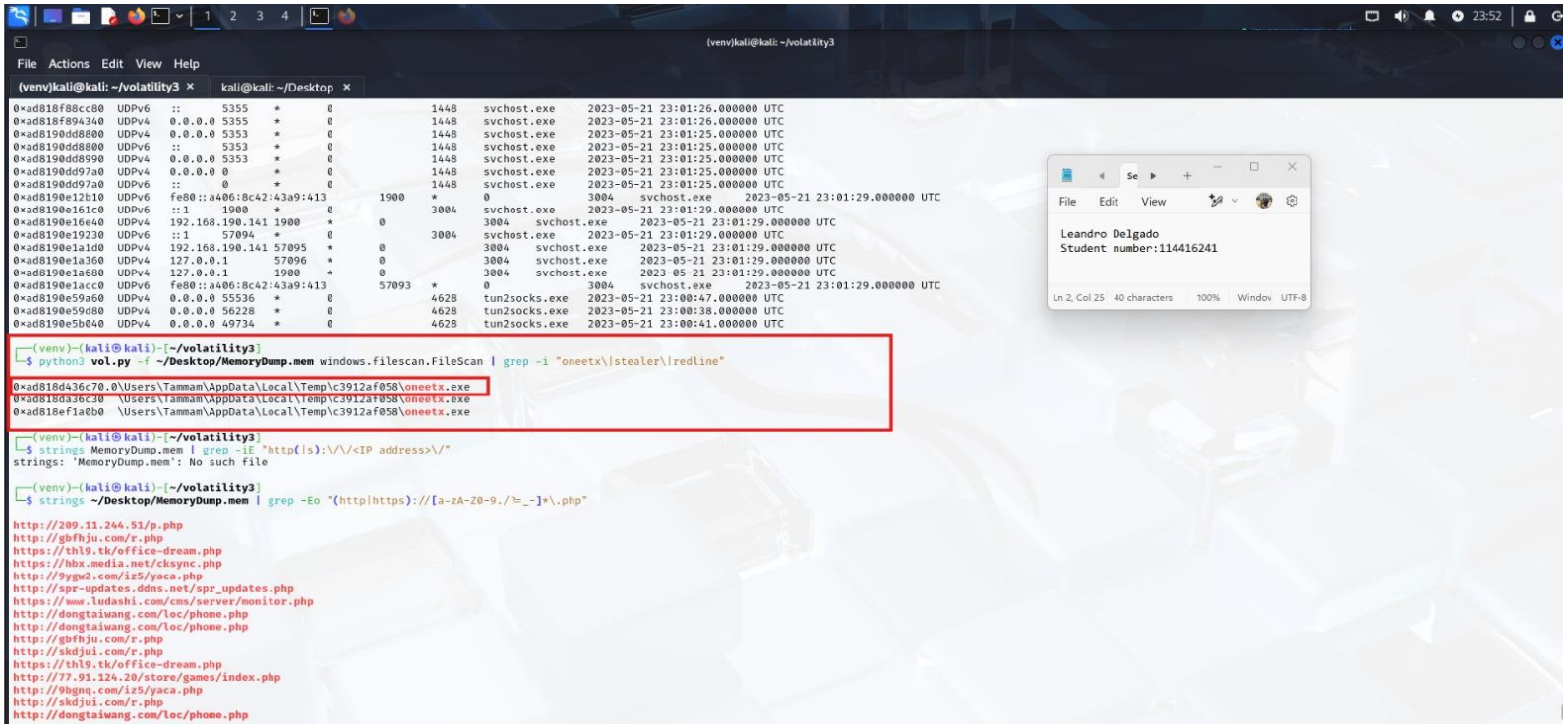


Figure 11 The full path of the malicious executable

Students Work required for this activity	• Go to the challenge https://cyberdefenders.org/blueteam-ctf-challenges/106#nav-questions • Create an account and Login. • Download the Challenge. Uncompress the challenge (pass: cyberdefenders.org). • Answer the 8 challenge questions. Tool Used: Volatility. • Show complete screenshots of all your work.
Grading Alerts	• If you do NOT use this template or delete any part of it or use any other template, you will be degraded. • If you do NOT follow the fie naming convention, you will be degraded. • If you do NOT submit your file in PDF; you will be degraded. • If you do NOT show your account real name (when applicable); you will be degraded. • If you do NOT show your machine desktop background (with date & time) and IP, you will be degraded. If you do NOT write (in your own words) your learning experience for the activity practices, you will be degraded.