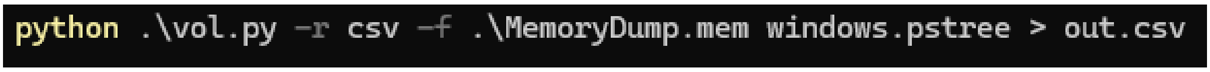
CyberDefenders: Redline

The following writeup is for Redline on CyberDefenders, it involves investigating a memory dump using Volatility 3.

Scenario: As a member of the Security Blue Team, your assignment is to analyse 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.

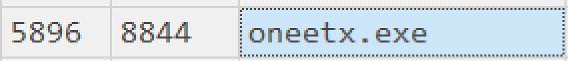
What is the name of the suspicious process?

I started off by using the pstree plugin to see all parent-child processes running at the time of the memory capture:



```
python .\vol.py -r csv -f .\MemoryDump.mem windows.pstree > out.csv
```

I then came across oneetx.exe which is pretty suspicious:

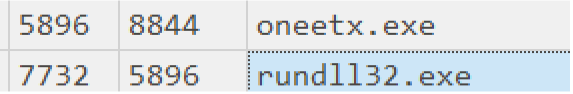


5896	8844	oneetx.exe

After doing some research, it seems as if this executable is affiliated with the Redline stealer.

What is the child process name of the suspicious process?

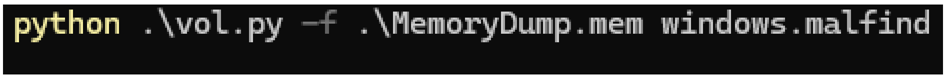
rundll32.exe:



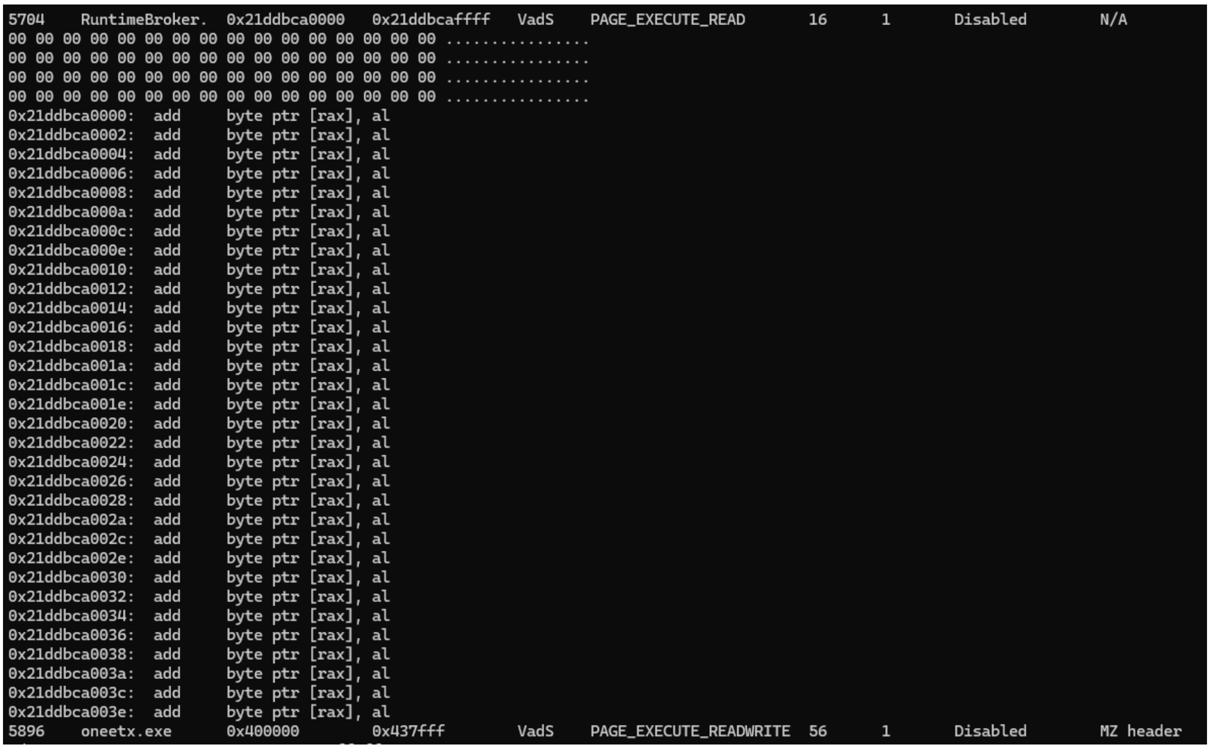
5896	8844	oneetx.exe
7732	5896	rundll32.exe

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

The malfind plugin finds hidden or injected code/DLLs in memory based on VAD tag and page permissions. We can use this plugin to find the memory protection applied to oneetx.exe:



```
python .\vol.py -f .\MemoryDump.mem windows.malfind
```



```
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
```

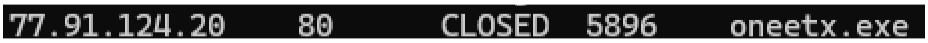
Therefore, the memory protection is PAGE_EXECUTE_READWRITE.

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

We can use the netscan plugin to find all network connections at the time of acquisition. The process is outline.exe.

What is the attacker's IP address?

If we look in the output of the netscan command, we can see that oneetx.exe is connecting to a remote IP address:

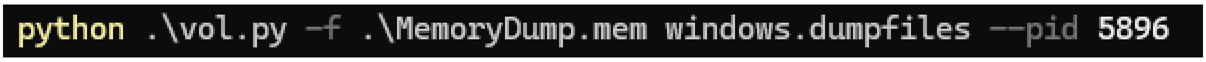


```
77.91.124.20    80      CLOSED  5896    oneetx.exe
```

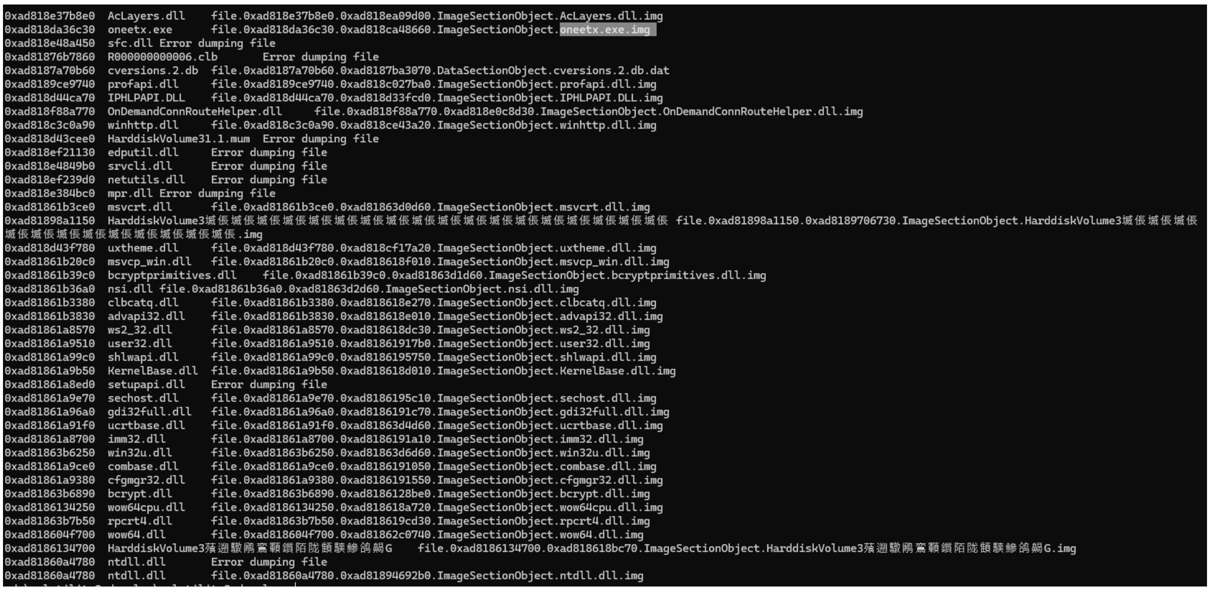
This remote IP is the answer.

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

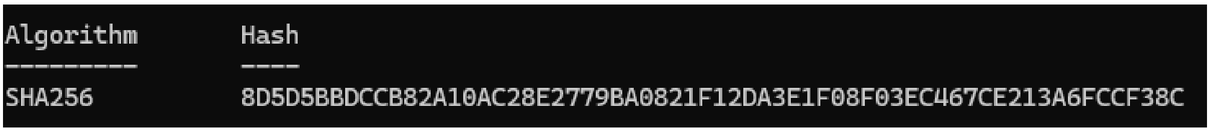
There are multiple ways to determine this, such as uploading the remote IP we just found, or we can upload a file hash of the malicious executable. To do this, we can use the dumpfiles plugin and supply the PID of the malicious process like as follows:



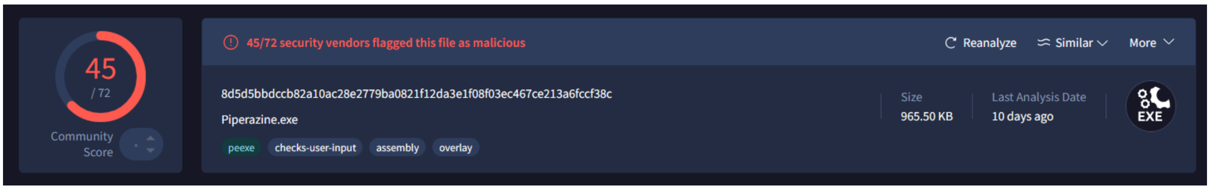
```
python .\vol.py -f .\MemoryDump.mem windows.dumpfiles --pid 5896
```



```
0xad818e37b8e0  AcLayers.dll    file.0xad818e37b8e0.0xad818ea09d00.ImageSectionObject.AcLayers.dll.img
0xad818da36c30  oneetx.exe      file.0xad818da36c30.0xad818ca48660.ImageSectionObject.oneetx.exe.img
0xad818e48a450  sfc.dll Error dumping file
0xad81876b7860  R000000000006.clb       Error dumping file
0xad8187a70b60  cversions.2.db  file.0xad8187a70b60.0xad8187ba3070.DataSectionObject.cversions.2.db.dat
0xad8189ce9740  profapi.dll     file.0xad8189ce9740.0xad818c027ba0.ImageSectionObject.profapi.dll.img
0xad818d44ca70  IPHLPAPI.DLL    file.0xad818d44ca70.0xad818d33fcd0.ImageSectionObject.IPHLPAPI.DLL.img
0xad818f88a770  OnDemandConnRouteHelper.dll     file.0xad818f88a770.0xad818e0c8d30.ImageSectionObject.OnDemandConnRouteHelper.dll.img
0xad818c3c0a90  winhttp.dll     file.0xad818c3c0a90.0xad818ce43a20.ImageSectionObject.winhttp.dll.img
0xad818d43cee0  HarddiskVolume31.1.mum  Error dumping file
0xad818ef21130  edputil.dll     Error dumping file
0xad818e4849b0  srvcli.dll      Error dumping file
0xad818ef239d0  netutils.dll    Error dumping file
0xad818e384bc0  mpr.dll Error dumping file
0xad81861b3ce0  msvcrt.dll      file.0xad81861b3ce0.0xad81863d0d60.ImageSectionObject.msvcrt.dll.img
0xad81898a1150  HarddiskVolume3墄倀墄倀墄倀墄倀墄倀墄倀墄倀墄倀墄倀墄倀墄倀墄倀墄倀墄倀墄倀墄倀墄倀墄倀 file.0xad81898a1150.0xad8189706730.ImageSectionObject.HarddiskVolume3墄倀墄倀墄倀
墄倀墄倀墄倀墄倀墄倀墄倀墄倀墄倀墄倀.img
0xad818d43f780  uxtheme.dll     file.0xad818d43f780.0xad818cf17a20.ImageSectionObject.uxtheme.dll.img
0xad81861b20c0  msvcp_win.dll   file.0xad81861b20c0.0xad818618f010.ImageSectionObject.msvcp_win.dll.img
0xad81861b39c0  bcryptprimitives.dll    file.0xad81861b39c0.0xad81863d1d60.ImageSectionObject.bcryptprimitives.dll.img
0xad81861b36a0  nsi.dll file.0xad81861b36a0.0xad81863d2d60.ImageSectionObject.nsi.dll.img
0xad81861b3380  clbcatq.dll     file.0xad81861b3380.0xad818618e270.ImageSectionObject.clbcatq.dll.img
0xad81861b3830  advapi32.dll    file.0xad81861b3830.0xad818618e010.ImageSectionObject.advapi32.dll.img
0xad81861a8570  ws2_32.dll      file.0xad81861a8570.0xad818618dc30.ImageSectionObject.ws2_32.dll.img
0xad81861a9510  user32.dll      file.0xad81861a9510.0xad81861917b0.ImageSectionObject.user32.dll.img
0xad81861a99c0  shlwapi.dll     file.0xad81861a99c0.0xad8186195750.ImageSectionObject.shlwapi.dll.img
0xad81861a9b50  KernelBase.dll  file.0xad81861a9b50.0xad818618d010.ImageSectionObject.KernelBase.dll.img
0xad81861a8ed0  setupapi.dll    Error dumping file
0xad81861a9e70  sechost.dll     file.0xad81861a9e70.0xad8186195c10.ImageSectionObject.sechost.dll.img
0xad81861a96a0  gdi32full.dll   file.0xad81861a96a0.0xad8186191c70.ImageSectionObject.gdi32full.dll.img
0xad81861a91f0  ucrtbase.dll    file.0xad81861a91f0.0xad81863d4d60.ImageSectionObject.ucrtbase.dll.img
0xad81861a8700  imm32.dll       file.0xad81861a8700.0xad8186191a10.ImageSectionObject.imm32.dll.img
0xad81863b6250  win32u.dll      file.0xad81863b6250.0xad81863d6d60.ImageSectionObject.win32u.dll.img
0xad81861a9ce0  combase.dll     file.0xad81861a9ce0.0xad8186191050.ImageSectionObject.combase.dll.img
0xad81861a9380  cfgmgr32.dll    file.0xad81861a9380.0xad8186191550.ImageSectionObject.cfgmgr32.dll.img
0xad81863b6890  bcrypt.dll      file.0xad81863b6890.0xad8186128be0.ImageSectionObject.bcrypt.dll.img
0xad8186134250  wow64cpu.dll    file.0xad8186134250.0xad818618a720.ImageSectionObject.wow64cpu.dll.img
0xad81863b7b50  rpcrt4.dll      file.0xad81863b7b50.0xad818619cd30.ImageSectionObject.rpcrt4.dll.img
0xad818604f700  wow64.dll       file.0xad818604f700.0xad81862c0740.ImageSectionObject.wow64.dll.img
0xad8186134700  HarddiskVolume3蕵遡駿鹇鳶顬鑕陌陇餖騤鰺鸽鶡G    file.0xad8186134700.0xad818618bc70.ImageSectionObject.HarddiskVolume3蕵遡駿鹇鳶顬鑕陌陇餖騤鰺鸽鶡G.img
0xad81860a4780  ntdll.dll       Error dumping file
0xad81860a4780  ntdll.dll       file.0xad81860a4780.0xad81894692b0.ImageSectionObject.ntdll.dll.img
```



```
Algorithm       Hash
---------       ----
SHA256          8D5D5BBDCCB82A10AC28E2779BA0821F12DA3E1F08F03EC467CE213A6FCCF38C
```



45/72 security vendors flagged this file as malicious

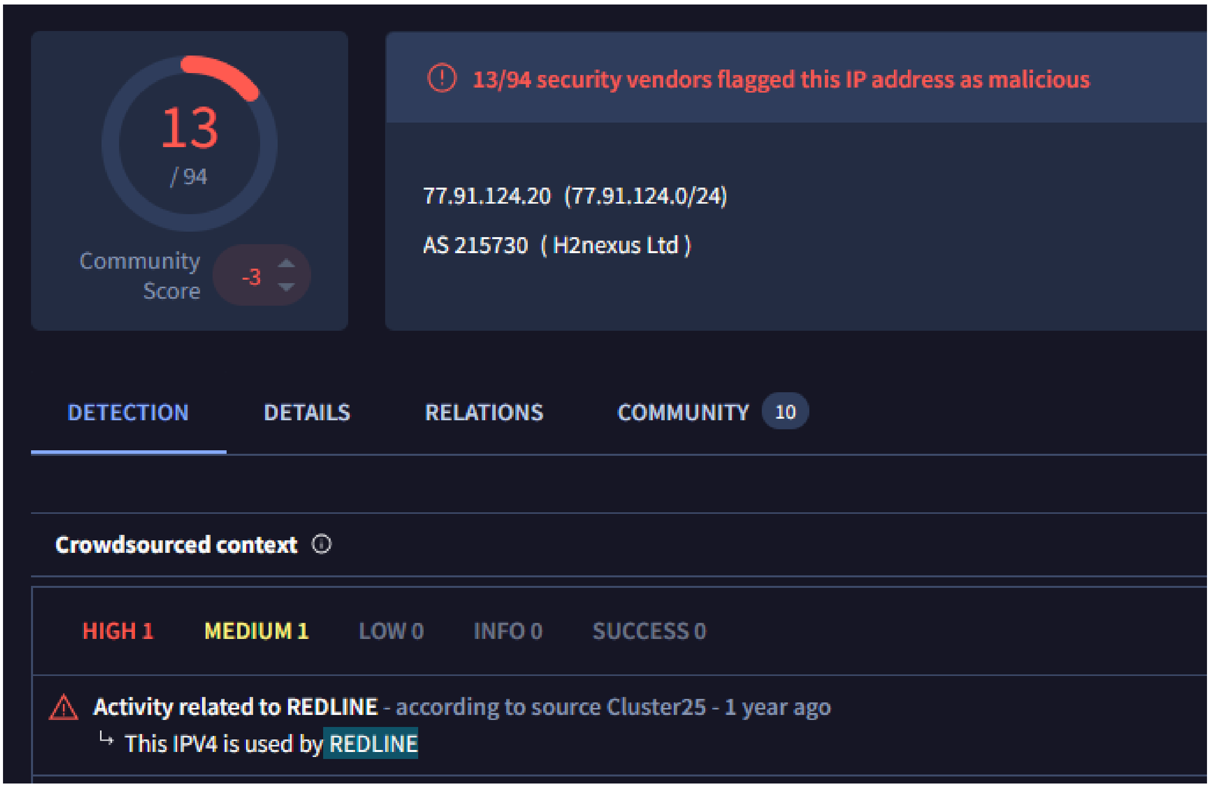
8d5d5bbdccb82a10ac28e2779ba0821f12da3e1f08f03ec467ce213a6fccf38c

Piperazine.exe

Size 965.50 KB

Last Analysis Date 10 days ago

After exploring the relations tab and threat graph, there is no concrete proof on what malware family this executable is a part of. Therefore, I searched for the IP addresses we found earlier and we can determine that the malware family is Redline Stealer:



13

/ 94

Community Score -3

13/94 security vendors flagged this IP address as malicious

77.91.124.20 (77.91.124.0/24)

AS 215730 (H2nexus Ltd)

Crowdsourced context

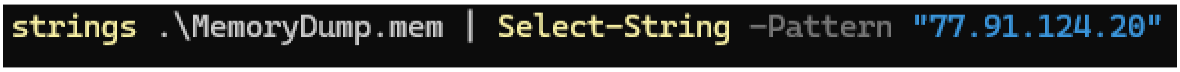
HIGH 1 MEDIUM 1 LOW 0 INFO 0 SUCCESS 0

Activity related to REDLINE - according to source Cluster25 - 1 year ago

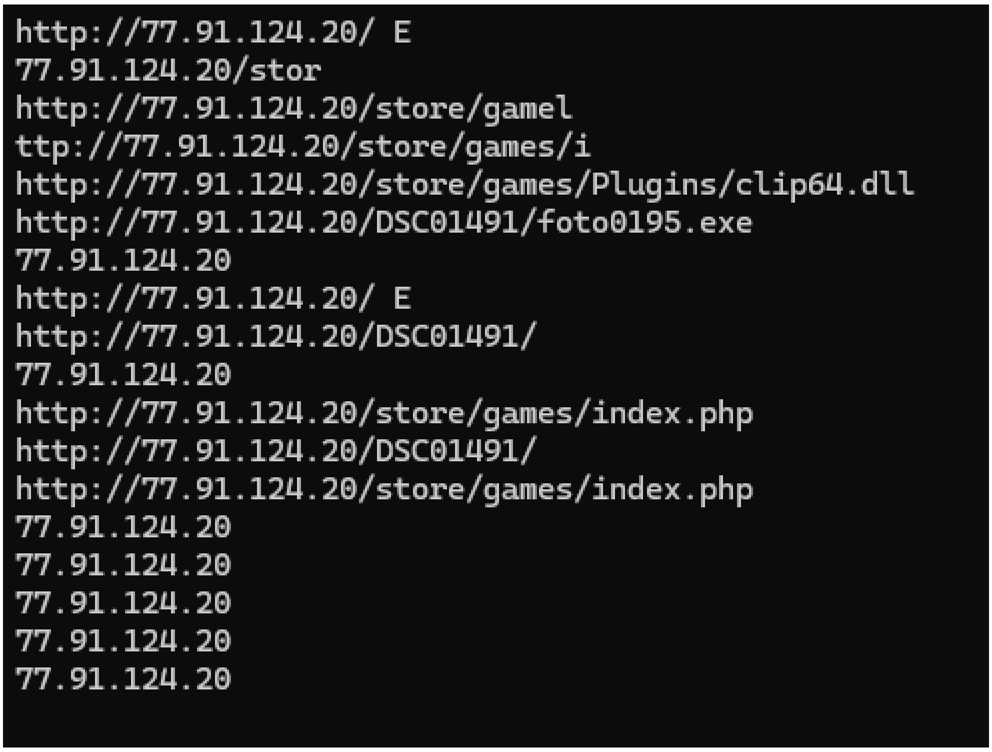
↳ This IPV4 is used by REDLINE

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

If you use the strings command, you can determine the URL of the PHP file visited by the attacker:



```
strings .\MemoryDump.mem | Select-String -Pattern "77.91.124.20"
```

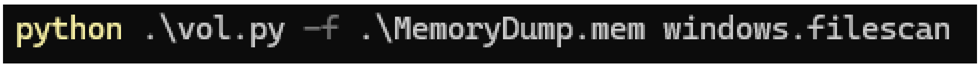


```
http://77.91.124.20/ E
77.91.124.20/stor
http://77.91.124.20/store/gamel
ttp://77.91.124.20/store/games/i
http://77.91.124.20/store/games/Plugins/clip64.dll
http://77.91.124.20/DSC01491/foto0195.exe
77.91.124.20
http://77.91.124.20/ E
http://77.91.124.20/DSC01491/
77.91.124.20
http://77.91.124.20/store/games/index.php
http://77.91.124.20/DSC01491/
http://77.91.124.20/store/games/index.php
77.91.124.20
77.91.124.20
77.91.124.20
77.91.124.20
77.91.124.20
```

http://77.91.124.20/store/games/index.php

What is the full path of the malicious executable?

We can use the filescan plugin:



```
python .\vol.py -f .\MemoryDump.mem windows.filescan
```

Make sure to grep the output and look for oneetx.exe:

C:\Users\Tammam\AppData\Local\Temp\c3912af058\oneetx.exe