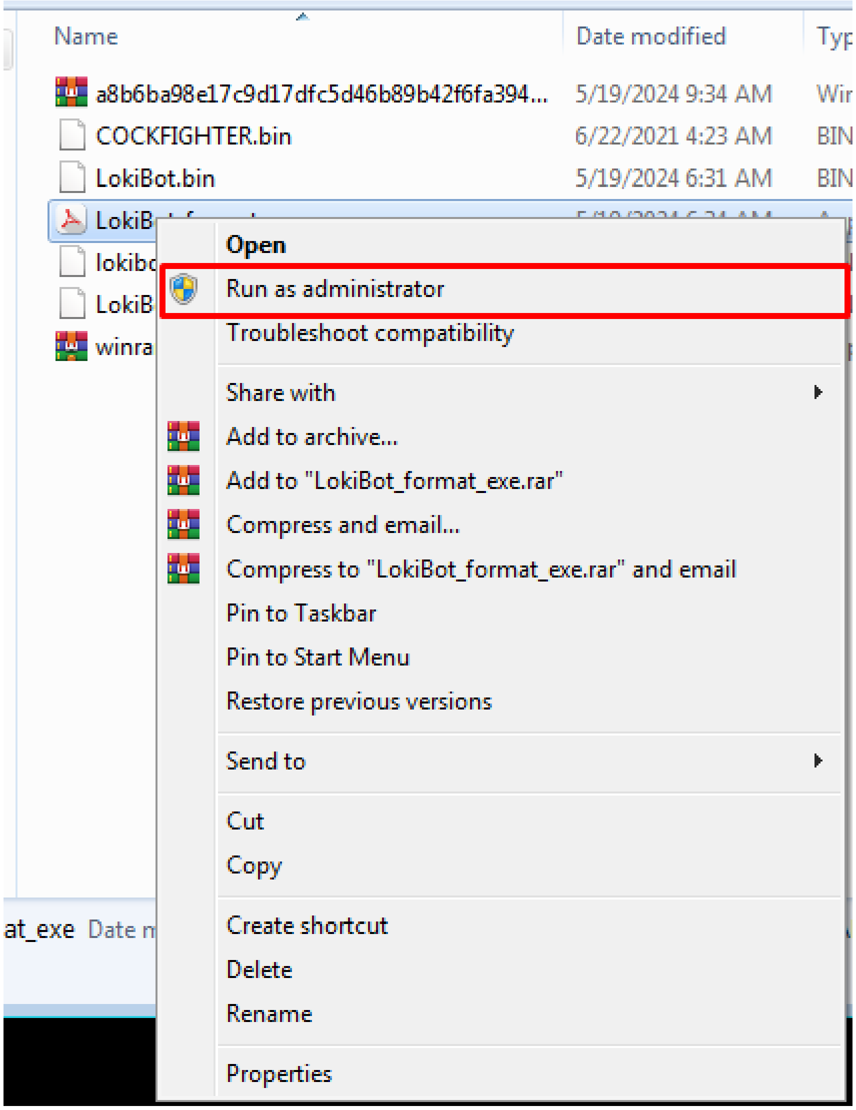
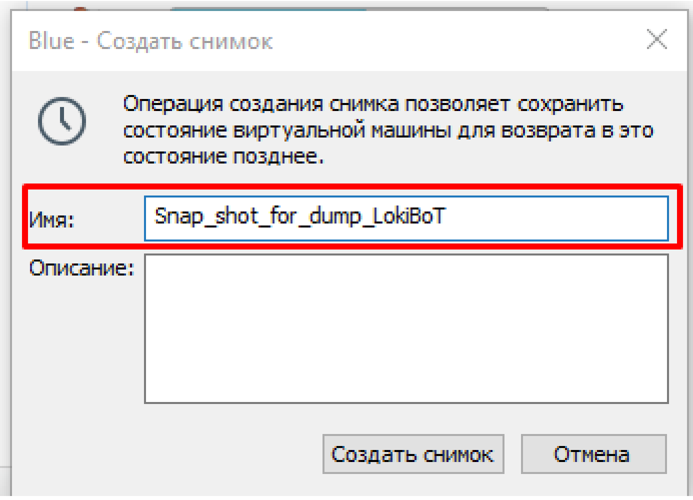
Analiza memorie RAM

Rulam malware:



Dupa rularea `LokiBot` facem un snapshot la machina noastra:



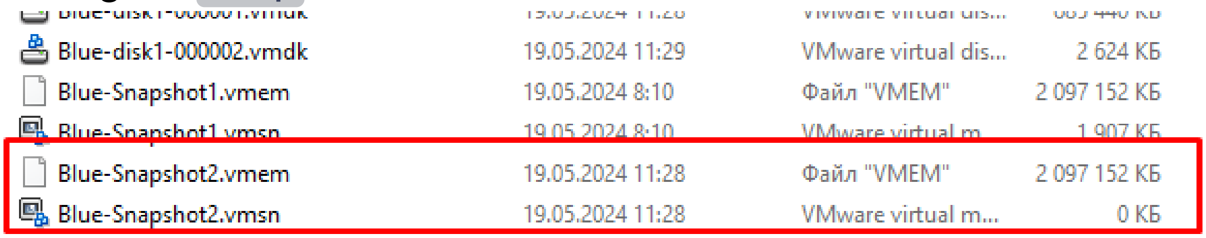
Blue - Создать снимок

Операция создания снимка позволяет сохранить состояние виртуальной машины для возврата в это состояние позднее.

Имя: Snap_shot_for_dump_LokiBoT

Описание:

Retragem `dump`-ul de memorie:

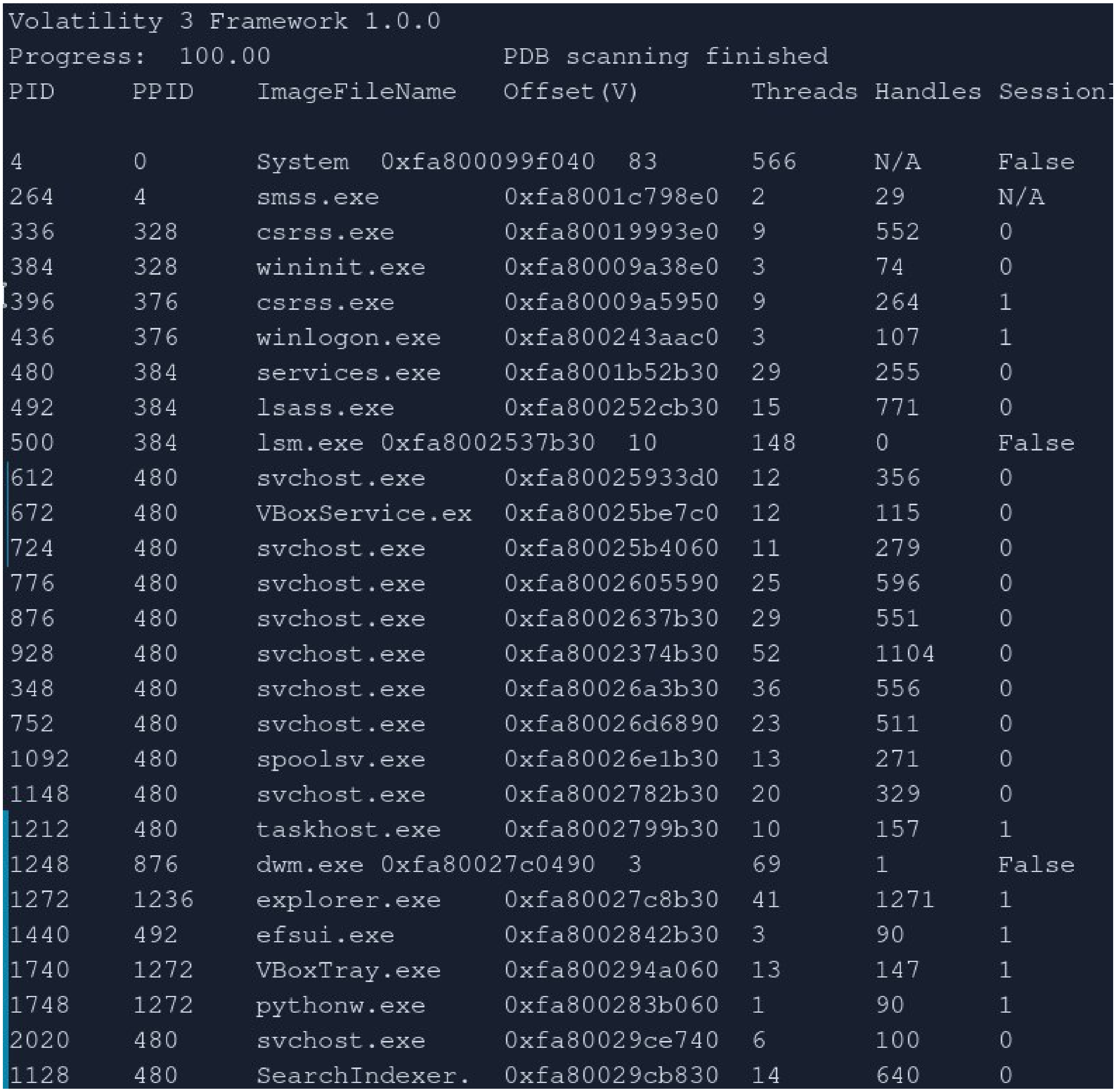


Blue-disk1-000001.vmdk	19.05.2024 11:28	VMware virtual dis...	685 440 КБ
Blue-disk1-000002.vmdk	19.05.2024 11:29	VMware virtual dis...	2 624 КБ
Blue-Snapshot1.vmem	19.05.2024 8:10	Файл "VMEM"	2 097 152 КБ
Blue-Snapshot1.vmsn	19.05.2024 8:10	VMware virtual m...	1 907 КБ
Blue-Snapshot2.vmem	19.05.2024 11:28	Файл "VMEM"	2 097 152 КБ
Blue-Snapshot2.vmsn	19.05.2024 11:28	VMware virtual m...	0 КБ

Fisierul cu extensia `.vmem` si este dumpul nostru cel `.vmsn` este pentru configurarea VmWare.

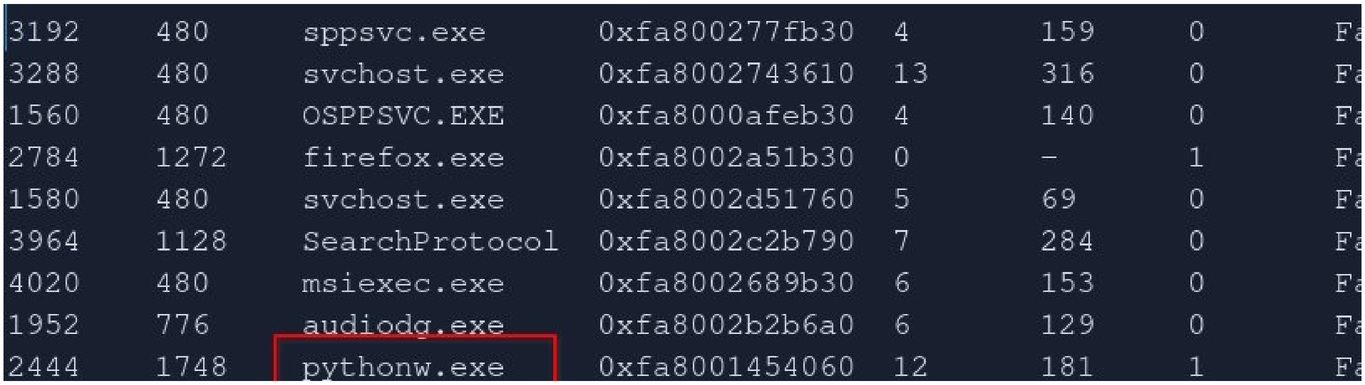
Analizam procesele care sunt rulate pe masina infectata:

```
vol3 -f Loki_dump_memory.vmem windows.pslist
```



```
Volatility 3 Framework 1.0.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionI

4       0       System  0xfa800099f040  83      566     N/A     False
264     4       smss.exe        0xfa8001c798e0  2       29      N/A
336     328     csrss.exe       0xfa80019993e0  9       552     0
384     328     wininit.exe     0xfa80009a38e0  3       74      0
396     376     csrss.exe       0xfa80009a5950  9       264     1
436     376     winlogon.exe    0xfa800243aac0  3       107     1
480     384     services.exe    0xfa8001b52b30  29      255     0
492     384     lsass.exe       0xfa800252cb30  15      771     0
500     384     lsm.exe 0xfa8002537b30  10      148     0       False
612     480     svchost.exe     0xfa80025933d0  12      356     0
672     480     VBoxService.ex  0xfa80025be7c0  12      115     0
724     480     svchost.exe     0xfa80025b4060  11      279     0
776     480     svchost.exe     0xfa8002605590  25      596     0
876     480     svchost.exe     0xfa8002637b30  29      551     0
928     480     svchost.exe     0xfa8002374b30  52      1104    0
348     480     svchost.exe     0xfa80026a3b30  36      556     0
752     480     svchost.exe     0xfa80026d6890  23      511     0
1092    480     spoolsv.exe     0xfa80026e1b30  13      271     0
1148    480     svchost.exe     0xfa8002782b30  20      329     0
1212    480     taskhost.exe    0xfa8002799b30  10      157     1
1248    876     dwm.exe 0xfa80027c0490  3       69      1       False
1272    1236    explorer.exe    0xfa80027c8b30  41      1271    1
1440    492     efsui.exe       0xfa8002842b30  3       90      1
1740    1272    VBoxTray.exe    0xfa800294a060  13      147     1
1748    1272    pythonw.exe     0xfa800283b060  1       90      1
2020    480     svchost.exe     0xfa80029ce740  6       100     0
1128    480     SearchIndexer.  0xfa80029cb830  14      640     0
```

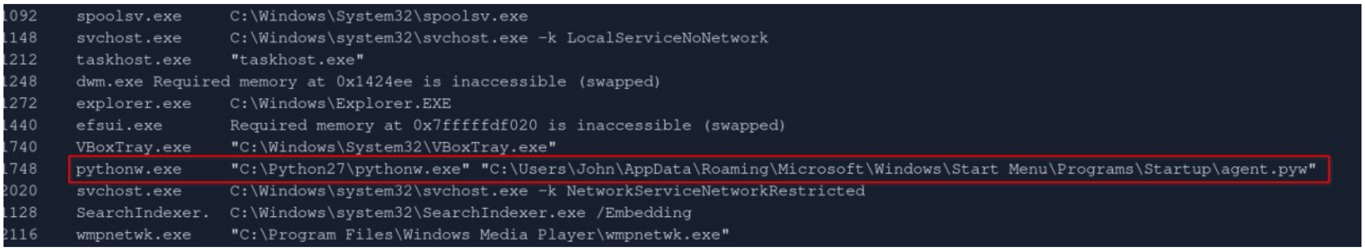
In cazul nostru procesul infectat este `pythonw.exe` care are `pid` 2444:



```
3192    480     sppsvc.exe      0xfa800277fb30  4       159     0       Fa
3288    480     svchost.exe     0xfa8002743610  13      316     0       Fa
1560    480     OSPPSVC.EXE     0xfa8000afeb30  4       140     0       Fa
2784    1272    firefox.exe     0xfa8002a51b30  0       -       1       Fa
1580    480     svchost.exe     0xfa8002d51760  5       69      0       Fa
3964    1128    SearchProtocol  0xfa8002c2b790  7       284     0       Fa
4020    480     msiexec.exe     0xfa8002689b30  6       153     0       Fa
1952    776     audiodg.exe     0xfa8002b2b6a0  6       129     0       Fa
2444    1748    pythonw.exe     0xfa8001454060  12      181     1       Fa
```

Verificam ce comenzi pornesc acest proces:

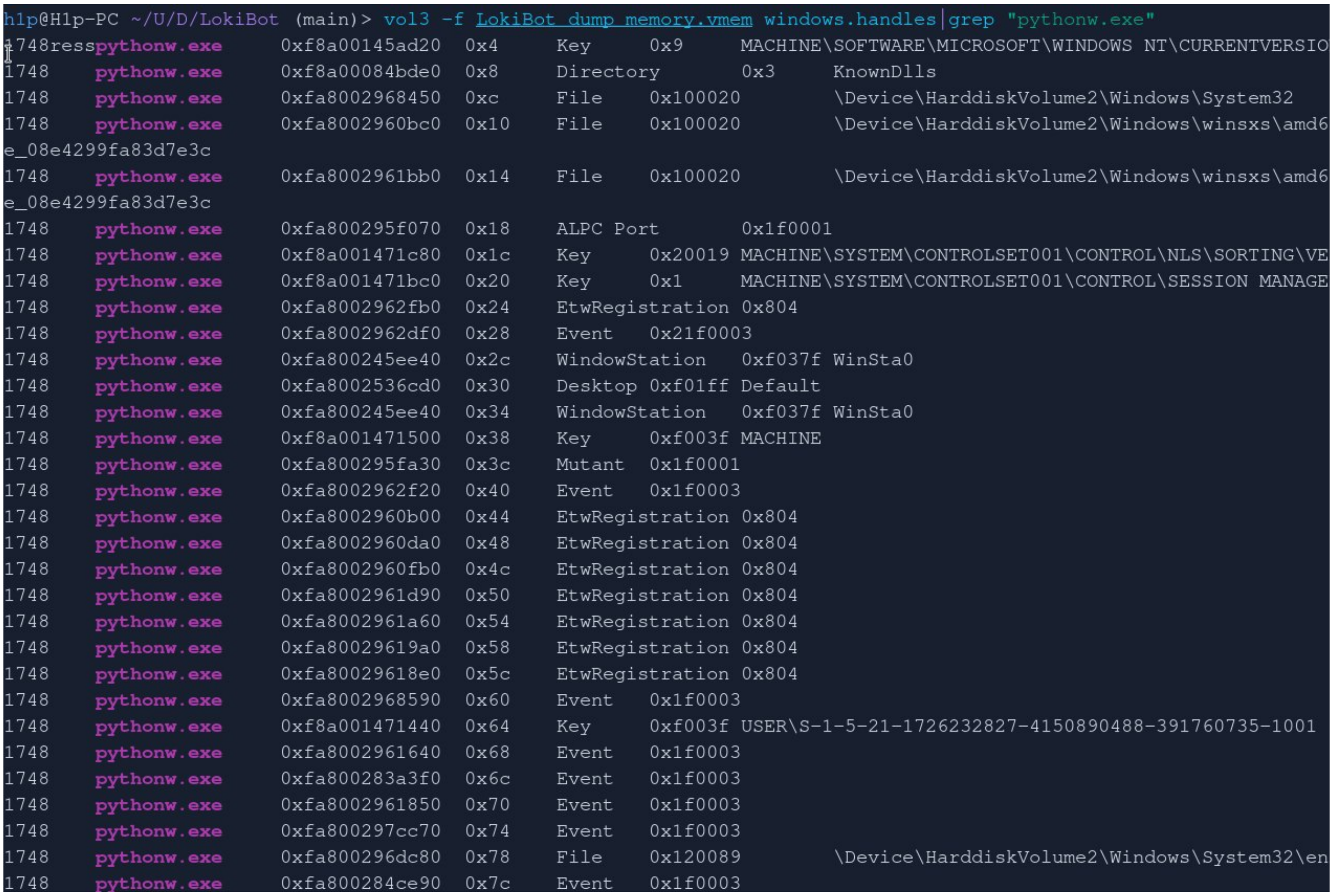
```
vol3 -f LokiBot_dump_memory.vmem windows.cmdline
```



```
1092    spoolsv.exe     C:\Windows\System32\spoolsv.exe
1148    svchost.exe     C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork
1212    taskhost.exe    "taskhost.exe"
1248    dwm.exe Required memory at 0x1424ee is inaccessible (swapped)
1272    explorer.exe    C:\Windows\Explorer.EXE
1440    efsui.exe       Required memory at 0x7fffffdf020 is inaccessible (swapped)
1740    VBoxTray.exe    "C:\Windows\System32\VBoxTray.exe"
1748    pythonw.exe     "C:\Python27\pythonw.exe" "C:\Users\John\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\agent.pyw"
2020    svchost.exe     C:\Windows\system32\svchost.exe -k NetworkServiceNetworkRestricted
1128    SearchIndexer.  C:\Windows\system32\SearchIndexer.exe /Embedding
2116    wmpnetwk.exe    "C:\Program Files\Windows Media Player\wmpnetwk.exe"
```

Aceste handle-uri includ ferestre, fișiere, procese și alte obiecte gestionate de sistemul de operare.

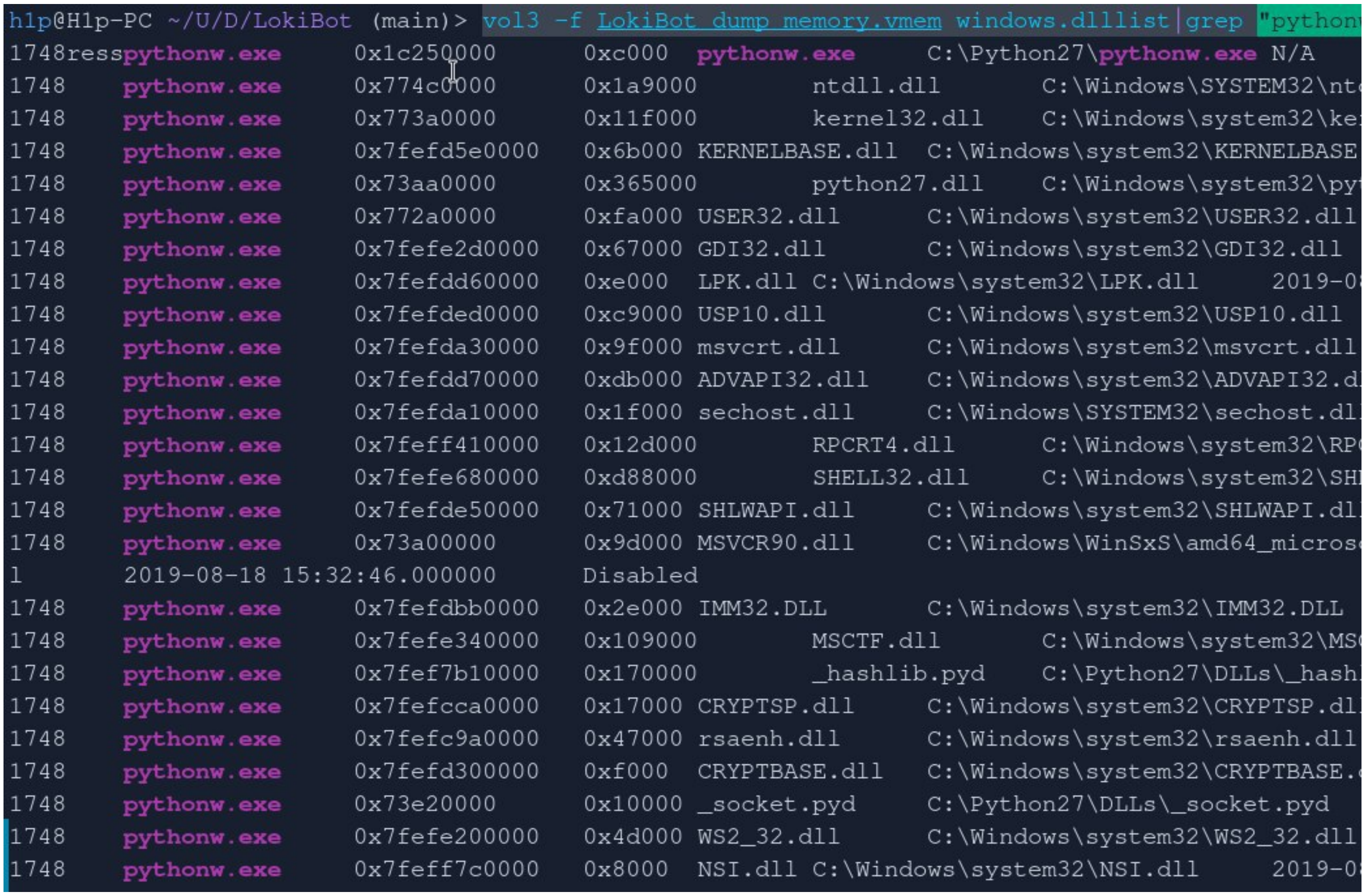
```
vol3 -f LokiBot_dump_memory.vmem windows.handles|grep
"pythonw.exe"
```



```
h1p@H1p-PC ~/U/D/LokiBot (main)> vol3 -f LokiBot_dump_memory.vmem windows.handles|grep "pythonw.exe"
1748resspythonw.exe     0xf8a00145ad20  0x4     Key     0x9     MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSIO
1748    pythonw.exe     0xf8a00084bde0  0x8     Directory       0x3     KnownDlls
1748    pythonw.exe     0xfa8002968450  0xc     File    0x100020        \Device\HarddiskVolume2\Windows\System32
1748    pythonw.exe     0xfa8002960bc0  0x10    File    0x100020        \Device\HarddiskVolume2\Windows\winsxs\amd6
e_08e4299fa83d7e3c
1748    pythonw.exe     0xfa8002961bb0  0x14    File    0x100020        \Device\HarddiskVolume2\Windows\winsxs\amd6
e_08e4299fa83d7e3c
1748    pythonw.exe     0xfa800295f070  0x18    ALPC Port       0x1f0001
1748    pythonw.exe     0xf8a001471c80  0x1c    Key     0x20019 MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\SORTING\VE
1748    pythonw.exe     0xf8a001471bc0  0x20    Key     0x1     MACHINE\SYSTEM\CONTROLSET001\CONTROL\SESSION MANAGE
1748    pythonw.exe     0xfa8002962fb0  0x24    EtwRegistration 0x804
1748    pythonw.exe     0xfa8002962df0  0x28    Event   0x21f0003
1748    pythonw.exe     0xfa800245ee40  0x2c    WindowStation   0xf037f WinSta0
1748    pythonw.exe     0xfa8002536cd0  0x30    Desktop 0xf01ff Default
1748    pythonw.exe     0xfa800245ee40  0x34    WindowStation   0xf037f WinSta0
1748    pythonw.exe     0xf8a001471500  0x38    Key     0xf003f MACHINE
1748    pythonw.exe     0xfa800295fa30  0x3c    Mutant  0x1f0001
1748    pythonw.exe     0xfa8002962f20  0x40    Event   0x1f0003
1748    pythonw.exe     0xfa8002960b00  0x44    EtwRegistration 0x804
1748    pythonw.exe     0xfa8002960da0  0x48    EtwRegistration 0x804
1748    pythonw.exe     0xfa8002960fb0  0x4c    EtwRegistration 0x804
1748    pythonw.exe     0xfa8002961d90  0x50    EtwRegistration 0x804
1748    pythonw.exe     0xfa8002961a60  0x54    EtwRegistration 0x804
1748    pythonw.exe     0xfa80029619a0  0x58    EtwRegistration 0x804
1748    pythonw.exe     0xfa80029618e0  0x5c    EtwRegistration 0x804
1748    pythonw.exe     0xfa8002968590  0x60    Event   0x1f0003
1748    pythonw.exe     0xf8a001471440  0x64    Key     0xf003f USER\S-1-5-21-1726232827-4150890488-391760735-1001
1748    pythonw.exe     0xfa8002961640  0x68    Event   0x1f0003
1748    pythonw.exe     0xfa800283a3f0  0x6c    Event   0x1f0003
1748    pythonw.exe     0xfa8002961850  0x70    Event   0x1f0003
1748    pythonw.exe     0xfa800297cc70  0x74    Event   0x1f0003
1748    pythonw.exe     0xfa800296dc80  0x78    File    0x120089        \Device\HarddiskVolume2\Windows\System32\en
1748    pythonw.exe     0xfa800284ce90  0x7c    Event   0x1f0003
```

Verificam toate `dll` care sunt folosite pentru instansat noastra:

```
vol3 -f LokiBot_dump_memory.vmem windows.dlllist|grep
"pythonw.exe"
```



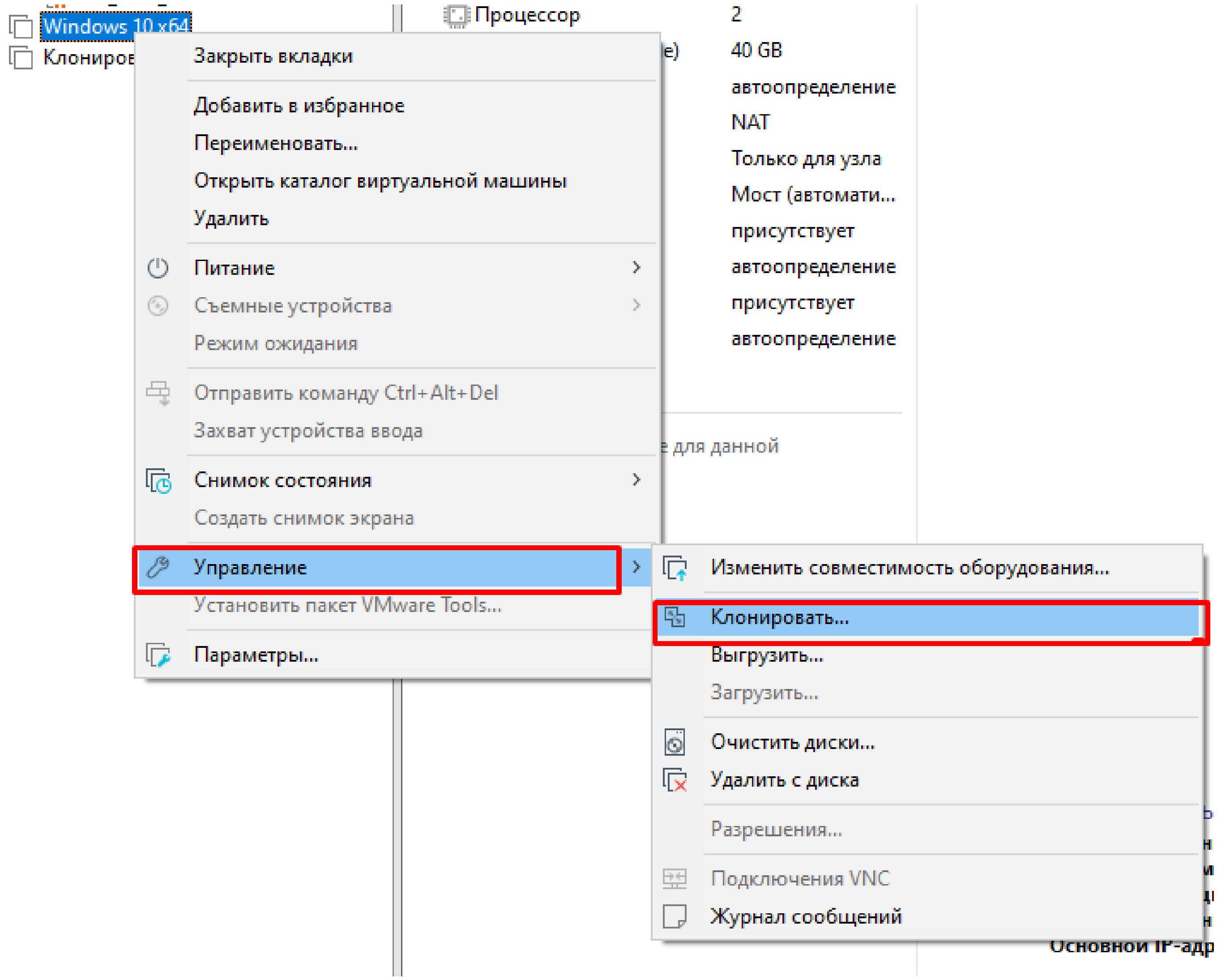
```
h1p@H1p-PC ~/U/D/LokiBot (main)> vol3 -f LokiBot_dump_memory.vmem windows.dlllist|grep "python
1748resspythonw.exe      0x1c250000      0xc000  pythonw.exe      C:\Python27\pythonw.exe N/A
1748    pythonw.exe      0x774c0000      0x1a9000        ntdll.dll       C:\Windows\SYSTEM32\nt
1748    pythonw.exe      0x773a0000      0x11f000        kernel32.dll    C:\Windows\system32\ke
1748    pythonw.exe      0x7fefd5e0000   0x6b000 KERNELBASE.dll  C:\Windows\system32\KERNELBASE
1748    pythonw.exe      0x73aa0000      0x365000        python27.dll    C:\Windows\system32\py
1748    pythonw.exe      0x772a0000      0xfa000 USER32.dll      C:\Windows\system32\USER32.dll
1748    pythonw.exe      0x7fefe2d0000   0x67000 GDI32.dll       C:\Windows\system32\GDI32.dll
1748    pythonw.exe      0x7fefdd60000   0xe000  LPK.dll C:\Windows\system32\LPK.dll     2019-0
1748    pythonw.exe      0x7fefded0000   0xc9000 USP10.dll       C:\Windows\system32\USP10.dll
1748    pythonw.exe      0x7fefda30000   0x9f000 msvcrt.dll      C:\Windows\system32\msvcrt.dll
1748    pythonw.exe      0x7fefdd70000   0xdb000 ADVAPI32.dll    C:\Windows\system32\ADVAPI32.d
1748    pythonw.exe      0x7fefda10000   0x1f000 sechost.dll     C:\Windows\SYSTEM32\sechost.dl
1748    pythonw.exe      0x7feff410000   0x12d000        RPCRT4.dll      C:\Windows\system32\RP
1748    pythonw.exe      0x7fefe680000   0xd88000        SHELL32.dll     C:\Windows\system32\SH
1748    pythonw.exe      0x7fefde50000   0x71000 SHLWAPI.dll     C:\Windows\system32\SHLWAPI.dl
1748    pythonw.exe      0x73a00000      0x9d000 MSVCR90.dll     C:\Windows\WinSxS\amd64_micros
1       2019-08-18 15:32:46.000000      Disabled
1748    pythonw.exe      0x7fefdbb0000   0x2e000 IMM32.DLL       C:\Windows\system32\IMM32.DLL
1748    pythonw.exe      0x7fefe340000   0x109000        MSCTF.dll       C:\Windows\system32\MS
1748    pythonw.exe      0x7fef7b10000   0x170000        _hashlib.pyd    C:\Python27\DLLs\_hash
1748    pythonw.exe      0x7fefcca0000   0x17000 CRYPTSP.dll     C:\Windows\system32\CRYPTSP.dl
1748    pythonw.exe      0x7fefc9a0000   0x47000 rsaenh.dll      C:\Windows\system32\rsaenh.dll
1748    pythonw.exe      0x7fefd300000   0xf000  CRYPTBASE.dll   C:\Windows\system32\CRYPTBASE.
1748    pythonw.exe      0x73e20000      0x10000 _socket.pyd     C:\Python27\DLLs\_socket.pyd
1748    pythonw.exe      0x7fefe200000   0x4d000 WS2_32.dll      C:\Windows\system32\WS2_32.dll
1748    pythonw.exe      0x7feff7c0000   0x8000  NSI.dll C:\Windows\system32\NSI.dll     2019-0
```

Avem drumul absolut

```
2444    pythonw.exe     0x1c250000      0xc000
pythonw.exe     C:\Python27\pythonw.exe N/A     Disabled
```

Analiza memorie hard

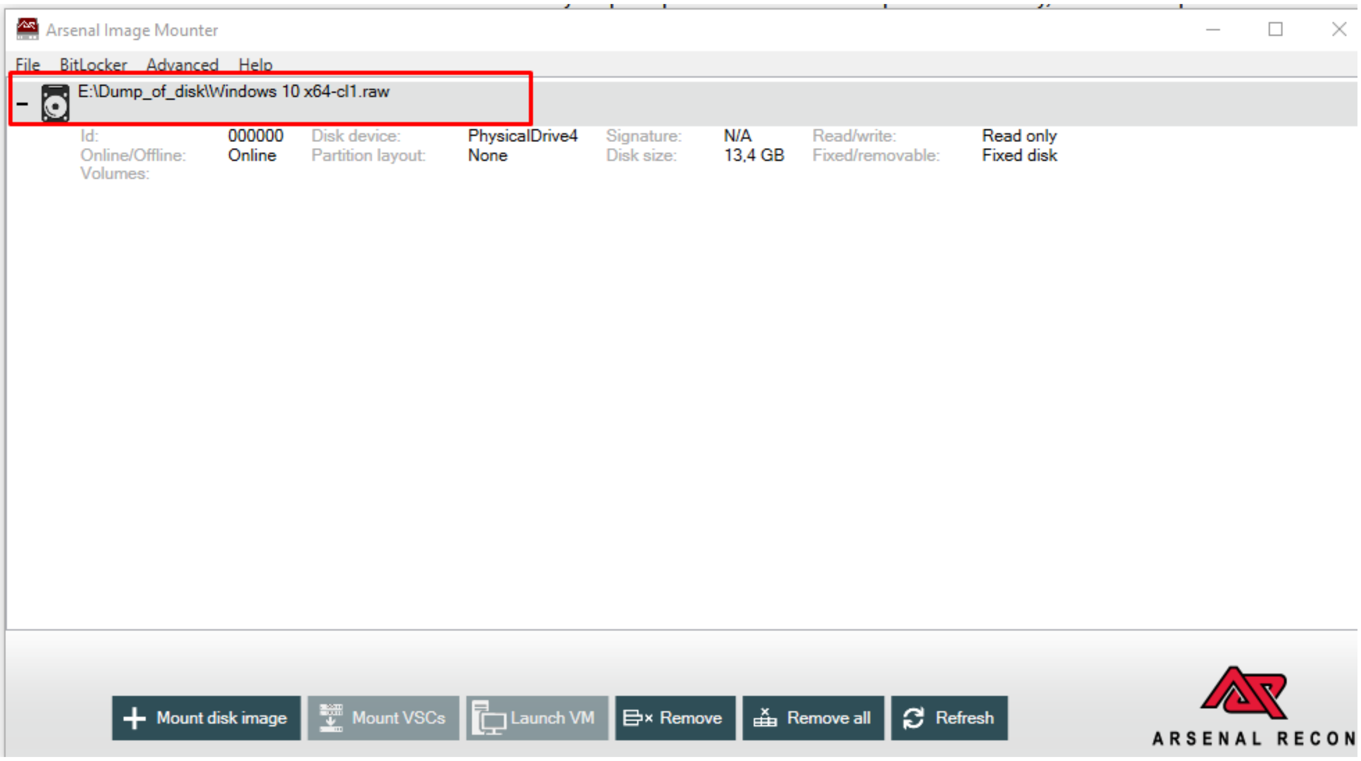
Cloname masina virtuala:



Transformam din extensia de `.vmdk` in `.raw`:

```
vmware-vdiskmanager -r "D:\VirtualMachine\Clone
Win10\Windows 10 x64-cl1.vmdk" -t 0
"E:\Dump_of_disk\Windows 10 x64-cl1.raw"
```

Montam discul nostru:



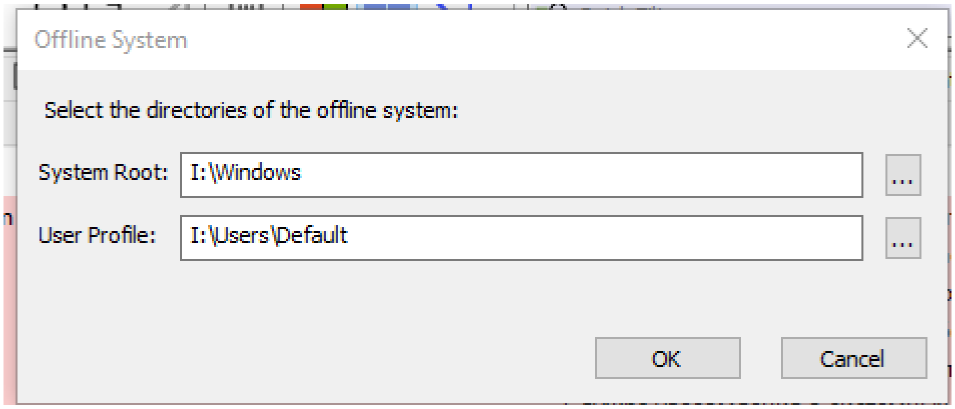
E:\Dump_of_disk\Windows 10 x64-cl1.raw

Id: 000000 Disk device: PhysicalDrive4 Signature: N/A Read/write: Read only

Online/Offline: Online Partition layout: None Disk size: 13,4 GB Fixed/removable: Fixed disk

Volumes:

Urmatorul pas este sa analizam discul nostru offline in putem face asta cu autorun:

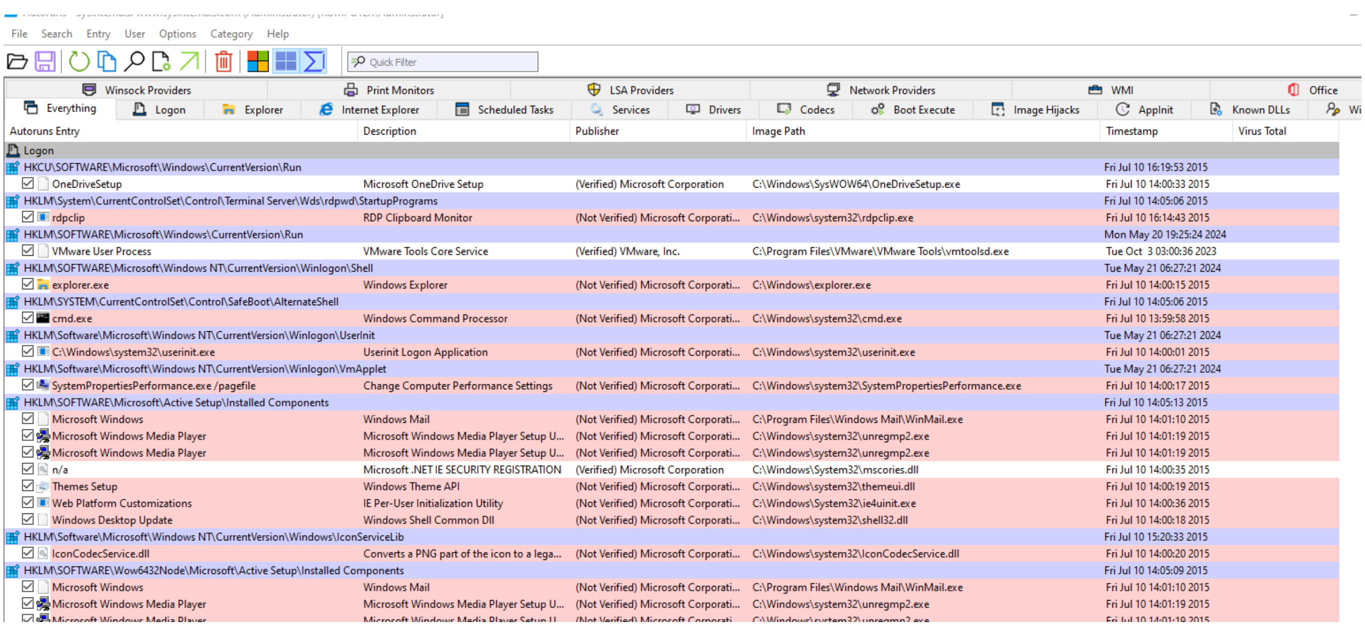


Select the directories of the offline system:

System Root: I:\Windows

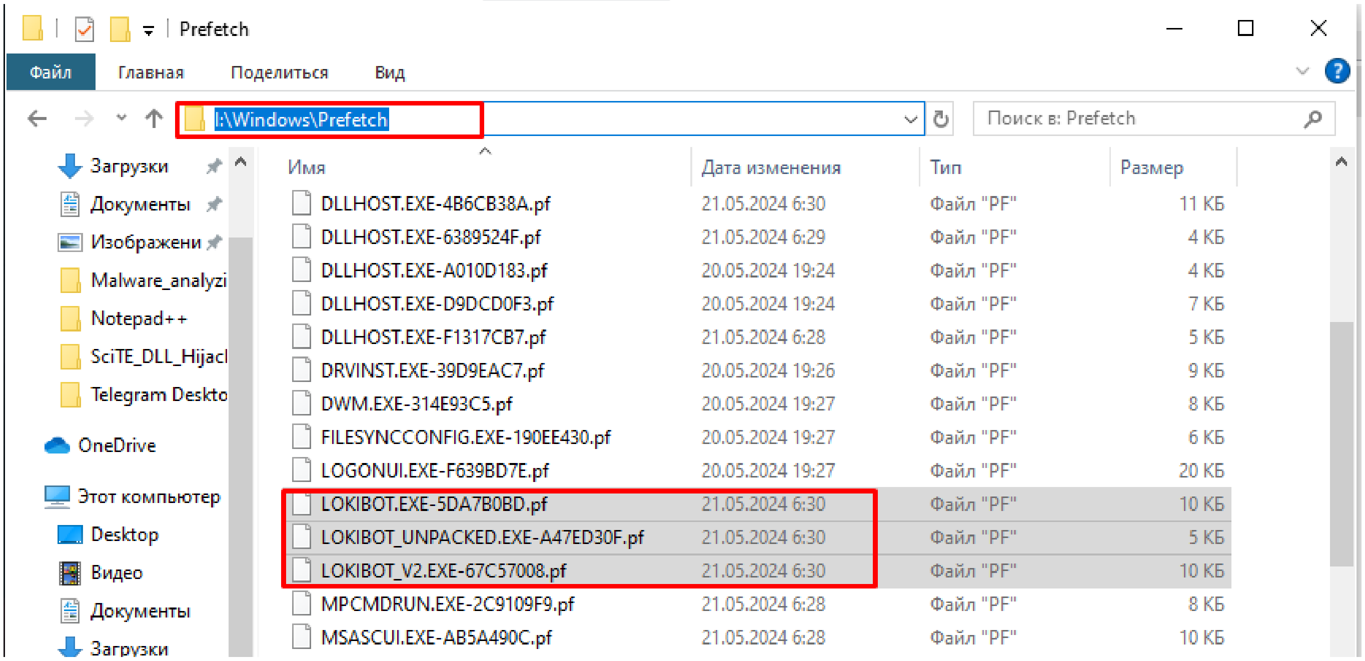
User Profile: I:\Users\Default

Dupa un tip de timp avem schimbarile care sau produs in sistema:



Autoruns Entry	Description	Publisher	Image Path	Timestamp	Virus Total
Logon					
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				Fri Jul 10 16:19:53 2015	
☑ OneDriveSetup	Microsoft OneDrive Setup	(Verified) Microsoft Corporation	C:\Windows\SysWOW64\OneDriveSetup.exe	Fri Jul 10 14:00:33 2015	
HKLM\System\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\StartupPrograms				Fri Jul 10 14:05:06 2015	
☑ rdpclip	RDP Clipboard Monitor	(Not Verified) Microsoft Corporati...	C:\Windows\system32\rdpclip.exe	Fri Jul 10 16:14:43 2015	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				Mon May 20 19:25:24 2024	
☑ VMware User Process	VMware Tools Core Service	(Verified) VMware, Inc.	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	Tue Oct 3 03:00:36 2023	
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell				Tue May 21 06:27:21 2024	
☑ explorer.exe	Windows Explorer	(Not Verified) Microsoft Corporati...	C:\Windows\explorer.exe	Fri Jul 10 14:00:15 2015	
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				Fri Jul 10 14:05:06 2015	
☑ cmd.exe	Windows Command Processor	(Not Verified) Microsoft Corporati...	C:\Windows\system32\cmd.exe	Fri Jul 10 13:59:58 2015	
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\UserInit				Tue May 21 06:27:21 2024	
☑ C:\Windows\system32\userinit.exe	Userinit Logon Application	(Not Verified) Microsoft Corporati...	C:\Windows\system32\userinit.exe	Fri Jul 10 14:00:01 2015	
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\VmApplet				Tue May 21 06:27:21 2024	
☑ SystemPropertiesPerformance.exe /pagefile	Change Computer Performance Settings	(Not Verified) Microsoft Corporati...	C:\Windows\system32\SystemPropertiesPerformance.exe	Fri Jul 10 14:00:17 2015	
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				Fri Jul 10 14:05:13 2015	
☑ Microsoft Windows	Windows Mail	(Not Verified) Microsoft Corporati...	C:\Program Files\Windows Mail\WinMail.exe	Fri Jul 10 14:01:10 2015	
☑ Microsoft Windows Media Player	Microsoft Windows Media Player Setup U...	(Not Verified) Microsoft Corporati...	C:\Windows\system32\unregmp2.exe	Fri Jul 10 14:01:19 2015	
☑ Microsoft Windows Media Player	Microsoft Windows Media Player Setup U...	(Not Verified) Microsoft Corporati...	C:\Windows\system32\unregmp2.exe	Fri Jul 10 14:01:19 2015	
☑ n/a	Microsoft .NET IE SECURITY REGISTRATION	(Verified) Microsoft Corporation	C:\Windows\System32\mscories.dll	Fri Jul 10 14:00:35 2015	
☑ Themes Setup	Windows Theme API	(Not Verified) Microsoft Corporati...	C:\Windows\system32\themeui.dll	Fri Jul 10 14:00:19 2015	
☑ Web Platform Customizations	IE Per-User Initialization Utility	(Not Verified) Microsoft Corporati...	C:\Windows\System32\ie4uinit.exe	Fri Jul 10 14:00:36 2015	
☑ Windows Desktop Update	Windows Shell Common Dll	(Not Verified) Microsoft Corporati...	C:\Windows\system32\shell32.dll	Fri Jul 10 14:00:18 2015	
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows\IconServiceLib				Fri Jul 10 15:20:33 2015	
☑ IconCodecService.dll	Converts a PNG part of the icon to a lega...	(Not Verified) Microsoft Corporati...	C:\Windows\system32\IconCodecService.dll	Fri Jul 10 14:00:20 2015	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				Fri Jul 10 14:05:09 2015	
☑ Microsoft Windows	Windows Mail	(Not Verified) Microsoft Corporati...	C:\Program Files\Windows Mail\WinMail.exe	Fri Jul 10 14:01:10 2015	
☑ Microsoft Windows Media Player	Microsoft Windows Media Player Setup U...	(Not Verified) Microsoft Corporati...	C:\Windows\system32\unregmp2.exe	Fri Jul 10 14:01:19 2015	
☑ Microsoft Windows Media Player	Microsoft Windows Media Player Setup U...	(Not Verified) Microsoft Corporati...	C:\Windows\system32\unregmp2.exe	Fri Jul 10 14:01:19 2015	

Localizarea fisierilor din `Prefetch`:

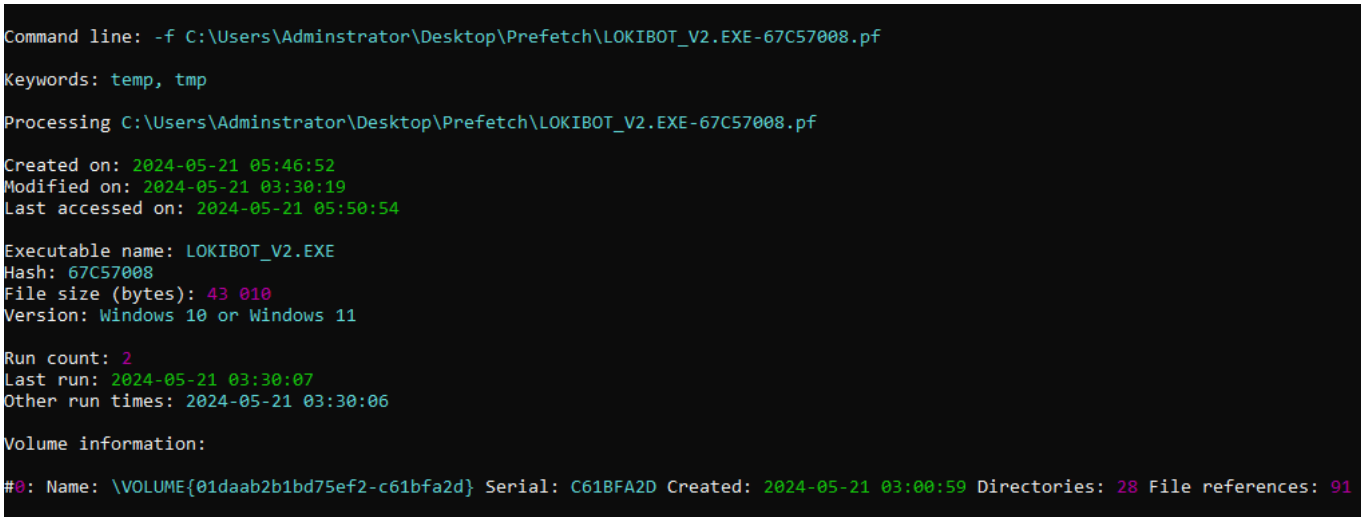


I:\Windows\Prefetch

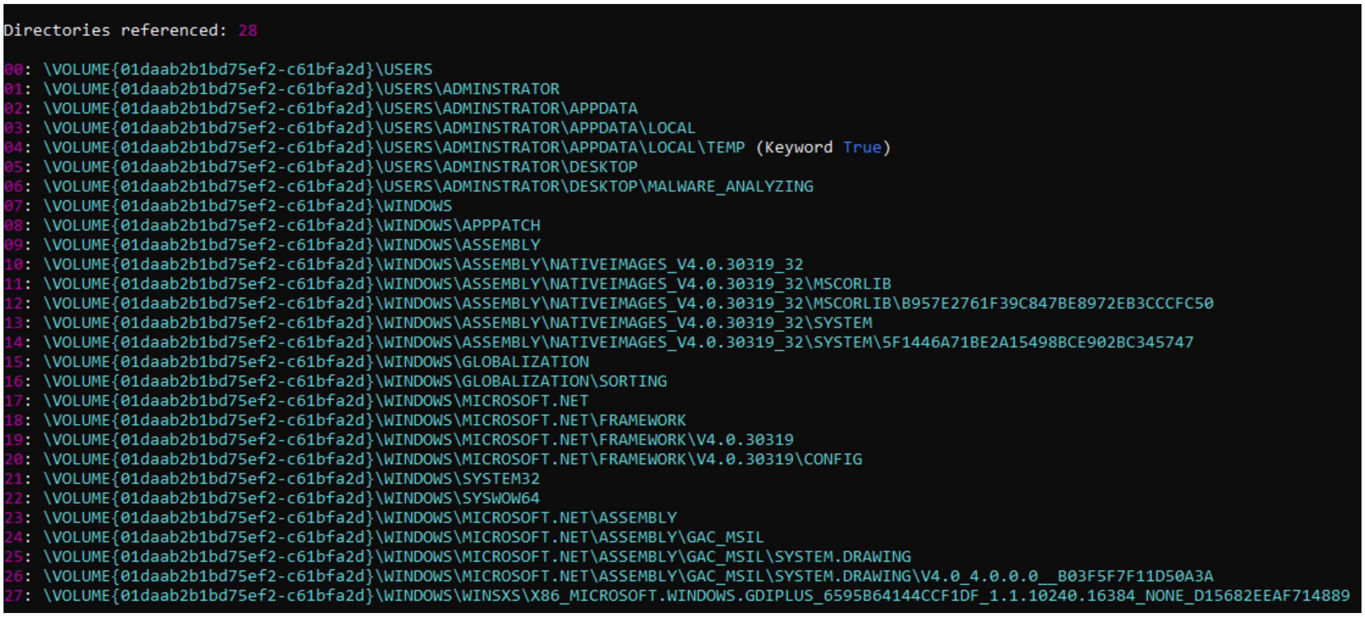
Имя	Дата изменения	Тип	Размер
DLLHOST.EXE-4B6CB38A.pf	21.05.2024 6:30	Файл "PF"	11 КБ
DLLHOST.EXE-6389524F.pf	21.05.2024 6:29	Файл "PF"	4 КБ
DLLHOST.EXE-A010D183.pf	20.05.2024 19:24	Файл "PF"	4 КБ
DLLHOST.EXE-D9DCD0F3.pf	20.05.2024 19:24	Файл "PF"	7 КБ
DLLHOST.EXE-F1317CB7.pf	21.05.2024 6:28	Файл "PF"	5 КБ
DRVINST.EXE-39D9EAC7.pf	20.05.2024 19:26	Файл "PF"	9 КБ
DWM.EXE-314E93C5.pf	20.05.2024 19:27	Файл "PF"	8 КБ
FILESYNCCONFIG.EXE-190EE430.pf	20.05.2024 19:27	Файл "PF"	6 КБ
LOGONUI.EXE-F639BD7E.pf	20.05.2024 19:27	Файл "PF"	20 КБ
LOKIBOT.EXE-5DA7B0BD.pf	21.05.2024 6:30	Файл "PF"	10 КБ
LOKIBOT_UNPACKED.EXE-A47ED30F.pf	21.05.2024 6:30	Файл "PF"	5 КБ
LOKIBOT_V2.EXE-67C57008.pf	21.05.2024 6:30	Файл "PF"	10 КБ
MPCMDRUN.EXE-2C9109F9.pf	21.05.2024 6:28	Файл "PF"	8 КБ
MSASCUI.EXE-AB5A490C.pf	21.05.2024 6:28	Файл "PF"	10 КБ

Analiza fisierilor `pf` din `Prefetch`:

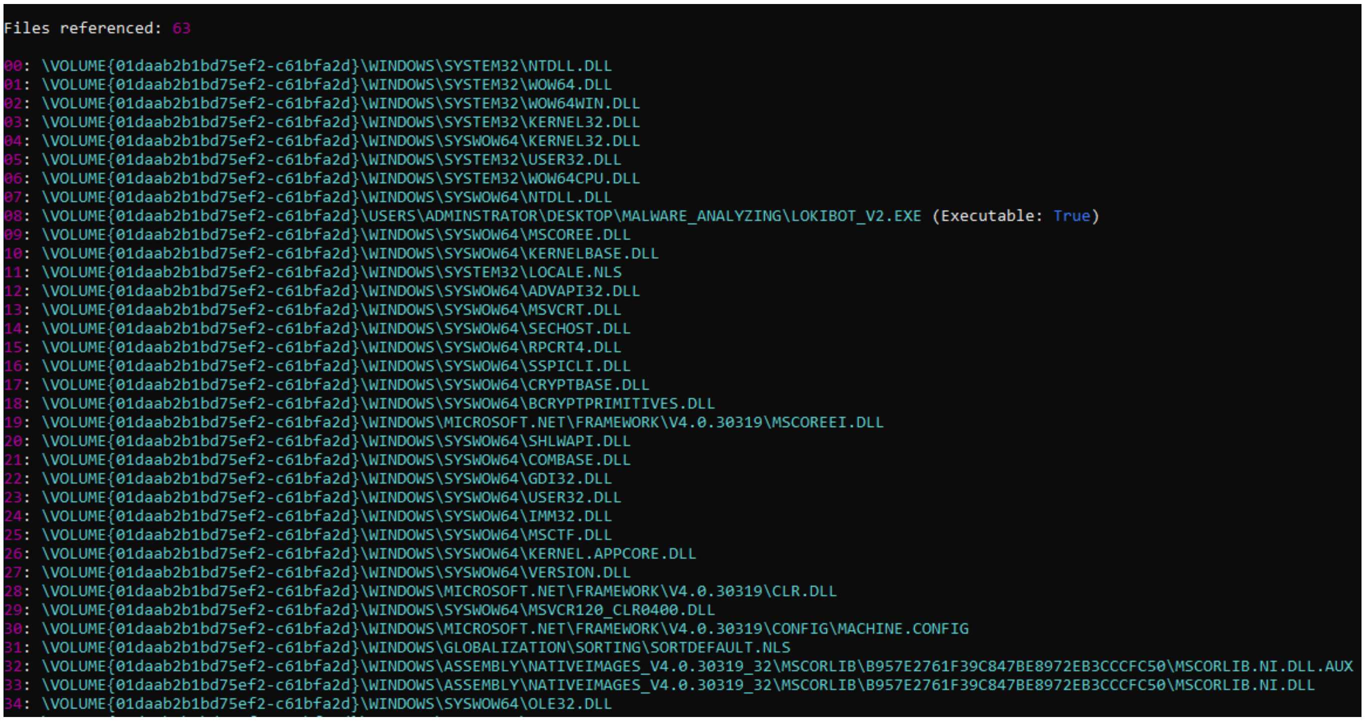
```
PECmd.exe -f
"C:\Users\Adminstrator\Desktop\Prefetch\LOKIBOT_V2.EXE-
67C57008.pf"
```



```
Command line: -f C:\Users\Adminstrator\Desktop\Prefetch\LOKIBOT_V2.EXE-67C57008.pf

Keywords: temp, tmp

Processing C:\Users\Adminstrator\Desktop\Prefetch\LOKIBOT_V2.EXE-67C57008.pf

Created on: 2024-05-21 05:46:52
Modified on: 2024-05-21 03:30:19
Last accessed on: 2024-05-21 05:50:54

Executable name: LOKIBOT_V2.EXE
Hash: 67C57008
File size (bytes): 43 010
Version: Windows 10 or Windows 11

Run count: 2
Last run: 2024-05-21 03:30:07
Other run times: 2024-05-21 03:30:06

Volume information:

#0: Name: \VOLUME{01daab2b1bd75ef2-c61bfa2d} Serial: C61BFA2D Created: 2024-05-21 03:00:59 Directories: 28 File references: 91
```



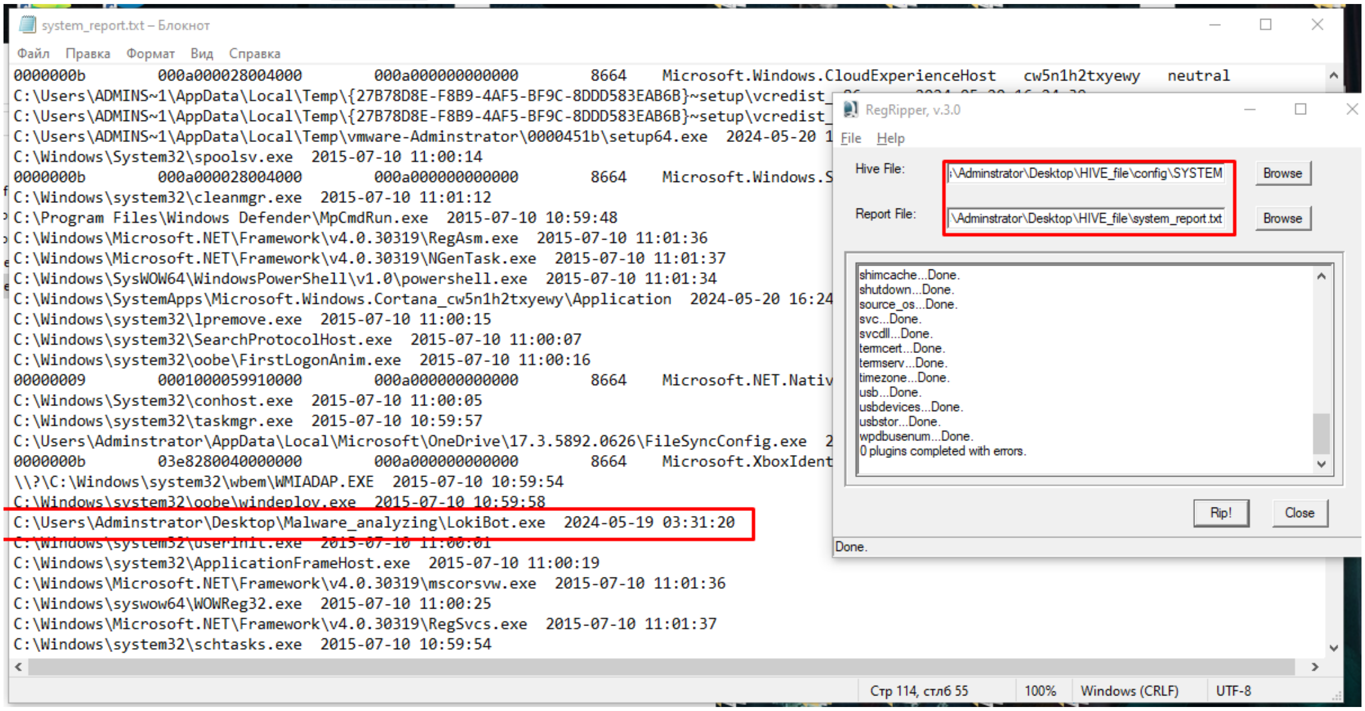
```
Directories referenced: 28

00: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\USERS
01: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\USERS\ADMINSTRATOR
02: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\USERS\ADMINSTRATOR\APPDATA
03: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\USERS\ADMINSTRATOR\APPDATA\LOCAL
04: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\USERS\ADMINSTRATOR\APPDATA\LOCAL\TEMP (Keyword True)
05: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\USERS\ADMINSTRATOR\DESKTOP
06: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\USERS\ADMINSTRATOR\DESKTOP\MALWARE_ANALYZING
07: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS
08: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\APPPATCH
09: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\ASSEMBLY
10: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\ASSEMBLY\NATIVEIMAGES_V4.0.30319_32
11: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\ASSEMBLY\NATIVEIMAGES_V4.0.30319_32\MSCORLIB
12: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\ASSEMBLY\NATIVEIMAGES_V4.0.30319_32\MSCORLIB\B957E2761F39C847BE8972EB3CCCFC50
13: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\ASSEMBLY\NATIVEIMAGES_V4.0.30319_32\SYSTEM
14: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\ASSEMBLY\NATIVEIMAGES_V4.0.30319_32\SYSTEM\5F1446A71BE2A15498BCE902BC345747
15: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\GLOBALIZATION
16: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\GLOBALIZATION\SORTING
17: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\MICROSOFT.NET
18: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\MICROSOFT.NET\FRAMEWORK
19: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\MICROSOFT.NET\FRAMEWORK\V4.0.30319
20: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\MICROSOFT.NET\FRAMEWORK\V4.0.30319\CONFIG
21: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\SYSTEM32
22: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\SYSWOW64
23: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\MICROSOFT.NET\ASSEMBLY
24: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\MICROSOFT.NET\ASSEMBLY\GAC_MSIL
25: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\MICROSOFT.NET\ASSEMBLY\GAC_MSIL\SYSTEM.DRAWING
26: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\MICROSOFT.NET\ASSEMBLY\GAC_MSIL\SYSTEM.DRAWING\V4.0_4.0.0.0__B03F5F7F11D50A3A
27: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\WINSXS\X86_MICROSOFT.WINDOWS.GDIPLUS_6595B64144CCF1DF_1.1.10240.16384_NONE_D15682EEAF714889
```



```
Files referenced: 63

00: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\SYSTEM32\NTDLL.DLL
01: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\SYSTEM32\WOW64.DLL
02: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\SYSTEM32\WOW64WIN.DLL
03: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\SYSTEM32\KERNEL32.DLL
04: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\SYSWOW64\KERNEL32.DLL
05: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\SYSTEM32\USER32.DLL
06: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\SYSTEM32\WOW64CPU.DLL
07: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\SYSWOW64\NTDLL.DLL
08: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\USERS\ADMINSTRATOR\DESKTOP\MALWARE_ANALYZING\LOKIBOT_V2.EXE (Executable: True)
09: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\SYSWOW64\MSCOREE.DLL
10: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\SYSWOW64\KERNELBASE.DLL
11: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\SYSTEM32\LOCALE.NLS
12: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\SYSWOW64\ADVAPI32.DLL
13: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\SYSWOW64\MSVCRT.DLL
14: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\SYSWOW64\SECHOST.DLL
15: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\SYSWOW64\RPCRT4.DLL
16: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\SYSWOW64\SSPICLI.DLL
17: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\SYSWOW64\CRYPTBASE.DLL
18: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\SYSWOW64\BCRYPTPRIMITIVES.DLL
19: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\MICROSOFT.NET\FRAMEWORK\V4.0.30319\MSCOREEI.DLL
20: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\SYSWOW64\SHLWAPI.DLL
21: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\SYSWOW64\COMBASE.DLL
22: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\SYSWOW64\GDI32.DLL
23: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\SYSWOW64\USER32.DLL
24: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\SYSWOW64\IMM32.DLL
25: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\SYSWOW64\MSCTF.DLL
26: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\SYSWOW64\KERNEL.APPCORE.DLL
27: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\SYSWOW64\VERSION.DLL
28: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\MICROSOFT.NET\FRAMEWORK\V4.0.30319\CLR.DLL
29: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\SYSWOW64\MSVCR120_CLR0400.DLL
30: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\MICROSOFT.NET\FRAMEWORK\V4.0.30319\CONFIG\MACHINE.CONFIG
31: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\GLOBALIZATION\SORTING\SORTDEFAULT.NLS
32: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\ASSEMBLY\NATIVEIMAGES_V4.0.30319_32\MSCORLIB\B957E2761F39C847BE8972EB3CCCFC50\MSCORLIB.NI.DLL.AUX
33: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\ASSEMBLY\NATIVEIMAGES_V4.0.30319_32\MSCORLIB\B957E2761F39C847BE8972EB3CCCFC50\MSCORLIB.NI.DLL
34: \VOLUME{01daab2b1bd75ef2-c61bfa2d}\WINDOWS\SYSWOW64\OLE32.DLL
```

Pentru a înțelege mai bine comportamentul aplicațiilor.

Analiza fisierilor `HIVE` care:



system_report.txt – Блокнот

```
0000000b        000a000028004000        000a000000000000        8664    Microsoft.Windows.CloudExperienceHost   cw5n1h2txyewy   neutral
C:\Users\ADMINS~1\AppData\Local\Temp\{27B78D8E-F8B9-4AF5-BF9C-8DDD583EAB6B}~setup\vcredist_
C:\Users\ADMINS~1\AppData\Local\Temp\{27B78D8E-F8B9-4AF5-BF9C-8DDD583EAB6B}~setup\vcredist_
C:\Users\ADMINS~1\AppData\Local\Temp\vmware-Adminstrator\0000451b\setup64.exe  2024-05-20 1
C:\Windows\System32\spoolsv.exe  2015-07-10 11:00:14
0000000b        000a000028004000        000a000000000000        8664    Microsoft.Windows.S
C:\Windows\system32\cleanmgr.exe  2015-07-10 11:01:12
C:\Program Files\Windows Defender\MpCmdRun.exe  2015-07-10 10:59:48
C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe  2015-07-10 11:01:36
C:\Windows\Microsoft.NET\Framework\v4.0.30319\NGenTask.exe  2015-07-10 11:01:37
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe  2015-07-10 11:01:34
C:\Windows\SystemApps\Microsoft.Windows.Cortana_cw5n1h2txyewy\Application  2024-05-20 16:24
C:\Windows\system32\lpremove.exe  2015-07-10 11:00:15
C:\Windows\system32\SearchProtocolHost.exe  2015-07-10 11:00:07
C:\Windows\system32\oobe\FirstLogonAnim.exe  2015-07-10 11:00:16
00000009        0001000059910000        000a000000000000        8664    Microsoft.NET.Nativ
C:\Windows\System32\conhost.exe  2015-07-10 11:00:05
C:\Windows\system32\taskmgr.exe  2015-07-10 10:59:57
C:\Users\Adminstrator\AppData\Local\Microsoft\OneDrive\17.3.5892.0626\FileSyncConfig.exe  2
0000000b        03e8280040000000        000a000000000000        8664    Microsoft.XboxIdent
\\?\C:\Windows\system32\wbem\WMIADAP.EXE  2015-07-10 10:59:54
C:\Windows\system32\oobe\windeploy.exe  2015-07-10 10:59:58
C:\Users\Adminstrator\Desktop\Malware_analyzing\LokiBot.exe  2024-05-19 03:31:20
C:\Windows\system32\userinit.exe  2015-07-10 11:00:01
C:\Windows\system32\ApplicationFrameHost.exe  2015-07-10 11:00:19
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorsvw.exe  2015-07-10 11:01:36
C:\Windows\syswow64\WOWReg32.exe  2015-07-10 11:00:25
C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe  2015-07-10 11:01:37
C:\Windows\system32\schtasks.exe  2015-07-10 10:59:54
```

RegRipper, v.3.0

Hive File: :\Adminstrator\Desktop\HIVE_file\config\SYSTEM

Report File: \Adminstrator\Desktop\HIVE_file\system_report.txt

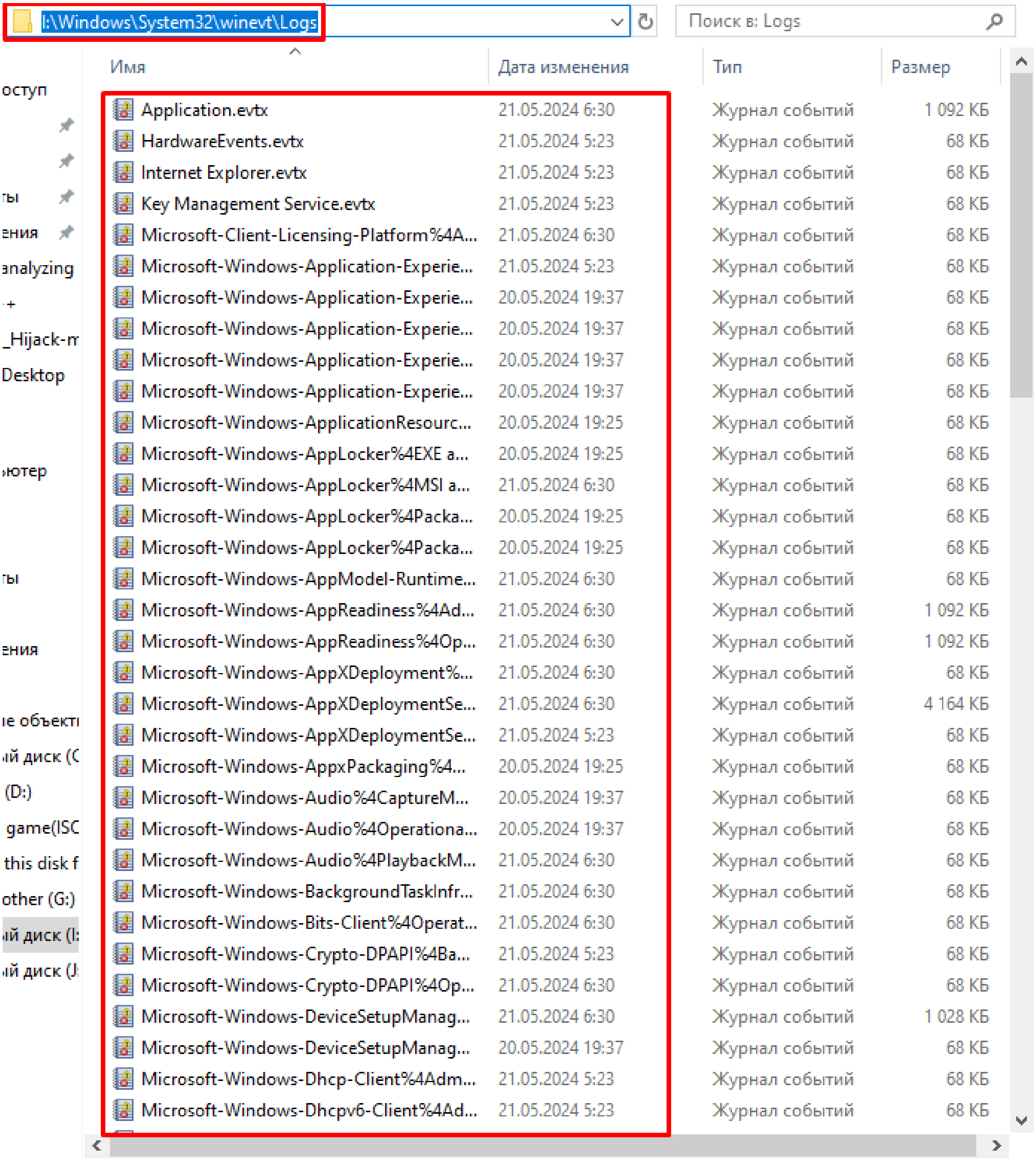
```
shimcache...Done.
shutdown...Done.
source_os...Done.
svc...Done.
svcdll...Done.
termcert...Done.
termserv...Done.
timezone...Done.
usb...Done.
usbdevices...Done.
usbstor...Done.
wpdbusenum...Done.
0 plugins completed with errors.
```

Done.

Din pacate informatie utila este doar data si cine a rulat fisierul.

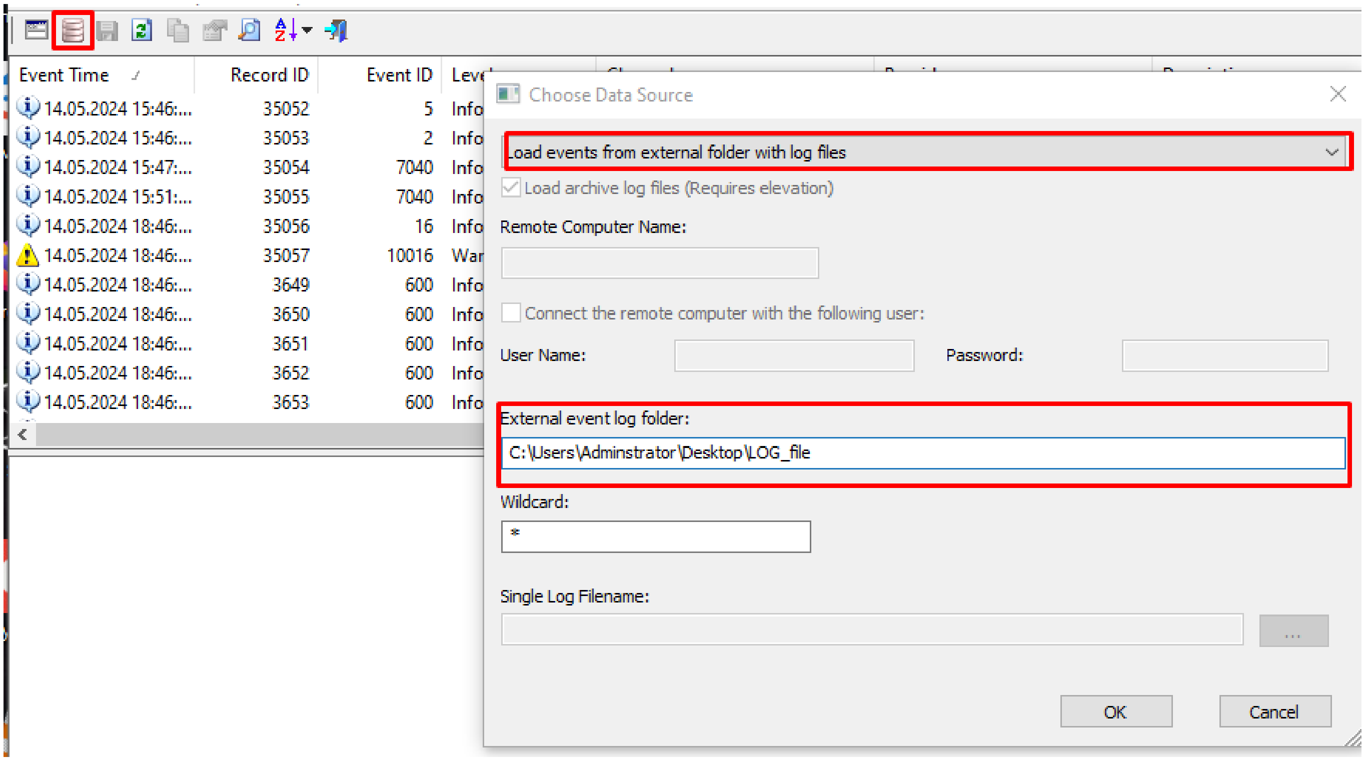
Analiza logurilor:

```
I:\Windows\System32\winevt\Logs
```



Имя	Дата изменения	Тип	Размер
Application.evtx	21.05.2024 6:30	Журнал событий	1 092 КБ
HardwareEvents.evtx	21.05.2024 5:23	Журнал событий	68 КБ
Internet Explorer.evtx	21.05.2024 5:23	Журнал событий	68 КБ
Key Management Service.evtx	21.05.2024 5:23	Журнал событий	68 КБ
Microsoft-Client-Licensing-Platform%4A...	21.05.2024 6:30	Журнал событий	68 КБ
Microsoft-Windows-Application-Experie...	21.05.2024 5:23	Журнал событий	68 КБ
Microsoft-Windows-Application-Experie...	20.05.2024 19:37	Журнал событий	68 КБ
Microsoft-Windows-Application-Experie...	20.05.2024 19:37	Журнал событий	68 КБ
Microsoft-Windows-Application-Experie...	20.05.2024 19:37	Журнал событий	68 КБ
Microsoft-Windows-Application-Experie...	20.05.2024 19:37	Журнал событий	68 КБ
Microsoft-Windows-ApplicationResourc...	20.05.2024 19:25	Журнал событий	68 КБ
Microsoft-Windows-AppLocker%4EXE a...	20.05.2024 19:25	Журнал событий	68 КБ
Microsoft-Windows-AppLocker%4MSI a...	21.05.2024 6:30	Журнал событий	68 КБ
Microsoft-Windows-AppLocker%4Packa...	20.05.2024 19:25	Журнал событий	68 КБ
Microsoft-Windows-AppLocker%4Packa...	20.05.2024 19:25	Журнал событий	68 КБ
Microsoft-Windows-AppModel-Runtime...	21.05.2024 6:30	Журнал событий	68 КБ
Microsoft-Windows-AppReadiness%4Ad...	21.05.2024 6:30	Журнал событий	1 092 КБ
Microsoft-Windows-AppReadiness%4Op...	21.05.2024 6:30	Журнал событий	1 092 КБ
Microsoft-Windows-AppXDeployment%...	21.05.2024 6:30	Журнал событий	68 КБ
Microsoft-Windows-AppXDeploymentSe...	21.05.2024 6:30	Журнал событий	4 164 КБ
Microsoft-Windows-AppXDeploymentSe...	21.05.2024 5:23	Журнал событий	68 КБ
Microsoft-Windows-AppxPackaging%4...	20.05.2024 19:25	Журнал событий	68 КБ
Microsoft-Windows-Audio%4CaptureM...	20.05.2024 19:37	Журнал событий	68 КБ
Microsoft-Windows-Audio%4Operationa...	20.05.2024 19:37	Журнал событий	68 КБ
Microsoft-Windows-Audio%4PlaybackM...	21.05.2024 6:30	Журнал событий	68 КБ
Microsoft-Windows-BackgroundTaskInfr...	21.05.2024 6:30	Журнал событий	68 КБ
Microsoft-Windows-Bits-Client%4Operat...	21.05.2024 6:30	Журнал событий	68 КБ
Microsoft-Windows-Crypto-DPAPI%4Ba...	21.05.2024 5:23	Журнал событий	68 КБ
Microsoft-Windows-Crypto-DPAPI%4Op...	21.05.2024 6:30	Журнал событий	68 КБ
Microsoft-Windows-DeviceSetupManag...	21.05.2024 6:30	Журнал событий	1 028 КБ
Microsoft-Windows-DeviceSetupManag...	20.05.2024 19:37	Журнал событий	68 КБ
Microsoft-Windows-Dhcp-Client%4Adm...	21.05.2024 5:23	Журнал событий	68 КБ
Microsoft-Windows-Dhcpv6-Client%4Ad...	21.05.2024 5:23	Журнал событий	68 КБ

Setam locatia pentru fisierile noastre de log:



Event Time	Record ID	Event ID	Leve
14.05.2024 15:46:...	35052	5	Info
14.05.2024 15:46:...	35053	2	Info
14.05.2024 15:47:...	35054	7040	Info
14.05.2024 15:51:...	35055	7040	Info
14.05.2024 18:46:...	35056	16	Info
14.05.2024 18:46:...	35057	10016	War
14.05.2024 18:46:...	3649	600	Info
14.05.2024 18:46:...	3650	600	Info
14.05.2024 18:46:...	3651	600	Info
14.05.2024 18:46:...	3652	600	Info
14.05.2024 18:46:...	3653	600	Info

Choose Data Source

Load events from external folder with log files

☑ Load archive log files (Requires elevation)

Remote Computer Name:

□ Connect the remote computer with the following user:

User Name: Password:

External event log folder:

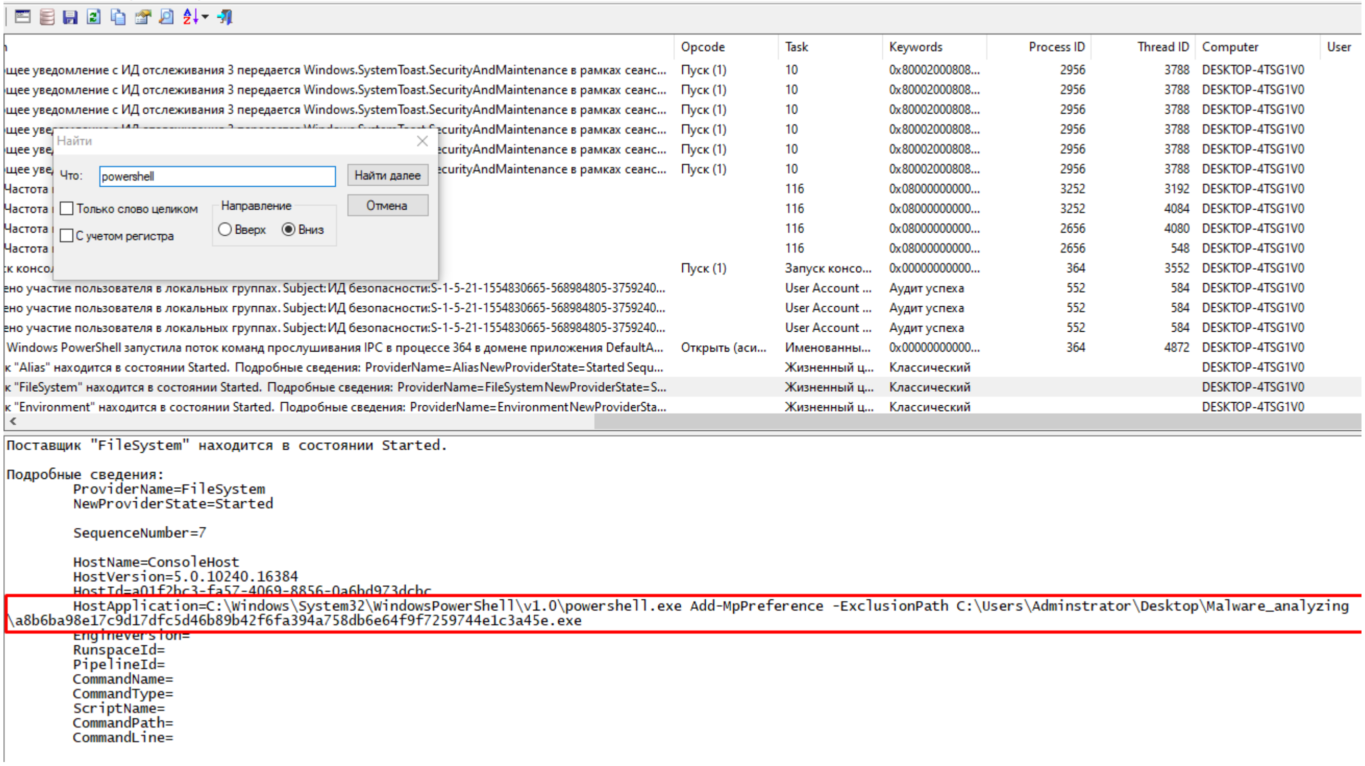
C:\Users\Adminstrator\Desktop\LOG_file

Wildcard:

*

Single Log Filename:

Lol am gasit cum am adaugat ca un dir sa nu fii scanat dar nu am gasit nimic despre `malware→lokibot` =(



h	Opcode	Task	Keywords	Process ID	Thread ID	Computer	User
щее уведомление с ИД отслеживания 3 передается Windows.SystemToast.SecurityAndMaintenance в рамках сеанс...	Пуск (1)	10	0x80002000808...	2956	3788	DESKTOP-4TSG1V0	
щее уведомление с ИД отслеживания 3 передается Windows.SystemToast.SecurityAndMaintenance в рамках сеанс...	Пуск (1)	10	0x80002000808...	2956	3788	DESKTOP-4TSG1V0	
щее уведомление с ИД отслеживания 3 передается Windows.SystemToast.SecurityAndMaintenance в рамках сеанс...	Пуск (1)	10	0x80002000808...	2956	3788	DESKTOP-4TSG1V0	
щее уве ... curityAndMaintenance в рамках сеанс...	Пуск (1)	10	0x80002000808...	2956	3788	DESKTOP-4TSG1V0	
щее уве ... curityAndMaintenance в рамках сеанс...	Пуск (1)	10	0x80002000808...	2956	3788	DESKTOP-4TSG1V0	
щее уве ... curityAndMaintenance в рамках сеанс...	Пуск (1)	10	0x80002000808...	2956	3788	DESKTOP-4TSG1V0	
Частота		116	0x08000000000...	3252	3192	DESKTOP-4TSG1V0	
Частота		116	0x08000000000...	3252	4084	DESKTOP-4TSG1V0	
Частота		116	0x08000000000...	2656	4080	DESKTOP-4TSG1V0	
Частота		116	0x08000000000...	2656	548	DESKTOP-4TSG1V0	
к консо	Пуск (1)	Запуск консо...	0x00000000000...	364	3552	DESKTOP-4TSG1V0	
ено участие пользователя в локальных группах. Subject:ИД безопасности:S-1-5-21-1554830665-568984805-3759240...		User Account ...	Аудит успеха	552	584	DESKTOP-4TSG1V0	
ено участие пользователя в локальных группах. Subject:ИД безопасности:S-1-5-21-1554830665-568984805-3759240...		User Account ...	Аудит успеха	552	584	DESKTOP-4TSG1V0	
ено участие пользователя в локальных группах. Subject:ИД безопасности:S-1-5-21-1554830665-568984805-3759240...		User Account ...	Аудит успеха	552	584	DESKTOP-4TSG1V0	
Windows PowerShell запустила поток команд прослушивания IPC в процессе 364 в домене приложения DefaultA...	Открыть (аси...	Именованны...	0x00000000000...	364	4872	DESKTOP-4TSG1V0	
к "Alias" находится в состоянии Started. Подробные сведения: ProviderName=AliasNewProviderState=Started Sequ...		Жизненный ц...	Классический			DESKTOP-4TSG1V0	
к "FileSystem" находится в состоянии Started. Подробные сведения: ProviderName=FileSystemNewProviderState=S...		Жизненный ц...	Классический			DESKTOP-4TSG1V0	
к "Environment" находится в состоянии Started. Подробные сведения: ProviderName=EnvironmentNewProviderSta...		Жизненный ц...	Классический			DESKTOP-4TSG1V0	

Найти

Что: powershell

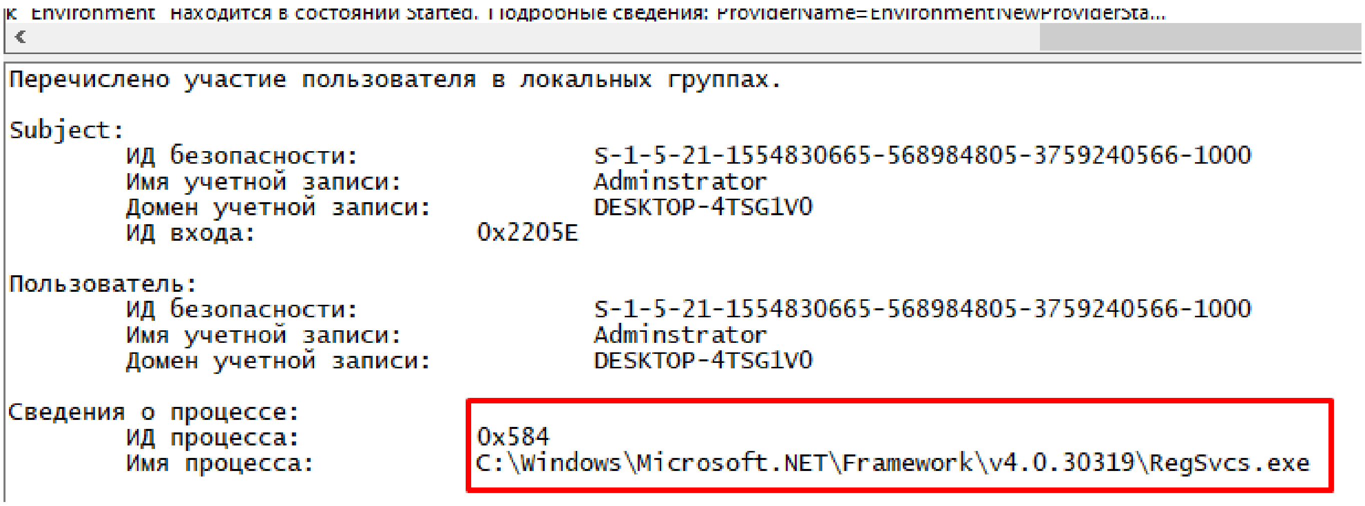
□ Только слово целиком

□ С учетом регистра

Направление: ○ Вверх ● Вниз

```
Поставщик "FileSystem" находится в состоянии Started.

Подробные сведения:
        ProviderName=FileSystem
        NewProviderState=Started

        SequenceNumber=7

        HostName=ConsoleHost
        HostVersion=5.0.10240.16384
        HostId=a01f2bc3-fa57-4069-8856-0a6bd973dcbc
        HostApplication=C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\Adminstrator\Desktop\Malware_analyzing
\a8b6ba98e17c9d17dfc5d46b89b42f6fa394a758db6e64f9f7259744e1c3a45e.exe
        EngineVersion=
        RunspaceId=
        PipelineId=
        CommandName=
        CommandType=
        ScriptName=
        CommandPath=
        CommandLine=
```

Presupunerea mea este ca acesta este procesul infectat:



```
k Environment  находится в состоянии Started. Подробные сведения: ProviderName=EnvironmentNewProviderSta...
```

```
Перечислено участие пользователя в локальных группах.

Subject:
        ИД безопасности:                S-1-5-21-1554830665-568984805-3759240566-1000
        Имя учетной записи:             Adminstrator
        Домен учетной записи:           DESKTOP-4TSG1V0
        ИД входа:               0x2205E

Пользователь:
        ИД безопасности:                S-1-5-21-1554830665-568984805-3759240566-1000
        Имя учетной записи:             Adminstrator
        Домен учетной записи:           DESKTOP-4TSG1V0

Сведения о процессе:
        ИД процесса:            0x584
        Имя процесса:           C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
```

Concluzie: În cele din urmă, deoarece prima versiune a malware-ului a fost scursă și clonată, devenind în cele din urmă disponibilă pentru un preț semnificativ mai mic decât originalul, Spyware-ul LokiBot a devenit un malware larg răspândit, care continuă să apară în mai multe campanii de mail-spam. De fapt, virusul a devenit atât de popular încât videoclipurile sale explicative de configurare privind furtul de acreditări sunt disponibile public pe YouTube.