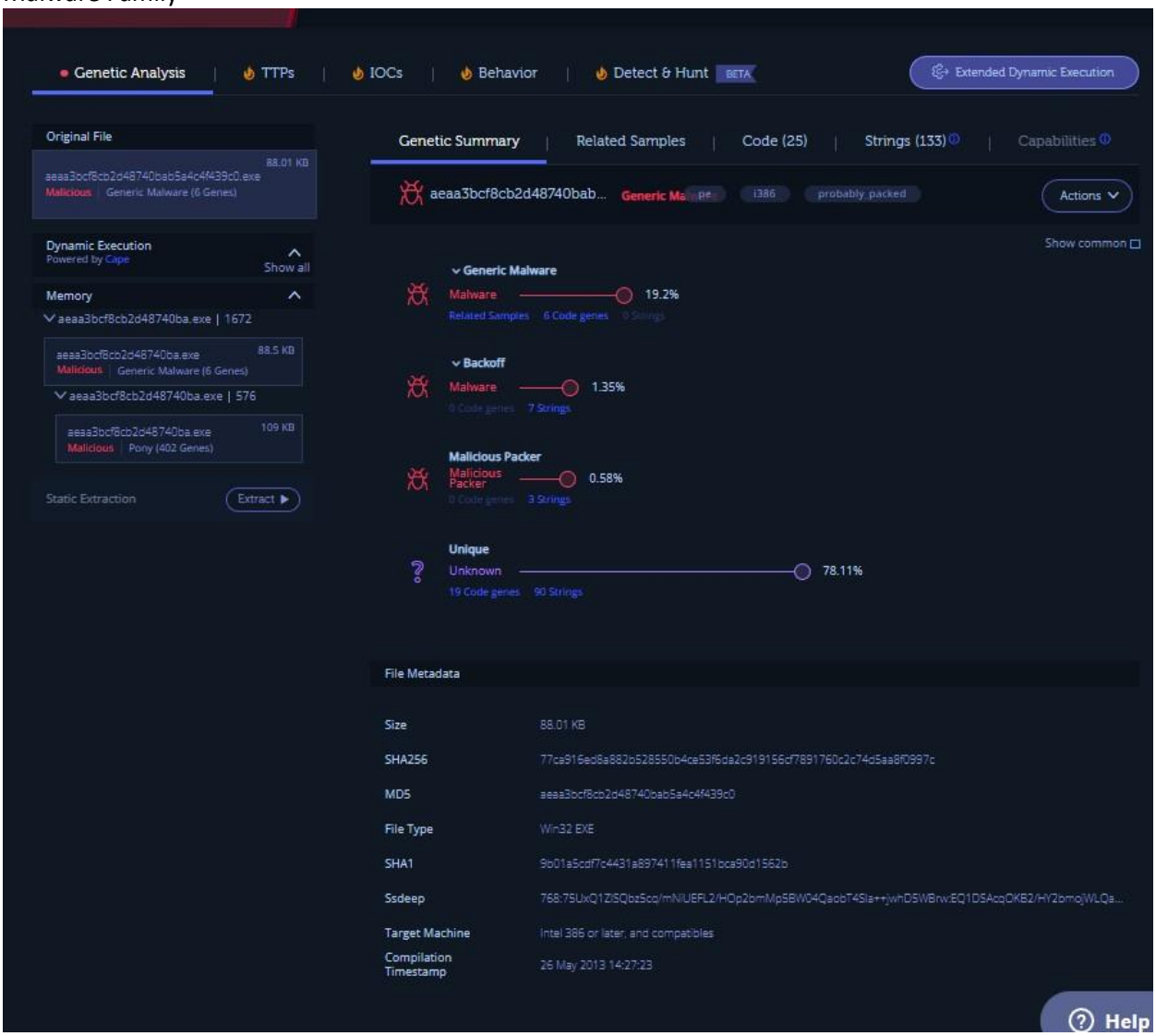
Malware Reverse Engineering- CSEC 743 : Reversing Project.

Nilesh Jakamputi, Msc. Information Technology and Analytics.

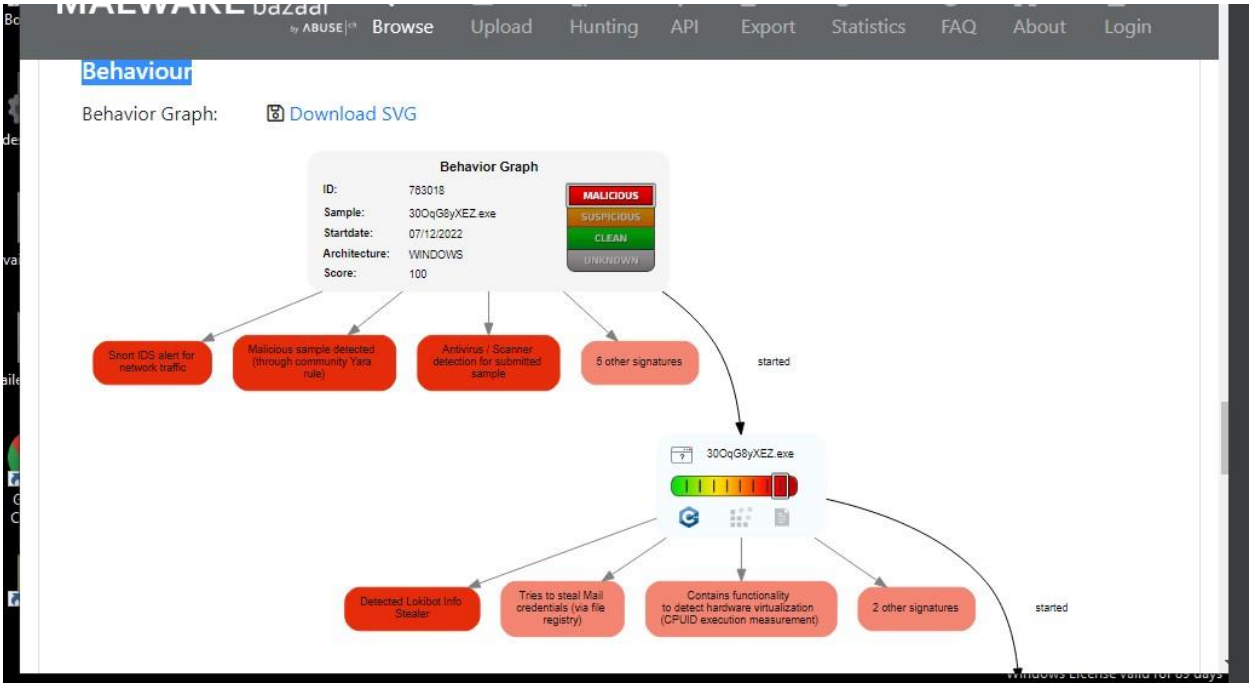
Select a malware program to analyze from one of the repositories listed above.

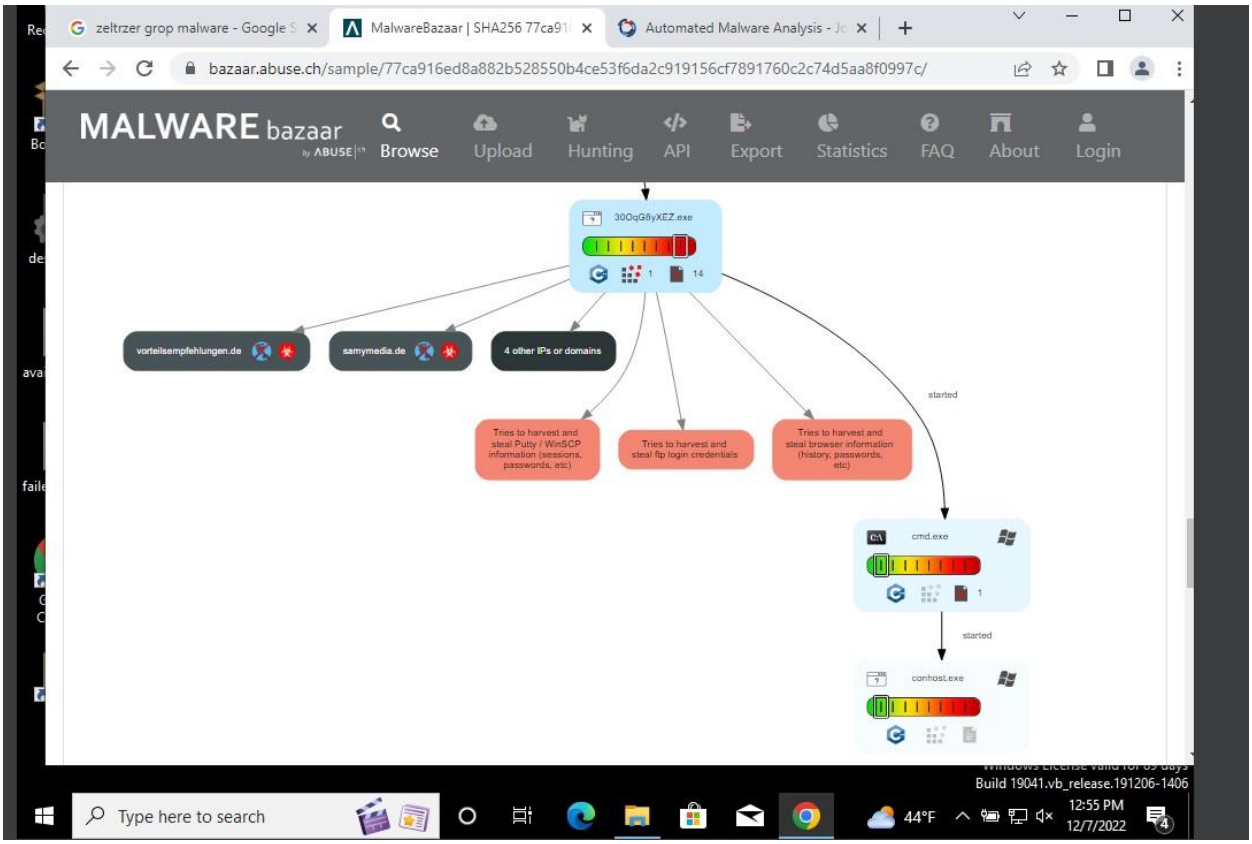
Malware Specimen- 300qg8yXEZ.exe
https://bazaar.abuse.ch/sample/77ca916ed8a882b528550b4ce53f6da2c919156cf7891760c2c74d5aa8f0997c/
Malware Family -



Unfortunate, that this is a mixture of a couple different families of malware, but it's mostly pony according to INTEZER ANALYZE, JOES sandbox etc.

Behaviour Overview – Grabbed from a few sandboxes – Basic Dynamic essentially.

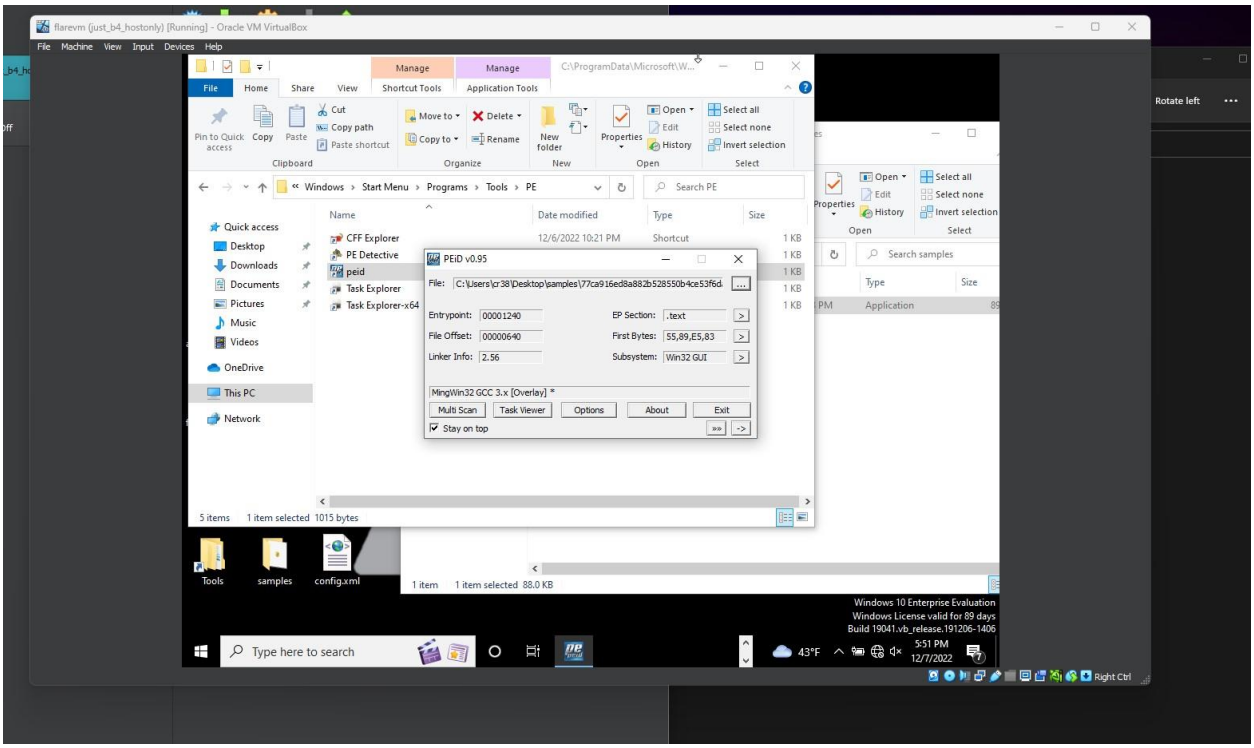


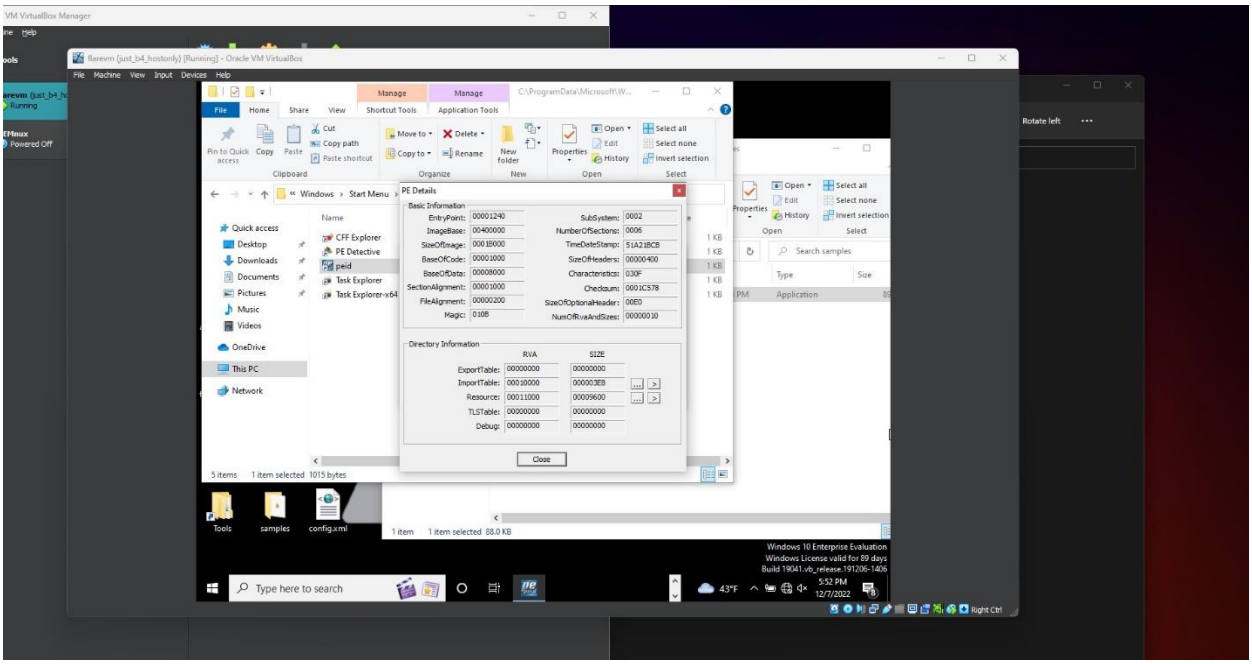


Basic Static Analysis of file titled -
77ca916ed8a882b528550b4ce53f6da2c919156cf7891760c2c74d5aa8f0997c.exe

Tools used for Basic static phase -
Strings[Standalone version, IDA strings], PEID, Dependency Walker, Cff explorer 8 , FLOSS[nothing to deobfuscate in static, all dlls and strings are brought in at runtime.].

PE ID -

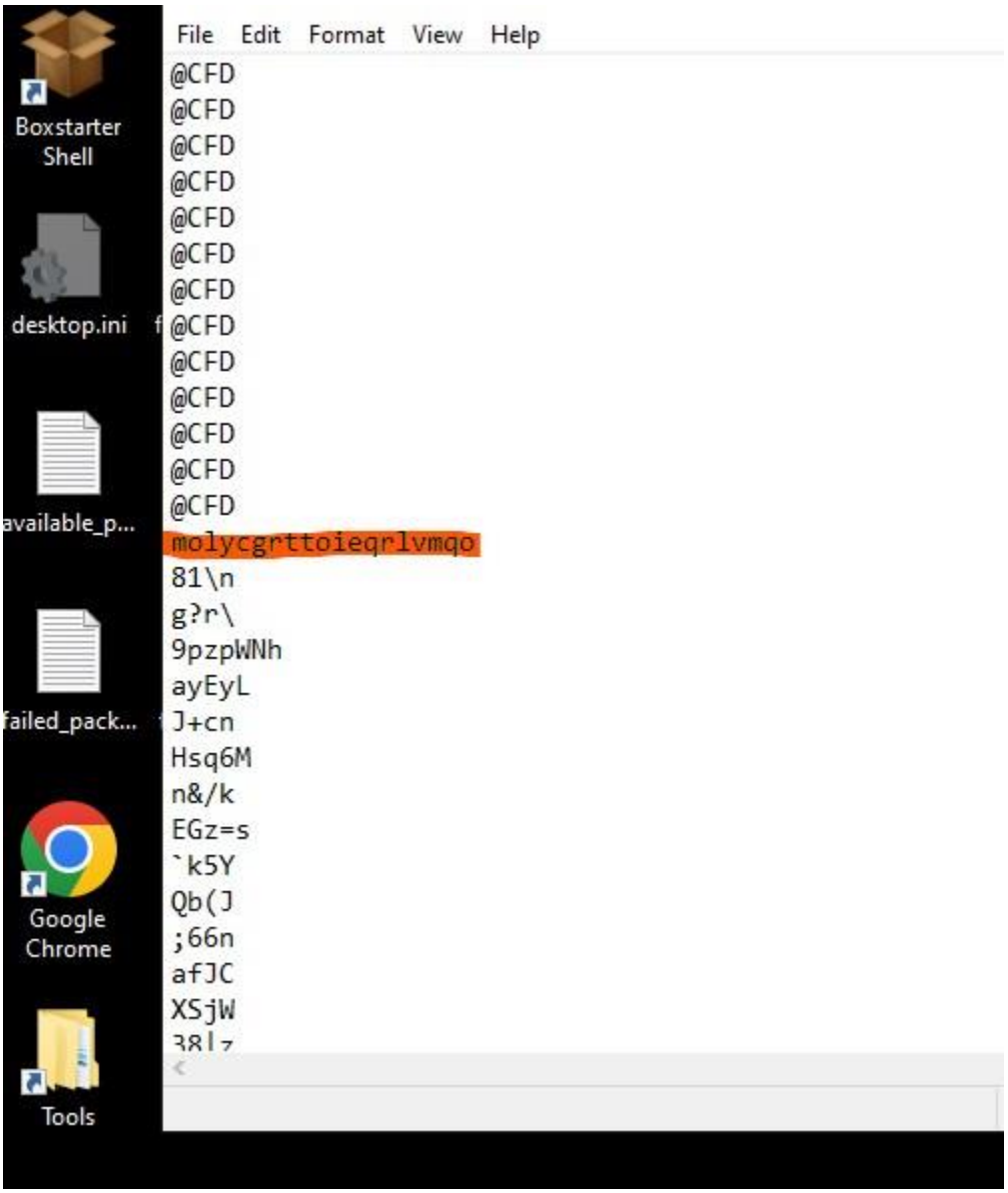




Got the base image, header sizes, offsets, linker information, DateStamp, etc. Not too useful, but gave linker info, can enumerate further using some popular linker scripts and try matching some compiled pseudocode to get exact information.

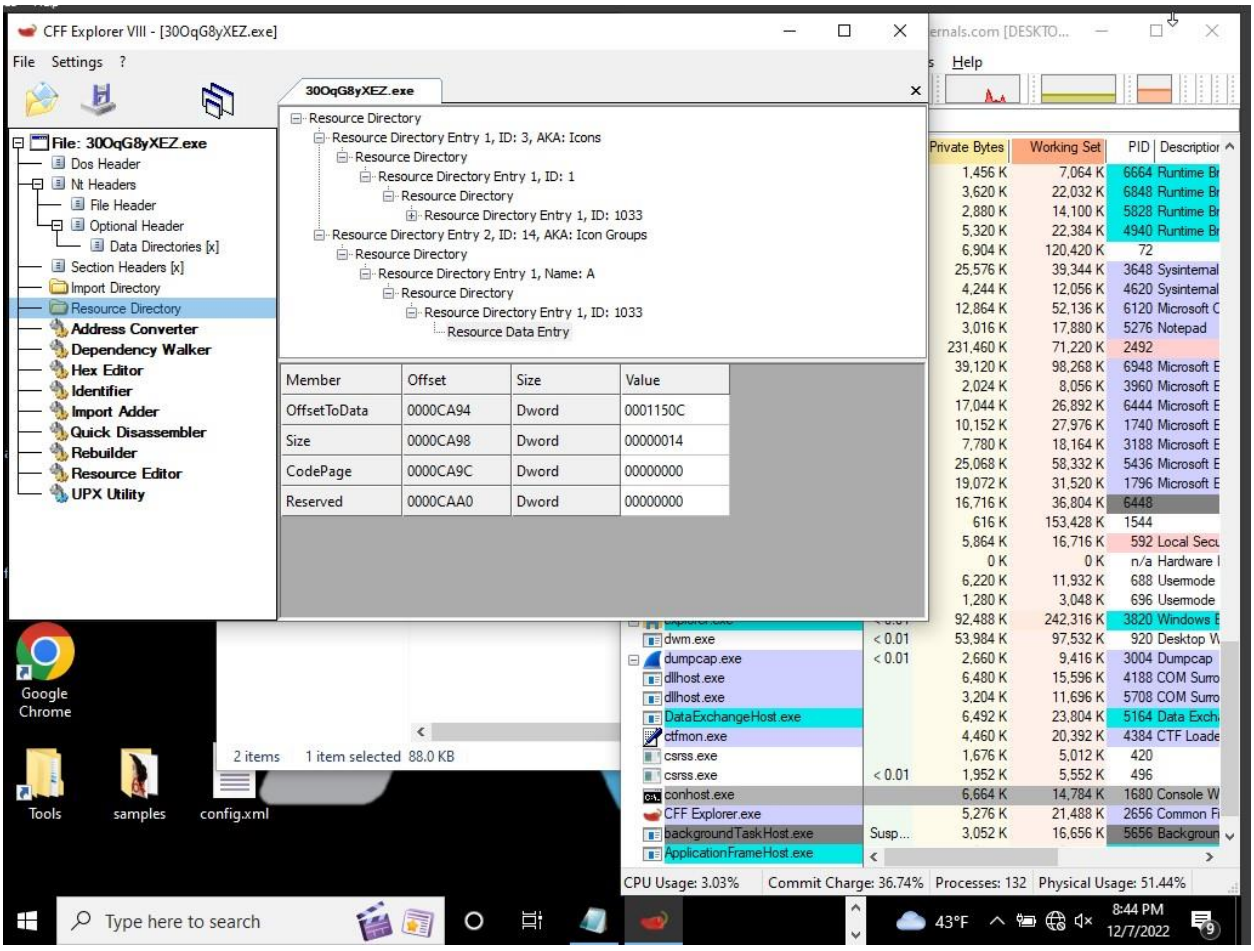
Strings –

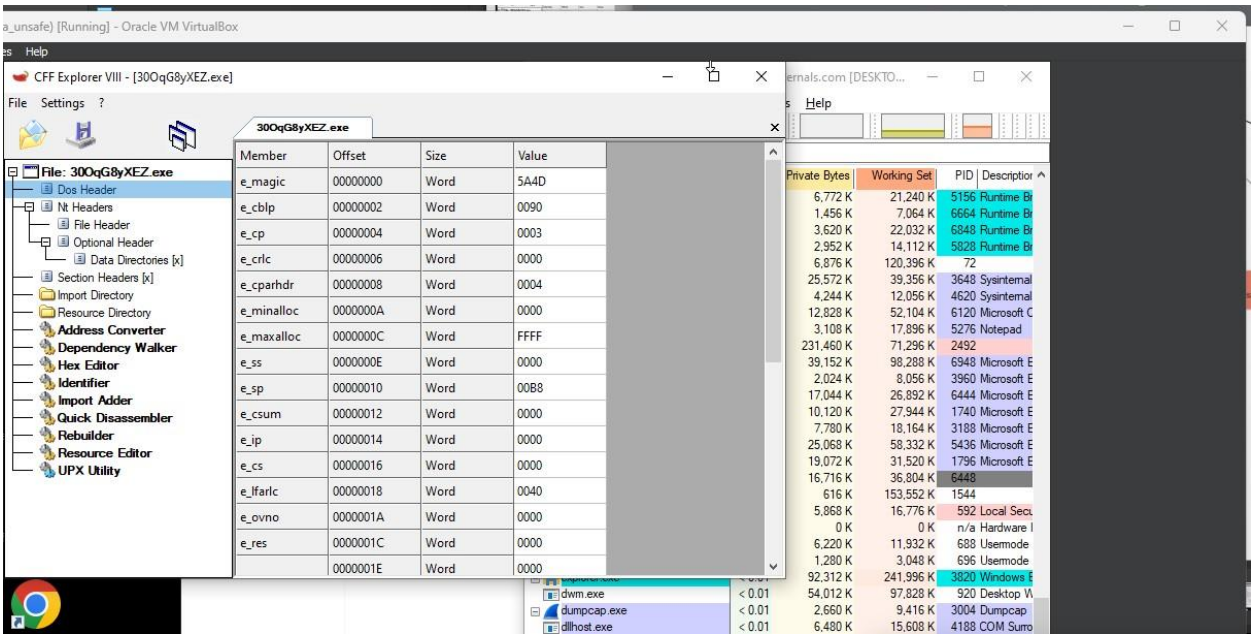
Before runtime Unpacking –



The unpacker, with a few checks.

Interesting information from CFF explorer -
DOS header information

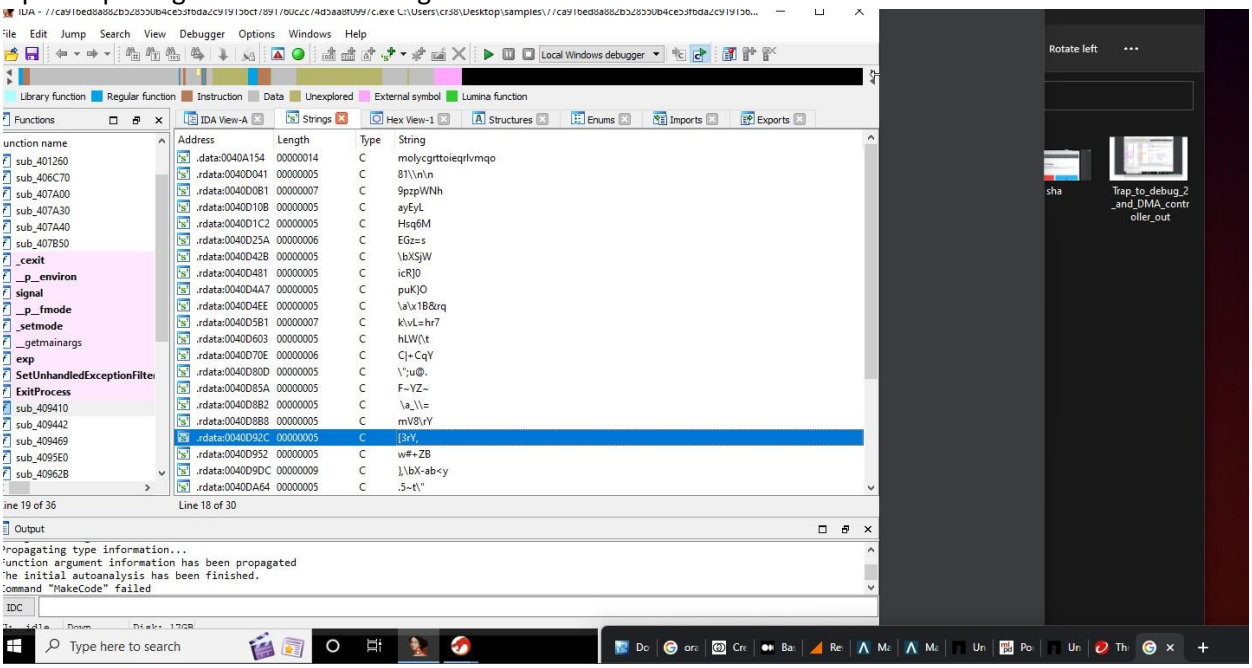




From this, I was able to hypothesize that something is packed in resource section, 1 icon but metadata

about icon is greater that the icon size, so that was fishy.

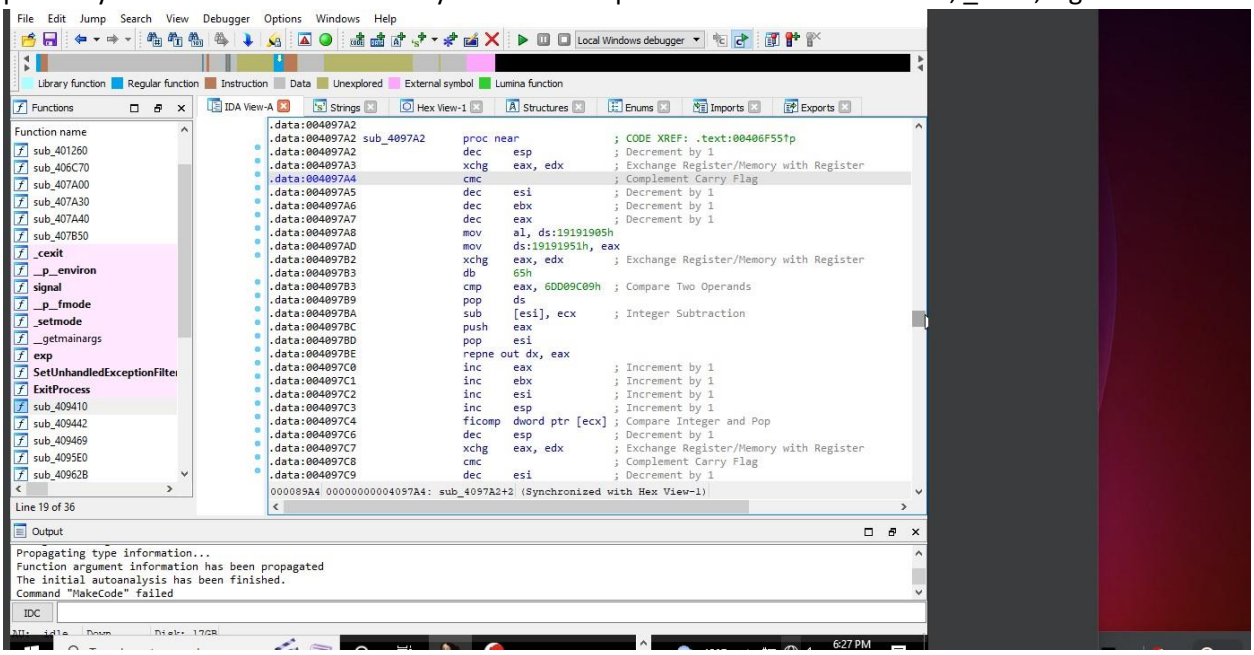
Upon exploring further in IDA Strings -



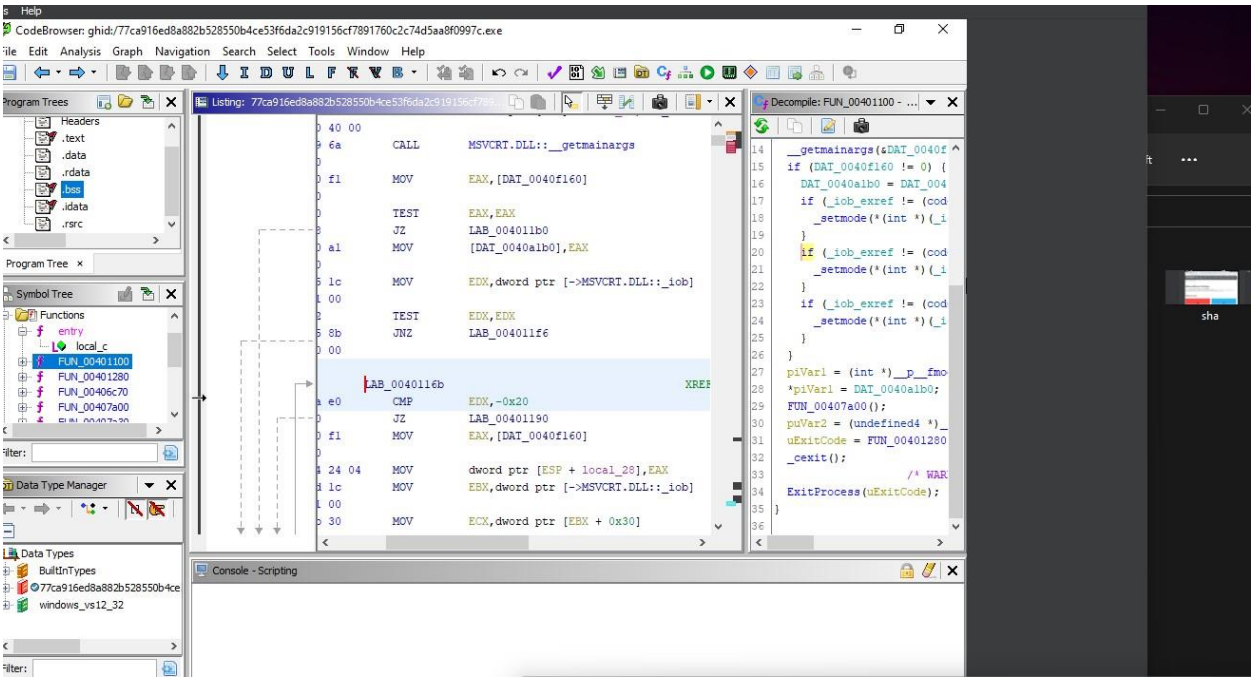
Same thing.

Moving on to Advanced Static yields better results –
Tools : IDA Free, Ghidra.

Was able tell its packed because of repeated instructions with small changes in certain values, junk code probably. This was done about every function except the ones the named ones, _cexit, Signal etc etc.

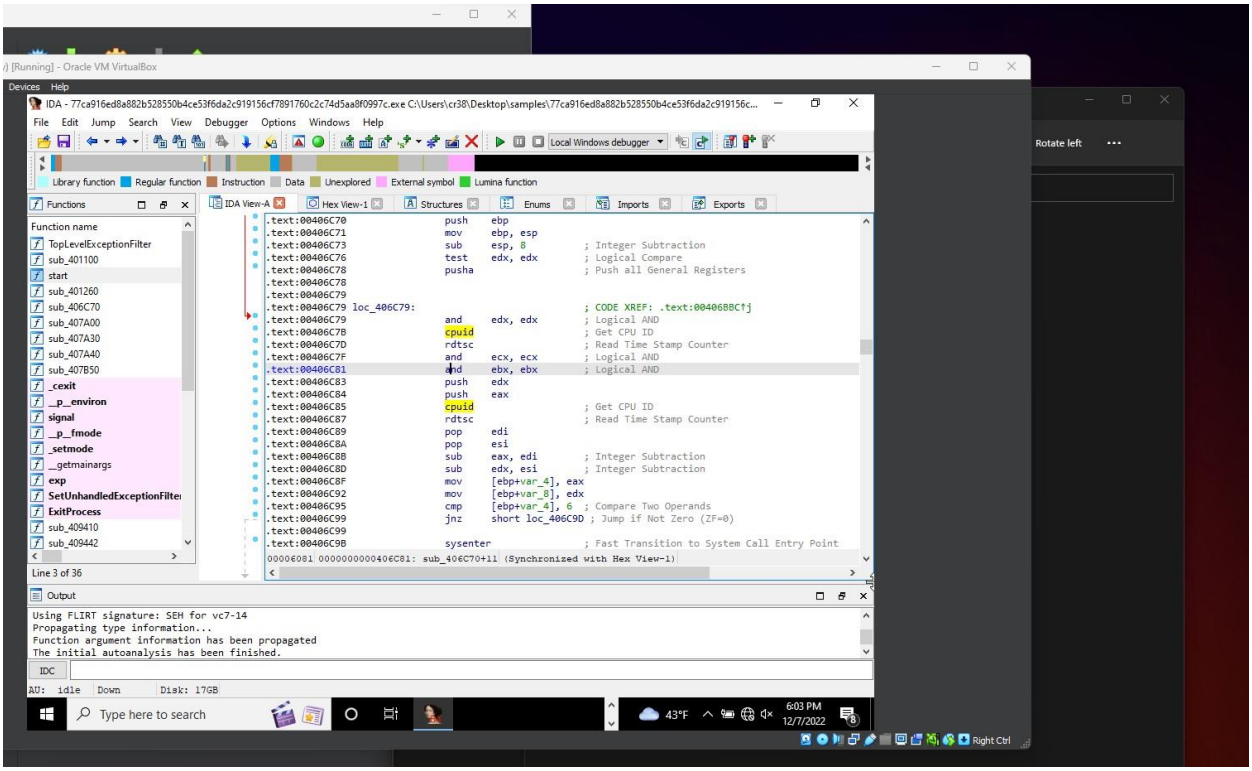


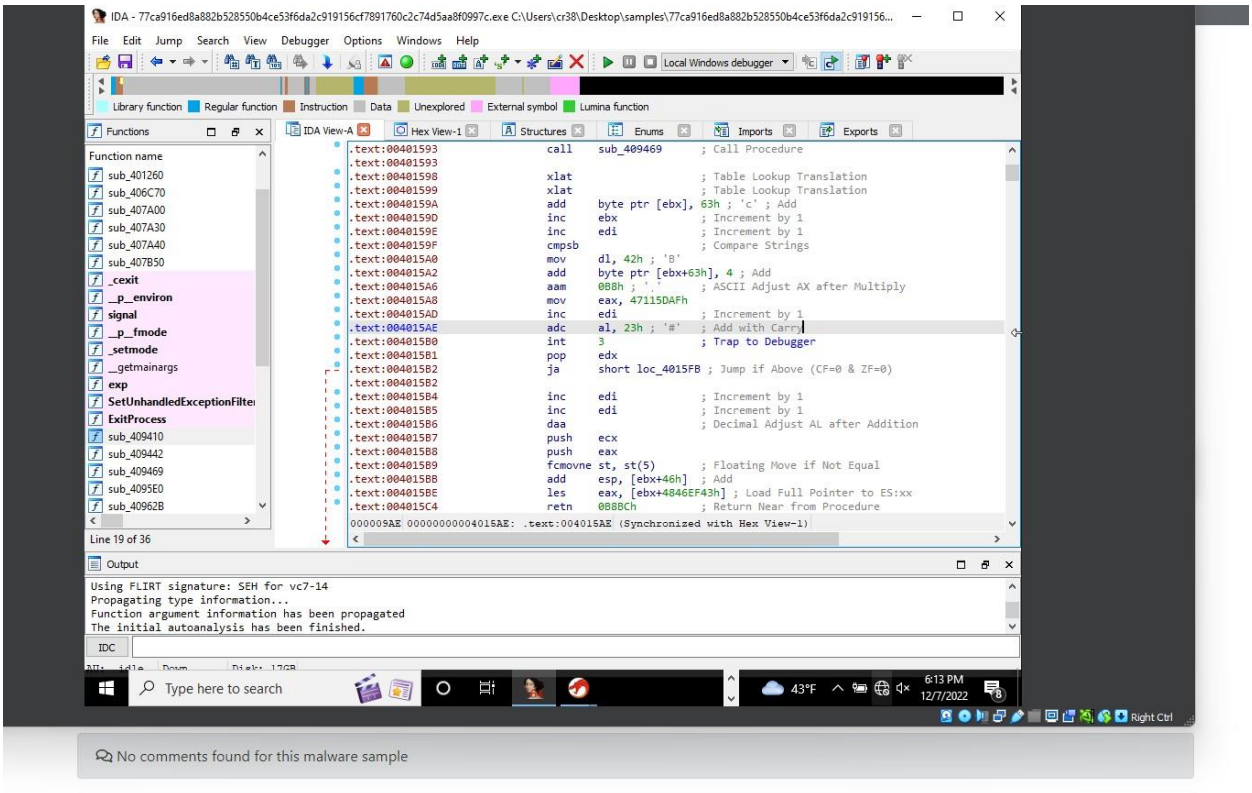
After looking at ida and ghidra, I was able to trace to actual main function that unpacks the file, couldnt tell which packer was used, But looking at a decent packer such as Aegis Cryptor, I understood that its packed with stubs. What aegis Cryptor does is make 3 process using malloc, all of them are legitimate, after creating a new process, it injects the actual program into the process space, similar to fork() exec(). In this case they manipulating headers- .



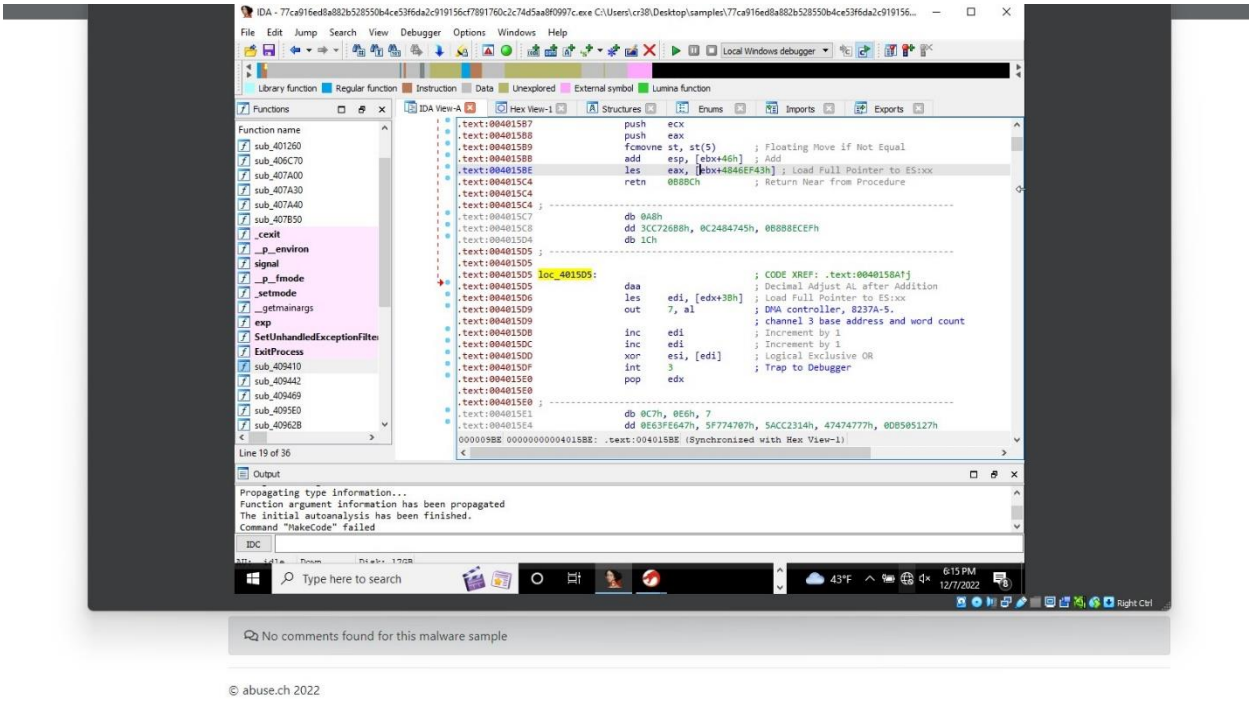
Algorithm to extract real exe that sets the connection host and all the fun stuff.

But before we even get to unpacking, this version of the malware does N number of checks, all to setup a safe space for the real exe,I was able to get these





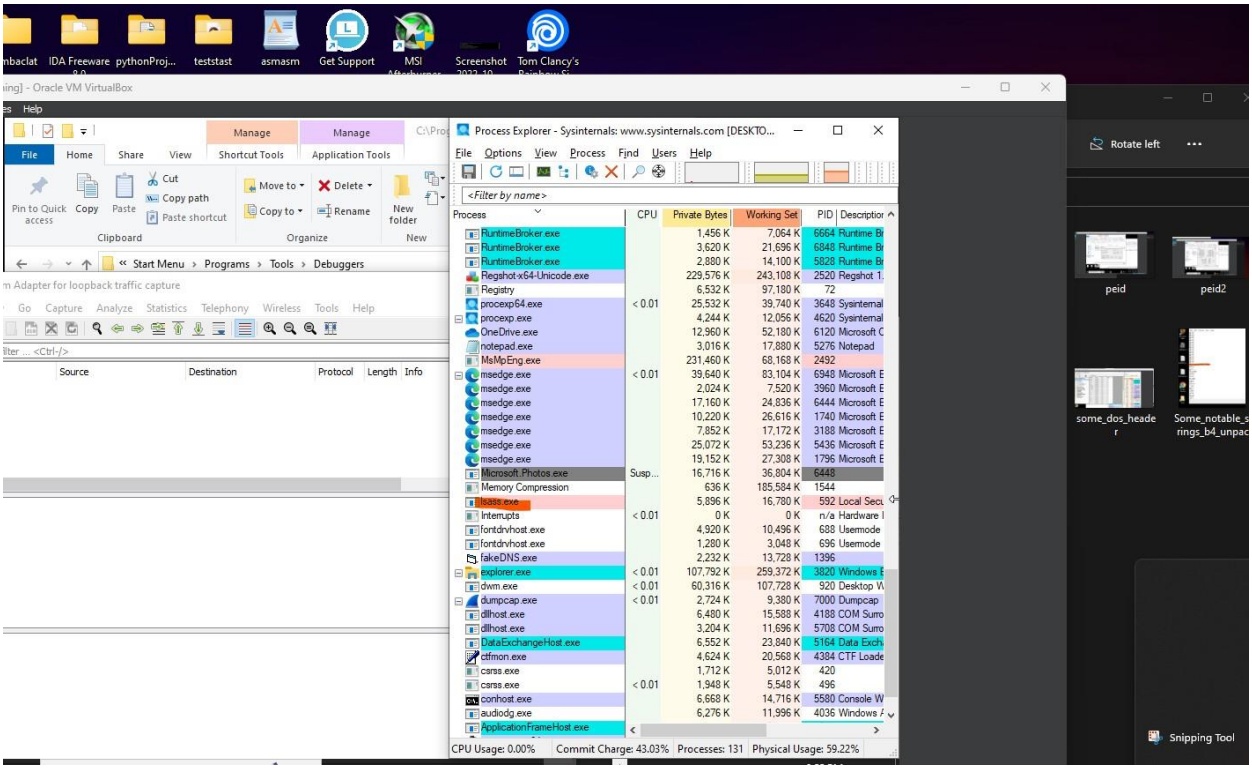
Anti-Debugging.



Exception handling dictates control flow. Certain api calls are made at runtime to check for debuggers and exceptions, ideally, the program only wants 1 exception to be hit so it goes to specific jump. I will show you the results of hitting that check in dynamic, the file deletes itself if wrong exception gets hit.

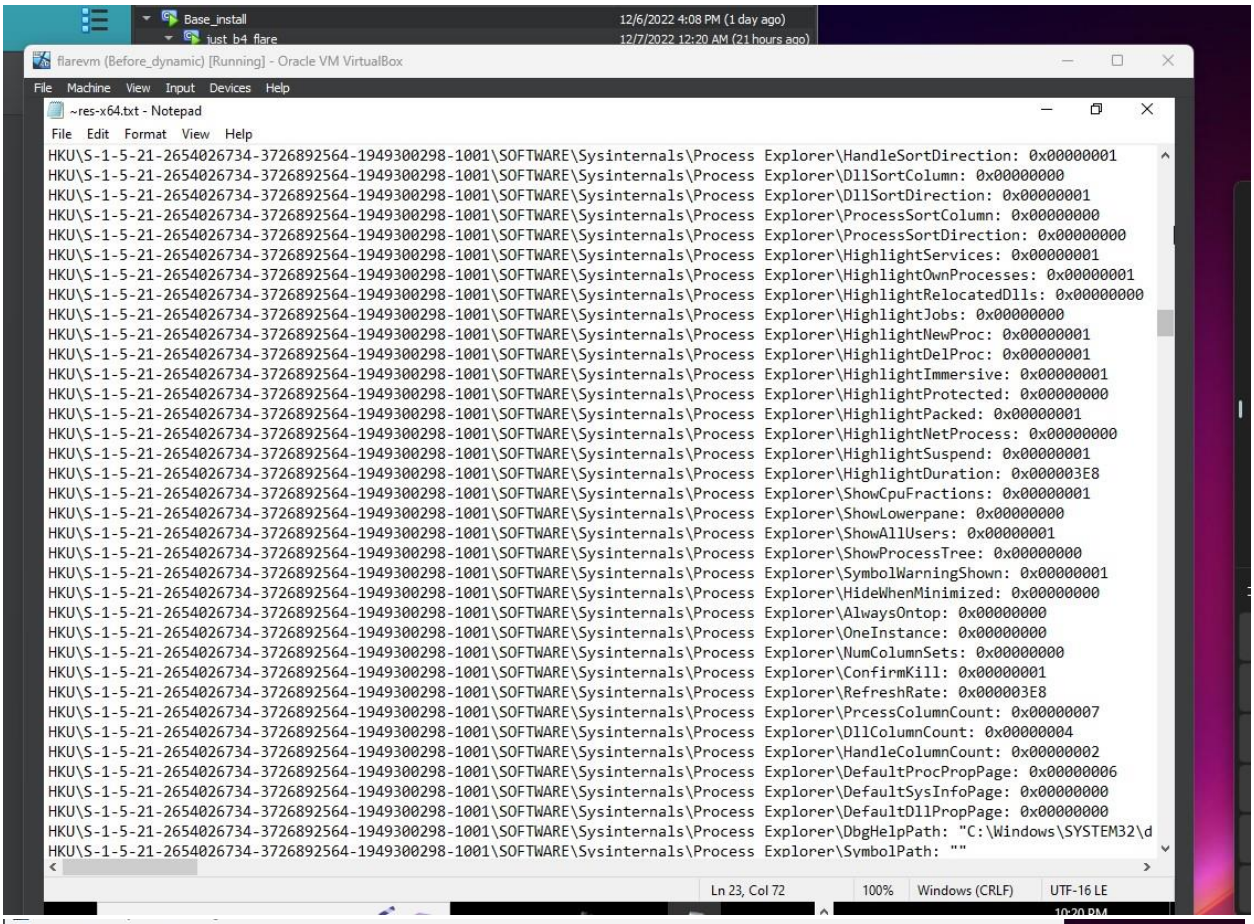
Basic Dynamic Analysis -
Tools used : Multiple sandboxes , Procmon, Regshot

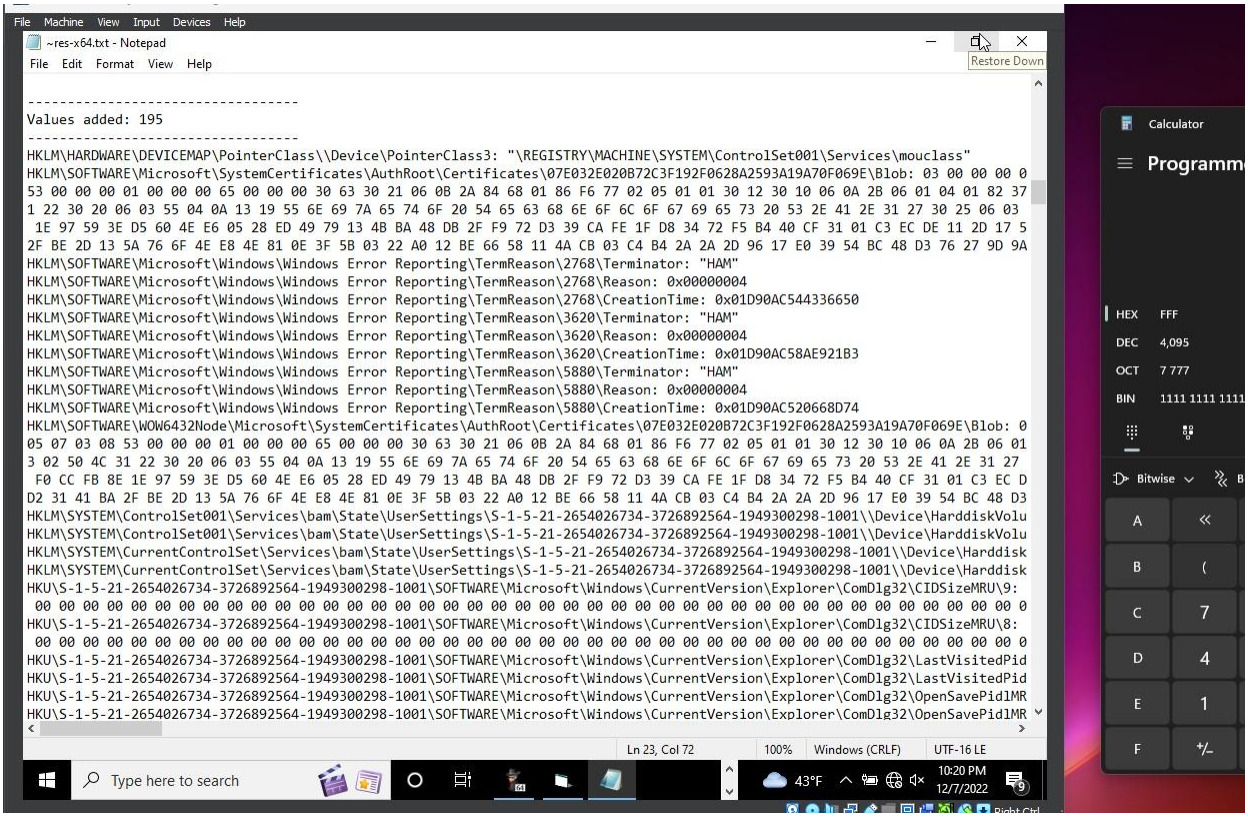
For these I just used online sandboxes, the behaviour and malware family descriptions are from the sandboxes.
With procmon, I took a snapshot and ran the exe as an admin before which I also took regshot captures.

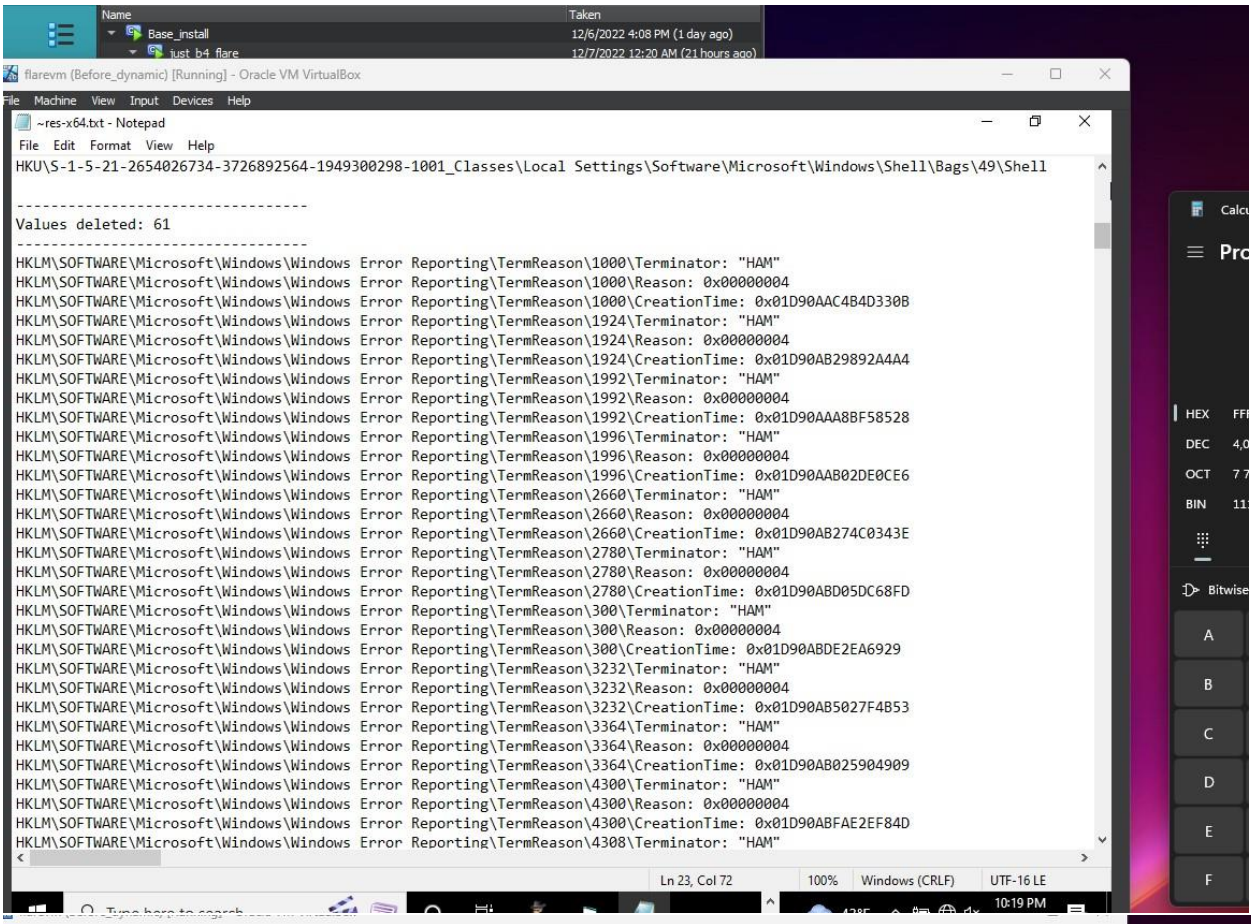


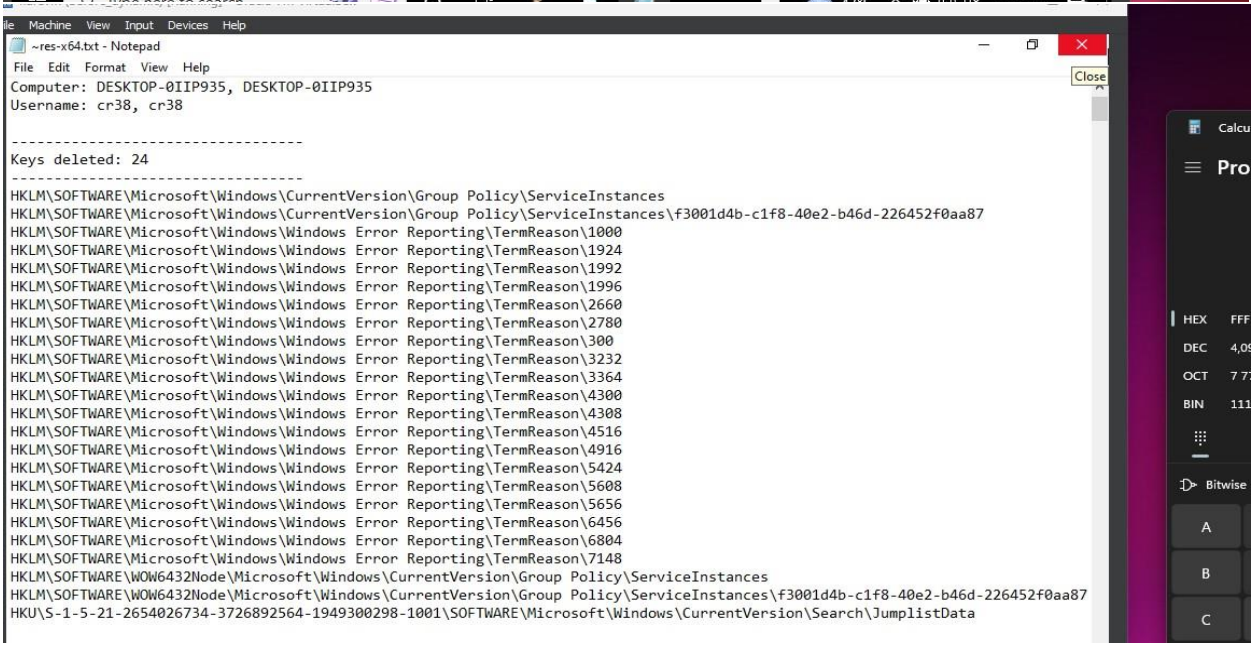
The Connhost was new, lssas was new as well, I don't understand why that process. But the connhost is from the exe post execution itself, the malware launches as random program, then a foreign address is chosen to be unpacked to and the original program after completing checks and setting up a SAFE space for the program, exits. Can trace it with dynamic analysis, malloc and virtual realloc functions are used.

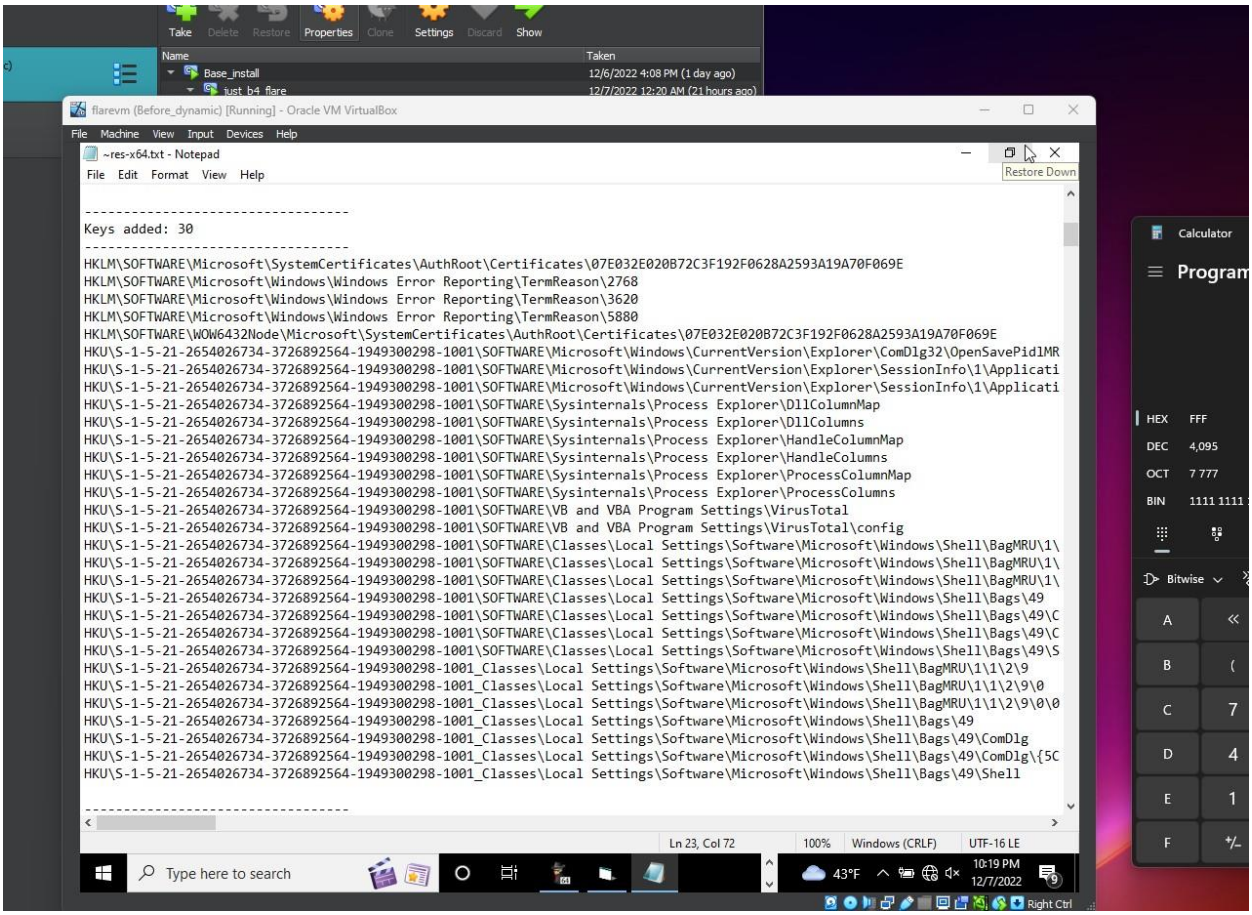
REGSHOT – Post Run.

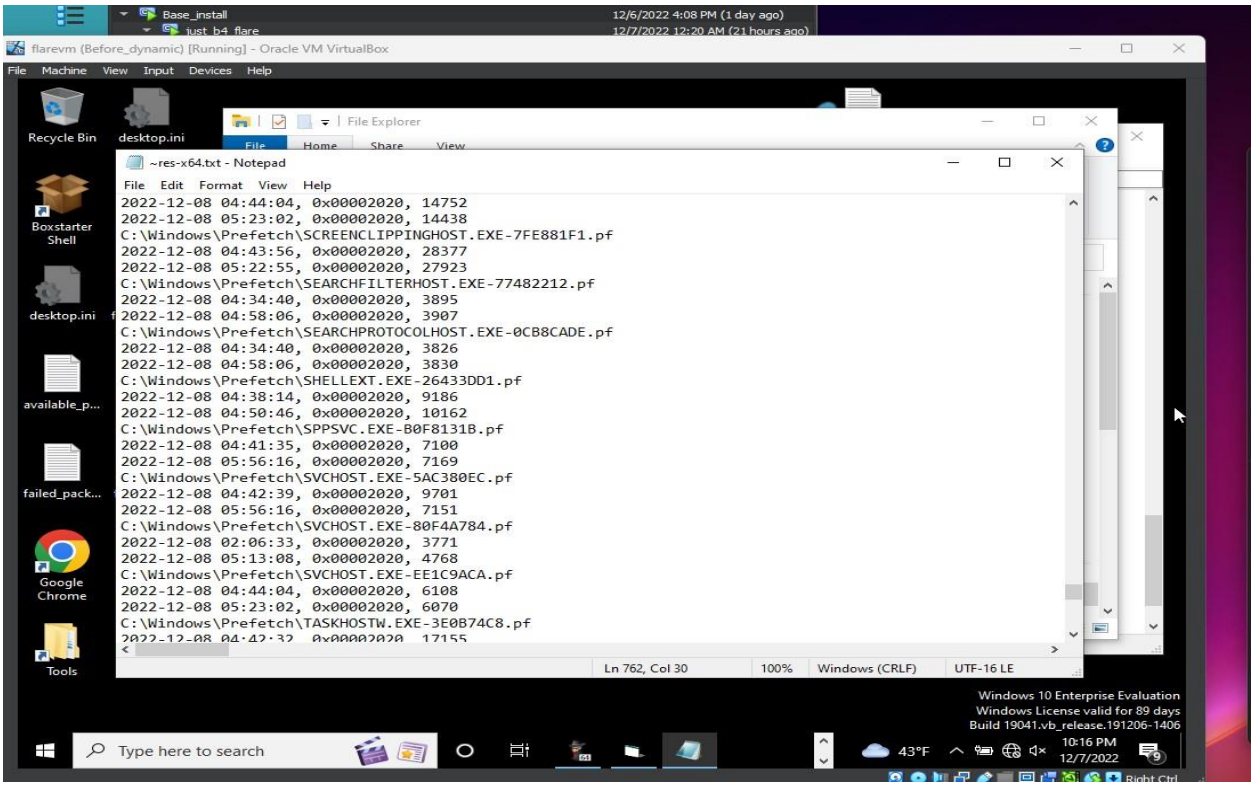

Base_install
12/6/2022 4:08 PM (1 day ago)
just_b4_flare
12/7/2022 12:20 AM (21 hours ago)
flarevm (Before_dynamic) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
~res-x64.txt - Notepad
File Edit Format View Help
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\HandleSortDirection: 0x00000001
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\DllSortColumn: 0x00000000
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\DllSortDirection: 0x00000001
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\ProcessSortColumn: 0x00000000
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\ProcessSortDirection: 0x00000000
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\HighlightServices: 0x00000001
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\HighlightOwnProcesses: 0x00000001
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\HighlightRelocatedDlls: 0x00000000
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\HighlightJobs: 0x00000000
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\HighlightNewProc: 0x00000001
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\HighlightDelProc: 0x00000001
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\HighlightImmersive: 0x00000001
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\HighlightProtected: 0x00000000
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\HighlightPacked: 0x00000001
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\HighlightNetProcess: 0x00000000
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\HighlightSuspend: 0x00000001
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\HighlightDuration: 0x000003E8
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\ShowCpuFractions: 0x00000001
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\ShowLowerpane: 0x00000000
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\ShowAllUsers: 0x00000001
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\ShowProcessTree: 0x00000000
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\SymbolWarningShown: 0x00000001
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\HideWhenMinimized: 0x00000000
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\AlwaysOntop: 0x00000000
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\OneInstance: 0x00000000
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\NumColumnSets: 0x00000000
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\ConfirmKill: 0x00000001
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\RefreshRate: 0x000003E8
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\PrcessColumnCount: 0x00000007
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\DllColumnCount: 0x00000004
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\HandleColumnCount: 0x00000002
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\DefaultProcPropPage: 0x00000006
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\DefaultSysInfoPage: 0x00000000
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\DefaultDllPropPage: 0x00000000
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\DbgHelpPath: "C:\Windows\SYSTEM32\d
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\SymbolPath: ""
Ln 23, Col 72
100%
Windows (CRLF)
UTF-16 LE

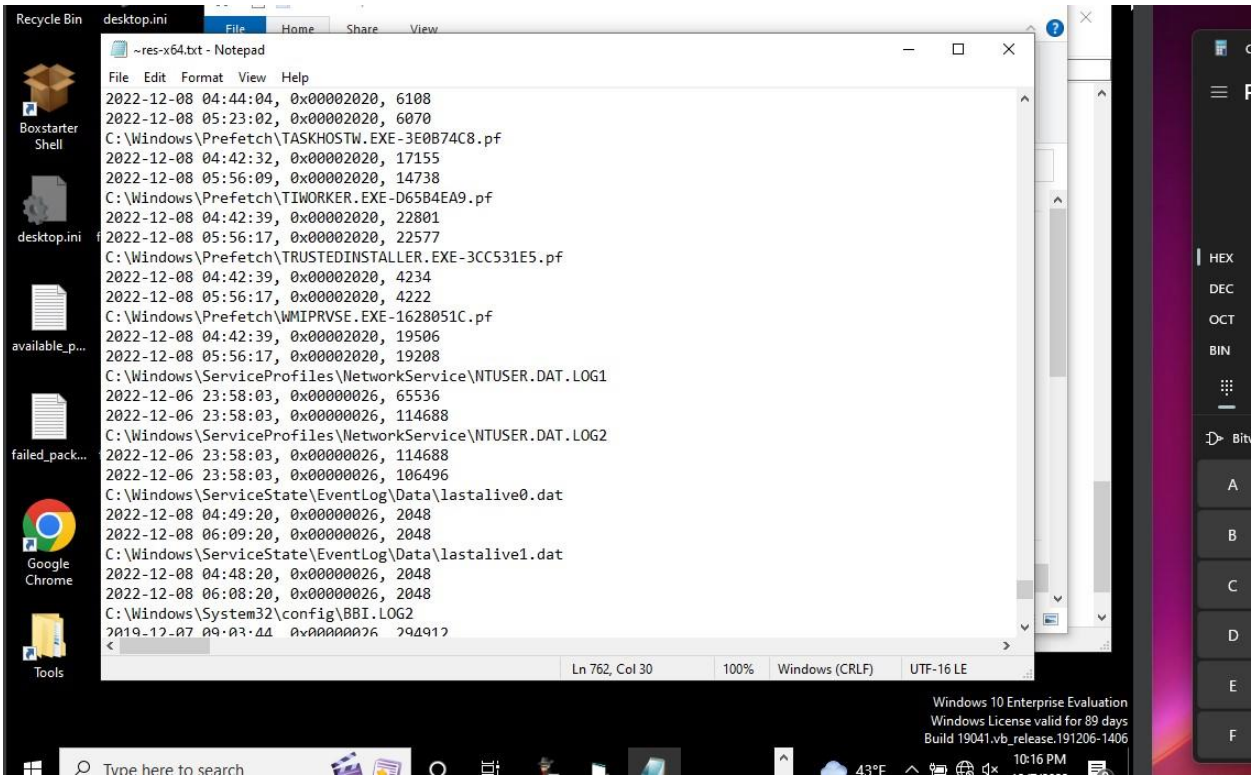

File Machine View Input Devices Help
~res-x64.txt - Notepad
File Edit Format View Help
Restore Down
Values added: 195
HKLM\HARDWARE\DEVICEMAP\PointerClass\\Device\PointerClass3: "\REGISTRY\MACHINE\SYSTEM\ControlSet001\Services\mouclass"
HKLM\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\07E032E020B72C3F192F0628A2593A19A70F069E\Blob: 03 00 00 00 0
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\2768\Terminator: "HAM"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\2768\Reason: 0x00000004
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\2768\CreationTime: 0x01D90AC544336650
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\3620\Terminator: "HAM"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\3620\Reason: 0x00000004
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\3620\CreationTime: 0x01D90AC58AE921B3
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\5880\Terminator: "HAM"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\5880\Reason: 0x00000004
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\5880\CreationTime: 0x01D90AC520668D74
HKLM\SOFTWARE\WOW6432Node\Microsoft\SystemCertificates\AuthRoot\Certificates\07E032E020B72C3F192F0628A2593A19A70F069E\Blob: 0
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-2654026734-3726892564-1949300298-1001\\Device\HarddiskVolu
HKLM\SYSTEM\ControlSet001\Services\bam\State\UserSettings\S-1-5-21-2654026734-3726892564-1949300298-1001\\Device\HarddiskVolu
HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-2654026734-3726892564-1949300298-1001\\Device\Harddisk
HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-2654026734-3726892564-1949300298-1001\\Device\Harddisk
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\CIDSizeMRU\9:
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\CIDSizeMRU\8:
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPid
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPid
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMR
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMR
Ln 23, Col 72
100%
Windows (CRLF)
UTF-16 LE
Type here to search
43°F
10:20 PM
12/7/2022
Calculator
Programm
HEX FFF
DEC 4,095
OCT 7 777
BIN 1111 1111 1111
Bitwise


Name
Taken
Base_install
12/6/2022 4:08 PM (1 day ago)
just_b4_flare
12/7/2022 12:20 AM (21 hours ago)
flarevm (Before_dynamic) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
~res-x64.txt - Notepad
File Edit Format View Help
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\49\Shell
Values deleted: 61
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1000\Terminator: "HAM"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1000\Reason: 0x00000004
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1000\CreationTime: 0x01D90AAC4B4D330B
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1924\Terminator: "HAM"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1924\Reason: 0x00000004
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1924\CreationTime: 0x01D90AB29892A4A4
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1992\Terminator: "HAM"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1992\Reason: 0x00000004
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1992\CreationTime: 0x01D90AAA8BF58528
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1996\Terminator: "HAM"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1996\Reason: 0x00000004
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1996\CreationTime: 0x01D90AAB02DE0CE6
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\2660\Terminator: "HAM"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\2660\Reason: 0x00000004
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\2660\CreationTime: 0x01D90AB274C0343E
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\2780\Terminator: "HAM"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\2780\Reason: 0x00000004
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\2780\CreationTime: 0x01D90ABD05DC68FD
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\300\Terminator: "HAM"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\300\Reason: 0x00000004
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\300\CreationTime: 0x01D90ABDE2EA6929
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\3232\Terminator: "HAM"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\3232\Reason: 0x00000004
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\3232\CreationTime: 0x01D90AB5027F4B53
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\3364\Terminator: "HAM"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\3364\Reason: 0x00000004
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\3364\CreationTime: 0x01D90AB025904909
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\4300\Terminator: "HAM"
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\4300\Reason: 0x00000004
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\4300\CreationTime: 0x01D90ABFAE2EF84D
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\4308\Terminator: "HAM"
Ln 23, Col 72
100%
Windows (CRLF)
UTF-16 LE
10:19 PM
Calcu
Pro
HEX
DEC
OCT
BIN
Bitwise
A
B
C
D
E
F

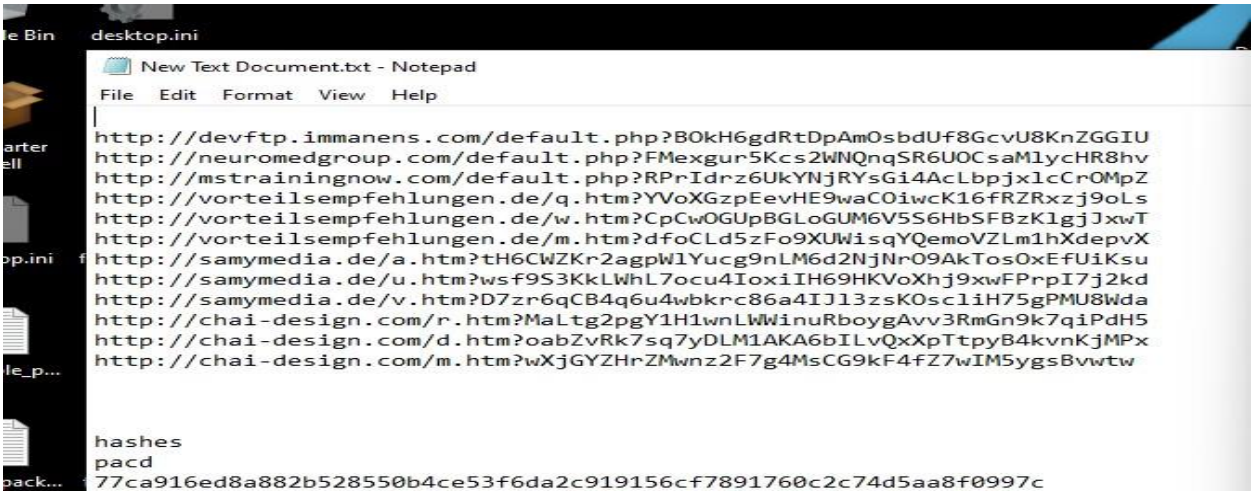

Machine View Input Devices Help
~res-x64.txt - Notepad
File Edit Format View Help
Close
Computer: DESKTOP-0IIP935, DESKTOP-0IIP935
Username: cr38, cr38
Keys deleted: 24
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances\f3001d4b-c1f8-40e2-b46d-226452f0aa87
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1000
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1924
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1992
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\1996
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\2660
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\2780
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\300
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\3232
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\3364
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\4300
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\4308
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\4516
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\4916
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\5424
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\5608
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\5656
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\6456
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\6804
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\7148
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Group Policy\ServiceInstances\f3001d4b-c1f8-40e2-b46d-226452f0aa87
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Search\JumplistData
Calcu
Pro
HEX
DEC
OCT
BIN
Bitwise
A
B
C


Take
Delete
Restore
Properties
Clone
Settings
Discard
Show
Name
Taken
Base_install
12/6/2022 4:08 PM (1 day ago)
just_b4_flare
12/7/2022 12:20 AM (21 hours ago)
flarevm (Before_dynamic) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
~res-x64.txt - Notepad
File Edit Format View Help
Restore Down
Keys added: 30
HKLM\SOFTWARE\Microsoft\SystemCertificates\AuthRoot\Certificates\07E032E020B72C3F192F0628A2593A19A70F069E
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\2768
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\3620
HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason\5880
HKLM\SOFTWARE\WOW6432Node\Microsoft\SystemCertificates\AuthRoot\Certificates\07E032E020B72C3F192F0628A2593A19A70F069E
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidlMR
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\Applicati
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\Applicati
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\DllColumnMap
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\DllColumns
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\HandleColumnMap
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\HandleColumns
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\ProcessColumnMap
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Sysinternals\Process Explorer\ProcessColumns
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\VB and VBA Program Settings\VirusTotal
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\VB and VBA Program Settings\VirusTotal\config
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\49
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\49\C
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\49\C
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001\SOFTWARE\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\49\S
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\1\2\9
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\1\2\9\0
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\1\2\9\0\0
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\49
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\49\ComDlg
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\49\ComDlg\{5C
HKU\S-1-5-21-2654026734-3726892564-1949300298-1001_Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags\49\Shell
Ln 23, Col 72
100%
Windows (CRLF)
UTF-16 LE
Type here to search
43°F
10:19 PM
12/7/2022
Right Ctrl
Calculator
Program
HEX FFF
DEC 4,095
OCT 7 777
BIN 1111 1111
Bitwise
A
B
C
D
E
F
7
4
1


Base_install
12/6/2022 4:08 PM (1 day ago)
just_b4_flare
12/7/2022 12:20 AM (21 hours ago)
flarevm (Before_dynamic) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
desktop.ini
Boxstarter Shell
desktop.ini
available_p...
failed_pack...
Google Chrome
Tools
File Explorer
File Home Share View
~res-x64.txt - Notepad
File Edit Format View Help
2022-12-08 04:44:04, 0x00002020, 14752
2022-12-08 05:23:02, 0x00002020, 14438
C:\Windows\Prefetch\SCREENCLIPPINGHOST.EXE-7FE881F1.pf
2022-12-08 04:43:56, 0x00002020, 28377
2022-12-08 05:22:55, 0x00002020, 27923
C:\Windows\Prefetch\SEARCHFILTERHOST.EXE-77482212.pf
2022-12-08 04:34:40, 0x00002020, 3895
2022-12-08 04:58:06, 0x00002020, 3907
C:\Windows\Prefetch\SEARCHPROTOCOLHOST.EXE-0CB8CADE.pf
2022-12-08 04:34:40, 0x00002020, 3826
2022-12-08 04:58:06, 0x00002020, 3830
C:\Windows\Prefetch\SHELLEXT.EXE-26433DD1.pf
2022-12-08 04:38:14, 0x00002020, 9186
2022-12-08 04:50:46, 0x00002020, 10162
C:\Windows\Prefetch\SPPSVC.EXE-B0F8131B.pf
2022-12-08 04:41:35, 0x00002020, 7100
2022-12-08 05:56:16, 0x00002020, 7169
C:\Windows\Prefetch\SVCHOST.EXE-5AC380EC.pf
2022-12-08 04:42:39, 0x00002020, 9701
2022-12-08 05:56:16, 0x00002020, 7151
C:\Windows\Prefetch\SVCHOST.EXE-80F4A784.pf
2022-12-08 02:06:33, 0x00002020, 3771
2022-12-08 05:13:08, 0x00002020, 4768
C:\Windows\Prefetch\SVCHOST.EXE-EE1C9ACA.pf
2022-12-08 04:44:04, 0x00002020, 6108
2022-12-08 05:23:02, 0x00002020, 6070
C:\Windows\Prefetch\TASKHOSTW.EXE-3E0B74C8.pf
Ln 762, Col 30
100%
Windows (CRLF)
UTF-16 LE
Windows 10 Enterprise Evaluation
Windows License valid for 89 days
Build 19041.vb_release.191206-1406
Type here to search
43°F
10:16 PM
12/7/2022
Right Ctrl



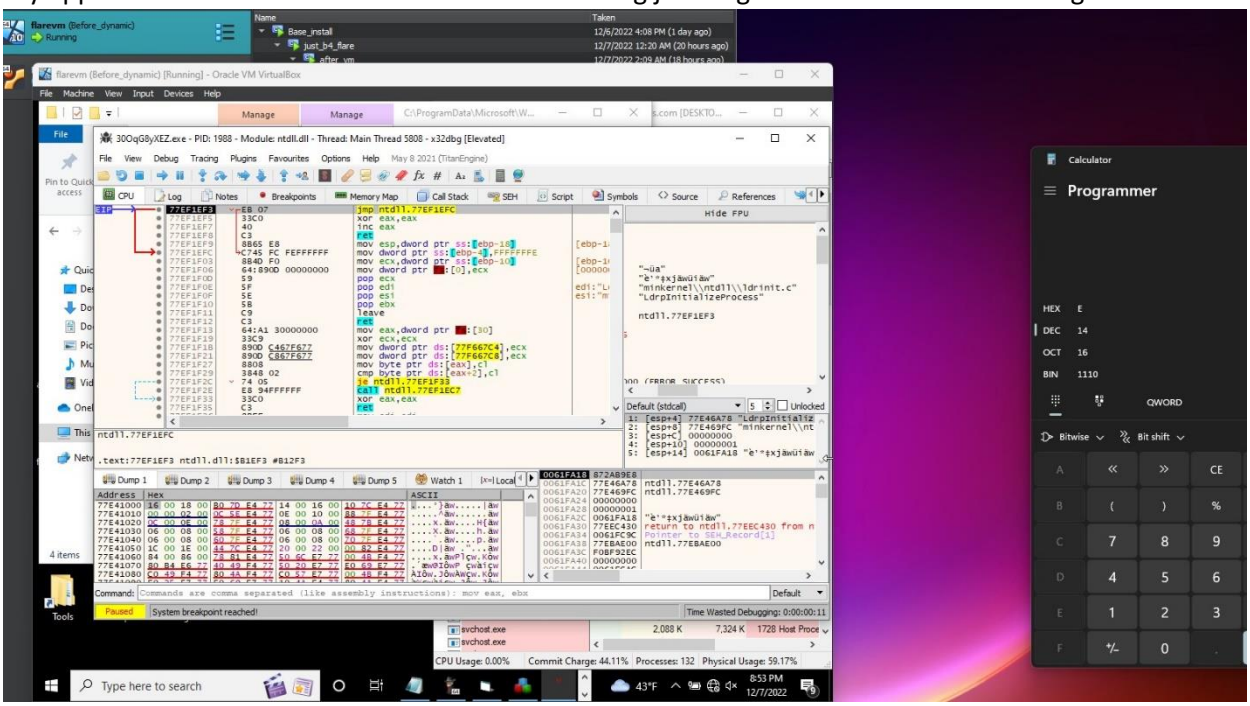
This malware keeps a log of all the tampering I did with as well as its own information in registry, I was trial and erring with x32 dbg and every exception that I missed or hit was tracked. This log combined with wireshark, I was able to see requests made to a foreign fqdn



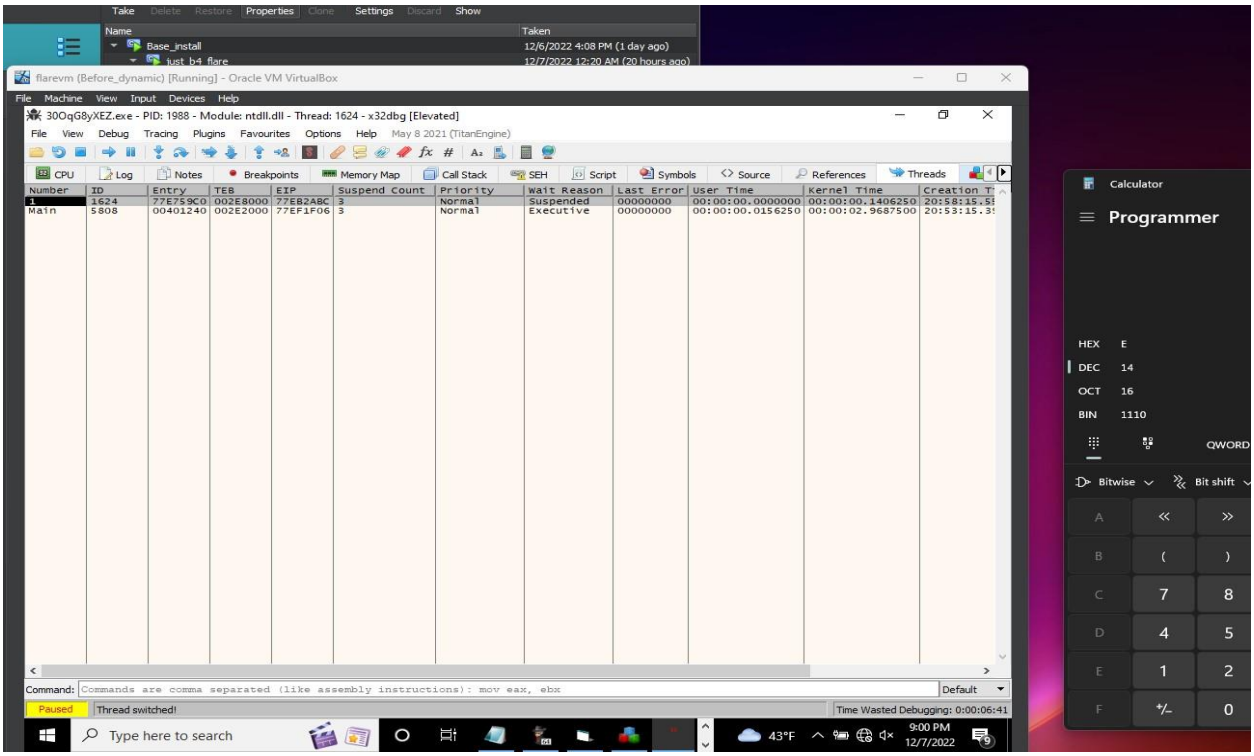
Advanced Dynamic Analysis : Tools:

Just x32 dbg.

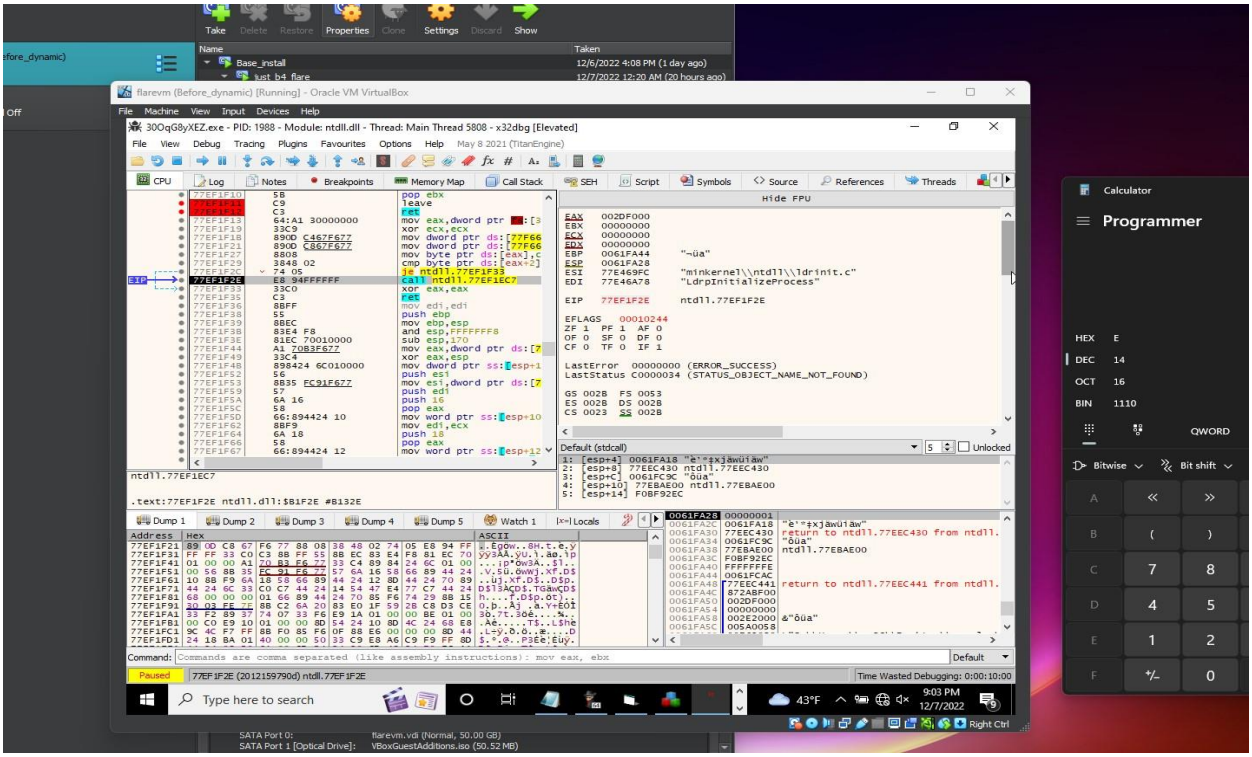
From the information in static, was able to understand that It was 32 bit binary. So loaded it up in x32
My approach was to beat the Anti VM and Anti Debug just to get to the file. This is what I got



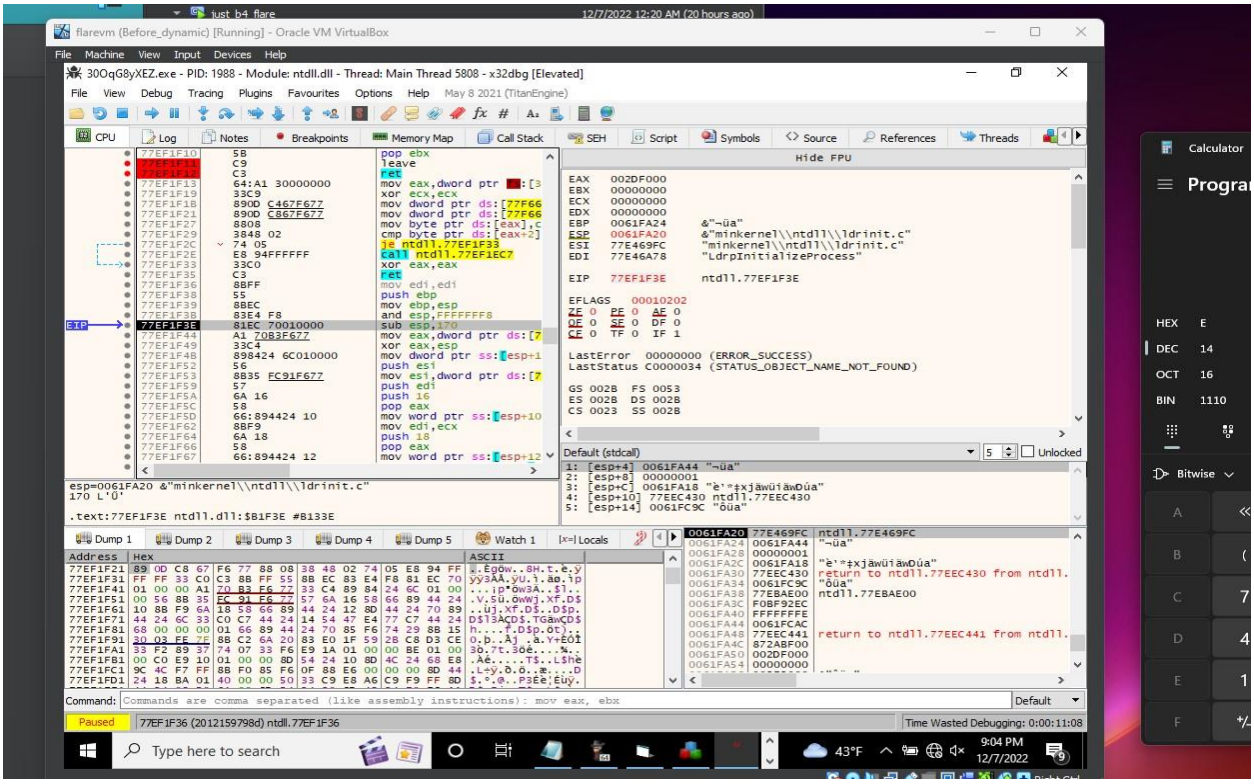
2 Threads –



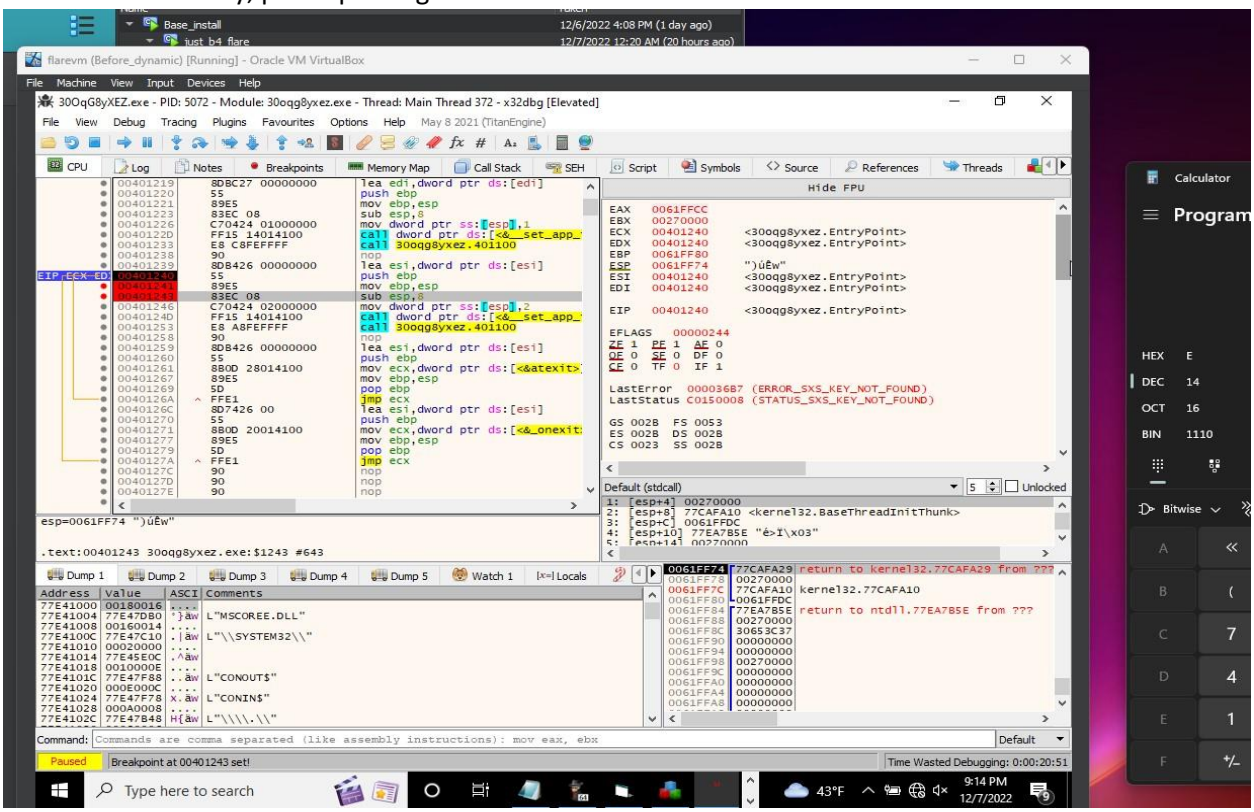
Trying to unpack it.



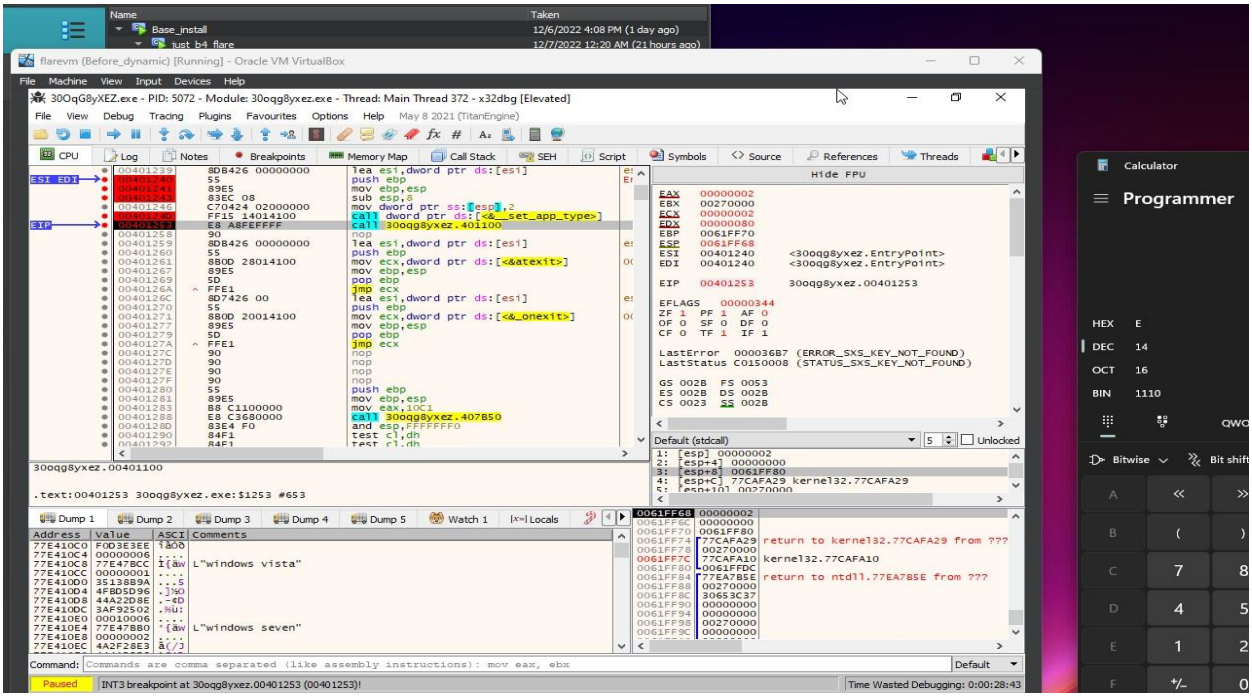
Strings at runtime.



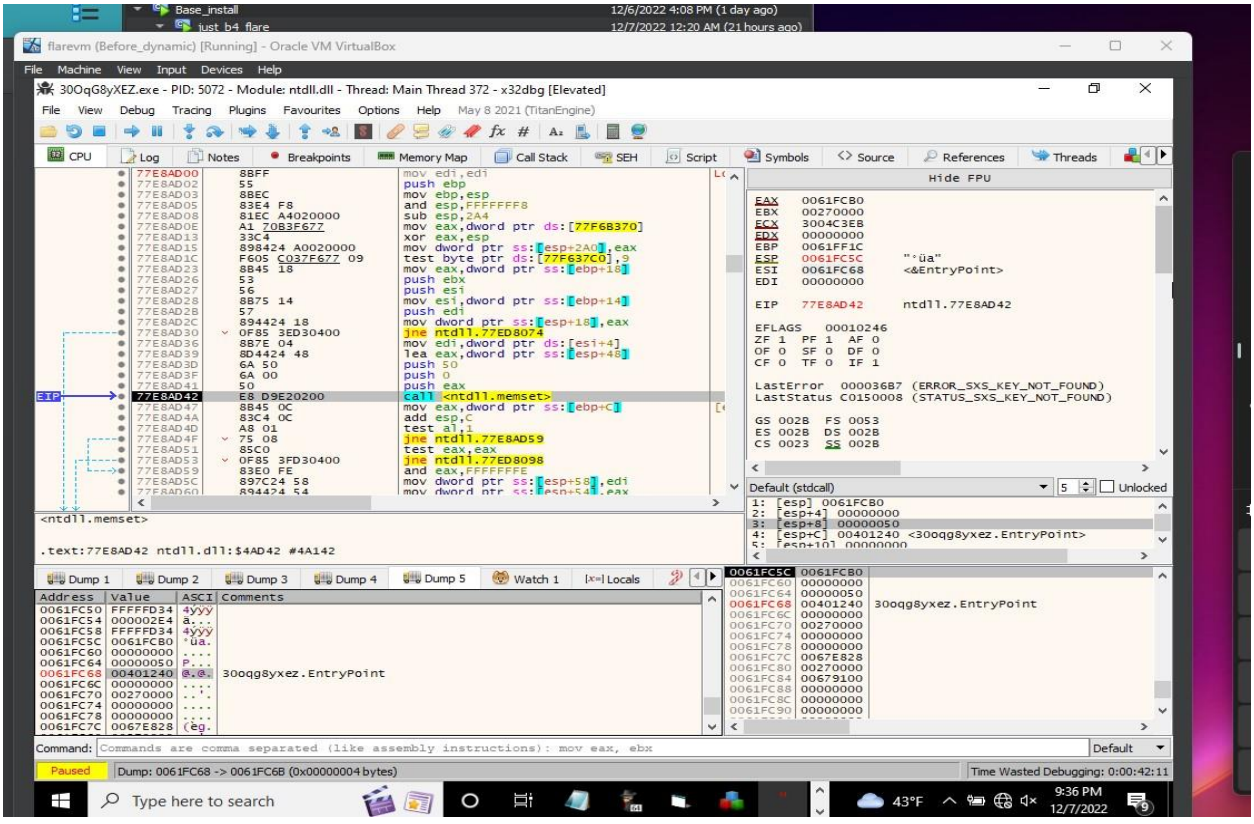
Found the real entry, pre unpacking .



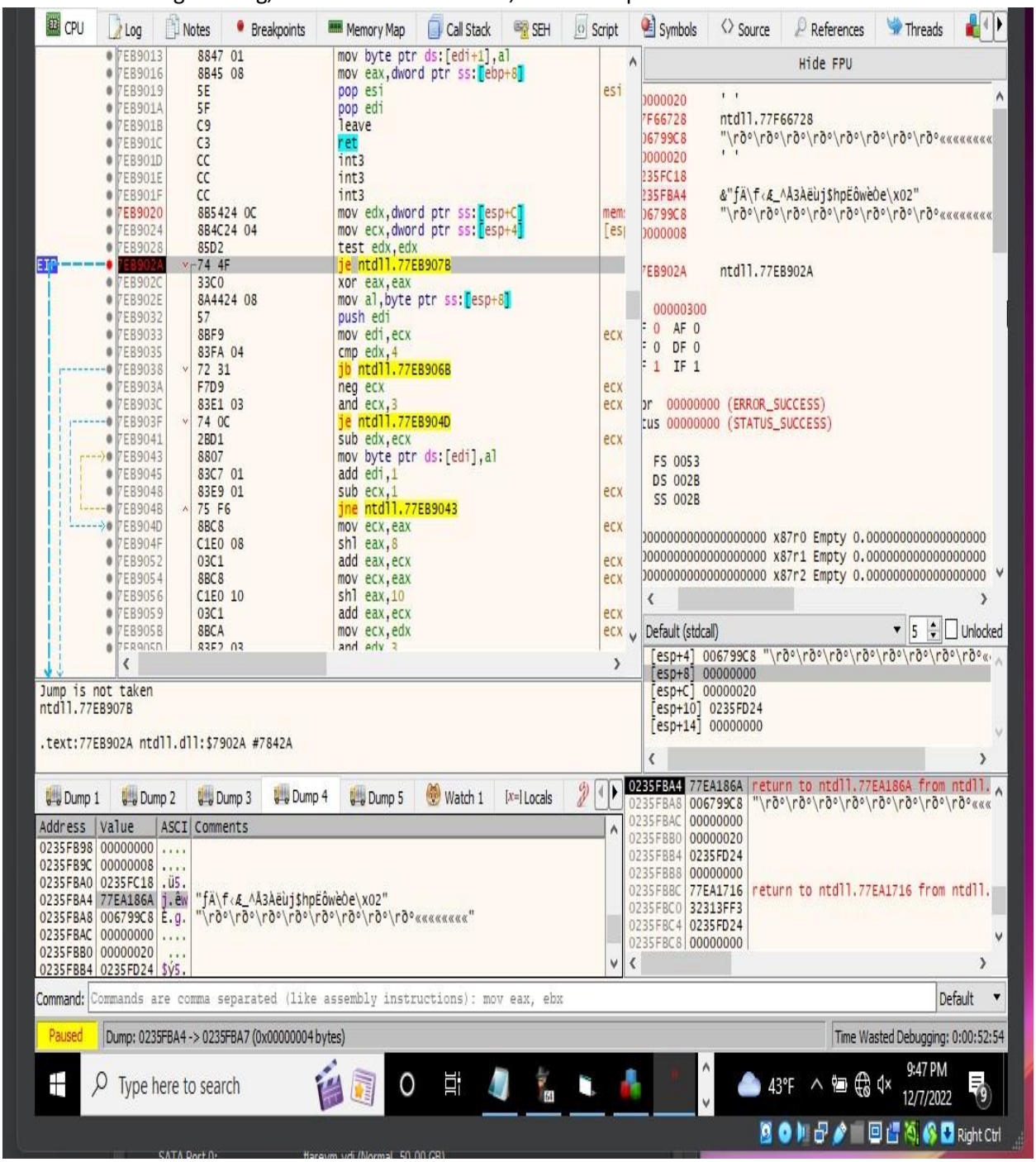
Checks for windows, cpu, filetime etc etc.

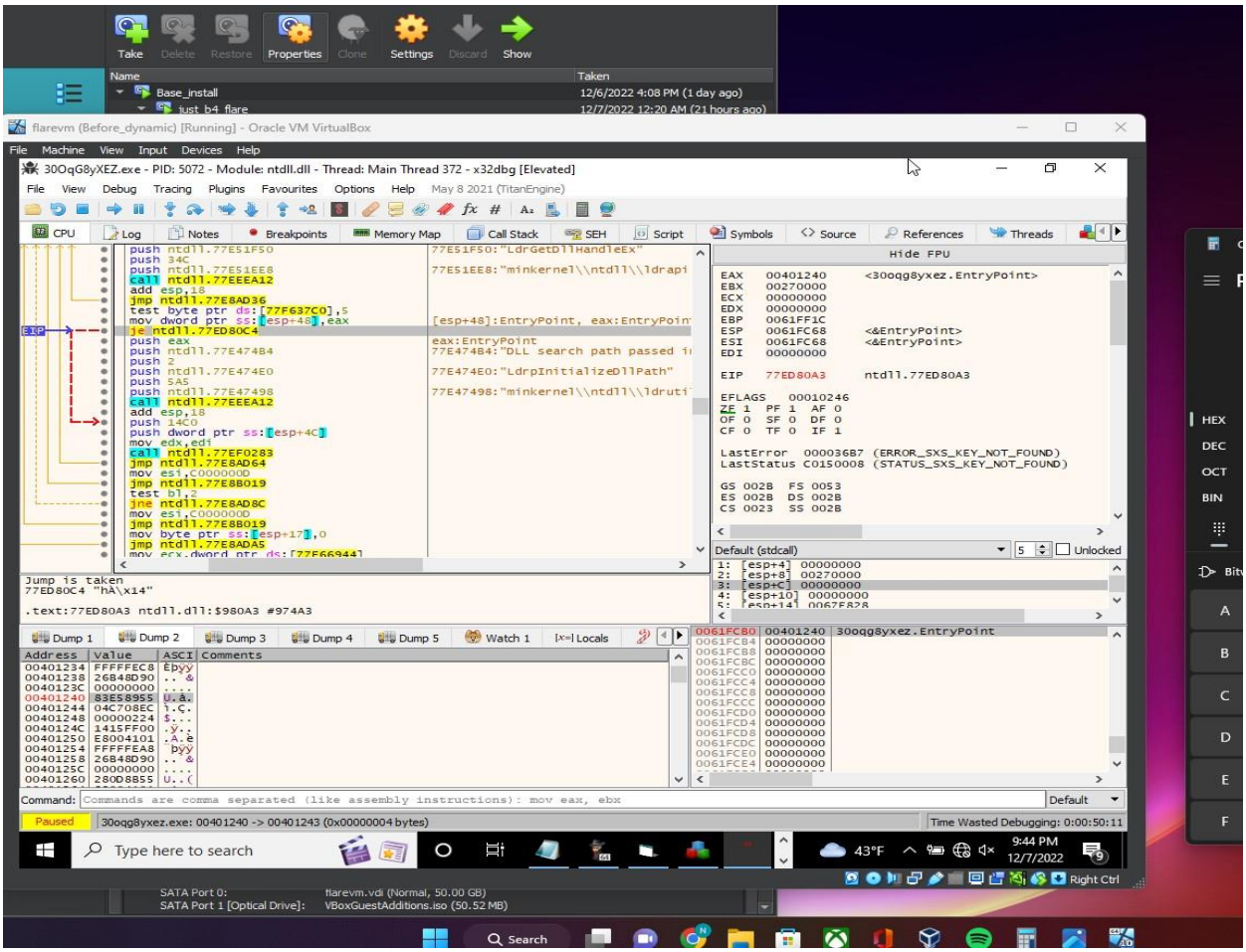


Memset, just before moving to new process space.

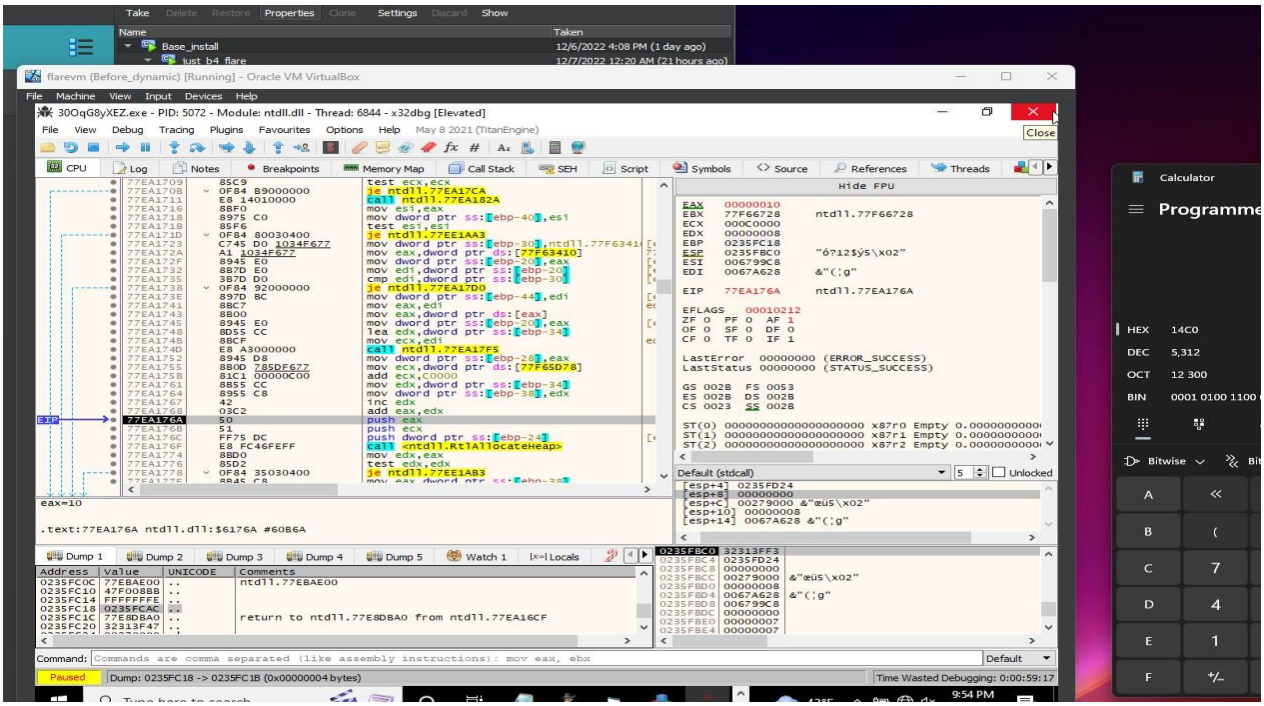


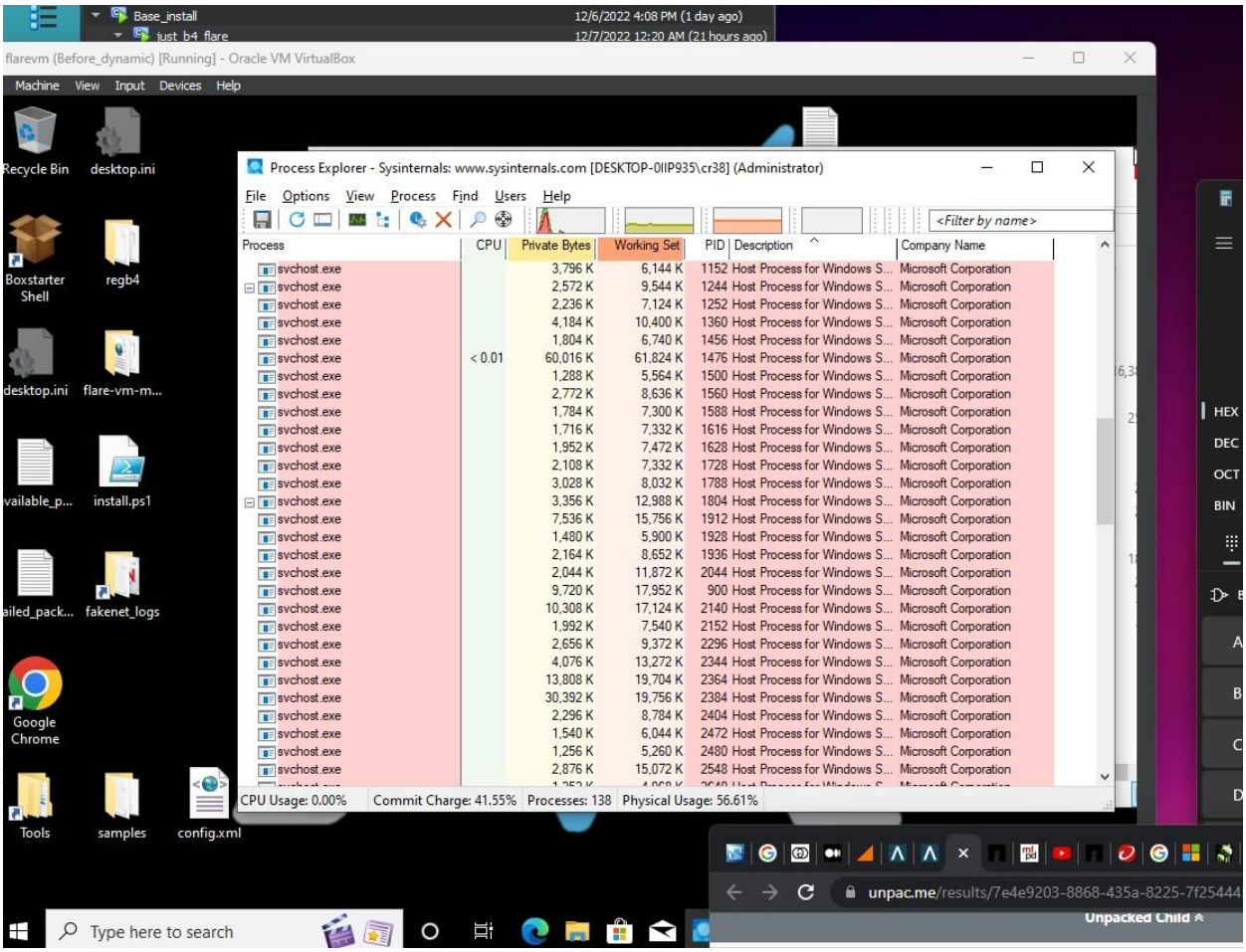
Post information gathering, vm checks and memset, the file filepath for extraction is found.





Realloc call.





All of these svchosts proc are from the malware, I ran it multiple times to get it to do this, also interesting to note, the process goes to sleep after a while, I couldn't find that function as such don't know where he defined it.

So this malware has too many strings to screenshot post runtime, but I will ty to mention a few more that I found.

```
2.5.29.37 wsock32.dll Software\FTPWare\COREFTP\Sites Software\Microsoft\Internet Account Manager value=" Password michael FTP Now
\BlazeFtp IMAP Password nss3.dll WSAStartup ;3+#>6.& WTSGetActiveConsoleSessionId NNTP User Name Software\VanDyke\SecureFX
Technology uM91$D}G CredEnumerateA Software\Microsoft\Internet Explorer\IntelliForms\Storage2 1234567890 StrStrIA account.cfg
Connection: close sqlite3.dll Process32Next HostName \SiteDesigner http://chai-design.com/m.htm?
wXjGYZHrZMwnz2F7g4MsCG9kF4fZ7wIM5ygsBvwtwH GetPrivateProfileStringA wiseftpsrvs.ini StrStrA InternetCreateUrlA iloveyou!
HostDirName kernel32.dll
```

This is a password stealer from the looks of it, with a lot of enumeration and c2 capabilities. This guy wouldn't run for the longest, I had to check Pafish, https://github.com/a0rtega/pafish, for antivm.

I didn’t encounter any c2 communications with tcp socket as such, create etc, but the function was there and I skipped over it., just the strings of fqdn were loaded in and I was able to grab them. This malware uses encryption to exfiltrate data using xor, but hashes it, with sha1/aes.

Remediation :

The malware gets removed, via malawre bytes and/ windows defender, all antivirus detect it via heuristics, but they are not able to tell me what exactly it does. General malware recovery steps will work for this, no fileless persistence as such, just a regedit to allow it start as a service.