MRUPrac.exe

Chandra Kant Bauri

Static Analysis Findings

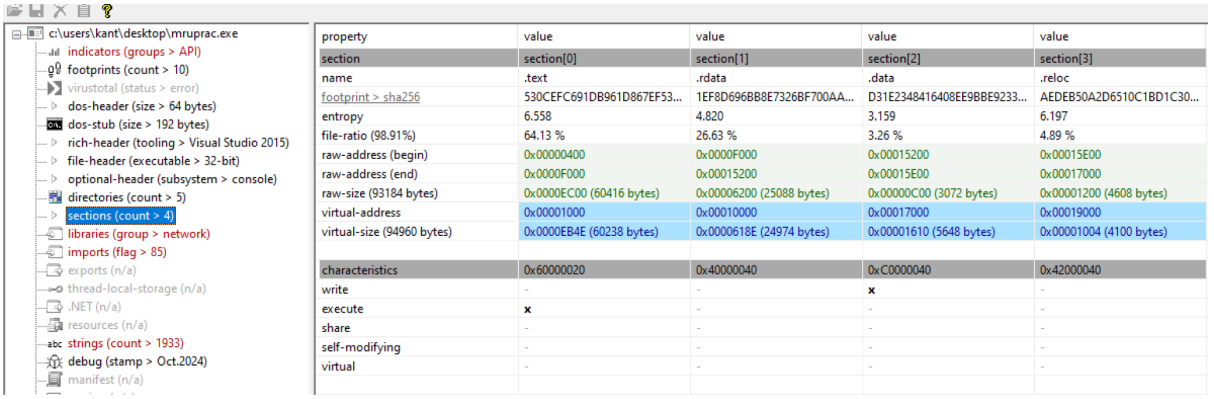
- SHA256 Hash

07f9bb352f46a7b0b99a3768f0ec4518a5d3627862215c1a1a40ab9ce655b1ac

- Interesting Strings

```
DecodePointer
InternetConnection
https://www.byp4ssm3.lol/haha/
Error
Failed to create file.
THALA FOR A REASON
Software\Microsoft\Windows\CurrentVersion\Run
M-a-l-w-a-r-e
Error
Failed Registry.
magic Started
Error
Failed to download image.
Error
Failed wallpaper.
Error
No Internet Found. Exiting.
Error
Anti-VM Triggered. Exiting.
d21pYyBvcyBnZXQgY2FwdGlvbg==
Error
Failed to decode command.
https://pbs.twimg.com/media/F1FbAD9XoAAxLkM.jpg
C:\Public
C:\Public\wallpaper.jpg
QGVjaG8gIkhlbGxvLCB3b3JsZCEi
C:\CheemTapakDumDum.bat
Error
Failed to decode script.
Operations completed successfully!
```

- Packed/Unpacked



property	value	value	value	value
section	section[0]	section[1]	section[2]	section[3]
name	.text	.rdata	.data	.reloc
footprint > sha256	530CEFC691DB961D867EF53...	1EF8D696BB8E7326BF700AA...	D31E2348416408EE9BBE9233...	AEDEB50A2D6510C1BD1C30...
entropy	6.558	4.820	3.159	6.197
file-ratio (98.91%)	64.13 %	26.63 %	3.26 %	4.89 %
raw-address (begin)	0x00000400	0x0000F000	0x00015200	0x00015E00
raw-address (end)	0x0000F000	0x00015200	0x00015E00	0x00017000
raw-size (93184 bytes)	0x0000EC00 (60416 bytes)	0x00006200 (25088 bytes)	0x00000C00 (3072 bytes)	0x00001200 (4608 bytes)
virtual-address	0x00001000	0x00010000	0x00017000	0x00019000
virtual-size (94960 bytes)	0x0000EB4E (60238 bytes)	0x0000618E (24974 bytes)	0x00001610 (5648 bytes)	0x00001004 (4100 bytes)
characteristics	0x60000020	0x40000040	0xC0000040	0x42000040
write	-	-	x	-
execute	x	-	-	-
share	-	-	-	-
self-modifying	-	-	-	-
virtual	-	-	-	-

Entropy is 6.5 and the .text section is present so the malware is not likely packed.

- Any other finding

No Internet Found. Exiting.

Anti-VM Triggered. Exiting.

d21pYyBvcyBnZXQgY2FwdGlvbg==

Failed to decode command.

https://pbs.twimg.com/media/F1FbAD9XoAAxLkM.jpg

C:\Public

C:\Public\wallpaper.jpg

QGVjaG8gIkhlbGxvLCB3b3JsZCEi

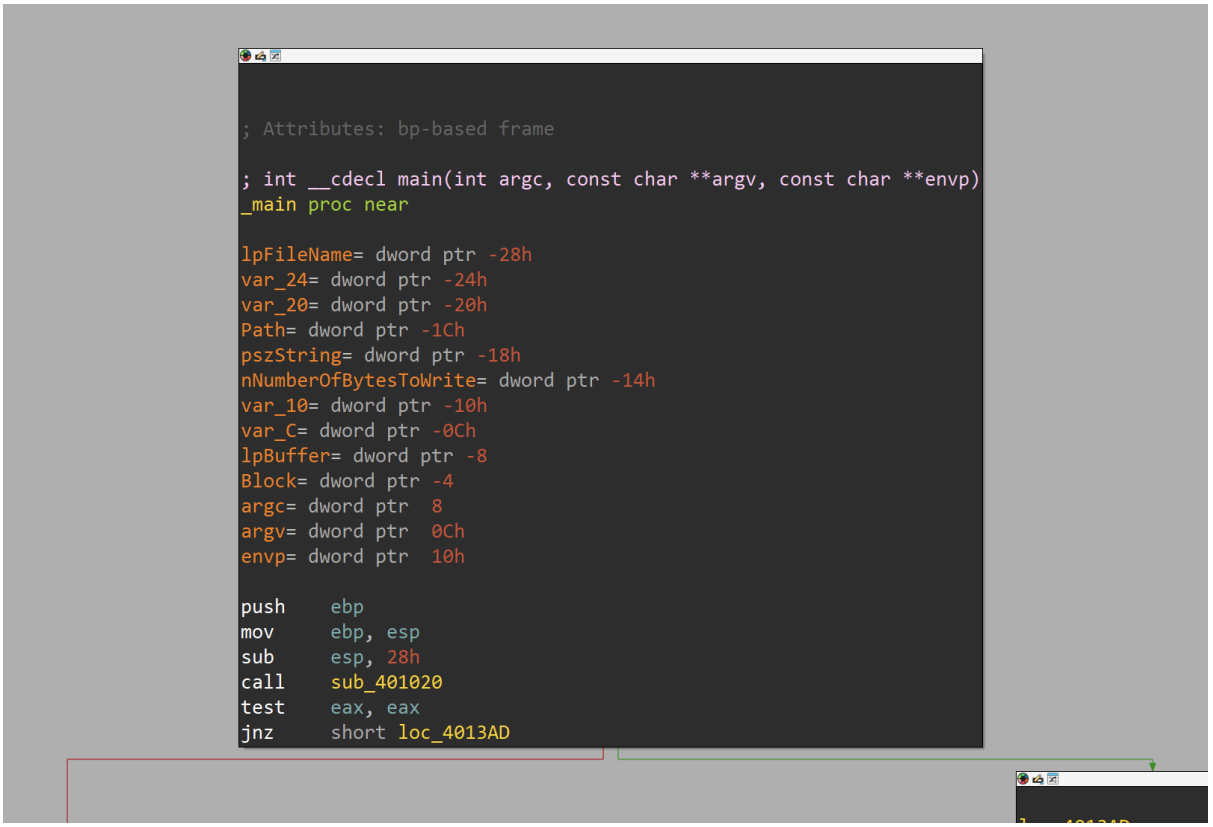
C:\CheemTapakDumDum.bat

Failed to decode script.

Operations completed successfully!

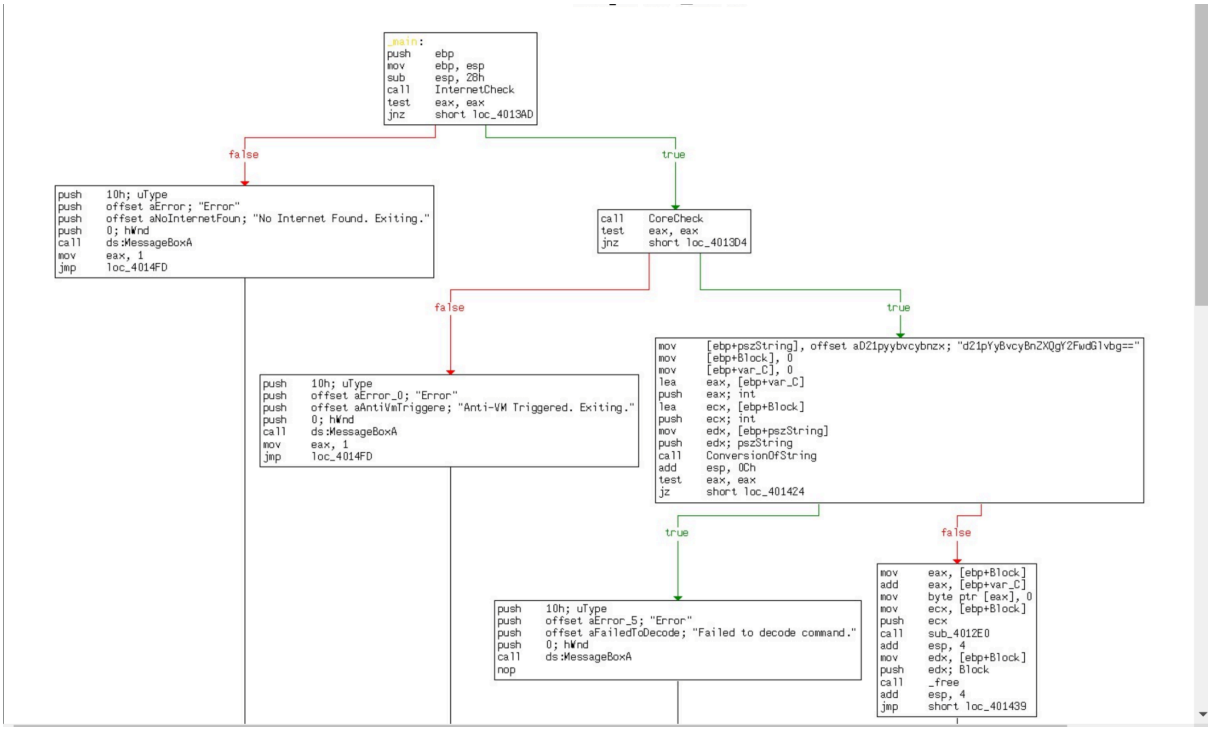
Dynamic Analysis Findings

Main Function

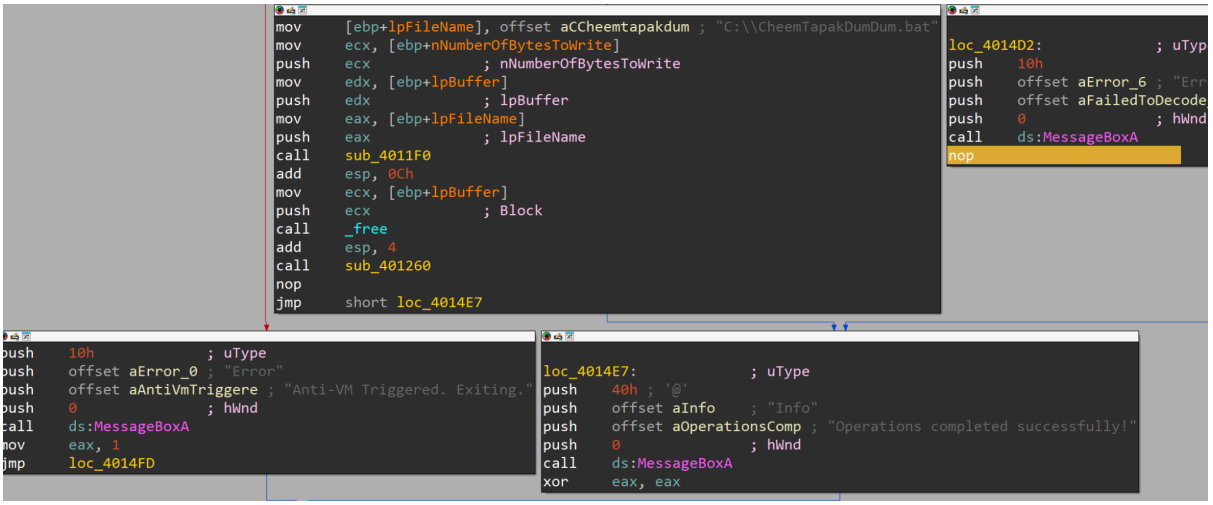


Code Analysis Findings

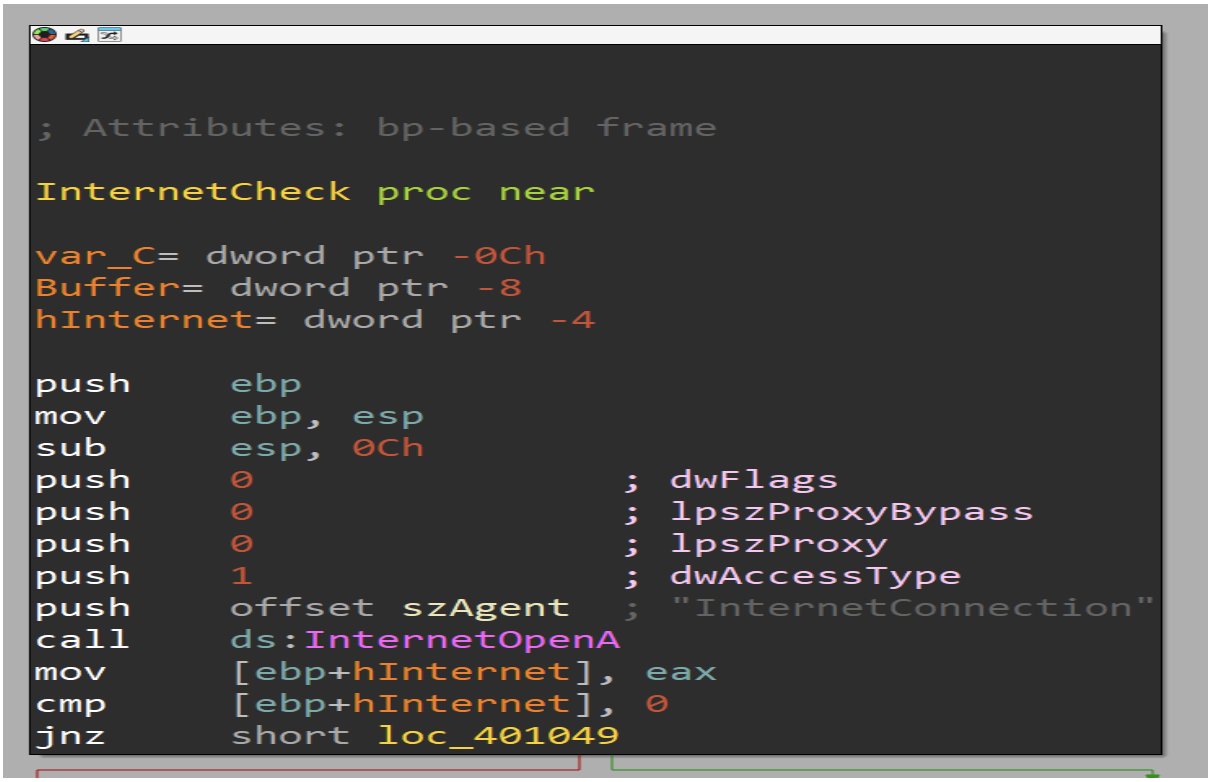
Execution flow



Anti vm techniques

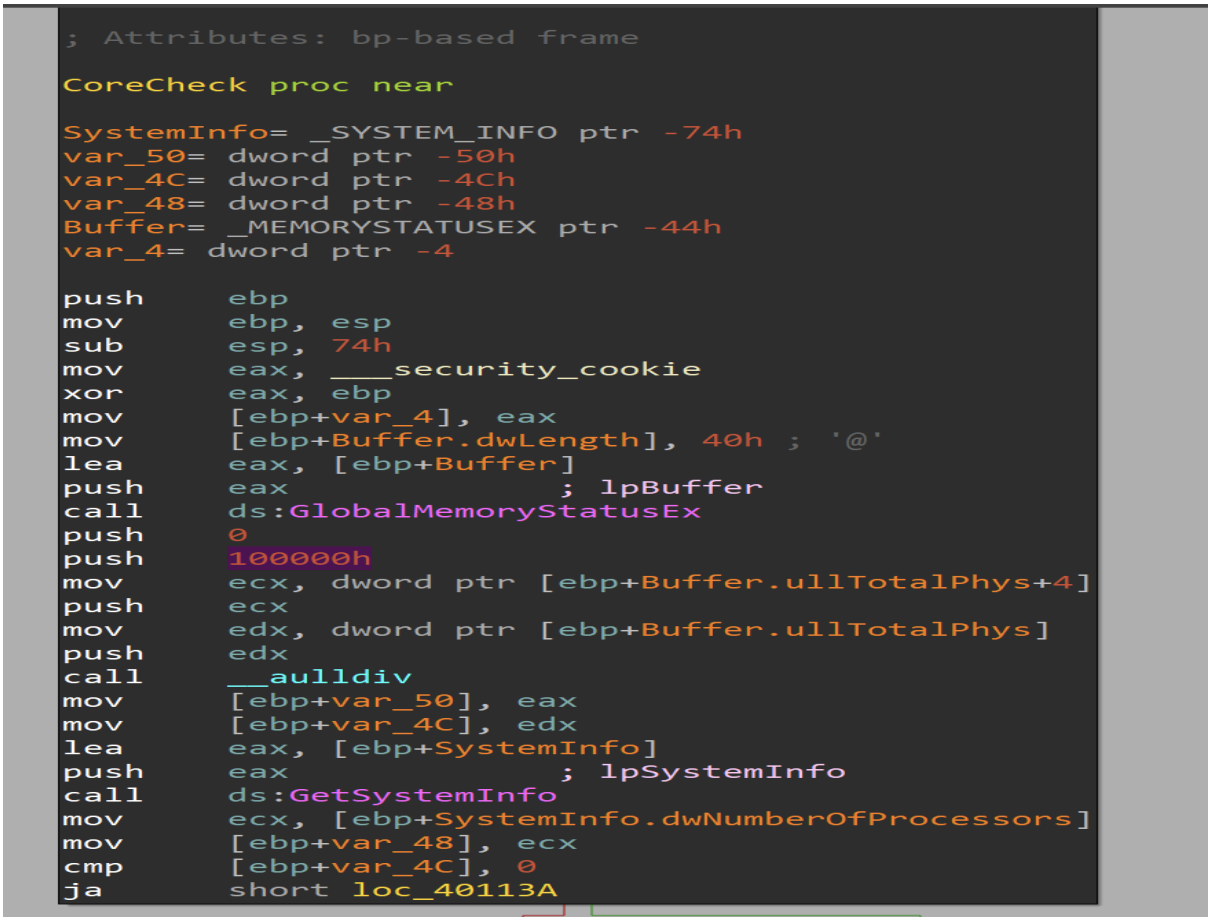


Sample is checking no. of cores, internet connection



```
; Attributes: bp-based frame

InternetCheck proc near

var_C= dword ptr -0Ch
Buffer= dword ptr -8
hInternet= dword ptr -4

push    ebp
mov     ebp, esp
sub     esp, 0Ch
push    0                   ; dwFlags
push    0                   ; lpszProxyBypass
push    0                   ; lpszProxy
push    1                   ; dwAccessType
push    offset szAgent      ; "InternetConnection"
call    ds:InternetOpenA
mov     [ebp+hInternet], eax
cmp     [ebp+hInternet], 0
jnz     short loc_401049
```

Core check

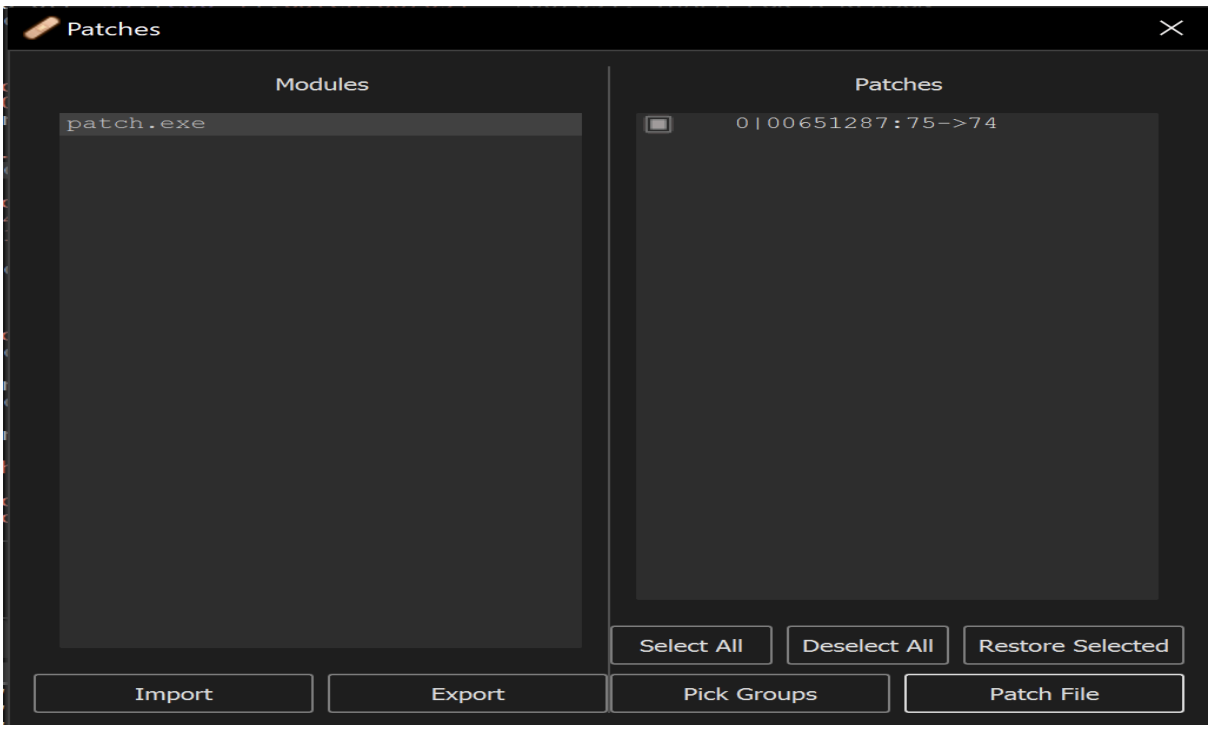


```
; Attributes: bp-based frame

CoreCheck proc near

SystemInfo= _SYSTEM_INFO ptr -74h
var_50= dword ptr -50h
var_4C= dword ptr -4Ch
var_48= dword ptr -48h
Buffer= _MEMORYSTATUSEX ptr -44h
var_4= dword ptr -4

push    ebp
mov     ebp, esp
sub     esp, 74h
mov     eax, ___security_cookie
xor     eax, ebp
mov     [ebp+var_4], eax
mov     [ebp+Buffer.dwLength], 40h ; '@'
lea     eax, [ebp+Buffer]
push    eax                 ; lpBuffer
call    ds:GlobalMemoryStatusEx
push    0
push    100000h
mov     ecx, dword ptr [ebp+Buffer.ullTotalPhys+4]
push    ecx
mov     edx, dword ptr [ebp+Buffer.ullTotalPhys]
push    edx
call    __aulldiv
mov     [ebp+var_50], eax
mov     [ebp+var_4C], edx
lea     eax, [ebp+SystemInfo]
push    eax                 ; lpSystemInfo
call    ds:GetSystemInfo
mov     ecx, [ebp+SystemInfo.dwNumberOfProcessors]
mov     [ebp+var_48], ecx
cmp     [ebp+var_4C], 0
ja      short loc_40113A
```

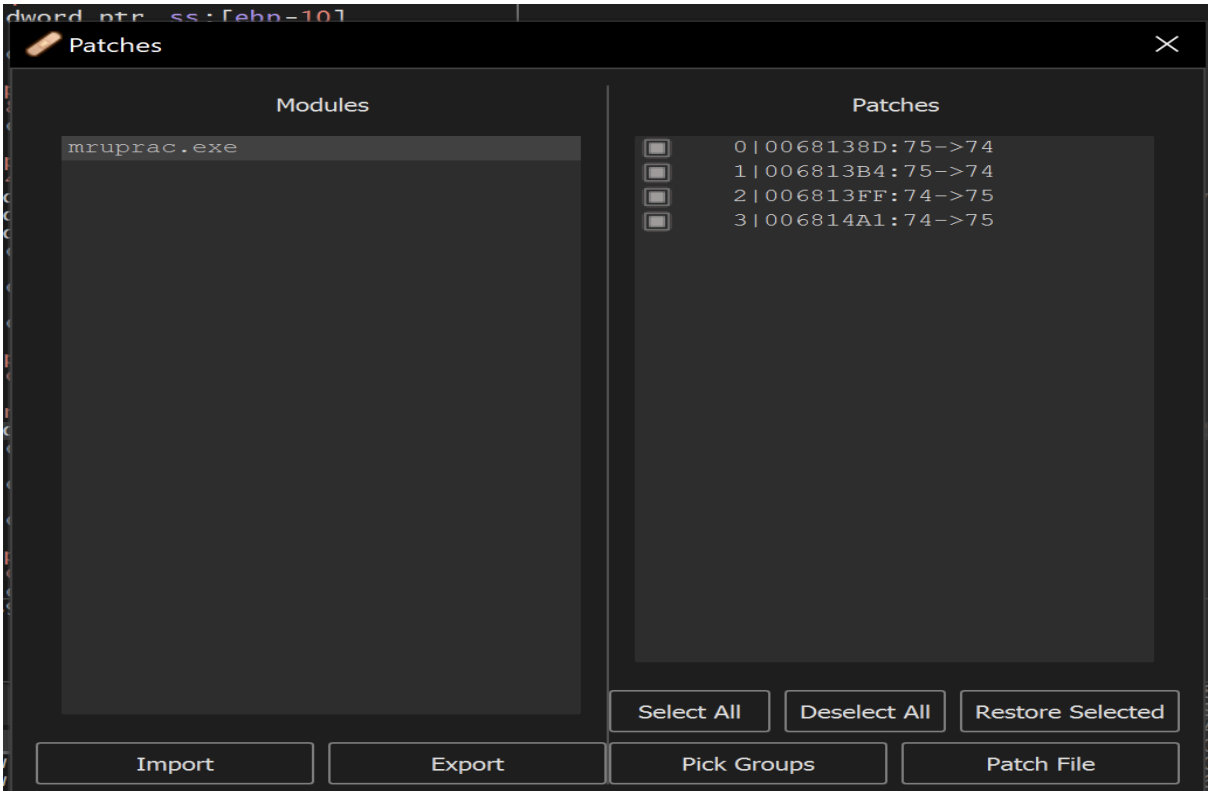
Debugging and Patching

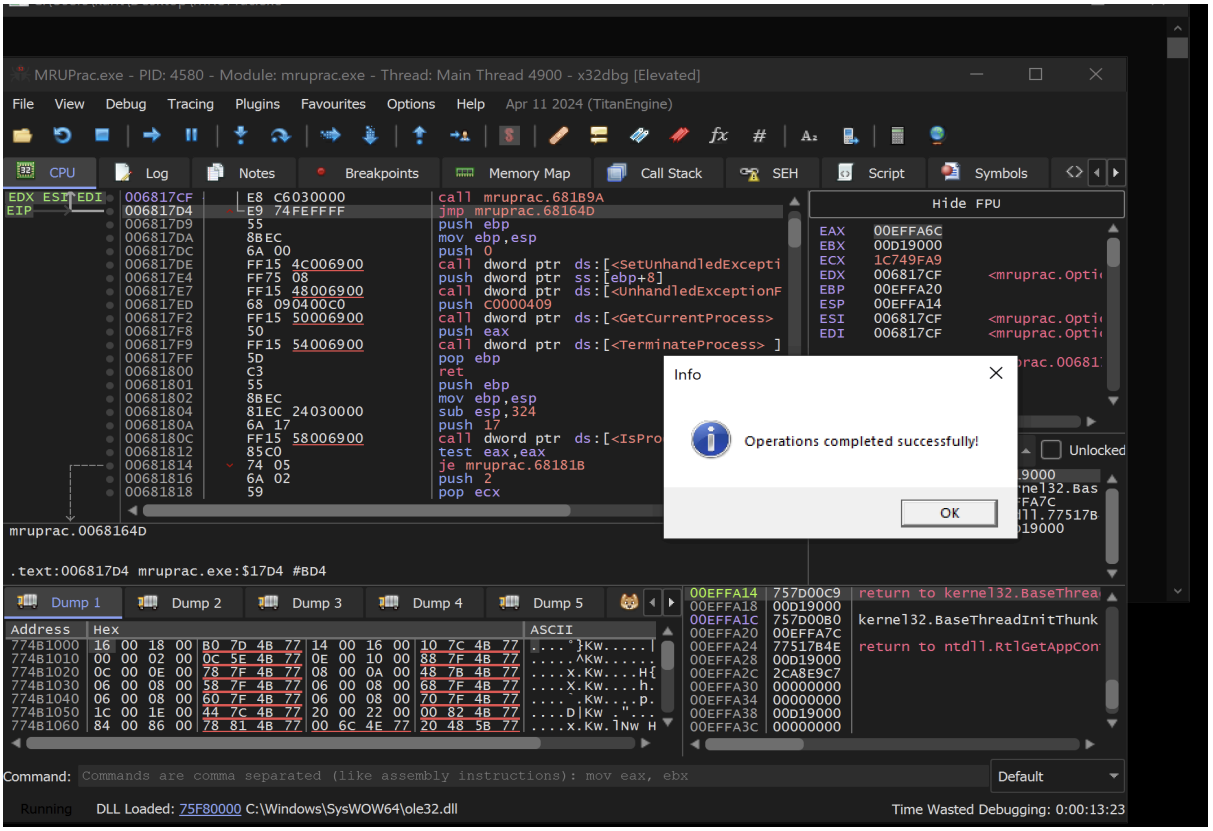
Patches applied.

Internet Patch



Anti VM Patch





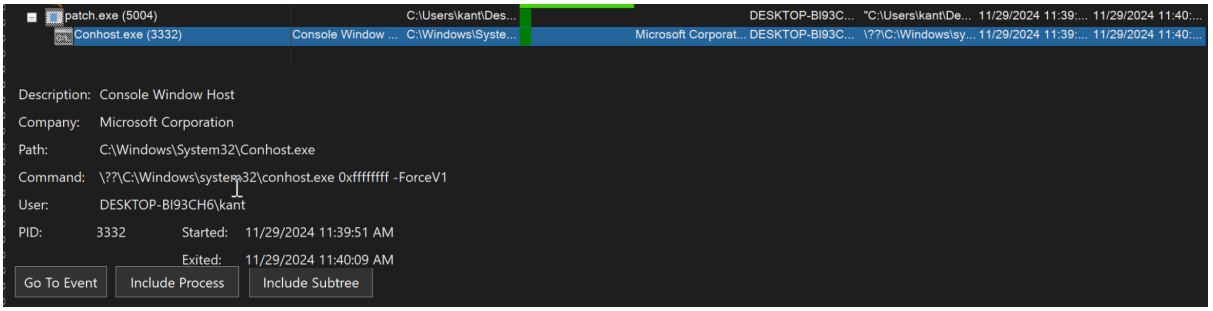
Dynamic Analysis Findings (Part 2)

Findings

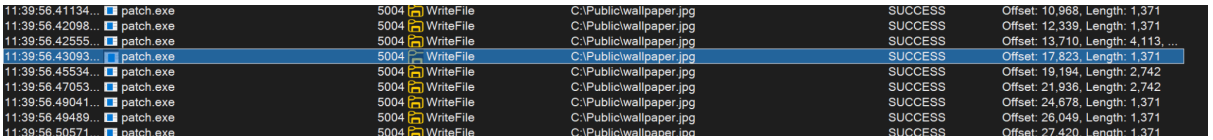
Initial Execution: The sample Changes the wallpaper

Sample is downloading image from this url:
https://pbs.twimg.com/media/F1FbAD9XoAAxLkM.jpg

Process Tree



Sample saves the wallpaper in location: C:\Public\wallpaper.jpg



File Summary: