Ilaria Pedrelli

Progetto fine modulo 6

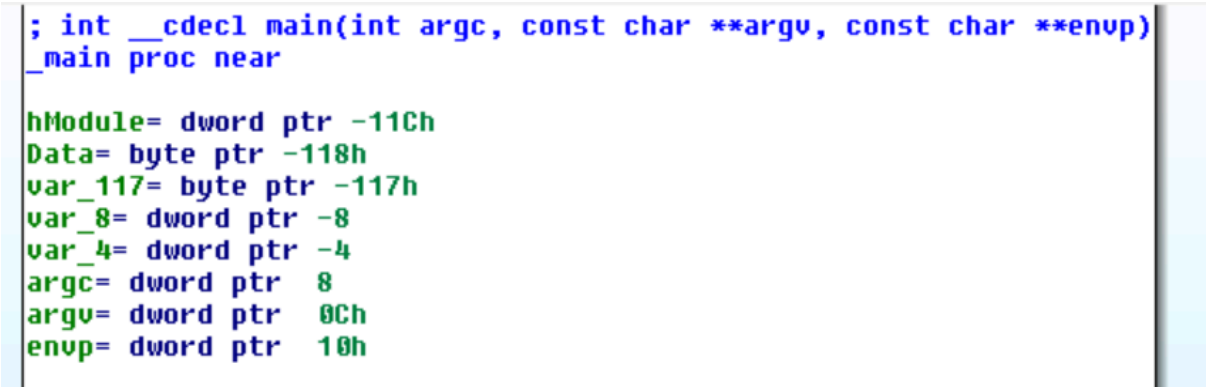
Analisi Statica

1. **Quanti parametri sono passati alla funzione Main()?**

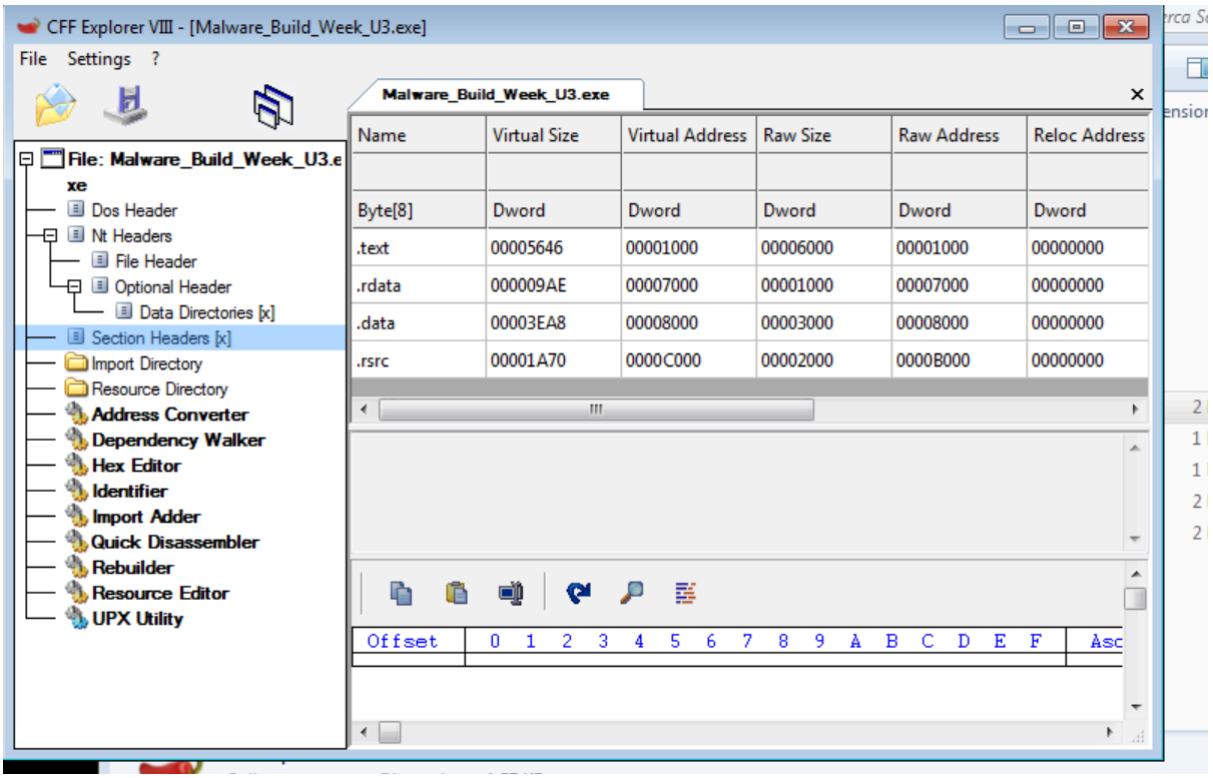
2. **Quante variabili sono dichiarate all'interno della funzione Main()?**

Alla funzione main vengono passati **3 parametri**: Un **int** e due char e **5 variabili**: hModule, Data, var_117, var_8 e var_4.
Le variabili si distinguono dai parametri in quanto sono ad un offset negativo rispetto al registro EBP mentre, argc, argv e envp, essendo parametri, si trovano ad un offset positivo rispetto a EBP.

Di seguito lo screen da IDA:



3. **Quali sezioni sono presenti all'interno del file eseguibile? Descrivete brevemente almeno due di quelle identificate.**

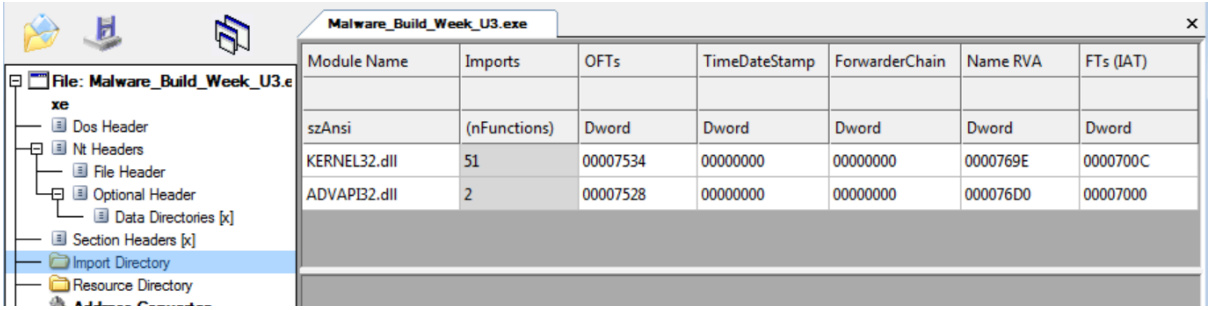


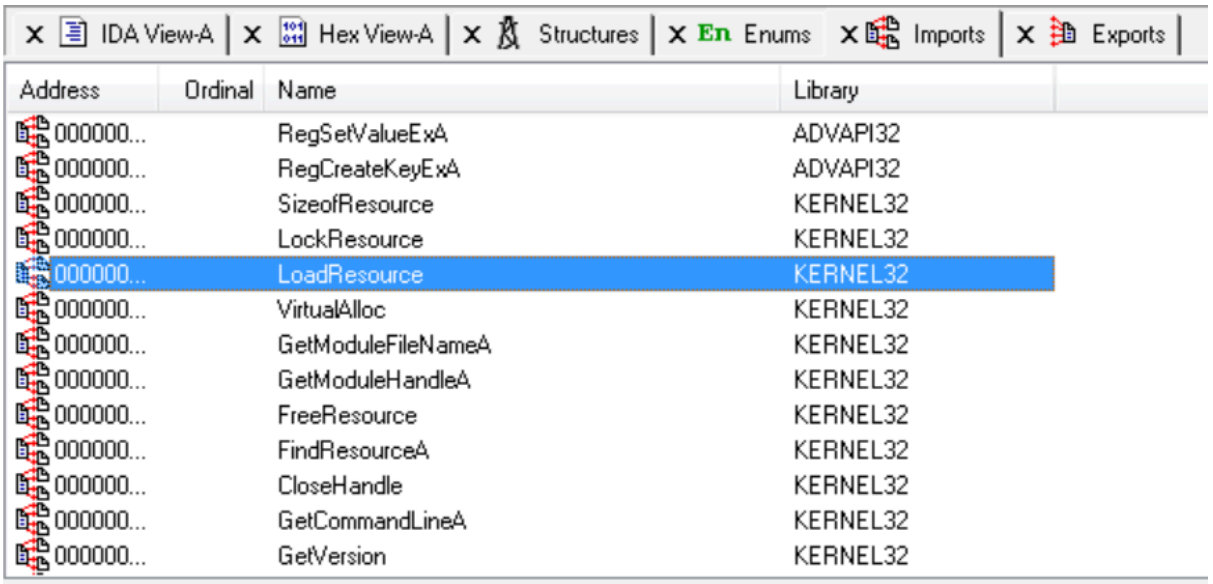
Da CFF posso vedere che le sezioni sono 4: **.text, .data, .rsrc e .rdata.**

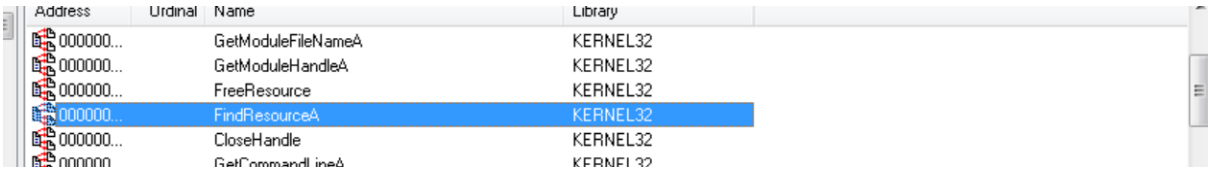
.text: questa sezione contiene le istruzioni che la CPU esegue a software avviato, cioè le righe di codice.

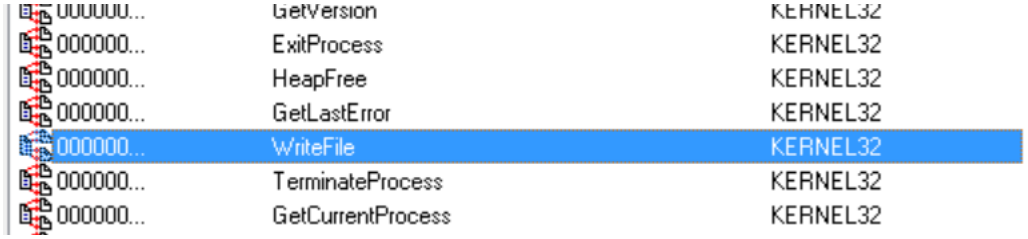
.rsrs: questa sezione include le informazioni circa le librerie e le funzioni importate ed esportate dall'eseguibile.

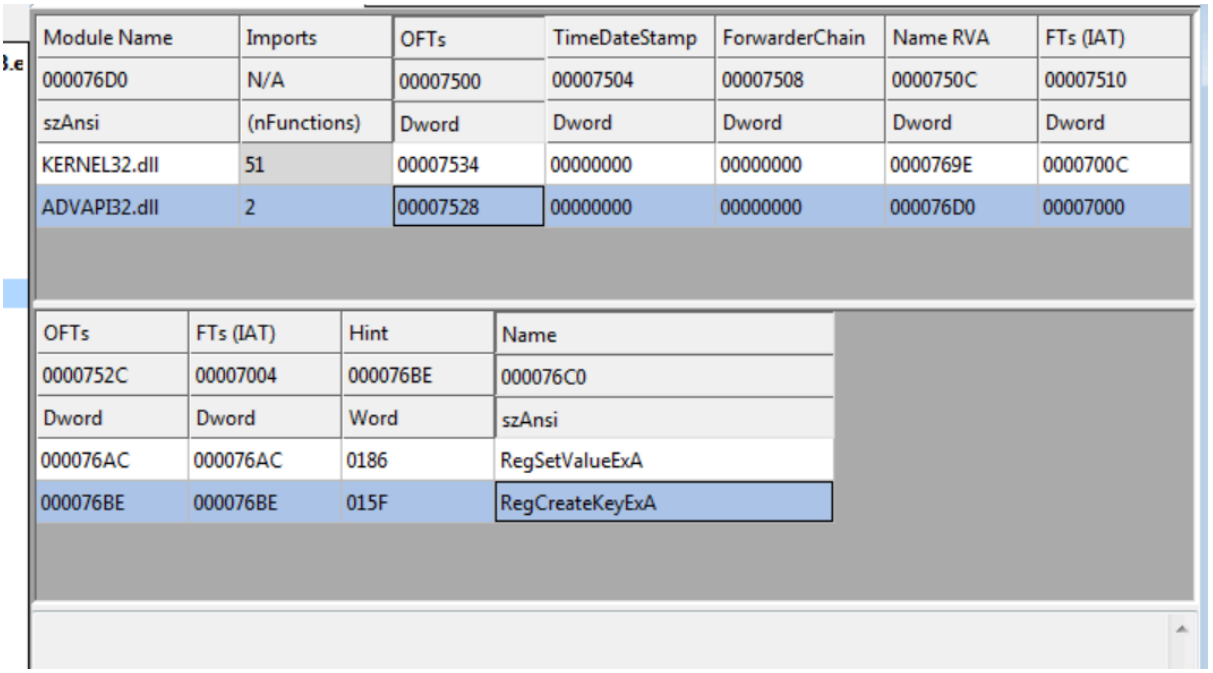
4. **Quali librerie importa il Malware? Per ognuna delle librerie importate, fate delle ipotesi sulla base della sola analisi statica delle funzionalità che il Malware potrebbe implementare. Utilizzate le funzioni che sono richiamate all'interno delle librerie per supportare le vostre ipotesi.**











Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
000076D0	N/A	00007500	00007504	00007508	0000750C	00007510
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	51	00007534	00000000	00000000	0000769E	0000700C
ADVAPI32.dll	2	00007528	00000000	00000000	000076D0	00007000

OFTs	FTs (IAT)	Hint	Name
0000752C	00007004	000076BE	000076C0
Dword	Dword	Word	szAnsi
000076AC	000076AC	0186	RegSetValueExA
000076BE	000076BE	015F	RegCreateKeyExA

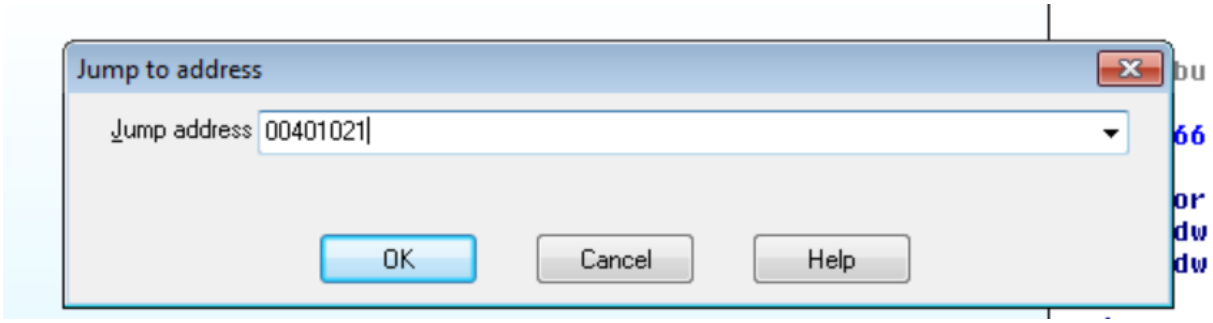
Il Malware importa due librerie, la **KERNEL32.dll** e **ADVAPI.dll**. Concentrandoci sulle funzioni chiamate nella KERNEL32 possiamo notare le APIs **LoadRosource, FinResource** e **LockRosource** tipiche dei malware di tipo Dropper che utilizzano queste APIs per localizzare all'interno della sezione «risorse» il malware da estrarre, e successivamente da caricare in memoria per l'esecuzione o da salvare sul disco per esecuzione futura. In questo caso, notiamo che tra le funzioni c'è anche un **CreateFile** e **WriteFile** utilizzato dal malware per creare un file vuoto e scrivere al suo interno il malware appena estratto e salvarlo.
Nell'altra libreria, invece, sono contenute funzioni che vanno a creare e modificare le chiavi di registro.

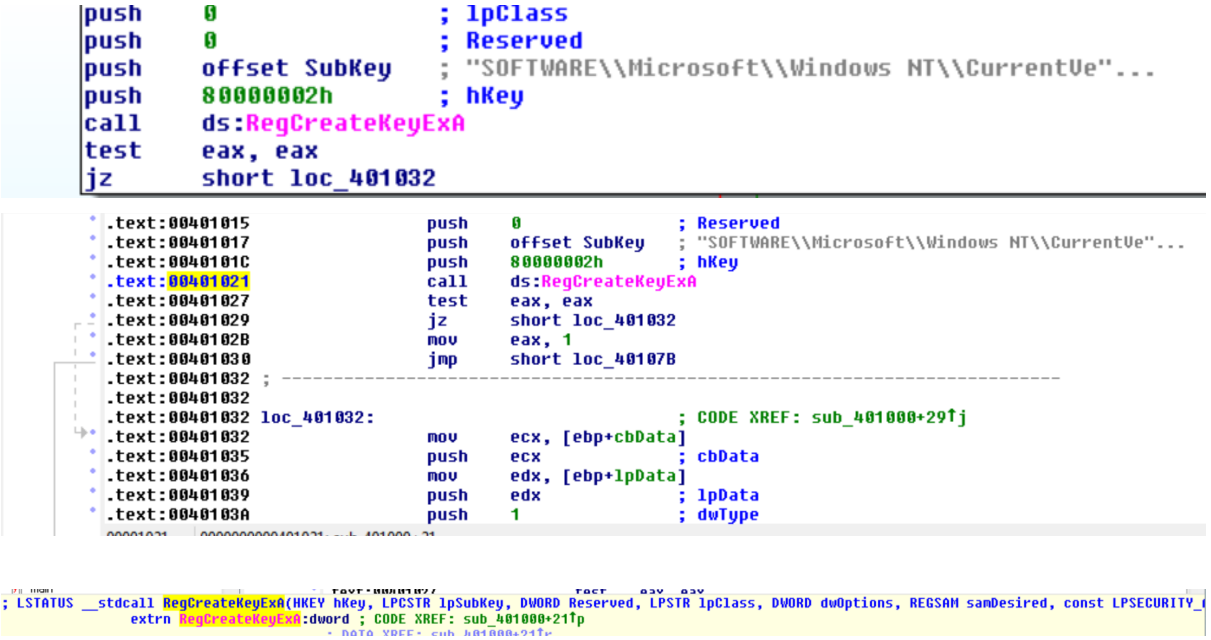
Tools utilizzati: CFF Explorer e IDA pro.

Malware Analysis

5. **Lo scopo della funzione chiamata alla locazione di memoria 00401021**

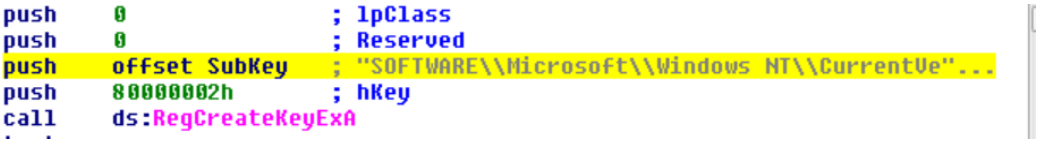
6. **Come vengono passati i parametri alla funzione alla locazione 00401021;**





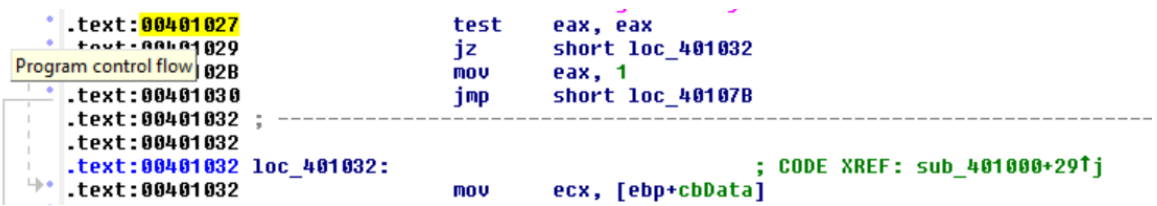
Nella Locazione di memoria 00401021 si trova una **call**, un'istruzione utilizzata per chiamare una funzione. In questo caso la funzione chiamata è **RegCreateKeyExa** cioè una funzione che permette di creare o aprire una chiave di registro già esistente. Vediamo che i parametri sono passati sullo stack tramite istruzione **push**. Se la subkey è già esistente la apre altrimenti verrà creata.

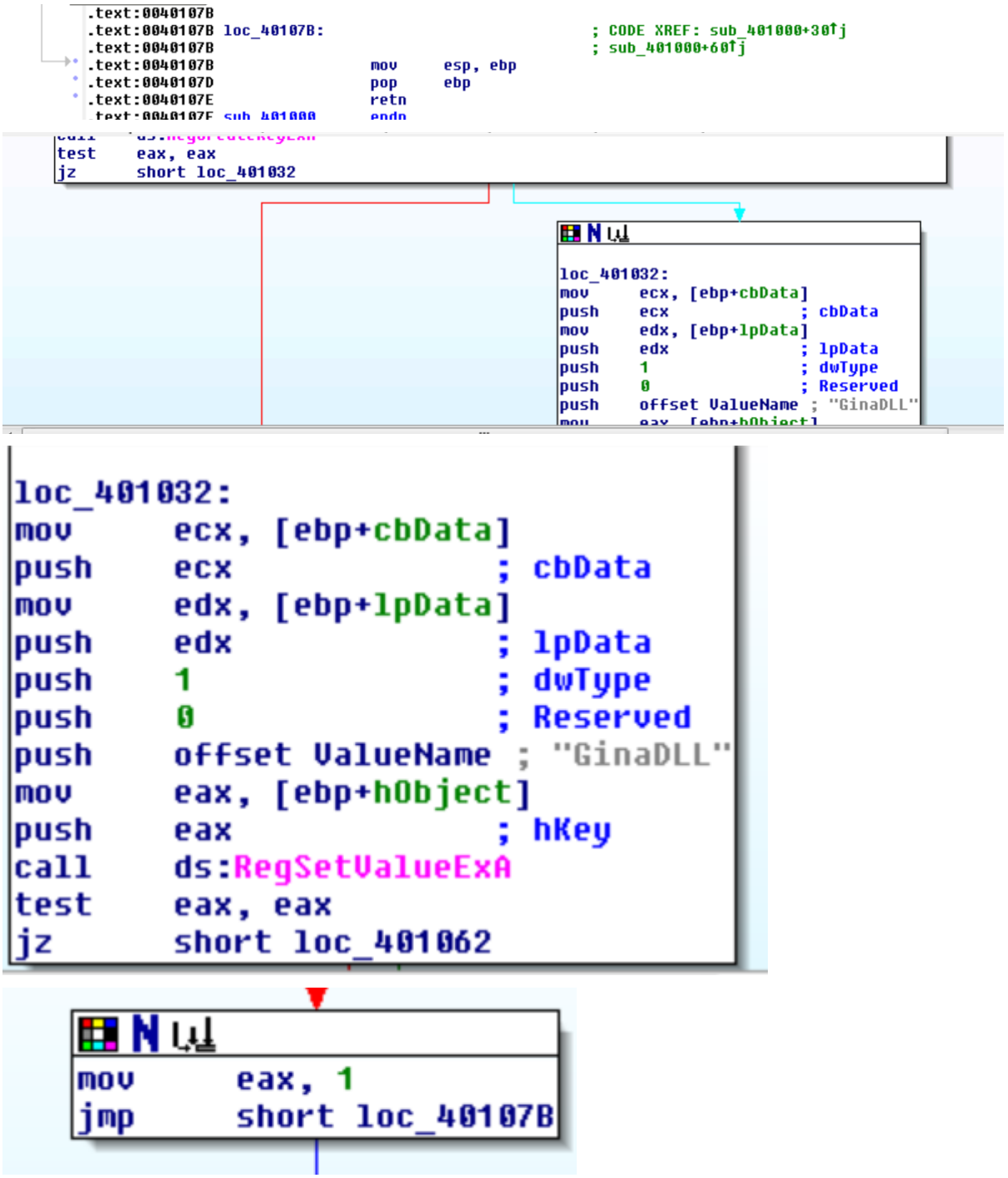
7. **Che oggetto rappresenta il parametro alla locazione 00401017**



L'oggetto rappresentato è l'offset della stringa "SubKey". La subkey è un valore/sottocartella contenuto in una chiave di registro.

8. **Il significato delle istruzioni comprese tra gli indirizzi 00401027 e 00401029.**





Tra le **istruzioni comprese tra gli indirizzi 00401027 e 00401029 troviamo** l'istruzione condizionale **Test** che verifica un valore senza modificare il contenuto del registro ma "setta" lo zero flag a 1 solo se il risultato è zero. Viene utilizzato per controllare se un valore è zero o meno.

- **test eax, eax**: verificherà che eax sia zero e in tal caso imposterà il zero flag.

- **jz short loc_401032**: istruzione di salto condizionale, se il Zero flag è impostato, il controllo salta a loc_401032.

Se dovessimo tradurre il codice Assembly il relativo costrutto in C sarebbe:

```
if (eax == 0) {
   // Codice da eseguire se eax è zero (istruzioni contenute nelle due locazioni)
}
```

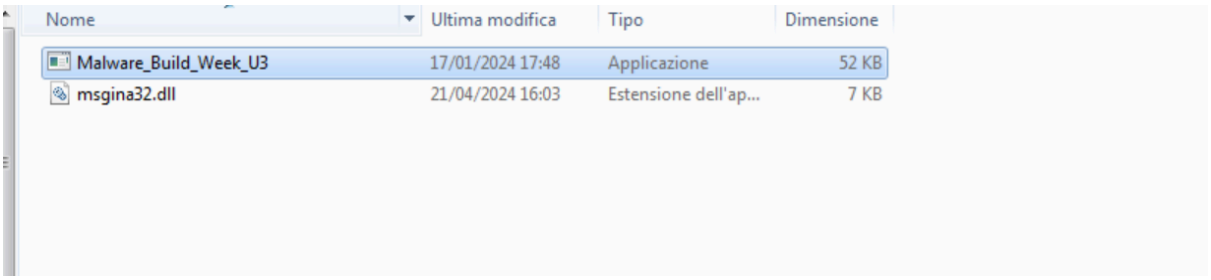
9. **Valutate ora la chiamata alla locazione 00401047, qual è il valore del parametro «ValueName»?**

```
.text:0040103C    push    0               ; Reserved
.text:0040103E    push    offset ValueName ; "GinaDLL"
.text:00401043    mov     eax, [ebp+hObject]
.text:00401046    push    eax             ; hKey
.text:00401047    call    ds:RegSetValueExA
```

Il valore di ValueName è la stringa "GinaDLL" che viene quindi passata come parametro alla funzione RegSetValueExA.

Analisi Dinamica

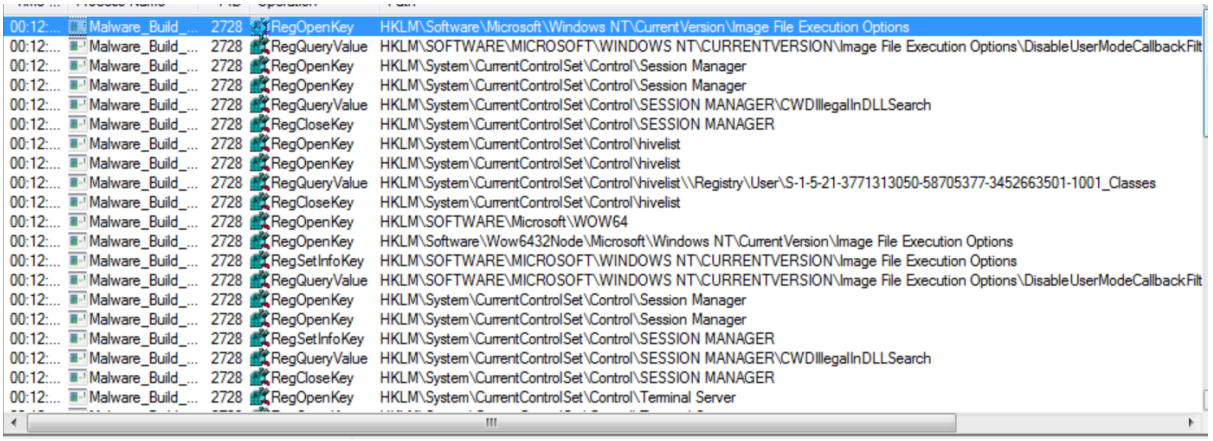
10. **Cosa notate all'interno della cartella dove è situato l'eseguibile del Malware? Spiegate cosa è avvenuto, unendo le evidenze che avete raccolto finora per rispondere alla domanda**



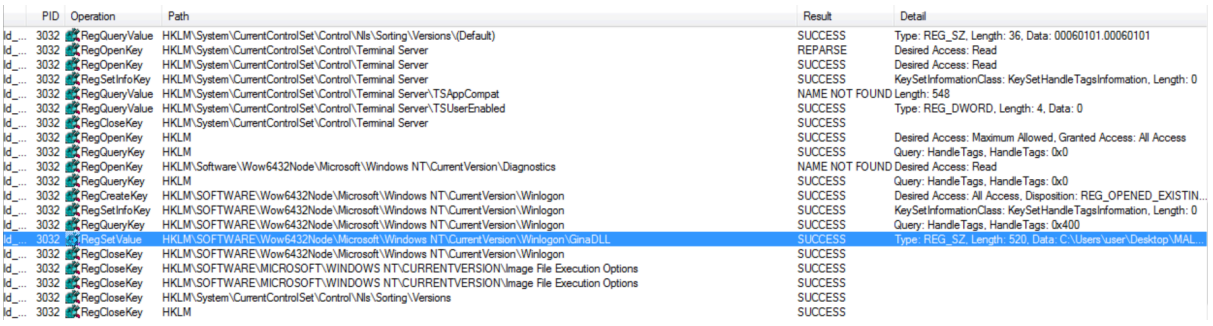
Nella cartella viene creata la libreria **msgina32.dll**. "GinaDLL" viene caricato dal sistema in HKLM per poi essere passata come parametro alla funzione RegSetValueExA per modificarne il valore o sostituirlo.

11. Quale chiave di registro viene creata?

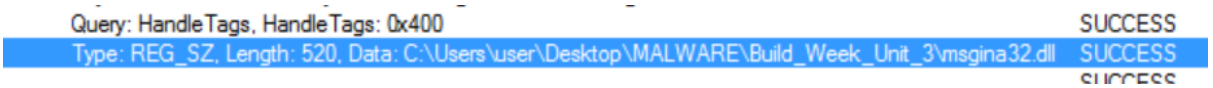
12. -Quale valore viene associato alla chiave di registro creata?



00:12:...	Malware_Build_...	2728	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
00:12:...	Malware_Build_...	2728	RegQueryValue	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\Image File Execution Options\DisableUserModeCallbackFilt
00:12:...	Malware_Build_...	2728	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager
00:12:...	Malware_Build_...	2728	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager
00:12:...	Malware_Build_...	2728	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANAGER\CWDIllegalInDLLSearch
00:12:...	Malware_Build_...	2728	RegCloseKey	HKLM\System\CurrentControlSet\Control\SESSION MANAGER
00:12:...	Malware_Build_...	2728	RegOpenKey	HKLM\System\CurrentControlSet\Control\hivelist
00:12:...	Malware_Build_...	2728	RegOpenKey	HKLM\System\CurrentControlSet\Control\hivelist
00:12:...	Malware_Build_...	2728	RegQueryValue	HKLM\System\CurrentControlSet\Control\hivelist\\Registry\User\S-1-5-21-3771313050-58705377-3452663501-1001_Classes
00:12:...	Malware_Build_...	2728	RegCloseKey	HKLM\System\CurrentControlSet\Control\hivelist
00:12:...	Malware_Build_...	2728	RegOpenKey	HKLM\SOFTWARE\Microsoft\WOW64
00:12:...	Malware_Build_...	2728	RegOpenKey	HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
00:12:...	Malware_Build_...	2728	RegSetInfoKey	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\Image File Execution Options
00:12:...	Malware_Build_...	2728	RegQueryValue	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\Image File Execution Options\DisableUserModeCallbackFilt
00:12:...	Malware_Build_...	2728	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager
00:12:...	Malware_Build_...	2728	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager
00:12:...	Malware_Build_...	2728	RegSetInfoKey	HKLM\System\CurrentControlSet\Control\SESSION MANAGER
00:12:...	Malware_Build_...	2728	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANAGER\CWDIllegalInDLLSearch
00:12:...	Malware_Build_...	2728	RegCloseKey	HKLM\System\CurrentControlSet\Control\SESSION MANAGER
00:12:...	Malware_Build_...	2728	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server



	PID	Operation	Path	Result	Detail
ld_...	3032	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions\(Default)	SUCCESS	Type: REG_SZ, Length: 36, Data: 00060101.00060101
ld_...	3032	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	REPARSE	Desired Access: Read
ld_...	3032	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	Desired Access: Read
ld_...	3032	RegSetInfoKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
ld_...	3032	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	NAME NOT FOUND	Length: 548
ld_...	3032	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSUserEnabled	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
ld_...	3032	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	
ld_...	3032	RegOpenKey	HKLM	SUCCESS	Desired Access: Maximum Allowed, Granted Access: All Access
ld_...	3032	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
ld_...	3032	RegOpenKey	HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Diagnostics	NAME NOT FOUND	Desired Access: Read
ld_...	3032	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
ld_...	3032	RegCreateKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	Desired Access: All Access, Disposition: REG_OPENED_EXISTIN...
ld_...	3032	RegSetInfoKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
ld_...	3032	RegQueryKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	Query: HandleTags, HandleTags: 0x400
ld_...	3032	RegSetValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL	SUCCESS	Type: REG_SZ, Length: 520, Data: C:\Users\user\Desktop\MAL...
ld_...	3032	RegCloseKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	
ld_...	3032	RegCloseKey	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\Image File Execution Options	SUCCESS	
ld_...	3032	RegCloseKey	HKLM\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\Image File Execution Options	SUCCESS	
ld_...	3032	RegCloseKey	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versions	SUCCESS	
ld_...	3032	RegCloseKey	HKLM	SUCCESS	

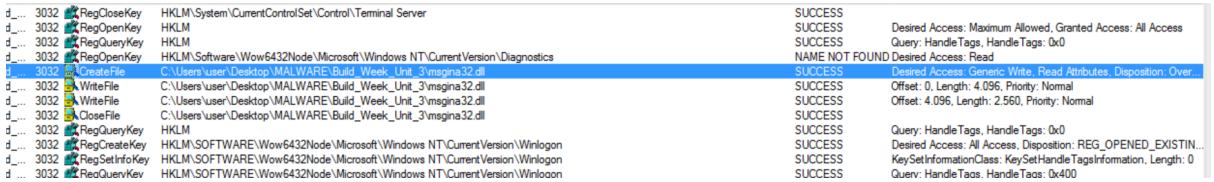


Query: HandleTags, HandleTags: 0x400	SUCCESS
Type: REG_SZ, Length: 520, Data: C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3\msgina32.dll	SUCCESS

Da una analisi su Procmon possiamo notare che viene creata la chiave **HKEY_LOCAL_MACHINE (HKLM)**: dove sono contenuti i record e le configurazioni della macchina

Con riguardo al file creato nella cartella: msgina32.dll. Il parametro passato è GinaDLL (Graphical Identification and Authentication Dynamic Link Library) un importante componente per il processo di avvio di Windows.
La funzione API del parametro è **RegsetValue** che viene utilizzata per impostare il valore di una chiave di registro, in questo caso notiamo che il path porta alla libreria creata in precedenza Gina.dll.

13. Quale chiamata di sistema ha modificato il contenuto della cartella dove è presente l'eseguibile del Malware?



d_...	3032	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	
d_...	3032	RegOpenKey	HKLM	SUCCESS	Desired Access: Maximum Allowed, Granted Access: All Access
d_...	3032	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
d_...	3032	RegOpenKey	HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Diagnostics	NAME NOT FOUND	Desired Access: Read
d_...	3032	CreateFile	C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3\msgina32.dll	SUCCESS	Desired Access: Generic Write, Read Attributes, Disposition: Over...
d_...	3032	WriteFile	C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3\msgina32.dll	SUCCESS	Offset: 0, Length: 4.096, Priority: Normal
d_...	3032	WriteFile	C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3\msgina32.dll	SUCCESS	Offset: 4.096, Length: 2.560, Priority: Normal
d_...	3032	CloseFile	C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3\msgina32.dll	SUCCESS	
d_...	3032	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
d_...	3032	RegCreateKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	Desired Access: All Access, Disposition: REG_OPENED_EXISTIN...
d_...	3032	RegSetInfoKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
d_...	3032	RegQueryKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	Query: HandleTags, HandleTags: 0x400

Con la funzione **CreateFile** possiamo notare che è stato generato un file.dll quindi una libreria all'interno della cartella del malware. In questo caso msgina32.dll.

14. Unite tutte le informazioni raccolte fin qui sia dall'analisi statica che dall'analisi dinamica per delineare il funzionamento del Malware.

Dalle analisi effettuate, possiamo dedurre che si tratta di un programma malevolo che contiene al suo interno un malware. Dalla analisi delle librerie importate e dalle modifiche alle chiavi di registro, possiamo dedurre che si tratti presumibilmente di un Dropper che viene salvato su disco per l'esecuzione futura (avvio del sistema operativo). Dalla modifica, o probabilmente sostituzione, della libreria msgina32.dll possiamo dedurre che il malware verrà avviato durante il processo di accesso. Gina.dll infatti, è una libreria che gestisce il processo di autenticazione degli utenti e viene chiamata durante il processo di avvio del sistema operativo per fornire l'interfaccia utente per la sua identificazione. Con la sostituzione del valore di msgina32.dll, il malware crea persistenza all'interno del sistema operativo e quindi si riavvierà ogni volta che verrà riavviato il sistema tramite questa libreria.