Malware Analysis

Il Malware da analizzare è nella cartella **Build_Week_Unit_3** presente sul desktop della macchina virtuale.

Analisi statica

- *Quanti parametri sono passati alla funzione Main()?*

```
; int __cdecl main(int argc,const char **argv,const char *envp)
_main proc near

hModule= dword ptr -11Ch
Data= byte ptr -118h
var_8= dword ptr -8
var_4= dword ptr -4
argc= dword ptr  8
argv= dword ptr  0Ch
envp= dword ptr  10h
```

Apriamo il malware sopracitato con IDA pro.
Ida ci posiziona nell'albero mostrando la funzione main e relativi parametri:

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

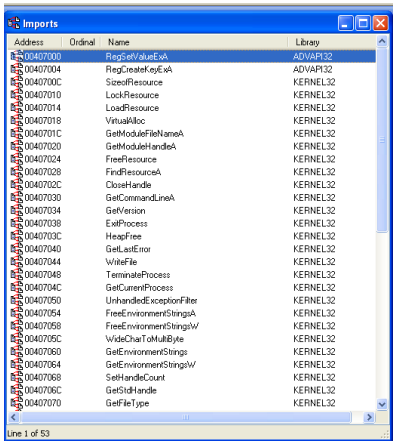
Per parametro si intendono le variabili passate alla funzione, si possono notare in blu dopo la "main (" o, nelle scritte in verde in basso dove l'offset è positivo (dove non c'è un "-" nella parte verde a dx della corrispondente linea):
argc, argv, envp
le restanti, con offset negativo, sono variabili,
hModule, Data, var_8, var_4

- *Quali sezioni sono presenti all'interno del file eseguibile? Descrivete brevemente almeno 2 di quelle identificate*

Notiamo diverse sezioni nel codice:

In celeste c'è del codice generato dalle librerie,
in blu il codice scritto dal'utente,
in rosso il codice generato dal compilatore,
il resto si tratta dati, o sezioni che non contengono codice

- *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.*



Ora andiamo nella view riguardante gli **imports**, notiamo 2 librerie usate dall'eseguibile:
ADVAPI32:
Dalle funzioni di chiamate dalla libreria, RegSetValueExA & RegCreateKeyExA, si nota che il malware crea e valorizza delle chiavi di registro
KERNEL32:
Questa è una libreria con tutte le funzioni per permettere al pc di funzionare correttamente; vediamo dei lock e dei load resources, diverse operazioni con i processi, write file…

- *Lo scopo della funzione chiamata alla locazione di memoria 00401021*

Nella top bar in alto, “Jump”, “Jump to Address” e scriviamo 00401021, ci viene mostrata la funzione RegCreateKeyExA, una funzione che serve a creare una specifica chiave di registro

- *Come vengono passati i parametri alla funzione alla locazione 00401021;*

Sappiamo che i parametri per queste funzioni sono pushati nello stack di memoria poche righe prima:

```
push    ebp
mov     ebp, esp
push    ecx
push    0               ; lpdwDisposition
lea     eax, [ebp+hObject]
push    eax             ; phkResult
push    0               ; lpSecurityAttributes
push    0F003Fh         ; samDesired
push    0               ; dwOptions
push    0               ; lpClass
push    0               ; Reserved
push    offset SubKey   ; "SOFTWARE\\Microsoft\\Windows NT\\CurrentVe"...
push    80000002h       ; hKey
call    ds:RegCreateKeyExA
test    eax, eax
jz      short loc_401032
```

IDA provvede a mettere dei commenti che aiutano ad identificare che parametri stiamo passando

- *Che oggetto rappresenta il parametro alla locazione 00401017*

00401017 invece ci porta all’istruzione “push offset SubKey” poco sopra.
Togliendo la parte dopo il punto e virgola che si tratta di un commento (il contenuto di “SubKey”), questa istruzione va ad aggiungere in cima allo stack di memoria, pusha, l’indirizzo si SubKey

- *I significato delle istruzioni comprese tra gli indirizzi 00401027 e 00401029.*

tra 00401027 e 00401029 sono contenute le varie istruzioni per il push in memoria dei vari parametri per la regCreateKeyExA nello screen sopra.
Cosa importante da notare, è che come “phkResult” è stato usato il registro EAX.
phkResult è un parametro di OUTPUT della funzione, che contiene l’indirizzo di memoria della nuova chiave creata, per una lettura più rapida ed informata, si può consultare il sito ufficiale Microsoft:

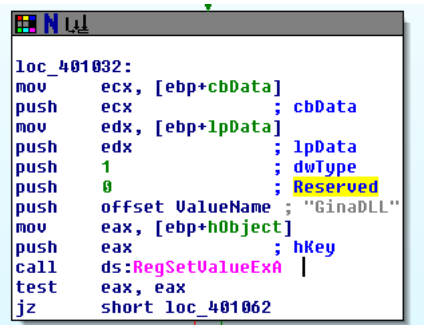
Subito dopo la chiamata della funzione regCreateKeyExA con l’istruzione call, viene fatto un test, se il contenuto di EAX non è 0, quindi è stata creata la chiave nel registro, lo ZeroFlag viene messo a 1, quindi con JZ, salta a loc_401032

- *Con riferimento all’ultimo quesito, tradurre il codice Assembly nel corrispondente costrutto C.*

EAX = RegCreateKeyExA(0, 983103, 0, 0, 0, subkey)
If(EAX != 0) {
… codice di loc_401032
}

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

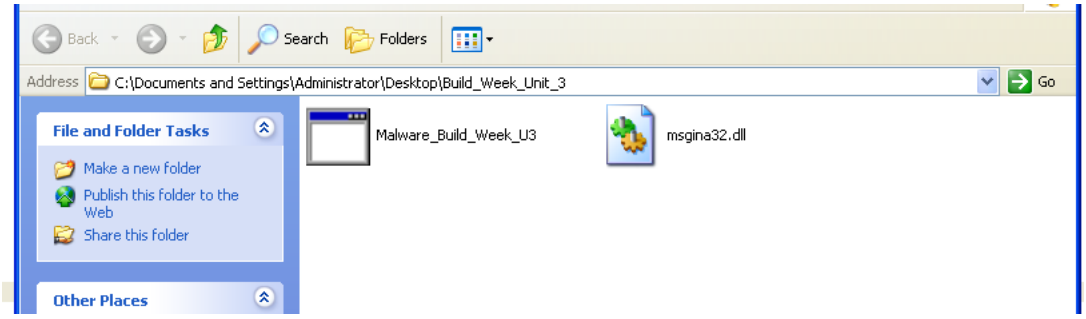
L'indirizzo 00401047 ci porta ad una serie di istruzioni che si concludono con il set del valore della chiave registro sopra creata. Nella riga di "push offset ValueName" si sta assegnando il valore alla chiave creata, dal commento di IDA ci viene suggerito che il nome sia "GinaDLL"



Analisi dinamica

- *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*

Notiamo che viene creato un file dopo l'esecuzione del programma:



- *Analizzate ora i risultati di Process Monitor*

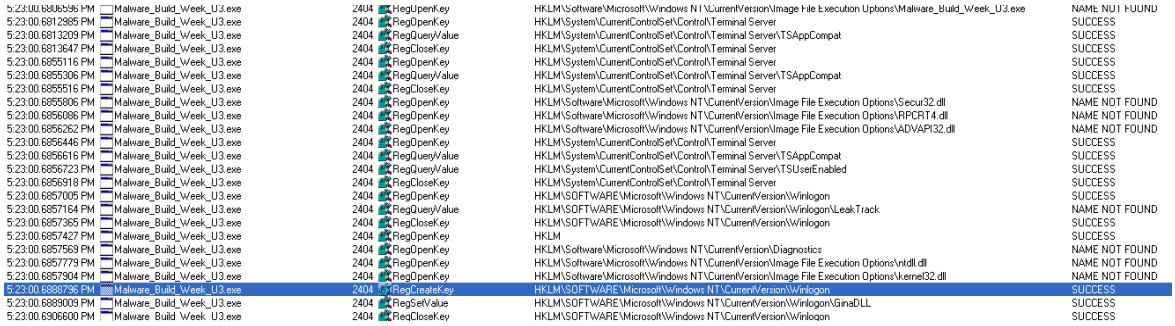
Dall'analisi statica abbiamo visto che c'erano dei processi che creavano dei file, non siamo andati nel dettaglio, ma sono stati visti nella tabella di funzioni importate.

L'ulteriore conferma ce la da ProcMon:

5:23:00.6856918 PM	Malware_Build_Week_U3.exe	2404	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS
5:23:00.6857005 PM	Malware_Build_Week_U3.exe	2404	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS
5:23:00.6857164 PM	Malware_Build_Week_U3.exe	2404	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\LeakTrack	NAME NOT FOUND
5:23:00.6857365 PM	Malware_Build_Week_U3.exe	2404	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS
5:23:00.6857427 PM	Malware_Build_Week_U3.exe	2404	RegOpenKey	HKLM	SUCCESS
5:23:00.6857569 PM	Malware_Build_Week_U3.exe	2404	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Diagnostics	NAME NOT FOUND
5:23:00.6857779 PM	Malware_Build_Week_U3.exe	2404	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ntdll.dll	NAME NOT FOUND
5:23:00.6857904 PM	Malware_Build_Week_U3.exe	2404	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\kernel32.dll	NAME NOT FOUND
5:23:00.6860824 PM	Malware_Build_Week_U3.exe	2404	CreateFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll	SUCCESS
5:23:00.6861430 PM	Malware_Build_Week_U3.exe	2404	CreateFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3	SUCCESS
5:23:00.6861882 PM	Malware_Build_Week_U3.exe	2404	CloseFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3	SUCCESS
5:23:00.6861991 PM	Malware_Build_Week_U3.exe	2404	IRP_MJ_CLOSE	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3	SUCCESS
5:23:00.6866347 PM	Malware_Build_Week_U3.exe	2404	WriteFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll	SUCCESS
5:23:00.6885084 PM	Malware_Build_Week_U3.exe	2404	WriteFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll	FAST IO DISALLOWED
5:23:00.6885723 PM	Malware_Build_Week_U3.exe	2404	WriteFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll	SUCCESS
5:23:00.6886916 PM	Malware_Build_Week_U3.exe	2404	CloseFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll	SUCCESS
5:23:00.6888369 PM	Malware_Build_Week_U3.exe	2404	IRP_MJ_CLOSE	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll	SUCCESS

La linea in blu mostra come il malware che stiamo analizzando ha eseguito una createFile creando quello specifico file dll (libreria) nella cartella del malware stesso.

- *Quale chiave di registro viene creata?*
- *Quale valore viene associato alla chiave di registro creata?*

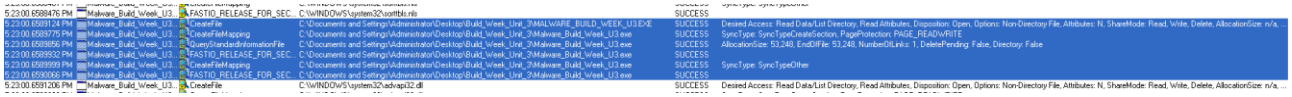


5:23:00.6806596 PM	Malware_Build_Week_U3.exe	2404	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Malware_Build_Week_U3.exe	NAME NOT FOUND
5:23:00.6812985 PM	Malware_Build_Week_U3.exe	2404	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS
5:23:00.6813209 PM	Malware_Build_Week_U3.exe	2404	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	SUCCESS
5:23:00.6813647 PM	Malware_Build_Week_U3.exe	2404	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS
5:23:00.6855116 PM	Malware_Build_Week_U3.exe	2404	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS
5:23:00.6855306 PM	Malware_Build_Week_U3.exe	2404	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	SUCCESS
5:23:00.6855516 PM	Malware_Build_Week_U3.exe	2404	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS
5:23:00.6855806 PM	Malware_Build_Week_U3.exe	2404	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Secur32.dll	NAME NOT FOUND
5:23:00.6856086 PM	Malware_Build_Week_U3.exe	2404	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\RPCRT4.dll	NAME NOT FOUND
5:23:00.6856262 PM	Malware_Build_Week_U3.exe	2404	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ADVAPI32.dll	NAME NOT FOUND
5:23:00.6856446 PM	Malware_Build_Week_U3.exe	2404	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS
5:23:00.6856616 PM	Malware_Build_Week_U3.exe	2404	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	SUCCESS
5:23:00.6856723 PM	Malware_Build_Week_U3.exe	2404	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSUserEnabled	SUCCESS
5:23:00.6856918 PM	Malware_Build_Week_U3.exe	2404	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS
5:23:00.6857005 PM	Malware_Build_Week_U3.exe	2404	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS
5:23:00.6857164 PM	Malware_Build_Week_U3.exe	2404	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\LeakTrack	NAME NOT FOUND
5:23:00.6857365 PM	Malware_Build_Week_U3.exe	2404	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS
5:23:00.6857427 PM	Malware_Build_Week_U3.exe	2404	RegOpenKey	HKLM	SUCCESS
5:23:00.6857569 PM	Malware_Build_Week_U3.exe	2404	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Diagnostics	NAME NOT FOUND
5:23:00.6857779 PM	Malware_Build_Week_U3.exe	2404	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ntdll.dll	NAME NOT FOUND
5:23:00.6857904 PM	Malware_Build_Week_U3.exe	2404	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\kernel32.dll	NAME NOT FOUND
5:23:00.6888795 PM	Malware_Build_Week_U3.exe	2404	RegCreateKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS
5:23:00.6889009 PM	Malware_Build_Week_U3.exe	2404	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL	SUCCESS
5:23:00.6906600 PM	Malware_Build_Week_U3.exe	2404	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS

Vengono effettuate diverse operazioni sulle chiavi, tutte HKLM, quindi sui settings della macchina locale. Viene creata la chiave GinaDLL in WinLogon, cartella che contiene le chiavi al login di Windows. I dati sono all'interno del file creato con lo stesso nome nella cartella del malware

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

Filtrando le attività su file system, vediamo dov'è stato creato il file .dll che vediamo nella cartella del malware



5:23:00.6589476 PM	Malware_Build_Week_U3...	FASTIO_RELEASE_FOR_SEC...	C:\WINDOWS\system32\ssttbl.nls	SUCCESS	
5:23:00.6589124 PM	Malware_Build_Week_U3...	CreateFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\MALWARE_BUILD_WEEK_U3.EXE	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, ...
5:23:00.6589775 PM	Malware_Build_Week_U3...	CreateFileMapping	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\Malware_Build_Week_U3.exe	SUCCESS	SyncType: SyncTypeCreateSection, PageProtection: PAGE_READWRITE
5:23:00.6589956 PM	Malware_Build_Week_U3...	QueryStandardInformationFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\Malware_Build_Week_U3.exe	SUCCESS	AllocationSize: 53,248, EndOfFile: 53,248, NumberOfLinks: 1, DeletePending: False, Directory: False
5:23:00.6589932 PM	Malware_Build_Week_U3...	FASTIO_RELEASE_FOR_SEC...	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\Malware_Build_Week_U3.exe	SUCCESS	
5:23:00.6589999 PM	Malware_Build_Week_U3...	CreateFileMapping	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\Malware_Build_Week_U3.exe	SUCCESS	SyncType: SyncTypeOther
5:23:00.6590066 PM	Malware_Build_Week_U3...	FASTIO_RELEASE_FOR_SEC...	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\Malware_Build_Week_U3.exe	SUCCESS	
5:23:00.6591206 PM	Malware_Build_Week_U3...	CreateFile	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read, Write, Delete, AllocationSize: n/a, ...

Una serie di istruzioni tipo createfile, e createFileMapping ci fanno identificare a che punto dell'esecuzione è stato creato il file e quali sono state le opzioni con cui è stato fatto

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

Le chiavi contenute in WinLogon si occupano della gestione delle credenziali e del login, GinaDLL e' si occupa di gestire la sicurezza relativa alle utenze, modificare quella libreria sostituendola con quella creata dal malware, vuol dire sovrascrivere le varie impostazioni di login e definire nuove regole compromettendo la sicurezza della macchina.