Benchmark – modulo 6

Malware analysis

Traccia:

Con riferimento al file eseguibile Malware_Build_Week_U3, rispondere ai seguenti quesiti utilizzando i tool e le tecniche apprese nelle lezioni teoriche:

- Quanti parametri sono passati alla funzione Main()?
- Quante variabili sono dichiarate all'interno della funzione Main()?
- Quali sezioni sono presenti all'interno del file eseguibile? Descrivete brevemente almeno 2 di quelle identificate
- 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.

- **Quanti parametri sono passati alla funzione Main ()?**
- **Quante variabili sono dichiarate all'interno della funzione Main()?**

```
; Attributes: bp-based frame

; 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
```

I parametri sono quelli indicati dopo la funzione **main**(), all'interno della parentesi, ovvero **argc**, **argv** e **envp**.

Le variabili sono quelle in verde sotto dove i valori hanno il meno davanti e sono in una posizione negativa rispetto alla base dello stack epb, e sono **hModule**, **Data**, **var_8** e **var_4**.

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

Le sezioni del malware sono invece 4, e sono visibili dal programma CFF explorer

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	Characteristics
00000250	00000258	0000025C	00000260	00000264	00000268	0000026C	00000270	00000272	00000274
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	00005646	00001000	00006000	00001000	00000000	00000000	0000	0000	60000020
.rdata	000009AE	00007000	00001000	00007000	00000000	00000000	0000	0000	40000040
.data	00003EA8	00008000	00003000	00008000	00000000	00000000	0000	0000	C0000040
.rsrc	00001A70	0000C000	00002000	0000B000	00000000	00000000	0000	0000	40000040

Di seguito andiamo a trattarne due:

La sezione **.rsrc** (resource)va ad includere le risorse utilizzate dall'eseguibile che non vengono considerate parte dell'eseguibile, come ad esempio: immagine, menu, stringhe, GUI ed icone. Queste risorse vengono incorporate nell'eseguibile durante la fase di compilazione e possono essere accessibili dall'applicazione in fase di esecuzione. È organizzata gerarchicamente in sottodirectory, ognuna delle quali contiene i vari tipi di risorse. Le risorse contenute nella sezione .rsrc possono essere richiamate utilizzando identificatori numerici o nomi simbolici, e il malware in questione può caricarle e utilizzarle in base alle sue necessità.

La sezione **.rdata** invece contiene le informazioni sull'import e sull'export. Può inoltre salvare dei dati read-only (o di sola lettura) usati dal programma. Questi dati possono includere costanti, tabelle di lookup, dati inizializzati che non possono essere modificati durante l'esecuzione del programma e altri dati simili.

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

Librerie importate: (sempre visibili da CFF explorerer)

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	51	00007534	00000000	00000000	0000769E	0000700C
ADVAPI32.dll	2	00007528	00000000	00000000	000076D0	00007000

La libreria **Kernel32.dll** è una libreria che può permettere al malware di utilizzare funzioni per la gestione della memoria oppure funzioni per interagire con il sistema operativo. Kernel32.dll è una delle librerie di sistema fondamentali nei sistemi operativi Windows. Contiene funzioni di basso livello per la gestione delle risorse del sistema, la gestione dei processi, la memoria, la gestione dei file, la comunicazione tra processi e altre attività essenziali.

Le funzioni fornite da Kernel32.dll coprono una vasta gamma di operazioni, tra cui:

Gestione dei processi e dei thread.

Gestione dei file e delle directory.

Allocazione e gestione della memoria.

La libreria **ADVAPI32.dll** invece permette al malware di avere accesso alle chiavi di registro. ADVAPI32.dll è un'altra importante libreria di sistema presente nei sistemi operativi Windows. Essa contiene funzioni che consentono l'accesso a servizi avanzati e funzionalità di sicurezza, inclusi i servizi di autenticazione, crittografia, controllo degli accessi e gestione dei servizi di Windows.

Le funzioni fornite da ADVAPI32.dll includono:

Gestione delle credenziali e delle identità utente.

Funzioni di crittografia e decrittografia.

Accesso alle informazioni di registrazione (event logs)

Malware Analysis

Con riferimento al Malware in analisi, spiegare:

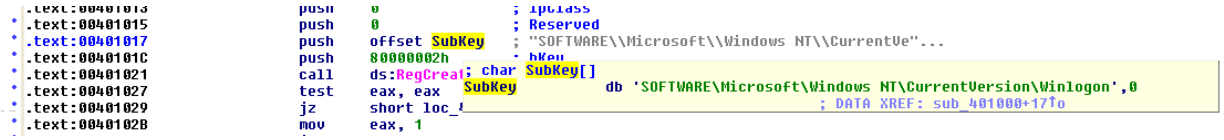
- Lo scopo della funzione chiamata alla locazione di memoria **00401021**
- Come vengono passati i parametri alla funzione alla locazione **00401021**;
- Che oggetto rappresenta il parametro alla locazione **00401017**
- Il significato delle istruzioni comprese tra gli indirizzi **00401027** e **00401029**.
- Con riferimento all'ultimo quesito, tradurre il codice Assembly nel corrispondente costrutto C.
- Valutate ora la chiamata alla locazione **00401047**, qual è il valore del parametro «ValueName»?

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

La funzione all'indirizzo 00401021 crea la chiave di registro

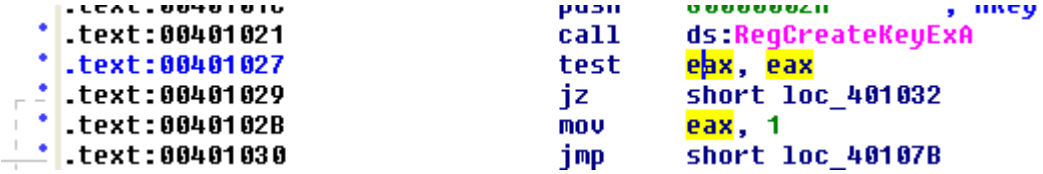
2- Come vengono passati i parametri alla funzione alla locazione 00401021

Attraverso i "push" vengono passati i parametri alla funzione alla locazione 00401021



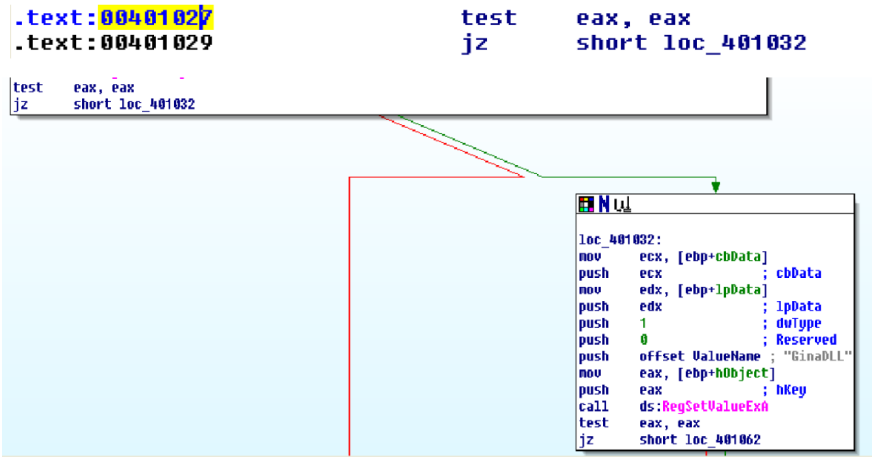
3- Che oggetto rappresenta il parametro alla locazione 00401017

All'indirizzo di memoria 00401017 invece troviamo la chiave di registro che porta all'avvio automatico della DLL compromessa



4- Il significato delle istruzioni comprese tra gli indirizzi 00401027 e 00401029

Per quanto riguarda le istruzioni tra l'indirizzo 00401027 e l'indirizzo 00401029, verificano se il malware è stato avviato come da prassi, in caso contrario, cioè negativo, fa direttamente il salto alla loc_401032. Se si è aperto correttamente parte l'istruzione che chiude il proseguimento:



Trasformazione della funzione in codice C:

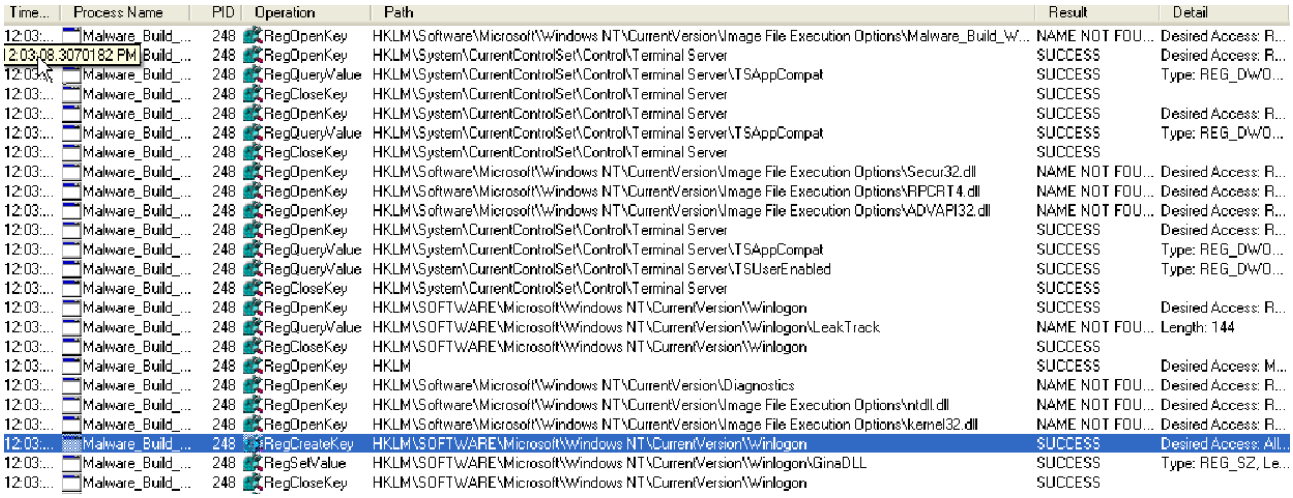
```
if (eax == 0)
 {
  funct_401032();
 }
else
 {
  eax = 1;
  funct_40107B();
}
```

5- Valutate ora la chiamata alla locazione 00401047, qual è il valore di ValueName?

Analizzando la chiamata alla funzione “RegSetValueExa” alla posizione di memoria 00401047 il valore del parametro ValueName è ‘GinaDLL’, come mostrato sotto

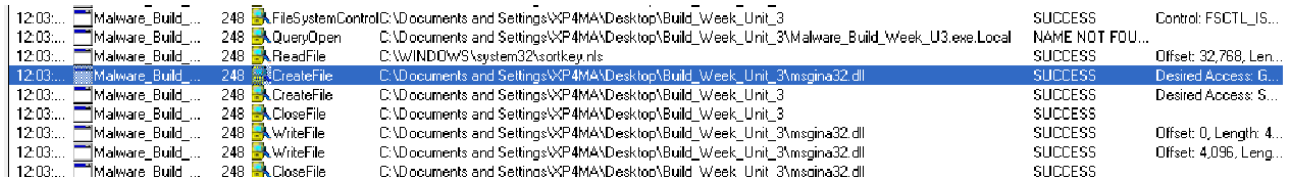
Una volta avviato il Malware, all’interno della cartella dove era situato, si è creato il file msgina32.dll, ovvero la versione corrotta della GINA DLL. Infatti, come spiega Microsoft, lo scopo vero e proprio della GINA DLL è di fornire procedure di identificazione e autenticazione dell’utente personalizzabili.

Analizzando poi le chiavi di registro con ProcMon, si evince che il malware crea la chiave di registro Winlogon e gli viene assegnato il valore msgina32.dll che aveva precedentemente trovato nella cartella del malware:



Time...	Process Name	PID	Operation	Path	Result	Detail
12:03:...	Malware_Build_...	248	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Malware_Build_W...	NAME NOT FOU...	Desired Access: R...
2:03:08.3070182 PM	Build_...	248	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	Desired Access: R...
12:03:...	Malware_Build_...	248	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	SUCCESS	Type: REG_DWO...
12:03:...	Malware_Build_...	248	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	
12:03:...	Malware_Build_...	248	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	Desired Access: R...
12:03:...	Malware_Build_...	248	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	SUCCESS	Type: REG_DWO...
12:03:...	Malware_Build_...	248	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	
12:03:...	Malware_Build_...	248	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Secur32.dll	NAME NOT FOU...	Desired Access: R...
12:03:...	Malware_Build_...	248	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\RPCRT4.dll	NAME NOT FOU...	Desired Access: R...
12:03:...	Malware_Build_...	248	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ADVAPI32.dll	NAME NOT FOU...	Desired Access: R...
12:03:...	Malware_Build_...	248	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	Desired Access: R...
12:03:...	Malware_Build_...	248	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	SUCCESS	Type: REG_DWO...
12:03:...	Malware_Build_...	248	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSUserEnabled	SUCCESS	Type: REG_DWO...
12:03:...	Malware_Build_...	248	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	
12:03:...	Malware_Build_...	248	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	Desired Access: R...
12:03:...	Malware_Build_...	248	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\LeakTrack	NAME NOT FOU...	Length: 144
12:03:...	Malware_Build_...	248	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	
12:03:...	Malware_Build_...	248	RegOpenKey	HKLM	SUCCESS	Desired Access: M...
12:03:...	Malware_Build_...	248	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Diagnostics	NAME NOT FOU...	Desired Access: R...
12:03:...	Malware_Build_...	248	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ntdll.dll	NAME NOT FOU...	Desired Access: R...
12:03:...	Malware_Build_...	248	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\kernel32.dll	NAME NOT FOU...	Desired Access: R...
12:03:...	Malware_Build_...	248	RegCreateKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	Desired Access: All...
12:03:...	Malware_Build_...	248	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL	SUCCESS	Type: REG_SZ, Le...
12:03:...	Malware_Build_...	248	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	

Chiamata Sistema per file system



12:03:...	Malware_Build_...	248	FileSystemControl	C:\Documents and Settings\XP4MA\Desktop\Build_Week_Unit_3	SUCCESS	Control: FSCTL_IS...
12:03:...	Malware_Build_...	248	QueryOpen	C:\Documents and Settings\XP4MA\Desktop\Build_Week_Unit_3\Malware_Build_Week_U3.exe.Local	NAME NOT FOU...	
12:03:...	Malware_Build_...	248	ReadFile	C:\WINDOWS\system32\sortkey.nls	SUCCESS	Offset: 32,768, Len...
12:03:...	Malware_Build_...	248	CreateFile	C:\Documents and Settings\XP4MA\Desktop\Build_Week_Unit_3\msgina32.dll	SUCCESS	Desired Access: G...
12:03:...	Malware_Build_...	248	CreateFile	C:\Documents and Settings\XP4MA\Desktop\Build_Week_Unit_3	SUCCESS	Desired Access: S...
12:03:...	Malware_Build_...	248	CloseFile	C:\Documents and Settings\XP4MA\Desktop\Build_Week_Unit_3	SUCCESS	
12:03:...	Malware_Build_...	248	WriteFile	C:\Documents and Settings\XP4MA\Desktop\Build_Week_Unit_3\msgina32.dll	SUCCESS	Offset: 0, Length: 4...
12:03:...	Malware_Build_...	248	WriteFile	C:\Documents and Settings\XP4MA\Desktop\Build_Week_Unit_3\msgina32.dll	SUCCESS	Offset: 4,096, Leng...
12:03:...	Malware_Build_...	248	CloseFile	C:\Documents and Settings\XP4MA\Desktop\Build_Week_Unit_3\msgina32.dll	SUCCESS	

In conclusione, si può affermare che il malware sia un dropper, ovvero un tipo di malware che al suo interno contiene e un altro malware.

Si evince dal fatto che avvalga della sezione .rsrc e contiene al suo interno un logger che copia le credenziali di accesso.

12:03:...	Malware_Build_...	248	WriteFile	C:\Documents and Settings\XP4MA\De...	SUCCESS	Offset: 4,096, Leng...
12:03:...	Malware_Build_...	248	CloseFile	C:\Documents and Settings\XP4MA\De...	SUCCESS	
12:03:...	Malware_Build_...	248	RegCreateKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Desired Access: All...
12:03:...	Malware_Build_...	248	RegSetValue	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Type: REG_SZ, Le...
12:03:...	Malware_Build_...	248	SetEndOfFileInf...	C:\WINDOWS\system32\config\softwa...	SUCCESS	EndOfFile: 12,288
12:03:...	Malware_Build_...	248	SetEndOfFileInf...	C:\WINDOWS\system32\config\softwa...	SUCCESS	EndOfFile: 12,288
12:03:...	Malware_Build_...	248	SetEndOfFileInf...	C:\WINDOWS\system32\config\softwa...	SUCCESS	EndOfFile: 20,480
12:03:...	Malware_Build_...	248	SetEndOfFileInf...	C:\WINDOWS\system32\config\softwa...	SUCCESS	EndOfFile: 24,576
12:03:...	Malware_Build_...	248	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	
12:03:...	Malware_Build_...	248	Thread Exit		SUCCESS	Thread ID: 1084, ...
12:03:...	Malware_Build_...	248	Process Exit		SUCCESS	Exit Status: 0, User...
12:03:...	Malware_Build_...	248	CloseFile	C:\Documents and Settings\XP4MA\De...	SUCCESS	