

Progetto 6

Analisi statica





-Nell'analisi statica del malware possiamo trovare nella funzione Main() la dichiarazione di 4 variabili, visto che l'offset della variabile è negativo in base al registro e sono le seguenti:

```
hModule= dword ptr -11Ch
Data= byte ptr -118h
var_8= dword ptr -8
var_4= dword ptr -4
```

-I parametri passati alla funzione Main() sono le seguenti, lo capiamo dato che l'offset è positivo in base al registro

```
argc= dword ptr 8
argv= dword ptr 0Ch
envp= dword ptr 10h
```

-Le sezioni presenti all'interno dell'eseguibile sono:

 .text	00401000	00407000	R	.	X	.	L	para	0001	public	CODE
 .idata	00407000	004070DC	R	.	.	.	L	para	0002	public	DATA
 .rdata	004070DC	00408000	R	.	.	.	L	para	0002	public	DATA
 .data	00408000	0040BEA8	R	W	.	.	L	para	0003	public	DATA

Tra le sezioni presenti si possono identificare la sezione “.text” dove al suo interno si troverà il codice che verrà eseguito quando verrà lanciato l'eseguibile.

La sezione “.data” dove al suo interno si trovano le variabili locali e globali che verranno utilizzate in fase di esecuzione.

-In base alle librerie importate dal programma possiamo notare che durante l'esecuzione andrà a creare un file dove al suo interno andrà a scrivere tutte le informazioni riguardanti il PC su cui viene lanciato il programma.

 00407000	RegSetValueExA	ADVAPI32
 00407004	RegCreateKeyExA	ADVAPI32
 0040700C	SizeofResource	KERNEL32
 00407010	LockResource	KERNEL32
 00407014	LoadResource	KERNEL32
 00407018	VirtualAlloc	KERNEL32
 0040701C	GetModuleFileNameA	KERNEL32
 00407020	GetModuleHandleA	KERNEL32
 00407024	FreeResource	KERNEL32
 00407028	FindResourceA	KERNEL32
 0040702C	CloseHandle	KERNEL32
 00407030	GetCommandLineA	KERNEL32
 00407034	GetVersion	KERNEL32
 00407038	ExitProcess	KERNEL32

```
.text:00401021          call     ds:RegCreateKeyExA
```

La seguente funzione ha lo scopo di creare una chiave di registro, i parametri vengono passati tramite push.

```
push    0                ; lpSecurityAttribute
push    0F003Fh          ; samDesired
push    0                ; dwOptions
push    0                ; lpClass
push    0                ; Reserved
push    offset SubKey    ; "SOFTWARE\\Microsoft
push    80000002h        ; hKey
```

```
.text:00401017          push    offset SubKey    ; "SOFTWARE\\Microsoft\\Windows NT\\CurrentVe"...
```

Questo parametro rappresenta la sottochiave che passerà alla funzione per creare la chiave di registro la versione del sistema presente.

```
.text:00401027          test     eax, eax
.text:00401029          jz      short loc_401032
```

La prima istruzione “test” andrà ad eseguire l'operazione AND al registro EAX, il risultato andrà a cambiare lo ZF(Zero Flags) portandolo a 1, quindi nella istruzione successiva verrà eseguito il salto alla locazione.

```
.text:00401047          call     ds:RegSetValueExA
```

L'istruzione andrà a chiamare la funzione per settare il valore della chiave di registro e il valore del parametro “ValueName” quando viene chiamata la funzione è “GinaDLL”.

Analisi dinamica

Dopo aver eseguito il malware, all'interno della cartella dove è presente l'eseguibile viene creato un file nominato “msgina32.dll”, dove all'interno saranno presenti la mappature delle funzioni che usa il sistema operativo.



La chiave di registro che viene creata è la winlogon che fornisce supporto interattivo per l'accesso.

1396	RegCreateKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
1396	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL
1396	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

La chiamata di sistema che va a modificare la cartella del contenuto è CreateFile con il path dove si trova il malware seguito dal nome del file creato.

CreateFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll
CreateFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3
CloseFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3
CreateFileMapping	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll
WriteFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll
WriteFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll
CloseFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll

Infine dalle informazioni raccolte dall'analisi statica e l'analisi dinamica si può capire che questo malware è un dropper che al suo avvio andrà ad accedere al sistema per crearne una mappatura per poter avere accesso ai file system, creando un file oggetto nella cartella contenente l'eseguibile del malware che contiene tutte le informazioni di sistema.