

M6_W24D4

Traccia:

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

Malware Analysis

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

Analisi statica

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.

Svolgimento:

Per identificare quanti parametri e quali variabili sono passati per la funzione Main del malware si utilizzerà IDApro.

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

hModule= dword ptr -11Ch
Data= byte ptr -118h
var_117= byte ptr -117h
var_8= dword ptr -8
var_4= dword ptr -4
argc= dword ptr 8
argv= dword ptr 0Ch
envp= dword ptr 10h
```

I parametri riscontrati nella funzione Main sono 3: **int argc, const char **argv, const char **envp**.

Le variabili dichiarate nella funzione all'interno della funzione Main sono 5: **hModule, Data, var_117, var_8, var_4**.

Successivamente si identificheranno le sezioni e le librerie importate dal malware. Nello specifico il malware include 4 sezioni e importa 2 librerie.

Malware_Build_Week_U3.exe									
Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
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

Si analizzeranno le sezioni **.text** e **.rdata** :

- **.text** : sezione fondamentale di un eseguibile contenente il codice eseguito dal processore quando il programma viene avviato.
- **.rdata** : sezione dell'eseguibile contenente i dati in sola lettura utilizzati dal programma durante l'esecuzione.

00000000...	RegSetValueExA	ADVAPI32
00000000...	RegCreateKeyExA	ADVAPI32
00000000...	SizeofResource	KERNEL32
00000000...	LockResource	KERNEL32
00000000...	LoadResource	KERNEL32
00000000...	VirtualAlloc	KERNEL32
00000000...	GetModuleFileNameA	KERNEL32
00000000...	GetModuleHandleA	KERNEL32
00000000...	FreeResource	KERNEL32
00000000...	FindResourceA	KERNEL32
00000000...	CloseHandle	KERNEL32
00000000...	GetCommandLineA	KERNEL32
00000000...	GetVersion	KERNEL32
00000000...	ExitProcess	KERNEL32
00000000...	HeapFree	KERNEL32
00000000...	GetLastError	KERNEL32
00000000...	WriteFile	KERNEL32
00000000...	TerminateProcess	KERNEL32
00000000...	GetCurrentProcess	KERNEL32
00000000...	UnhandledExceptionFilter	KERNEL32
00000000...	FreeEnvironmentStringsA	KERNEL32

Le librerie importate dal malware sono **ADVAPI32** e **KERNEL32**.

Analizzandole più nel dettaglio potremmo ipotizzare che il malware sta cercando di leggere o modificare le voci del registro per poi modificare i file o i dati di sistema. Osservando il comportamento dell'eseguibile quest'ultimo sta preparando un file o una risorsa da rilasciare sul sistema target proprio come farebbe un **dropper**.

Si procederà con l'analisi del malware.

- Lo scopo della funzione chiamata alla locazione di memoria 00401021 è **RegCreateKeyExA** quindi creare una chiave di registro o aprire una chiave esistente nel Registro di Sistema.
- L'oggetto rappresentato nella locazione 00401017 si riferisce al Registro di Sistema Windows: "Software\Microsoft\Windows NT\CurrentVersion"

- Il significato delle istruzioni tra gli indirizzi 00401027 e 00401029 rappresentano un salto condizionale quindi:

```
test  eax,eax
jz    short loc_401032
```

Significa che viene fatta una comparazione tra eax e eax se è 0 viene fatto un jump alla locazione 401032 con un jz ovvero jump zero.

In codice C potrebbe essere: if (eax==0) {

goto loc_401032

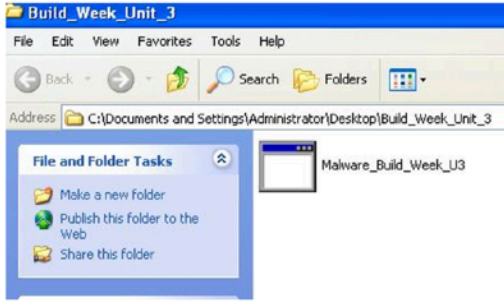
}

- Il valore del parametro ValueName della locazione 00401047 è GinaDLL. Il parametro ValueName in questo caso viene utilizzato per dettare il valore della chiave di registro appena creata.

Malware Analysis

Analisi dinamica

Preparate l'ambiente ed i tool per l'esecuzione del Malware (suggerimento: avviate principalmente Process Monitor ed assicurate di eliminare ogni filtro cliccando sul tasto «reset» quando richiesto in fase di avvio). Eseguite il Malware, facendo doppio click sull'icona dell'eseguibile



Malware Analysis

- 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

Analizzate ora i risultati di Process Monitor (consiglio: utilizzate il filtro come in figura sotto per estrarre solo le modifiche apportate al sistema da parte del Malware). Fate click su «ADD» poi su «Apply» come abbiamo visto nella lezione teorica.

Malware Analysis

Filtrate includendo solamente l'attività sul registro di Windows.

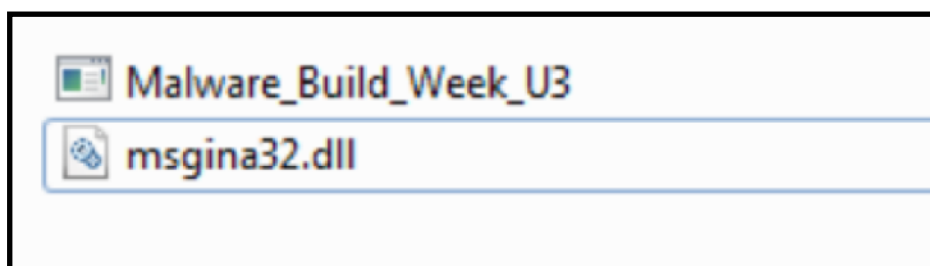
- Quale chiave di registro viene creata?
- Quale valore viene associato alla chiave di registro creata?

Passate ora alla visualizzazione dell'attività sul file system.

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

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

Eseguendo il malware notiamo la presenza di un file .dll “**msgina32.dll**” creato in seguito al cambio di valore del registro Gina.DLL .



Gina.DLL viene associato alla pagina di login utente di Windows ed è responsabile dell'autenticazione su sistemi, quindi potrebbe intercettare credenziali di login sul target.

Successivamente verranno filtrati i processi di Process Monitor includendo solo l'attività sul Registro di Windows.

Malware_Build_...	2880	RegOpenKey	HKLM\Software\Microsoft\Windows N...	SUCCESS	Desired Access: Q...
Malware_Build_...	2880	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	NAME NOT FOUND	Length: 1.024
Malware_Build_...	2880	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
Malware_Build_...	2880	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
Malware_Build_...	2880	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 1.024
Malware_Build_...	2880	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
Malware_Build_...	2880	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
Malware_Build_...	2880	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
Malware_Build_...	2880	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Type: REG_SZ, Le...
Malware_Build_...	2880	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
Malware_Build_...	2880	RegOpenKey	HKLM\SOFTWARE\Microsoft\WOW64	NAME NOT FOUND	Desired Access: Q...
Malware_Build_...	2880	RegOpenKey	HKLM\Software\Wow6432Node\Micro...	SUCCESS	Desired Access: Q...
Malware_Build_...	2880	RegSetInfoKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	KeySetInformation...
Malware_Build_...	2880	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	NAME NOT FOUND	Length: 1.024
Malware_Build_...	2880	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
Malware_Build_...	2880	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
Malware_Build_...	2880	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	KeySetInformation...
Malware_Build_...	2880	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 1.024
Malware_Build_...	2880	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
Malware_Build_...	2880	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: R...
Malware_Build_...	2880	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: R...
Malware_Build_...	2880	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	KeySetInformation...
Malware_Build_...	2880	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 548

Verrà creata la chiave di registro HKLM che salverà le informazioni generali di tutti gli utenti registrati sulla macchina confermando che lo scopo dell'eseguibile è quello di creare persistenza nel sistema memorizzando informazioni di configurazione e altre impostazioni importanti per il sistema operativo.

Si procederà con la visualizzazione dell'attività sul file system.

Malware_Build_...	2880	CreateFile	C:\Windows	SUCCESS	Desired Access: E...
Malware_Build_...	2880	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: R...
Malware_Build_...	2880	QueryBasicInfor...	C:\Windows\System32\wow64.dll	SUCCESS	CreationTime: 21/1...
Malware_Build_...	2880	CloseFile	C:\Windows\System32\wow64.dll	SUCCESS	
Malware_Build_...	2880	CreateFile	C:\Windows\System32\wow64.dll	SUCCESS	Desired Access: R...
Malware_Build_...	2880	CreateFileMapp...	C:\Windows\System32\wow64.dll	FILE LOCKED WI...	SyncType: SyncTy...
Malware_Build_...	2880	CreateFileMapp...	C:\Windows\System32\wow64.dll	SUCCESS	SyncType: SyncTy...
Malware_Build_...	2880	CloseFile	C:\Windows\System32\wow64.dll	SUCCESS	
Malware_Build_...	2880	CreateFile	C:\Windows\System32\wow64win.dll	SUCCESS	Desired Access: R...
Malware_Build_...	2880	QueryBasicInfor...	C:\Windows\System32\wow64win.dll	SUCCESS	CreationTime: 21/1...
Malware_Build_...	2880	CloseFile	C:\Windows\System32\wow64win.dll	SUCCESS	
Malware_Build_...	2880	CreateFile	C:\Windows\System32\wow64win.dll	SUCCESS	Desired Access: R...
Malware_Build_...	2880	CreateFileMapp...	C:\Windows\System32\wow64win.dll	FILE LOCKED WI...	SyncType: SyncTy...
Malware_Build_...	2880	CreateFileMapp...	C:\Windows\System32\wow64win.dll	SUCCESS	SyncType: SyncTy...
Malware_Build_...	2880	CloseFile	C:\Windows\System32\wow64win.dll	SUCCESS	
Malware_Build_...	2880	CreateFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Desired Access: R...
Malware_Build_...	2880	QueryBasicInfor...	C:\Windows\System32\wow64cpu.dll	SUCCESS	CreationTime: 21/1...
Malware_Build_...	2880	CloseFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	
Malware_Build_...	2880	CreateFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	Desired Access: R...
Malware_Build_...	2880	CreateFileMapp...	C:\Windows\System32\wow64cpu.dll	FILE LOCKED WI...	SyncType: SyncTy...
Malware_Build_...	2880	CreateFileMapp...	C:\Windows\System32\wow64cpu.dll	SUCCESS	SyncType: SyncTy...
Malware_Build_...	2880	CloseFile	C:\Windows\System32\wow64cpu.dll	SUCCESS	
Malware_Build_...	2880	CreateFile	C:\Windows\System32\wow64log.dll	NAME NOT FOUND	Desired Access: R...

Filtrando i risultati ci renderemo conto che le chiamate di sistema Create, Write e Close hanno creato, modificato e chiuso il contenuto del file **msgina32.dll** .

Concludendo:

- Il malware importa due librerie e quattro sezioni.
- Assegna valore alla chiave di registro Gina.DLL
- Crea una chiave di registro e ne associa un valore.
- Crea un file denominato msgina32.dll all'interno della cartella dell'eseguibile.

Lo scopo del Malware come si pensava è quello di raccogliere e registrare le autenticazioni degli utenti per ottenere persistenza sul sistema.