

M6 - Progetto finale

DATA

Cybersecurity Analyst

Studente:

Andrea Scarmagnani

Docente:

Federico Daidone

Cyber Security & Ethical Hacking Progetto

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.

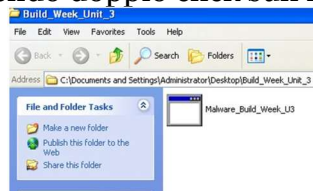
Malware Analysis

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 Analisi dinamica

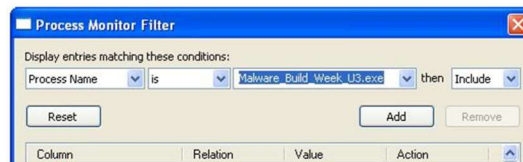
Preparate l'ambiente ed i tool per l'esecuzione del Malware (suggerimento: avviate principalmente Process Monitor ed assicurate di eliminare ogni filtro cliccando sul tasto «reset» quando richiesto in fase di avvio). Eseguite il Malware, facendo doppio click sull'icona dell'eseguibile



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.

Esecuzione:

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()?

R: Ha offset positivo e quindi sono (ARGC; ARGV; ENVP) **Totale: 3**

```
.text:004011D0 argv = dword ptr 8
.text:004011D0 argv = dword ptr 0Ch
.text:004011D0 envp = dword ptr 10h
```

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

R: Ha offset negativo quindi sono (hModule;Data;var_117,var_8;var_4) **Totale: 5**

```
.text:004011D0 hModule = dword ptr -11Ch
.text:004011D0 Data = byte ptr -118h
.text:004011D0 var_117 = byte ptr -117h
.text:004011D0 var_8 = dword ptr -8
.text:004011D0 var_4 = dword ptr -4
```

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





R: Ho trovato le seguenti sezioni (.text; .idata; .rdata; .data)

Nella sezione .text: Contiene le righe di codice che la cpu esegue avviato il software.

Nella sezione .idata: Contiene dati di importazione, esempio dalle librerie DLL.

Nella sezione .rdata: Contiene dati di sola lettura non modificabili.

Nella sezione .data: Contiene le variabili globali, accessibili da qualunque parte del codice.

Name	Start	End	R	W	X	D	L	Align	Base	Type
 .text	0000000000401000	0000000000407000	R	.	X	.	L	para	0001	public
 .idata	0000000000407000	00000000004070DC	R	.	.	.	L	para	0002	public
 .rdata	00000000004070DC	0000000000408000	R	.	.	.	L	para	0002	public
 .data	0000000000408000	000000000040C000	R	W	.	.	L	para	0003	public

-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.

R: Importa n°2 librerie ADVAPI32 e KERNEL32

ADVAPI32.dll: Interagisce con il registro di sistema Microsoft

KERNEL32.dll: Interagisce con il sistema operativo, manipolazione file e gestione memoria.

Library	
ADVAPI32	Il Malware, avendo accesso ai registri, file, e memoria, sicuramente cercherà di modificare il registro di sistema per ottenere una sua persistenza, poi cercare di accedere ai file (Lettura/Scrittura) probabilmente per ottenere informazioni. Cosa possa fare in questo momento non sono ancora in grado di rispondere.
ADVAPI32	
KERNEL32	
KERNEL32	

Malware Analysis

Con riferimento al Malware in analisi, spiegare:

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

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

R: L'istruzione "Call ds:RegCreateKeyExA" indica una chiamata a una funzione. È utilizzata per interagire con il Registro di sistema di Windows al fine di creare o aprire una sottochiave.

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

```
.text:00401013      push     0           ; lpClass
.text:00401015      push     0           ; Reserved
.text:00401017      push     offset SubKey ; "SOFTWARE\\Mic
.text:0040101C      push     80000002h    ; hKey
.text:00401021      call     ds:RegCreateKeyExA
```

R: 1. push offset subkey: Spinge l'indirizzo della stringa subkey nello stack. Nome della sottochiave del Registro di sistema che si desidera creare o aprire.
2. push 80000002h: Spinge il valore costante 80000002h nello stack. Flag o una costante utilizzata indica che si desidera aprire una sottochiave esistente o crearne una nuova se non esiste.

Dopo aver caricato i parametri nello stack, l'istruzione *Call ds:RegCreateKeyExA* esegue la chiamata alla funzione RegCreateKeyExA, passando i parametri precedentemente spinti nello stack.

-Che oggetto rappresenta il parametro alla locazione 00401017

```
5-14 00401015 6A 00 PUSH 0
5-12 00401017 68 54804000 PUSH Malware_.00408054 ASCII "SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon"
```

R: Rappresenta una chiave del registro windows.

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

```
00401027 85C0 TEST EAX,EAX
00401029 74 07 JE SHORT Malware_.00401032
```

R: Nell'indirizzo 00401027: Verifica se il valore è a 0 (Zero)
Nell'indirizzo 00401029: Se la verifica è Zero va all'indirizzo 00401032.

-Con riferimento all'ultimo quesito, tradurre il codice Assembly nel corrispondente costruito C.

R: All'inizio vengono dichiarate le variabili, successivamente c'è un controllo IF (JE)

```
Variabili;
int main() {
    if (0 ...;
}
```

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

R: Il valore ValueName è GinaDLL. Ho eseguito il codice da 004010000 a 00401047.

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

```
hKey = 44
ValueName = "GinaDLL"
Reserved = 0
ValueType = REG_SZ
Buffer = Malware_.<ModuleEntryPoint>
BufSize = 0
Malware_.<ModuleEntryPoint>
```


Malware Analysis Analisi dinamica

-Cosa notate all'interno della cartella dove è situato l'eseguibile del Malware?

R: Dopo aver preparato l'ambiente (Avviato e configurato i seguenti software: Process monitor, AateDNS, Regshot), ho eseguito il malware, all'interno della cartella è stato creato un nuovo file (Libreria DLL di nome msgina32.dll) già avevamo visto questo nome nella precedente analisi statica.

Nome	Ultima modifica
Malware_Build_Week_U3	17/01/2024 17:48
msgina32.dll	20/04/2024 12:29

Analizzate ora i risultati di Process Monitor:

R: Analizzato il risultato di Process Monitor, troviamo una serie di tentativi di letture e scritture nel registro di windows.

Process Monitor - Sysinternals: www.sysinternals.com						
File Edit Event Filter Tools Options Help						
Time ...	Process Name	PID	Operation	Path	Result	Detail
12:46:...	Malware_Build_Week_U3.exe	1904	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	REPARSE	Desired Access: Query Value, Set Value
12:46:...	Malware_Build_Week_U3.exe	1904	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	NAME NOT FOUND	Desired Access: Query Value, Set Value
12:46:...	Malware_Build_Week_U3.exe	1904	RegOpenKey	HKLM\System\CurrentControlSet\Control\Srp\GP\DLL	REPARSE	Desired Access: Read
12:46:...	Malware_Build_Week_U3.exe	1904	RegOpenKey	HKLM\System\CurrentControlSet\Control\Srp\GP\DLL	NAME NOT FOUND	Desired Access: Read
12:46:...	Malware_Build_Week_U3.exe	1904	RegOpenKey	HKLM\Software\Wow6432Node\Policies\Microsoft\Windows...	REPARSE	Desired Access: Query Value
12:46:...	Malware_Build_Week_U3.exe	1904	RegOpenKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\Co...	SUCCESS	Desired Access: Query Value
12:46:...	Malware_Build_Week_U3.exe	1904	RegSetInfoKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\cod...	SUCCESS	KeySetInformationClass: KeySetHandleTagsIn...
12:46:...	Malware_Build_Week_U3.exe	1904	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\cod...	NAME NOT FOUND	Length: 80
12:46:...	Malware_Build_Week_U3.exe	1904	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\cod...	SUCCESS	
12:46:...	Malware_Build_Week_U3.exe	1904	RegOpenKey	HKCU\Software\Policies\Microsoft\Windows\Safer\CodeId...	NAME NOT FOUND	Desired Access: Query Value
12:46:...	Malware_Build_Week_U3.exe	1904	RegOpenKey	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versio...	REPARSE	Desired Access: Read
12:46:...	Malware_Build_Week_U3.exe	1904	RegOpenKey	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versio...	SUCCESS	Desired Access: Read
12:46:...	Malware_Build_Week_U3.exe	1904	RegSetInfoKey	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versio...	SUCCESS	KeySetInformationClass: KeySetHandleTagsIn...
12:46:...	Malware_Build_Week_U3.exe	1904	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versio...	SUCCESS	Type: REG_SZ, Length: 36, Data: 00060101...
12:46:...	Malware_Build_Week_U3.exe	1904	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	REPARSE	Desired Access: Read
12:46:...	Malware_Build_Week_U3.exe	1904	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	Desired Access: Read
12:46:...	Malware_Build_Week_U3.exe	1904	RegSetInfoKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	KeySetInformationClass: KeySetHandleTagsIn...
12:46:...	Malware_Build_Week_U3.exe	1904	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\T...	NAME NOT FOUND	Length: 548
12:46:...	Malware_Build_Week_U3.exe	1904	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\T...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
12:46:...	Malware_Build_Week_U3.exe	1904	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	
12:46:...	Malware_Build_Week_U3.exe	1904	RegOpenKey	HKLM	SUCCESS	Desired Access: Maximum Allowed, Granted A...
12:46:...	Malware_Build_Week_U3.exe	1904	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
12:46:...	Malware_Build_Week_U3.exe	1904	RegOpenKey	HKLM\Software\Wow6432Node\Microsoft\Windows NT\...	NAME NOT FOUND	Desired Access: Read
12:46:...	Malware_Build_Week_U3.exe	1904	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
12:46:...	Malware_Build_Week_U3.exe	1904	RegCreateKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows N...	SUCCESS	Desired Access: All Access, Disposition: REG...
12:46:...	Malware_Build_Week_U3.exe	1904	RegSetInfoKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows N...	SUCCESS	KeySetInformationClass: KeySetHandleTagsIn...
12:46:...	Malware_Build_Week_U3.exe	1904	RegQueryKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows N...	SUCCESS	Query: HandleTags, HandleTags: 0x400
12:46:...	Malware_Build_Week_U3.exe	1904	RegSetValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows N...	ACCESS DENIED	Type: REG_SZ, Length: 520, Data: C:\Users\...
12:46:...	Malware_Build_Week_U3.exe	1904	RegCloseKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows N...	SUCCESS	
12:46:...	Malware_Build_Week_U3.exe	1904	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion...	SUCCESS	
12:46:...	Malware_Build_Week_U3.exe	1904	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion...	SUCCESS	
12:46:...	Malware_Build_Week_U3.exe	1904	RegCloseKey	HKLM\System\CurrentControlSet\Control\Nls\Sorting\Versio...	SUCCESS	

Qui sotto vediamo che il malware è stato in grado di scrivere dentro al registro di windows.

22:28:15.1404916	Malware_Build_Week_U3.exe	1552	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
22:28:15.1405063	Malware_Build_Week_U3.exe	1552	RegCreateKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	Desired Access: All Access, Disposition...
22:28:15.1405286	Malware_Build_Week_U3.exe	1552	RegSetInfoKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	KeySetInformationClass: KeySetHandle...

Malware Analysis

-Quale chiave di registro viene creata?

R: È stata creata questa chiave

22:28:15.1404916	Mahware_Bulid_Week_U3.exe	1552	RegOpenKey	HKLM		SUCCESS	Query: Handle Tags: Handle Tags: 0x0
22:28:15.1405693	Mahware_Bulid_Week_U3.exe	1552	RegOpenKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon		SUCCESS	Desired Access: ALL Access: Disposition
22:28:15.1405796	Mahware_Bulid_Week_U3.exe	1552	RegOpenKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon		SUCCESS	Kau: Kau Information Name: Kau: Kau Handle

Event Properties

Event

Process

Stack

Date:

20/04/2024 12:46:01

Thread:

2356

Class:

Registry

Operation:

RegCreateKey

Result:

SUCCESS

Path:

HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\Current

Duration:

0.0000165

Desired Access:

All Access

Disposition:

REG_OPENED_EXISTING_KEY

Qui sotto la chiave aggiunta al registro dal malware

[illegible]

-Quale valore viene associato alla chiave di registro creata?

R: Viene creata la libreria di sistema (msgina.dll) qui sotto l'estratto del registro:

14:06:...	Malware_Build_...	2200	CreateFileMapping	C:\Windows\SysWOW64\sechost.dll	SUCCESS	Sync type: Sync ty...
14:06:...	Malware_Build_...	2200	CloseFile	C:\Windows\SysWOW64\sechost.dll	SUCCESS	
14:06:...	Malware_Build_...	2200	CreateFile	C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3\msgina32.dll	SUCCESS	Desired Access: G...
14:06:...	Malware_Build_...	2200	WriteFile	C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3\msgina32.dll	SUCCESS	Offset: 0, Length: 4...
14:06:...	Malware_Build_...	2200	WriteFile	C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3\msgina32.dll	SUCCESS	Offset: 4,096, Leng...
14:06:...	Malware_Build_...	2200	CloseFile	C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3\msgina32.dll	SUCCESS	
14:06:...	Malware_Build_...	2200	QueryNameInformationFile	C:\Windows\System32\apiutilschema.dll	SUCCESS	Name: \Windows\...
14:06:...	Malware_Build_...	2200	QueryNameInformationFile	C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3\Malware_Build_Week_113.exe	SUCCESS	Name: \Users\user...

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?

R: Qui sotto si vede la parte che crea (msgina.dll) la libreria nella cartella del malware.

Process	Time	Operation	Path	Result	Details
Malware_Build...	2200	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
Malware_Build...	2200	RegOpenKey	HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Diagnostics	NAME NOT FOUND	Desired Access: R...
Malware_Build...	2200	CreateFile	C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3\msgina32.dll	SUCCESS	Desired Access: G...
Malware_Build...	2200	WriteFile	C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3\msgina32.dll	SUCCESS	Offset: 0, Length: 4...
Malware_Build...	2200	WriteFile	C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3\msgina32.dll	SUCCESS	Offset: 4,096, Leng...
Malware_Build...	2200	CloseFile	C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3\msgina32.dll	SUCCESS	
Malware_Build...	2200	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
Malware_Build...	2200	RegCreateKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	Desired Access: All...
Malware_Build...	2200	RegSetInfoKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	KeySetInformation...
Malware_Build...	2200	RegQueryKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	Query: HandleTag...
Malware_Build...	2200	RegSetValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL	ACCESS DENIED	Type: REG_SZ, Le...
Malware_Build...	2200	RegCloseKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	
Malware_Build...	2200	QueryNameInformationFile	C:\Windows\System32\apiset.schema.dll	SUCCESS	Name: \Windows\...

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

R: Si potrebbe dedurre che il malware in questione possa cercare di creare la sua persistenza in modo tale da avviarsi ogni volta che viene riavviato il pc.

Qui sotto esegue una serie di cicli if ed else:

004014E5	. 59	POP ECX
004014E6	. 85C0	TEST EAX,EAX
004014E8	. 75 08	JNZ SHORT Malware_.004014F2
004014EA	. 6A 1C	PUSH 1C
004014EC	. E8 9A000000	CALL Malware_.0040158B

Potrebbe essere un keylogger oppure un analizzatore di cartelle di windows.

Cybersecurity Analyst 2023