

Benchmark M6

esercitazione finale modulo 6

Malware Analysis

Ignazio Saba

TRACCIA

rispondere ai seguenti quesiti:

Analisi statica BASICA

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.

ANALISI STATICÀ BASICA

-QUANTI PARAMETRI SONO PASSATI ALLA FUNZIONE MAIN()?

alla funzione main vengono passati tre parametri

1. **int argc**
2. **char argv**
3. **char envp**

-QUANTE VARIABILI SONO DICHIARATE ALL'INTERNO DELLA FUNZIONE MAIN()?

All'interno della funzione mail sono dichiarate cinque variabili

hModule = dword ptr -11Ch

Data = byte ptr -118h

var_117 = byte ptr -117h

var_8 = dword ptr -8

var_4 = dword ptr -4

ANALISI STATICÀ BASICA

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

Name	Virtual Size	Virtual Address
00000250	00000258	0000025C
Byte[8]	Dword	Dword
.text	00005646	00001000
.rdata	000009AE	00007000
.data	00003EA8	00008000
.rsrc	00001A70	0000C000

Tramite CFF possiamo farci un'idea precisa delle sezioni che compongono il software

- **.text:** contiene le righe di codice che verranno eseguite una volta che il software viene avviato
- **.rdata:** contiene le informazioni sulle librerie importate
- **.data:** contiene i dati e le variabili globali
- **.rsrc:** contiene le risorse utili al software come immagini, icone etc...

ANALISI STATICÀ BASICA

-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.

Il malware importa due librerie la KERNEL32.DLL e la ADVAPI32.DLL
kernel32.dll incorpora 51 funzioni mentre la advapi32.dll ne incorpora 2.

Visto le funzioni CreateFileA, WriteFile potrebbero creare dei file nelle cartelle di startup di windows per stabilire una persistenza sulla macchina e avendo accesso ai registri di sistema tramite la dll advapi32 magari riavviare il software dopo un reboot senza lasciare dei file abbastanza evidenti nelle cartelle di startup

TRACCIA

ANALISI STATICÀ AVANZATA

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»?

ANALISI STATICÀ AVANZATA

LO SCOPO DELLA FUNZIONE CHIAMATA ALLA LOCAZIONE DI MEMORIA 00401021

Lo scopo della funzione **RegCreateKeyExA** è quello di scrivere sul registro una lista di comandi/software da avviare all'avvio della macchina

COME VENGONO PASSATI I PARAMETRI ALLA FUNZIONE ALLA LOCAZIONE 00401021

i parametri vengono passati alla funzione tramite le istruzioni push

.text:00401004	push	0	; lpdwDisposition
.text:00401006	lea	eax, [ebp+hObject]	
.text:00401009	push	eax	; phkResult
.text:0040100A	push	0	; lpSecurityAttributes
.text:0040100C	push	0F003Fh	; samDesired
.text:00401011	push	0	; dwOptions
.text:00401013	push	0	; lpClass
.text:00401015	push	0	; Reserved
.text:00401017	push	offset SubKey	; "SOFTWARE\\Microsoft\\
.text:0040101C	push	80000002h	; hKey
.text:00401021	call	ds:RegCreateKeyExA	

ANALISI STATICÀ AVANZATA

CHE OGGETTO RAPPRESENTA IL PARAMETRO ALLA LOCAZIONE 00401017

l'oggetto **SubKey** rappresenta un array di char e contiene un indirizzo

IL SIGNIFICATO DELLE ISTRUZIONI COMPRESE TRA GLI INDIRIZZI 00401027 E 00401029.

le istruzioni tra 00401027 e 00401029 rappresentano un ciclo if

test eax, eax

jz short loc_401032

CON RIFERIMENTO ALL'ULTIMO QUESITO,

TRADURRE IL CODICE ASSEMBLY NEL CORRISPONDENTE COSTRUTTO C

```
if (eax == eax) {  
    goto loc_401032;  
}
```

ANALISI STATICÀ AVANZATA

VALUTATE ORA LA CHIAMATA ALLA LOCAZIONE 00401047,
QUAL È IL VALORE DEL PARAMETRO «VALUENAME»?

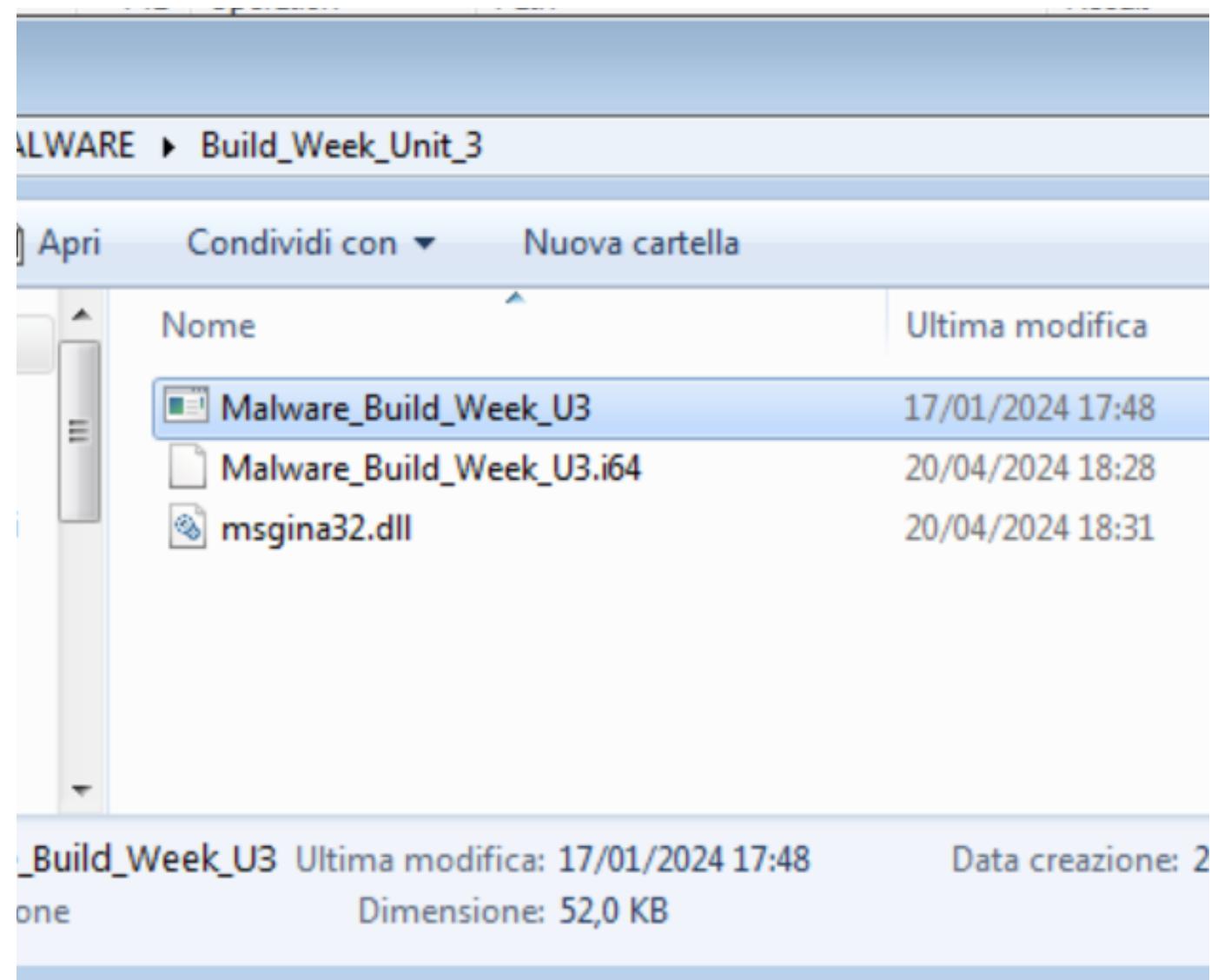
il valore del parametro ValueName è “**GinaDLL**”

- t:0040103E
- t:00401043
- t:00401046
- t:00401047

```
push    offset ValueName ; "GinaDLL"
mov     eax, [ebp+hObject]
push    eax             ; hKey
call    ds:RegSetValueExA
```

ANALISI DINAMICA AVANZATA

-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



si può notare che è stato creato un nuovo file con il nome “**msgina32.dll**” e che sono state appunto utilizzate le librerie citate in precedenza sia per creare il file sia per scrivere sul registro

ANALISI DINAMICA AVANZATA

FILTRATE INCLUDENDO SOLAMENTE L'ATTIVITÀ SUL REGISTRO DI WINDOWS.

-QUALE CHIAVE DI REGISTRO VIENE CREATA?

-QUALE VALORE VIENE ASSOCIAATO ALLA CHIAVE DI REGISTRO CREATA?

HKLM\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINLOGON\GINADLL

RegQueryKey	HKLM	S... Query: HandleTags, HandleTags: 0x0
RegCreateKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon	S... Desired Access: All Access, Disposition: REG_OPENED_EXISTING_KEY
RegSetInfoKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon	S... KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
RegQueryKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon	S... Query: HandleTags, HandleTags: 0x400
RegSetValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL	A... Type: REG_SZ, Length: 520, Data: C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3\msgina32.dll
RegCloseKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon	S...

QUALE CHIAMATA DI SISTEMA HA MODIFICATO IL CONTENUTO DELLA CARTELLA DOVE È PRESENTE
L'ESEGUIBILE DEL MALWARE?

1608	CreateFile	C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3\msgina32.dll	S... Desired Access: Generic Write, Read Attributes
1608	WriteFile	C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3\msgina32.dll	S... Offset: 0, Length: 4.096, Priority: Normal
1608	WriteFile	C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3\msgina32.dll	S... Offset: 4.096, Length: 2.560, Priority: Normal
1608	CloseFile	C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3\msgina32.dll	S...