Malware Analysis

Quanti parametri sono passati alla funzione Main()?

Alla funzione " Main " vengono passati 3 parametri.

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

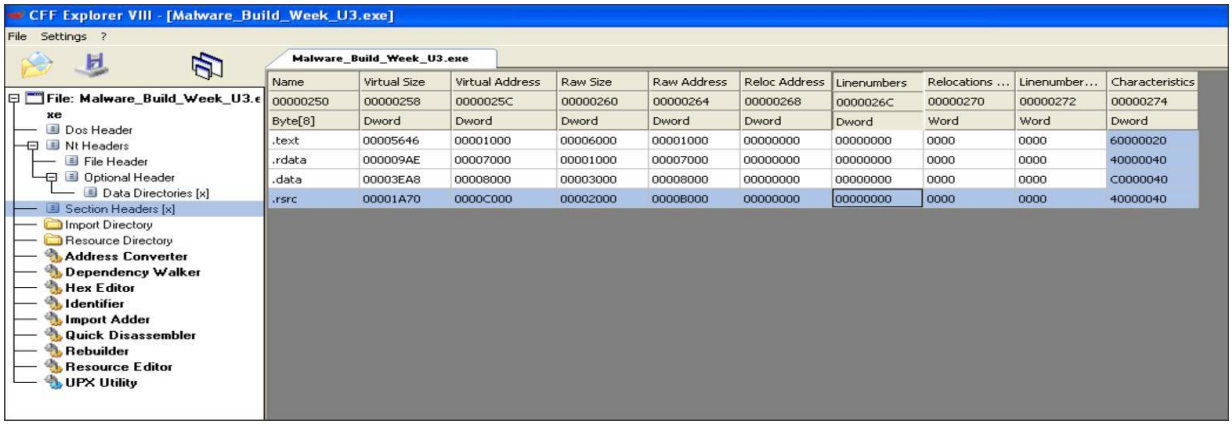
Quante variabili sono dichiarate all'interno della funzione Main()?

All interno della funzione " Main " sono state dichiarate 7 variabili.

```
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
```

Quali sezioni sono presenti all'interno del file eseguibile?

Possiamo trovare 4 sezioni differenti.



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

Descrivete brevemente almeno 2 di quelle identificate?

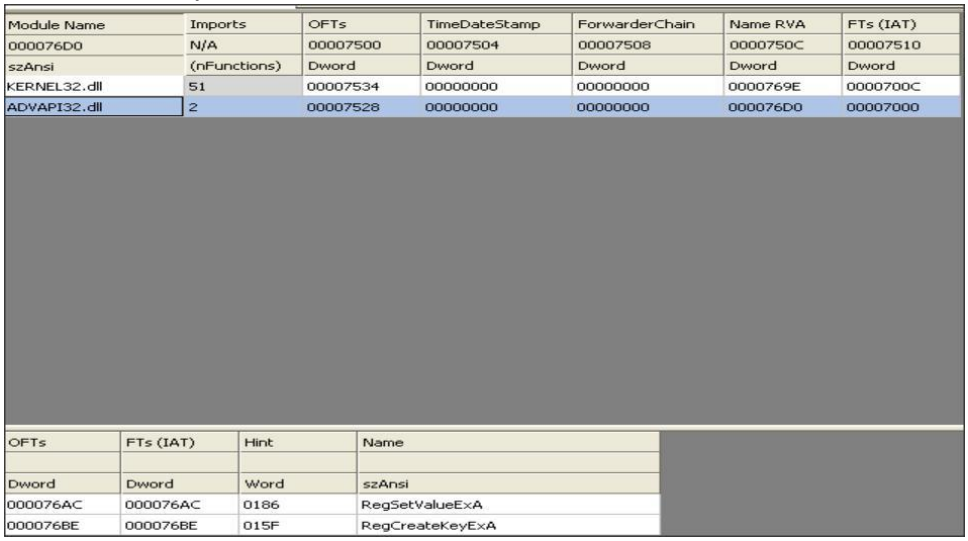
".data"-> In questa sezione, vengono definite le variabili globali e statiche insieme ai loro valori iniziali.

".rsrc"-> L'estensione di file ".rsrc" potrebbe essere utilizzata per mascherare o camuffare i file malevoli. I dropper malware sono progettati per depositare o scaricare ulteriori componenti dannosi sul sistema infetto.L'uso dell'estensione ".rsrc" potrebbe essere una tecnica utilizzata dagli attaccanti per eludere le misure di sicurezza, come i filtri basati sulle estensioni dei file.Quando un dropper malware

utilizza l'estensione ".rsrc", potrebbe far sembrare che il file sia legato a risorse del sistema o dati innocui.

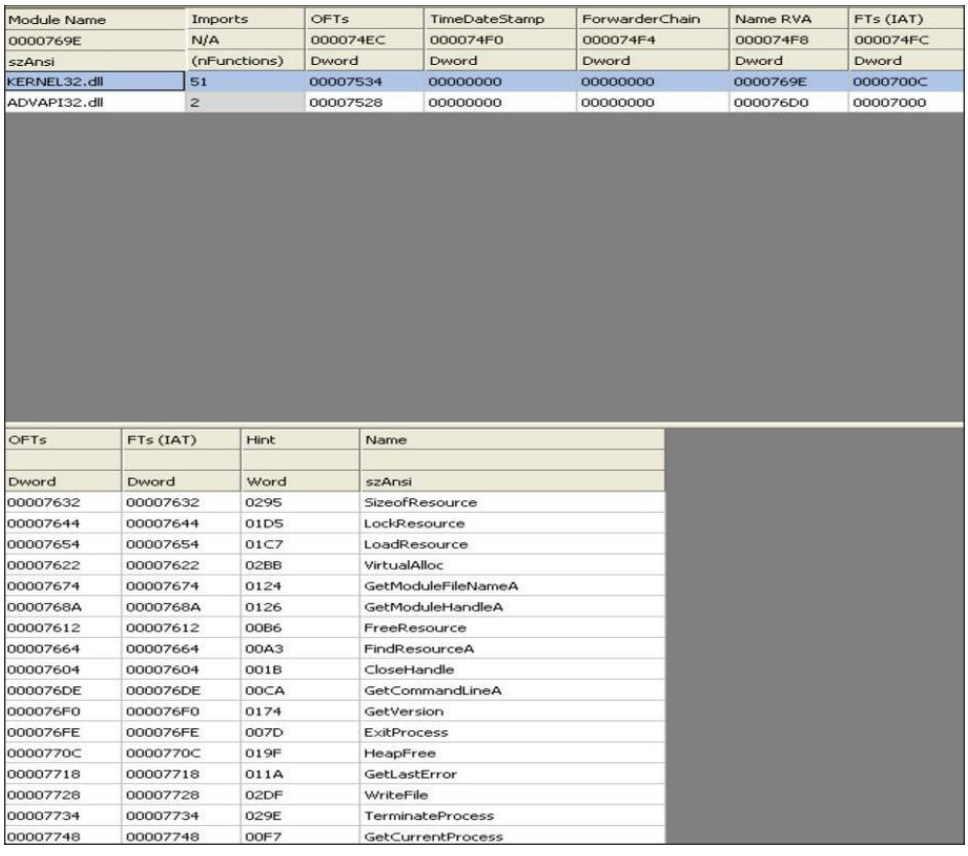
Quali librerie importa il Malware?

Il Malware importa le librerie relative al KERNEL32 e ADVAPI32



Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
000076D0	N/A	00007500	00007504	00007508	0000750C	00007510
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	51	00007534	00000000	00000000	0000769E	0000700C
ADVAPI32.dll	2	00007528	00000000	00000000	000076D0	00007000

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
000076AC	000076AC	0186	RegSetValueExA
000076BE	000076BE	015F	RegCreateKeyExA



Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
0000769E	N/A	000074EC	000074F0	000074F4	000074F8	000074FC
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	51	00007534	00000000	00000000	0000769E	0000700C
ADVAPI32.dll	2	00007528	00000000	00000000	000076D0	00007000

OFTs	FTs (IAT)	Hint	Name
Dword	Dword	Word	szAnsi
00007632	00007632	0295	SizeofResource
00007644	00007644	01D5	LockResource
00007654	00007654	01C7	LoadResource
00007622	00007622	02BB	VirtualAlloc
00007674	00007674	0124	GetModuleFileNameA
0000768A	0000768A	0126	GetModuleHandleA
00007612	00007612	00B6	FreeResource
00007664	00007664	00A3	FindResourceA
00007604	00007604	001B	CloseHandle
000076DE	000076DE	00CA	GetCommandLineA
000076F0	000076F0	0174	GetVersion
000076FE	000076FE	007D	ExitProcess
0000770C	0000770C	019F	HeapFree
00007718	00007718	011A	GetLastError
00007728	00007728	02DF	WriteFile
00007734	00007734	029E	TerminateProcess
00007748	00007748	00F7	GetCurrentProcess

Per ognuna delle librerie importate, fate delle ipotesi sulla base della sola analisi statica delle funzionalità che il Malware potrebbe implementare.

Queste librerie sono parte fondamentale del sistema operativo Windows e consentono l'accesso a una vasta gamma di funzionalità, inclusa la gestione dei processi, la comunicazione con il Registro di sistema, la gestione dei servizi di Windows e molto altro.

Ecco alcuni esempi di ciò che un malware dropper potrebbe fare utilizzando queste librerie:

- **Installazione persistente**: Il dropper potrebbe utilizzare le funzioni di Advapi32 per installarsi come servizio di Windows persistente. Questo consentirebbe al malware di essere eseguito automaticamente all'avvio del sistema, rendendo più difficile la sua individuazione e rimozione.
- **Elevazione dei privilegi**: Utilizzando funzioni specifiche di Kernel32 e Advapi32, il malware potrebbe tentare di elevare i suoi privilegi per ottenere accesso amministrativo al sistema. Ciò permetterebbe al malware di aggirare le restrizioni di sicurezza e avere un controllo maggiore sul sistema.
- **Attivazione di altre funzionalità dannose**: Una volta installato e con i privilegi elevati, il dropper potrebbe utilizzare le librerie per scaricare e installare componenti dannosi aggiuntivi sul sistema. Questi componenti potrebbero includere spyware, ransomware, botnet o altre minacce.
- **Manomissione del Registro di sistema**: Utilizzando le funzioni di Advapi32, il malware potrebbe modificare il Registro di sistema per ottenere persistenza, disabilitare strumenti di sicurezza o alterare le impostazioni di sicurezza del sistema.
- **Raccolta di informazioni**: Il dropper potrebbe utilizzare le librerie per raccogliere informazioni sensibili sul sistema o sull'utente, come password, informazioni di accesso o dettagli personali, e inviarli a un server controllato dall'attaccante.
- **Attacchi a reti**: Il malware potrebbe utilizzare le librerie per effettuare attacchi di rete, come scanner di porte o attacchi di forza bruta, per cercare di propagarsi ad altri sistemi nella stessa rete.
- **Disattivazione dei servizi di sicurezza**: Il malware potrebbe tentare di disabilitare o eludere software antivirus, firewall o altre misure di sicurezza presenti sul sistema.

Malware Analysis

Con riferimento al Malware in analisi, spiegare:

Lo scopo della funzione chiamata alla locazione di memoria 00401021

La funzione "RegCreateKeyExA" è una funzione dell'API di Windows, inclusa nella libreria di sistema "Advapi32.dll". Questa funzione è utilizzata per creare una nuova chiave di registro o aprire una chiave di registro esistente nel Registro di sistema di Windows.

Come vengono passati i parametri alla funzione alla locazione 00401021

Che oggetto rappresenta il parametro alla locazione 00401017

Il registro Windows del login

Il significato delle istruzioni comprese tra gli indirizzi 00401027 e 00401029

Il codice assembly effettua un'operazione di test e un salto condizionale. Questa sequenza di istruzioni è utilizzata per controllare se il valore contenuto nel registro EAX è uguale a zero.

- **TEST EAX, EAX**: Questa istruzione esegue un'operazione logica AND tra il registro EAX e se stesso. Questa istruzione verifica se il valore di EAX è zero o meno.
- **JE SHORT Malware_.00401032**: Questa è un'istruzione di salto condizionale, specificamente "Jump if Equal" (JE). Se il risultato del test precedente è uguale a zero (cioè EAX è zero), il salto verrà eseguito e il flusso di esecuzione del programma passerà all'etichetta "Malware_.00401032".

Il codice sta controllando se il valore contenuto nel registro EAX è zero. Se lo è, il flusso del programma salterà a un'etichetta denominata "Malware_.00401032", che probabilmente rappresenta una parte di codice associata al comportamento del malware in caso di condizione specifica.

Con riferimento all'ultimo quesito, tradurre il codice Assembly nel corrispondente costrutto C

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

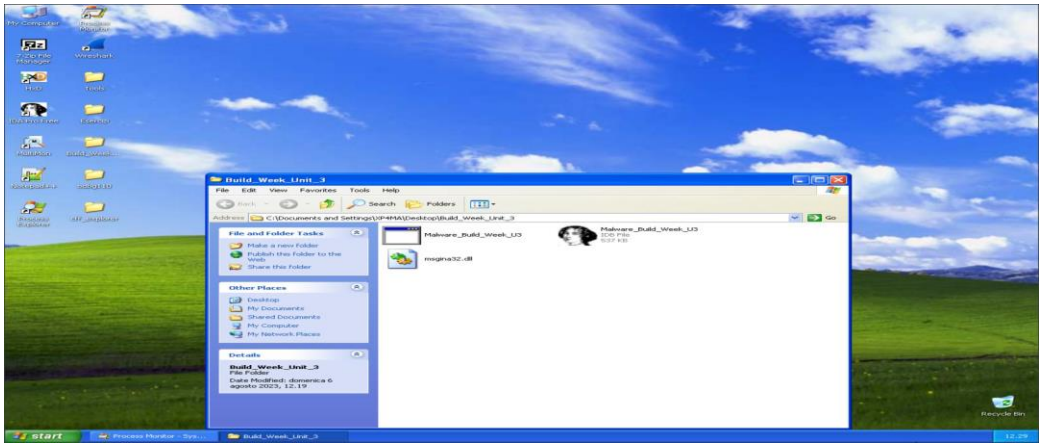
Valutate ora la chiamata alla locazione 00401047, qual è il valore del parametro «ValueName»?

Il valore del parametro " ValueName " è: GinaDLL

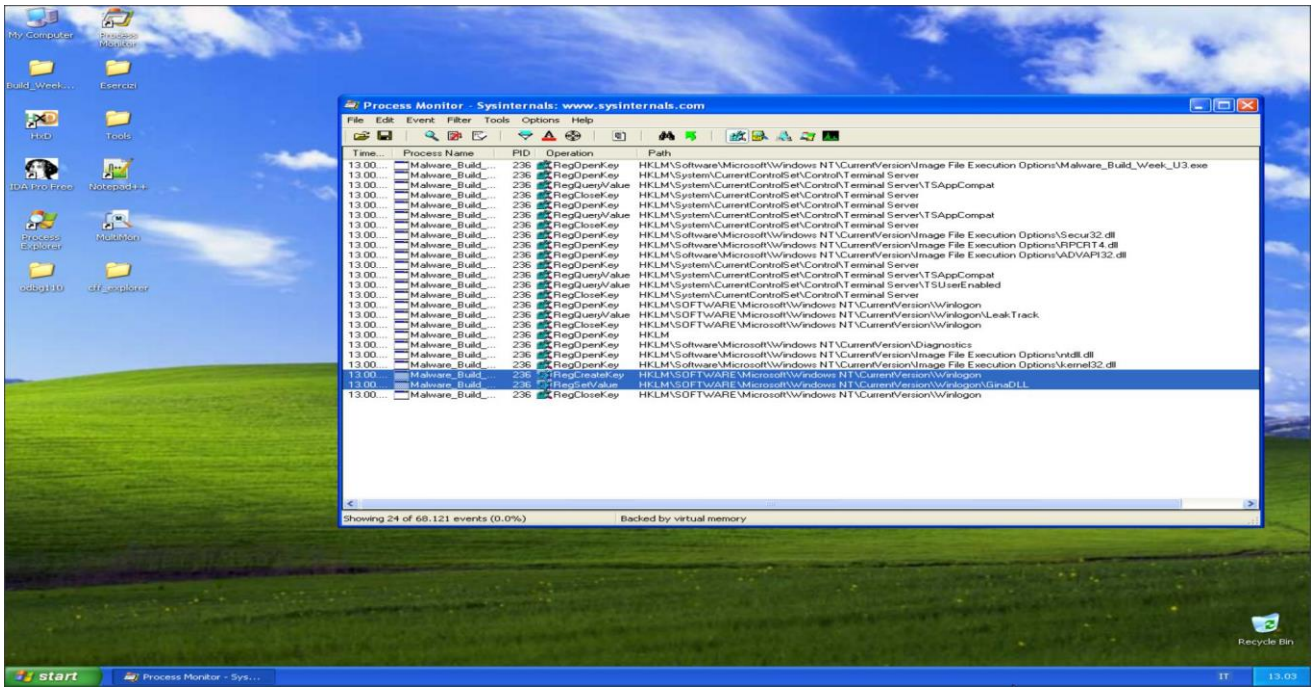
Malware Analysis

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

Il Malware va a modificare e ricreare nella sua cartella la libreria GinaDLL.



Quale chiave di registro viene creata?



Quale valore viene associato alla chiave di registro creata?

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.

Il Malware è probabilmente un tipo " dropper " in quanto utilizza la sezione ".rsrc" per essere meno individuabile e che contiene al suo interno un logger per copiare le credenziali d accesso che potrebbero essere mandate via internet a chi ha creato il codice malevole.