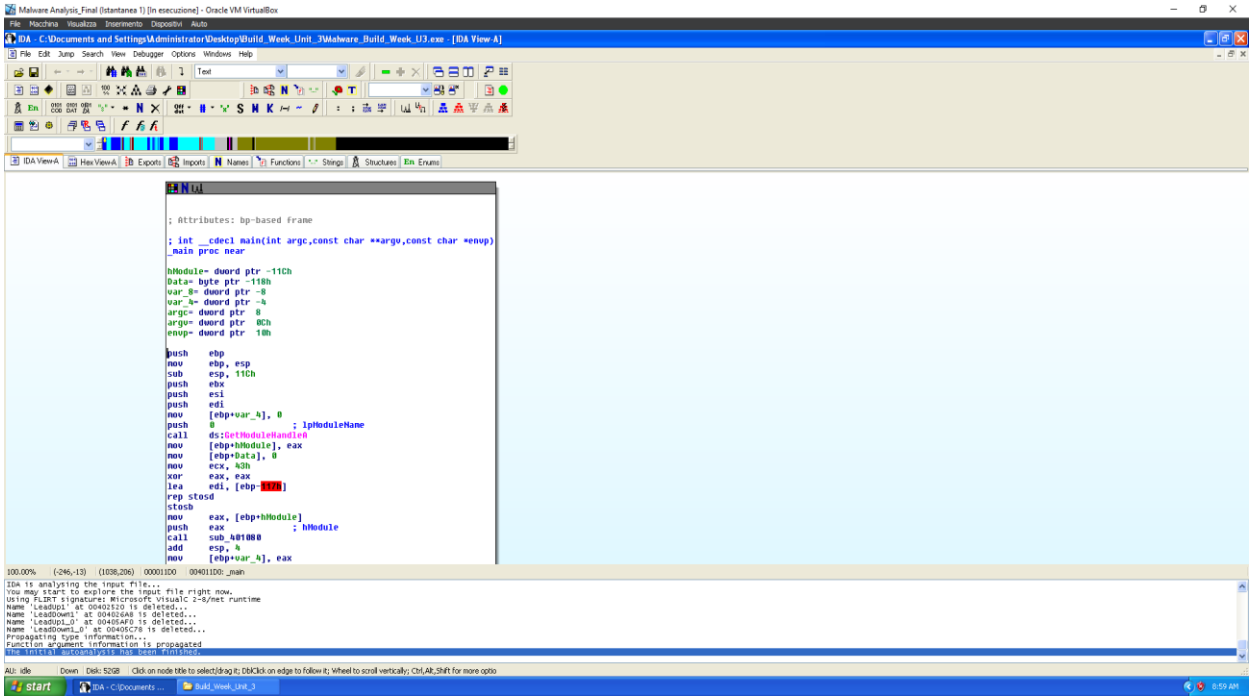
Funzione Main:



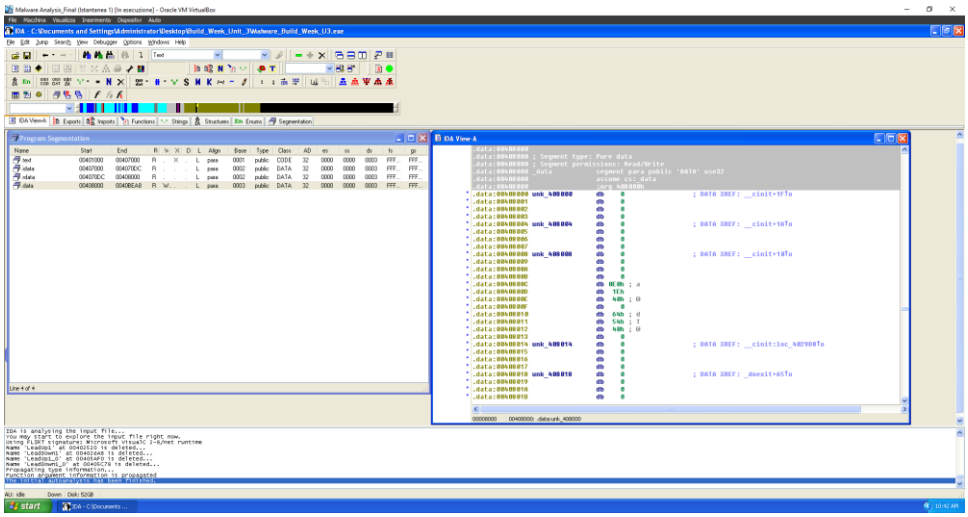

```
argc= dword ptr  8
argv= dword ptr  0Ch
envp= dword ptr  10h
```

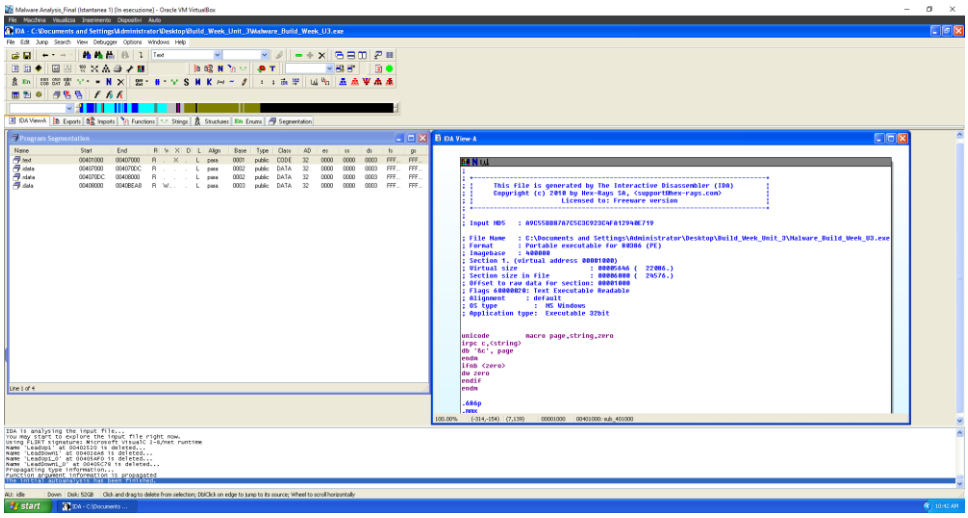
La 2 foto mostra i parametri scoperti nel codice 3 stringhe

```
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
```

La 3 foto mostra le variabili scoperte nel codice ovvero 7 stringhe di codice

Foto delle sezioni di eseguibile sotto:



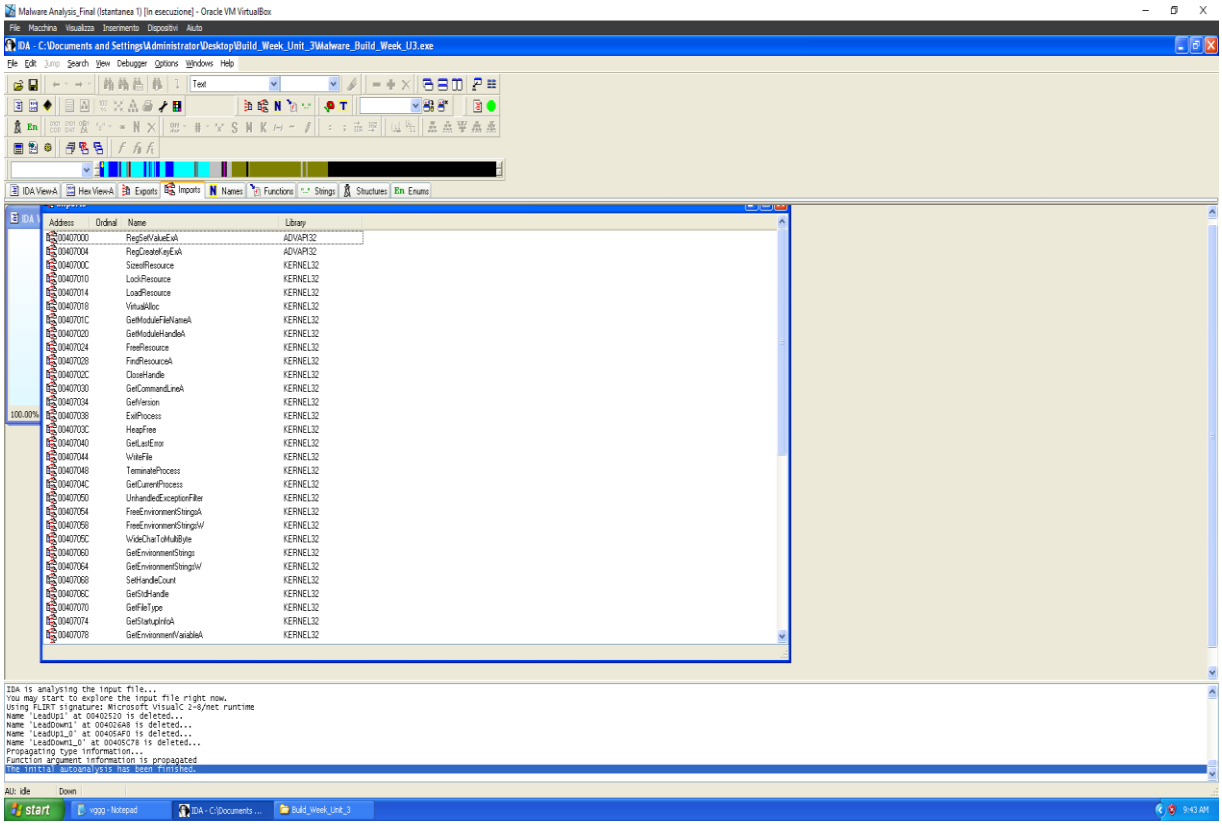


Descrizione:

Il primo file data e il 2 text, il data contiene i file inizializzati

e il text è il codice dell'eseguibile che viene eseguito. Le sezioni possono avere permessi di accesso specifici che indicano se i dati nella sezione possono essere letti, scritti o eseguiti

Librerie importate sono 53 circa



Ipotesi:

Il malware potrebbe chiaramente scrivere un file aprire i processi e prendere info del sistema operativo, ha anche cambiato una chiave di registro, il malware potrebbe installare programmi e rubare file, se si guarda attentamente le funzioni ci dicono RegSetCreateKey la prima qui sta parlando di creazioni chiave WriteFile,TerminateProcess, GetFileType,GetCPInfo,SizeofResource. Sono ipotesi di cosa possa fare il malware,ma fa queste librerie. GetProcAddress è la libreria che sta chiamando con la funzione o una variabile dalla dll.

Spiegazione delle funzioni:

1)La prima crea una funzione che crea una chiave di registro.

2)La seconda risposta, è attraverso il "Push stringa di comando" vengono passati nella funzione i parametri

3) codice di basso livello, dove il parametro , è un software che sta in una cartella del sistema windows.

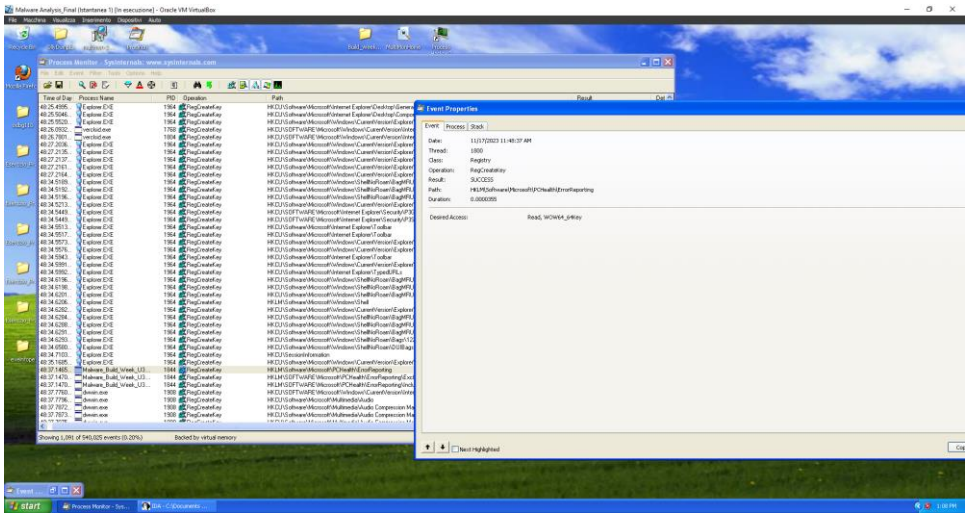
4) verifica che il registro EAX è uguale a 0. Je invece fa un salto

5) codice tradotto in C :

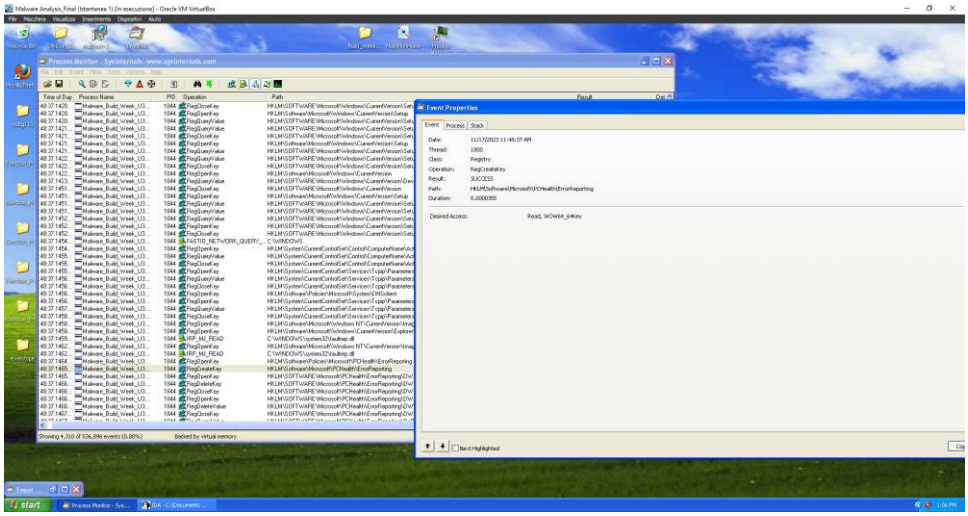
```
if (EAX == 0) {
   goto Malware_.00401032
}
```

6)Il valore di ValueName è 0 , nella stringa push Malware.0040804C,che fa riferimento a GinaDll come libreria

Risposte



1)si la funzione RegCreateKey lo dimostra la foto, la key creata WOW64_64Key



2)i valori sono nelle foto PID e THREAD

3)la chiamata irp_mj_create ha modificato il contenuto cartella attreverso regopenkey