

ANALISI STATICA

- 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.

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

I parametri sono tre:

argc= dword ptr 8;

argv= dword ptr 0Ch;

envp= dword ptr 10h.

Le variabili sono quattro:

hModule= dword ptr -11Ch;

Data= byte ptr -118h;

var_8= dword ptr -8;

var_4= dword ptr -4;

CFF Explorer VIII - [Malware_Build_Week_U3.exe]

File: Malware_Build_Week_U3.exe

Section Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations	Linenumbers	Characteristics
.text	00005446	00001000	00006000	00001000	00000000	00000000	0000	0000	60000020
.rdata	0000094E	00007000	00001000	00007000	00000000	00000000	0000	0000	40000040
.data	00003EAB	00008000	00003000	00008000	00000000	00000000	0000	0000	C0000040
.rsrc	00001A70	0000C000	00002000	0000C000	00000000	00000000	0000	0000	40000040

Hex Dump (Offset 00000000):

```

00000000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ | . . . yv
00000010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  . . . .
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  . . . .
00000030  00 00 00 00 00 00 00 00 00 00 00 00 E0 00 00 00  . . . .
00000040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  . . . . If, LI!Th
00000050  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
00000060  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS
00000070  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode.
00000080  65 2D 2F E7 21 4C 41 B4 21 4C 41 B4 21 4C 41 B4  e~c|LA'LA'LA'
00000090  17 6A 4A B4 20 4C 41 B4 A2 50 4F B4 2E 4C 41 B4  tJ LA'FO'LA'
000000A0  17 6A 4B B4 16 4C 41 B4 43 53 52 B4 24 4C 41 B4  tJ LA'CS'LA'
000000B0  21 4C 40 B4 17 4C 41 B4 17 6A 54 B4 20 4C 41 B4  tJ LA'1st'LA'
000000C0  E5 4A 47 B4 20 4C 41 B4 52 69 63 68 21 4C 41 B4  aJG'LA'Rich'LA'
000000D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  . . . .
000000E0  50 45 00 00 4C 01 04 00 0A D8 B6 4E 00 00 00 00  . . . .
000000F0  00 00 00 00 E0 00 0F 01 0B 01 06 00 00 60 00 00  . . . .
00000100  00 70 00 00 00 00 00 00 87 14 00 00 00 10 00 00  . . . .
00000110  00 70 00 00 00 00 40 00 00 00 10 00 00 10 00 00  . . . .

```

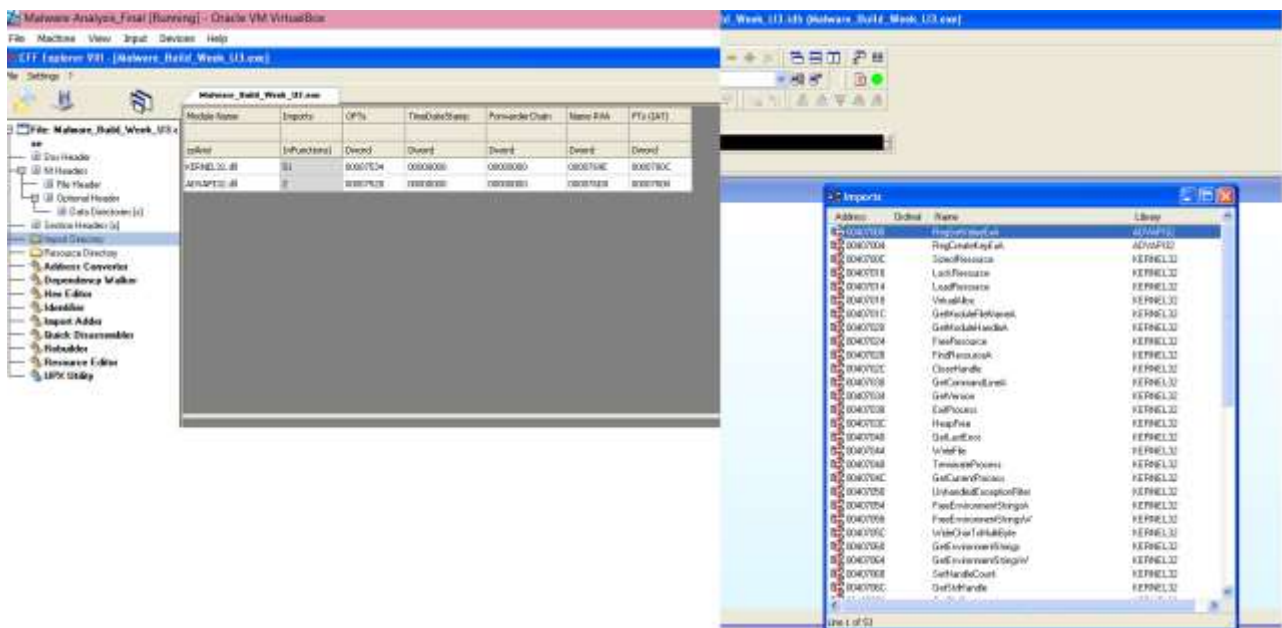
Analizzando il file con CFF Explorer notiamo che si compone di quattro sezioni:

.text: contiene le istruzioni (righe di codice) che la CPU eseguirà una volta che il software sarà avviato;

.rdata: include le informazioni circa le librerie e le funzioni importate ed esportate dall'eseguibile;

.data: contiene i file/le variabili globali del programma eseguibile che devono essere disponibili da qualsiasi parte del programma;

.rsrc: include le risorse utilizzate dall'eseguibile come ad esempio le icone, immagini, menù e stringhe che non sono parte dell'eseguibile stesso.



Le librerie che importa il malware sono KERNEL32 e ADVAPI32.

KERNEL32: contiene le funzioni principali per interagire con il sistema operativo: manipolazione dei file, gestione della memoria. Analizzando le funzioni chiamate notiamo **FindResource**; **LoadResource**; **LockResource**; **SizeOfResource**; Queste funzioni fanno pensare ad un Dropper (programma malevolo che contiene al suo interno un malware. Nel momento in cui viene eseguito inizia la sua esecuzione ed estrae il malware che contiene per salvarlo sul disco.

ADVAPI32: contiene le funzioni per interagire con i servizi ed i registri del sistema operativo Windows. Il malware servendosi di questa libreria potrebbe modificare delle chiavi di registro per copiare sé stesso nelle entry dei programmi infatti la funzione chiamata è **RegSetValueExA** che permette di aggiungere un nuovo valore all'interno del registro. Viene chiamata anche la funzione **RegCreateKeyExA** per creare o aprire una specifica chiave di registro.

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»?

```
.text:00401011      push     0                ; dwOptions
.text:00401013      push     0                ; lpClass
.text:00401015      push     0                ; Reserved
.text:00401017      push     offset SubKey    ; "SOFTWARE\\Microsoft\\Windows NT\\CurrentVe..."
.text:0040101C      push     80000002h        ; hKey
.text:00401021      call     ds:RegCreateKeyExA
.text:00401027      test     eax, eax
.text:00401029      jz       short loc_401032
.text:0040102B      mov     eax, 1
.text:00401030      jnp     short loc_40107B
.text:00401032      ; -----
.text:00401032      loc_401032:
.text:00401032      mov     ecx, [ebp+cbData] ; CODE XREF: sub_401000+29↑j
.text:00401035      push     ecx              ; cbData
.text:00401036      mov     edx, [ebp+lpData] ; lpData
.text:00401039      push     edx              ; lpData
.text:0040103A      push     1                ; dwType
.text:0040103C      push     0                ; Reserved
.text:0040103E      push     offset ValueName ; "GinaDLL"
.text:00401043      mov     eax, [ebp+hObject]
.text:00401046      push     eax              ; hKey
.text:00401047      call     ds:RegSetValueExA
.text:0040104D      test     eax, eax
.text:0040104F      jz       short loc_401062
.text:00401051      mov     ecx, [ebp+hObject]
.text:00401054      push     ecx              ; hObject
.text:00401055      call     ds:CloseHandle
.text:0040105B      mov     eax, 1
.text:00401060      jmp     short loc_40107B
.text:00401062      ; -----
.text:00401062
```

La funzione chiamata all'indirizzo 00401021 è RegCreateKeyExA serve per creare o aprire una specifica chiave di registro. I parametri di questa funzione sono:

```

.text:00401000      ; lpdwDisposition
.text:00401000      push     ebp
.text:00401001      mov      ebp, esp
.text:00401003      push     ecx
.text:00401004      push     0
.text:00401006      lea      eax, [ebp+hObject]
.text:00401009      push     eax
.text:0040100A      push     0
.text:0040100C      push     0F003Fh
.text:00401011      push     0
.text:00401013      push     0
.text:00401015      push     0
.text:00401017      push     offset SubKey
.text:0040101C      push     80000002h
.text:00401021      call     ds:RegCreateKeyEx

```

Notiamo che vengono passati con **push**.

Il parametro alla locazione 00401017

```

.text:00401013      push     0
.text:00401015      push     0
.text:00401017      push     offset SubKey
.text:0040101C      push     80000002h

```

Identifica la sottochiave di registro che si sta creando o modificando.

```

ext:0040101C      push     80000002h
ext:00401021      call     ds:RegCreateKeyEx
ext:00401027      test     eax, eax
ext:00401029      jz       short loc_401032
ext:0040102B      mov      eax, 1

```

All'indirizzo 00401027 troviamo TEST che è un'istruzione simile ad AND ma non modifica il contenuto degli operandi. Modifica il **ZeroFlag** del registro **EFlags** che viene settato a 1 se e solo se il risultato dell'AND è 0.

All'indirizzo 00401029 invece troviamo un salto condizionale. I salti condizionali utilizzano il contenuto dei flags per determinare se saltare o meno ad una data locazione che viene specificata come operando dell'istruzione jump. In quest caso è JZ (Jump If Zero), che setta ZF=1.

Se il valore di `eax` è 0 allora viene effettuato il salto. Altrimenti si prosegue con l'istruzione successiva.

TRADUZIONE IN C

```
int x;  
  
int y;  
  
if ( x == y ) {  
    printf("x equals y.\n")  
}  
else {  
    Printf("x is not equal to y.\n");  
}  
  
-----
```

Alla locazione 00401047 è chiamata la funzione `RegSetValueExA`

<pre>ext:00401046 ext:00401047 ext:0040104D ext:0040104F</pre>	<pre>mov eax, [ebp+00000004] push eax call ds:RegSetValueExA test eax, eax jz short loc_401062</pre>
--	--

Questa serve per impostare i dati e il tipo di valore specificato in una chiave di registro. Il valore del parametro `ValueName` (che è un parametro della funzione) ci permette di impostare il nome del valore da impostare per chiave di registro che si sta creando o modificando in questo caso è `GinaDLL.*`

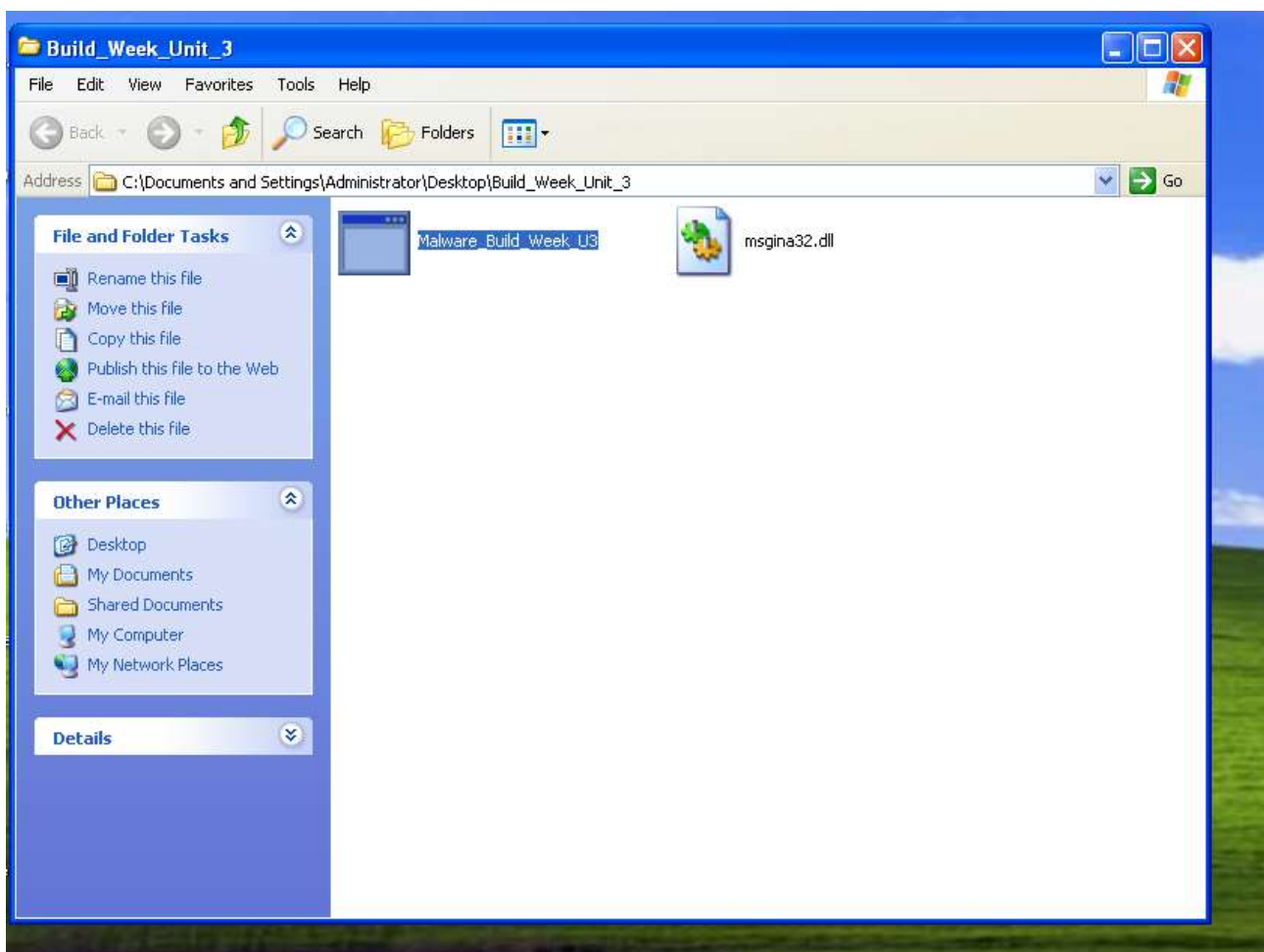
```

• ext:0040103A      push     1                ; dwType
• ext:0040103C      push     0                ; Reserved
• ext:0040103E      push     offset ValueName ; "GinaDLL"
• ext:00401043      mov      eax, [ebp+hObject]
• ext:00401046      push     eax                ; hKey
• ext:00401047      call    ds:RegSetValueExA

```

ANALISI DINAMICA

- 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



All'interno della cartella è stato creato il file msgina32.dll visto precedentemente, la quale non è altro che la chiave di registro

modificata dal malware creata con la funzione RegCreateKeyExA. È questo il modo in cui il malware ha ottenuto la persistenza.

Malware Analysis_Final [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time of Day	Process Name	PID	Operation	Path
5:25:43.77601...	Malware_Build_Week_U3...	1552	Process Start	
5:25:43.77601...	Malware_Build_Week_U3...	1552	Thread Create	
5:25:43.77624...	Malware_Build_Week_U3...	1552	QueryNameInformationFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\Malware_Build_\
5:25:43.77641...	Malware_Build_Week_U3...	1552	Load Image	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\Malware_Build_\
5:25:43.77655...	Malware_Build_Week_U3...	1552	Load Image	C:\WINDOWS\system32\ntdll.dll
5:25:43.77657...	Malware_Build_Week_U3...	1552	QueryNameInformationFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\Malware_Build_\
5:25:43.77672...	Malware_Build_Week_U3...	1552	CreateFile	C:\WINDOWS\Prefetch\MALWARE_BUILD_WEEK_U3.EXE-0E171D0F.pf
5:25:43.78094...	Malware_Build_Week_U3...	1552		
5:25:43.78103...	Malware_Build_Week_U3...	1552		
5:25:43.78105...	Malware_Build_Week_U3...	1552		
5:25:43.79867...	Malware_Build_Week_U3...	1552		
5:25:43.79900...	Malware_Build_Week_U3...	1552		
5:25:43.79903...	Malware_Build_Week_U3...	1552		
5:25:43.79906...	Malware_Build_Week_U3...	1552		
5:25:43.79968...	Malware_Build_Week_U3...	1552		
5:25:43.79971...	Malware_Build_Week_U3...	1552		
5:25:43.79980...	Malware_Build_Week_U3...	1552		
5:25:43.79985...	Malware_Build_Week_U3...	1552		
5:25:43.79992...	Malware_Build_Week_U3...	1552		
5:25:43.79998...	Malware_Build_Week_U3...	1552		
5:25:43.80012...	Malware_Build_Week_U3...	1552		
5:25:43.80017...	Malware_Build_Week_U3...	1552		
5:25:43.80061...	Malware_Build_Week_U3...	1552		
5:25:43.80064...	Malware_Build_Week_U3...	1552		
5:25:43.80073...	Malware_Build_Week_U3...	1552		
5:25:43.80078...	Malware_Build_Week_U3...	1552		
5:25:43.80089...	Malware_Build_Week_U3...	1552		
5:25:43.80104...	Malware_Build_Week_U3...	1552		
5:25:43.80124...	Malware_Build_Week_U3...	1552	QueryDirectory	C:\Documents and Settings\Administrator\Desktop
5:25:43.80135...	Malware_Build_Week_U3...	1552	CloseFile	C:\Documents and Settings\Administrator\Desktop
5:25:43.80160...	Malware_Build_Week_U3...	1552	CreateFile	C:\Documents and Settings\Administrator\Desktop\BUILD_WEEK_UNIT_3
5:25:43.80168...	Malware_Build_Week_U3...	1552	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3
5:25:43.80182...	Malware_Build_Week_U3...	1552	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3
5:25:43.80190...	Malware_Build_Week_U3...	1552	CloseFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3
5:25:43.80201...	Malware_Build_Week_U3...	1552	CreateFile	C:\WINDOWS
5:25:43.80210...	Malware_Build_Week_U3...	1552	QueryDirectory	C:\WINDOWS
5:25:43.80246...	Malware_Build_Week_U3...	1552	QueryDirectory	C:\WINDOWS
5:25:43.80254...	Malware_Build_Week_U3...	1552	CloseFile	C:\WINDOWS
5:25:43.80271...	Malware_Build_Week_U3...	1552	CreateFile	C:\WINDOWS\AppPatch
5:25:43.80280...	Malware_Build_Week_U3...	1552	QueryDirectory	C:\WINDOWS\AppPatch
5:25:43.80296...	Malware_Build_Week_U3...	1552	QueryDirectory	C:\WINDOWS\AppPatch
5:25:43.80307...	Malware_Build_Week_U3...	1552	CloseFile	C:\WINDOWS\AppPatch
5:25:43.80321...	Malware_Build_Week_U3...	1552	CreateFile	C:\WINDOWS\system32

Process Monitor Filter

Display entries matching these conditions:



























Process Name is Malware_Build_Week_U3.exe then Include

Reset Add Remove

Column	Relation	Value	Action
<input checked="" type="checkbox"/> Process Name	is	Malware_Build_...	Include
<input checked="" type="checkbox"/> Process Name	is	Procmon.exe	Exclude
<input checked="" type="checkbox"/> Process Name	is	Procexp.exe	Exclude
<input checked="" type="checkbox"/> Process Name	is	Autoruns.exe	Exclude
<input checked="" type="checkbox"/> Process Name	is	System	Exclude
<input checked="" type="checkbox"/> Operation	begins with	IRP_MJ_	Exclude
<input checked="" type="checkbox"/> Operation	begins with	FASTIO_	Exclude

OK Cancel Apply

Impostando il filtro relativo al malware le chiavi di registro che vengono create sono:

Malware Analysis_Final [Running] - Oracle VM VirtualBox					
File Machine View Input Devices Help					
Process Monitor - Sysinternals: www.sysinternals.com					
File Edit Event Filter Tools Options Help					
                         					
Time of Day	Process Name	PID	Operation	Path	
5:25:43.88968...	Malware_Build_Week_U3...	1552	RegOpenKey	HKLM\Softwa	
5:25:43.89110...	Malware_Build_Week_U3...	1552	RegOpenKey	HKLM\Systemerr	
5:25:43.89113...	Malware_Build_Week_U3...	1552	RegQueryValue	HKLM\Systemerr	
5:25:43.89116...	Malware_Build_Week_U3...	1552	RegCloseKey	HKLM\Systemerr	
5:25:43.89900...	Malware_Build_Week_U3...	1552	RegOpenKey	HKLM\Systemerr	
5:25:43.89903...	Malware_Build_Week_U3...	1552	RegQueryValue	HKLM\Systemerr	
5:25:43.89906...	Malware_Build_Week_U3...	1552	RegCloseKey	HKLM\Systemerr	
5:25:43.89910...	Malware_Build_Week_U3...	1552	RegOpenKey	HKLM\Softwa	
5:25:43.89913...	Malware_Build_Week_U3...	1552	RegOpenKey	HKLM\Softwa	
5:25:43.89916...	Malware_Build_Week_U3...	1552	RegOpenKey	HKLM\Softwa	
5:25:43.89918...	Malware_Build_Week_U3...	1552	RegOpenKey	HKLM\Systemerr	
5:25:43.89920...	Malware_Build_Week_U3...	1552	RegQueryValue	HKLM\Systemerr	
5:25:43.89922...	Malware_Build_Week_U3...	1552	RegQueryValue	HKLM\Systemerr	
5:25:43.89925...	Malware_Build_Week_U3...	1552	RegCloseKey	HKLM\Systemerr	
5:25:43.89926...	Malware_Build_Week_U3...	1552	RegOpenKey	HKLM\SOFT\	
5:25:43.89928...	Malware_Build_Week_U3...	1552	RegQueryValue	HKLM\SOFT\	
5:25:43.89931...	Malware_Build_Week_U3...	1552	RegCloseKey	HKLM\SOFT\	
5:25:43.89931...	Malware_Build_Week_U3...	1552	RegOpenKey	HKLM	
5:25:43.89933...	Malware_Build_Week_U3...	1552	RegOpenKey	HKLM\Softwa	
5:25:43.89936...	Malware_Build_Week_U3...	1552	RegOpenKey	HKLM\Softwa	
5:25:43.89938...	Malware_Build_Week_U3...	1552	RegOpenKey	HKLM\Softwa	
5:25:43.90204...	Malware_Build_Week_U3...	1552	RegCreateKey	HKLM\SOFT\	
5:25:43.90210...	Malware_Build_Week_U3...	1552	RegSetValue	HKLM\SOFT\	
5:25:43.90642...	Malware_Build_Week_U3...	1552	RegCloseKey	HKLM\SOFT\	

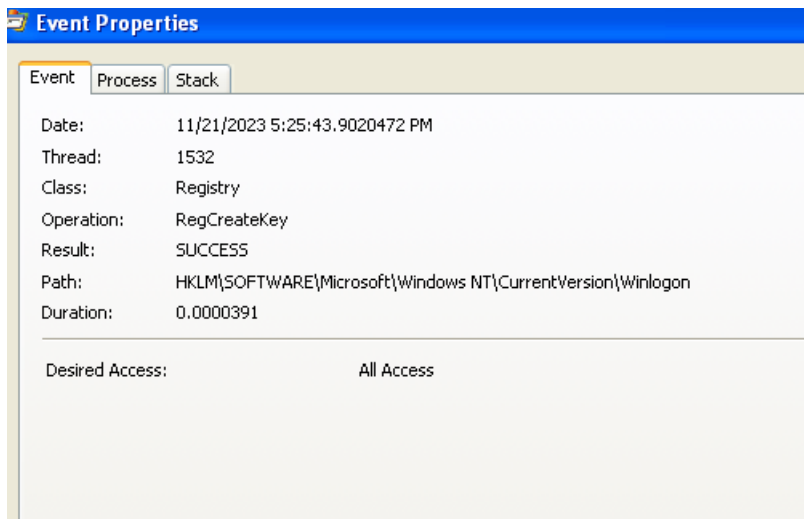
RegOpenKey: usa la maschera di accesso di sicurezza predefinita per aprire una chiave;

RegQueryKey: Recupera informazioni sulla chiave del Registro di sistema specificata;

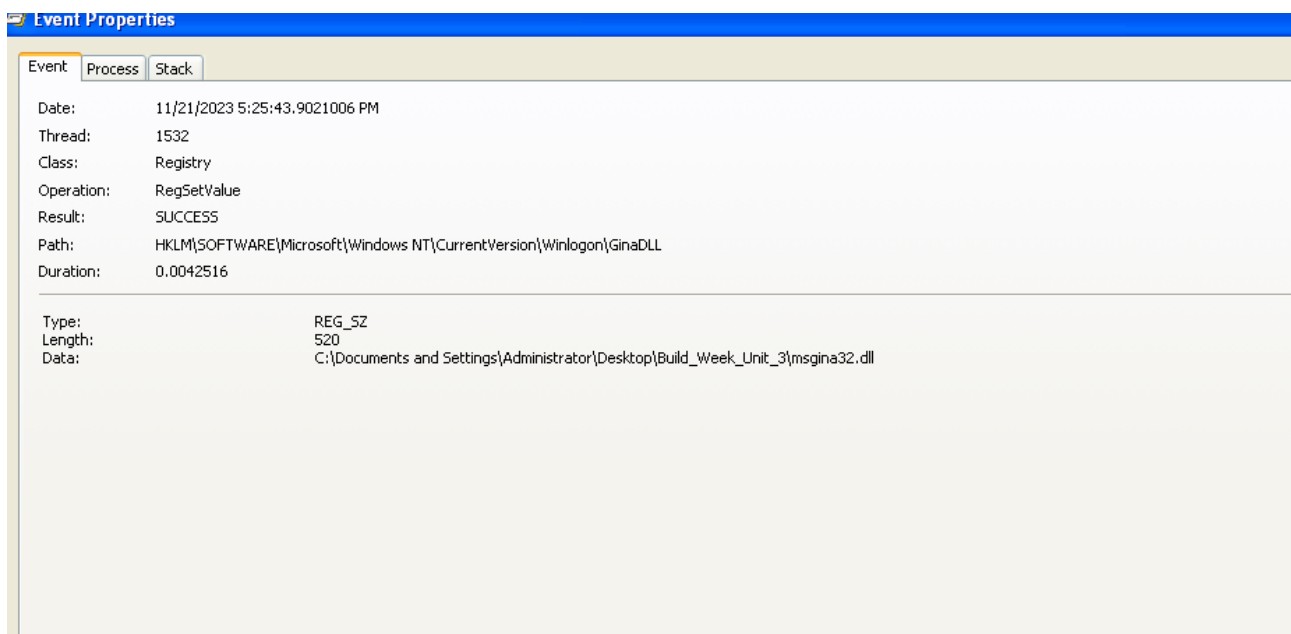
RegCloseKey: Chiude un handle alla chiave del Registro di sistema specificata;

RegSetKey: Imposta i dati per il valore specificato nella chiave e nella sottochiave del Registro di sistema specificati.

RegQueryValue: Recupera il tipo e i dati per un nome valore specificato associato a una chiave del Registro di sistema aperta.



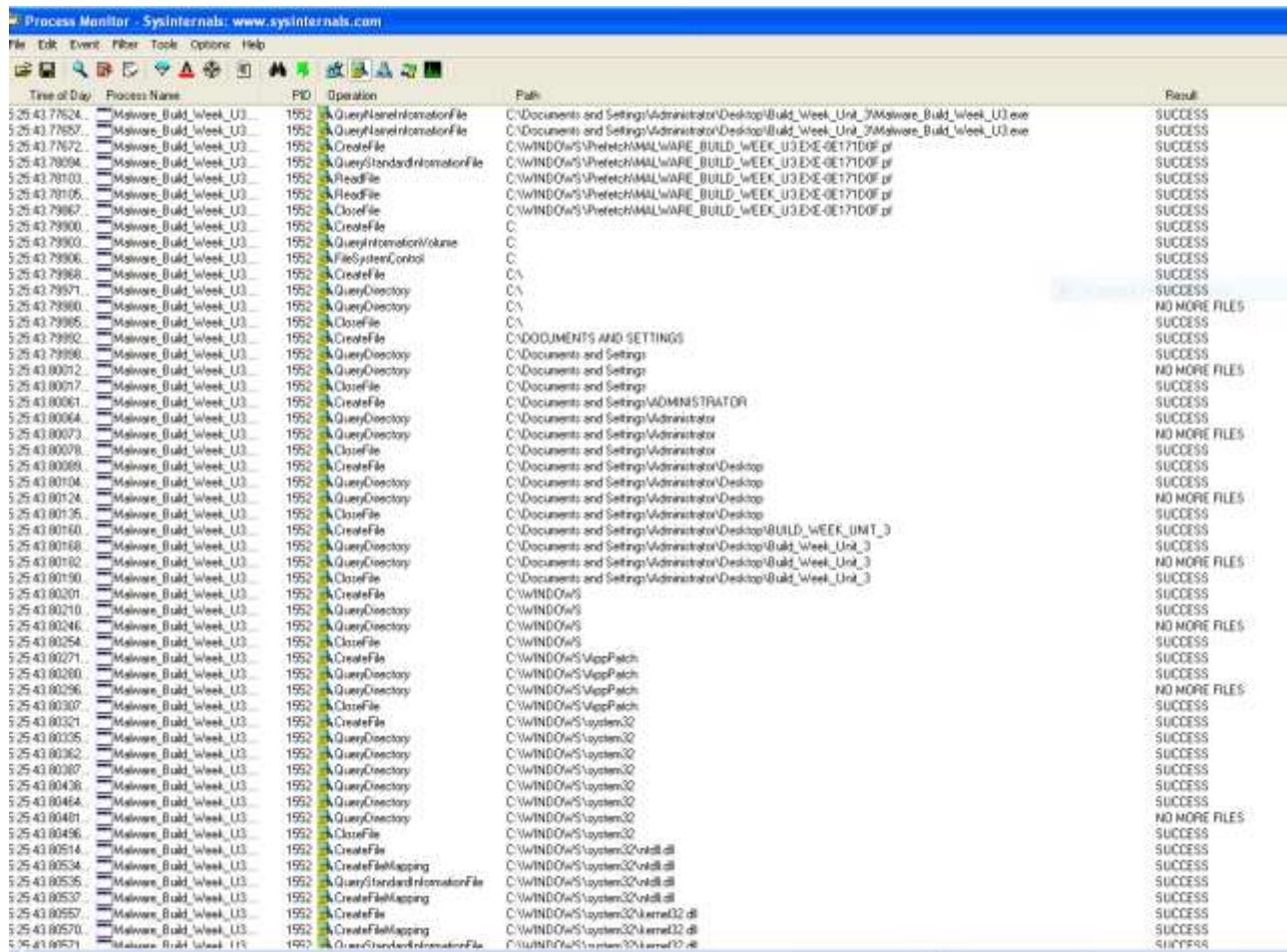
Dunque il malware ha aperto la chiave di registro del path
HKLM/SOFTWARE/Microsoft/Windows
NT/CurrentVersion/Winlogon
che si riferisce all'accesso automatico.



E ha inserito il valore GinaDLL.

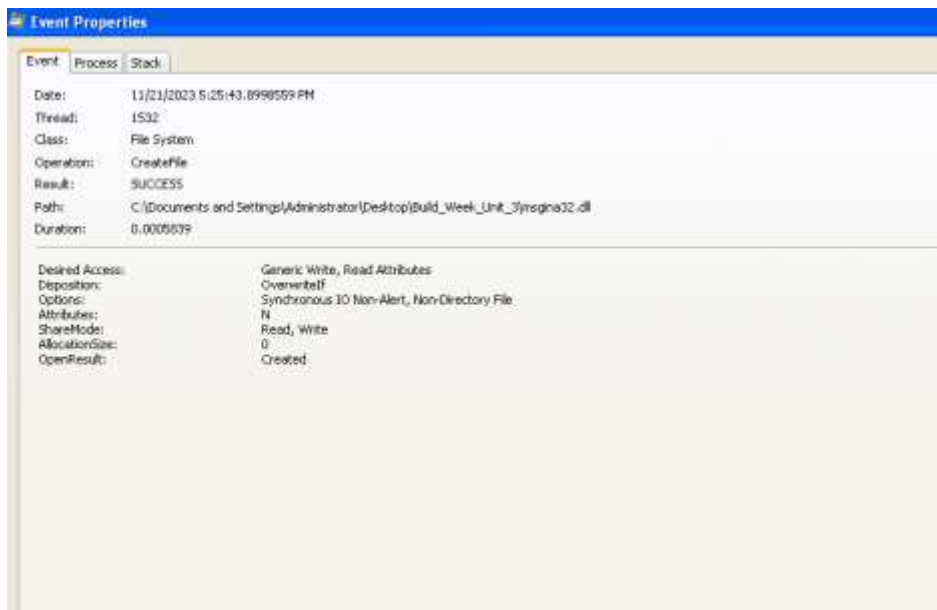
Per quanto riguarda il File System

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



Time of Day	Process Name	PID	Operation	Path	Result
0:25:43.77624	Malware_Bulk_Week_Unit_3	1552	QueryNameInformationFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\Malware_Bulk_Week_Unit_3.exe	SUCCESS
0:25:43.77657	Malware_Bulk_Week_Unit_3	1552	QueryNameInformationFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\Malware_Bulk_Week_Unit_3.exe	SUCCESS
0:25:43.77672	Malware_Bulk_Week_Unit_3	1552	CreateFile	C:\Windows\Shell\MALWARE_BUILD_WEEK_UNIT_3\GET17DOF.pl	SUCCESS
0:25:43.78094	Malware_Bulk_Week_Unit_3	1552	QueryStandardInformationFile	C:\Windows\Shell\MALWARE_BUILD_WEEK_UNIT_3\GET17DOF.pl	SUCCESS
0:25:43.78103	Malware_Bulk_Week_Unit_3	1552	ReadFile	C:\Windows\Shell\MALWARE_BUILD_WEEK_UNIT_3\GET17DOF.pl	SUCCESS
0:25:43.78105	Malware_Bulk_Week_Unit_3	1552	ReadFile	C:\Windows\Shell\MALWARE_BUILD_WEEK_UNIT_3\GET17DOF.pl	SUCCESS
0:25:43.78667	Malware_Bulk_Week_Unit_3	1552	CreateFile	C:\Windows\Shell\MALWARE_BUILD_WEEK_UNIT_3\GET17DOF.pl	SUCCESS
0:25:43.79300	Malware_Bulk_Week_Unit_3	1552	CreateFile	C:	SUCCESS
0:25:43.79303	Malware_Bulk_Week_Unit_3	1552	QueryInformationVolume	C:	SUCCESS
0:25:43.79306	Malware_Bulk_Week_Unit_3	1552	FileSystemControl	C:	SUCCESS
0:25:43.79368	Malware_Bulk_Week_Unit_3	1552	CreateFile	C:\	SUCCESS
0:25:43.79371	Malware_Bulk_Week_Unit_3	1552	QueryDirectory	C:\	SUCCESS
0:25:43.79380	Malware_Bulk_Week_Unit_3	1552	QueryDirectory	C:\	NO MORE FILES
0:25:43.79385	Malware_Bulk_Week_Unit_3	1552	CreateFile	C:\	SUCCESS
0:25:43.79392	Malware_Bulk_Week_Unit_3	1552	CreateFile	C:\DOCUMENTS AND SETTINGS	SUCCESS
0:25:43.79398	Malware_Bulk_Week_Unit_3	1552	QueryDirectory	C:\Documents and Settings	SUCCESS
0:25:43.80012	Malware_Bulk_Week_Unit_3	1552	QueryDirectory	C:\Documents and Settings	NO MORE FILES
0:25:43.80017	Malware_Bulk_Week_Unit_3	1552	CreateFile	C:\Documents and Settings	SUCCESS
0:25:43.80061	Malware_Bulk_Week_Unit_3	1552	CreateFile	C:\Documents and Settings\ADMINISTRATOR	SUCCESS
0:25:43.80064	Malware_Bulk_Week_Unit_3	1552	QueryDirectory	C:\Documents and Settings\Administrator	SUCCESS
0:25:43.80073	Malware_Bulk_Week_Unit_3	1552	QueryDirectory	C:\Documents and Settings\Administrator	NO MORE FILES
0:25:43.80078	Malware_Bulk_Week_Unit_3	1552	CreateFile	C:\Documents and Settings\Administrator	SUCCESS
0:25:43.80089	Malware_Bulk_Week_Unit_3	1552	CreateFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS
0:25:43.80104	Malware_Bulk_Week_Unit_3	1552	QueryDirectory	C:\Documents and Settings\Administrator\Desktop	SUCCESS
0:25:43.80124	Malware_Bulk_Week_Unit_3	1552	QueryDirectory	C:\Documents and Settings\Administrator\Desktop	NO MORE FILES
0:25:43.80135	Malware_Bulk_Week_Unit_3	1552	CreateFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS
0:25:43.80160	Malware_Bulk_Week_Unit_3	1552	CreateFile	C:\Documents and Settings\Administrator\Desktop\BUILD_WEEK_UNIT_3	SUCCESS
0:25:43.80168	Malware_Bulk_Week_Unit_3	1552	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3	SUCCESS
0:25:43.80182	Malware_Bulk_Week_Unit_3	1552	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3	NO MORE FILES
0:25:43.80190	Malware_Bulk_Week_Unit_3	1552	CreateFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3	SUCCESS
0:25:43.80201	Malware_Bulk_Week_Unit_3	1552	CreateFile	C:\Windows	SUCCESS
0:25:43.80210	Malware_Bulk_Week_Unit_3	1552	QueryDirectory	C:\Windows	SUCCESS
0:25:43.80246	Malware_Bulk_Week_Unit_3	1552	QueryDirectory	C:\Windows	NO MORE FILES
0:25:43.80254	Malware_Bulk_Week_Unit_3	1552	CreateFile	C:\Windows	SUCCESS
0:25:43.80271	Malware_Bulk_Week_Unit_3	1552	CreateFile	C:\Windows\MsgPatch	SUCCESS
0:25:43.80280	Malware_Bulk_Week_Unit_3	1552	QueryDirectory	C:\Windows\MsgPatch	SUCCESS
0:25:43.80296	Malware_Bulk_Week_Unit_3	1552	QueryDirectory	C:\Windows\MsgPatch	NO MORE FILES
0:25:43.80307	Malware_Bulk_Week_Unit_3	1552	CreateFile	C:\Windows\MsgPatch	SUCCESS
0:25:43.80321	Malware_Bulk_Week_Unit_3	1552	CreateFile	C:\Windows\System32	SUCCESS
0:25:43.80335	Malware_Bulk_Week_Unit_3	1552	QueryDirectory	C:\Windows\System32	SUCCESS
0:25:43.80362	Malware_Bulk_Week_Unit_3	1552	QueryDirectory	C:\Windows\System32	SUCCESS
0:25:43.80387	Malware_Bulk_Week_Unit_3	1552	QueryDirectory	C:\Windows\System32	SUCCESS
0:25:43.80436	Malware_Bulk_Week_Unit_3	1552	QueryDirectory	C:\Windows\System32	SUCCESS
0:25:43.80464	Malware_Bulk_Week_Unit_3	1552	QueryDirectory	C:\Windows\System32	SUCCESS
0:25:43.80481	Malware_Bulk_Week_Unit_3	1552	QueryDirectory	C:\Windows\System32	NO MORE FILES
0:25:43.80496	Malware_Bulk_Week_Unit_3	1552	CreateFile	C:\Windows\System32	SUCCESS
0:25:43.80514	Malware_Bulk_Week_Unit_3	1552	CreateFile	C:\Windows\System32\cmd.dll	SUCCESS
0:25:43.80534	Malware_Bulk_Week_Unit_3	1552	CreateFile	C:\Windows\System32\cmd.dll	SUCCESS
0:25:43.80535	Malware_Bulk_Week_Unit_3	1552	QueryStandardInformationFile	C:\Windows\System32\cmd.dll	SUCCESS
0:25:43.80537	Malware_Bulk_Week_Unit_3	1552	CreateFile	C:\Windows\System32\cmd.dll	SUCCESS
0:25:43.80557	Malware_Bulk_Week_Unit_3	1552	CreateFile	C:\Windows\System32\kernel32.dll	SUCCESS
0:25:43.80570	Malware_Bulk_Week_Unit_3	1552	CreateFile	C:\Windows\System32\kernel32.dll	SUCCESS
0:25:43.80571	Malware_Bulk_Week_Unit_3	1552	CreateFile	C:\Windows\System32\kernel32.dll	SUCCESS

Attraverso la funzione CreateFile è stato creato il file msgina.dll



FUNZIONAMENTO DEL MALWARE

Il malware in oggetto ha creato, attraverso le varie funzioni esaminate su, la chiave di registro GinaDLL, all'interno del path relativo all'avvio automatico, così facendo può ottenere l'accesso e compromettere il sistema.