

# Analisi Malware

## Tool usati:

- IDA Pro Free 5.0
- CFF Explorer VIII
- OllyDBG 1.10
- Process Monitor

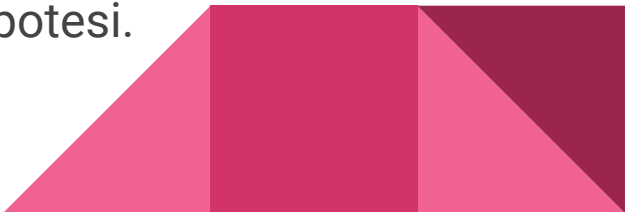
# Build week

Giorno 1

10.10.22

# Traccia

In questa Buildweek per il primo giorno ci viene chiesto di analizzare il Malware che si trova nella cartella `Malware_Build_Week_U3` rispondendo alle seguenti domande:

1. Quanti parametri sono passati alla funzione `Main()`
  2. Quante variabili sono dichiarate dentro la funzione `Main()`
  3. Quali sezioni sono presenti all'interno del malware descrivendo brevemente almeno due di quelle presenti.
  4. Quali librerie sono presenti all'interno del malware e per ognuna di esse fare delle ipotesi in base all'analisi statica sulle funzionalità del malware, utilizzare le funzioni all'interno delle librerie per supportare le ipotesi.
- 

# 1-2.Parametri e variabili funzione Main()

```
; Attributes: bp-based frame
```

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

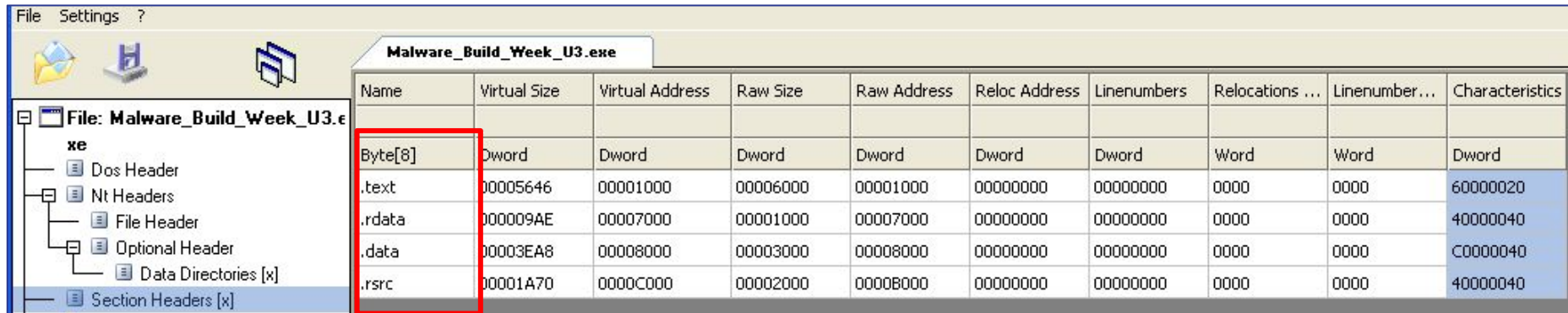
hModule= dword ptr -11Ch	variabile
Data= byte ptr -118h	variabile
var_8= dword ptr -8	variabile
var_4= dword ptr -4	variabile
argc= dword ptr 8	parametro
argv= dword ptr 0Ch	parametro
envp= dword ptr 10h	parametro

I **parametri** passati nella funzione Main() sono 3 (**argc**= dword ptr 8, **argv**=dword ptr 0Ch, **envp**= dword ptr 10h)

Le **variabili** dichiarate nella funzione Main() sono 4 (**hModule**= dword ptr -11Ch, **Data**=byte ptr -118h,**var\_8**=dword ptr -8, **var\_4**= dword ptr -4)

Possiamo distinguere le variabili dai parametri perchè le variabili hanno un valore negativo rispetto ad **EBP** (Extended **B**ased **P**ointer) mentre i parametri hanno valore positivo.

### 3. Sezioni presenti nel file eseguibile e descriverle



Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations ...	Linenumber...	Characteristics
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

### 3.

Le sezioni che compongono il malware sono “.text, .rdata, .data, .rsrc”

- **.text**: Questa sezione contiene le righe di codice e le variabili statiche, quindi le istruzioni che la CPU andrà ad eseguire una volta che il software verrà avviato.
- **.rdata**: Questa sezione contiene le informazioni delle librerie e le varie funzioni esportate e importate dal malware.
- **.data**: Questa sezione contiene le variabili globali e i dati del malware che devono essere disponibili da qualsiasi parte del programma
- **.rsrc**: Include le risorse utilizzate dal malware come ad esempio icone, immagini, menù e stringhe che non fanno parte del malware stesso.



## 4. Librerie importate dal Malware

File Settings ?

File: Malware\_Build\_Week\_U3.exe

- File: Malware\_Build\_Week\_U3.exe
  - Dos Header
  - Nt Headers
    - File Header
    - Optional Header
      - Data Directories [x]
  - Section Headers [x]
  - Import Directory

**Malware\_Build\_Week\_U3.exe**

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	51	00007534	00000000	00000000	0000769E	0000700C
ADVAPI32.dll	2	00007528	00000000	00000000	000076D0	00007000

## 4.KERNEL32.dll (Ipotesi)

Le librerie importate dal Malware in questo caso sono:

- **KERNEL32.dll** contiene le funzioni principali per interagire con il sistema operativo, come la gestione della memoria e la manipolazione dei file.

**Ipotesi:** Potrebbe trattarsi di un **dropper** perchè queste funzioni permettono di localizzare il malware ed estrarlo e successivamente caricarlo in memoria per eseguirlo. C'è anche la possibilità di salvarlo sul disco per un'esecuzione futura.

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



## 4. ADVAPI.dll (Ipotesi)

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

- **ADVAPI32.dll** contiene le funzioni per interagire con i servizi ed i registri del sistema operativo di Microsoft

**Ipotesi:** Con queste funzioni il malware tenta di cambiare i valori dei registri Windows per ottenere la persistenza

# Build week

Giorno 2

11.10.22

Con riferimento al Malware in analisi, spiegare:

1. Lo scopo della funzione chiamata alla locazione di memoria 00401021
2. Come vengono passati i parametri alla funzione alla locazione 00401021;
3. Che oggetto rappresenta il parametro alla locazione 00401017
4. Il significato delle istruzioni comprese tra gli indirizzi 00401027 e 00401029.
5. Con riferimento all'ultimo quesito, tradurre il codice Assembly nel corrispondente costruito C.
6. Valutate ora la chiamata alla locazione 00401047, qual è il valore del parametro «ValueName»?

Nel complesso delle due funzionalità appena viste, spiegate quale funzionalità sta implementando il Malware in questa sezione.



## 1/2- Scopo e parametri funzione

Lo scopo della funzione chiamata alla locazione di memoria **00401021** serve per creare una nuova chiave di registro. I parametri vengono passati alla funzione tramite i “**push**”.

```
.text:00401000      push    ebp
.text:00401001      mov     ebp, esp
.text:00401003      push    ecx
.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\\Windows NT\\CurrentVe"...
.text:0040101C      push    80000002h   ; hKey
.text:00401021      call    ds:RegCreateKeyExA
```

### 3- Oggetto rappresentato

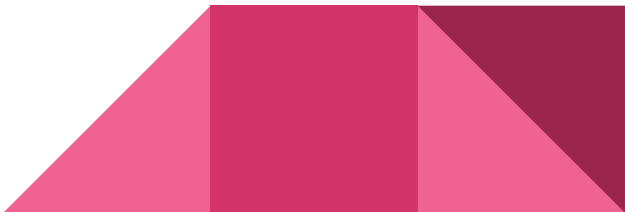
```
.text:00401000      push     ebp
.text:00401001      mov      ebp, esp
.text:00401003      push     ecx
.text:00401004      push     0                ; lpdwDisposition
.text:00401006      lea      eax, [ebp+hObject]
.text:00401009      push     eax                ; phkResult
.text:0040100A      push     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\\Windows NT\\CurrentVe"...
.text:0040101C      push     80000002h         ; hKey
.text:00401021      call     ds:RegCreateKeyExA
```

L'oggetto rappresenta la chiave del malware per ottenere la persistenza su un sistema operativo Windows

## 4- Significato istruzioni

<code>.text:00401027</code>	<code>test</code>	<code>eax, eax</code>
<code>.text:00401029</code>	<code>jz</code>	<code>short loc_401032</code>

Test è simile all' "AND", con la differenza che non modifica il contenuto degli operandi, ma bensì modifica lo **zf** (zero flag), che viene settato a 1 solo se il risultato dell' "AND" è 0, essendo che viene eseguito il confronto con se stessa, lo zf sarà sempre 1. Mentre jz è un salto condizionato, che viene eseguito solo se lo zf è 1, quindi in questo caso il salto viene eseguito.



## 5- Linguaggio C

A questo punto ci viene chiesto di tradurre il precedente codice Assembly in Linguaggio C.

Nella figura a lato possiamo vedere la nostra proposta di codice: dato che viene effettuato un salto condizionale in Assembly. Nel linguaggio C abbiamo tradotto questo salto con un “**if**”, quindi:

Se “**EAX**” è **uguale** a 0, **esegue il jz**, altrimenti non entra nel ciclo.

```
.text:00401027      test     eax, eax
.text:00401029      jz       short loc_401032
```



```
1  #include <stdio.h>
2  #include <stdlib.h>
3
4  int main()
5  {
6      int a;
7      if (a==0)
8      {
9          printf("jz 401032");
10
11         return 0;
12     }
13 }
```

## 6-ValueName

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

Come possiamo notare dall'immagine il valore del parametro "**ValueName**" è "**GinaDLL**".

Le funzioni che abbiamo analizzato prima ci possono confermare che il malware tenta di ottenere la **persistenza** tramite la modifica dei registri Windows



# Build week

Giorno 3

12.10.22

Il compito di oggi ci chiedeva di analizzare la routine tra le locazioni di memoria **00401080** e **00401128** rispondendo a questi quesiti:

- Valore del parametro “ResourceName” passato dalla funzione FindResource()
- Che funzionalità implementa il Malware
- Identificare questa funzione con una analisi statica
- Se sì, elencare le evidenze a supporto
- Disegnare un diagramma di flusso che comprende le 3 funzioni



# 1-Valore parametro

004010BD	. 50	PUSH EAX	[ResourceType => "BINARY" Malware_.00408038 ResourceName => "TGAD"  hModule FindResourceA
004010BE	. 8B0D 34804000	MOV ECX,DWORD PTR DS:[408034]	
004010C4	. 51	PUSH ECX	
004010C5	. 8B55 08	MOV EDX,DWORD PTR SS:[EBP+8]	
004010C8	. 52	PUSH EDX	
004010C9	. FF15 28704000	CALL DWORD PTR DS:[<&KERNEL32.FindResou	

Come possiamo vedere dalle immagini il valore che viene passato al parametro ResourceName è **"TGAD"**

## 2- Funzionalità del Malware

00401080	55	PUSH EBP	
00401081	8BEC	MOV EBP,ESP	
00401083	83EC 18	SUB ESP,18	
00401086	56	PUSH ESI	
00401087	57	PUSH EDI	
00401088	C745 EC 000000	MOV DWORD PTR SS:[EBP-14],0	
0040108F	C745 E8 000000	MOV DWORD PTR SS:[EBP-18],0	
00401096	C745 F8 000000	MOV DWORD PTR SS:[EBP-8],0	
0040109D	C745 F0 000000	MOV DWORD PTR SS:[EBP-10],0	
004010A4	C745 F4 000000	MOV DWORD PTR SS:[EBP-C],0	
004010AB	837D 08 00	CMP DWORD PTR SS:[EBP+8],0	
004010AF	75 07	JNZ SHORT Malware_.004010B8	
004010B1	33C0	XOR EAX,EAX	
004010B3	E9 07010000	JMP Malware_.004011BF	
004010B8	> A1 30804000	MOV EAX,DWORD PTR DS:[408030]	ResourceType => "BINARY"
004010BD	50	PUSH EAX	Malware_.00408038
004010BE	8B0D 34804000	MOV ECX,DWORD PTR DS:[408034]	ResourceName => "TGAD"
004010C4	51	PUSH ECX	hModule
004010C5	8B55 08	MOV EDX,DWORD PTR SS:[EBP+8]	FindResourceA
004010C8	52	PUSH EDX	
004010C9	FF15 28704000	CALL DWORD PTR DS:[<&KERNEL32.FindResou	
004010CF	8945 EC	MOV DWORD PTR SS:[EBP-14],EAX	
004010D2	837D EC 00	CMP DWORD PTR SS:[EBP-14],0	
004010D6	75 07	JNZ SHORT Malware_.004010DF	
004010D8	33C0	XOR EAX,EAX	
004010DA	E9 E0000000	JMP Malware_.004011BF	
004010DF	> 8B45 EC	MOV EAX,DWORD PTR SS:[EBP-14]	hResource
004010E2	50	PUSH EAX	
004010E3	8B4D 08	MOV ECX,DWORD PTR SS:[EBP+8]	hModule
004010E6	51	PUSH ECX	LoadResource
004010E7	FF15 14704000	CALL DWORD PTR DS:[<&KERNEL32.LoadResou	
004010ED	8945 E8	MOV DWORD PTR SS:[EBP-18],EAX	
004010F0	837D E8 00	CMP DWORD PTR SS:[EBP-18],0	
004010F4	75 05	JNZ SHORT Malware_.004010FB	
004010F6	E9 A0000000	JMP Malware_.004011A5	
004010FB	> 8B55 E8	MOV EDX,DWORD PTR SS:[EBP-18]	nHandles
004010FE	52	PUSH EDX	SetHandleCount
004010FF	FF15 10704000	CALL DWORD PTR DS:[<&KERNEL32.LockResou	
00401105	8945 F8	MOV DWORD PTR SS:[EBP-8],EAX	
00401108	837D F8 00	CMP DWORD PTR SS:[EBP-8],0	
0040110C	75 05	JNZ SHORT Malware_.00401113	
0040110E	E9 92000000	JMP Malware_.004011A5	
00401113	> 8B45 EC	MOV EAX,DWORD PTR SS:[EBP-14]	hResource
00401116	50	PUSH EAX	
00401117	8B4D 08	MOV ECX,DWORD PTR SS:[EBP+8]	hModule
0040111A	51	PUSH ECX	SizeofResource
0040111B	FF15 0C704000	CALL DWORD PTR DS:[<&KERNEL32.SizeofRes	
00401121	8945 F0	MOV DWORD PTR SS:[EBP-10],EAX	
00401124	837D F0 00	CMP DWORD PTR SS:[EBP-10],0	
00401126	77 02	JG SHORT Malware_.0040112C	

Come abbiamo visto queste sono le funzionalità importate dal dropper:

- **FindResourceA**: Viene usata per localizzare il malware da estrarre.
- **LoadResource**: Viene usato per caricare in memoria il malware per una esecuzione o salvato per una esecuzione futura.
- **LockResource**: Viene usato per recuperare un puntatore all'indirizzo di memoria.
- **SizeOfResource**: Viene usato per recuperare le dimensioni della risorsa specificata.

## ¾ - Identificazione

Come mostrato in figura è possibile identificare queste funzionalità anche solo con **l'analisi statica basica**

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

# -Diagramma



# Build week

Giorno 4

13.10.22

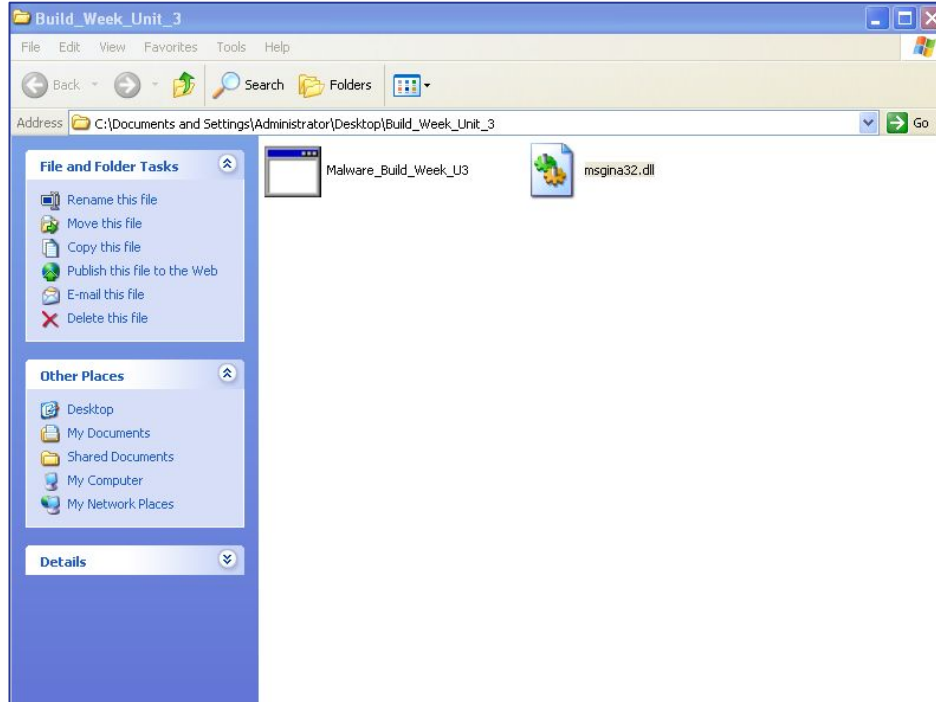
La traccia di oggi ci chiedeva di:

1. Cosa notate dentro la cartella dov'è situato il file eseguibile: Spiegare cosa è avvenuto.
2. Analizzare i risultati di Process Monitor
3. Quale chiave viene creata e quale valore viene associato alla chiave di registro che è stata creata
4. Quale chiamata di sistema ha modificato il contenuto della cartella dove è presente il file eseguibile del malware
5. Unite tutte le informazioni per delineare il funzionamento del malware





# 1- Esecuzione e spiegazione Malware



Come possiamo notare dalla figura, aprendo la cartella del malware, una volta eseguito, viene creato il file “**msgina32.dll**”. Questo perché la funzione del **dropper** è quella di scaricare un file.

# 2- Process Monitor

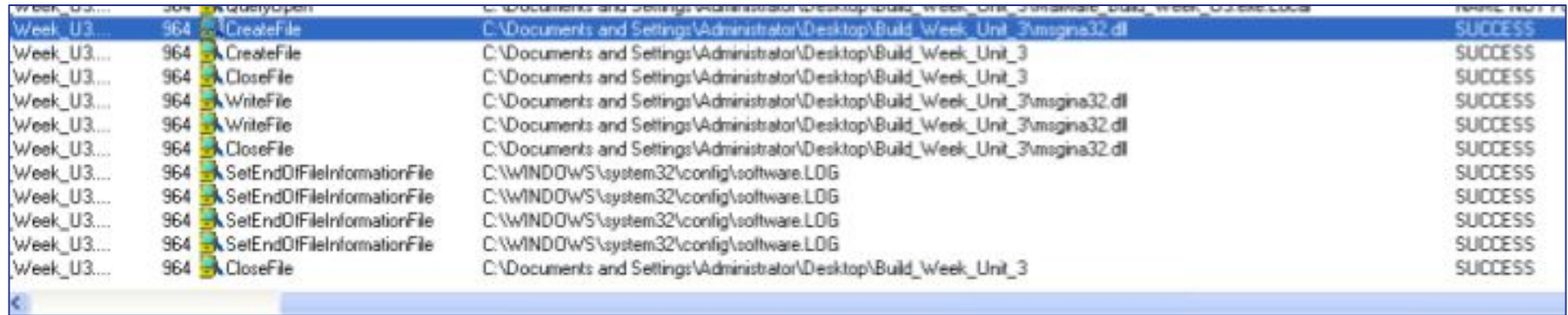
Process Monitor - Sysinternals: www.sysinternals.com						
Time of Day	Process Name	PID	Operation	Path	Result	Detail
9:17:36.50192	Malware_Build_Week_U3...	964	Process Start		SUCCESS	Parent PID: 2040, Command line: "C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\Malware_Build_Week_U3.exe"
9:17:36.50193	Malware_Build_Week_U3...	964	Thread Create		SUCCESS	Thread ID: 236
9:17:36.50206	Malware_Build_Week_U3...	964	QueryNameInformationFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\Malware_Build_Week_U3.exe	SUCCESS	Name: Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\Malware_Build_Week_U3.exe
9:17:36.50301	Malware_Build_Week_U3...	964	Load Image	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\Malware_Build_Week_U3.exe	SUCCESS	Image Base: 0x400000, Image Size: 0x0000
9:17:36.50319	Malware_Build_Week_U3...	964	Load Image	C:\WINDOWS\system32\ntldr.dll	SUCCESS	Image Base: 0x7c900000, Image Size: 0x0000
9:17:36.50320	Malware_Build_Week_U3...	964	QueryNameInformationFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\Malware_Build_Week_U3.exe	SUCCESS	Name: Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\Malware_Build_Week_U3.exe
9:17:36.50332	Malware_Build_Week_U3...	964	CreateFile	C:\WINDOWS\Prefetch\MALWARE_BUILD_WEEK_U3.DX-E-0E171D0F.pf	SUCCESS	Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Attributes: n/a, ShareMode: None, AllocationSize: n/a
9:17:36.50708	Malware_Build_Week_U3...	964	QueryStandardInformationFile	C:\WINDOWS\Prefetch\MALWARE_BUILD_WEEK_U3.DX-E-0E171D0F.pf	SUCCESS	AllocationSize: 12,288, EndOfFile: 10,856, NumberOfLinks: 1, DeletePending: False, Directory: False
9:17:36.50716	Malware_Build_Week_U3...	964	ReadFile	C:\WINDOWS\Prefetch\MALWARE_BUILD_WEEK_U3.DX-E-0E171D0F.pf	SUCCESS	Offset: 0, Length: 10,856
9:17:36.50718	Malware_Build_Week_U3...	964	ReadFile	C:\WINDOWS\Prefetch\MALWARE_BUILD_WEEK_U3.DX-E-0E171D0F.pf	SUCCESS	Offset: 0, Length: 10,856, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O
9:17:36.50784	Malware_Build_Week_U3...	964	CloseFile	C:\WINDOWS\Prefetch\MALWARE_BUILD_WEEK_U3.DX-E-0E171D0F.pf	SUCCESS	
9:17:36.50834	Malware_Build_Week_U3...	964	CreateFile	C:\	SUCCESS	Desired Access: Read Attributes, Write Attributes, Synchronize, Disposition: Open, Options: Synchronous IO Non-Alert, Attributes: n/a, Share
9:17:36.50836	Malware_Build_Week_U3...	964	QueryInformationVolume	C:\	SUCCESS	VolumeCreationTime: 3/20/2017 10:34:16 PM, VolumeSerialNumber: D98A-8021, SupportsObjects: True, VolumeLabel:
9:17:36.50938	Malware_Build_Week_U3...	964	FileSystemControl	C:\	SUCCESS	Control: FSCTL_FILE_PREFETCH
9:17:36.50975	Malware_Build_Week_U3...	964	CreateFile	C:\	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup
9:17:36.50977	Malware_Build_Week_U3...	964	QueryDirectory	C:\	SUCCESS	0: 65e5bdf5ca391440390554e9a7b7, 1: AUTOEXEC.BAT, FileInformationClass: FileNamesInformation, 3: CONFIG.SYS, 4: Documents and
9:17:36.51057	Malware_Build_Week_U3...	964	QueryDirectory	C:\	NO MORE FILES	
9:17:36.51061	Malware_Build_Week_U3...	964	CloseFile	C:\	SUCCESS	
9:17:36.51067	Malware_Build_Week_U3...	964	CreateFile	C:\DOCUMENTS AND SETTINGS	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup
9:17:36.51071	Malware_Build_Week_U3...	964	QueryDirectory	C:\Documents and Settings	SUCCESS	0: ., 1: ., FileInformationClass: FileNamesInformation, 3: All Users, 4: Default User, 5: LocalService, 6: NetworkService
9:17:36.51075	Malware_Build_Week_U3...	964	QueryDirectory	C:\Documents and Settings	NO MORE FILES	
9:17:36.51079	Malware_Build_Week_U3...	964	CloseFile	C:\Documents and Settings	SUCCESS	
9:17:36.51112	Malware_Build_Week_U3...	964	CreateFile	C:\Documents and Settings\ADMINISTRATOR	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup
9:17:36.51115	Malware_Build_Week_U3...	964	QueryDirectory	C:\Documents and Settings\Administrator	SUCCESS	0: ., 1: ., FileInformationClass: FileNamesInformation, 3: Cookies, 4: Desktop, 5: Favorites, 6: Local Settings, 7: My Documents, 8: NetHood,
9:17:36.51121	Malware_Build_Week_U3...	964	QueryDirectory	C:\Documents and Settings\Administrator	NO MORE FILES	
9:17:36.51125	Malware_Build_Week_U3...	964	CloseFile	C:\Documents and Settings\Administrator	SUCCESS	
9:17:36.51133	Malware_Build_Week_U3...	964	CreateFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup
9:17:36.51141	Malware_Build_Week_U3...	964	QueryDirectory	C:\Documents and Settings\Administrator\Desktop	SUCCESS	0: ., 1: ., FileInformationClass: FileNamesInformation, 3: CFF Explorer.lnk, 4: Command Prompt.lnk, 5: Exerciso_Pratico_U3_W2_L1, 6: Exerc
9:17:36.51148	Malware_Build_Week_U3...	964	QueryDirectory	C:\Documents and Settings\Administrator\Desktop	NO MORE FILES	
9:17:36.51155	Malware_Build_Week_U3...	964	CloseFile	C:\Documents and Settings\Administrator\Desktop	SUCCESS	
9:17:36.51165	Malware_Build_Week_U3...	964	CreateFile	C:\Documents and Settings\Administrator\Desktop\BUILD_WEEK_UNIT_3	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup
9:17:36.51171	Malware_Build_Week_U3...	964	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3	SUCCESS	0: ., 1: ., FileInformationClass: FileNamesInformation
9:17:36.51181	Malware_Build_Week_U3...	964	QueryDirectory	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3	NO MORE FILES	
9:17:36.51187	Malware_Build_Week_U3...	964	CloseFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3	SUCCESS	
9:17:36.51195	Malware_Build_Week_U3...	964	CreateFile	C:\WINDOWS	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup
9:17:36.51202	Malware_Build_Week_U3...	964	QueryDirectory	C:\WINDOWS	SUCCESS	0: ., 1: ., FileInformationClass: FileNamesInformation, 3: 0.log, 4: addins, 5: AppPatch, 6: assembly, 7: Blue Lace 16.bmp, 8: bootdata.dat, 9: c
9:17:36.51221	Malware_Build_Week_U3...	964	QueryDirectory	C:\WINDOWS	NO MORE FILES	
9:17:36.51227	Malware_Build_Week_U3...	964	CloseFile	C:\WINDOWS	SUCCESS	
9:17:36.51241	Malware_Build_Week_U3...	964	CreateFile	C:\WINDOWS\AppPatch	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup
9:17:36.51249	Malware_Build_Week_U3...	964	QueryDirectory	C:\WINDOWS\AppPatch	SUCCESS	0: ., 1: ., FileInformationClass: FileNamesInformation, 3: AcGeneral.dll, 4: AclLayers.dll, 5: AclLsa.dll, 6: AcSpect.dll, 7: AcTol.dll, 8: apphe
9:17:36.51264	Malware_Build_Week_U3...	964	QueryDirectory	C:\WINDOWS\AppPatch	NO MORE FILES	
9:17:36.51273	Malware_Build_Week_U3...	964	CloseFile	C:\WINDOWS\AppPatch	SUCCESS	
9:17:36.51283	Malware_Build_Week_U3...	964	CreateFile	C:\WINDOWS\system32	SUCCESS	Desired Access: Read Data/List Directory, Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup
9:17:36.51307	Malware_Build_Week_U3...	964	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: ., 1: ., FileInformationClass: FileNamesInformation, 3: -1, 4: 1025, 5: 1028, 6: 1031, 7: 1033, 8: 1037, 9: 1041, 10: 1042, 11: 1054, 12: 125
9:17:36.51329	Malware_Build_Week_U3...	964	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: exproc.dll, 1: edit.com, FileInformationClass: FileNamesInformation, 3: edit.exe, 4: efadu.dll, 5: ega.cpi, 6: els.dll, 7: emptyregdb.dat, 8: e
9:17:36.51347	Malware_Build_Week_U3...	964	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: more.com, 1: monicon.dll, FileInformationClass: FileNamesInformation, 3: mouse.drv, 4: mp43dmtd.dll, 5: mp43dmtd.dll, 6: mpeg2data.as
9:17:36.51377	Malware_Build_Week_U3...	964	QueryDirectory	C:\WINDOWS\system32	SUCCESS	0: program.exe, 1: PROMID.dll, FileInformationClass: FileNamesInformation, 3: PR0ID.exe, 4: procy.exe, 5: psapi.dll, 6: psbase.dll, 7:
9:17:36.51419	Malware_Build_Week_U3...	964	QueryDirectory	C:\WINDOWS\system32	NO MORE FILES	0: vjop.dll, 1: vmgtslib.dll, FileInformationClass: FileNamesInformation, 3: vmghs.dll, 4: VMUpgradeStandaloneVSP.dll, 5: vmwsg32.dll
9:17:36.51432	Malware_Build_Week_U3...	964	CloseFile	C:\WINDOWS\system32	SUCCESS	
9:17:36.51448	Malware_Build_Week_U3...	964	CreateFile	C:\WINDOWS\system32\ntldr.dll	SUCCESS	Desired Access: Read Data/List Directory, Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: N, ShareMode: Read,
9:17:36.51468	Malware_Build_Week_U3...	964	CreateFileMapping	C:\WINDOWS\system32\ntldr.dll	SUCCESS	Synctype: SyncTypeCreateSection, PageProtection: PAGE_READWRITE

# 3-Valore e chiave

Process Monitor - Sysinternals: www.sysinternals.com						
File Edit Event Filter Tools Options Help						
Time of Day	Process Name	PID	Operation	Path	Result	Detail
9:17:36.55348	Malware_Build_Week_U3...	964	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Malware_Build_Week_U3.exe	NAME NOT FOUND	Desired Access: Read
9:17:36.55416	Malware_Build_Week_U3...	964	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	Desired Access: Read
9:17:36.55418	Malware_Build_Week_U3...	964	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
9:17:36.55510	Malware_Build_Week_U3...	964	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	
9:17:36.56033	Malware_Build_Week_U3...	964	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	Desired Access: Read
9:17:36.56035	Malware_Build_Week_U3...	964	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
9:17:36.56038	Malware_Build_Week_U3...	964	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	
9:17:36.56041	Malware_Build_Week_U3...	964	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Secu32.dll	NAME NOT FOUND	Desired Access: Read
9:17:36.56044	Malware_Build_Week_U3...	964	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\RPCRT4.dll	NAME NOT FOUND	Desired Access: Read
9:17:36.56046	Malware_Build_Week_U3...	964	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ADVAPI32.dll	NAME NOT FOUND	Desired Access: Read
9:17:36.56048	Malware_Build_Week_U3...	964	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	Desired Access: Read
9:17:36.56049	Malware_Build_Week_U3...	964	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
9:17:36.56051	Malware_Build_Week_U3...	964	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server\TSUserEnabled	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
9:17:36.56053	Malware_Build_Week_U3...	964	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	
9:17:36.56054	Malware_Build_Week_U3...	964	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	Desired Access: Read
9:17:36.56056	Malware_Build_Week_U3...	964	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\LeakTrack	NAME NOT FOUND	Length: 144
9:17:36.56058	Malware_Build_Week_U3...	964	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	
9:17:36.56059	Malware_Build_Week_U3...	964	RegOpenKey	HKLM	SUCCESS	Desired Access: Maximum Allowed
9:17:36.56060	Malware_Build_Week_U3...	964	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Diagnostics	NAME NOT FOUND	Desired Access: Read
9:17:36.56063	Malware_Build_Week_U3...	964	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ntldr.dll	NAME NOT FOUND	Desired Access: Read
9:17:36.56064	Malware_Build_Week_U3...	964	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\kernel32.dll	NAME NOT FOUND	Desired Access: Read
9:17:36.56471	Malware_Build_Week_U3...	964	RegCreateKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	Desired Access: All Access
9:17:36.56474	Malware_Build_Week_U3...	964	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\MsginaDLL	SUCCESS	Type: REG_SZ, Length: 520, Data: C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll
9:17:36.56565	Malware_Build_Week_U3...	964	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	

La chiave che viene creata è visibile tramite l'operazione **“RegCreateKey”**, mentre il suo valore è quello che gli viene assegnato tramite l'operazione **“RegSetValue”** ovvero **msgina32.dll**.

## 4-Chiamata di sistema



Week_U3...	964	CreateFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll	SUCCESS
Week_U3...	964	CreateFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3	SUCCESS
Week_U3...	964	CloseFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3	SUCCESS
Week_U3...	964	WriteFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll	SUCCESS
Week_U3...	964	WriteFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll	SUCCESS
Week_U3...	964	CloseFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3\msgina32.dll	SUCCESS
Week_U3...	964	SetEndOfFileInformationFile	C:\WINDOWS\system32\config\software.LDG	SUCCESS
Week_U3...	964	SetEndOfFileInformationFile	C:\WINDOWS\system32\config\software.LDG	SUCCESS
Week_U3...	964	SetEndOfFileInformationFile	C:\WINDOWS\system32\config\software.LDG	SUCCESS
Week_U3...	964	SetEndOfFileInformationFile	C:\WINDOWS\system32\config\software.LDG	SUCCESS
Week_U3...	964	CloseFile	C:\Documents and Settings\Administrator\Desktop\Build_Week_Unit_3	SUCCESS

Dall'immagine sopra possiamo vedere che la chiamata per la creazione del file all'interno della cartella dov'è presente il malware viene effettuata da **“Create File”** ed il path dov'è presente l'eseguibile.

# 5-Funzione Malware

Come abbiamo visto essendo un dropper lui modifica i registri di Windows per creare questo file chiamato “**msgina32.dll**”

**Gina** è un componente di Windows che permette l'autenticazione tramite interfaccia grafica.

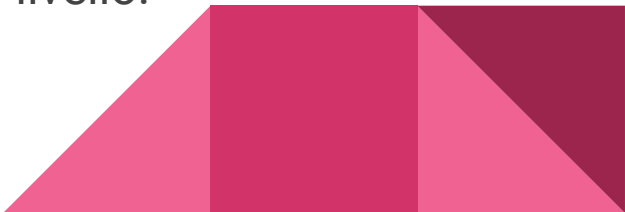


# Build week

Giorno 5

14.10.22

Gina (Graphic authentication & authentication) è un componente lecito di Windows che permette l'autenticazione degli utenti tramite interfaccia grafica. In questo caso permette agli utenti di inserire username e password nel riquadro Windows:

1. Cosa può succedere se il file .dll lecito viene sostituito con il file .dll malevolo che intercetta i dati inseriti?
  2. In base alla risposta delineare il profilo del Malware e le sue funzionalità.
  3. Creare un grafico che ne rappresenti lo scopo ad alto livello.
- 

# 1-Sostituzione del file .dll

Nel caso in cui il malware riuscisse a sostituire il file .dll lecito con uno malevolo, riuscirebbe ad **intercettare le credenziali** (username e password) dell'utente.

Riuscendo così ad **accedere** al computer.

## 2-Funzione malware

Dopo aver analizzato il malware abbiamo visto che il suo scopo, essendo un **dropper**, è quello di **scaricare un file** (msgina32.dll) e **sostituirlo** ad un file lecito.

Inoltre modificando i registri Windows riesce ad ottenere la **persistenza** in modo che al riavvio del computer l'utente non troverà più l'interfaccia grafica lecita ma quella scaricata dal malware riuscendo così ad ottenere le credenziali.





