M6 D8

PROGETTO

MALWARE ANALYSIS

Il Malware da analizzare è nella cartella Build_Week_Unit_3 che troviamo nel desktop della macchina virtuale.

Sarà da analizzare attraverso un' analisi statica ed un' analisi dinamica.

ANALISI STATICA:

1) **Nella funzione Main() vengono passati questi parametri:**

argc (argument count) → è un parametro in posizione 0 (primo parametro) e viene rappresentato da dword ptr 8, occupa 4 byte;

argv (argument vector) → è un parametro in posizione 1 (secondo parametro) e viene rappresentato da dword ptr 0Ch, occupa 4 byte;

envp (environment pointer) → è un parametro in posizione 2 (terzo parametro) e viene rappresentato da dword ptr 10h, ocupa 4 byte.

```
; Attributes: bp-based frame

; 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

push    ebp
mov     ebp, esp
sub     esp, 11Ch
push    ebx
push    esi
push    edi
mov     [ebp+var_4], 0
push    0               ; lpModuleName
call    ds:GetModuleHandleA
```

2) **All' interno della funzione Main() sono dichiarate 4 variabili:**

hModule → è una variabile di tipo dword (4 byte) che viene dichiarata come -11Ch rispetto all' indirizzo della base dello stack (ebp). Occupa 4 byte di spazio nello stack;

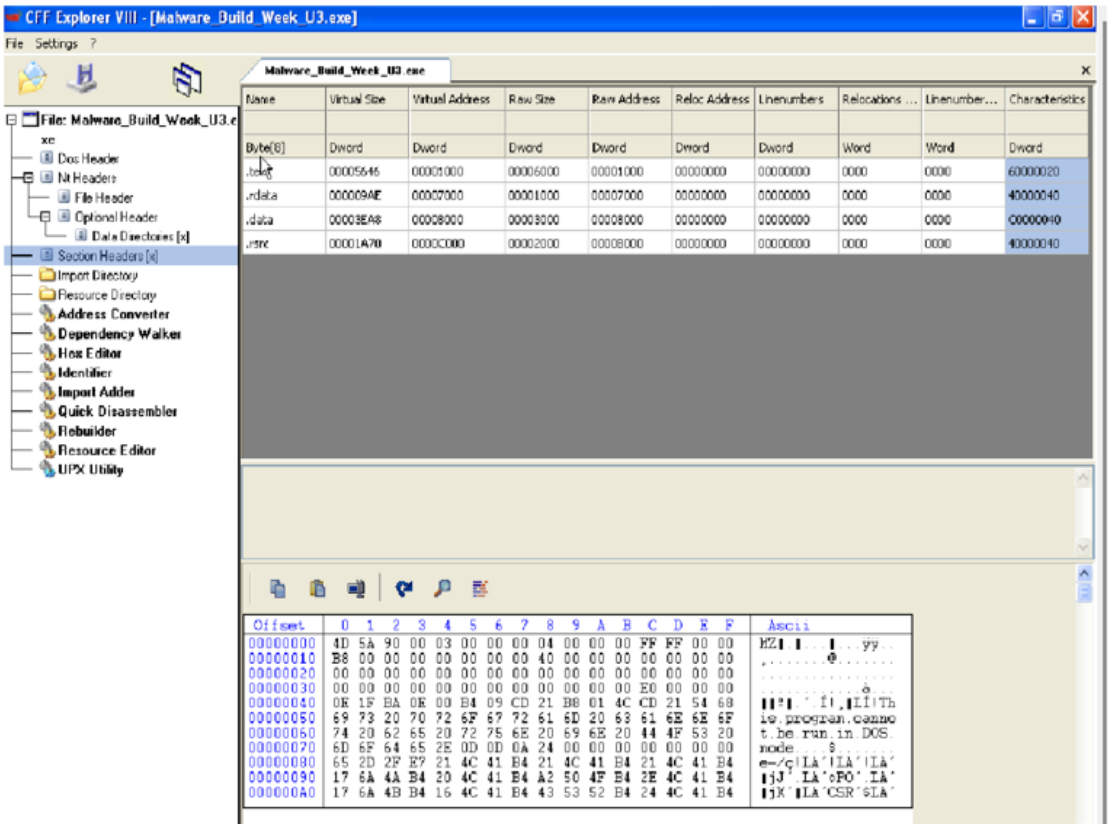
Data → è una variabile di tipo byte (1 byte) che viene dichiarata come -118h rispetto all' indirizzo della base dello stack (ebp). Occupa 1 byte di spazio nello stack;

var_8 → è una variabile di tipo dword (4 byte) che viene dichiarata come -8 rispetto all' indirizzo della base dello stack (ebp). Occupa 4 byte di spazio nello stack;

var_4 → è una variabile di tipo dword (4 byte) che viene dichiarata come -4 rispetto all' indirizzo della base dello stack (ebp). Occupa 4 byte di spazio nello stack.

Le variabili sono quelle in verde, dove i valori hanno il – davanti e sono in una posizione negativa rispetto alla base dello stack ebp.
Ben divisi dalla parte dove sono presenti le istruzioni dell' eseguibile.

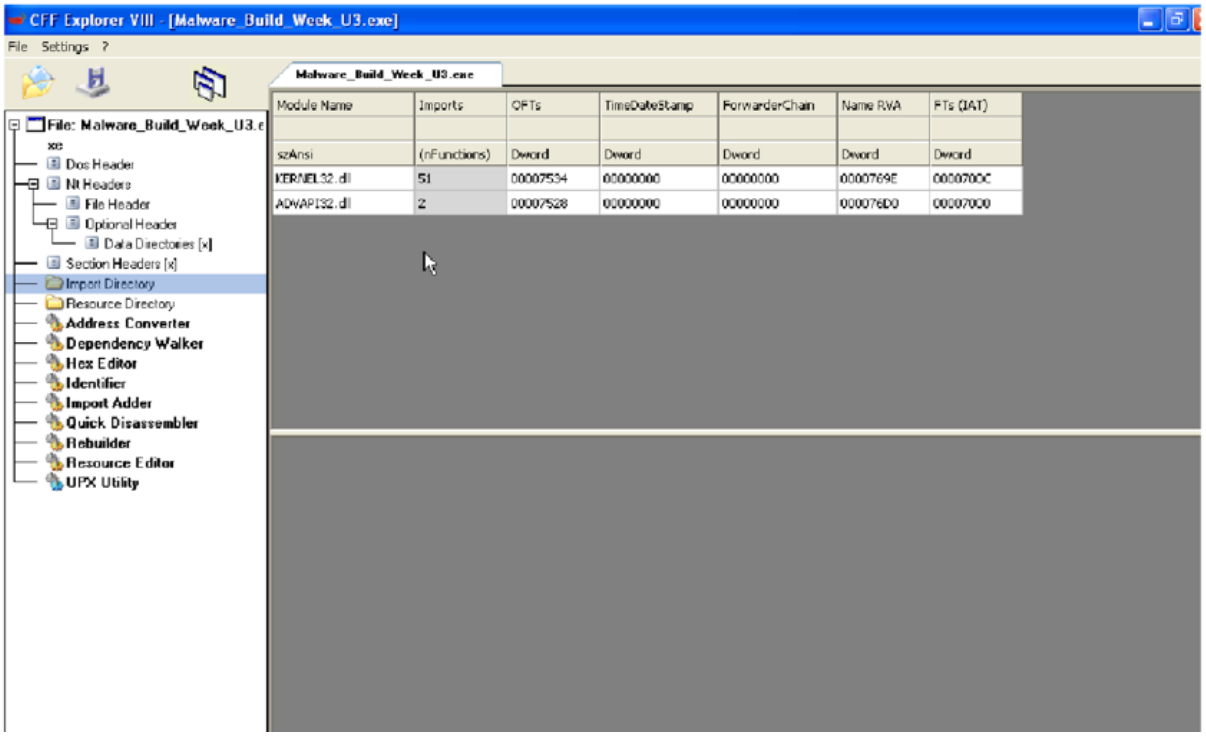
3) **All' interno del file eseguibile presenti 4 sezioni principali visibili con CFF Explorer:**



sezione .rsc → include le risorse utilizzate dall' eseguibile che non vengono considerate all' interno dell' eseguibile come immagine, menù, stringhe ed icone;

sezione .rdata → contiene le info sull' import e sull' export, con possibilità di salvataggio dati read-only usati dal programma;

4) **Il Malware importa 2 librerie:**



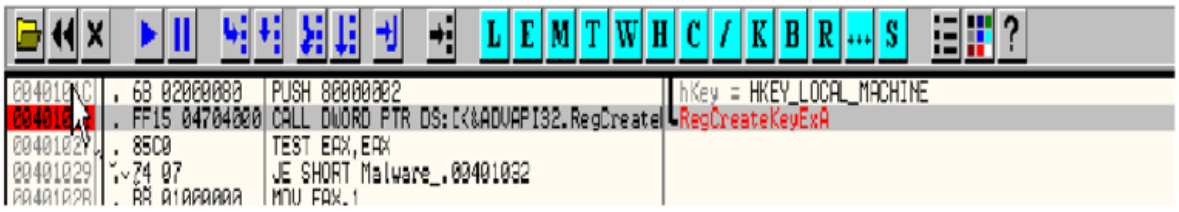
libreria Kernel32.dll → permette al malware di utilizzare funzioni per per la gestione della memoria oppure funzioni per interagire con il sistema operativo;

libreria ADVAPI32.dll → permette al malware di avere accesso alle chiavi di registro.

5) **Scopo della funzione chiamata alla locazione di memoria 00401021:**

Creazione della chiave di registro:

“SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon”



6) **Parametri passati alla funzione alla locazione 00401021:**

```
push    ebp
mov     ebp, esp
push    ecx
push    0               ; lpdwDisposition
lea     eax, [ebp+hObject]
push    eax             ; phkResult
push    0               ; lpSecurityAttributes
push    0F003Fh         ; samDesired
push    0               ; dwOptions
push    0               ; lpClass
push    0               ; Reserved
push    offset SubKey   ; "SOFTWARE\\Microsoft\\Windows NT\\CurrentVe"...
push    80000002h       ; hKey
call    ds:RegCreateKeyExA
```

7) **All' indirizzo di memoria 00401017 troviamo la chiave di registro che porta all' avvio automatico della DLL compromessa:**

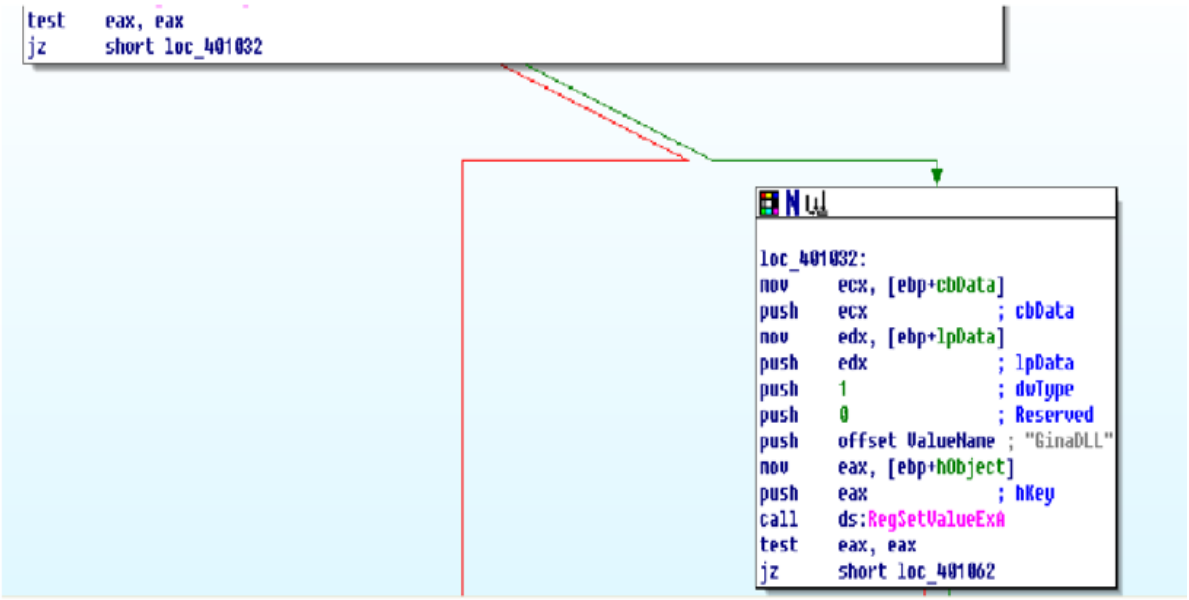
```
.text:00401000
.text:00401000                push    ebp
.text:00401001                mov     ebp, esp
.text:00401003                push    ecx
.text:00401004                push    0               ; lpdwDisposition
.text:00401006                lea     eax, [ebp+hObject]
.text:00401009                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
```

8) **Il significato delle istruzioni comprese tra gli indirizzi 00401027 e 00401029:**

Stanno a verificare se il malware è stato avviato, in caso contrario fa direttamente il salto alla locazione 00401032. Se l' apertura è avvenuta correttamente parte l' istruzione che chiude il proseguimento:

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

Presente di seguito il diagramma a flusso:



9) **Istruzioni del codice Assembly tradotte in codice C:**

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

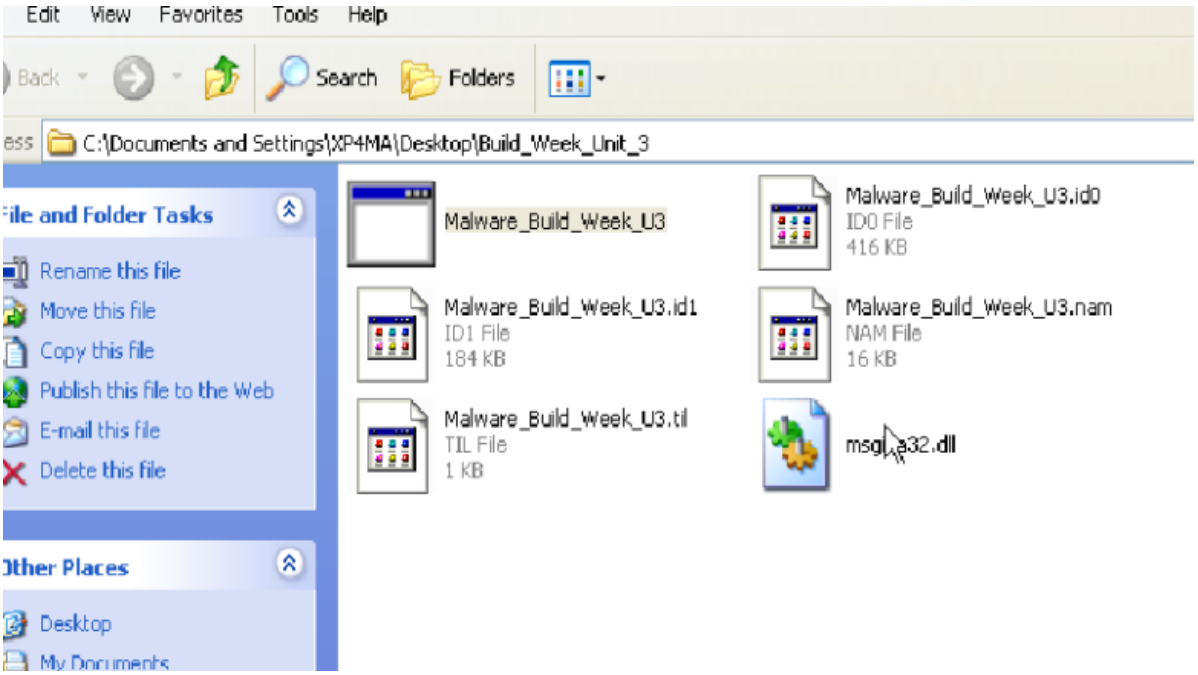
10) **Valutare il parametro "ValueName" della chiamata alla locazione 00401047:**

```
.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
```

Analizzata la chiamata alla funzione "RegSetValueExa" alla posizione di memoria 00401047 il valore del parametro "ValueName" è 'GinaDLL'.

ANALISI DINAMICA:

Avviato il Malware, in seguito all' analisi statica, all' interno della cartella dove era situato si è creato il file 'msgina32.dll' nonché la versione corrotta della 'GinaDLL'.



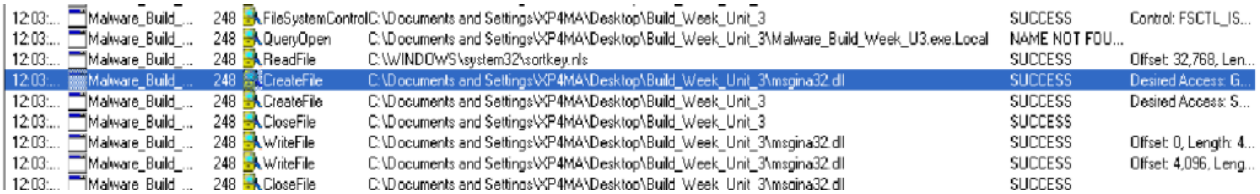
Dalla spiegazione online di Microsoft lo scopo della 'GinaDLL' è fornire procedure di identificazione e autenticazione dell' utente personalizzabili.

Analizzando i risultati e le chiavi di registro di Process Monitor (Procmon) si nota che:

- **Il Malware crea la chiave di registro Winlogon;**
- **Gli viene assegnato il valore msgina32.dll che aveva trovato nella cartella del Malware.**

Time...	Process Name	PID	Operation	Path	Result	Detail
12:03:...	Malware_Build_...	248	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Malware_Build_W...	NAME NOT FOU...	Desired Access: R...
12:03:08.3070182 PM	Build_...	248	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	Desired Access: R...
12:03:...	Malware_Build_...	248	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	SUCCESS	Type: REG_DWO...
12:03:...	Malware_Build_...	248	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	
12:03:...	Malware_Build_...	248	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	Desired Access: R...
12:03:...	Malware_Build_...	248	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	SUCCESS	Type: REG_DWO...
12:03:...	Malware_Build_...	248	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	
12:03:...	Malware_Build_...	248	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\Secur32.dll	NAME NOT FOU...	Desired Access: R...
12:03:...	Malware_Build_...	248	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\RPCRT4.dll	NAME NOT FOU...	Desired Access: R...
12:03:...	Malware_Build_...	248	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ADVAPI32.dll	NAME NOT FOU...	Desired Access: R...
12:03:...	Malware_Build_...	248	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	Desired Access: R...
12:03:...	Malware_Build_...	248	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	SUCCESS	Type: REG_DWO...
12:03:...	Malware_Build_...	248	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSUserEnabled	SUCCESS	Type: REG_DWO...
12:03:...	Malware_Build_...	248	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	
12:03:...	Malware_Build_...	248	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	Desired Access: R...
12:03:...	Malware_Build_...	248	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\LeakTrack	NAME NOT FOU...	Length: 144
12:03:...	Malware_Build_...	248	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	
12:03:...	Malware_Build_...	248	RegOpenKey	HKLM	SUCCESS	Desired Access: M...
12:03:...	Malware_Build_...	248	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Diagnostics	NAME NOT FOU...	Desired Access: R...
12:03:...	Malware_Build_...	248	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ntdll.dll	NAME NOT FOU...	Desired Access: R...
12:03:...	Malware_Build_...	248	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\kernel32.dll	NAME NOT FOU...	Desired Access: R...
12:03:...	Malware_Build_...	248	RegCreateKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	Desired Access: All...
12:03:...	Malware_Build_...	248	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL	SUCCESS	Type: REG_SZ, Le...
12:03:...	Malware_Build_...	248	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	

Valore msgina32.dll assegnato:



12:03:...	Malware_Build_...	248	FileSystemControl	C:\Documents and Settings\XP4MA\Desktop\Build_Week_Unit_3	SUCCESS	Control: FSCTL_IS...
12:03:...	Malware_Build_...	248	QueryOpen	C:\Documents and Settings\XP4MA\Desktop\Build_Week_Unit_3\Malware_Build_Week_U3.exe.Local	NAME NOT FOU...	
12:03:...	Malware_Build_...	248	ReadFile	C:\WINDOWS\system32\sortkey.nls	SUCCESS	Offset: 32,768, Len...
12:03:...	Malware_Build_...	248	CreateFile	C:\Documents and Settings\XP4MA\Desktop\Build_Week_Unit_3\msgina32.dll	SUCCESS	Desired Access: G...
12:03:...	Malware_Build_...	248	CreateFile	C:\Documents and Settings\XP4MA\Desktop\Build_Week_Unit_3	SUCCESS	Desired Access: S...
12:03:...	Malware_Build_...	248	CloseFile	C:\Documents and Settings\XP4MA\Desktop\Build_Week_Unit_3	SUCCESS	
12:03:...	Malware_Build_...	248	WriteFile	C:\Documents and Settings\XP4MA\Desktop\Build_Week_Unit_3\msgina32.dll	SUCCESS	Offset: 0, Length: 4...
12:03:...	Malware_Build_...	248	WriteFile	C:\Documents and Settings\XP4MA\Desktop\Build_Week_Unit_3\msgina32.dll	SUCCESS	Offset: 4,096, Leng...
12:03:...	Malware_Build_...	248	CloseFile	C:\Documents and Settings\XP4MA\Desktop\Build_Week_Unit_3\msgina32.dll	SUCCESS	

Conclusione:

Unendo tutte le info relative all' analisi statica e l' analisi dinamica si può pensare che il Malware in questione si tratti di un Dropper : un tipo di malware che al suo interno contiene e rilascia un altro malware.

Questo perchè si nota che si avvale della sezione .rsrc e contiene al suo interno un logger che copia le credenziali di accesso.