

Malware Analysis Report di benedetto bordonaro



Introduzione

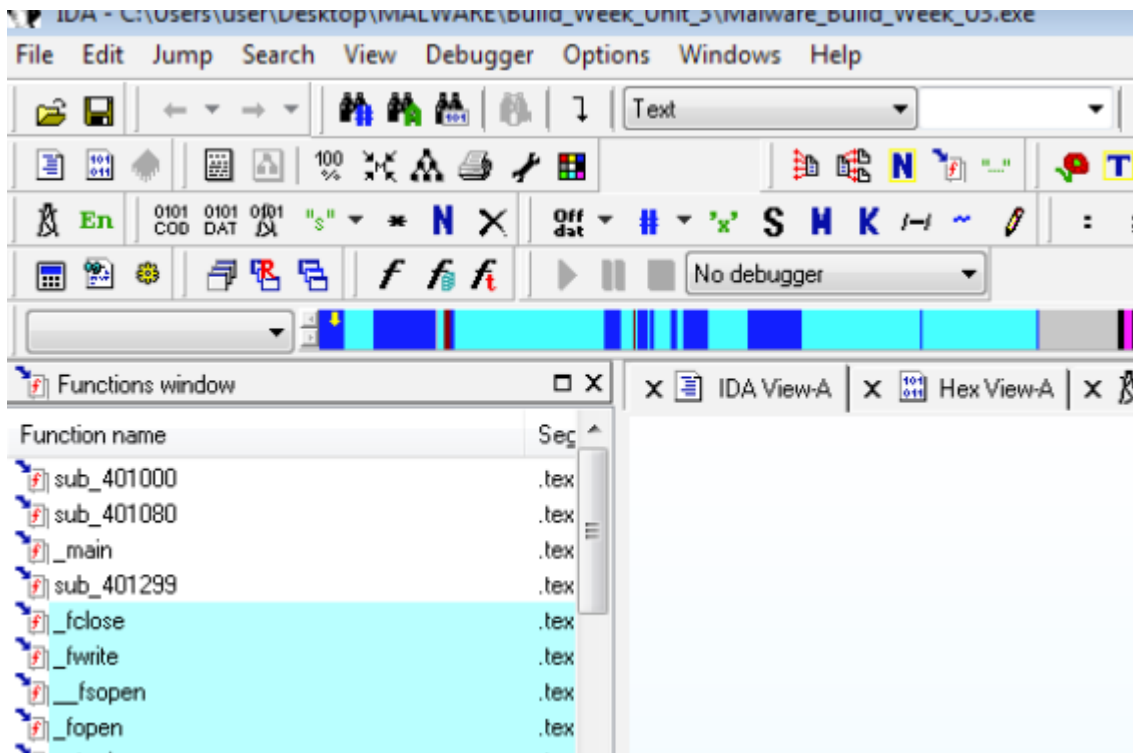
Il presente report ha l'obiettivo di analizzare in modo dettagliato un file eseguibile maligno denominato `Malware_Build_Week_U3`, situato nella cartella `Build_Week_Unit_3` sul desktop di una macchina virtuale dedicata. L'analisi è stata suddivisa in due fasi principali: analisi statica e analisi dinamica. Ognuna di queste fasi fornisce informazioni cruciali per comprendere il comportamento del malware e le sue potenziali minacce.

1. Analisi Statica

1.1 Parametri e Variabili della Funzione `Main()`

Durante l'analisi statica dell'eseguibile, utilizzando il tool IDA Pro, abbiamo osservato che la funzione `Main()` accetta tre parametri. Questi parametri sono utilizzati per il passaggio di argomenti al programma durante la sua esecuzione.

All'interno della stessa funzione `Main()`, sono dichiarate cinque variabili locali. Le variabili vengono utilizzate per la gestione interna dei dati e per controllare il flusso del programma.



```

; 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_117= byte ptr -117h
var_8= dword ptr -8
var_4= dword ptr -4
argc= dword ptr 8
argv= dword ptr 0Ch
envp= dword ptr 10h

```

1.2 Sezioni dell'Eseguibile

L'eseguibile analizzato contiene quattro sezioni principali:

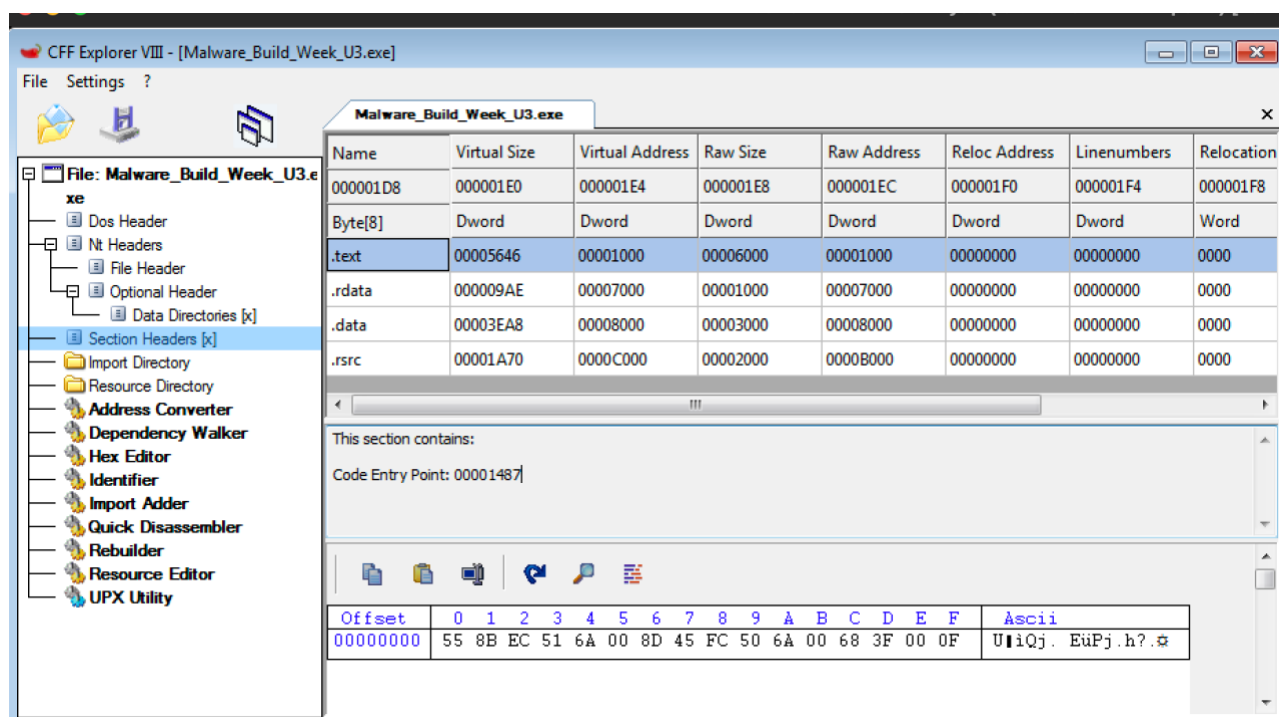
.text: Contiene il codice eseguibile effettivo, ovvero le istruzioni che saranno eseguite dalla CPU.

.rdata: Questa sezione contiene dati di sola lettura come stringhe costanti e puntatori.

.data: Contiene variabili globali e dati inizializzati.

.rsrc: Include le risorse utilizzate dall'eseguibile, come icone, immagini, e altre risorse necessarie all'applicazione.

Per estrarre queste informazioni, è stato utilizzato il tool CFF Explorer, che ha permesso di identificare e analizzare le sezioni del file in dettaglio.



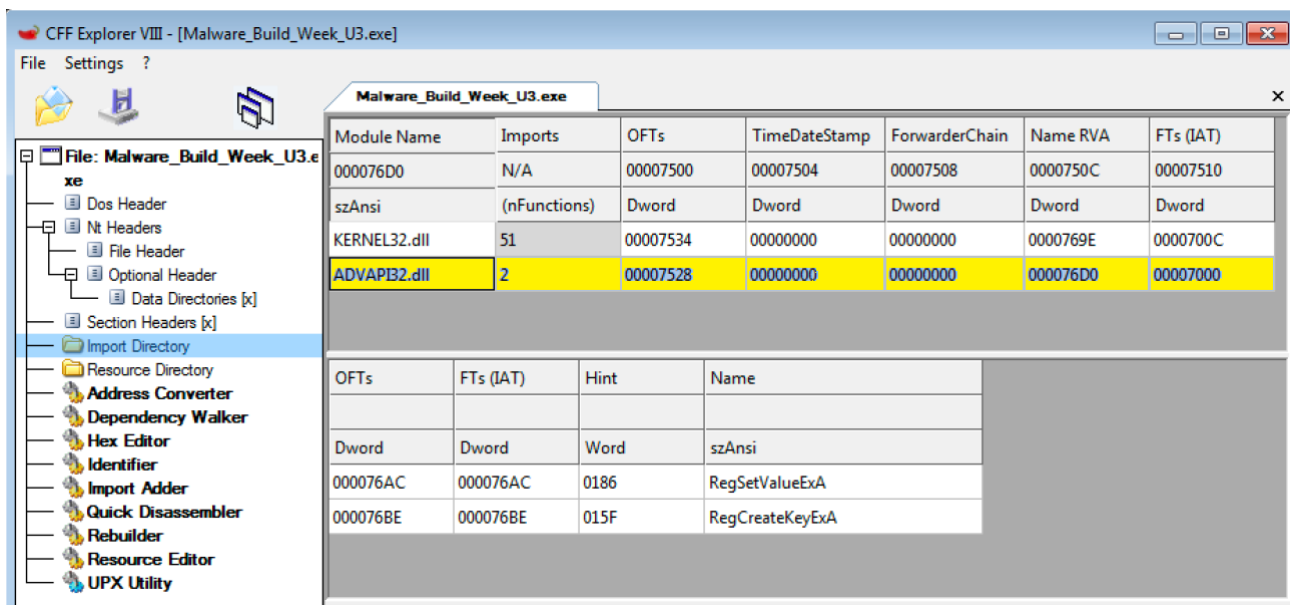
1.3 Librerie Importate dal Malware

Il malware carica due librerie dinamiche fondamentali: KERNEL32.dll e ADVAPI32.dll.

KERNEL32.dll: Questa libreria è fondamentale per le operazioni di basso livello sul sistema operativo, come la gestione dei file, la memoria e i processi. La presenza di questa libreria suggerisce che il malware potrebbe essere coinvolto in operazioni di manipolazione di file o nella gestione della memoria, aspetti cruciali per l'esecuzione di payload malevoli.

ADVAPI32.dll: Questa libreria include funzioni per interagire con il registro di Windows e i servizi di sicurezza. L'analisi delle funzioni richiamate da questa libreria, come RegCreateKeyExA e RegSetValueExA, indica che il malware potrebbe modificare il registro di sistema per garantirsi la persistenza o alterare configurazioni critiche del sistema operativo.

L'ipotesi principale è che il malware utilizzi queste librerie per alterare il registro di Windows, probabilmente per garantirsi l'esecuzione automatica all'avvio del sistema.



2. Analisi del Codice Assembly

Per comprendere il comportamento del malware a livello di codice assembly, sono state analizzate diverse locazioni di memoria.

2.1 Funzione alla Locazione 00401021

Alla locazione di memoria 00401021, viene chiamata la funzione RegCreateKeyExA. Questa funzione è utilizzata per creare o aprire una chiave di registro specificata. L'obiettivo del malware potrebbe essere quello di modificare il registro di sistema per eseguire operazioni malevole al successivo avvio del sistema.

<pre> .text:00401017 .text:0040101C .text:00401021 .text:00401027 .text:00401029 .text:0040102B .text:00401030 </pre>	<pre> push offset SubKey ; "SOFTWARE\\Microsoft\\Windows NT\\CurrentVe... push 80000002h ; hKey call ds:RegCreateKeyExA test eax, eax jz short loc_401032 mov eax, 1 jmp short loc_40107B </pre>
---	--

2.2 Passaggio dei Parametri

I parametri per la funzione RegCreateKeyExA vengono passati allo stack attraverso una serie di istruzioni push. Questo metodo di passaggio dei parametri è comune in molte architetture, e in questo caso, serve a preparare i dati necessari per l'esecuzione della funzione.

<pre> .text:00401000 .text:00401000 .text:00401001 .text:00401003 .text:00401004 .text:00401006 .text:00401009 .text:0040100A .text:0040100C .text:00401011 .text:00401013 .text:00401015 .text:00401017 .text:0040101C .text:00401021 </pre>	<pre> 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 </pre>
---	---

2.3 Rappresentazione del Parametro alla Locazione 00401017

Alla locazione 00401017, il malware crea un offset per memorizzare il valore dell'oggetto SubKey, che rappresenta una sottocartella del registro di sistema di Windows. Questo suggerisce che il malware è progettato per modificare specifiche sottosezioni del registro, probabilmente per eseguire operazioni persistenti.

2.4 Traduzione del Codice Assembly

L'analisi delle istruzioni tra 00401027 e 00401029 rivela una serie di test condizionali e salti (test EAX, EAX seguito da jz ShortLoc). Queste istruzioni vengono tradotte in linguaggio C come segue:

```
if (var == 0) {

}
```

Questo codice verifica se una determinata variabile è uguale a zero, e in tal caso, esegue una porzione di codice condizionale.

```
.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      jmp     short loc_40107B
.text:00401032      -
```

2.5 Valore del Parametro "ValueName"

Il parametro lpValueName alla locazione 00401047 è identificato come GinaDLL. Questa stringa è probabilmente utilizzata dal malware per indirizzare una DLL malevola nel registro di Windows, suggerendo che il malware cerca di sostituire o modificare le normali procedure di autenticazione di Windows.

```
.text:00401035      push     ecx                ; cbData
.text:00401036      mov     edx, [ebp+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
```

Traduzione delle istruzioni assembly in linguaggio C

```
// Verifica se la variabile 'var' è uguale a zero

if (var == 0) {

    // Esegui il codice contenuto in questo blocco

}
```

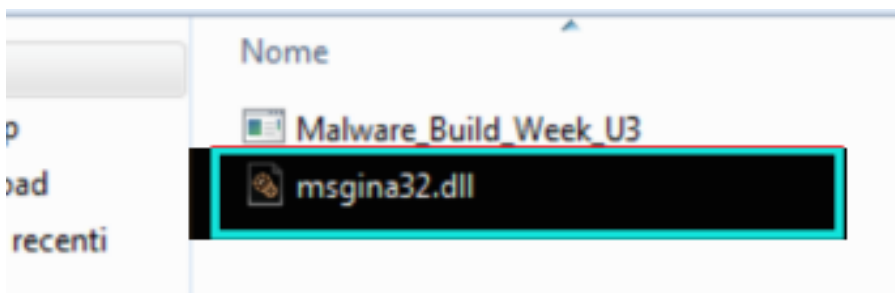
```
// Assegna il valore "GinaDLL" al parametro lpValueName
```


```
LPCSTR lpValueName = "GinaDLL";
```

3. Analisi Dinamica


3.1 Osservazioni Post-Esecuzione

Dopo l'esecuzione del malware, abbiamo osservato la creazione di un file msgina32.dll nella stessa cartella dell'eseguibile. Questo file è stato analizzato con VirusTotal, confermando la presenza di un trojan-dropper.



 57d8d248a8741176348b5d12dcf29f34c8f48ede0ca13c30d12e5ba0384056d7

VirusTotal has updated its Privacy Notice and its Terms of Use effective July 18, 2024. You can view the updated [Privacy Notice](#) and [Terms of Use](#).



52
/ 71

Community Score

52/71 security vendors and no sandboxes flagged this file as malicious

57d8d248a8741176348b5d12dcf29f34c8f48ede0ca13c30d12e5ba0384056d7

Lab11-01.exe

peexe spreader armadillo checks-user-input

DETECTION

DETAILS


RELATIONS

BEHAVIOR

TELEMETRY

COMMUNITY 10

[Join the VT Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Popular threat label  trojan.doina/totbrick

Threat categories trojan

51

/ 71

Community Score

51/71 security vendors and no sandboxes flagged this file as malicious

Reanalyze

Similar

More

f8a4f61bccd5bab1cad0ab9e57f6f3092a8bd4dd0adfdc4853e89ba96afc93f9

msgina32.dll

Size

6.50 KB

Last Modification Date

20 days ago

DLL

pedll

detect-debug-environment

armadillo

idle

DETECTION

DETAILS

RELATIONS

BEHAVIOR

TELEMETRY

COMMUNITY 4

Join the VT Community

and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Popular threat label

Trojan.fragtor/tiggre

Threat categories

trojan

Family labels

fragtor

tiggre

Security vendors' analysis

Do you want to automate checks?

Alibaba	Trojan.Win32/Tiggre.387d5a16	AliCloud	Trojan.Win.Generic.f3be1728
ALYac	Gen:Variant.Fragtor.510142	Antiy-AVL	Trojan/Win32.FakeGina
Arcabit	Trojan.Fragtor.D7C8BE	Avast	Win32:Trojan-gen
AVG	Win32:Trojan-gen	Avira (no cloud)	HEUR/AGEN.1326250
BitDefender	Gen:Variant.Fragtor.510142	BitDefenderTheta	Gen:NN.ZedlAf.36802.aq4@a0c1rOb

3.2 Attività sul Registro di Windows

L'analisi dinamica con Process Monitor ha rivelato che il malware esegue operazioni sul registro, specificamente creando e settando valori nelle chiavi di registro utilizzando le funzioni RegCreateKeyExA e RegSetValueExA. Queste operazioni sono cruciali per l'obiettivo del malware di mantenere la sua persistenza nel sistema.

Process	Operation	Path	Result	Details
1621: Malware_Buid	RegOpenKey	HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Diagnostics	NAME NOT FOUND	Desired Access: Read
1621: Malware_Buid	RegQueryValue	HKLM	SUCCESS	Query: Handle Tags: Handle Tags: 0x0
1621: Malware_Buid	RegCreateKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	Desired Access: All Access, Disposition: REG_OPENED_EXISTING_KEY
1621: Malware_Buid	RegSetInfoKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
1621: Malware_Buid	RegQueryValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	Query: Handle Tags: Handle Tags: 0x400
1621: Malware_Buid	RegSetValue	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL	SUCCESS	Type: REG_SZ, Length: 520, Data: C:\Users\user\Desktop\MALWARE\Build_Week_Unit
1621: Malware_Buid	RegCloseKey	HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	
1621: Malware_Buid	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\License File Function Options	SUCCESS	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon			SUCCESS	Desired Access: All Access, Disposition: REG_OPENED_EXISTING_KEY
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon			SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon			SUCCESS	Query: Handle Tags: Handle Tags: 0x400
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL			SUCCESS	Type: REG_SZ, Length: 520, Data: C:\Users\user\Desktop\MALWARE\Build_Week_Unit\msina32

3.3 Attività sul File System

È stata rilevata una chiamata di sistema `CreateFile` che crea il file `msgina32.dll`, seguito da una `write file` che inserisce il contenuto malevolo nel file. Infine, il file viene chiuso con la chiamata `close file`. Queste azioni suggeriscono che il malware non solo crea la DLL, ma la popola con codice malevolo, pronto per essere eseguito.

00:43:...	Malware_Build_...	1644	CreateFileMapping	C:\Windows\SysWOW64\sechost.dll
00:43:...	Malware_Build_...	1644	CloseFile	C:\Windows\SysWOW64\sechost.dll
00:43:...	Malware_Build_...	1644	CreateFile	C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3\msgina32.dll
00:43:...	Malware_Build_...	1644	WriteFile	C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3\msgina32.dll
00:43:...	Malware_Build_...	1644	WriteFile	C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3\msgina32.dll
00:43:...	Malware_Build_...	1644	CloseFile	C:\Users\user\Desktop\MALWARE\Build_Week_Unit_3\msgina32.dll

Conclusioni

L'analisi combinata statica e dinamica del malware Malware_Build_Week_U3 evidenzia che questo codice malevolo è progettato per ottenere persistenza nel sistema attraverso modifiche al registro di Windows e la creazione di una DLL malevola (msgina32.dll). Il comportamento del malware suggerisce che il suo obiettivo principale sia l'intercettazione delle credenziali di autenticazione degli utenti, potenzialmente per scopi di furto di identità o per ottenere accesso non autorizzato al sistema.

Data l'importanza della DLL msgina.dll nel processo di autenticazione di Windows, è probabile che il malware miri a sostituire o alterare le normali procedure di login per registrare e sottrarre credenziali utente. Questo tipo di minaccia sottolinea la necessità di implementare misure di sicurezza avanzate e di eseguire regolarmente analisi del sistema per individuare eventuali compromissioni.