

Malware Analysis

Analisi statica basica e linguaggio assembly

1. Librerie importate dal malware

All'interno di questo report, andremo ad analizzare il comportamento del malware contenuto nella cartella U3_W2_L5 attraverso la tecnica dell'analisi statica basica.

L'analisi statica basica è un tipo di analisi che studia il comportamento del malware senza eseguirlo; quindi, risulta molto semplice da effettuare ma allo stesso tempo abbastanza inefficace.

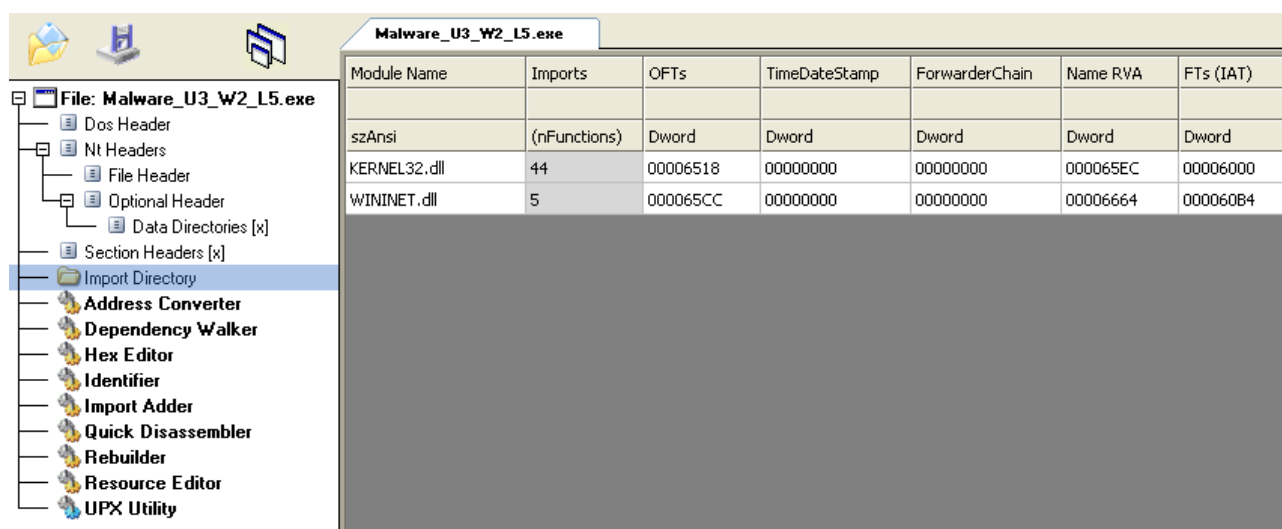
Per fare ciò, utilizzeremo uno dei tool più comuni nell'analisi statica, ovvero CFF Explorer.

CFF Explorer è un tool che fa da editor per i file eseguibili PE e ci permette di recuperare delle informazioni importanti sul comportamento del malware senza l'esecuzione dello stesso.

Si aprirà una schermata dove vengono visualizzate varie informazioni sul malware, tra cui le sezioni degli header e le directory importate, ovvero le librerie caricate dall'attaccante pronte ad essere utilizzate.

Le librerie importate in questo caso sono:

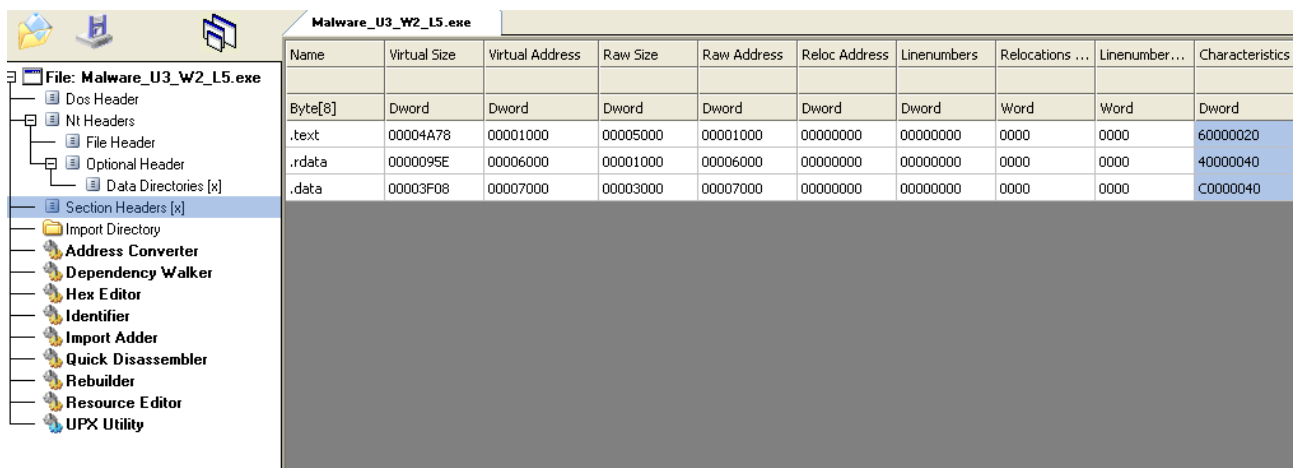
- **KERNEL32.dll**→ libreria comune che contiene le funzioni principali per interagire con il sistema operativo e può gestire, ad esempio, la manipolazione dei file o la memoria.
- **WININET.dll**→ libreria che contiene le funzioni per l'attivazione di alcuni protocolli di rete come http, FTP, NTP.



2. Sezioni degli headers

Per quanto riguarda le sezioni degli headers, all'interno di questo malware possiamo individuare tre sezioni del file PE:

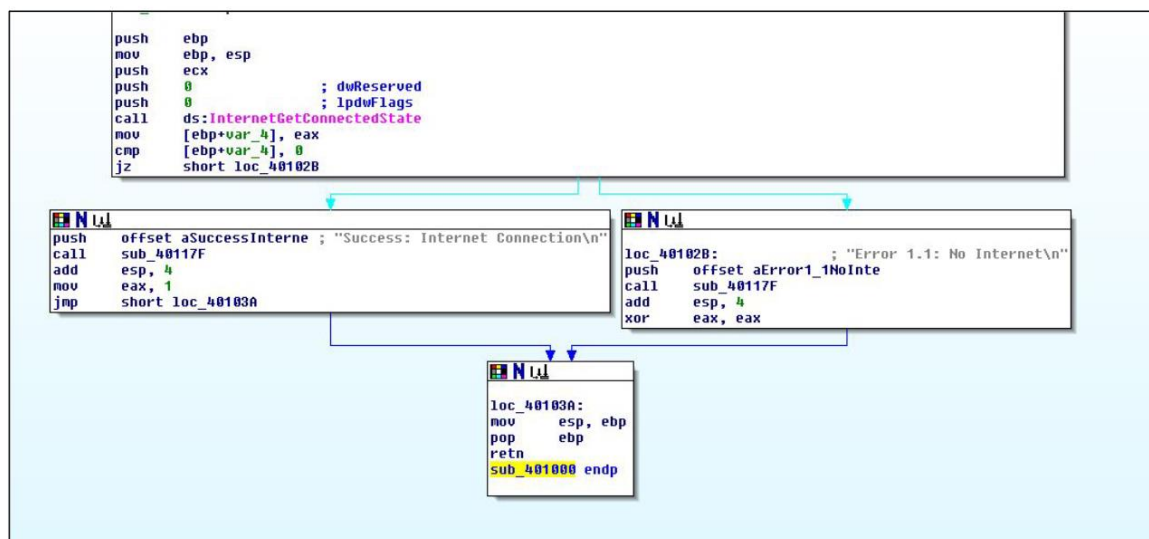
- **.text** → la sezione "text" contiene le istruzioni (le righe di codice) che la CPU va ad eseguire una volta che il software è avviato.
- **.rdata** → include generalmente le informazioni sulle librerie e le funzioni importate ed esportate dall'eseguibile. Queste informazioni possono essere ricavate con CFF Explorer.
- **.data** → contiene i dati e le variabili globali del programma eseguibile, che devono essere disponibili da qualsiasi parte del programma.



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	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

3. Analisi statica avanzata

Figura 1



Nella figura 1 sopra riportata, vi è un codice di un malware scritto in linguaggio Assembly.

Al suo interno possiamo individuare **6 macrocategorie**.

Per avere un'idea più chiara dei blocchi di codice principali, possiamo riportarli all'interno di una tabella, come quella di seguito.

Blocco di istruzioni	Descrizione
“Push EBP / Push ECX”	creazione dello stack
“Push 0 ;dwReserved” / “Call ds: InternetGetConnectedState”	funzione chiamante dello stato della connessione internet. I parametri vengono inseriti tramite “push”.
“mov [ebp+var_4], eax” / “jz short loc_40102B”	creazione del ciclo if che poi viene ricondotto alle macrocategorie successive
“push offset aSuccessInterne” / “jmp short loc_40103A”	continua il percorso prestabilito per il programma in esecuzione, se ZF è uguale a 0. In questo caso, la connessione internet è attiva.
“loc_40102B” / “xor eax,eax”	il programma effettua il salto se ZF è uguale a 1. In questo caso, avremo l'evidenza che la connessione internet non è attiva.
“loc_401030A” / “sub 401000 endp”	in entrambi i casi, viene ripulito e rimosso lo stack, che viene riportato allo stato iniziale.

4. Ipotesi del comportamento del malware

Attraverso le evidenze collezionate, possiamo ipotizzare che il malware in questione possa utilizzare la connessione ad internet per cercare di connettersi ad un dominio specifico e scaricare probabilmente altri malware sulla macchina. Solitamente, i malware che utilizzano la rete possono essere identificati come “**downloader**” oppure potrebbe utilizzare la connessione per installare una backdoor all’interno della macchina vittima.

5. ANALISI DINAMICA BASICA AGGIUNTIVA

Per avere un quadro generale completo, possiamo servirci dell’analisi dinamica basica.

La differenza tra l’analisi dinamica e l’analisi statica sta nell’esecuzione del malware. Nel primo caso il malware viene eseguito e il comportamento viene studiato durante l’esecuzione. Questo processo risulta più efficace.

Utilizzando CFF Explorer, possiamo ricavare il codice hash del malware per poi utilizzarlo su siti come Virus Total per ricavare informazioni presenti sui database dei software antivirus più noti.

Malware_U3_W2_L5.exe	
Property	Value
File Name	C:\Documents and Settings\Administrator\Desktop\Esercizio_Pratico_U3_W...
File Type	Portable Executable 32
File Info	No match found.
File Size	40.00 KB (40960 bytes)
PE Size	40.00 KB (40960 bytes)
Created	Tuesday 16 August 2022, 14.37.31
Modified	Wednesday 02 February 2011, 16.29.05
Accessed	Friday 23 September 2022, 10.49.49
MD5	C0B54534E188E1392F28D17FAFF3D454
SHA-1	BB6F01B1FEF74A9CFC83EC2303D14F492A671F3C
Property	Value
Empty	No additional info available

Una volta inserito l’hash del malware corrente su Virus Total, nella figura di seguito abbiamo evidenza del fatto che la sottocategoria riscontrata è quella del trojan in maniera generica oppure sospetto downloader.

Security Vendors' Analysis ⓘ

Alibaba	① Trojan:Win32/Generic.be125c32	Antiy-AVL	① Trojan/Generic.ASMalwS.3E79
Avast	① Win32:Trojan-gen	AVG	① Win32:Trojan-gen
Avira (no cloud)	① HEUR/AGEN.1240704	Comodo	① Malware@#13bka6m1o8w1f
CrowdStrike Falcon	① Win/malicious_confidence_100% (W)	Cybereason	① Malicious.1fe774
Cylance	① Unsafe	Cynet	① Malicious (score: 99)
DrWeb	① Trojan.MulDrop7.63090	Elastic	① Malicious (high Confidence)
ESET-NOD32	① Win32/Agent.WOO	Fortinet	① W32/Agent.WOOltr
GData	① Win32:Trojan.Agent.DZ3C1W	Google	① Detected
Gridinsoft (no cloud)	① Trojan.Win32.Agent.ns	Ikarus	① Trojan.Win32.Agent
Lionic	① Trojan.Win32.Generic.4lc	Malwarebytes	① Trojan.Agent.PMA
MAX	① Malware (ai Score=97)	MaxSecure	① Trojan.Malware.300983.susgen
McAfee	① GenericRXAA-AAIC0B54534E188	McAfee-GW-Edition	① ArtemisITrojan
Microsoft	① Trojan:Win32/Ymacro.AAB7	NANO-Antivirus	① Trojan.Win32.Agent.dveqkx
Palo Alto Networks	① Generic.ml	Rising	① Trojan.AgentI8.B1E (TFE:5:W5kRu0pSw...

Per quanto riguarda il comportamento di questo malware, possiamo ricavare delle informazioni dal portale di Virus Total.

In questo caso, i comportamenti riscontrati sono:

- Privilege escalation;
- Iniezione di processi;
- Modifiche del registro;
- Disabilita o modifica i tools;
- Lettura di file;
- Lettura di policy dei software;
- Utilizza https per sfruttare la connessione.

Di seguito le evidenze riportate su Virus Total.

Mitre ATT&CK Tactics And Techniques

Privilege Escalation TA0004

- Process Injection T1055
 - Spawns processes

Defense Evasion TA0005

- Masquerading T1036
 - Creates files inside the user directory
- Process Injection T1055
 - Spawns processes
- Modify Registry T1112
 - Stores large binary data to the registry
- Disable or Modify Tools T1562.001
 - Adds / modifies Windows certificates

Discovery TA0007

- Remote System Discovery T1018
 - Reads the hosts file
- System Information Discovery T1082
 - Reads software policies

Command and Control TA0011

- Application Layer Protocol T1071
 - Uses HTTPS
 - Downloads files from webservers via HTTP
 - Performs DNS lookups
 - Tries to download or post to a non-existing http route (HTTP/1.1 404 Not Found / 503 Service Unavailable)
- Non-Application Layer Protocol T1095
 - Downloads files from webservers via HTTP
 - Performs DNS lookups
 - Tries to download or post to a non-existing http route (HTTP/1.1 404 Not Found / 503 Service Unavailable)
- Ingress Tool Transfer T1105
 - Downloads files from webservers via HTTP
 - Some HTTP requests failed (404). It is likely the sample will exhibit less behavior
 - Tries to download or post to a non-existing http route (HTTP/1.1 404 Not Found / 503 Service Unavailable)
- Encrypted Channel T1573
 - Uses HTTPS
 - Uses HTTPS for network communication, use the SSL MITM Proxy cookbook for further analysis

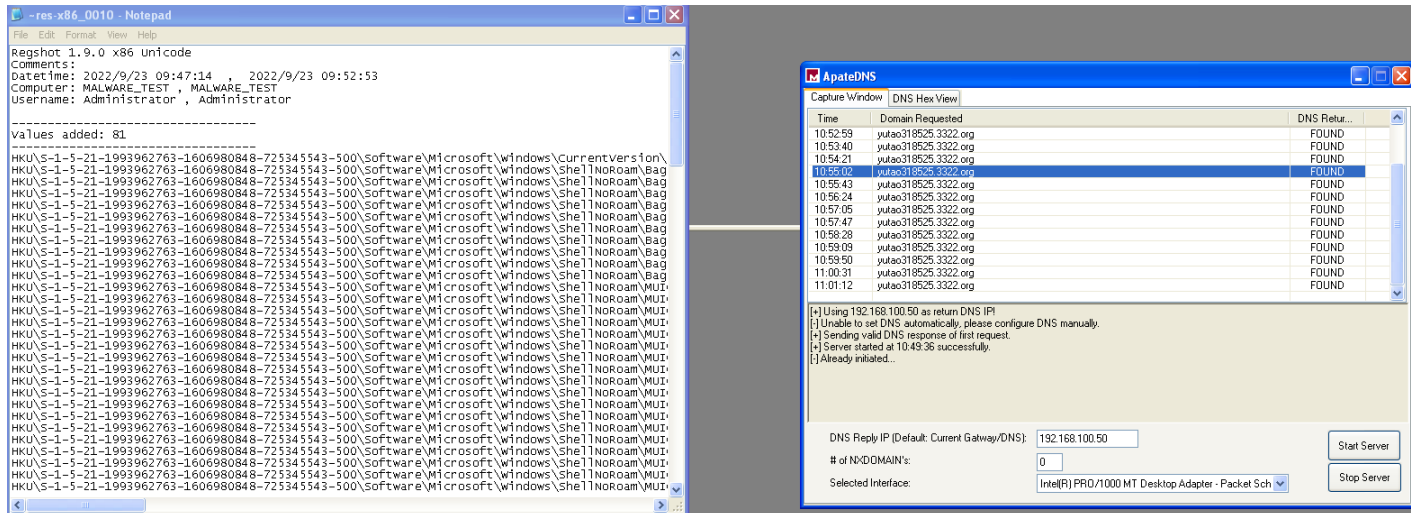
Attraverso Process Monitor possiamo visualizzare il caricamento di moltissime librerie all'interno della cartella Windows, utilizzate per implementare delle funzioni, come ad esempio "advapi" per modificare i registri o "gdi" per le icone, menù, ecc.

Innanzitutto viene creato il processo e il thread, poi vengono caricate le librerie. Infine, il thread e il processo vengono chiusi.

10:49:48.6514...	Malware_U3_W2_L5.exe	2828	Process Start	
10:49:48.6514...	Malware_U3_W2_L5.exe	2828	Thread Create	
10:49:48.6527...	Malware_U3_W2_L5.exe	2828	Load Image	C:\Documents and Settings\Administrator\...
10:49:48.6529...	Malware_U3_W2_L5.exe	2828	Load Image	C:\WINDOWS\system32\ntdll.dll
10:49:48.6946...	Malware_U3_W2_L5.exe	2828	Load Image	C:\WINDOWS\system32\kernel32.dll
10:49:48.7002...	Malware_U3_W2_L5.exe	2828	Load Image	C:\WINDOWS\system32\wininet.dll
10:49:48.7004...	Malware_U3_W2_L5.exe	2828	Load Image	C:\WINDOWS\system32\advapi32.dll
10:49:48.7006...	Malware_U3_W2_L5.exe	2828	Load Image	C:\WINDOWS\system32\iprct4.dll
10:49:48.7008...	Malware_U3_W2_L5.exe	2828	Load Image	C:\WINDOWS\system32\secur32.dll
10:49:48.7010...	Malware_U3_W2_L5.exe	2828	Load Image	C:\WINDOWS\system32\crypt32.dll
10:49:48.7012...	Malware_U3_W2_L5.exe	2828	Load Image	C:\WINDOWS\system32\msasn1.dll
10:49:48.7014...	Malware_U3_W2_L5.exe	2828	Load Image	C:\WINDOWS\system32\msvcrt.dll
10:49:48.7016...	Malware_U3_W2_L5.exe	2828	Load Image	C:\WINDOWS\system32\user32.dll
10:49:48.7019...	Malware_U3_W2_L5.exe	2828	Load Image	C:\WINDOWS\system32\gdi32.dll
10:49:48.7022...	Malware_U3_W2_L5.exe	2828	Load Image	C:\WINDOWS\system32\oleaut32.dll
10:49:48.7024...	Malware_U3_W2_L5.exe	2828	Load Image	C:\WINDOWS\system32\ole32.dll
10:49:48.7026...	Malware_U3_W2_L5.exe	2828	Load Image	C:\WINDOWS\system32\shlwapi.dll
10:49:48.7249...	Malware_U3_W2_L5.exe	2828	Load Image	C:\WINDOWS\WinSxS\x86_Microsoft.Wir...
10:49:48.7510...	Malware_U3_W2_L5.exe	2828	Load Image	C:\WINDOWS\system32\shell32.dll
10:49:48.7639...	Malware_U3_W2_L5.exe	2828	Load Image	C:\WINDOWS\system32\comctl32.dll
10:49:48.7954...	Malware_U3_W2_L5.exe	2828	Load Image	C:\WINDOWS\system32\rasapi32.dll
10:49:48.7965...	Malware_U3_W2_L5.exe	2828	Load Image	C:\WINDOWS\system32\rasman.dll
10:49:48.7967...	Malware_U3_W2_L5.exe	2828	Load Image	C:\WINDOWS\system32\netapi32.dll
10:49:48.7977...	Malware_U3_W2_L5.exe	2828	Load Image	C:\WINDOWS\system32\ws2_32.dll
10:49:48.8002...	Malware_U3_W2_L5.exe	2828	Load Image	C:\WINDOWS\system32\rtutils.dll
10:49:48.8011...	Malware_U3_W2_L5.exe	2828	Load Image	C:\WINDOWS\system32\api32.dll
10:49:48.8029...	Malware_U3_W2_L5.exe	2828	Load Image	C:\WINDOWS\system32\winmm.dll
10:49:48.8041...	Malware_U3_W2_L5.exe	2828	Load Image	C:\WINDOWS\system32\msv1_0.dll
10:49:48.8363...	Malware_U3_W2_L5.exe	2828	Load Image	C:\WINDOWS\system32\iphlpapi.dll
10:49:48.8634...	Malware_U3_W2_L5.exe	2828	Load Image	C:\WINDOWS\system32\sensapi.dll
10:49:48.8742...	Malware_U3_W2_L5.exe	2828	Thread Exit	
10:49:48.8745...	Malware_U3_W2_L5.exe	2828	Process Exit	

Inoltre, servendomi di tool come Regshot per la cattura degli screen prima e dopo l'esecuzione del malware e ApatDNS per la simulazione del servizio DNS, ho riscontrato i valori aggiunti dopo l'esecuzione del malware e molte richieste di connessione ad Internet.

La richiesta di connessione veniva inoltrata al dominio yutao318525.3322.org. Questo tipo di richieste non veniva però rilevata da Procmon nella sezione network.



Seconda ipotesi

Successivamente all'esecuzione del malware e allo studio dinamico di esso, possiamo confermare che il malware in questione è un "downloader", in quanto prova molte volte la connessione ad un sito sconosciuto.

Inoltre, aggiunge molte librerie utili a raggiungere il suo scopo iniziale, ovvero quello di scaricare presumibilmente altri malware all'interno della macchina vittima.