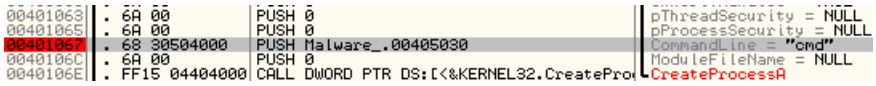
ANALISI DINAMICA AVANZATA CON OLLYDBG

Traccia:

Fate riferimento al malware: **Malware_U3_W3_L3**, presente all'interno della cartella **Esercizio_Pratico_U3_W3_L3** sul desktop della macchina virtuale dedicata all'analisi dei malware. Rispondete ai seguenti quesiti utilizzando OllyDBG.

- All'indirizzo 0040106E il Malware effettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «CommandLine» che viene passato sullo stack? (1)
- Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX? (2) Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX (3) motivando la risposta (4). Che istruzione è stata eseguita? (5)
- Inserite un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX? (6) Eseguite un step-into. Qual è ora il valore di ECX? (7) Spiegate quale istruzione è stata eseguita (8).
- BONUS: spiegare a grandi linee il funzionamento del malware

1. Valore del parametro CommandLine



Il parametro passato è **cmd**.

2. Valore del registro EDX

EDX 00000A28 in decimale 2600.

3. Valore del registro EDX dopo lo step-into

EDX 00000000 in decimale 0.

4. Motivazione del punto 3

Il registro viene inizializzato a 0 per via dello xor che pulisce la destinazione.

5. Quale istruzione viene eseguita?

XOR: operatore logico detto anche or esclusivo che restituisce vero quando tutti e 2 gli operandi sono veri.

6. Valore registro ECX

ECX 0A280105 in decimale 170393861.

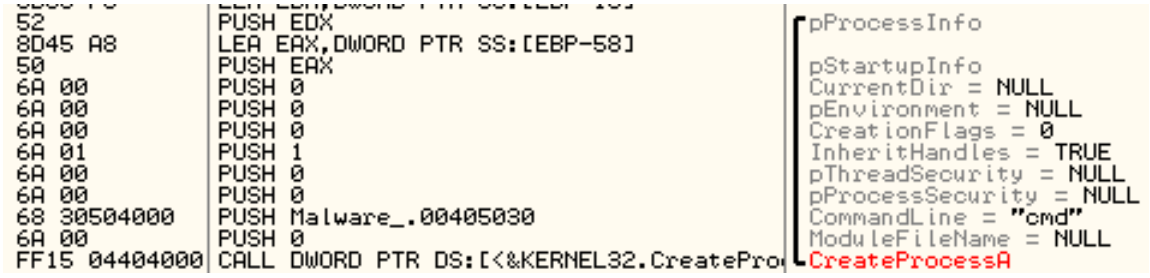
7. Valore del registro ECX dopo lo step-into

ECX 00000005 in decimale 5.

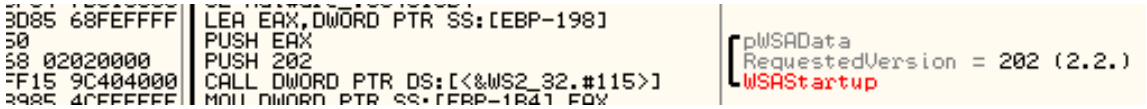
8. Quale istruzione viene eseguita?

AND: operatore logico che restituisce vero quando tutti e 2 gli operandi sono veri; viene usato come congiunzione logica e nelle istruzioni di ciclo e condizionali.

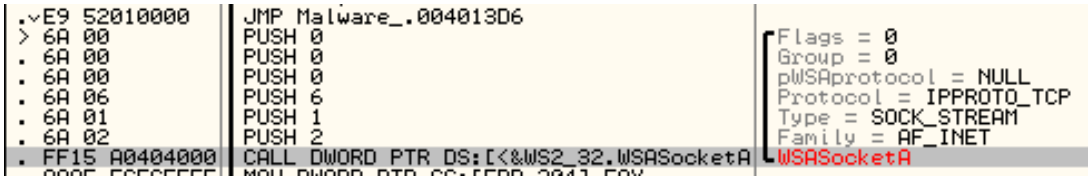
9. Funzionamento malware



Chiamata alla funzione per creare un nuovo processo, in questo caso la riga di comando **cmd**.



Qui c'è la chiamata alla funzione WSAStartup che, molto brevemente, avvia la libreria Winsock la quale serve per usare in modo più semplificato i protocolli TCP/IP.



La funzione chiamata crea un socket associato ad un provider. I parametri SOCK_STREAM ed AF_INET vengono passati rispettivamente per utilizzare il protocollo TCP con il socket e specificare la famiglia di indirizzi IP (IPv4).
In base a tutti questi dati raccolti, possiamo dedurre sia un malware che prova a connettersi con un server in remoto e crea una reverse shell in modo da permettere a chi è in ascolto sul server di eseguire comandi sul pc infettato e operare perciò direttamente sul sistema.