EPICODE

Esercizio S11 – L3

TRACCIA

Fate riferimento al malware: Malware\_U3\_W3\_L3, presente all’interno della cartella Esercizio\_Pratico\_U3\_W3\_L3sul 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 uno 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

SOLUZIONE

• 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)

- Il valore del parametro CommandLine è: Malware\_.00405030.

• 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)

- Dopo aver inserito il breakpoint software all’indirizzo 004015A3 il valore del registro EDX è: 00001DB1 (2)

- Dopo aver effettuato uno step-into il valore di EDX è diventato: 0 (3). Questo è avvenuto perché il programma ha appena passato la riga in cui, tramite l’istruzione XOR (5), reinizializza il valore del registro EDX (4).

• Inserite un secondo breakpoint all’indirizzo di memoria 004015AF. Qual è il valore del registro ECX? (6) Eseguite uno step-into. Qual è ora il valore di ECX? (7) Spiegate quale istruzione è stata eseguita. (8)

- Dopo aver messo il breakpoint all’indirizzo di memoria 004015AF il valore del registro ECX è: 1DB10106 (6)

- Dopo aver effettuato uno step-into il valore di ECX è diventato: 6. (7)

- L’istruzione: AND ECX, 0FF esegue un’operazione di AND bit a bit tra il valore corrente di ECX e il valore immediato 0xFF (che in binario è 11111111). L’operazione AND restituisce un valore in cui i bit sono impostati solo se entrambi i bit corrispondenti nei due operandi sono impostati a 1. Ecco come funziona:

Valore iniziale di ECX: 1DB10106 (in binario: 00011101101100010000000100000110).

Valore immediato 0xFF: 00000000000000000000000011111111.

Risultato dell’operazione AND: 00000000000000000000000000000110 (in decimale: 6).

Quindi, l’istruzione AND ECX, 0FF ha impostato tutti i bit di ECX a 0, tranne gli ultimi due, che sono rimasti invariati. Questo spiega perché il valore di ECX è diventato 00000006 dopo l’esecuzione dell’istruzione.

In breve, l’istruzione AND ha “mascherato” i primi 30 bit di ECX, lasciando solo gli ultimi due intatti. (8)

• BONUS: spiegare a grandi linee il funzionamento del malware

- Il malware modifica le chiavi di registro e ottiene la persistenza (rimane attivo anche in caso di spegnimento dell’host). Chiama la funzione WSAStartup per permettere al malware di usare risorse per il networking. Tramite la funzione gethostbyname ricerca l’indirizzo ip dell’host. Stabilisce poi una connessione Internet con quello che presumibilmente è un server remoto sotto controllo dell’attaccante. Il malware è un Trojan e un downloader.