EPICODE

Esercizio S11 – L2

TRACCIA

Lo scopo dell’esercizio di oggi è di acquisire esperienza con IDA, un tool fondamentale per l’analisi statica. A tal proposito, con riferimento al malware chiamato «Malware\_U3\_W3\_L2» presente all’interno della cartella «Esercizio\_Pratico\_U3\_W3\_L2» sul Desktop della macchina virtuale dedicata all’analisi dei malware, rispondere ai seguenti quesiti, utilizzando IDA Pro.  
1. Individuare l’indirizzo della funzione DLLMain (così com’è, in esadecimale)  
2. Dalla scheda «imports» individuare la funzione «gethostbyname». Qual è l’indirizzo dell’import? Cosa fa la funzione?  
3. Quante sono le variabili locali della funzione alla locazione di memoria 0x10001656?  
4. Quanti sono, invece, i parametri della funzione sopra?  
5. Inserire altre considerazioni macro-livello sul malware (comportamento)

SOLUZIONE

1. Individuare l’indirizzo della funzione DLLMain (così com’è, in esadecimale)

- Come è possibile notare nell’immagine sotto l’indirizzo della funzione DllMain è: .text:1000D02E

Immagine che contiene testo, schermata, Carattere, linea

Descrizione generata automaticamente

2. Dalla scheda «imports» individuare la funzione «gethostbyname». Qual è l’indirizzo dell’import? Cosa fa la funzione?

- L’indirizzo della funzione è: .idata:100163CC. La funzione gethostbyname restituisce un puntatore a una struttura hostent , ovvero una struttura allocata da Windows Sockets. La struttura hostent contiene i risultati di una ricerca corretta dell'host specificato nel parametro name. Se l'host specificato nel parametro name ha indirizzi IPv4 e IPv6, verranno restituiti solo gli indirizzi IPv4. La funzione gethostbyname può restituire solo indirizzi IPv4 per il parametro name.

3. Quante sono le variabili locali della funzione alla locazione di memoria 0x10001656?

- Secondo la convenzione di IDA per cui le variabili sono ad un offset negativo rispetto al registro EBP, le variabili sono 23. Nell’immagine sottostante alcuni esempi di variabili con offset negativo (p.e. -544h)

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

4. Quanti sono, invece, i parametri della funzione sopra?

- La funzione ha anche un parametro (offset positivo: 4).

Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

5. Inserire altre considerazioni macro-livello sul malware (comportamento)

- Il malware modifica le chiavi di registro e ottiene la persistenza (rimane attivo anche in caso di spegnimento dell’host). Effettua quindi una scalata dei privilegi e successivamente 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 include anche delle funzioni di creazione e modifica dei file.