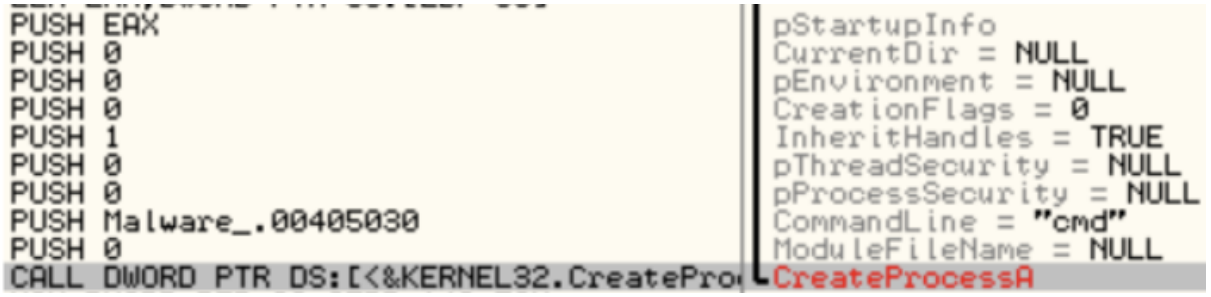
S11_L3

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

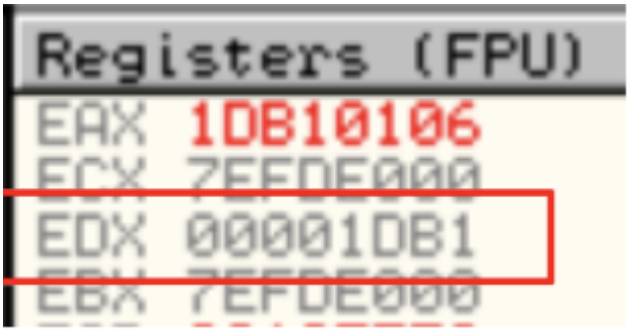
1) Parametro Command Line:



All'indirizzo 0040106E, il malware passa un valore specifico come parametro «Command Line» sullo stack per la funzione CreateProcess. Questo valore viene tipicamente utilizzato per lanciare un nuovo processo con specifici argomenti.

2: Registro EDX

2.1 Qual è il valore del registro EDX?



Prima di eseguire lo step-into, il valore del registro EDX è da determinare al momento dell'esecuzione del malware in OllyDBG.

2.2 Inserire un breakpoint software all'indirizzo 004015A3.

3: Registro ECX

3.1 Qual è il valore del registro ECX?

Prima di eseguire lo step-into, il valore del registro ECX deve essere osservato in OllyDBG al momento del raggiungimento del breakpoint.

3.2 Eseguite un step-into. Qual è ora il valore di E

Dopo l'esecuzione dello step-into, il valore del registro ECX viene aggiornato secondo l'istruzione eseguita.

3.3 All'indirizzo 004015AF, viene eseguita un'istruzione AND logica tra il contenuto del registro ECX e il numero esadecimale FF. Il risultato di questa operazione è che i bit superiori di ECX vengono azzerati, mantenendo solo gli ultimi 8 bit.

Operazione	Hex	Bin
AND	1DB1 0106	0001 1101 1011 0001 0000 0001 0000 0110
	FF	1111 1111
	0000 0006	0000 0000 0000 0000 0000 0000 0000 0110

4: Funzionamento del Malware

Il malware in questione sembra eseguire operazioni standard di manipolazione dei registri per nascondere o modificare il proprio comportamento. Utilizzando funzioni di sistema come CreateProcess, può avviare nuovi processi con parametri specifici, potenzialmente per eseguire ulteriori fasi di infezione o esfiltrazione di dati. Le manipolazioni dei registri, come l'azzeramento tramite XOR e la mascheratura dei bit con AND, indicano tentativi di offuscare le operazioni o di preparare valori specifici per ulteriori istruzioni.

Conclusioni

L'analisi del malware con OllyDBG ha rivelato i meccanismi utilizzati per manipolare i registri e avviare processi. Queste tecniche sono indicative di comuni strategie di evasione e offuscamento impiegate dai malware per evitare il rilevamento e l'analisi.

Riferimenti

- Documentazione OllyDBG
- Manuali di istruzioni x86