Report sull'Analisi del Malware Utilizzando OllyDBG

Data 14/02/24

Introduzione

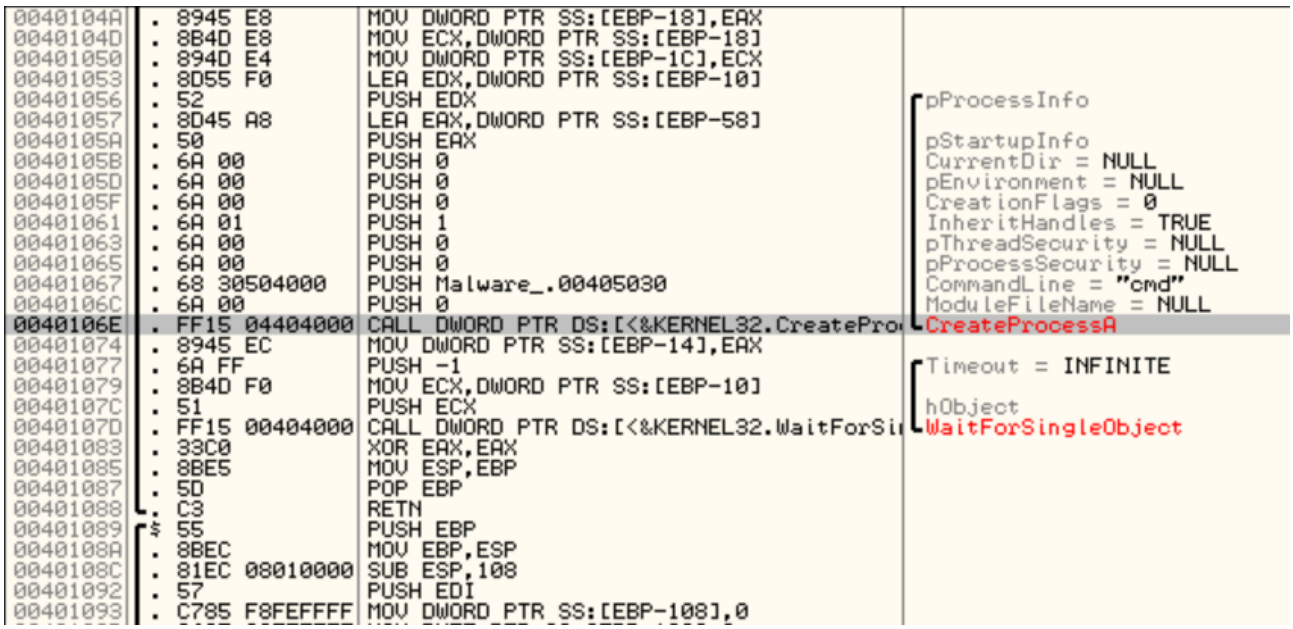
Nell'ambito dell'analisi del malware "Malware_U3_W3_L3", si è fatto riferimento al debugger OllyDBG per rispondere a una serie di quesiti. Questo strumento è essenziale per eseguire analisi dinamica dei malware, consentendo di esaminare il comportamento del malware in esecuzione e rivelando dettagli importanti sulle sue funzionalità.

Analisi dei Quesiti

Valore del Parametro "CommandLine" per la Chiamata alla Funzione "CreateProcess" (Indirizzo 0040106E)

Utilizzando OllyDBG, è stato individuato l'indirizzo 0040106E, dove il malware effettua una chiamata alla funzione "CreateProcess". Analizzando il contenuto dello stack in quel punto, è stato identificato il valore del parametro "CommandLine" passato alla funzione.

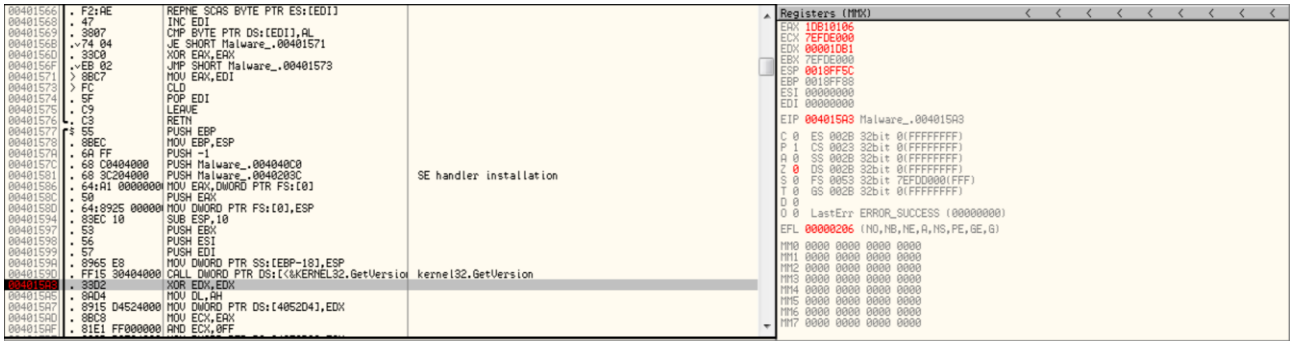
Il comando corrispondente è una stringa : “cmd”



Valore del Registro EDX dopo l'Inserimento di un Breakpoint Software (Indirizzo 004015A3)

È stato inserito un breakpoint software all'indirizzo 004015A3 e successivamente è stato osservato il valore del registro EDX. Questo valore fornisce informazioni utili per comprendere lo stato del programma in quel punto.

Il valore del registro EDX dopo aver effettuato il breakpoint è 00001DB1



Da notare è la funzione al registro di memoria dove abbiamo effettuato il breakpoint. La funzione infatti " XOR EDX, EDX " è una condizione booleana che porta il valore del registro EDX a 0.

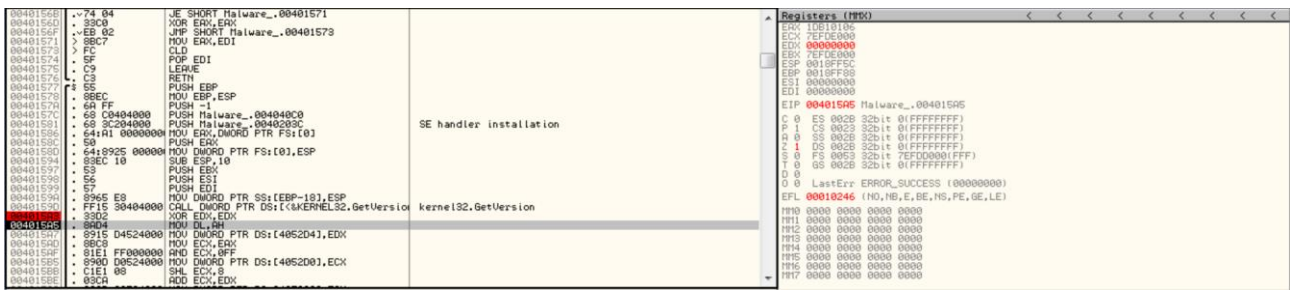
Eseguito il breakpoint a quel determinato punto del programma il valore del registro EDX corrisponde al valore che ha il registro prima di effettuare la funzione "XOR EDX, EDX".

Valore del Registro EDX dopo uno "Step-Into" (Indirizzo 004015A3)

Dopo aver eseguito uno "step-into" dal breakpoint software, è stato verificato il nuovo valore del registro EDX. Questo passaggio è cruciale per comprendere come il malware sta elaborando i dati o le istruzioni in quel punto.

Possiamo subito notare che una volta effettuato lo step-into dopo aver eseguito il breakpoint, il tool ci rimanda alla riga di codice successa a quella del breakpoint. Per cui la funzione "XOR EDX, EDX" è stata eseguita ed il valore del registro EDX è stato aggiornato e corrisponde a:

- EDX 00000000

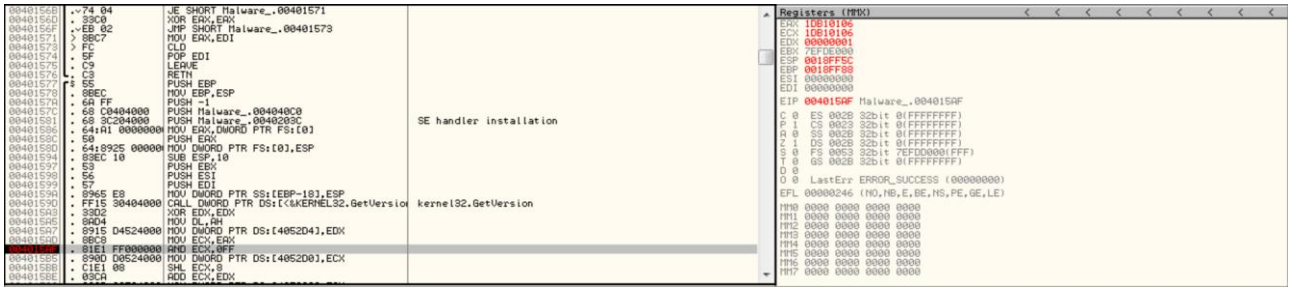


Valore del Registro ECX dopo l'Inserimento di un Breakpoint (Indirizzo 004015AF)

Un secondo breakpoint è stato inserito all'indirizzo di memoria 004015AF per monitorare il valore del registro ECX. Questo indirizzo di memoria corrisponde alla funzione “AND ECX, OFF”

Il procedimento utilizzato è lo stesso di prima. Abbiamo eseguito il breakpoint all’indirizzo di memoria specificato e preso nota del valore del registro ECX che corrisponde a:

- ECX 1DB10106



Valore del Registro ECX dopo uno "Step-Into" (Indirizzo 004015AF)

Dopo aver eseguito uno "step-into" dal secondo breakpoint, è stato osservato il nuovo valore del registro ECX. Il valore del registro ECX è cambiato e corrisponde a :

- ECX 00000006

La funzione AND ECX, OFF è un operazione booleana di confronto bit a bit dove due bit a confronto daranno 1 come risultato solo se si confrontano 1 con 1, tutti gli altri confronti “0 e 1” o “0 e 0” avranno come risultato 0. Di conseguenza per ottenere il valore 00000006 mettendo a confronto il valore che aveva ECX con OFF il valore di OFF sarà uguale a 00000006.

Conclusioni

L'analisi dinamica del malware "Malware_U3_W3_L3" utilizzando OllyDBG ha consentito di rispondere con successo ai quesiti posti. Attraverso l'identificazione dei valori dei registri, l'analisi delle istruzioni eseguite e l'esame dei dati nello stack, è stato possibile ottenere una visione dettagliata del comportamento del malware in esecuzione.

BONUS: Spiegazione a Grandi Linee

Il debugger OllyDBG è uno strumento potente per l'analisi dei malware, consentendo agli analisti di esaminare il comportamento del malware in tempo reale, monitorare lo stato dei registri e delle variabili, e comprendere il flusso di esecuzione del codice. Utilizzando funzionalità come i breakpoint e gli step-into, è possibile eseguire un'analisi dettagliata del malware e rispondere a domande specifiche sulla sua funzionalità e comportamento. Questo approccio dinamico all'analisi dei malware è complementare all'analisi statica e fornisce informazioni cruciali per comprendere appieno le minacce e sviluppare contro-misure efficaci. Purtropo però basandoci su quanto appreso durante l'esercitazione abbiamo capito che il programma crea una shell.

Abbiamo caricato l'hash MD5 del malware su virustotal per avere un idea sul tipo di malware in esame ed è risultato che il file in questione è un Trojan, probabilmente capace di aprire una shell di comandi da remoto.