Epicode
CS-0124
Pratica S11/L3

Francesco Ficetti

1. Traccia

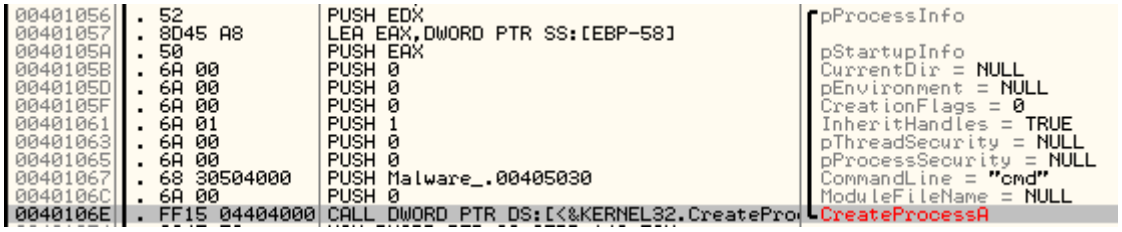
Con riferimento al malware allegato, rispondere ai seguenti quesiti utilizzando OllyDBG:

1. All’indirizzo 0040106E il malware effettua una chiamata alla funzione «CreateProcess». Qual è il valore del parametro “CommandLine” che viene passato sullo stack?
2. Inserire un breakpoint software all’indirizzo 004015A3. Qual è il valore del registro EDX?
   Eseguire uno step-into. Qual è il valore del registro EDX e motivare la risposta. Che istruzione è stata eseguita?
3. Inserire un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX?
   Eseguire uno step-into. Qual è il valore di ECX? Spiegare quale istruzione è stata eseguita.
4. BONUS. Spiegare a grandi linee il funzionamento del malware.

2. Svolgimento

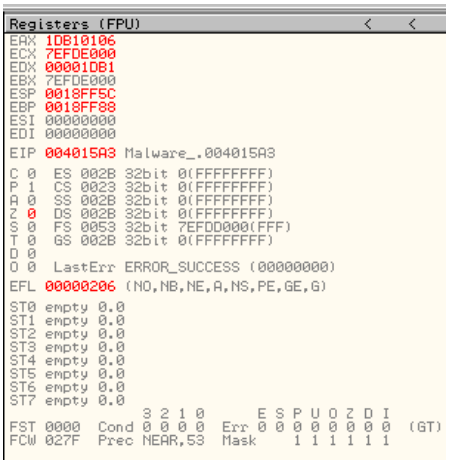
2.1 Parametro “CommandLine”

Il valore del parametro “CommandLine” è “cmd”.

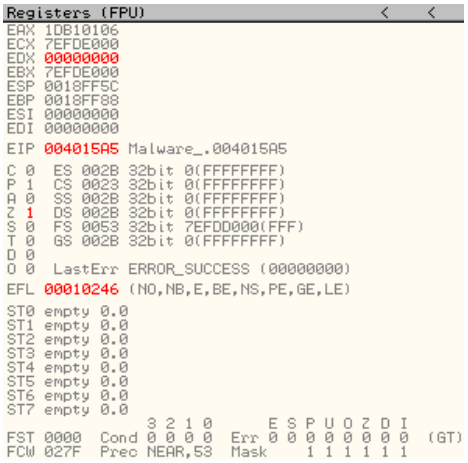


2.2 Registro EDX

Il valore del registro EDX, prima che venga eseguita l’istruzione alla riga 004015A3, è “00001DB1”.



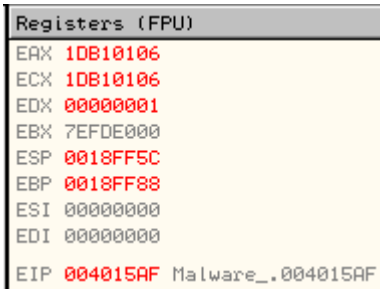
Il valore del registro EDX, dopo che è stata eseguita l’istruzione, è 00000000.



Il valore del registro EDX è *0*, perché è stato effettuato uno *xor* del registro con se stesso. L'operatore logico *xor* restituisce *0*, quando i due valori confrontati sono uguali, confrontando quindi un valore con se stesso, il risultato sarà sempre *0*. Questa operazione viene effettuata quando si vuole azzerare il valore di un registro.

2.3 Registro ECX

Il valore del registro ECX, prima che venga eseguita l'istruzione alla riga 004015AF, è "1DB10106".



Il valore del registro ECX, dopo che è stata eseguita l'istruzione, è 00000006.

Il valore del registro ECX è *6*, perché è stato effettuato un *and* del registro con il numero *0ff*. L'operatore logico and, restituisce 0, se i due valori confrontati sono diversi, 1 se i due valori confrontati sono uguali.

2.4 Funzionamento del malware

Controllando l'hash del file su VirusTotal, viene segnalato che molto probabilmente si tratta di un trojan.