S11L3

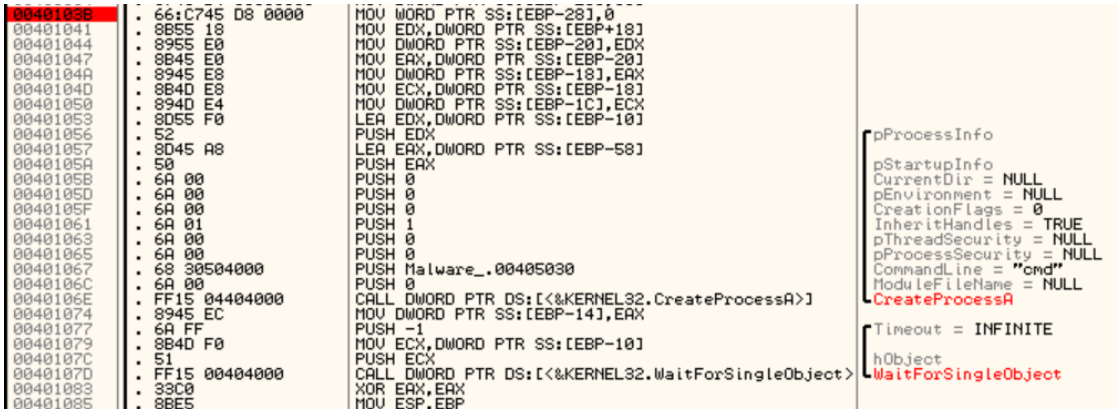
Traccia: Fate riferimento al malware: Malware_U3_W3_L3, presente all'interno della cartella Esercizio_Pratico_U3_W3_L3sul desktop della macchina virtuale dedicata all'analisi dei malware. Rispondete ai seguenti quesiti utilizzando OllyDBG.

1. All'indirizzo 0040106E il Malware Effettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «CommandLine» che viene passato sullo stack?
2. 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)
3. Inserite un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX? (6) Eseguite un step-into. Qual è ora il valore di ECX? (7) Spiegate quale istruzione è stata eseguita (8).
4. BONUS: spiegare a grandi linee il funzionamento del malware.

SVOLGIMENTO:

1. Funzione CreateProcess

All'indirizzo 0040106E il malware effettua una chiamata di funzione alla funzione <CreateProcess>, come mostrato in figura sotto. Da notare i commenti nella colonna di destra immessi dallo stesso programma OllyDBG per una breve descrizione del malware.

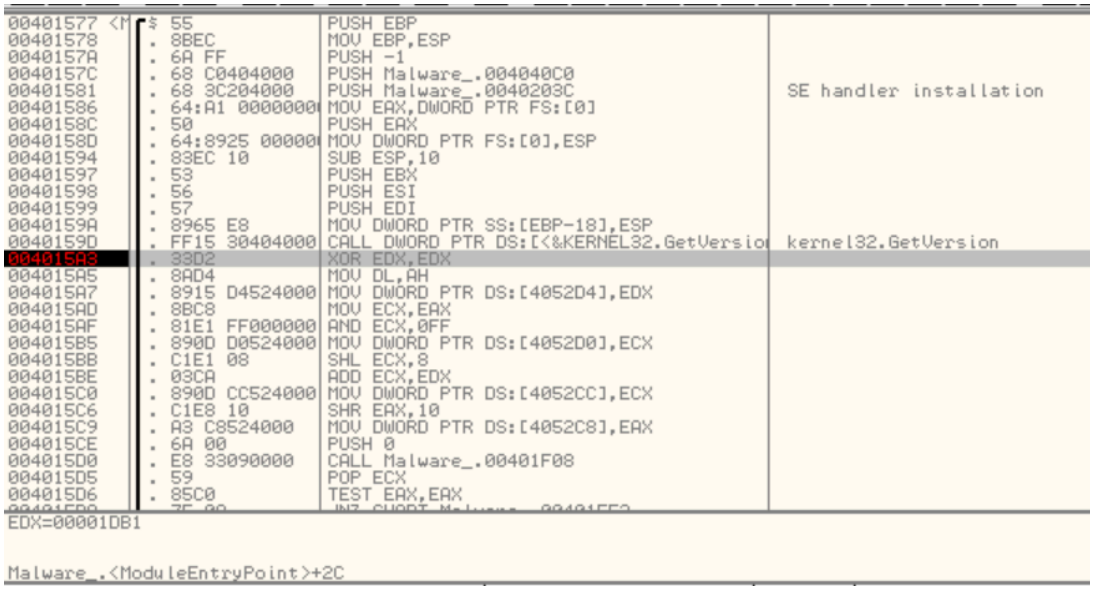


Come si può vedere dalla figura, il valore del parametro <CommandLine> è **cmd**.

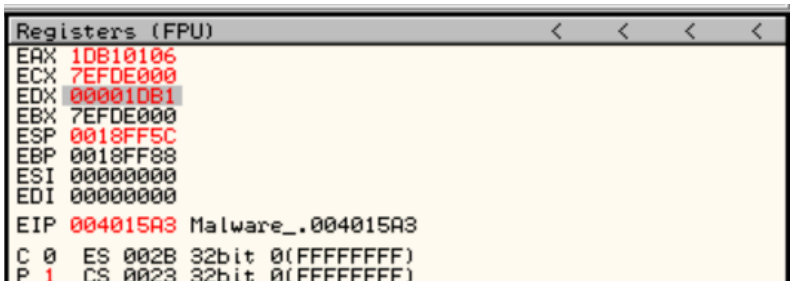
2. Registro EDX

2.1: Qual è il valore del registro EDX?

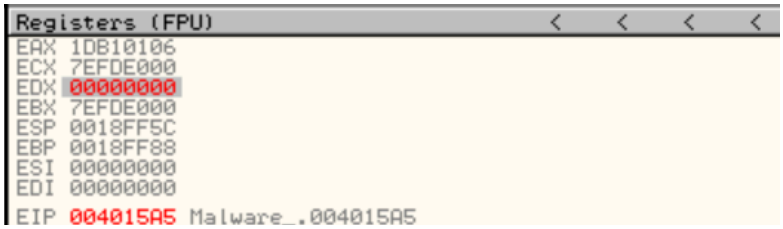
Per questa richiesta è stato inizialmente inserito un breakpoint software (Toggle breakpoint) all'indirizzo 004015A3 e successivamente è stato eseguito il programma.



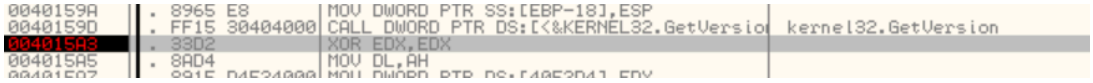
È stato quindi trovato il valore del registro EDX richiesto dall'esercizio, pari a **00001DB1**.



2.2 - 2.3: Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX motivando la risposta. Che istruzione è stata eseguita?
Successivamente è stato eseguito uno <step-into>, utilizzato per esaminare righe di codice e a fronte di una chiamata di funzione accedere alla sua implementazione. Ricontrollando il registro EDX ora si nota che il suo valore è cambiato, come mostrato in figura sotto.



Tale variazione è dovuta all'utilizzo dell'istruzione XOR logico. Tale operazione ritorna in output il valore 1 nel caso in cui i due valori di input siano diversi tra loro. Siccome l'operatore XOR è usato con gli input EDX ed EDX, l'output sarà sempre 0. Da cui il nuovo valore del registro EDX.
Istruzione eseguita: XOR

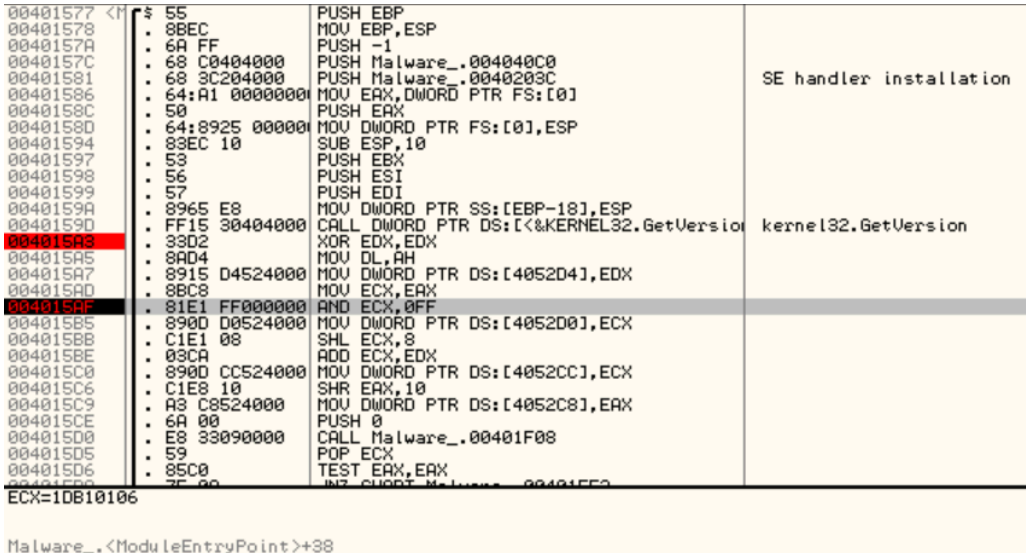


3. Registro ECX

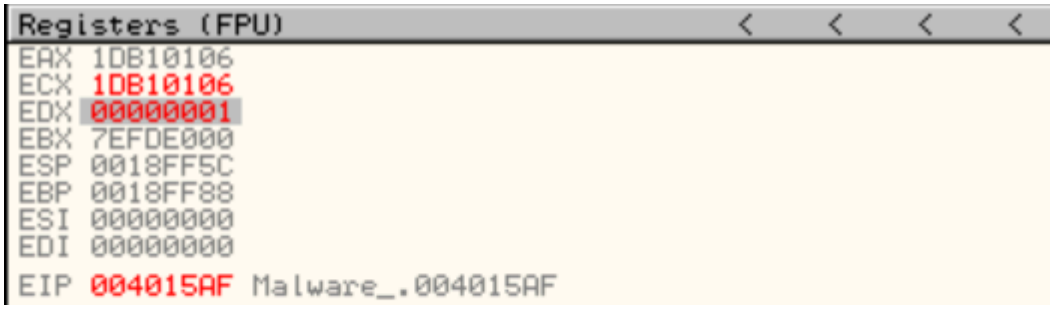
Per le richieste del punto 3 è stato eseguito lo stesso procedimento del punto 2.

3.1: Qual è il valore del registro ECX?

Per questa richiesta è stato inizialmente inserito un breakpoint software (Toggle breakpoint) all'indirizzo 004015AF e successivamente è stato eseguito il programma.

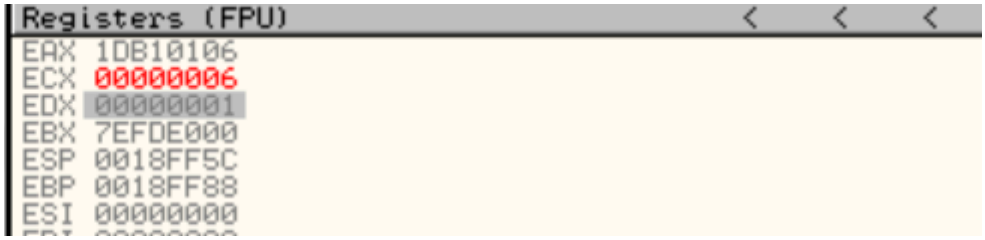


È stato quindi trovato il valore del registro ECX richiesto dall'esercizio, pari a **1DB10106**.

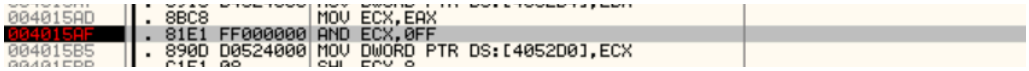


3.2 - 3.3 : Eseguite un step-into. Qual è ora il valore di ECX? Spiegate quale istruzione è stata eseguita.

Successivamente è stato eseguito uno <step-into>, utilizzato per esaminare righe di codice e a fronte di una chiamata di funzione accedere alla sua implementazione. Ricontrollando il registro ECX ora si nota che il suo valore è cambiato, come mostrato in figura sotto.



Tale variazione è dovuta all'utilizzo dell'istruzione AND logico tra il valore del registro ECX ed il numero esadecimale FF.

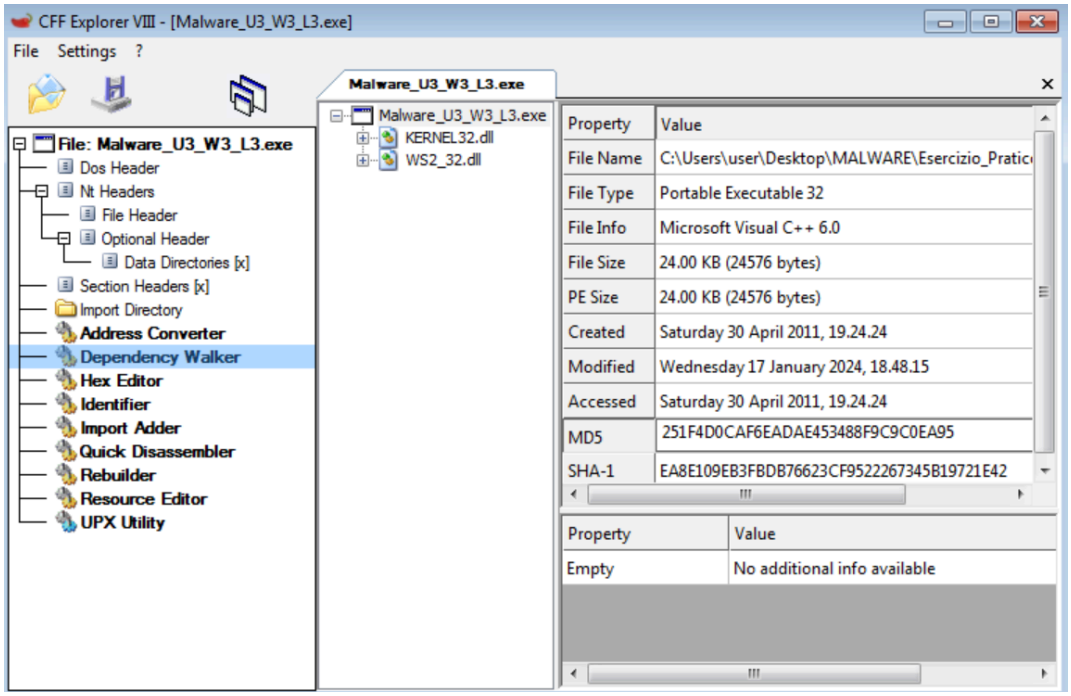


Il nuovo valore del contenuto del registro ECX è il risultato dell'operazione mostrata nella tabella seguente.

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**

Dopo questa analisi dinamica, ci siamo avvalsi di CFF Explorer per confermare le nostre ipotesi. Possiamo infatti intuire che il malware apra una CMD e vediamo con CFF Explorer importi le librerie Kernel32.dll e WS2_32.dll.



Per confermare il tipo di malware, usiamo Virus Total.
Il risultato ottenuto è stata l'identificazione del malware analizzato come un Trojan virus.