Progetto S11-L3

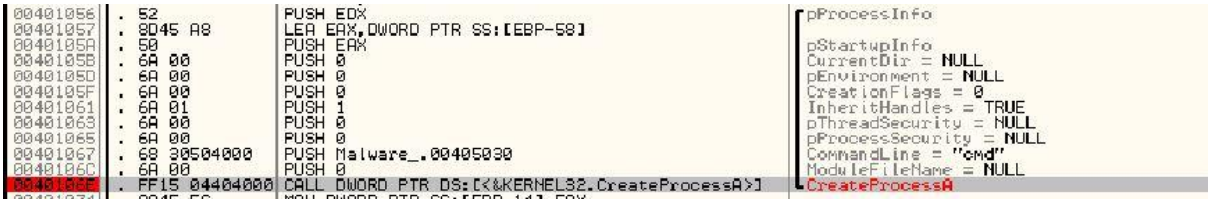
Studente: Simone Mininni

Traccia:

Fate riferimento al malware: **Malware_U3_W3_L3**, presente all'interno della cartella **Esercizio_Pratico_U3_W3_L3** sul desktop della macchina virtuale dedicata all'analisi dei malware. Rispondete ai seguenti quesiti utilizzando OllyDBG.

- 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**? **(1)**
- 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)**
- 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)**.
- BONUS: spiegare a grandi linee il funzionamento del malware

1)



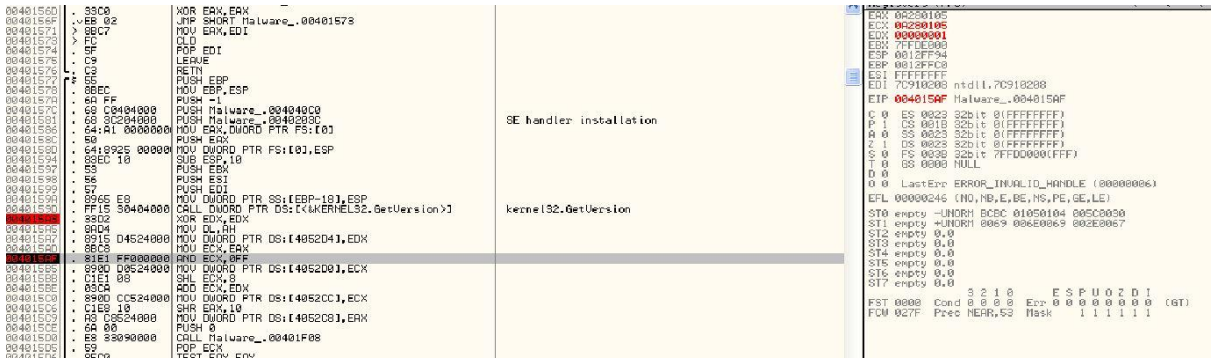
Per la chiamata di funzione CreateProcessA, come parametro commandLine viene passato il valore "cmd"(il command prompt di windows)

2)

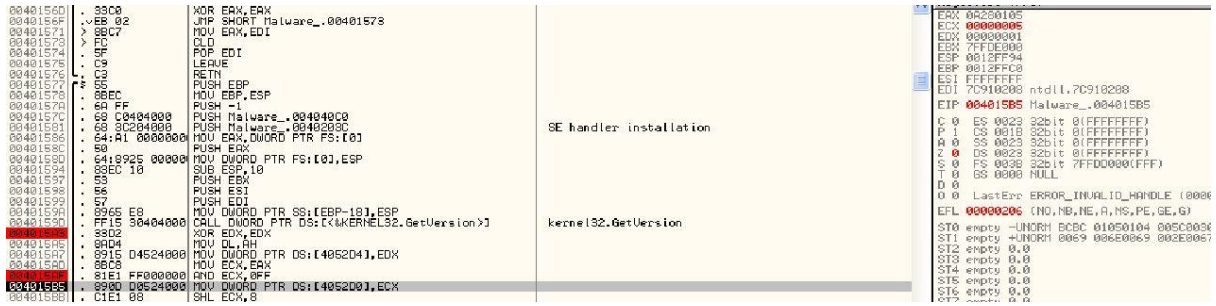
Inizialmente il valore del registro edx è 0x00000A28, dopo l 'istruzione xor edx, edx ,il valore del registro è 0.

L’ istruzione xor mette 1 se i valori confrontati sono diversi, mette 0 se sono uguali, quindi lo xor tra due valori uguali restituirà 0.

3)

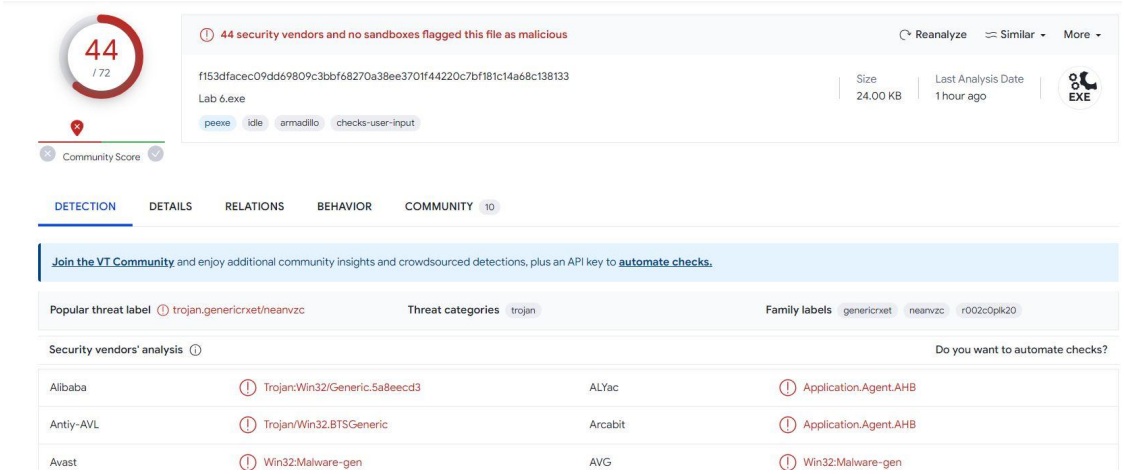


Il valore iniziale contenuto nel registro ecx è 0A280105.
Dopo l ‘istruzione AND il valore restituito è 0x00000005



AND mette 0 se i valori confrontati sono diversi, mette 1 se i valori confrontati sono uguali.

3)
Hash: 251F4D0CAF6EADAE453488F9C9C0EA95 md5
Virus Total:



Si può notare la creazione di un socket.
Quindi, considerando anche la funzione “CreateProcessA”, probabilmente si tratta di una backdoor che sfrutta una reverse shell, collegandosi al server attaccante con “connect”.