Relazione S11L3

Lo scopo dell'esercizio di oggi consiste nell'effettuare l'analisi dinamica avanzata di un malware attraverso l'utilizzo di OllyDBG.
Vengono richiesti i seguenti punti:

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? (1)

Come possiamo vedere dal programma, il parametro CommandLine ha il valore settato a "cmd". Ci viene mostrato tra i vari parametri passati alla funzione.

2. Inserite un breakpointsoftware 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)

Il valore del registro EDX è 00000000 questo perché viene effettuato uno XOR EDX, EDX e lo xor tra due valori uguali torna sempre 0. In pratica viene inizializzato il registro EDX.

3. Inserite un secondo breakpointall'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).

Il valore di ECX inizialmente è 7FFDF000

Al secondo breakpoint invece possiamo vedere che è 0A280105. Quello che vediamo dalle righe del codice assembly è che viene copiato il valore di EAX su ECX e poi viene fatto un AND tra ECX e 0FF e se è vero il valore di ECX viene modificato.

4. BONUS: spiegare a grandi linee il funzionamento del malware

Guardando su VirusTotal e sempre con OllyDBG si capisce che questo è malware è molto probabilmente un trojan che modifica e crea i processi del sistema operativo.

Davide Lecci