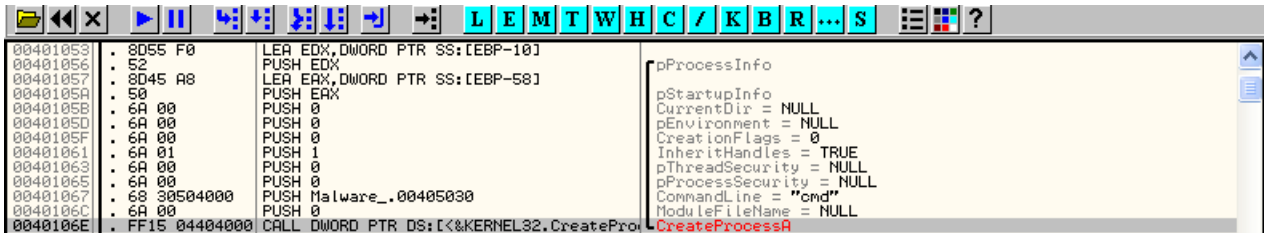
**ANALISI DINAMICA AVANZATA CON OLLYDBG**

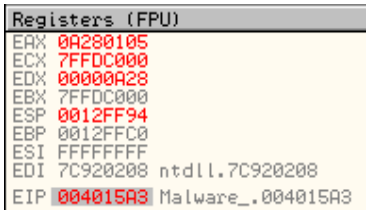
- All'indirizzo 0040106E il Malware effettua una chiamata di funzione alla funzione «CreateProcess». Qual è il valore del parametro «CommandLine» che viene passato sullo stack?
- Inserite un breakpoint software all'indirizzo 004015A3. Qual è il valore del registro EDX? Eseguite a questo punto uno «step-into». Indicate qual è ora il valore del registro EDX, motivando la risposta. Che istruzione è stata eseguita?
- Inserite un secondo breakpoint all'indirizzo di memoria 004015AF. Qual è il valore del registro ECX? Eseguite un step-into. Qual è ora il valore di ECX? Spiegate quale istruzione è stata eseguita.
- BONUS: spiegare a grandi linee il funzionamento del malware.

Nell'esercizio di oggi procediamo con un'analisi dinamica avanzata di un malware tramite il tool OllyDBG.

Il primo quesito richiede si identificare il valore del parametro CommandLine alla chiamata della funzione "CreateProcess". Con OllyDBG ci spostiamo sull'indirizzo di chiamata della funzione e diamo un'occhiata ai push sullo stack che la precedono. Vediamo che il parametro "CommandLIne" assume il valore di "cmd". Ciò significa che quando viene inseito il comando "cmd" veà inseito il codice malevolo.



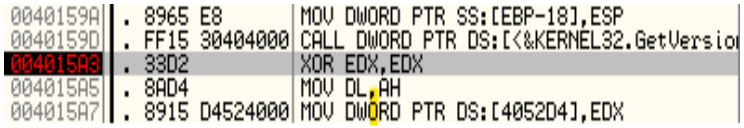

Ci spostiamo alla locazione di memoria 004015A3 e inseriamo qui un breakpoint. Il valore del registro EDX a questo punto è 00000A28 (in decimale 2.600).




Procedendo con lo step-into, il valore di EDX cambierà a 0, in quanto alla locazione 004015A3 avviene un'opeazione logia XOR tra EDX e se stesso; in questi casi il risultato è sempre 0.

00000A28 = 101000101000

| | |
|---|---|
| 101000101000 | XOR |
| 101000101000 | |
| 000000000000 | 0 |





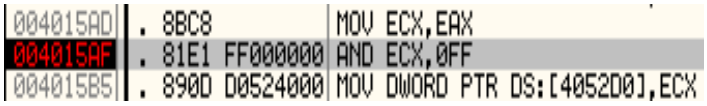
Infine inseriamo un nuovo breakpoint all'indirizzo 004015AF, dove troviamo un altro operatore logico, AND. Il valore del registro ECX è 0A280105 (170.393.861 in decimale).

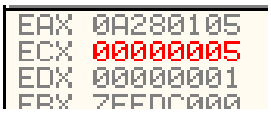

Come detto sopra, ci troviamo davanti ad un'operazione AND tra ECX e 0FF, l'esadecimale per 255; l'operatore AND compare i due valori nella loro forma binaria e salva il risultato nel registro ECX, il cui nuovo valore sarà 5.

0A280105 = 10100010100000000000100000101

0FF = 11111111

| | |
|---|---|
| 10100010100000000000100000101 | AND |
| 00000000000000000000011111111 | |
| 00000000000000000000000000101 | 5 |




Il malware usa la funzione WSAStartup (indirizzo 00401265), quindi sicuramente si connette alla rete, crea un socket e ottiene l'indirizzo IP della macchina target.

Guardando le funzioni presenti, sembra che possa anche aprire file dal file system e creare heap sulla RAM.