

MALWARE ANALYSIS

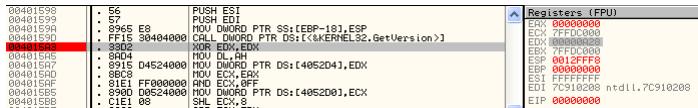
ANALISI AVANZATA

04-05-2023

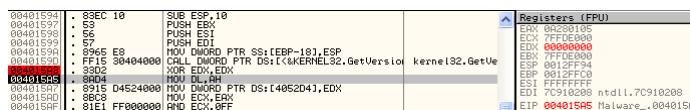
Il valore del parametro `CommandLine` passato allo stack è successivamente alla funzione `CreateProcessA` è "cmd" ovvero il comando per ottenere il controllo di una shell su windows.



Mettendo un breakpoint all'indirizzo "004015A3" possiamo notare come il valore dei suoi registri EH ed EL siano rispettivamente "0A" e "28".



Ma eseguendo uno "step-into" otteniamo come valore 0 in tutti i bit dato che la comparazione logica bit a bit XOR applicata a due oggetti simili da come risultato 0.



In questo caso la comparazione logica bit a bit è stata effettuata con l'operatore AND che scomponete i numeri dei registri in codice binario e restituendo 1 solo se i bit dei due numeri in corrispondenza d'ordine sono uguali, in questo caso il risultato dell'operazione è 000000000000101 che tradotto in decimale si riassume nel contenuto del registro ECX della seconda immagine.



BONUS

Probabilmente il malware in questione è del tipo Backdoor o al massimo Dos data la grande mole di funzioni volte alla connessione,

soprattutto la struttura suggerisce questo dato che come mostrato sotto si può notare la creazione ricorsiva di richieste web con un tempo di riposo del programma probabilmente per non farlo individuare dagli anti-malware, quindi secondo me il codice riportato sotto rappresenta una struttura beacon like con un tempo di intervallo prestabilito con cui comunica probabilmente inviando richieste get più volte al secondo ad un server remoto in cui l'attaccante carica i comandi da lanciare nella macchina vittima , un'ulteriore prova è il fatto che il programma richiede specifiche di sistema ed apre una sessione di Command Line probabilmente fornendo accesso remoto all'attaccante.

