Report sull'analisi del malware "Malware_U3_W3_L3"

Introduzione

In questa esercitazione ho analizzato il malware "Malware_U3_W3_L3" utilizzando OllyDBG, un debugger per Windows. L'obiettivo era rispondere a specifiche domande riguardanti l'esecuzione e i registri durante il funzionamento del malware. La cartella contenente il malware si trova sul desktop della macchina virtuale dedicata all'analisi dei malware, sotto il nome "Esercizio_Pratico_U3_W3_L3".

Domanda 1: Valore del parametro "CommandLine" passato alla funzione CreateProcess

Procedura:

1. Ho aperto OllyDBG e caricato il malware "Malware_U3_W3_L3".
2. Ho navigato all'indirizzo 0040106E utilizzando il comando "Ctrl+G".
3. Ho impostato un breakpoint all'indirizzo 0040106E premendo F2.
4. Ho eseguito il programma fino al raggiungimento del breakpoint premendo F9.
5. Una volta raggiunto il breakpoint, ho esaminato lo stack per individuare il valore del parametro "CommandLine" passato alla funzione CreateProcess.

Risultato:

Il valore del parametro "CommandLine" passato alla funzione CreateProcess è "CMD". Questo parametro è visibile nello stack all'indirizzo 00401067, come mostrato nella figura sottostante:

Domanda 2: Valore del registro EDX all'indirizzo 004015A3 prima dell'esecuzione

Procedura:

1. Ho rimosso il precedente breakpoint e navigato all'indirizzo 004015A3.
2. Ho impostato un breakpoint all'indirizzo 004015A3 premendo F2.
3. Ho eseguito il programma fino al raggiungimento del breakpoint.
4. Ho osservato il valore del registro EDX nella finestra "Registers" di OllyDBG.

Risultato:

Il valore del registro EDX prima di eseguire l'istruzione all'indirizzo 004015A3 era 00000A28.

Domanda 3: Valore del registro EDX dopo l'esecuzione dello "step-into" e istruzione eseguita

Procedura:

1. Con il breakpoint all'indirizzo 004015A3 attivo, ho eseguito uno "step-into" premendo F7.
2. Ho osservato nuovamente il valore del registro EDX nella finestra "Registers".
3. Ho identificato l'istruzione eseguita.

Risultato:

Dopo l'istruzione "XOR EDX, EDX", il valore del registro EDX è diventato 0. Questa istruzione viene utilizzata per azzerare il registro EDX.

Domanda 4: Valore del registro ECX all'indirizzo 004015AF prima dell'esecuzione

Procedura:

1. Ho navigato all'indirizzo 004015AF e impostato un breakpoint.
2. Ho eseguito il programma fino al raggiungimento del breakpoint.
3. Ho osservato il valore del registro ECX nella finestra "Registers".

Risultato:

Il valore del registro ECX prima di eseguire l'istruzione all'indirizzo 004015AF era 0A280105.

Domanda 5: Valore del registro ECX dopo l'esecuzione dello "step-into" e istruzione eseguita

Procedura:

1. Con il breakpoint all'indirizzo 004015AF attivo, ho eseguito uno "step-into" premendo F7.
2. Ho osservato nuovamente il valore del registro ECX nella finestra "Registers".
3. Ho identificato l'istruzione eseguita.

Risultato:

Dopo l'istruzione "AND ECX, FF", il valore del registro ECX è stato modificato in 00000005. Questa istruzione esegue un AND logico tra il valore corrente di ECX e il valore esadecimale FF, mantenendo solo l'ultimo byte del registro.

Dettagli dell'Istruzione "AND ECX, FF":

1. Ho convertito i valori in formato binario:
    - 0A280105 -> 0000 1010 0010 1000 0000 0000 0000 0101
    - FF -> 0000 0000 0000 0000 0000 0000 1111 1111
2. Ho eseguito l'AND logico bit a bit:
    - 0000 1010 0010 1000 0000 0000 0000 0101 AND 0000 0000 0000 0000 0000 0000 1111 1111 = 0000 0000 0000 0000 0000 0000 0000 0101
3. Il risultato in esadecimale è 00000005.

Conclusioni

Attraverso questa esercitazione, ho imparato a utilizzare OllyDBG per analizzare il comportamento del malware "Malware_U3_W3_L3". Ho osservato come il malware utilizza la funzione CreateProcess per eseguire il comando "CMD" e come manipola i registri EDX ed ECX durante l'esecuzione. Questa esperienza mi ha permesso di comprendere meglio le tecniche utilizzate dai malware per eseguire operazioni malevole e come possiamo analizzarle utilizzando strumenti di debugging.