Bonus S11-L5

Traccia:

Analizzare il file **C: \Users\user\Desktop \Software Malware analysis\SysinternalsSuite \Tcpvcon.exe** con IDA Pro Analizzare SOLO la "funzione corrente" una volta aperto IDA La funzione corrente la visualizze con il tasto F12 oppure con il tasto blu indicato nella slide successiva.
Esercizio Traccia e requisiti Se necessario, reperire altre informazioni con OllyDBG oppure effettuando ulteriori analisi con IDA (o altri software). Mi interessa soltanto il significato/funzionamento/senso di questa parte di codice visualizzato alla pagina successiva.

Descrizione Generale:

La funzione **main** nel file eseguibile **Tcpvcon.exe** gestisce il processo di avvio dell'applicazione, comprendendo l'inizializzazione delle risorse necessarie e l'elaborazione degli argomenti passati al programma.
La funzione è suddivisa in diverse sezioni, ciascuna responsabile di operazioni specifiche, come la gestione della memoria, la preparazione degli argomenti per altre funzioni, e l'inizializzazione delle componenti di rete.

Dettagli Tecnici:

1) Inizializzazione dello Stack e delle Variabili:

- La funzione alloca spazio sullo **stack** per variabili locali e salva i registri di base. Viene utilizzata un'operazione di XOR tra eax e ebp per inizializzare una variabile locale, probabilmente per offuscare o proteggere il valore.

```
push    ebp
mov     ebp, esp
sub     esp, 19Ch
mov     eax, dword_4272B4
xor     eax, ebp
mov     [ebp+var_4], eax
```

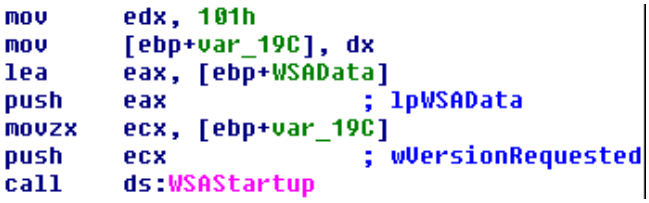
2) Preparazione degli Argomenti e Chiamate di Funzione:

- La funzione carica gli argomenti della linea di comando (**argv, argc**) e prepara una stringa "TCPview" per una funzione chiamata sub_420CE0. Questo suggerisce che la funzione principale sta preparando la configurazione per un componente o modulo chiamato TCPview.

```
mov     eax, [ebp+argv]
push    eax             ; int
lea     ecx, [ebp+argc]
```

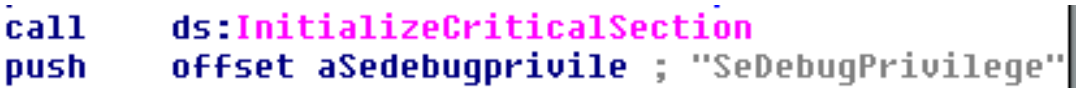
3) Inizializzazione di WinSock:

- La funzione procede con l'inizializzazione della libreria WinSock, necessaria per le operazioni di rete. Viene chiamata WSAStartup, e se l'inizializzazione fallisce, viene gestito un errore specifico.



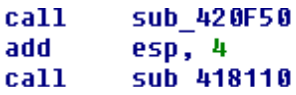
4) Gestione delle Sezioni Critiche e Privilegi di Debug:

- Viene configurata una sezione critica tramite InitializeCriticalSection, utile per la sincronizzazione in ambienti multi-thread. Inoltre, la funzione tenta di acquisire privilegi di debug, il che potrebbe suggerire che l'applicazione richiede operazioni con privilegi elevati.



5) Esecuzione di Altre Funzioni:

- La funzione main include ulteriori chiamate a funzioni come sub_41BB90 e sub_41A380, che probabilmente gestiscono ulteriori configurazioni o inizializzazioni necessarie per il funzionamento completo dell'applicazione.



In sintesi, la funzione **main** di **Tcpvcon.exe** è principalmente dedicata all'**inizializzazione** delle risorse di sistema e alla **preparazione** degli argomenti e delle **configurazioni** necessarie per il funzionamento dell'applicazione, in particolare in relazione alle operazioni di rete.
L'uso di funzioni di basso livello per la gestione delle sezioni critiche e dei privilegi suggerisce che il programma potrebbe essere destinato a operazioni avanzate o critiche, potenzialmente con capacità di supervisione o monitoraggio di reti.