

S11-L3



Traccia: La figura nella slide successiva mostra un estratto del codice di un malware. Identificate:

1. Il tipo di Malware in base alle chiamate di funzione utilizzate. Esercizio Funzionalità Malware
2. Evidenziate le chiamate di funzione principali aggiungendo una descrizione per ognuna di essa
3. Il metodo utilizzato dal Malware per ottenere la persistenza sul sistema operativo
4. BONUS: Effettuare anche un'analisi basso livello delle singole istruzioni

```
.text:00401010    push eax  
.text:00401014    push ebx  
.text:00401018    push ecx  
.text:0040101C    push WH_Mouse ; hook to Mouse  
[red box] .text:0040101F    call SetWindowsHook()  
.text:00401040    XOR ECX,ECX  
.text:00401044    mov ecx, [EDI] ; EDI = <path to startup_folder_system>  
.text:00401048    mov edx, [ESI] ; ESI = path_to_Malware  
.text:0040104C    push ecx ; destination folder  
.text:0040104F    push edx ; file to be copied  
[red box] .text:00401054    call CopyFile()
```

Sulla base delle due chiamate a funzione evidenziate nel codice questo malware può essere classificato principalmente come malware persistente con potenziali funzionalità di keylogger. L'obiettivo principale è rimanere attivo sul sistema grazie alla persistenza ottenuta tramite la copia nella cartella di avvio e potenzialmente monitorare o intercettare l'attività dell'utente.

Il malware effettua due chiamate a funzione principali:

- SetWindowsHook() : questa funzione viene utilizzata per installare una procedura di hook che monitora eventi del sistema, come i movimenti del mouse o gli input da tastiera. In questo caso, viene effettuata una chiamata con WH\_MOUSE come parametro, il che indica che il malware sta installando un hook per monitorare o intercettare gli eventi del mouse.
- CopyFile() : questa funzione viene utilizzata per copiare un file da una posizione a un'altra. Nel codice, i parametri passati a questa funzione includono il percorso del malware (indicato da ESI) e la destinazione, che è una cartella di avvio del sistema (indicato da EDI). Questo è un comportamento tipico dei malware che cercano di ottenere persistenza, copiando se stessi in una posizione che garantisce l'esecuzione automatica all'avvio del sistema.

Per ottenere la persistenza il malware copia sè stesso nella cartella di avvio, questa è una cartella speciale su Windows dove i file o collegamenti presenti vengono eseguiti automaticamente quando l'utente accede o il sistema viene avviato. Copiando il file del malware in questa cartella, il malware si assicura di essere eseguito ogni volta che il sistema viene avviato.

push eax	salva il contenuto del registro EAX nello stack
push ebx	salva il contenuto del registro EBX nello stack
push ecx	salva il contenuto del registro ECX nello stack
push WH_Mouse	Mette il parametro WH_MOUSE nello stack
call SetWindowsHook()	Chiama la funzione SetWindowsHook(), che installa un hook di sistema L'hook permette al malware di intercettare gli eventi del mouse
XOR ECX,ECX	Esegue uno XOR sul registro ECX con se stesso per azzerarlo
mov ecx, [EDI]	Carica il valore memorizzato nell'indirizzo di memoria puntato da EDI nel registro ECX
mov edx, [ESI]	Carica il valore memorizzato nell'indirizzo di memoria puntato da ESI nel registro EDX
push ecx	Mette il valore di ECX nello stack
push edx	Mette il valore di ECX nello stack
call CopyFile()	Chiama la funzione CopyFile() che copia un file da una sorgente a una destinazione. In questo caso, il malware copia se stesso nella cartella di avvio del sistema, garantendo così la persistenza