S11 L4

Report Esercizio Malware Analysis

GiuliaSalani

INDICE

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.
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

```
push eax
push ebx
push ecx
push WH_Mouse                ; hook to Mouse
call SetWindowsHook()
XOR ECX, ECX
mov ecx, [EDI]               EDI = "path to startup_folder_system"
mov edx, [ESI]               ESI = path_to_Malware
push ecx                     ; destination folder
push edx                     ; file to be copied
call CopyFile();
```

SVOLGIMENTO

QUESITO 1

Il tipo di Malware in base alle chiamate di funzione utilizzate.

È possibile identificare il tipo di Malware dalla funzione SetWindowsHook: si tratta di un keylogger che utilizza, appunto, il metodo (o funzione) chiamato «hook». Tale metodo è dedicato al monitoraggio degli eventi di una data periferica, in questo caso il mouse. Il metodo «hook» verrà allertato ogni qualvolta l'utente utilizzerà il mouse:

```
push eax
push ebx
push ecx
push WH_Mouse              ; hook to Mouse
call SetWindowsHook()
XOR ECX, ECX
mov ecx, [EDI]             EDI = "path to startup_folder_system"
mov edx, [ESI]             ESI = path_to_Malware
push ecx                   ; destination folder
push edx                   ; file to be copied
call CopyFile();
```

QUESITO 2

Evidenziate le chiamate di funzione principali aggiungendo una descrizione per ognuna di essa

Le chiamate di funzione sono due e sono evidenziate di seguito, lo capiamo dal fatto che sono precedute dall'istruzione "call":

```
push eax
push ebx
push ecx
push WH_Mouse              ; hook to Mouse
call SetWindowsHook()
XOR ECX, ECX
mov ecx, [EDI]             EDI = "path to startup_folder_system"
mov edx, [ESI]             ESI = path_to_Malware
push ecx                   ; destination folder
push edx                   ; file to be copied
call CopyFile();
```

SetWindowsHook:

La funzione SetWindowsHook è una funzione di Windows API utilizzata per installare un hook di sistema o di applicazione. Gli hooks sono procedure che vengono chiamate automaticamente quando si verificano eventi specifici nel sistema o in un'applicazione. In questo caso si tratta di un hook del mouse (WH_Mouse), che consente di intercettare e gestire gli eventi del mouse come clic, movimenti, etc.
Il parametro della funzione è "WH_Mouse".

CopyFile:
La funzione CopyFile è una funzione di Windows API utilizzata per copiare un file da una posizione a un'altra. Accetta due parametri: il percorso del file da copiare e il percorso di destinazione in cui copiare il file. In questo frammento di codice, la funzione CopyFile viene chiamata con i percorsi del file sorgente (edx, o "path_to_Malware") e della cartella di destinazione (ecx, o "path to startup_folder_system").
Il malware sta cercando di copiare se stesso in una posizione specifica, ad esempio la cartella di avvio del sistema, per assicurarsi che venga eseguito all'avvio del sistema.

QUESITO 3

Il metodo utilizzato dal Malware per ottenere la persistenza sul sistema operativo

Il metodo è evidenziato di seguito in arancione:

```
push eax
push ebx
push ecx
push WH_Mouse              ; hook to Mouse
call SetWindowsHook()
XOR ECX, ECX
mov ecx, [EDI]             EDI = "path to startup_folder_system"
mov edx, [ESI]             ESI = path_to_Malware
push ecx                   ; destination folder
push edx                   ; file to be copied
call CopyFile();
```

Con queste istruzioni il malware sta copiando il proprio file (path_to_Malware) nella cartella di startup del sistema (path to startup_folder_system). Esegue l'istruzione con la chiamata di funzione CopyFile. In questo modo, ad ogni avvio del sistema si avvierà anche il malware.

QUESITO 4 - BONUS

Effettuare anche un'analisi basso livello delle singole istruzioni

push eax		Salva nello stack il valore del registro "eax".
push ebx		Salva nello stack il valore del registro "ebx".
push ecx		Salva nello stack il valore del registro "ecx".
push WH_Mouse	; hook to Mouse	Salva nello stack il valore associato all'hook del mouse, che sarà il parametro della successiva funzione.
call SetWindowsHook()		Chiama la funzione SetWindowsHook(). Questa funzione installa un hook per intercettare eventi del mouse.
XOR ECX, ECX		Azzera il registro "ecx".
mov ecx, [EDI]	EDI = "path to startup_folder_system"	Sposta il valore a cui punta il registro "edi" nel registro "ecx".
mov edx, [ESI]	ESI = path_to_Malware	Sposta il valore a cui punta il registro "esi" nel registro "edx".
push ecx	; destination folder	Salva il valore nel registro ecx (il "destination folder") nello stack.

push edx	; file to be copied	Salva il valore nel registro edz (il "file to be copied") nello stack.
call CopyFile();		Chiama la funzione “CopyFile”.