Funzionalità del Malware

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

Figura 1:

.text: 00401010	push eax	
.text: 00401014	push ebx	
.text: 00401018	push ecx	
.text: 0040101C	push WH_Mouse	; hook to Mouse
.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
.text: 00401054	call CopyFile();	

1) In base alle funzioni il malware lo possiamo identificare come → Keylogger

è presente un SetWindows**Hook** per monitorare gli eventi e il mouse, copiando i file nella cartella di avvio del sistema

2) Vengono chiamate le funzioni SetWindowsHook e CopyFile

CopyFile → copia edx(path Malware) in ecx(cartella di avvio)

SetWindowsHook → Esegue la cattura degli eventi

3)Il metodo
il file viene copiato nella cartella di avvio del sistema, facendo in modo che verrà eseguito in automatico all'avvio del sistema

4)BONUS

```
push eax
push ebx
push ecx
```

Il valore viene salvato nello stack

```
push WH_Mouse   ; hook to Mouse
```

```
call SetWindowsHook()
```

Il valore di Wh_mouse verrà salvato nello stack, parametro per la funzione SetWindowshook

```
XOR ECX, ECX
```

Azzera il registro ecx.

```
Call CopyFile
```

esegue la copia del file

```
mov ecx, [EDI] ; EDI = <<path to startup_folder_system>>
```

```
mov edx, [ESI] ; ESI = path_to_Malware
```

I percorsi degli indirizzi puntati vengono copiati

```
push ecx ; cartella di destinazione
```

```
push edx ; file da copiare
```

I parametri vengono salvati sullo stack per la funzione CopyFile