PHANTOM s.r.l
IMPOSSIBLE IS OUR TARGET

PHANTOM SRL

Report

Prepared by

Pignatello Giuseppe
D'Ottavio Alessio
Iannone Luca

INDICE

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

```
.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();
```

TIPO DI MALWARE

DATO IL CODICE ASSEMBLY FORNITO E LE SUE CARATTERISTICHE, L'IPOTESI PIÙ PROBABILE È CHE SI TRATTI DI UN KEYLOGGER, PRINCIPALMENTE DA DUE FATTORI:

INSTALLAZIONE DI UN HOOK DI SISTEMA PER IL MOUSE: LA PRESENZA DI ISTRUZIONI CHE SEMBRANO INSTALLARE UN HOOK DI SISTEMA PER MONITORARE GLI EVENTI DEL MOUSE È UNA CARATTERISTICA COMUNE NEI KEYLOGGER. QUESTO TIPO DI FUNZIONALITÀ CONSENTE AL MALWARE DI INTERCETTARE LE AZIONI DELL'UTENTE, COME CLIC DEL MOUSE E MOVIMENTI, PER RUBARE INFORMAZIONI SENSIBILI COME LE PASSWORD O I DETTAGLI DELLA CARTA DI CREDITO.

ATTIVITÀ DI COPIA DEI FILE: ANCHE SE IL CODICE NON FORNISCE DETTAGLI SPECIFICI SUL MOTIVO DELLA COPIA DEI FILE, QUESTA AZIONE È SPESSO ASSOCIATA AI KEYLOGGER CHE POSSONO SCARICARE E INSTALLARE COMPONENTI AGGIUNTIVI, MODIFICARE I FILE DI SISTEMA O RUBARE DATI DA UN COMPUTER INFETTO.

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

PERSISTENZA

NEL CODICE PROPOSTO LA PERSISTENZA LA TROVIAMO IN 2 PUNTI DIVERSI:

.TEXT: 0040101C PUSH WH_MOUSE ; HOOK TO MOUSE
.TEXT: 0040101F CALL SETWINDOWSHOOK()

QUESTI DUE COMANDI FANNO PARTE DI UNA PROCEDURA DI INIZIALIZZAZIONE CHE IMPOSTA UN HOOK DI WINDOWS PER CATTURARE EVENTI DEL MOUSE. SE QUESTO HOOK VIENE CORRETTAMENTE STABILITO, IL PROGRAMMA MALWARE POTREBBE ESSERE ESEGUITO OGNI VOLTA CHE SI VERIFICA UN EVENTO DEL MOUSE, PERMETTENDO COSÌ ALLA SUA FUNZIONALITÀ DI ESSERE PERSISTENTE.

INOLTRE, POTREBBE ESSERCI UNA PERSISTENZA AGGIUNTIVA ATTRAVERSO OPERAZIONI DI COPIA DEL FILE. IL CODICE SI PREPARA PER COPIARE UN FILE SPECIFICATO DA PATH_TO_MALWARE IN UNA POSIZIONE SPECIFICATA DA PATH TO STARTUP_FOLDER_SYSTEM. SE IL FILE COPIATO VIENE ESEGUITO ALL'AVVIO DEL SISTEMA O IN ALTRE CONDIZIONI SPECIFICHE, CIÒ POTREBBE GARANTIRE UNA FORMA DI PERSISTENZA DEL MALWARE.

UNA POSSIBILE STRATEGIA DI PERSISTENZA POTREBBE COINVOLGERE LA CREAZIONE DI UN PROGRAMMA DI INSTALLAZIONE O UN'ENTRATA NELL'HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN (NEL REGISTRO DI SISTEMA DI WINDOWS) CHE ASSICURI CHE IL MALWARE VENGA ESEGUITO OGNI VOLTA CHE IL SISTEMA VIENE AVVIATO.

```
.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();
```

TRACCIA BONUS

IL CODICE FORNITO È UN FRAMMENTO DI CODICE ASSEMBLY CHE È SICURAMENTE PARTE DI UN PROGRAMMA PIÙ GRANDE. ECCO UNA RILEVAZIONE A BASSO LIVELLO DEL CODICE:

PREPARAZIONE PER L'HOOKING DI WINDOWS:

LE ISTRUZIONI PUSH EAX, PUSH EBX, E PUSH ECX METTONO I VALORI DEI REGISTRI EAX, EBX, E ECX NELLO STACK. QUESTO POTREBBE ESSERE NECESSARIO PER SALVARE I VALORI DEI REGISTRI PRIMA DI MODIFICARLI IN SEGUITO NEL CODICE.
LE ISTRUZIONI PUSH WH_MOUSE E CALL SETWINDOWSHOOK() FANNO PARTE DELLA PREPARAZIONE PER L'HOOKING DI WINDOWS PER CATTURARE EVENTI DEL MOUSE.

COPIA DI FILE:

L'ISTRUZIONE XOR ECX, ECX IMPOSTA IL REGISTRO ECX A ZERO.
LE ISTRUZIONI MOV ECX, [EDI] E MOV EDX, [ESI] CARICANO I PERCORSI DEI FILE DI DESTINAZIONE E DI ORIGINE RISPETTIVAMENTE.
LE ISTRUZIONI PUSH ECX E PUSH EDX METTONO I PERCORSI DEI FILE NELLO STACK, CHE VENGONO USATI PER LA SUCCESSIVA CHIAMATA A UNA FUNZIONE DI COPIA FILE.

```
.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();
```

PHANTOM s.r.l

IMPOSSIBLE IS
OUR TARGET

GRAZIE

BY PHANTOM SRL

Prepared by

Pignatello Giuseppe
D'Ottavio Alessio
Iannone Luca