

Report  
Task

Con riferimento agli estratti di un malware reale presenti nelle prossime slide, rispondere alle seguenti domande:

- 1 ☐ Descrivere come il malware ottiene la persistenza, evidenziando il codice assembly dove le relative istruzioni e chiamate di funzioni vengono eseguite
- 2 ☐ Identificare il client software utilizzato dal malware per la connessione ad Internet
- 3 ☐ Identificare l'URL al quale il malware tenta di connettersi ed evidenziare la chiamata di funzione che permette al malware di connettersi ad un URL

1)Proviamo a

descrivere come il Malware ottiene la persistenza ,con le istruzioni e chiamate di funzioni che vengono eseguite di sotto riporto il codice.

```
0040286F push 2 ; samDesired
00402871 push eax ; ulOptions
00402872 push offset SubKey ; "Software\\Microsoft\\Windows\\CurrentVersion\\Run"
00402877 push HKEY_LOCAL_MACHINE ; hKey
0040287C call esi ; RegOpenKeyExW
0040287E test eax, eax
00402880 jnz short loc_4028C5
00402882
00402882 loc_402882:
00402882 lea ecx, [esp+424h+Data]
00402886 push ecx ; lpString
00402887 mov bl, 1
00402889 call ds:strlenW
0040288F lea edx, [eax+eax+2]
00402893 push edx ; cbData
00402894 mov edx, [esp+428h+hKey]
00402898 lea eax, [esp+428h+Data]
0040289C push eax ; lpData
0040289D push 1 ; dwType
0040289F push 0 ; Reserved
004028A1 lea ecx, [esp+434h+ValueName]
004028A8 push ecx ; lpValueName
004028A9 push edx ; hKey
004028AA call ds:RegSetValueExW
```

In rosso possiamo vedere quale e la chiave di registro viene utilizzata dal malware per ottenere la persistenza.

Notiamo 2 Chiamate :1call esi ; RegOpenKeyexw → questa funzione viene usata per aprire la chiave e permette le modifiche.2 chiama :call ds: RegSetValueExW → quest funzione permette di aggiungere un nuovo valore all'interno del registro e di settare i rispettivi dati

In viola vediamo quale chiave viene modificata.

2)Indichiamo il software utilizzata dal malware per la connessione al internet .

```

t:00401150
t:00401150 ; DWORD __stdcall StartAddress(LPVOID)
t:00401150 StartAddress proc near ; DATA XREF: sub_401040+EC70
t:00401150 push esi
t:00401151 push edi
t:00401152 push 0 ; dwFlags
t:00401154 push 0 ; lpszProxyBypass
t:00401156 push 0 ; lpszProxy
t:00401158 push 1 ; dwAccessType
t:0040115A push offset szAgent ; "Internet Explorer 8.0"
t:0040115F call ds:InternetOpenA
t:00401165 mov edi, ds:InternetOpenUrlA
t:00401168 mov esi, eax
t:0040116D loc_40116D: ; CODE XREF: StartAddress+304j
t:0040116D push 0 ; dwContext
t:0040116F push 80000000h ; dwFlags
t:00401174 push 0 ; dwHeadersLength
t:00401176 push 0 ; lpszHeaders
t:00401178 push offset szUrl ; "http://www.malware12.COM"
t:0040117D push esi ; hInternet
t:0040117E call edi ; InternetOpenUrlA
t:00401180 jmp short loc_40116D
t:00401180 StartAddress endp
t:00401180
t:00401180 - -----

```

In blu ho sottolineato il software utilizzato dal malware → Internet Explorer 8.0

e la chiamata alla funzione :call ds:InternetOpenA → Questa funzione viene utilizzata per iniziare una connessione a Internet.

3)Indicare il URL e la chiama che lo permette .

In rosso ho sottolineato il Url della :°<http://www.malware12.com>° e la chiamata :call edi ;

InternetOpenUrlA → questa funzione permette di conettersi ad un url e permette lo scambio di dati .