Malware Analysis 2

Analisi statica avanzata

1. Persistenza di un malware

Nell'esercizio di oggi ci è richiesto di individuare le seguenti informazioni, osservando la figura rappresentata nelle slide:

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. Persistenza dei malware

Per persistenza si intende quando il malware si auto aggiunge alle entry dei programmi che devono essere avviati all'avvio del PC in modo tale da essere eseguiti in automatico senza richiedere il permesso dell'utente.

Nella figura possiamo trovare due chiamate di funzioni:

- RegOpenKeyEx: la funzione permette di aprire una chiave di registro con il fine di modificarla in seguito. I parametri da essa accettati sono: la chiave da aprire.

- RegSetValueEx: la funzione permette di aggiungere un valore all'interno del registro e di settare i dati. I parametri che accetta sono: la chiave, la sottochiave ed il dato da inserire.

RegOpenKeyEx

```
)040286F   push    2                   ; samDesired
)0402871   push    eax                 ; ulOptions
)0402872   push    offset SubKey       ; "Software\\Microsoft\\Windows\\CurrentVersion\\Run"
)0402877   push    HKEY_LOCAL_MACHINE ; hKey
)040287C   call    esi ; RegOpenKeyExW
```

Con la funzione qui sopra rappresentata, il malware ha accesso alla chiave di registro prima di modificare il suo valore.

HKEY_LOCAL_MACHINE = è una delle cinque macrocategorie delle quali si compone il registro di Windows ed è il luogo contenente i record e le configurazioni della macchina.

RegSetValueEx

```
)04028A1   lea     ecx, [esp+434h+ValueName]
)04028A8   push    ecx             ; lpValueName
)04028A9   push    edx             ; hKey
)04028AA   call    ds:RegSetValueExW
```

Questa funzione viene utilizzata per aggiungere una nuova entry e dunque modificare il registro. Facendo così ottiene la persistenza all'avviamento della macchina.

2/3 Client software utilizzato - URL

Il software client utilizzato dal malware per la connessione sono le API di WinINet della libreria Wininet.dll.

Lo possiamo denotare dal fatto che nell'esercizio viene utilizzata la funzione 'InternetOpenUrl'. L'url al quale tenta di conntersi è quello cerchiato in figura.