1. Descrizione della persistenza del malware e codice assembly relativo:

Il malware esegue una serie di operazioni per ottenere la persistenza nel sistema operativo Windows. Innanzitutto, utilizza la funzione `RegOpenKeyExW` per aprire o creare una chiave di registro nel registro di sistema di Windows. Questa chiave di registro è situata nel percorso `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`, che è comunemente utilizzato per avviare automaticamente i programmi all'avvio del sistema. Le istruzioni assembly coinvolte in questa operazione sono:

```
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
```

Successivamente, il malware memorizza l'indirizzo del buffer `Data` nello stack utilizzando l'istruzione `lea`. Questo buffer probabilmente contiene i dati che il malware desidera scrivere nella chiave di registro per ottenere la persistenza.

```
00402882   lea     ecx, [esp+424h+Data]
```

In seguito, il malware calcola l'indirizzo in cui memorizzare i dati da scrivere nella chiave di registro utilizzando nuovamente l'istruzione `lea`. Qui, `eax` contiene l'handle della chiave di registro precedentemente aperta.

```
0040288F   lea     edx, [eax+eax+2]
```

Dopo aver preparato i dati, il malware chiama la funzione `RegSetValueExW` per scrivere i dati nella chiave di registro, assicurandosi che il programma venga avviato all'avvio del sistema.

```
00402898   lea     eax, [esp+428h+Data]
004028AA   call    ds:RegSetValueExW
```

Queste istruzioni formano il processo attraverso il quale il malware ottiene la persistenza nel sistema operativo Windows, assicurando che venga eseguito ogni volta che il sistema viene avviato.

2. Identificazione del client software utilizzato per la connessione ad Internet:

Nel secondo estratto, il malware utilizza le funzioni `InternetOpen` e `InternetOpenUrl` per aprire una connessione Internet. Queste funzioni fanno parte della libreria di WinINet di Windows, comunemente utilizzata per la comunicazione su Internet. Il client software utilizzato è Internet Explorer.

3. Identificazione dell'URL a cui il malware tenta di connettersi e chiamata di funzione relativa:

L'URL a cui il malware tenta di connettersi è “http://www.naluare12.com”. Questo viene evidenziato nel codice assembly:


4. BONUS: Significato e funzionamento del comando assembly "lea":

Il comando `lea` (Load Effective Address) calcola l'indirizzo effettivo di un operando e lo memorizza in un registro. È spesso utilizzato per eseguire semplici operazioni di calcolo degli indirizzi senza necessariamente caricare dati dalla memoria. In pratica, viene utilizzato per ottenere l'indirizzo di un oggetto o una variabile invece di caricarne il valore stesso. Ad esempio, nel codice assembly fornito, `lea` viene utilizzato per calcolare gli indirizzi necessari per l'accesso a variabili o dati nelle operazioni successive.