-Con riferimento agli estratti di un malware

-Descrizione di come il malware ottiene la persistenza evidenziando dove le relative istruzioni e chiamate di funzioni vengono eseguite:

Il programma malevolo utilizza la chiave RegOpenKeyExW nella funzione call esi;RegOpenKeyExW (questa funzione permette di aprire una chiave di registro al fine di modificarla),i parametri di questa funzione sono passati sullo stack tramite le istruzioni "push" precedenti ad essa.
Con la funzione call ds:lstrlenW andra' a salvare in un registro il valore delle funzioni precedenti(push ecx ;lpstring,mov bl,1).
La chiamata alla funzione RegSetValueEx viene utilizzata dal malware per modificare il valore del registro ed ottenere cosi la persistenza all'avvio del sistema operativo,anche in questo caso i valori sono passati sullo stack tramite le istruzioni "pusch ecx" e "push edx".

-Identificare client software:

IL client software utilizzato dal malware e' un client web in questo caso internet explorer e' cio' che la vittima pensera' di usare,tra i parametri abbiamo dwFlags,lpszProxyBypass,lpszProxy,dwAccessType eccone le funzioni delle singole:dwAccessType:

dwAccessType: specifica il tipo di accesso alla risorsa Internet. Ad esempio, può essere INTERNET_OPEN_TYPE_DIRECT per un accesso diretto, INTERNET_OPEN_TYPE_PROXY per un accesso tramite proxy o INTERNET_OPEN_TYPE_PRECONFIG per utilizzare la configurazione del sistema.

lpszProxy: un puntatore a una stringa che specifica il server proxy da utilizzare per la connessione. Questo parametro viene utilizzato quando dwAccessType è impostato su INTERNET_OPEN_TYPE_PROXY.

lpszProxyBypass: un puntatore a una stringa che specifica una lista separata da punto e virgola di host o pattern che devono essere ignorati quando si utilizza il proxy specificato. Questo parametro è opzionale e viene utilizzato solo quando dwAccessType è impostato su INTERNET_OPEN_TYPE_PROXY.

dwFlags: un insieme di flag che specifica le opzioni aggiuntive per l'apertura della sessione Internet. Ad esempio, può includere INTERNET_FLAG_ASYNC per operazioni asincrone o INTERNET_FLAG_NO_CACHE_WRITE per impedire la scrittura nella cache locale.

-Identificare l'URL al quale il malware tenta di connettersi evidenziandone la chiamata di funzione:

push offset szurl ;http://www.malware12.com
call edi ;InternetOpenUrlA

-Significato e funzionamento del comando assembly "lea"

il comando "lea"(LoadEffectiveAddress) e' un'istruzione utilizzata per caricare l'indirizzo effettivo di una sorgente di dati di un registro,senza deferenziare o caricare i dati stessi,quindi calcola l'indirizzo di memoria dell'operando specificato e lo carica in un registro,senza accedere effettivamente alla memoria stessa.