COME OTTIENE LA PERSISTENZA IL MALWARE

Chiama la funzione RegOpenKeyExW per aprire una chiave di registro. Successivamente, viene controllato il valore di ritorno dell'operazione e, se è diverso da zero, viene saltato a loc_4028C5. In caso contrario, viene calcolata la lunghezza della stringa contenuta in Data e viene effettuata una chiamata alla funzione RegSetValueEx per impostare il valore di una chiave di registro. Questo può essere utilizzato per ottenere la persistenza di un malware, in quanto il programma verrà eseguito automaticamente all'avvio del sistema.

CLIENT UTILIZZATO DAL MALWARE

Il client software in questo codice sembra essere Internet Explorer 8.0, come indicato dalla stringa "Internet Explorer 8.0"

URL A CUI TENTA LA CONNESSIONE

La funzione `InternetOpenUrlA` viene chiamata per aprire una connessione all'URL "http://www.malware12.com/". Questa funzione è utilizzata per effettuare una richiesta HTTP ad un server remoto

BONUS: LEA

Il comando `lea`(Load Effective Address) carica l'indirizzo effettivo di una locazione di memoria in un registro, senza accedere alla memoria stessa. In questo caso, il comando `lea` viene utilizzato per caricare l'indirizzo della variabile `Data` nello stack, in modo da poter essere passata come parametro alla successiva chiamata di funzione `RegSetValueEx`.