Inżynieria wsteczna złośliwego oprogramowania - zadanie domowe 1

Zadanie 1

Hashe

- md5: FB1569B5A3266444D676E5F82D6BAC85
- sha1: F0D76B3806E58AE5363A78DCC62B5E27A90A7ECF
- sha256: 5B7228947B256F36BD98DDE1622799CDA8F7A7AA0F3196ABA08200FE8439DFEE

Ciekawe stringsy

- RegSetValueEx
- GetEnvironmentVariable
- InternetGetConnectionState
- SetFileAttributes
- DeleteFile

Importowane funkcje

Sporo funkcji z grupy network, np.:

- send
- socket
- connect
- select

oraz funkcji z grupy file:

- DeleteFileA
- WriteFile
- SetFileAtrributesA

Na podstawie tych informacji możemy wywnioskować, że malware zbiera dane o systemie i połączeniu internetowym, modyfikuje pliki, modyfikuje rejestr, może również coś pobrać lub wysłać.

Zadanie 2

- **Nazwa/Rodzina mawlare'u** - Worm
- **Infrastruktura z jaką się komunikuje (domeny i/lub adresy IP)** - www.microsoft.com:80, 96.17.191.121
- **Cel malware'u** - Odczytuje klucze związane z usługami, często powiązane z RDP

- **Sposób w jaki osiąga swój cel i znajduje ofiary** - Sprawnie się ukrywa przez wypytywanie internetu o ustawienia cache w celu usunięcia swojego wirtualnego odcisku palca oraz przez łączenie się z internetem na nietypowych portach. Swoje ofiary znajduje poprzez skanowanie dużej ilości zapytań ARP
- **Jak uzyskuje persistance (przetrwanie restartu)** - Modyfikuje samowyzwalającą się funkcję autouruchomienia poprzez zmodyfikowanie rejestru