Przygotowanie środowiska do analizy

Skład zespołu: Julia Sadecka, Marcel Trzaskawka

1. Środowisko

   Analizę będziemy przeprowadzać na systemie Windows 10 Flare VM oraz jeżeli będzie taka potrzeba na Windows XP. Środowisko Flare VM zawiera już wszystkie potrzebne narzędzia, które wypisaliśmy poniżej. Maszyny są odseparowane od Hosta oraz od sieci, aby bezpiecznie analizować szkodliwe wirusy. Zrobione zostały również migawki (snapshot) w celu powrócenia do punktu startowego w razie kiedy coś pójdzie nie tak 💀.

2. Rysunek techniczny przedstawiający adresacje i ewentualne połączenia z innymi maszynami.

Maszyna 1 - 10.0.0.1 255.255.255.0 Maszyna 2 - 10.0.0.2 255.255.255.0

3. Lista narzędzi umożliwiających przeprowadzenie analizy statycznej.
   - PeStudio (Informacje o plikach wykonywalnych)
   - PEiD (Informacje o plikach wykonywalnych)
   - PPEE (Puppy)
   - x64ddbg (Debugger)
   - OllyDbg (Debugger)
   - Ghidra (Disassembler, Decompiler)
   - IDA Free (Disassembler, Decompiler)
   - Binwalk (Określa typ pliku)
   - Strings (Wypisuje stringi)

4. Lista narzędzi umożliwiających przeprowadzenie analizy dynamicznej.
    - Wireshark (przechwytywanie pakietów i nagrywanie logów)
    - Radare2/Cutter (reverse engineering)
    - Autoruns (Sprawdza nowo dodane aplikacje do autostartu)
    - Process Hacker (Wyświetla nowe procesy kolorkami)
    - Any.run (Głęboka analiza)
    - regshot (Porównanie całości systemu przed i po uruchomieniu wirusa)
    - cuckoo (Głęboka analiza)

5. Lista narzędzi umożliwiających przeprowadzenie analizy sieciowej.
    - Wireshark (przechwytywanie pakietów i nagrywanie logów)
    - Netcat (podobne do nmap)
    - apateDNS (kontrolowanie zapytań dns)