SC4014 Concepts and Technique for Malware Analysis

Assignment 2

Deadline: 15 Apr 2024, 2359hrs

Instructions

Submit a word document with the answers and include screenshots to illustrate the answer. The sample is zipped with password "infected".

Questions

The following question will be relating to the server.exe of MD5 hash (B710A46A3A8C3DDC2903BBD21C82AD32). Please make sure the image base address within IDA is 0x400000. If you wish to detonate the malware, run it as administrator.

1. There are two config strings delimited by two different set of alphanumeric ASCII values.
   a. Provide both the raw file offset of the EXE that contains the two config. (1 mark)
   b. Provide both the value of the config string in raw hex bytes. (1 mark)
   c. Are you able to find these config string within IDA (Use hex view and search->Text). If not, please provide a brief explanation. (Hint - What does opening the PE file in IDAPro simulates in the PE file execution process) (3 mark)
2. The two config strings found in question 1 are encoded
   a. Please provide a brief description (referencing addresses from IDA) including screenshots of the encoding algorithm used. Including the keys/value used for the encoding in hex. (4 mark)
3. There are two possible set of service name created by the malware depending on the certain requirements
   a. There are 2 algorithm to generate Service names for persistence. Please provide a brief description (referencing addresses from IDA) including screenshots. (5 mark)

The following question will be relating to the dropped DLL. Please make sure the image base address within IDA is 0x10000000.

4. a. Is it possible to statically extract the dropped DLL from the first sample server.exe. Please provide a brief description including screenshots. (1 mark)

   b. What is the service DLL location that is stated after the service is created, provide a screenshot of this information. Are you able to find the DLL at this location, if not please provide an adequate explanation(2 mark)

   c. Previously, the config string was found in part 1. Please elaborate on how this DLL obtains it config string again. (Hint - Does the malware uses the technique in part 1) (1 mark)

   d. The malware enumerates host system information before sending the information to the C2 server at function sub_10009700. Please state the 2 of multiple data enumerated from the host. (2 mark)