Assignment 2

Total Marks: 20

Due: 15 Septem[illegible] PM

Submission: On[illegible]rough Moodle)

!!!Important!!!

The executable t[illegible] assignment are live malware and need to be handled safely. Pl[illegible]nload and execute files on your host machine. Download and execute the files in a Windows Virtual Machine (VM) and isolate the environment by setting the network adapter to host only as described in the Lab setup document. Revert to a clean snapshot after each execution.

This assignment has three parts.

Part 1- Dynamic Analysis - 8 marks

(Do not download and execute the ransomware file on your host machine.)

In this part of the assignment, you will execute a live ransomware in an isolated environment on a Windows VM and collect some information about it. Download the ***ransomware*** file from moodle and change the extension to .exe for it to execute. Remember the malware is a live ransomware and will encrypt the files when executed. It will not encrypt the files if it can't connect to a command-and-control server. You may also need to set up a gateway VM running Wireshark and/or a proxy through which the Windows VM will route all the traffic. You may already have this set up if you followed the instructions in the lab set up document or video provided to you for lab setup. We have also discussed in lecture related to setting up a VM as a gateway.

Task 1: The ransomware runs a Domain Generation Algorithm to generate multiple domain names that it then tries to resolve through DNS queries. Once it finds a registered domain, it communicates with this domain as its Command-and-control server. In this task you need to get a list of the domains generated by the ransomware and submit the first 10 for the assignment. (Marks: 2)

Task 2: In the persistence mechanism lecture we looked at the registry keys that are likely to be used for persistence by malware on Windows. In this task you will need to find out which registry keys are being used by the ransomware for persistence. You will find the tool RegShot useful for this task. Once you find the key(s), submit a screenshot. Make sure your screenshot contains the date on which you took the screenshot somewhere in it. A screenshot without a date will not be accepted. (Marks: 2)

Task3: In this task, you will find the location where the ransomware makes a copy of the executable for persistence. Take a screenshot that shows the file on the disk. Make sure your screenshot contains the date on which you took the screenshot somewhere in it. A screenshot without a date will not be accepted. (Marks: 2)

Task4: In this task, you will write YARA rules for the ransomware variant by creating your comments, strings and defining your conditions. Give your rule a name and add some metadata.

Your rule must make use of the hash and the PE modules. Your rule must have at least two strings. In addition to the two strings, it must have at least one function from the hash module and at least two functions from the PE module. Include the YARA rule in your report and provide it as a .yara file separately too. (Marks: 2)

mic Analysis – 5 marks

(Do not download a 7z file on your host machine.)

The SOC team has fou lication putty.exe on a computer in an unusual location. In this part of the assi estigate the file following the steps below and complete the tasks.

Step 1: Download ***putty.7z*** from moodle in an isolated environment on a Windows VM and extract the executable (password:infected). Putty is a well-known open source SSH and telnet client for Windows. If you have not used putty before, familiarise yourself with putty and its capabilities.

Step 2: Execute the file and observe the behaviour before the appearance of standard putty interface.

Task1: Report the behaviour which you have observed. (Marks: 1)

Task 2: Use Procmon (Process Monitor) to discover the reason for the observed behaviour. Report the screenshot of the entry for this behaviour. We will call this the payload. (Marks: 1)

Task 3: To execute the payload multiple arguments are used. One of these arguments comprises of various function calls over a string. The function calls show two main operations and their order. Use cyberchef or any other tools to reverse these operations and decode the string. The decoded information contains a host and a remote port number. Provide screenshots for decoding process and decoded information. Briefly summarise your findings from the analysis. (Marks: 3)

Part 3 – Reverse Engineering – 7 marks

In this part of the assignment, you will reverse engineer the assembly code provided in the ***assemcode.txt*** file.

Task 1: You need to submit pseudo-code that shows the high-level logic that is implemented in the assembly. (Marks: 5)

Task2: You need to provide explanation of what each function in the assembly does. (Marks: 2)

The purpose of the program is to check the validity of a 20-byte key. The code has been compiled for x64 architecture and therefore you will find some differences from the x86 code you saw in the lectures. The file also contains some comments to help you along the way.

Remember that anything that starts with keyword LAB is a label. The start of each function is marked so you can easily locate the functions. The program starts from main(). The comments also show the local variables that are allocated space on the stack for that function. These are not part of the code but have been provided for your reference. The variables have been given arbitrary names for easy decompilation and ease of reading. You will find that there are calls to the printf function in the code, but the code does not have the subroutine for printf. You can

assume that a call to the printf function will result in printing the value at the address stored in the RDI register.

Assignment submission

Submit everything in [illegible]t on moodle. You must also submit .yara file you have created.

Extensions

No extensions will [illegible]pproved by the Department of Computer Science (https://www.cs.wai[illegible]esources/application-for-an-extension-of-deadline) You can submit late. However, late submissions will be deducted **1 mark/ day.**

Plagiarism

Credit all sources you refer to. Students found plagiarising will be reported to the disciplinary committee. You are expected to follow the University's guidelines here: https://www.waikato.ac.nz/students/academic-integrity/student-information/plagiarism. Assignments will be checked against anti-plagiarism checkers.