Assignment No.1

CS-5051 Malware Analysis and Detection

Submission Deadline: Sunday 27th March until 4:59 pm on Google Classroom

Total Marks: 100

AIM of this assignment is to write a Static Analysis Report and give you practice of tools and concepts, which you have learned in last 2 – 3 weeks. Through this assignment, you will also learn how to safely download and extract malware files.

Description:

In this assignment, you have to do Basic Static analysis and write a comprehensive and effective Static Malware Analysis Report. For this purpose, you have to write a static analysis report for eight malwares downloaded from following link:

https://dasmalwerk.eu/

Remember *you have to download all these malwares in* ***safe environment*** *(malware Lab) all these file are malicious and can damage your system. As we are doing static analysis,* ***do not run*** *these malwares.*

Malwares you have to download are:

1. Gen:Heur.PonyStealer.4
2. Dropped:Trojan.Dropper.Agent.VOE
3. Trojan.GenericKD.3652107
4. Password-Stealer (003bbfec1)
5. Gen:Variant.Ransom.Cerber.171
6. in32/Tnega.bXRKZUB
7. W32.SecretKAN.Trojan
8. Backdoor.TXLK-8101

Password to extract/unzip all these malwares is: **infected**

Questions you have to answer in your report.

Following are the list of questions you must have to answer in your report.

1. What is complete information each malware file i.e., complete identification of file? This includes:
    a. Magic byte
    b. File signature
    c. Machine information
    d. Exe type (32/64 bit)
    e. Identify file types from their binary (using ***TrIdNet*** and ***python magic*** library)
    f. Other important information's you need to Report (Think cleverly)
2. What is the fingerprinting information of each malware file? This can be done by calculating cryptographic checksums (MD5, SHA1, and SHA256). For this, you must use different tools like ***calcHash*** and ***Python library*** for check sums (MD5, SHA1, and SHA256) and report it accordingly.
3. What type of malicious strings are in Malware files? For this purpose you can take following steps:
    a. Read context and information of each malware file.
    b. Write strings of each malware in a text file and once read it very carefully.
    c. Write an appropriate YARA rule/rules to scan and extract important information.
4. Number, type and offset of different sections of each Malware?
5. Which DLLs and their number of functions used by each Malware?
6. What is packing information if Malware is packed?

You must use and report following tools in your report:

1. Notepad++ with hex plugin
2. Tridnet GUI
3. Python Magic library ((https://pypi.org/project/python-magic/)
4. HashCalc or (md5sum, sha1sum and sha256sum) commands
5. Hashlib (http://pymotw.com/2/hashlib/)
6. VirusTotal: (https://www.virustotal.com/gui/home/upload)
7. Hybrid Analysis: (https://www.hybrid-analysis.com/)
8. SNDBOX: (https://www.sndbox.com/)
9. Any.run: (https://any.run/)
10. CFF explorer
11. Process Hacker
12. Exeinfope

13. pestodio
14. YARA scripts
15. You have complete freedom to use any other tool of your choice with complete description.

What to include in Static Malware Analysis report?

Summary of the analysis: Key takeaways should the reader get from the report regarding the specimen's nature, origin, capabilities, and other relevant characteristics.

Identification: The type of the file, its name, size, hashes, malware names

Dependencies: Files and network resources related to the specimen's functionality, such as supported OS versions and required initialization files, custom DLLs, executables, URLs, and scripts.

Supporting figures: Logs, screenshots, string excerpts, function listings, and other exhibits that support the investigators analysis.

Malware analysis should be performed according to a repeatable process. To accomplish this, the analyst should save logs, take screen shots, and maintain notes during the examination. This data will allow the person to create an analysis report with sufficient detail that will allow a similarly-skilled analyst to arrive at equivalent results.

Important:

- For any help or confusion, you people can email at jawad.hassan@nu.edu.pk.
- Write an effective and detailed report in word format.
- Do not plagiarize. If found ***ZERO*** marks will be assigned.
- Late submission will also result in ***ZERO*** credit.

Best of Luck ☺