Sections: 600, 601, and 602 | Spring 2024

Static Malware Analysis

Hands-On Practice

"You are the investigator"

A) Objectives:

This hands-on training session aims to empower students to apply and refine the techniques introduced in the module, focusing on the secure and confident handling of malware samples. Engaging in group activities with Basic Static Malware Analysis tools, participants will gain practical experience within a protected environment, simulating real-world malware analysis scenarios. Students will be presented with limited initial information about the software under investigation, a strategic approach intended to bolster analytical and critical thinking skills as they navigate the complexities of malware analysis and interpretation.

The collaborative nature of this exercise is central to its design, offering a realistic representation of professional malware investigations and fostering a team-based approach to learning. Through teamwork and the practical application of concepts taught in the module, students will gain invaluable exposure to the tools and techniques of Static Malware Analysis. This method is meticulously crafted to advance the group's collective ability to critically assess and dissect malware, all while adhering to best practices for secure analysis. The ultimate goal is to equip students with the competence to handle malware securely, leveraging their acquired knowledge to confidently navigate the intricacies of malware examination.

B) To obtain the malware samples for analysis, follow one of these procedures:

1) **From the Official GitHub Repository of the Book:**
   - Navigate to the repository at https://github.com/mikesiko/PracticalMalwareAnalysis-Labs
   - Download the samples and extract them on the Windows host machine.
   - Carefully transfer them to the Linux virtual machine for analysis.

   Ref.: Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski and Andrew Honig

And/Or

2) **From the Class's GitHub Repository:**
   - Access the class repository at https://github.com/RITDubaiCSEC202/TheGOOD_TheBad_and_TheUgly
   - Directly download and extract the samples on your Linux virtual machine.

Warning: Under no circumstances should you run the binaries on your Windows host machine. Always conduct your analyses within a secure and isolated virtual environment to prevent any potential harm.

C) Groups and Malware:

Troop #	Malware	Done?
1	Lab01-01.exe (*be aware of the folder's content*)	
2	Lab01-02.exe	
3	Lab01-03.exe	
4	Lab01-04.exe	
5	Lab03-01.exe	
6	Lab03-03.exe	
7	Lab03-04.exe	

D) Tasks

1. Identify File Type

- Use tools like **file** on Unix or file properties on Windows to determine the type of the file (e.g., executable, script, document)

2. Determine File Fingerprint

- Generate MD5, SHA-1, and SHA-256 hashes of the file using hashing tools to create a unique fingerprint.

3. Online Scanner Analysis

- Upload the file or its hash to an online scanner like VirusTotal to check for known signatures of malware.

4. Review Online Scan Reports

- Visit **VirusTotal** and analyze the reports. Determine if the file is recognized as malicious by any security vendors.
- Try other platforms such as Cuckoo Sandbox and hybrid-analysis

5. **Extract Strings**
    - Utilize tools such as strings on Unix or a hex editor on Windows to extract human-readable strings from the file, which may reveal insights into its functionality.

6. **Analyze Import Functions**
    - Inspect the import table with tools like Dependency Walker to see which system functions the file uses. Look for functions that are commonly used by malware, such as those for network communication, process injection, or file manipulation.

7. **Network Communication Check**
    - Analyze strings and import functions for references to network activity (e.g., send, recv, URLs, IP addresses).

8. **Detect Packing or Obfuscation**
    - Look for signs of packing or obfuscation, such as a high entropy rate, the presence of packer strings, or unusual import tables.

9. **Assess Purpose and Behavior**
    - Based on the gathered information, make an educated guess about the purpose of the files. Consider whether the file behaves like typical malware, such as a trojan, ransomware, or downloader.

E: Appendix GitHub Repository README File

Educational Malware Archive

Warning

This repository contains real malware samples intended strictly for educational purposes.

Purpose

The files in this archive are used as practical, hands-on supplements for the book *"Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software"* by Michael Sikorski and Andrew Honig. These samples are used for training and educational exercises that teach malware analysis and reverse engineering skills.

Original Source

The original files and further resources are available at the official No Starch Press website: https://nostarch.com/malware.

Usage

The malware samples stored here are dangerous and should be handled with extreme caution. Do not execute or analyze the malware on any computer that is connected to a network or contains sensitive data.

Recommended Practices

Run malware analysis in a controlled and isolated environment, such as a virtual machine that has no network access.

Ensure that you have legal permission to handle malware for analysis. It is your responsibility to comply with all applicable laws and regulations.

Understand the risks involved and take appropriate security measures to prevent accidental execution or containment failures.

Liability

The maintainers of this repository and contributors to the *"Practical Malware Analysis"* book are not liable for any damages that may arise from the misuse of the malware samples. The responsibility lies with the individual who downloads and uses these samples.

Acknowledgments

This repository is created and maintained for educational purposes and is in no way affiliated with the authors or publishers of the book *"Practical Malware Analysis"* other than the use of provided samples.

Contact

For any inquiries or issues related to this archive, please open an issue on this repository.