## General Overview of the assignment

This assignment is divided into two sections:

* **First section:** This part can be completed as a group, with a maximum of two people per group. You will start by forming your group and completing various tasks in Lab 11, followed by submitting a report later. This section is designed to assess your practical skills and is worth 15% of the total mark.
* **Second section:** This is an individual assignment requiring you to conduct your own research and write a scientific report. You only need to complete this section if you are aiming for a Distinction (D) or High Distinction (HD). This section is worth 20% of the total mark.

**Group Submission:** Please submit a Word document that includes the assignment cover page, listing the full names and student IDs of all group members. This document should encompass all your responses to the questions, along with screenshots of the command list. Furthermore, please include a few paragraphs at the end that reflect on this assignment, addressing the challenges you faced and the highlights experienced both individually and as a group.

**Individual Submissions (D and HD only):** Each individual must submit a separate research report in PDF or DOCX format. On the first page, include your name, student ID, group number, and the names of your team members as a comment in the Canvas submission. The report should contain at least 10 references from reputable journals and conferences, complete with proper in-text citations and a bibliography at the end in either APA, IEEE, or Harvard style. The only permissible use of generative AI for this report is to help correct your own written content.

A template for the report has been provided.

## Section 1: Group Project: Technical Report writing

## Purpose

Writing analysis reports is a very important step in malware analysis. With a well-structured and well-written report, you can properly share the knowledge gained through analyzing malware samples with others.

Regardless of the audience of the report, a malware analysis report should contain certain technical details as well as short descriptive sections explaining the overall malicious behaviour and what each stage of the malware is responsible for.

Furthermore, you can add any extra details or information that can be used by specific readers as further sections to the end of the report.

## Outcome

* Learn what technical details of a malware sample are important for writing an analysis report.
* Learn how to put together details from the analysis of different stages of malware in a single coherent report.

## Section 1 – Writing report for a multi-stage malware

In this assignment, you will be tasked with writing a technical report on a multi-stage malware that we have previously analyzed. This malware takes the form of a malicious document file containing a VBA macro that installs a backdoor module on the victim's machine. We examined the document file and its macro script in Lab 7, while the backdoor payload, developed for the .NET framework, was analyzed in Lab 9. The first stage involves the malware discussed in Lab 7, and the second stage focuses on the .NET malware from Lab 9.

Please refer to your previous lab documents and utilize the following template to create your technical report on this multi-stage malware.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| <A Descriptive Title>  1- Summary of the attack  <In this section provide a high-level view of the contents of this report. You can write this section once you have finished the other sections of the report>  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  2- Execution Diagram  <In this section create a diagram that shows the stages of the malware and their connection with each other>  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  3 - Stage 1  **3.1 - Technical details:**  **md5** -  **sha1** -  **sha256** -  **File name** -  **File type** -  **Timestamp** -  **3.2 - Description:**  <In this section provide a high-level description of this malware. Explain what the main responsibility of this stage is.>  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  4 - Stage 2  **4.1 - Technical details:**  **md5** -  **sha1** -  **sha256** -  **File name** -  **File type** -  **Timestamp** -  **4.2 - Description:**  <In this section provide a high-level description of this malware. Explain what the main responsibility of this stage is.>  **4.3 - Communication with the server:**  <In this section explain how this malware connects to a remote server. Find the IP address and Port numbers used and the function(s) responsible for handling the connection to the remote server and explain what they do. Include screenshots of the function(s).>  **4.4 - How malware does reconnaissance on the victim’s system:**  <In this section explain how this malware collects information from the victim’s machine and how it sends this information to its remote server. Find the function(s) responsible for this operation and explain what they do. Include screenshots of the functions(s).>  **4.5 - Download and execute another malware from the remote server:**  <In this section explain how this malware downloads and executes another malicious executable from its remote server. Find the function(s) responsible for this operation and explain what they do. Include screenshots of the functions(s).>  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  5 - Analysis methods  <In this section explain the techniques and methods used for the analysis of the malware samples described in this report. You can explain what tools were used for the analysis of each stage>  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  6 - Conclusion  <Add a short conclusion to the report>  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  7 - Scripts or automated techniques used for analysis  <In this section you can add your Python script used for generating stage 2 of the attack. You can also add the CyberChef recipe which does the same task>  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  8 - Yara rule  <Add Yara rules to match each stage of the attack>  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  9 - Indicators of Compromise  <In this section add a list of all md5, sha1 and sha256 hashes of the malicious stages involved in the attack. Add any malicious IP address or URL found in the malware samples.>  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  10 - MITTRE ATT&CK  <In this section add a list of MITRE ATT&CK technique IDs and Names used in this attack and add notes to reflect how the technique is used in this attack. For this section, refer to the MITRE ATT&CK website (https://attack.mitre.org/), read the titles of the techniques from the Matrix and add to the following table what you see relevant. Add more rows as you find more relevant techniques.>   |  |  |  | | --- | --- | --- | | Technique ID | Technique Name | Notes | |  |  |  | |  |  |  | |  |  |  | |  |  |  | |

|  |
| --- |
| Section 1 – Advanced Yara: Writing a YARA rule for heuristic malware detection  As described in the paper “Attributes of Malicious Files” (https://sansorg.egnyte.com/dl/zdmLYMKnP1), unusual PE metadata is a very useful indicator that a file may be malicious. In this exercise, you will write a YARA rule for detecting malware based on the indicators listed in this paper.    Write a YARA rule that:   * Matches as many files in the malicious directory as possible * Matches as few files in the benign directory as possible * Check that the file is a PE file * Has at least five conditions based on indicators from the “Attributes of Malicious Files” paper * You may include anything else in your YARA rule that you wish   Section 1- Scripting- write the Python script in the extension task in lab 9 related to APK malware (this is a separate task than the above report). |

## Section 2 - Individual Advanced Research

## Purpose

Research skills are fundamental skills for security and malware analysts. In this section, you are going to perform some advanced research on the latest technologies and techniques related to malware analysis.

## Outcome

* Learn to conduct research as a cybersecurity analyst and malware researcher.
* Learn how to perform scientific research and write a coherent research article.

Below are the topics you can choose from for the second section. While we prefer a diverse distribution of topics across the tutorial, it is acceptable if more than one student selects the same topic.

1. Machine learning techniques for function similarity detection in reversed engineered code /malware
2. Packer Detection methods
3. Machine learning methods for malware analysis
4. Crypto Ransomware and major open-source algorithms used
5. Polymorphic and metamorphic malware their examples, analysis and their operational mechanisms
6. Malware Attribution techniques and their recent advancements
7. A background study on keyloggers and their fundamental operating mechanism
8. Malware for LLMs, AI-driven (self-learning) malware and their techniques
9. IoT malware and their analysis and detection methods
10. Research on the black market for Zero vulnerabilities and malware

Marking Guidelines

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Mark** | **Items** | **Most Common Deductions** |
| **Section1(15%)** | 100\* 0.15 | 1. Summary (5 marks) 2. Diagram (5 marks) 3. Technical details (2 marks) 4. Description (4 marks) 5. Technical details (2 marks) 6. Description (4 marks) 7. Communication with the server (4 marks) 8. Reconnaissance (4 marks) 9. Download and execute (10) 10. Analysis methods (4 marks) 11. Conclusion (4 marks) 12. Script 1 (5 marks) 13. Yara rules (10 marks) 14. IOCs (3 marks) 15. MITRE ATT&CK (10 marks) 16. Script 2 (4) 17. Advanced Yara (10 marks) 18. Reflection (10 marks) | * No proper description of how items are found * Images too large or too small and not readable * Reflection lacks technical details and how it was resolved |
| **Section 2 (20%)** | 100\*0.2 | * Depth and breadth of the research (40 marks) * Style and Formatting (10 marks) * Cohesive Writing and clarity (20 marks) * Proper references and in-text citation format (10 marks) * Quality relevant references (20 marks) | * Inconsistency in referencing style * Too many old and outdated references * General reports that lack details are indicators of using generative AI * Inconsistent style, figures and tables lack captions. |
| **Total** | 35 |  |  |