Fabino

MALWARE ANALYSIS

To Analyze and Identify Behavior of Malware

PRESENTED TO
Cyberthon

PRESENTED BY
Team Fabino
Abhilash R (423)
Sumresh (402)
Surya Teja(419)

14-03-2023

FABINO

INTRODUCTION

Cyber security refers to every aspect of protecting an organization and its employees and assets against cyber threats.

Malware Analysis is the practice of determining and analyzing suspicious files on endpoints and within networks.

ABSTRACT

The purpose of malware analysis is to obtain and provide the information needed to rectify a network or system intrusion.

When we analyze potential malware, the intended result is typically

- to determine what a suspected malware can do,
- how to detect it once it is in our network, and
- how to measure and contain the damage.

Once we identify which files require full analysis, we develop signatures to detect malware infections on our network.

Fabino

Problem Statement

To analyze a provided malware sample and identify its

- behavior
- functionality and
- potential impact

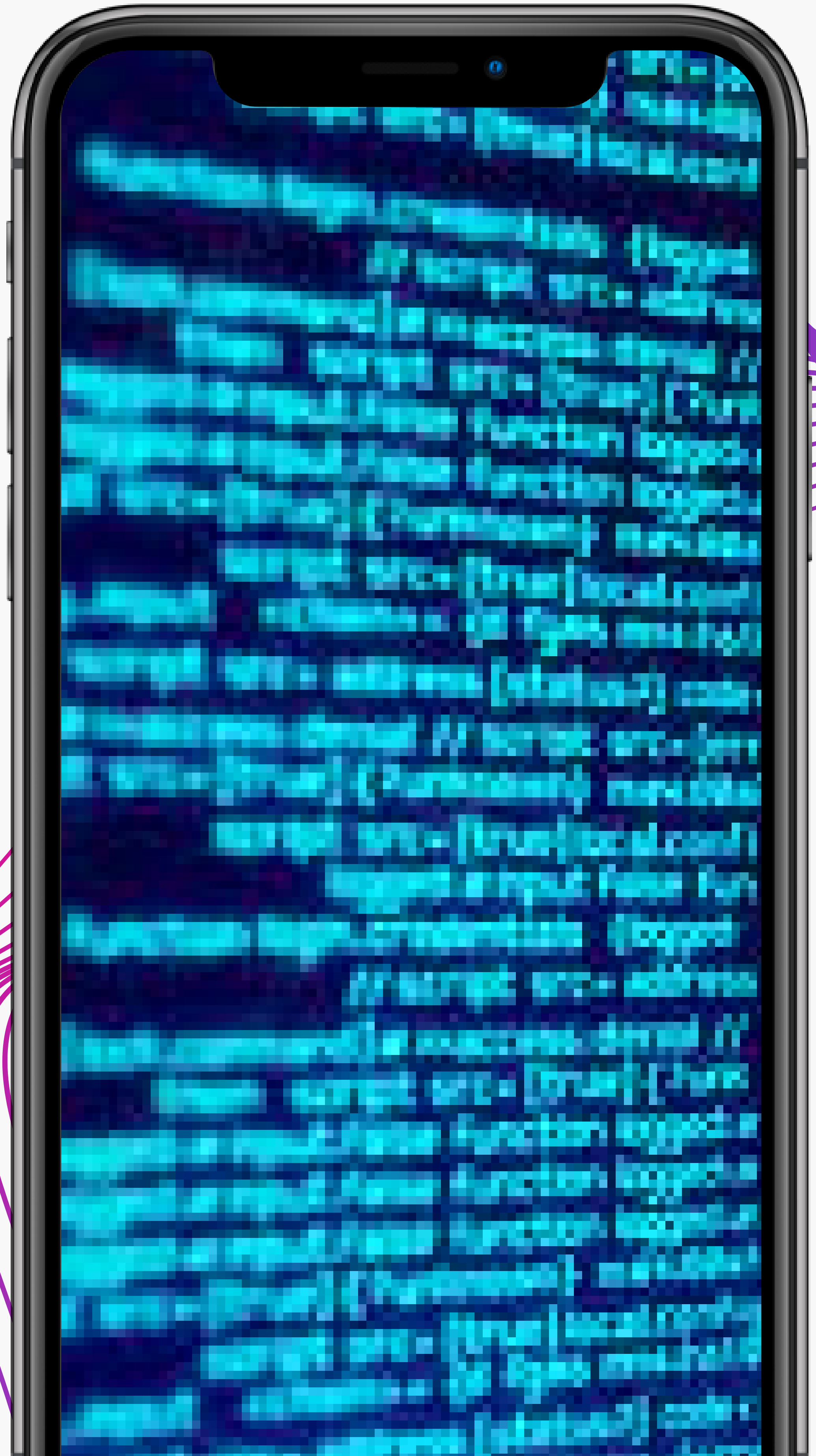
They will also be required to suggest countermeasures and best practices to prevent future attacks.

Types Of **Malwares**

1. Ransomware
2. Fileless Malware
3. Spyware
4. Virus
5. Adware
6. Trojan
7. Worms
8. Rootkits

Malware Analysis

- The study or process of determining the functionality, origin and potential impact of a given malware sample .
- Malware or malicious software is any computer software intended to harm the host operating system or to steal sensitive data from users, organizations or companies.
- Malware may include software that gathers user information without permission.



FABINO

Types Of

Malware Analysis

1. Static Analysis
2. Dynamic Analysis
3. Reverse Engineering

FABINO

STEPS FOR MALWARE ANALYSIS

Step 1: Capture the malware.

Step 2: Build a malware lab.

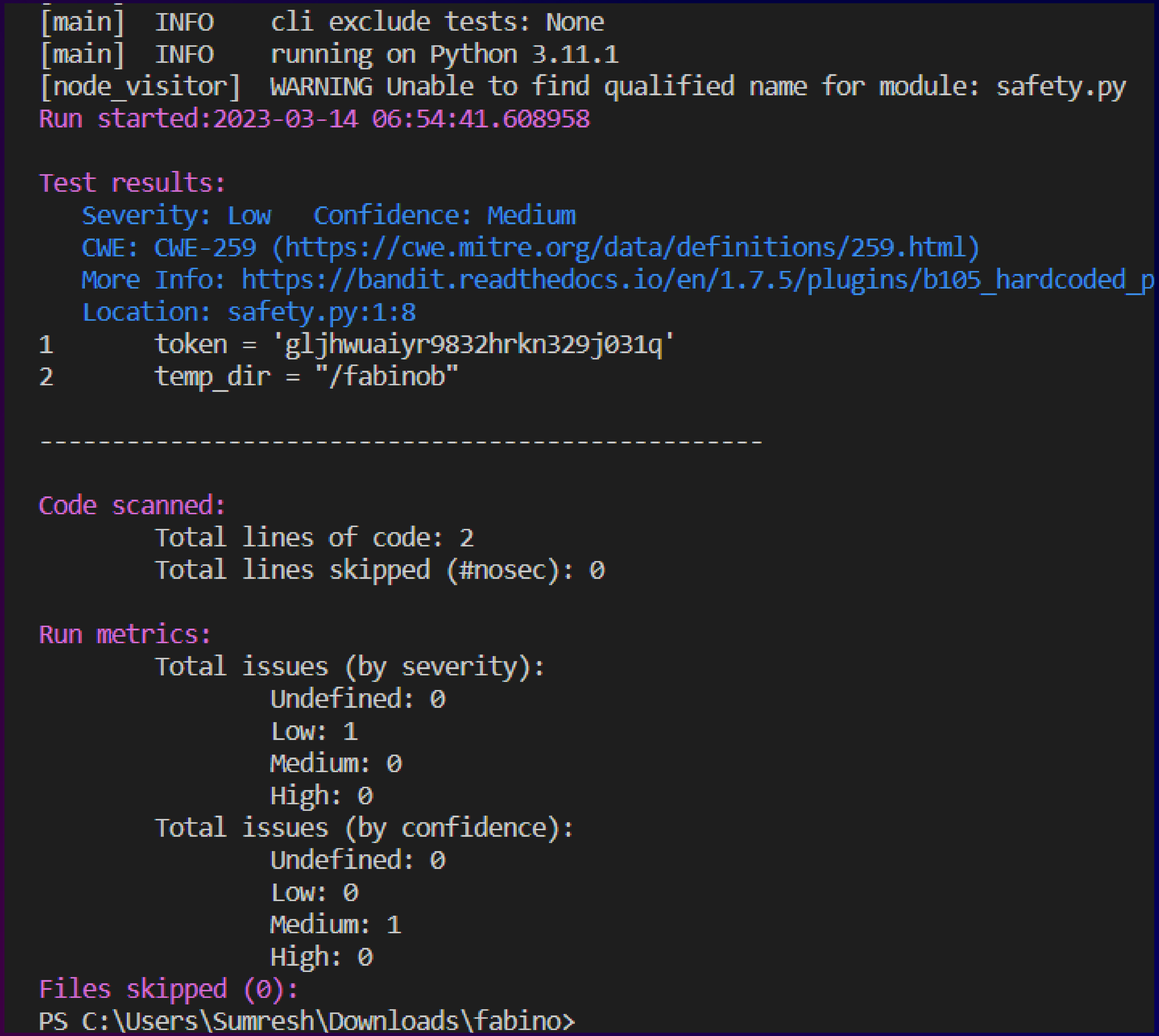
Step 3: Install your tools.

Step 4: Record the baseline.

Step 5: Commence your investigation.

Step 6: Document the results.

CODE EXPLANATION



```
[main]  INFO    cli exclude tests: None
[main]  INFO    running on Python 3.11.1
[node_visitor]  WARNING Unable to find qualified name for module: safety.py
Run started:2023-03-14 06:54:41.608958

Test results:
   Severity: Low   Confidence: Medium
   CWE: CWE-259 (https://cwe.mitre.org/data/definitions/259.html)
   More Info: https://bandit.readthedocs.io/en/1.7.5/plugins/b105_hardcoded_p
   Location: safety.py:1:8
1       token = 'gljhwuaiyr9832hrkn329j031q'
2       temp_dir = "/fabinob"

--------------------------------------------------

Code scanned:
        Total lines of code: 2
        Total lines skipped (#nosec): 0

Run metrics:
        Total issues (by severity):
                Undefined: 0
                Low: 1
                Medium: 0
                High: 0
        Total issues (by confidence):
                Undefined: 0
                Low: 0
                Medium: 1
                High: 0
Files skipped (0):
PS C:\Users\Sumresh\Downloads\fabino>
```

Sample

Output

FABINO

THANK YOU