Sample Malware Hash Study Report

Cyber Security Internship – Task 5

Analysis Platform: VirusTotal

1. Introduction

This report presents a study-based analysis of a known malware sample hash using VirusTotal. The purpose of this study is to understand how malware is identified and classified by security vendors without executing the malicious file. The selected hash belongs to a well-known test malware sample.

2. Sample Hash Information

Sample Hash (MD5): 44d88612fea8a8f36de82e1278abb02f This hash corresponds to the EICAR (European Institute for Computer Antivirus Research) test file. It is a harmless file designed to test antivirus detection capabilities.

3. VirusTotal Detection Results

When the sample hash was searched on VirusTotal, it was detected by multiple antivirus engines. Most vendors classified the file as test malware or malicious, confirming the effectiveness of signature-based detection mechanisms.

4. Threat Classification

The sample was classified as a test malware rather than an active threat. Threat labels provided by vendors indicated that the file is used for detection testing purposes. Despite being harmless, it behaves similarly to real malware in detection scenarios.

5. Observed Behavior Indicators

Behavior indicators observed in the report included file-based detection and signature matching. No malicious runtime behavior was observed because the analysis was performed using a hash-based lookup and not through dynamic execution.

6. Risk Assessment

The EICAR test file poses no real risk to systems. However, it is useful for demonstrating how malware is detected and classified. Studying such samples helps security professionals understand detection workflows without exposing systems to real threats.

7. Conclusion

This study demonstrates how VirusTotal can be used to safely analyze malware hashes. By examining detection results and classifications, it is possible to gain insight into malware identification techniques used by antivirus vendors. Such analysis forms the foundation for advanced malware research and threat intelligence.

Author: Mohammed Nihal