Malware Analysis Report - VirusTotal

# 1. Introduction

This report presents the analysis of a suspected malware sample using VirusTotal. The sample used is a well-known antivirus test file called 'eicar.txt'. The analysis was conducted within a Kali Linux environment running inside Oracle VirtualBox.

# 2. Tool Used

Tool: VirusTotal

Environment: Kali Linux in VirtualBox

File: eicar.txt

Size: 69 bytes

SHA-256 Hash: c7c5500ec3246920bb361d68a3b32a92c680b09b50ef4ca220844a0b96295ebf

# 3. Scan Results

Detection: 4 / 61 engines flagged the file

Detected by:

• AhnLab-V3: Virus/EICAR\_Test\_File

• TrendMicro: Eicar\_test\_1

• TrendMicro-HouseCall: Eicar\_test\_1

• VirIT: EICAR-Test-File

# 4. Static Info

File Type: ASCII / Powershell

MD5: cbf9e382a8c1db4d27d1208e816950b

SHA-1: c25058203c6e36262db1f57fb9ea70bc199f9f7

SHA-256: c7c5500ec3246920bb361d68a3b32a92c680b09b50ef4ca220844a0b96295ebf

# 5. Screenshots





