Static Malware Analysis Report

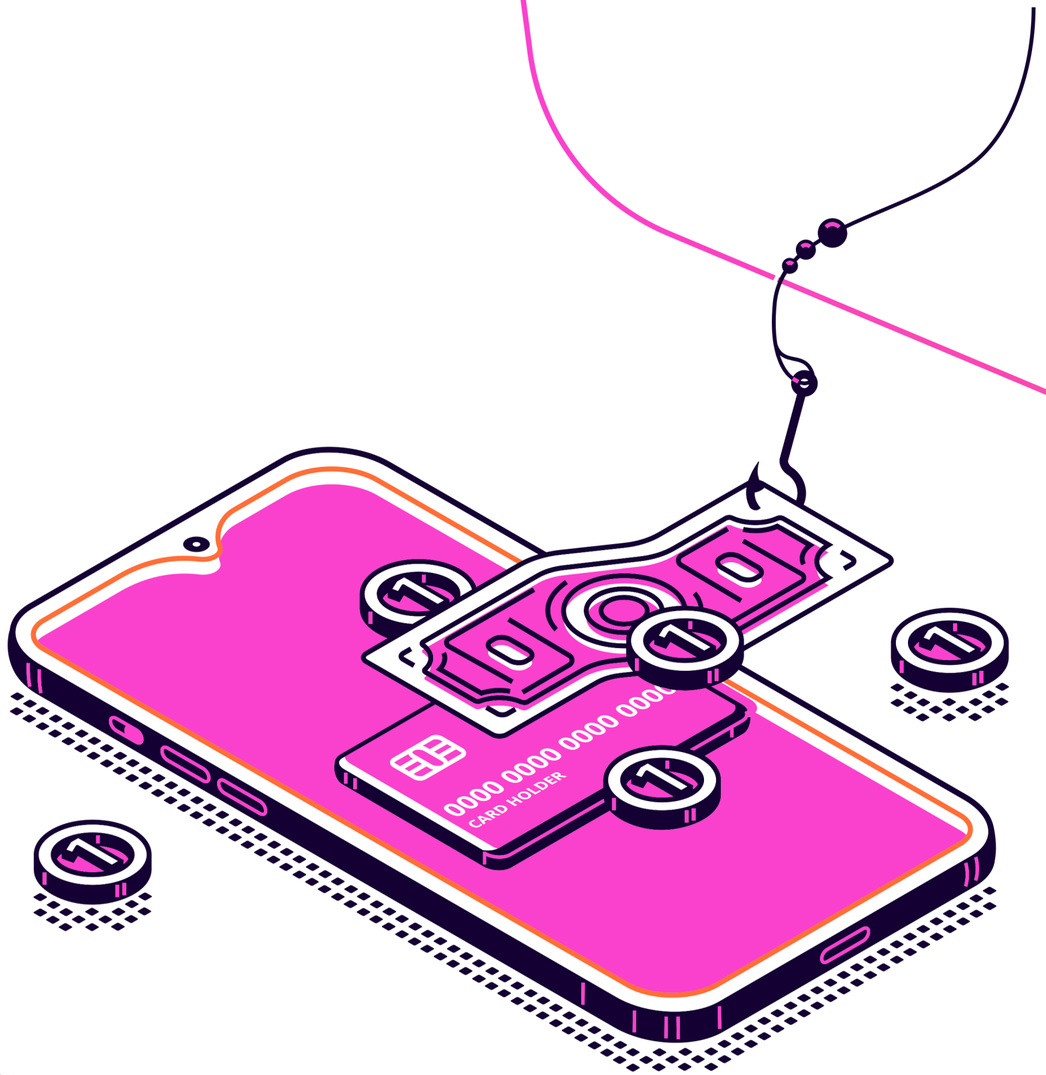
Michele Covi

10/06/2024

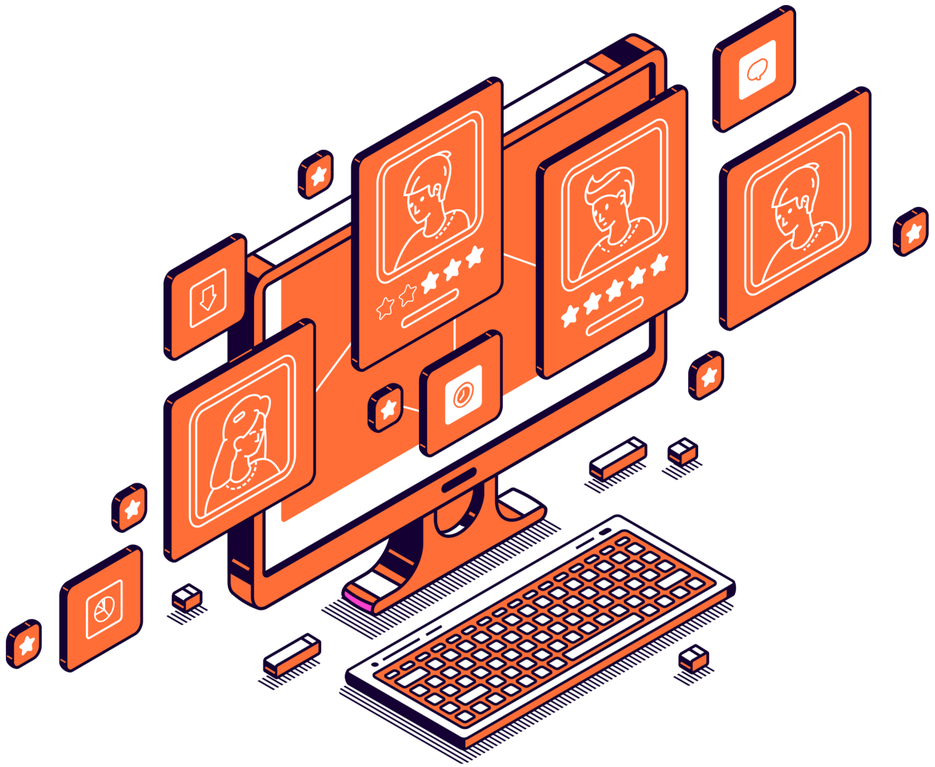
Introduction

This report details the static analysis of the executable file Malware_U3_W2_L1.exe, conducted as part of cybersecurity activities to identify and understand the potential threats posed by the file under examination. The objective is to assess the malware's capabilities, its interactions with the host system, and outline appropriate preventive and mitigation measures.

The analysis was performed using CFF Explorer, an advanced tool for analyzing Windows executable files. This tool allows for a detailed examination of the file's internal structures, including headers, sections, and library imports, providing a comprehensive overview of the malware's operational capabilities.



File Analysis Details



- File Name:: Malware_U3_W2_L1.exe
- File Size: 16 KB
- File Type: Windows Executable (PE)

Imported Libraries Analysis

During the static analysis with CFF Explorer, several critical dynamic libraries essential for the malware's functionality were identified:

Kernel32.dll

Handles core system operations such as process and thread creation, as well as memory manipulation.

Advapi32.dll

Implements advanced security-related functions, including Windows registry and service management.

Msvcrt.dll

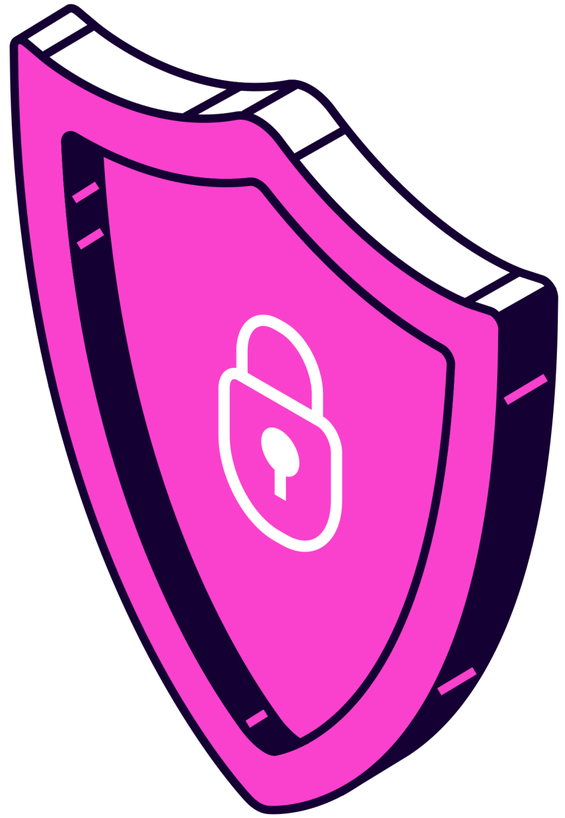
Microsoft's standard C library, used for general operations like string manipulation and calculations.

Wininet.dll

Provides networking capabilities, including protocols like HTTP and FTP, for direct communications.

File Section Analysis

The file contains three main sections that were examined to better understand the distribution of code and data:



01.

.text:

Section containing the malware's executable code. This section is marked as executable and non-modifiable.

02.

.rdata:

Contains constant data, such as strings and configurations. It is configured as non-executable and read-only.

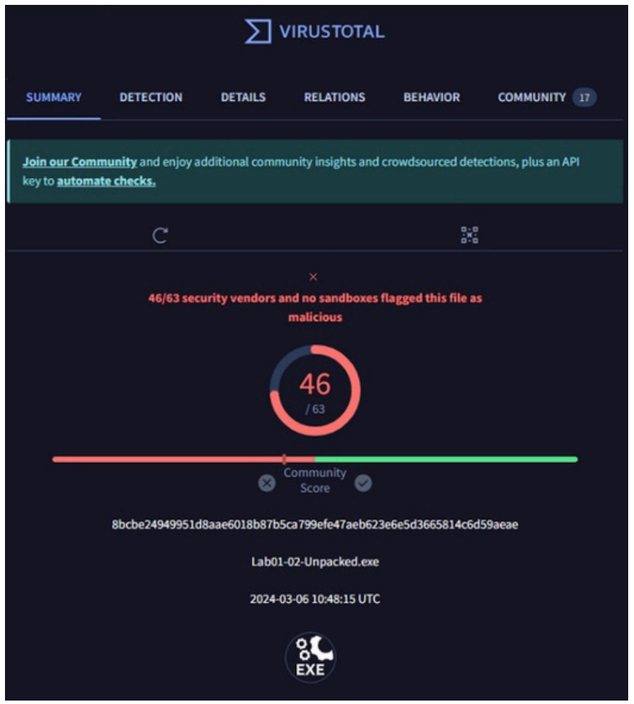
03.

.data:

Stores variable data used by the malware during execution, marked as readable and writable.

VirusTotal Analysis

The file was also analyzed using VirusTotal, which involved 63 different security engines. The file was flagged as malicious by 46 engines, demonstrating widespread recognition of its harmful potential across security tools. It was primarily classified as a Trojan, with spyware and rogue attributes, indicating significant compromise capabilities.



Final Considerations and Recommendations

The static analysis reveals a concerning picture of the malware's damaging potential, demonstrating capabilities for operating system manipulation and communication with external servers. The following actions are recommended:

- Continuous Monitoring: Implement dynamic analysis to track the malware's behavior in a controlled environment.
- Security Updates: Ensure all operating systems and applications are updated to mitigate known vulnerabilities.
- Training and Awareness: Educate end users on identifying and handling suspicious files.