



Static Malware Analysis Report

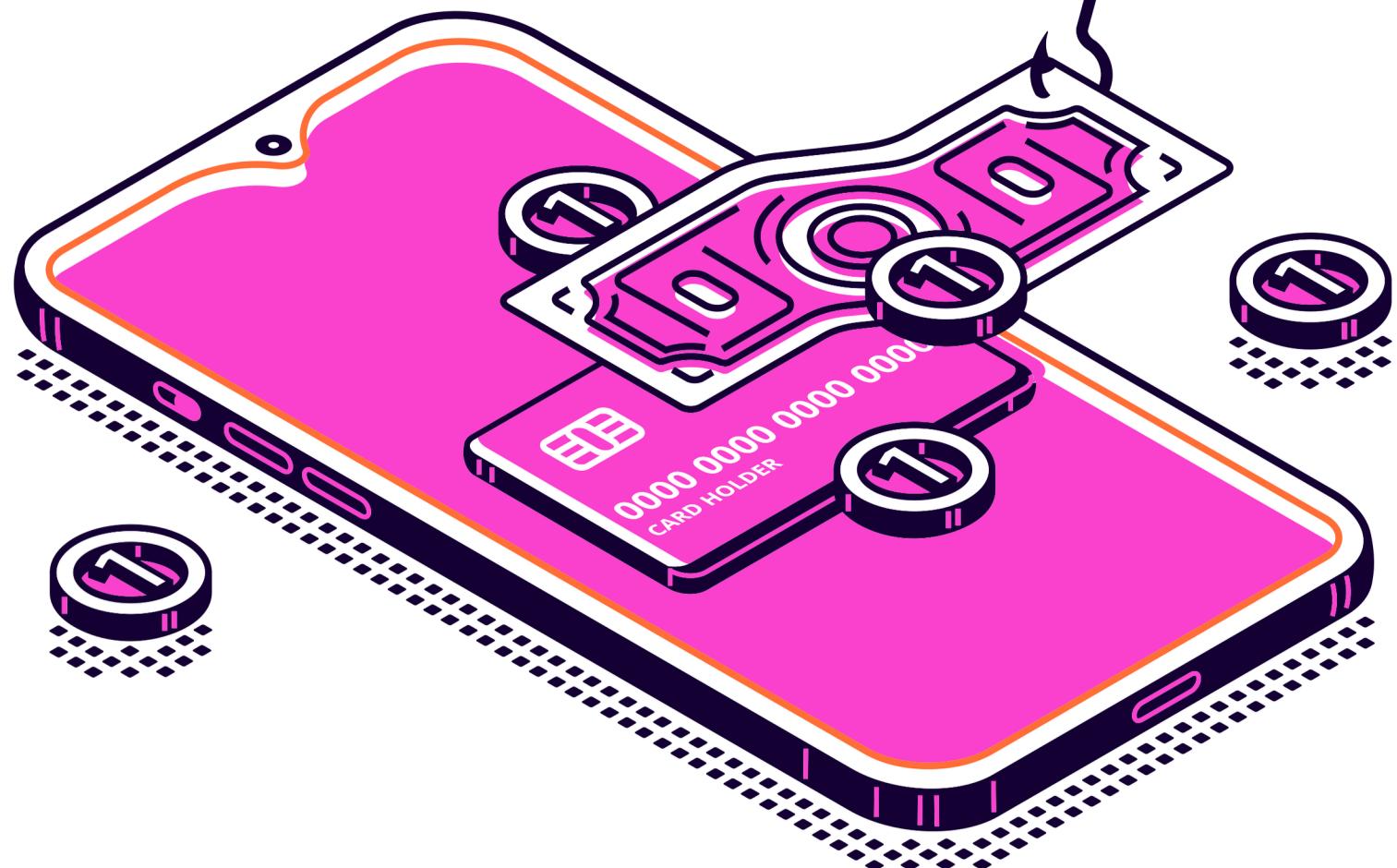
Michele Covi

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.

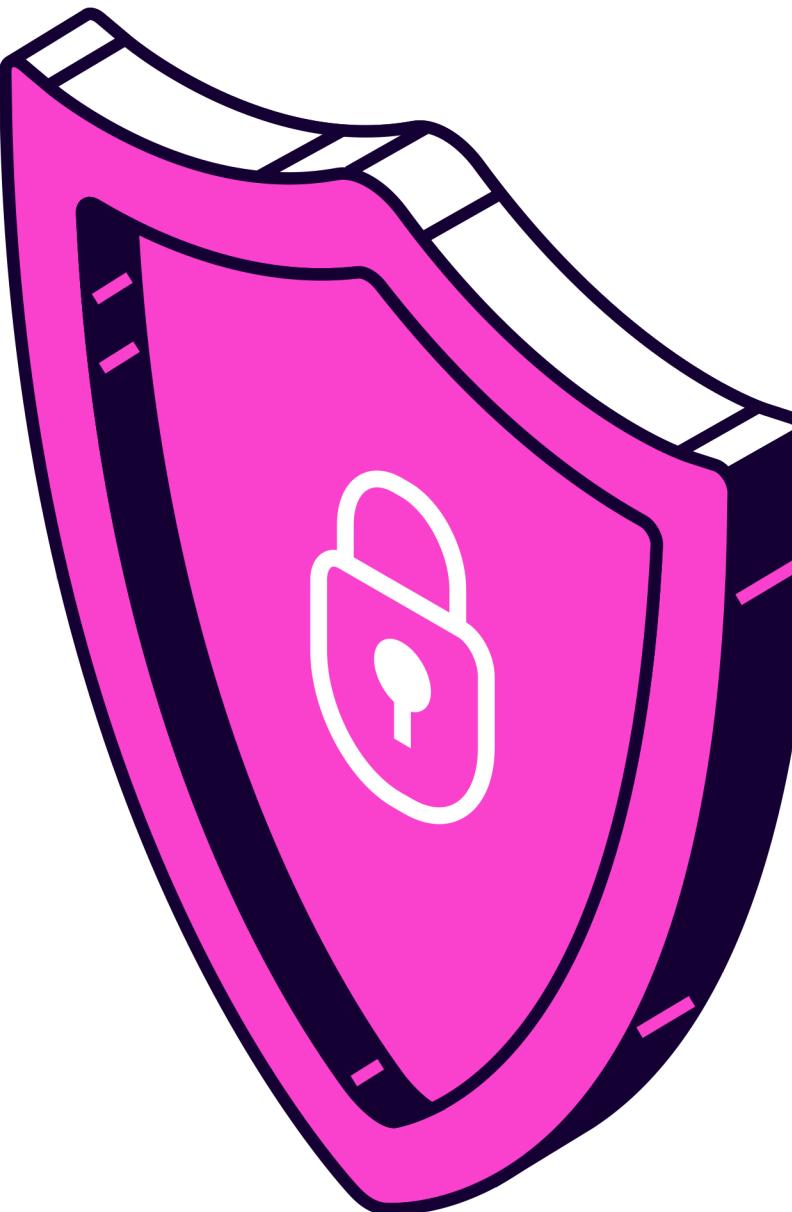


Wininet.dll

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.

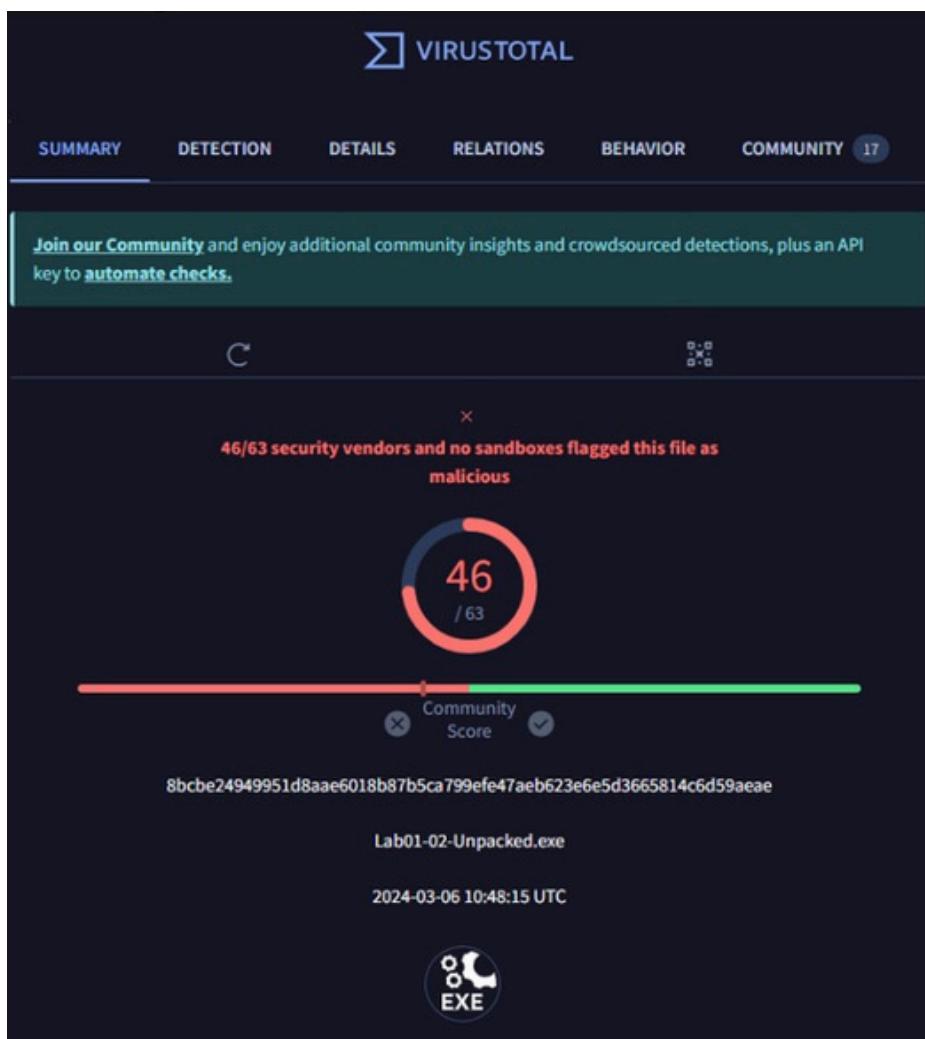
03.

.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.



Popular threat label	Threat categories	Family labels
Security vendors' analysis		
Do you want to automate checks?		
AhnLab-V3	Trojan/Win32.StartPage.C26214	
Alibaba	TrojanClicker:Win32/Tnega.2f275f7c	
ALYac	Gen:Variant.Ser.Ulise.216	
Anti-AVL	Trojan/Win32.TSGeneric	
Avast	Win32:AdwareX-gen [Adw]	
Avert Labs	GenericRXXE-YSAE4CA70697DF	
AVG	Win32:AdwareX-gen [Adw]	
Avira (no cloud)	TR/Rogue.7734716	
BitDefenderTheta	Gen:NN.Zexaf.F.36802.bmW@aG9@v0b	
Bkav Pro	W32.AIDetectMalware	
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	
Cylance	Unsafe	
Cynet	Malicious (score: 100)	
DeepInstinct	MALICIOUS	
Elastic	Malicious (high Confidence)	
eScan	Gen:Variant.Ser.Ulise.216	
ESET-NOD32	A Variant Of Win32/TrojanClicker.Agent.NVM	
Fortinet	W32/Agent.NVM!tr	
Google	Detected	
iKarus	Trojan.Win32.TrojanClicker	
Jiangmin	Trojan.Generic.fxq	
K7Antivirus	Spyware (0049d4ae1)	
K7GW	Spyware (0049d4ae1)	
Kingssoft	Win32.Troj.Generic.a	
Lionic	Trojan.Win32.Rogue.4lc	
Malwarebytes	RiskWare.Agent.MWLA	
MaxSecure	Trojan.Malware.2588.susgen	

Microsoft	Trojan:Win32/Tnega!MSR
NANO-Antivirus	Trojan.Win32.Click3.ivtlgd
Rising	Trojan.Clicker-Agent!8.13 (TFE:5:kDlhMGEbcJ)
Sangfor Engine Zero	Suspicious.Win32.Save.ins
Skyhigh (SWG)	GenericRXXE-YSAE4CA70697DF
Sophos	Mal/Generic-R
Symantec	ML.Attribute.HighConfidence
Trapmine	Malicious.moderate.ml.score
Trellix (FireEye)	Generic.mg.ae4ca70697df5506
TrendMicro	TROJ_GEN.R002C0DAK24
TrendMicro-HouseCall	TROJ_GEN.R002C0DAK24
Varist	W32/Agent.DJC.gen!Eldorado
VBA32	Trojan.Click
VirIT	Trojan.Win32.Generic.CMEY
Webscar	W32.Malware.Heur
Xcitium	Trojan.TR/Rogue.7734716
Yandex	Malware@#2m8d1kwsdlvz3
Zillya	Trojan.GenAsa+r0rTzlz07A
Acronis (Static ML)	Trojan.Agent.Win32.557086
Baidu	Undetected
ClamAV	Undetected
CMC	Undetected
Gridinsoft (no cloud)	Undetected
Kaspersky	Undetected
Palo Alto Networks	Undetected
Panda	Undetected
QuickHeal	Undetected

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.