Malware Analysis Report

By: **Nijat Ismayilov**

31st March 2025

Table of Contents

1. **Introduction**
2. **What is Malware?**
3. **The Importance of Malware Analysis**
4. **Types of Malware**
5. **Malware Analysis Methods**

    5.1.Static Analysis

    5.2.Dynamic Analysis

    5.3 Malware Analysis Sample

6. **Sandboxing & Detection Techniques**
7. **Indicators of Compromise (IOCs)**
8. **Tools Used for Malware Analysis**
9. **Conclusion & Recommendations**

1. Introduction

With the rise in cyber threats, malware remains a significant tool for attackers. Organizations must understand malware behavior to improve defense mechanisms. This report dissects a malware sample through **static and dynamic analysis**, examines its behavior in a **sandboxed environment**, and provides **Indicators of Compromise (IOCs).**

2. What is Malware?

Malware (malicious software) is any software designed to disrupt, damage, or gain unauthorized access to systems. Common examples include viruses, worms, Trojans, ransomware, and spyware.

3. The Importance of Malware Analysis

Malware analysis helps organizations to:

1.Identify how malware spreads.
2. Understand its behavior.
3. Develop effective detection and mitigation strategies.
4. Gather IOCs for future defense mechanisms.

4. Types of Malware

Type	Description
Virus	Attaches itself to legitimate files and spreads when executed.
Worms	Self-replicating malware that spreads across networks.
Trojans	Disguised as legitimate software to trick users into executing it.
Ransomware	Encrypts files and demands payment for decryption.
Spyware	Secretly collects user data without consent.
Rootkits	Hides malicious processes to maintain persistent access.

5. Malware Analysis Methods

5.1 Static Analysis

Static analysis examines malware **without executing it**, using reverse engineering tools. This includes:

- **Examining file properties** (using PEiD, Exeinfo PE).
- **Extracting strings** (using Strings, Floss).
- **Checking dependencies** (Dependency Walker).
- **Disassembling code** (Ghidra, IDA Pro).

Example (Using Ghidra):

- **Load the binary into Ghidra** and analyze its functions.
- Look for **suspicious API calls** (e.g., `CreateRemoteThread`, `VirtualAllocEx`).
- Identify **hardcoded IPs, domains, or URLs**.

5.2 Dynamic Analysis

Dynamic analysis involves **executing malware in a controlled environment (sandbox)** to observe its behavior.

- **Cuckoo Sandbox** – Runs malware in a virtualized environment.
- **Remnux** – A Linux distro specialized for malware analysis.
- **Wireshark** – Captures network traffic generated by the malware.
- **Procmon & RegShot** – Monitors system changes.

5.3 Malware Sample Overview

Sample Details

- **SHA-256 Hash:** `33f2ddf371bcd01156ebac2c17567c1e61e7518fa3b77ab274d07706e04f5cc1`

- **File Type:** `.TAR Archive` (Compressed file)
- **Size:** 1.20 MB
- **Detection Rate:** 29/64 antivirus engines flagged it as malicious

5.3.1 Analysis of the Malware

5.3.1.1 Static Analysis

Static analysis involves examining the malware binary without executing it.

- **Identified as:** `Trojan.Droptor/GenSteal.MSIL`
- **Threat Category:** Trojan
- **Family Labels:** `droptor`, `gensteal`, `msil`
- **Signature-Based Detections:**
    - Multiple vendors flagged it as `MSILZilla`, indicating it is written in `.NET/MSIL`
    - Microsoft detected it as `Trojan.Script.Wacatac.B!ml`
    - Possible threat indicator: **Stealer Trojan**, often used for credential theft

5.3.1.2 Dynamic Analysis

Dynamic analysis involves running the malware in a controlled environment to observe behavior.

- **Potential Behavior (Based on Signature Matching):**
    - **Data Exfiltration**: May attempt to steal credentials or sensitive data
    - **Persistence Mechanism**: Could modify registry keys for persistence
    - **Network Activity**: Likely connects to external command-and-control (C2) servers

- ○ **File Modifications**: May drop additional payloads

5.3.2 Indicators of Compromise (IOCs)

Indicators of Compromise help detect similar infections.

IOC Type	Value
SHA-256	`33f2ddf371bcd01156ebac2c17567c1e61e7518fa3b77ab274d07706e04f5cc1`
Malware Family	Trojan.Droptor / GenSteal
Possible C2 Domains	(Need further network analysis)
Registry Modifications	Suspicious persistence mechanisms

5.3.3 Recommendations and Mitigation

Prevention Strategies

Avoid downloading unknown `.tar` files or executables
Regularly update antivirus signatures
Monitor network traffic for suspicious outgoing connections
Implement endpoint security and behavioral analysis tools

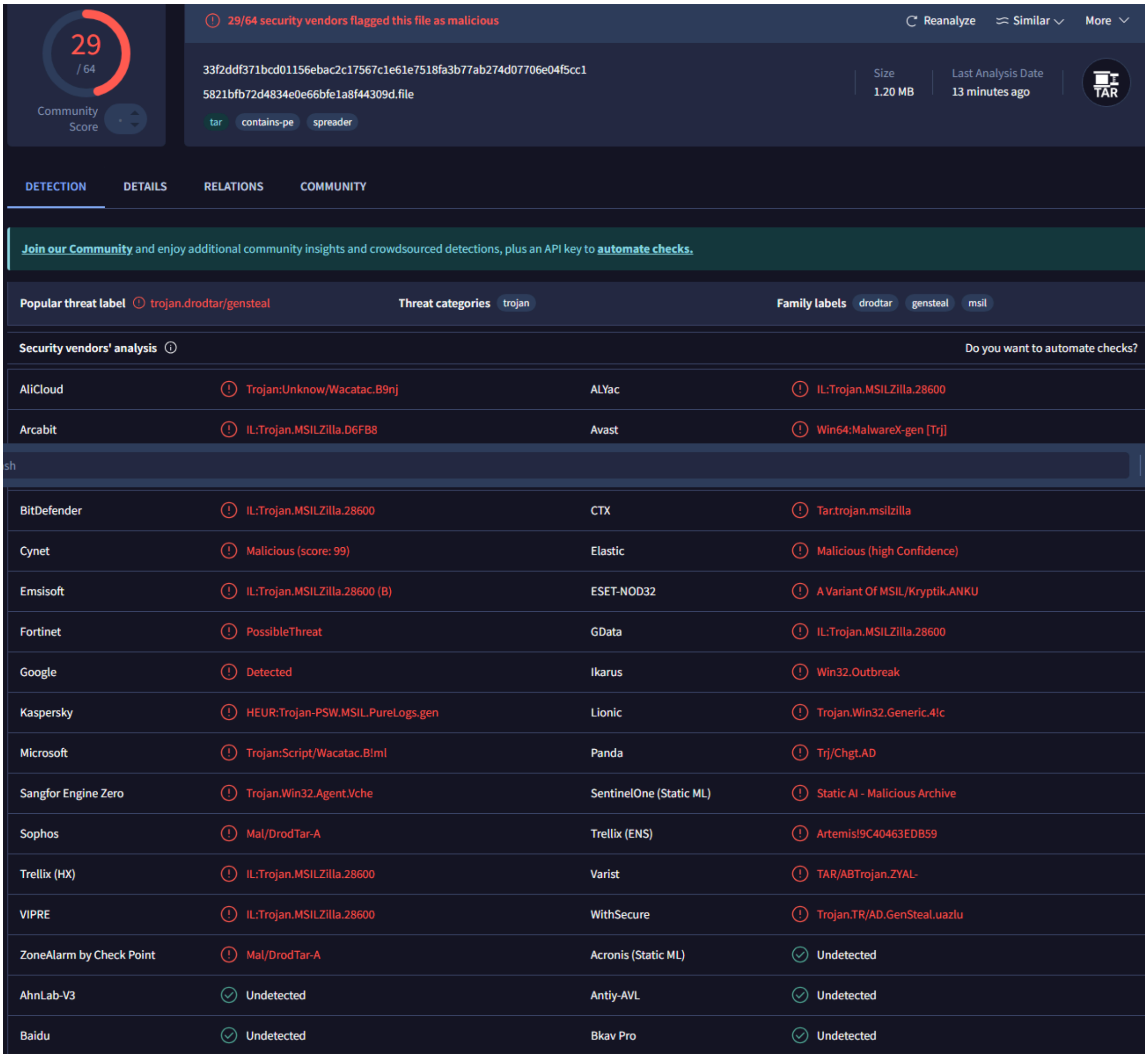
Incident Response Steps

1: **Isolation**: Quarantine infected machines
2: **Forensics**: Examine logs, file system changes, and memory dumps

3: **Mitigation**: Block related domains, remove persistence mechanisms
4: **Patch & Protect**: Keep OS and software updated

5.3.4 Conclusion

This analysis highlights that the malware is a potential **Trojan Stealer**, likely designed to extract credentials or sensitive data. Given its `.NET/MSIL` nature, it can be obfuscated and challenging to detect. Proper security measures and endpoint monitoring can help mitigate similar threats.



29/64 security vendors flagged this file as malicious

33f2ddf371bcd01156ebac2c17567c1e61e7518fa3b77ab274d07706e04f5cc1
5821bfb72d4834e0e66bfe1a8f44309d.file

tar contains-pe spreader

Size
1.20 MB

Last Analysis Date
13 minutes ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks.**

Popular threat label trojan.drodtar/gensteal **Threat categories** trojan **Family labels** drodtar gensteal msil

Security vendors' analysis Do you want to automate checks?

AliCloud	Trojan:Unknow/Wacatac.B9nj	ALYac	IL:Trojan.MSILZilla.28600
Arcabit	IL:Trojan.MSILZilla.D6FB8	Avast	Win64:MalwareX-gen [Trj]
BitDefender	IL:Trojan.MSILZilla.28600	CTX	Tar.trojan.msilzilla
Cynet	Malicious (score: 99)	Elastic	Malicious (high Confidence)
Emsisoft	IL:Trojan.MSILZilla.28600 (B)	ESET-NOD32	A Variant Of MSIL/Kryptik.ANKU
Fortinet	PossibleThreat	GData	IL:Trojan.MSILZilla.28600
Google	Detected	Ikarus	Win32.Outbreak
Kaspersky	HEUR:Trojan-PSW.MSIL.PureLogs.gen	Lionic	Trojan.Win32.Generic.4!c
Microsoft	Trojan:Script/Wacatac.B!ml	Panda	Trj/Chgt.AD
Sangfor Engine Zero	Trojan.Win32.Agent.Vche	SentinelOne (Static ML)	Static AI - Malicious Archive
Sophos	Mal/DrodTar-A	Trellix (ENS)	Artemis!9C40463EDB59
Trellix (HX)	IL:Trojan.MSILZilla.28600	Varist	TAR/ABTrojan.ZYAL-
VIPRE	IL:Trojan.MSILZilla.28600	WithSecure	Trojan.TR/AD.GenSteal.uazlu
ZoneAlarm by Check Point	Mal/DrodTar-A	Acronis (Static ML)	✓ Undetected
AhnLab-V3	✓ Undetected	Antiy-AVL	✓ Undetected
Baidu	✓ Undetected	Bkav Pro	✓ Undetected

6. Sandboxing & Detection Techniques

Technique	Purpose
API Hooking	Monitors system calls made by malware.
Code Injection	Determines if malware injects itself into other processes.
Memory Analysis	Analyzes malicious behavior in RAM.
Network Analysis	Identifies malicious IPs, domains, and traffic patterns.

7. Indicators of Compromise (IOCs)

IOCs help in identifying **infected systems** and **tracking malware activity**.

Type of IOC	Example
File Hash (MD5, SHA-256)	`a2c4f3...3d2f7e7f`
Malicious Domains	`badsite[.]com`
IP Addresses	`192.168.1.100`
Registry Modifications	`HKLM\Software\Microsoft\Windows\CurrentVersion\Run\malware.exe`
Mutexes	`Global\Malware_Mutex`

8. Tools Used for Malware Analysis

Tool	Purpose
Ghidra	Static analysis and reverse engineering.
IDA Pro	Advanced disassembly and debugging.
Cuckoo Sandbox	Safe execution of malware for analysis.
Wireshark	Captures and analyzes network traffic.
Procmon	Monitors system activity in real time.
VirusTotal	Checks malware signatures against known databases.

---

9. Conclusion & Recommendations

🔹 **Avoid downloading untrusted software.**
🔹 **Use endpoint protection (EDR, antivirus, sandboxing).**
🔹 **Regularly update security tools to detect new malware variants.**
🔹 **Monitor network activity for abnormal patterns.**