MALWARE ANALYSIS

1. Introduction :

This report documents the analysis of a malicious Windows executable submitted to VirusTotal. It covers both static analysis (hashes, file properties, antivirus detections) and dynamic behavior (sandbox activity, network traffic), along with IOCs and tactics.

2. Malware Overview

- **File name(s):**
  - malware_1.exe / tinysolaris.exe (aliases include malware 1, malware_1[1], malware_1[2])
- **File type:** PE32 executable (GUI) for Intel x86, UPX-compressed
- **File size:** 222 000 bytes (~217 KB)

3. Static Analysis

3.1 Hashes and Signatures

- MD5: 4b0596d3f69ea231546c336967d9f051
- SHA-1: c9029ba1cf9ddaeb7d0fec83aa5faec59a5ddd7f
- SHA-256: 1280e38562fbb405fa46dec150288fd890e077c653de863bcfecf20a6c3dd873

3.2 PE and Packer Info

- Rich PE header hash: 2bd26b22bb65b1859bc8269f4c1c2104
- Packer: UPX 2.90 [LZMA]

- Compiler/Linker:
  - Compiled with Microsoft Visual C/C++ 15.00.24427; MS Linker 14.00.24247

3.3 Compiled Timestamp

- Compilation Time / PE time-stamp: 2025-02-22 16:33:45 UTC

3.4 Antivirus Detection Summary

Out of 72 scanners, 58 flagged it as malicious (~81%)

- Popular threat name: Trojan.Lazy/DiskWriter (families: lazy, diskwriter, badjoke)
- Notable detections:
  - AhnLab-V3: Trojan/Win.Generic.C5733813
  - Kaspersky: Trojan.Win32.DiskWriter.mkf
  - Palo Alto NANO-Antivirus: Trojan.Win32.DiskWriter.kvusuy
  - TrendMicro-HouseCall: TROJ_GEN.R002H09BN25
  - ...and many others indicating a disk-writer Trojan or «lazy» variant

4. Dynamic Analysis

4.1 Behavioral Tags (from execution)

- checks-disk-space, checks-user-input, detect-debug-environment, long-sleeps, obfuscated, upx

4.2 Sandbox Results

- Flagged by **Yomi Hunter** and **VMRay** sandboxes as MALWARE
- Activity summary:
  - MITRE categories detected (Execution TA0002, Persistence TA0003, Privilege Escalation TA0004, Defense Evasion TA0005, Credential Access TA0006, Discovery TA0007, Collection TA0009, Command & Control TA0011)

4.3 Artifacts and Network Indicators

- **Contacted domain:** res.public.onecdn.static.microsoft.com (no detections); domain created 2023-05-05
- **Contacted IPs:**
    - Local 192.168.0.43, .53 (likely sandbox environment)
    - External US IP ranges: 20.69.140.28, 20.99.133.109, 23.196.145.221, 23.213.37.172, 23.32.75.11–20, 23.32.75.23–24
- **Dropped files:** 4 unknown files (none flagged); includes one named “DR0”
- **Bundled files:** 3 additional items (e.g. XML)

5. IOCs & MITRE Mapping

Indicator	Value / Technique
SHA-256	1280e38562f...d873
First seen	2025-02-23 21:21:24 UTC
Compilation timestamp	2025-02-22 16:33:45 UTC
Packer	UPX 2.90
Dropper behavio	Creates files, scheduled tasks
Domain	res.public.onecdn.static.microsoft.com
IP Addresses	Listed above
Detected Techniques	Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, C2 (TA0002–TA0011)

6. Static vs. Dynamic Analysis – Comparison

- **Static Analysis** (hashes, packer detection, AV hits): safe and fast; gives early indicators and metadata cybermaxx.comlinkedin.com
- **Dynamic Analysis** (sandbox execution): reveals runtime behaviors—file drops, network access, MITRE tactics—especially useful for packed malware cybermaxx.comlinkedin.combitdefender.com

7. Conclusion & Recommendations

1. **Confirmed as malicious Trojan**: flagged by both static AV scans and dynamic sandboxes.
2. **Primary behavior**: disk-writing (possibly damaging or extorting data), persistence mechanisms, environmental checks to avoid debuggers.
3. **Suggested response**:
   - Block the associated domain and IPs at the firewall.
   - Eradicate dropped/bundled files.
   - Monitor for scheduled task artifacts.
4. **Further analysis**:
   - Reverse engineer unpacked binary to inspect capabilities in detail.
   - Capture full sandbox logs (API calls, registry, network) for additional IOCs.

8. References

- VirusTotal detection and behavior screenshots
- Microsoft & TrendMicro definitions for DiskWriter microsoft.comtrendmicro.com
- Static vs. Dynamic malware analysis descriptions cybermaxx.comlinkedin.combitdefender.com