# Malware Analysis

## 1. Static Malware Analysis

### File Information :

* **File Name:** malware 1.unknown
* **SHA256**: 1280e38562fbb405fa4d54b03dd3c54de863bcfecf20a6c3dd873
* **Size**: 222.00 KB
* **Type**: Win32 EXE
* **Compiled On**: 2023-05-08 07:13:28 UTC
* **First Submission**: 2023-05-08
* **Last Analysis**: 2023-06-08
* **Signature:** Unsigned
* Detection Summary
* **Detected as Malicious by**: 58 / 72 antivirus engines
* **Community Score:** Malicious
* Secondary names:
* malware 1.unknown
* malware\_1[2].unknown
* malware\_1[1].unknown
* tinySolaris.exe
* tinysolaris.exe
* malware1
* 1280e38562fbb405fa46dec150288fd890e077c653de863bcfecf20a6c3dd873.exe
* Common Detection Names
* Trojan.Win32.Generic
* Trojan.MalPack
* Packed.Generic
* Trojan.Dropper
* Win32:Malware-gen
* Execution Parents:

1. Name: Static Analysis.7z
   * + - Type: 7ZIP
       - Scanned: 2025-06-09
       - Detections: 24 / 57
2. Name: ViewerMade2-Malwares.zip
   * + - Type: ZIP
       - Scanned: 2025-03-29
       - Detections: 23 / 45
3. Name: Wormhole jE1x20.zip
   * + - Type: ZIP
       - Scanned: 2025-06-09
       - Detections: 22 / 55
4. Name: my-malwares-main.zip
   * + - Type: ZIP
       - Scanned: 2025-04-18
       - Detections: 41 / 58
5. Name: MA-1.7z
   * + - Type: 7ZIP
       - Scanned: 2025-06-09
       - Detections: 40 / 63

### Tags

* packer
* checks-disk-space
* checks-system
* detects-debug-environment
* upx
* Network Indicators
* **Contacted Domains:** mailtrack.linkedmailtrack.com
* **Contacted IPs:** 23.21.117.137, 20.99.132.53, 52.217.132.41, 52.217.41.228, 3.217.13.170, 23.21.71.37, 23.23.73.53

### Execution Parents

* Static-Analysis-2.zip
* Wormhole03dd4ea.zip
* Wormhole-Fixed.zip
* my-malware-email.zip
* Mal3.zip

### Static Properties

* MD5: 24fce03f2f2d27675831abdb2b8ff79b
* SHA1: cf96f5d0c3f0a84a1be42de73bbcb9f37f0d9fc7
* File Type: PE32 executable (GUI) Intel 80386, for MS Windows
* Machine Type: Intel 386 or later, and compatible processors
* Imphash: fef2f1e5f4ee02bb0b7e46c57b17b1a1

### Imports

* Kernel32.dll
* User32.dll
* Advapi32.dll
* Shell32.dll
* Gdi32.dll
* Ws2\_32.dll