



 File Name:
 virussign.com_0f44b81c33a38e7725714b89c0bbe02a.vir

 File Type:
 PE32 executable (GUI) Intel 80386, for MS Windows

 SHA1:
 72377207577f6222000794b56cf54b61c09f24cc

MD5: 0f44b81c33a38e7725714b89c0bbe02a **First Seen Date:** 2024-07-14 13:50:45 UTC

Number of Clients Seen: 2

Last Analysis Date: 2024-07-15 14:15:07 UTC

Human Expert Analysis Date: 2024-07-15 14:14:59 UTC

Human Expert Analysis Result: Malware

Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Analysis Summary

| ANALYSIS TYPE | DATE | VERDICT | |
|---------------------------------------|-------------------------|-------------------|---|
| Signature Based Detection | 2024-07-14 16:16:33 UTC | Malware | 0 |
| Static Analysis Overall Verdict | 2024-07-14 13:51:12 UTC | Highly Suspicious | 0 |
| Precise Detectors Overall Verdict | 2024-07-15 14:15:07 UTC | No Match | ? |
| Human Expert Analysis Overall Verdict | 2024-07-15 14:14:59 UTC | Malware | 0 |
| File Certificate Validation | | Not Applicable | ? |

Static Analysis

| STATIC ANALYSIS OVERALL VERDICT | RESULT | |
|---|------------|----------|
| Highly Suspicious | | 0 |
| DETECTOR | RESULT | |
| Optional Header LoaderFlags field is valued illegal | Clean | • |
| Non-ascii or empty section names detected | Clean | • |
| Illegal size of optional Header | Clean | • |
| Packer detection on signature database | Unknown | ? |
| Based on the sections entropy check! file is possibly packed | Suspicious | 0 |
| Timestamp value suspicious | Clean | • |
| Header Checksum is zero! | Suspicious | 0 |
| Enrty point is outside the 1st(.code) section! Binary is possibly packed | Clean | • |
| Optional Header NumberOfRvaAndSizes field is valued illegal | Clean | • |
| Anti-vm present | Clean | ② |
| The Size Of Raw data is valued illegal! Binary might crash your disassembler/debugger | Clean | ② |
| TLS callback functions array detected | Clean | • |

Dynamic Analysis

No Dynamic Analysis Result Received

Behavioral Information is not Available

Precise Detectors Analysis Results

| DETECTOR NAME | DATE | VERDICT | | REASON |
|-----------------------------------|-------------------------|----------|---|-------------|
| Static Precise PUA Detector 1 | 2024-07-14 13:51:08 UTC | No Match | ? | NotDetected |
| Static Precise PUA Detector 4 | 2024-07-14 13:51:08 UTC | No Match | ? | NotDetected |
| Static Precise NI Detector 3 | 2024-07-14 13:51:08 UTC | No Match | ? | NotDetected |
| Static Precise PUA Detector 5 | 2024-07-14 13:51:08 UTC | No Match | ? | NotDetected |
| Static Precise Trojan Detector 1 | 2024-07-14 13:51:08 UTC | No Match | ? | NotDetected |
| Static Precise Trojan Detector 3 | 2024-07-14 13:51:08 UTC | No Match | ? | NotDetected |
| Static Precise PUA Detector 6 | 2024-07-14 13:51:08 UTC | No Match | ? | NotDetected |
| Static Precise Trojan Detector 12 | 2024-07-14 13:51:08 UTC | No Match | ? | NotDetected |
| Static Precise Virus Detector 1 | 2024-07-14 13:51:08 UTC | No Match | ? | NotDetected |
| Static Precise Virus Detector 2 | 2024-07-14 13:51:08 UTC | No Match | ? | NotDetected |
| Static Precise Trojan Detector 13 | 2024-07-14 13:51:08 UTC | No Match | ? | NotDetected |
| Static Precise PUA Detector 2 | 2024-07-14 13:51:08 UTC | No Match | ? | NotDetected |

Advance Heuristics

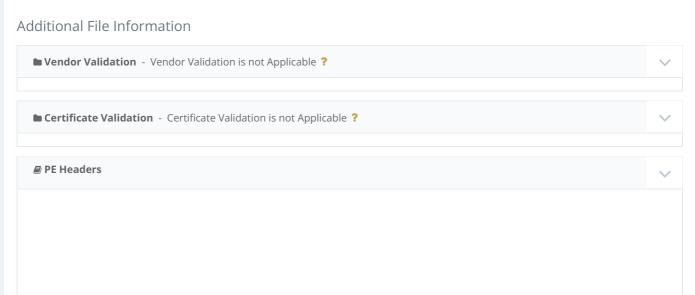
No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2024-07-15 06:18:56 UTC
Analysis End Date: 2024-07-15 14:14:59 UTC
File Upload Date: 2024-07-14 13:50:36 UTC
Human Expert Analyst Feedback:

Verdict: Malware Malware Family:

Malware Type: Trojan Generic



| PROPERTY | VALUE |
|------------------------|--|
| Compilation Time Stamp | 0x4407306D [Thu Mar 2 17:50:37 2006 UTC] |
| Debug Artifacts | |
| Entry Point | 0x404c20 (.text) |
| Exifinfo | |
| File Size | 1553603 |
| File Type Enum | 6 |
| Imphash | |
| Machine Type | Intel 386 or later - 32Bit |
| Magic Literal Enum | 3 |
| Mime Type | application/x-dosexec |
| Number Of Sections | 3 |
| Sha256 | a8a358485e1b69cf2d9200cfe275dc529319eff74ea4b0b1c1b9e4ec66e25e44 |
| Ssdeep | |
| Trid | |

| # PE Sections | | | | | | ~ |
|---------------|-----------------|--------------|----------|---------------|----------------------------------|---|
| NAME | VIRTUAL ADDRESS | VIRTUAL SIZE | RAW SIZE | ENTROPY | MD5 | |
| .text | 0x1000 | 0xa566 | 0xa600 | 6.44597193467 | 5b219decd6fd463ad3ad0dddf889571c | |
| .rdata | 0xc000 | 0x6504 | 0x6600 | 5.17229189334 | 8806421e2c7a0ca959009736cb2393d1 | |
| .data | 0×13000 | 0x18000 | 0x17200 | 7.64612659165 | 9d6482c94c45cf571f1e743c3f41f923 | |