Static analysis of Goldenhelper Malware (Golden Tax malware)

By Adetomiwa

Published: 2022-03-04 · Archived: 2026-04-05 18:17:01 UTC

“GoldenHelper” was discovered on July 14, 2020 embedded in Golden Tax Invoicing Software, an invoice issuing software used by Chinese banks. This malware variant seems to have been active between January 2018 and July 2019.

Press enter or click to view image in full size

```
seg000:0000000000000000 ;
seg000:0000000000000000 ; +-------------------------------------------------------------------------+
seg000:0000000000000000 ; |   This file has been generated by The Interactive Disassembler (IDA)    |
seg000:0000000000000000 ; |           Copyright (c) 2018 Hex-Rays, <support@hex-rays.com>           |
seg000:0000000000000000 ; |                         Freeware version                                |
seg000:0000000000000000 ; +-------------------------------------------------------------------------+
seg000:0000000000000000 ;
seg000:0000000000000000 ; Input SHA256 : A1AA0684813CFE9D7ED5C491C8AB132E5583B4FD02187FDAE8AA4D934D933F29
seg000:0000000000000000 ; Input MD5    : 490D17A5B016F3ABC14CC57F955B49B3
seg000:0000000000000000 ; Input CRC32  : 38374316
seg000:0000000000000000
seg000:0000000000000000 ; File Name   : C:\Users\User\Desktop\Malware_Samples (VBoxSvr)\Malware-Feed-master\
seg000:0000000000000000 ; Format      : Binary file
seg000:0000000000000000 ; Base Address: 0000h Range: 0000h - 1EE00h Loaded length: 1EE00h
seg000:0000000000000000
seg000:0000000000000000                 .686p
seg000:0000000000000000                 .mmx
seg000:0000000000000000                 .model flat
seg000:0000000000000000
seg000:0000000000000000 ; ===========================================================================
seg000:0000000000000000
seg000:0000000000000000 ; Segment type: Regular
seg000:0000000000000000 seg000          segment byte public '' use64
seg000:0000000000000000                 assume cs:seg000
seg000:0000000000000000                 assume es:nothing, ss:nothing, ds:nothing, fs:nothing, gs:nothing
seg000:0000000000000000                 db  4Dh ; M
seg000:0000000000000001                 db  5Ah ; Z
seg000:0000000000000002                 db  90h
seg000:0000000000000003                 db    0
seg000:0000000000000004                 db    3
```

Fig 1.0: First bytes of malware sample

Press enter or click to view image in full size

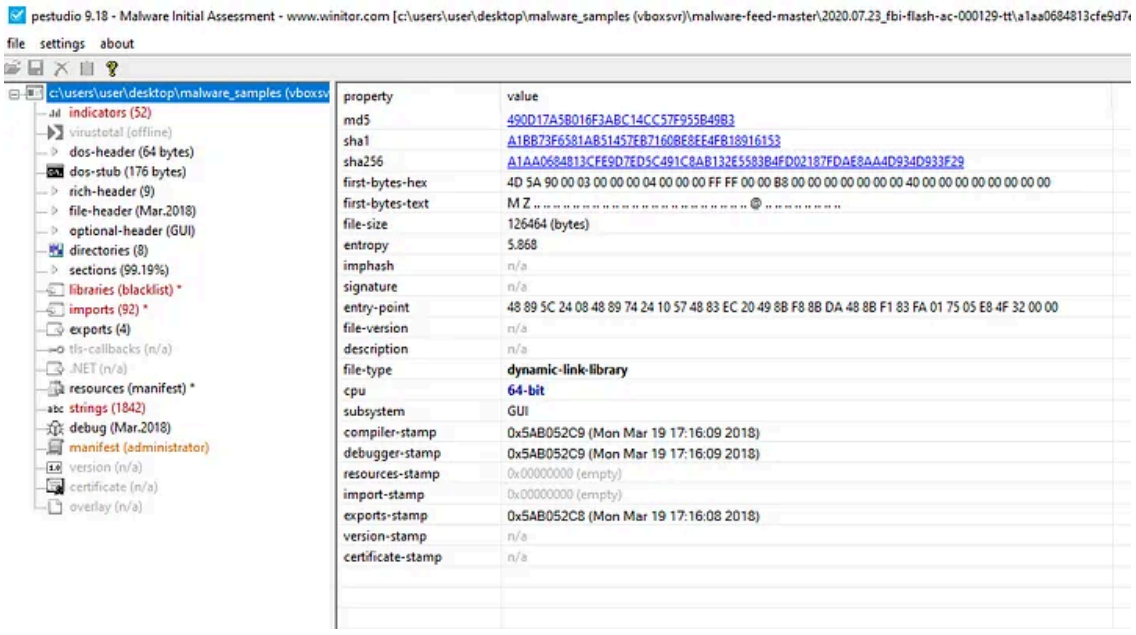

Fig 1.1: File header in PE studio

The following details were obtained from initial static analysis:

- File-type: dynamic-link-library (.dll)
  CPU: 64-bit
  Subsystem: GUI
  Compiler-stamp: 0x5AB052C9 (Mon Mar 19 17:16:09 2018)
  Debugger-stamp: 0x5AB052C9 (Mon Mar 19 17:16:09 2018)
  File-size: 126464 (bytes)
- Hashes:
  md5: 490D17A5B016F3ABC14CC57F955B49B3
  sha1: A1BB73F6581AB51457EB7160BE8EE4FB18916153
  sha256:A1AA0684813CFE9D7ED5C491C8AB132E5583B4FD02187FDAE8AA4D934D933F29
- File path: F:\DLL\dll-client-0309\x64\Release\SvcDll.pdb

Embedded Strings.

PE Studio identified ~1870 strings, the following have been highlighted:

- The following appear to be files that will be loaded during runtime
  http://%s/app/taxver[.]jpg
  http://%s/app/tps32[.]gif
  http://%s/data/msabs[.]dat
  http://%s/data/msabb[.]rar
  http://%s/data/tax32[.]zip…
