Analysis Zeus Banking trojan report

Fingerprint

Pestudio hashes:

footprint > sha256,69E966E730557FDE8FD84317CDEF1ECE00A8BB3470C0B58F3231E170168AF169

Filename : invoice_2318362983713_823931342io.pdf.exe

first-bytes-hex,4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00

first-bytes-text,M Z .. .. @ .. ..

Basic Static Analysis

Pestudio:

names	
file	c:\users\io\desktop\invoice_2318362983713_823931342io.pdf.exe
debug	n/a
export	corect.com
version	n/a
manifest	n/a
.NET > module	n/a
certificate > program-name	n/a

Corect.com yielded no interesting results

property	value
section	section[0]
name	.text
footprint > sha256	8309B5D320B3D392E25AFD5...
entropy	6.707
file-ratio (99.60%)	18.42 %
raw-address (begin)	0x00000400
raw-address (end)	0x0000BA00
raw-size (251904 bytes)	0x0000B600 (46592 bytes)
virtual-address	0x00001000
virtual-size (250379 bytes)	0x0000B571 (46449 bytes)

Raw address size and virtual siza are similar. Most likely is not packet.

API calls:

- AllowSetForegroundWindow
- GetEnvironmentVariable
- GetEnvironmentVariable
- VkKeyScan
- GetAsyncKeyState
- PathRenameExtension
- WriteFile
- FindNextFile

- GetCurrentThread
- WinExec
- GlobalAddAtom
- GetClipboardOwner
- GetClipboardData
- EnumClipboardFormats
- DdeQueryNextServer
- GetConsoleAliasExesLength
- SetCurrentDirectory
- CallWindowProc
- UpdateWindow
- GetCapture
- IsWindowEnabled
- GetWindowTextLength
- DeleteCriticalSection
- SizeofResource
- GetLogicalDrives
- GetTickCount
- GetDriveType
- LocalUnlock
- HeapFree
- VirtualQueryEx
- LocalAlloc
- LocalFree
- CopyAcceleratorTable
- SwapMouseButton
- PathQuoteSpaces
- PathCombine
- GetCompressedFileSize
- CreateFileMapping
- GetPrivateProfileInt
- FreeLibrary
- GetModuleHandle

Library:

SHLWAPI.dll,-,-,0x00020208,0x00020078,implicit,21,-,Shell Light-weight Utility Library

KERNEL32.dll,-,-,0x00020190,0x00020000,implicit,29,-,Windows NT BASE API Client

USER32.dll,-,-,0x00020260,0x000200D0,implicit,27,-,Multi-User Windows USER API Client Library

CAPA output:

md5	ea039a854d20d7734c5add48f1a51c34
sha1	9615dca4c0e46b8a39de5428af7db060399230b2
sha256	69e966e730557fde8fd84317cdef1ece00a8bb3470c0b58f3231e170168af169
analysis	static
os	windows
format	pe
arch	i386
path	C:/Users/IO/Desktop/invoice_2318362983713_823931342io.pdf.exe

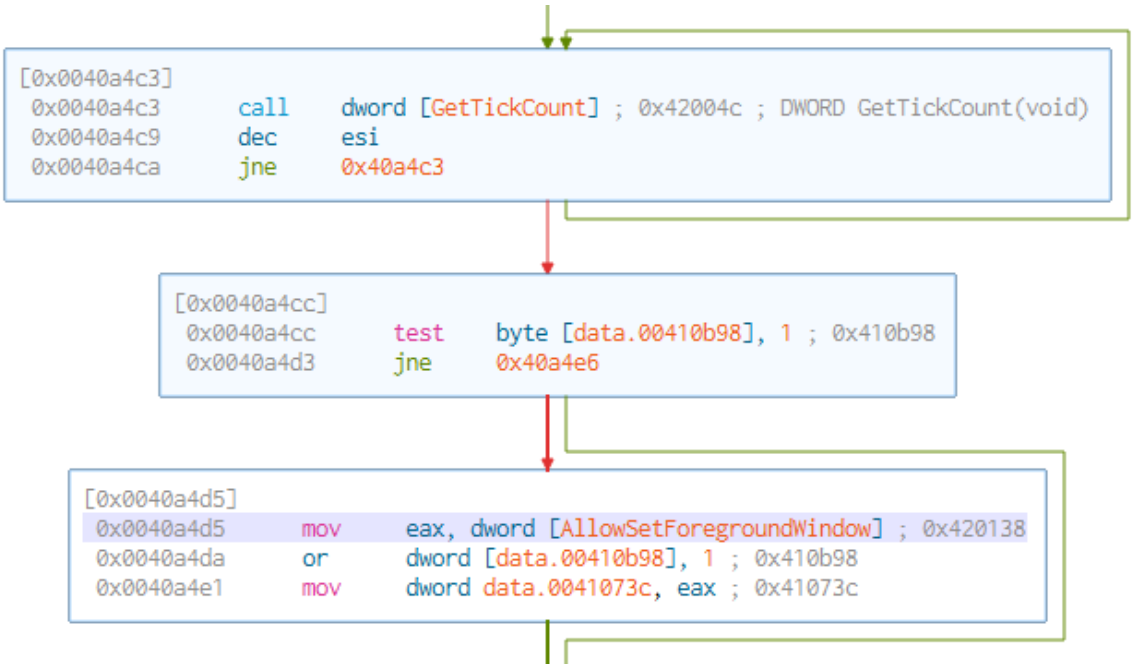
ATT&CK Tactic	ATT&CK Technique
DEFENSE EVASION	Virtualization/Sandbox Evasion::System Checks T1497.001

MBC Objective	MBC Behavior
ANTI-BEHAVIORAL ANALYSIS	Virtual Machine Detection [B0009]

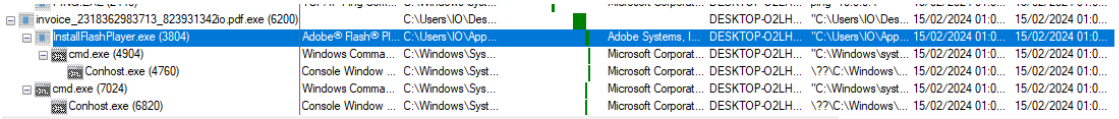
Capability	Namespace
reference anti-VM strings targeting VMWare	anti-analysis/anti-vm/vm-detection
resolve function by parsing PE exports	load-code/pe

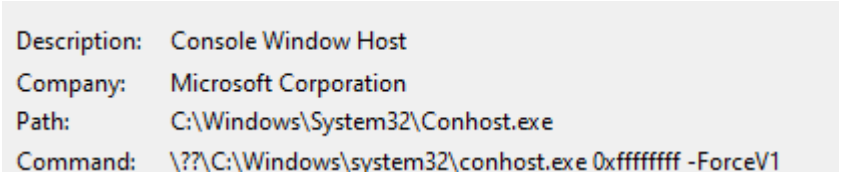
Advanced Static Analysis

Cutter Output:



Basic Dynamic Analysis





Wireshark output:

```
GET /get/flashplayer/update/current/install/install_all_win_cab_64_ax_sgn.z HTTP/1.1
User-Agent: Flash Player Seed/3.0
Host: fpdownload.macromedia.com
Cache-Control: no-cache

HTTP/1.1 200 OK
Content-Length: 258
Date: Thu, 15 Feb 2024 01:38:25 GMT
Server: INetSim HTTP Server
Connection: Close
Content-Type: text/html

<html>
  <head>
    <title>INetSim default HTML page</title>
  </head>
  <body>
    <p></p>
    <p align="center">This is the default HTML page for INetSim HTTP server fake mode.</p>
    <p align="center">This file is an HTML document.</p>
  </body>
</html>
```

YARA (IOC)