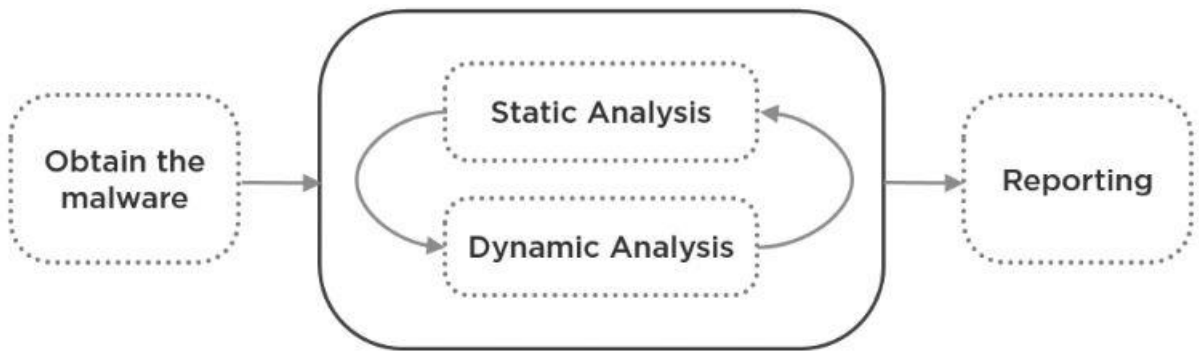
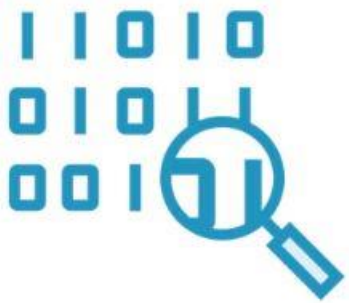
Intro to Static and Dynamic Analysis

Malware Analysis Process

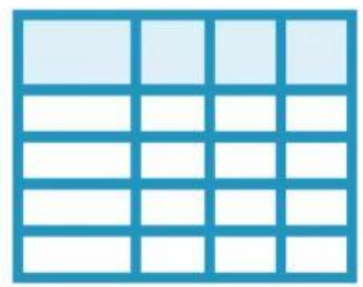


Static Analysis



Hashing

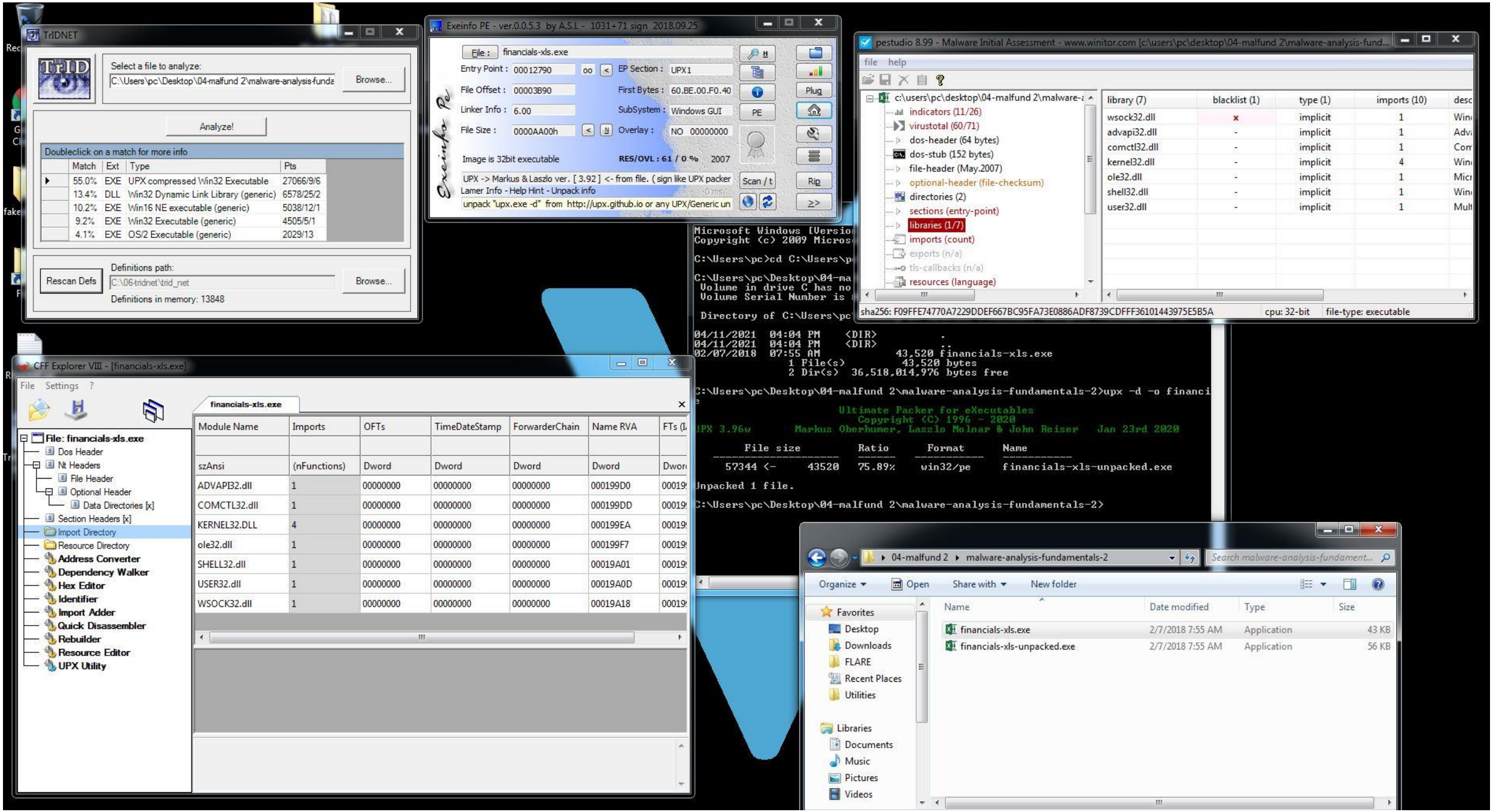
Embedded Strings



PE Header

Static Analysis Tools

- Tridnet
- ExePE Info
- Bintext
- Strings
- Xorsearch
- CFF Explorer
- PE Studio
- Hashmyfile


TrIDNET
Select a file to analyze:
C:\Users\pc\Desktop\04-malfund 2\malware-analysis-funda
Browse...
Analyze!
Doubleclick on a match for more info
Match Ext Type Pts
55.0% EXE UPX compressed Win32 Executable 27066/9/6
13.4% DLL Win32 Dynamic Link Library (generic) 6578/25/2
10.2% EXE Win16 NE executable (generic) 5038/12/1
9.2% EXE Win32 Executable (generic) 4505/5/1
4.1% EXE OS/2 Executable (generic) 2029/13
Rescan Defs
Definitions path:
C:\06-tridnet\trid_net
Browse...
Definitions in memory: 13848
Exeinfo PE - ver.0.0.5.3 by A.S.L - 1031+71 sign 2018.09.25
File : financials-xls.exe
Entry Point : 00012790
EP Section : UPX1
File Offset : 00003B90
First Bytes : 60.BE.00.F0.40
Linker Info : 6.00
SubSystem : Windows GUI
File Size : 0000AA00h
Overlay : NO 00000000
Image is 32bit executable
RES/OVL : 61 / 0 %
2007
UPX -> Markus & Laszlo ver. [3.92] <- from file. (sign like UPX packer
Lamer Info - Help Hint - Unpack info
unpack "upx.exe -d" from http://upx.github.io or any UPX/Generic un
Scan / t
Plug
PE
Rip
pestudio 8.99 - Malware Initial Assessment - www.winitor.com [c:\users\pc\desktop\04-malfund 2\malware-analysis-fund...
file help
c:\users\pc\desktop\04-malfund 2\malware-a
indicators (11/26)
virustotal (60/71)
dos-header (64 bytes)
dos-stub (152 bytes)
file-header (May.2007)
optional-header (file-checksum)
directories (2)
sections (entry-point)
libraries (1/7)
imports (count)
exports (n/a)
tls-callbacks (n/a)
resources (language)
library (7) blacklist (1) type (1) imports (10)
wsock32.dll x implicit 1
advapi32.dll - implicit 1
comctl32.dll - implicit 1
kernel32.dll - implicit 4
ole32.dll - implicit 1
shell32.dll - implicit 1
user32.dll - implicit 1
sha256: F09FFE74770A7229DDEF667BC95FA73E0886ADF8739CDFFF36101443975E5B5A
cpu: 32-bit
file-type: executable
Microsoft Windows [Version
Copyright (c) 2009 Micros
C:\Users\pc>cd C:\Users\p
C:\Users\pc\Desktop\04-ma
Volume in drive C has no
Volume Serial Number is
Directory of C:\Users\pc
04/11/2021 04:04 PM <DIR> .
04/11/2021 04:04 PM <DIR> ..
02/07/2018 07:55 AM 43,520 financials-xls.exe
1 File(s) 43,520 bytes
2 Dir(s) 36,518,014,976 bytes free
C:\Users\pc\Desktop\04-malfund 2\malware-analysis-fundamentals-2>upx -d -o financi
e
Ultimate Packer for eXecutables
Copyright (C) 1996 - 2020
UPX 3.96w Markus Oberhumer, Laszlo Molnar & John Reiser Jan 23rd 2020
File size Ratio Format Name
57344 <- 43520 75.89% win32/pe financials-xls-unpacked.exe
Unpacked 1 file.
C:\Users\pc\Desktop\04-malfund 2\malware-analysis-fundamentals-2>
CFF Explorer VIII - [financials-xls.exe]
File Settings ?
financials-xls.exe
File: financials-xls.exe
Dos Header
Nt Headers
File Header
Optional Header
Data Directories [x]
Section Headers [x]
Import Directory
Resource Directory
Address Converter
Dependency Walker
Hex Editor
Identifier
Import Adder
Quick Disassembler
Rebuilder
Resource Editor
UPX Utility
Module Name Imports OFTs TimeDateStamp ForwarderChain Name RVA FTs (I
szAnsi (nFunctions) Dword Dword Dword Dword Dwor
ADVAPI32.dll 1 00000000 00000000 00000000 000199D0 00019
COMCTL32.dll 1 00000000 00000000 00000000 000199DD 00019
KERNEL32.DLL 4 00000000 00000000 00000000 000199EA 00019
ole32.dll 1 00000000 00000000 00000000 000199F7 00019
SHELL32.dll 1 00000000 00000000 00000000 00019A01 00019
USER32.dll 1 00000000 00000000 00000000 00019A0D 00019
WSOCK32.dll 1 00000000 00000000 00000000 00019A18 00019
04-malfund 2 malware-analysis-fundamentals-2
Search malware-analysis-fundament...
Organize Open Share with New folder
Favorites
Desktop
Downloads
FLARE
Recent Places
Utilities
Libraries
Documents
Music
Pictures
Videos
Name Date modified Type Size
financials-xls.exe 2/7/2018 7:55 AM Application 43 KB
financials-xls-unpacked.exe 2/7/2018 7:55 AM Application 56 KB

Dynamic Analysis

Monitor Changes

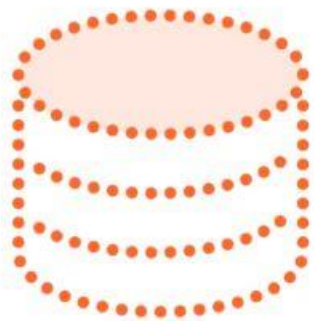
Behavior Monitoring

Dynamic Analysis Tools

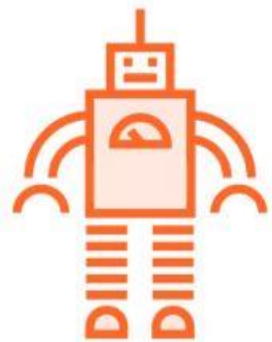
- Regshot
- Autoruns
- Fakenet
- Wireshark
- Procmon
- Procdot

More Techniques

Reverse Engineering



Memory Analysis



Automation

Focus Your Analysis