



black hat[®]
ARSENAL

DECEMBER 2-5, 2019
EXCEL LONDON, UK

Malware Initial Assessment with pestudio

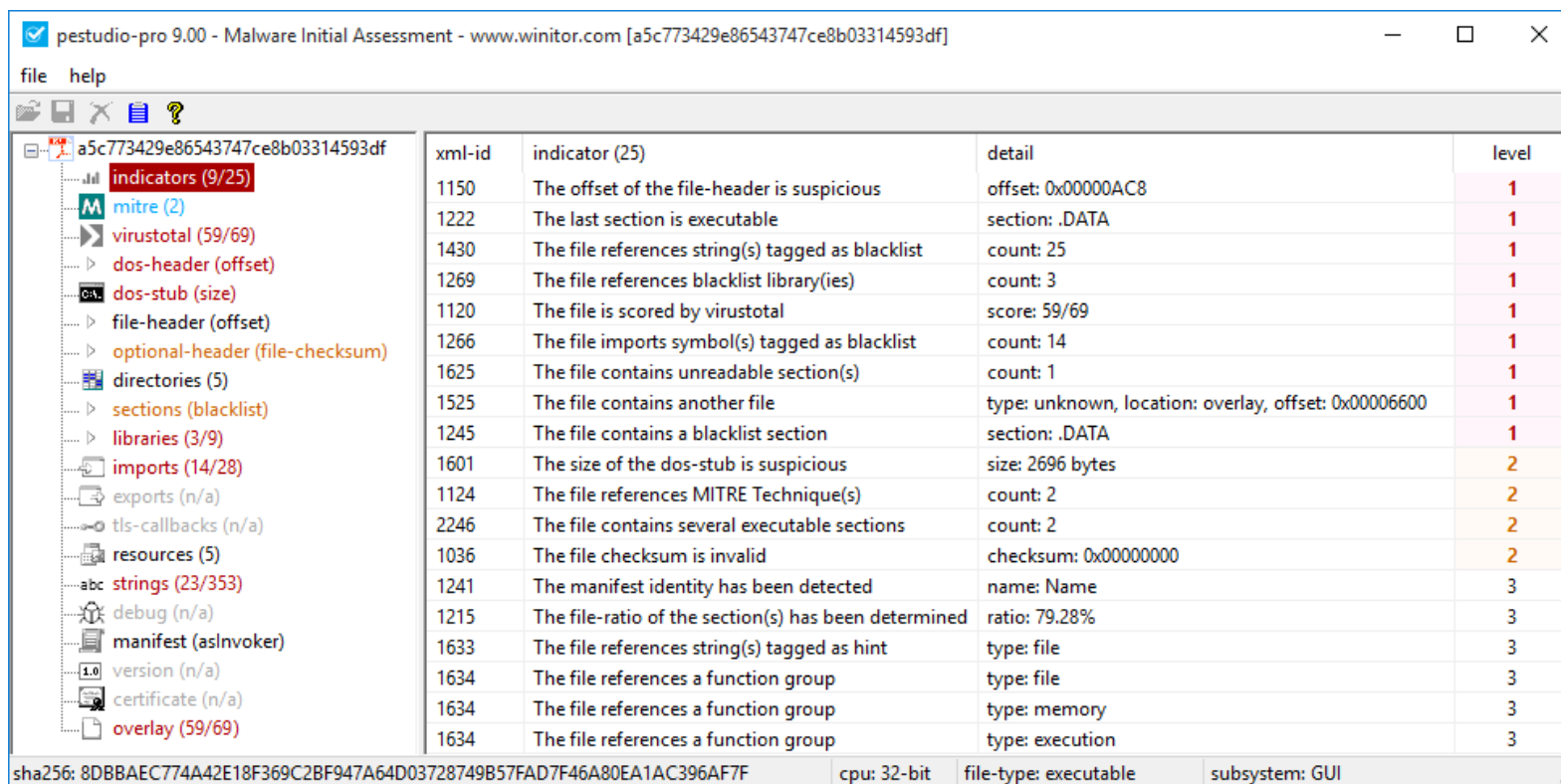
- spot artifacts
- detect embedded items
- collect hints
- group elements
- transform data into information
- show Tactics & Techniques [@MITREattack](#)
- retrieve scores from [@VirusTotal](#)
- consume configurations files
- create XML report

Characteristics

- no infection risk
- no sandbox needed
- no expertise required
- no installation
- zero footprint

Front-end

- Graphical User Interface (GUI)



pestudio-pro 9.00 - Malware Initial Assessment - www.winator.com [a5c773429e86543747ce8b03314593df]

file help

a5c773429e86543747ce8b03314593df

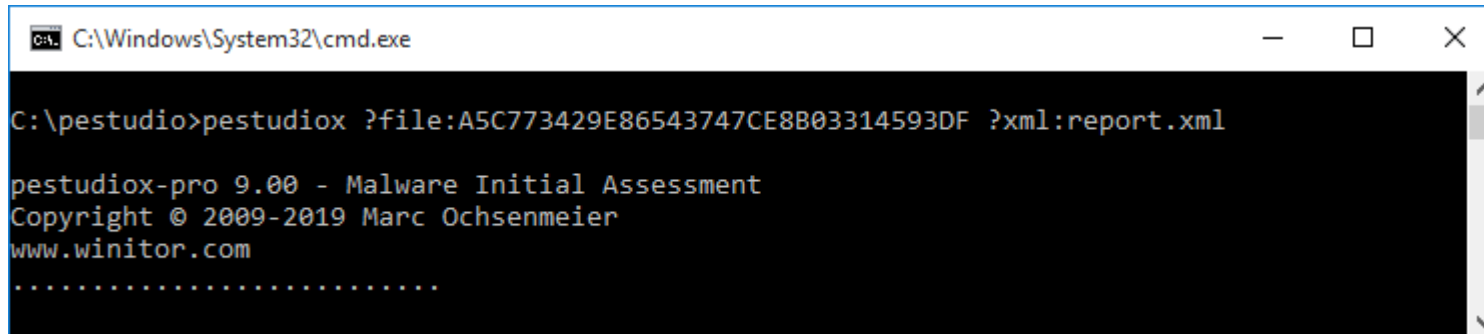
- indicators (9/25)
- mitre (2)
- virustotal (59/69)
- dos-header (offset)
- dos-stub (size)
- file-header (offset)
- optional-header (file-checksum)
- directories (5)
- sections (blacklist)
- libraries (3/9)
- imports (14/28)
- exports (n/a)
- tls-callbacks (n/a)
- resources (5)
- strings (23/353)
- debug (n/a)
- manifest (asInvoker)
- version (n/a)
- certificate (n/a)
- overlay (59/69)

xml-id	indicator (25)	detail	level
1150	The offset of the file-header is suspicious	offset: 0x00000AC8	1
1222	The last section is executable	section: .DATA	1
1430	The file references string(s) tagged as blacklist	count: 25	1
1269	The file references blacklist library(ies)	count: 3	1
1120	The file is scored by virustotal	score: 59/69	1
1266	The file imports symbol(s) tagged as blacklist	count: 14	1
1625	The file contains unreadable section(s)	count: 1	1
1525	The file contains another file	type: unknown, location: overlay, offset: 0x00006600	1
1245	The file contains a blacklist section	section: .DATA	1
1601	The size of the dos-stub is suspicious	size: 2696 bytes	2
1124	The file references MITRE Technique(s)	count: 2	2
2246	The file contains several executable sections	count: 2	2
1036	The file checksum is invalid	checksum: 0x00000000	2
1241	The manifest identity has been detected	name: Name	3
1215	The file-ratio of the section(s) has been determined	ratio: 79.28%	3
1633	The file references string(s) tagged as hint	type: file	3
1634	The file references a function group	type: file	3
1634	The file references a function group	type: memory	3
1634	The file references a function group	type: execution	3

sha256: 8DBBAEC774A42E18F369C2BF947A64D03728749B57FAD7F46A80EA1AC396AF7F cpu: 32-bit file-type: executable subsystem: GUI

Front-end

- Command Line Interface (CLI) for the creation of an XML report



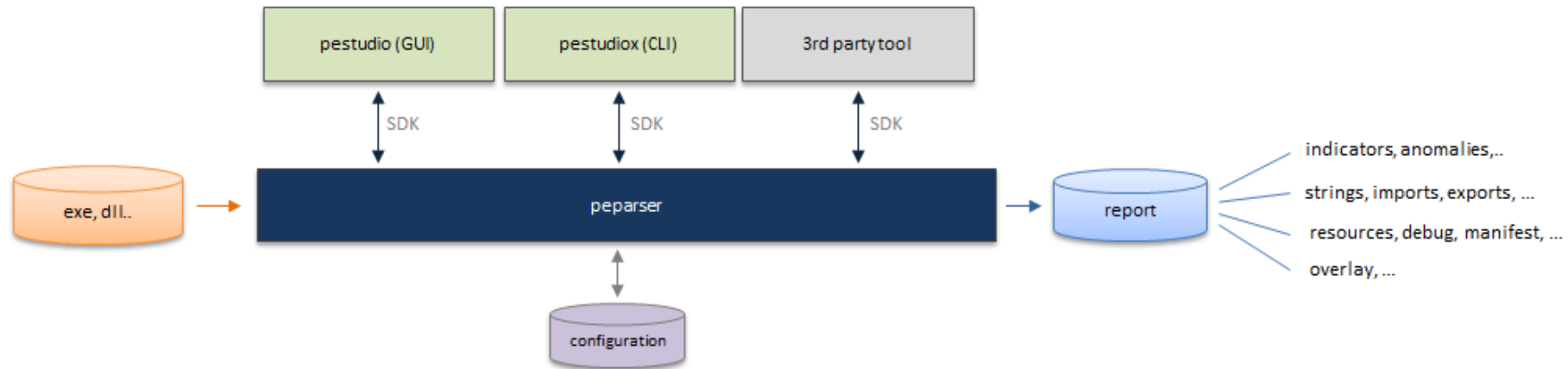
```
C:\Windows\System32\cmd.exe

C:\pestudio>pestudiox ?file:A5C773429E86543747CE8B03314593DF ?xml:report.xml

pestudiox-pro 9.00 - Malware Initial Assessment
Copyright © 2009-2019 Marc Ochsenmeier
www.winator.com
.....
```

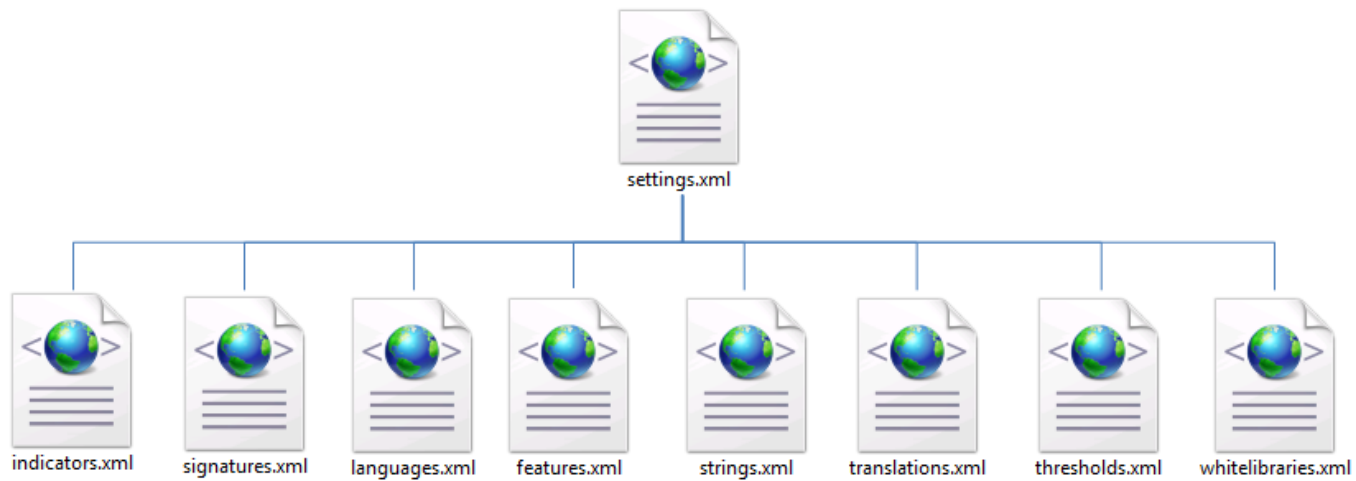
Architecture

- The tool has a clean design



Configuration

- The tool can be customized



Report

- The result of an Analysis can be integrated as input of a tool chain

```
<?xml version="1.0" encoding="UTF-8"?>
<!--pestudio-pro 9.00 - Malware Initial Assessment - www.winitor.com-->
- <image>
+ <overview name="f:\exe,01901882c4c01625fd2eeecdd7e6745a">
+ <indicators hint="4/34">
- <mitre hint="6">
  <mitre-tactic name="Initial Acces" ta="TA0001"/>
  - <mitre-tactic name="Execution" ta="TA0002">
    <mitre-technique name="Execution through API" ti="T1106"/>
  </mitre-tactic>
  <mitre-tactic name="Persistence" ta="TA0003"/>
  <mitre-tactic name="Privilege Escalation" ta="TA0004"/>
  - <mitre-tactic name="Defense Evasion" ta="TA0005">
    <mitre-technique name="Virtualization/Sandbox Evasion" ti="T1497"/>
    <mitre-technique name="Process Injection" ti="T1055"/>
  </mitre-tactic>
  <mitre-tactic name="Credential Access" ta="TA0006"/>
  - <mitre-tactic name="Discovery" ta="TA0007">
    <mitre-technique name="System Time Discovery" ti="T1124"/>
    <mitre-technique name="Process Discovery" ti="T1057"/>
  </mitre-tactic>
  <mitre-tactic name="Lateral Movement" ta="TA0008"/>
  - <mitre-tactic name="Collection" ta="TA0009">
    <mitre-technique name="Man in the Browser" ti="T1185"/>
  </mitre-tactic>
  <mitre-tactic name="Exfiltration" ta="TA0010"/>
  <mitre-tactic name="Command and Control" ta="TA0011"/>
  <mitre-tactic name="Impact" ta="TA0040"/>
</mitre>
+ <dos-header hint="64 bytes">
+ <dos-stub hint="152 bytes">
+ <file-header hint="Aug.2014 ">
+ <strings bl="90" count="1812">
  <tls-callbacks>n/a</tls-callbacks>
  <certificate>n/a</certificate>
  <overlay>n/a</overlay>
</image>
```


Author

- Marc Ochsenmeier
- Malware Analyst
- [@ochsenmeier](#)
- www.winitor.com