black hat® ARSENAL

DECEMBER 2-5, 2019

EXCEL LONDON, UK

#BHEU @BLACK HAT EVENTS

Malware Initial Assessment with pestudio

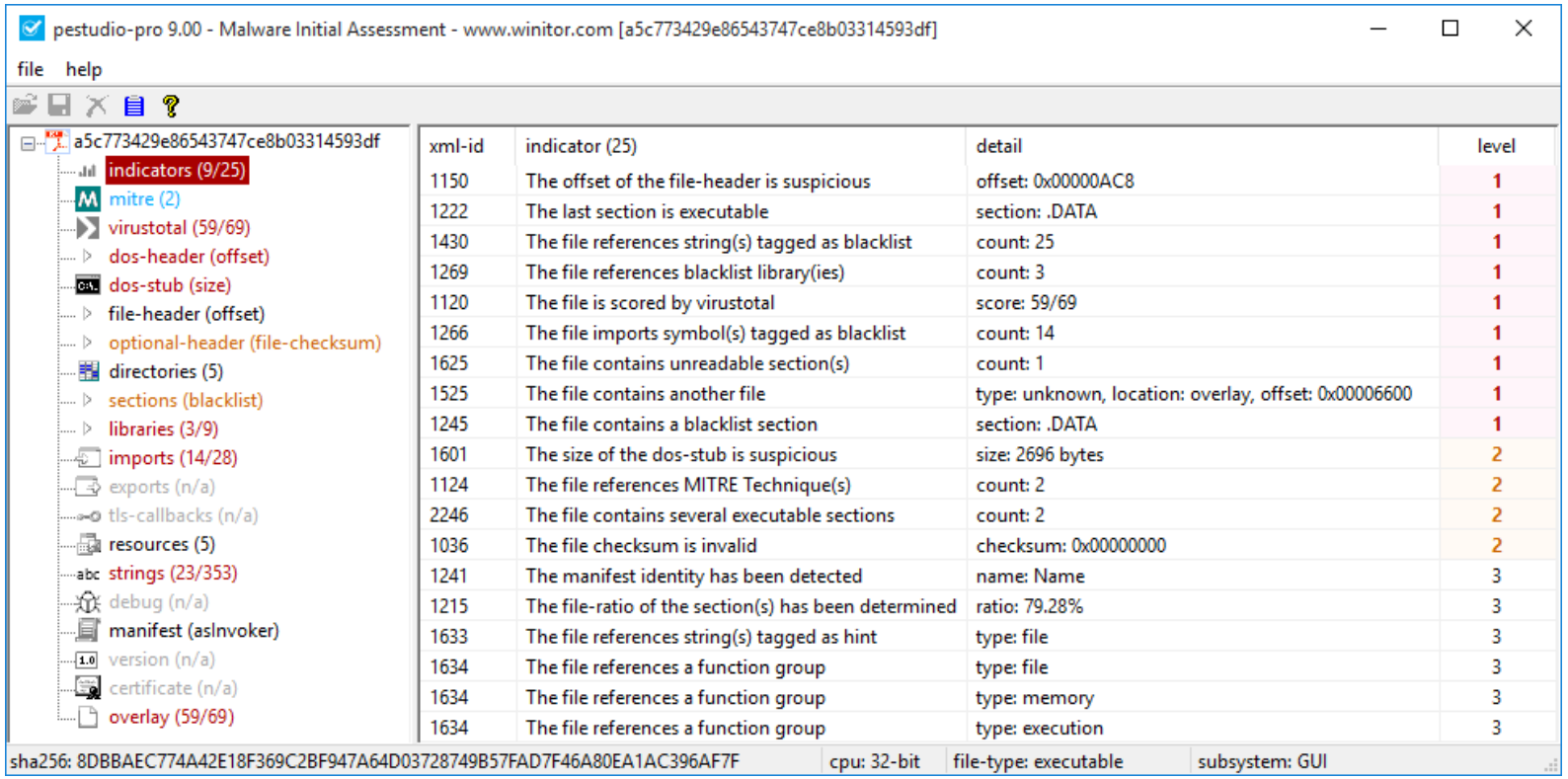
- spot artifacts
- detect embedded items
- collect hints
- group elements
- transform data into information
- show Tactics & Techniques @MITREattack
- retrieve scores from @Virustotal
- consume configurations files
- create XML report

Characteristics

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

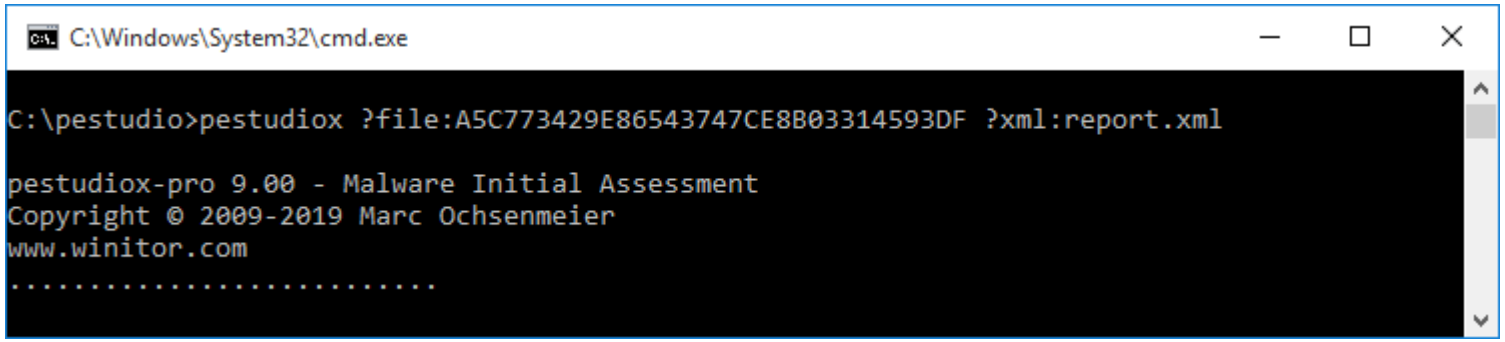
Front-end

- Graphical User Interface (GUI)



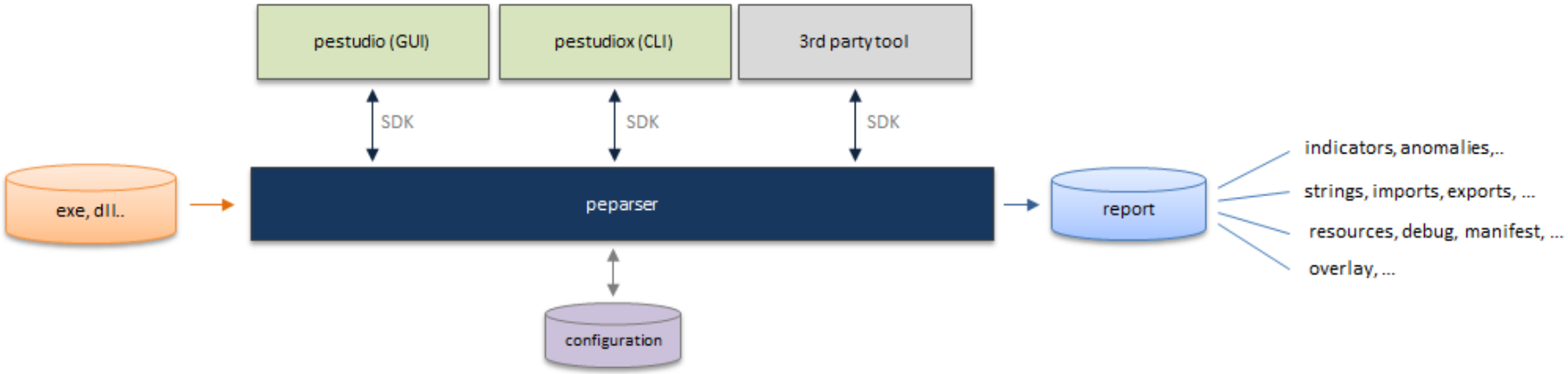
Front-end

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



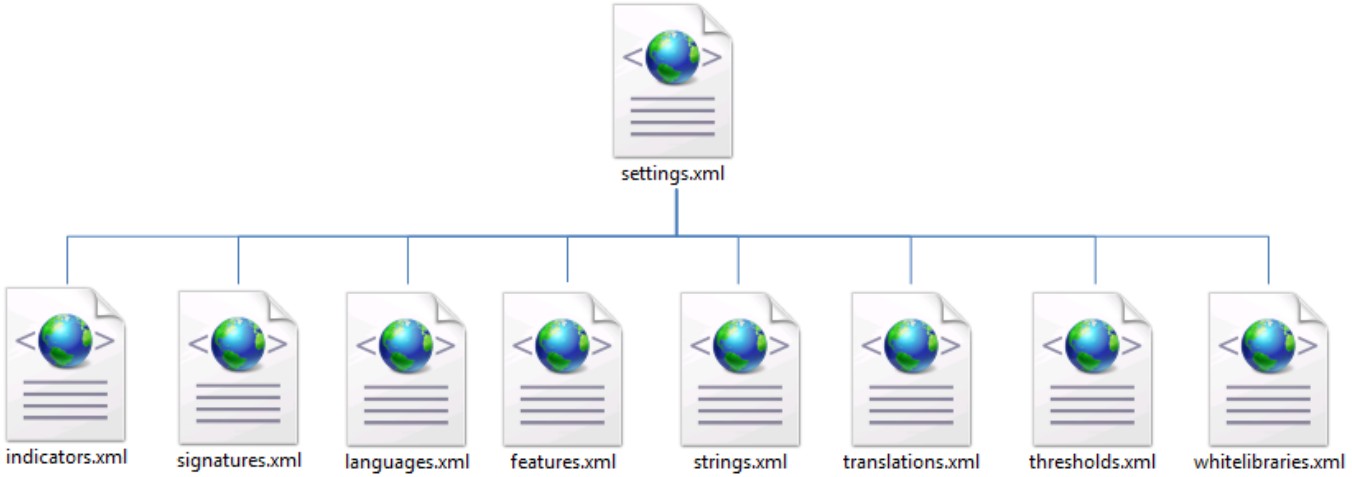
Architecture

- 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