PeStudio

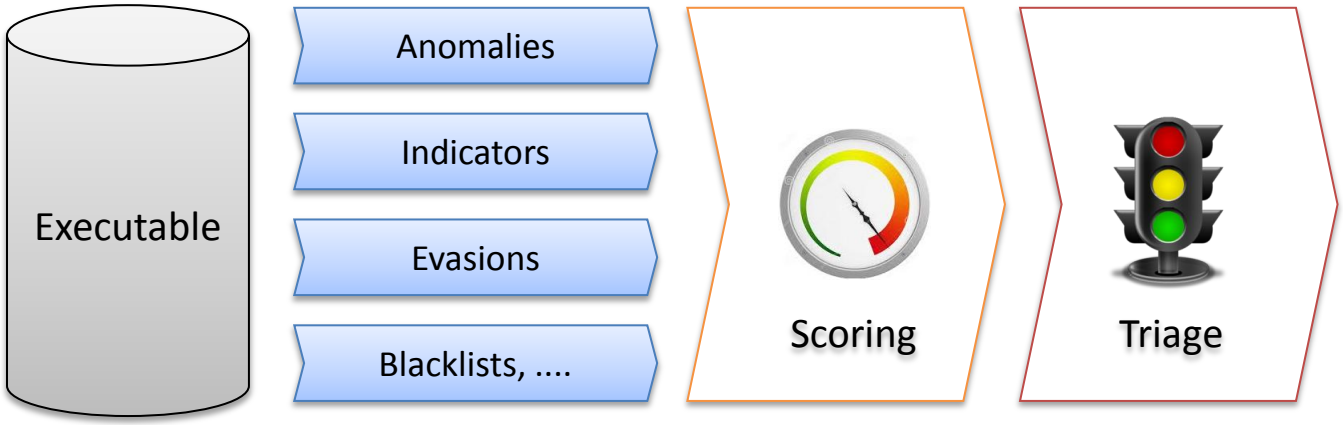
Black Hat 2014 Amsterdam

October 17, 2014

Author	Marc Ochsenmeier
Web	www.winitor.com
Email	info@winitor.com
Twitter	@ochsenmeier

Goal

- Early malware detection, scoring and triage



Features

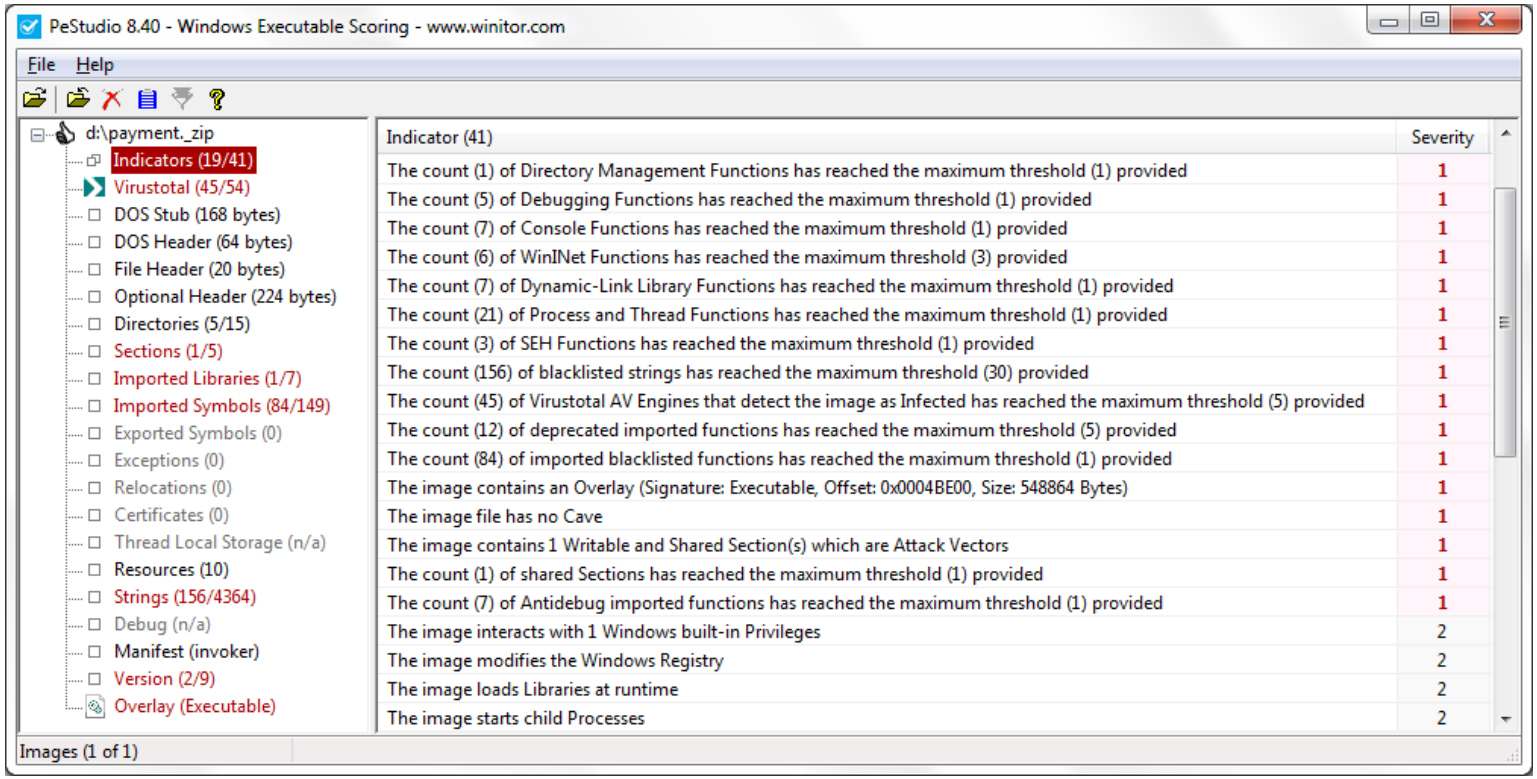
- **Static** analysis
- Collect **hints**
- Detect **anomalies**
- Verify **thresholds**
- Spot **embedded** files
- Provide **indicators**
- Lookup **scores** @virustotal
- Generate XML **report**

Characteristics

- No installation (zero footprint)
- No infection risk (executable never started)
- Low cost (no Sandbox needed)
- Easy to use (no expertise required)

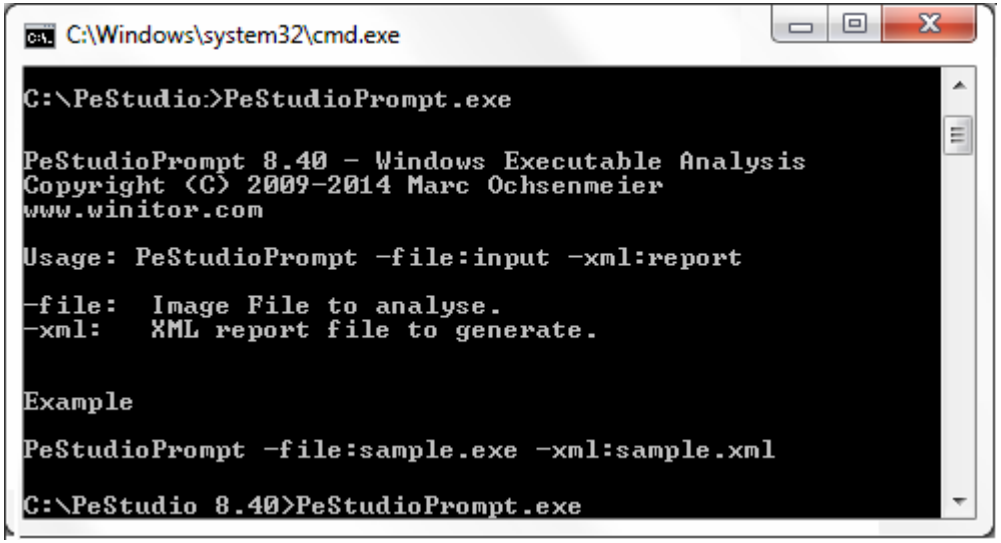
GUI Interface

- Transform complex data into clear indicators



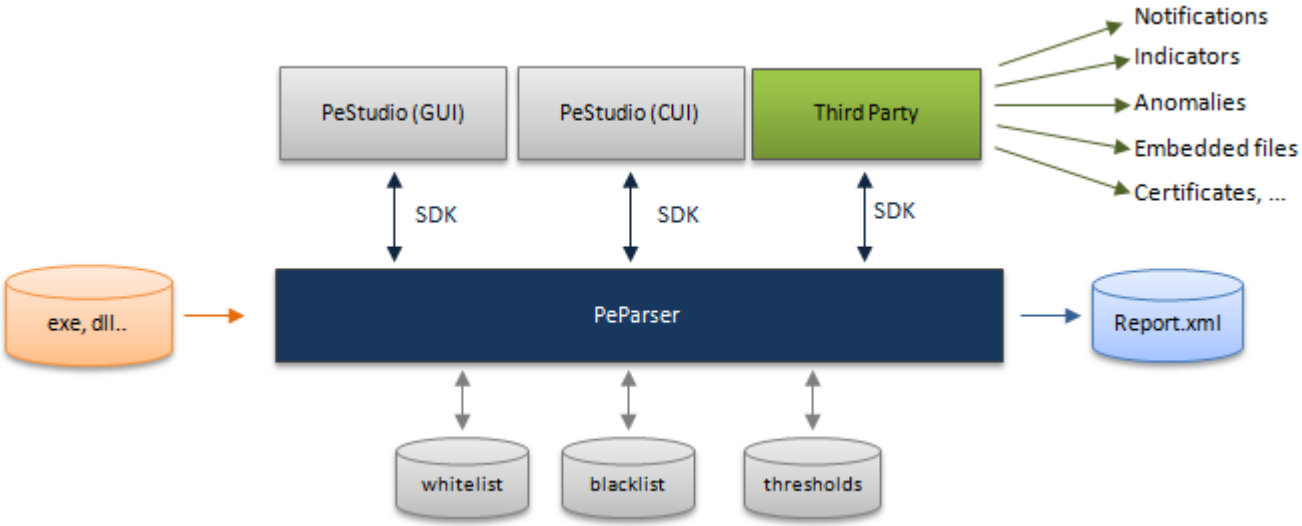
CUI Interface

- Creation of XML report in batch mode



Architecture

- Clean set of granular interfaces
- Asynchronous sink notificators



Configuration

- Large set of XML files
  - Indicators
  - Filterings
  - Thresholds
  - Blacklists
    - Libraries
    - Functions
    - Strings
    - Languages..

Input

- Any Windows Executable file
  - Exe, dll, sys, drv, cpl, scr, ...
- Any file
- Any PID

Report

```
<?xml version="1.0" encoding="UTF-8"?>
<!--this document has been created with PeStudio Version 7.83-->
<image name="3._exe">
  - <Indicators count="27">
        <Indicator id="280">The image is Obfuscated (encrypted, compressed)</Indicator>
        <Indicator id="432">The image contains 16 Blacklisted Strings</Indicator>
        <Indicator id="57">The image is statically linked to the C Run-Time Libraries</Indicator>
        <Indicator id="1">The size (64 Bytes) of the MS-DOS Header is standard</Indicator>
        <Indicator id="101">The image does NOT use Data Execution Prevention (DEP) as Mitigation technique</Indicator>
        <Indicator id="103">The image does NOT use Address Space Layout Randomization (ASLR) as Mitigation technique</Indicator>
        <Indicator id="6">The size (20 Bytes) of the File Header is standard</Indicator>
        <Indicator id="4">The size (224 Bytes) of the Optional Header is standard</Indicator>
        <Indicator id="36">The image Checksum is Empty</Indicator>
        <Indicator id="233">The image contains Resources in 2 Languages</Indicator>
        <Indicator id="234">The image contains 2 custom Resource Item(s)</Indicator>
        <Indicator id="43">The image has NO Manifest</Indicator>
        <Indicator id="500">The image has NO Version</Indicator>
        <Indicator id="107">The image does NOT use Cookies placed on the Stack (GS) as Mitigation technique</Indicator>
        <Indicator id="40">The image is NOT digitally signed</Indicator>
        <Indicator id="261">The image Imports 1 Obsolete Symbol(s)</Indicator>
        <Indicator id="266">The image imports 16 Blacklisted Functions (API)</Indicator>
        <Indicator id="521">The image contains an Overlay (Offset: 0x0000A000, Size: 1885 Bytes)</Indicator>
        <Indicator id="109">The image does NOT use Code Integrity</Indicator>
        <Indicator id="117">The Checksum (0x00000000) of the Image is Invalid</Indicator>
        <Indicator id="422">A cave has been detected in the file (Offset: 0x000040F6, Size: 3850 bytes)</Indicator>
        <Indicator id="422">A cave has been detected in the file (Offset: 0x000058B0, Size: 1872 bytes)</Indicator>
        <Indicator id="422">A cave has been detected in the file (Offset: 0x000087CC, Size: 2100 bytes)</Indicator>
        <Indicator id="226">The Entry Point (0x0000160F) is in the First Section (name:.text)</Indicator>
        <Indicator id="222">The Last Section (name:.rsrc) is Executable</Indicator>
        <Indicator id="221">The image has 2 duplicated Sections names</Indicator>
        <Indicator id="215">The image has 1 Writable and Executable Section(s)</Indicator>
    </Indicators>
  + <headers>
  + <libraries count="2">
  + <resources Types="2">
  + <manifest>
  + <Strings count="132">
  + <virustotal>
</image>
```

Challenges

- Resist malformations
  - evade (crash) static analysis tools
- Handle the unexpected
  - deprecated, invalid and missing fields
- Avoid false-positiv

Thank you