Discovering C&C in Malicious PDF using deobfuscation, encoding and other techniques

@FilipiPires

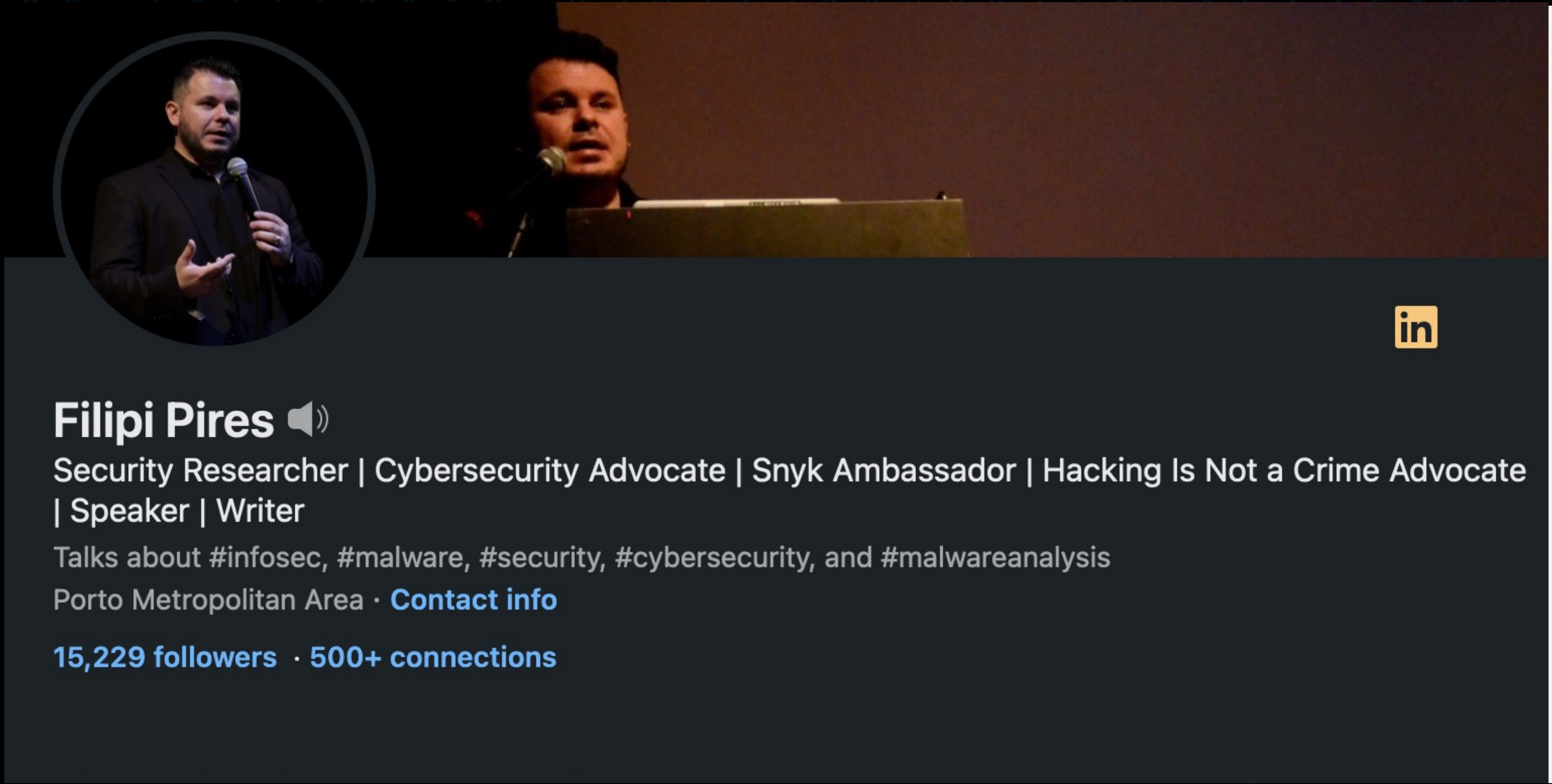
HackInBo Spring 2022 Edition

18ª EDIZIONE

HackInBo Spring 2022 Edition
18ª EDIZIONE

#WHOAMI

- https://filipipires.com
- https://twitter.com/FilipiPires
- https://github.com/filipi86
- https://www.linkedin.com/in/filipipires/



Filipi Pires

Security Researcher | Cybersecurity Advocate | Snyk Ambassador | Hacking Is Not a Crime Advocate | Speaker | Writer

Talks about #infosec, #malware, #security, #cybersecurity, and #malwareanalysis

Porto Metropolitan Area · Contact info

15,229 followers · 500+ connections

Filipi Pires

Researcher | Security Researcher | Speaker | Writer | Cybersecurity Advoc...

#WHOAMI

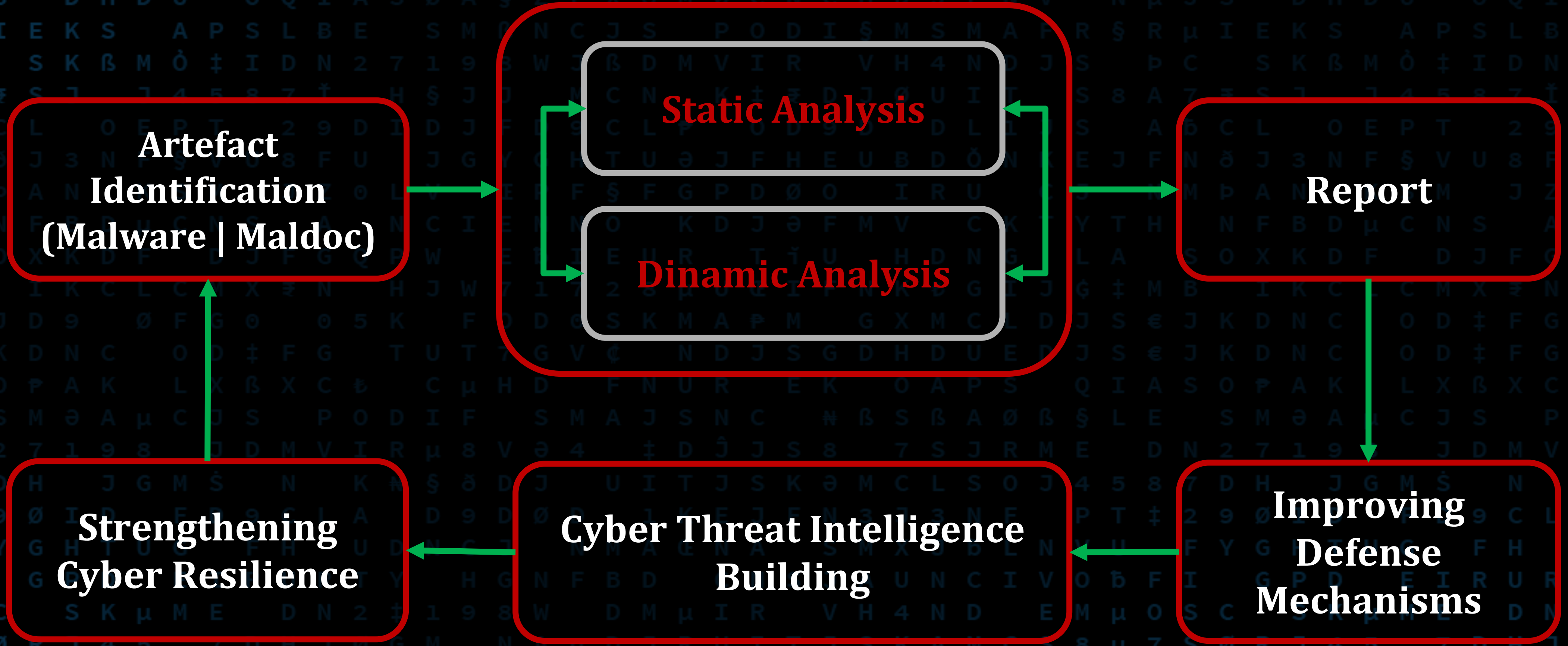
- Security Researcher SAPORO ORDER IN CHAOS
- Cybersecurity Advocate senhasegura®
- Hacking is Not a Crime Advocate HACKING IS NOT A CRIME
- Snyk Ambassador snyk
- DCG 5511 DEFCON GROUPS DCG5511 · SÃO PAULO · BRASIL JOIN US DISCORD.IO/DCG5511
- Instructor, Writer and Reviewer PenTest magazine Haking eForensics Magazine

What is a Threat???

# What is a Threat???

According to ISO 27005, a threat is defined as a potential cause of an incident that may cause harm to systems and organization.

- Software attacks
- Theft of intellectual property
- Identity theft
- Sabotage
- Information extortion are examples of information security threats.



Artefact Identification (Malware | Maldoc)

Static Analysis

Dinamic Analysis

Report

Improving 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, in the interaction that malware has when it’s executed or a maldoc is used, also known like **“runtime”** analysis

It can be easyly automated, there are sites today that already perform analysis of malicious artefacts, using the concept **called “Sandbox”**

Physical and Logical Structure of PDF files

HackInBo Spring 2022 Edition

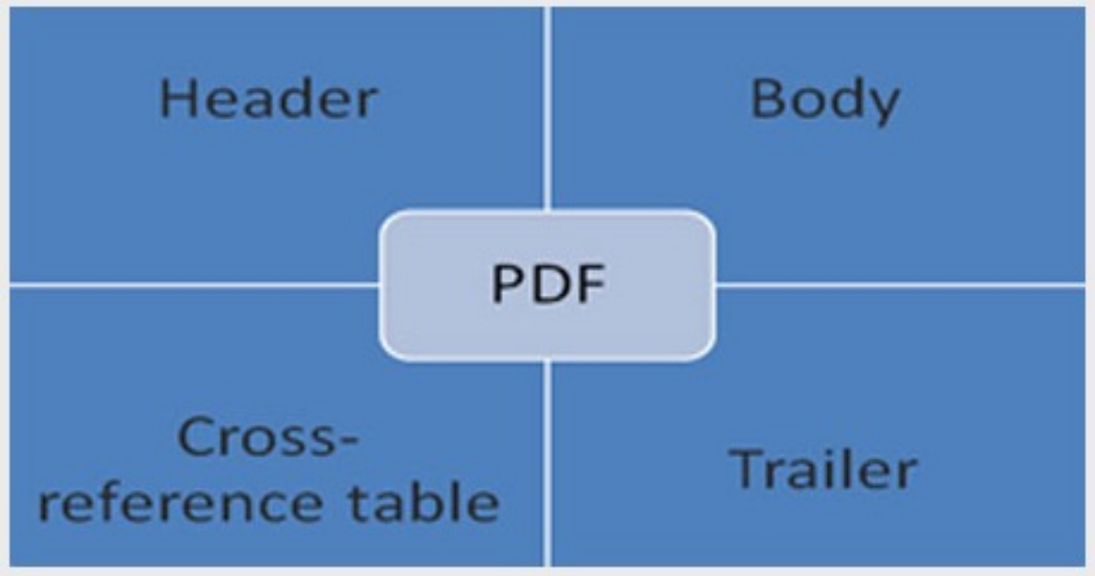
18ª EDIZIONE

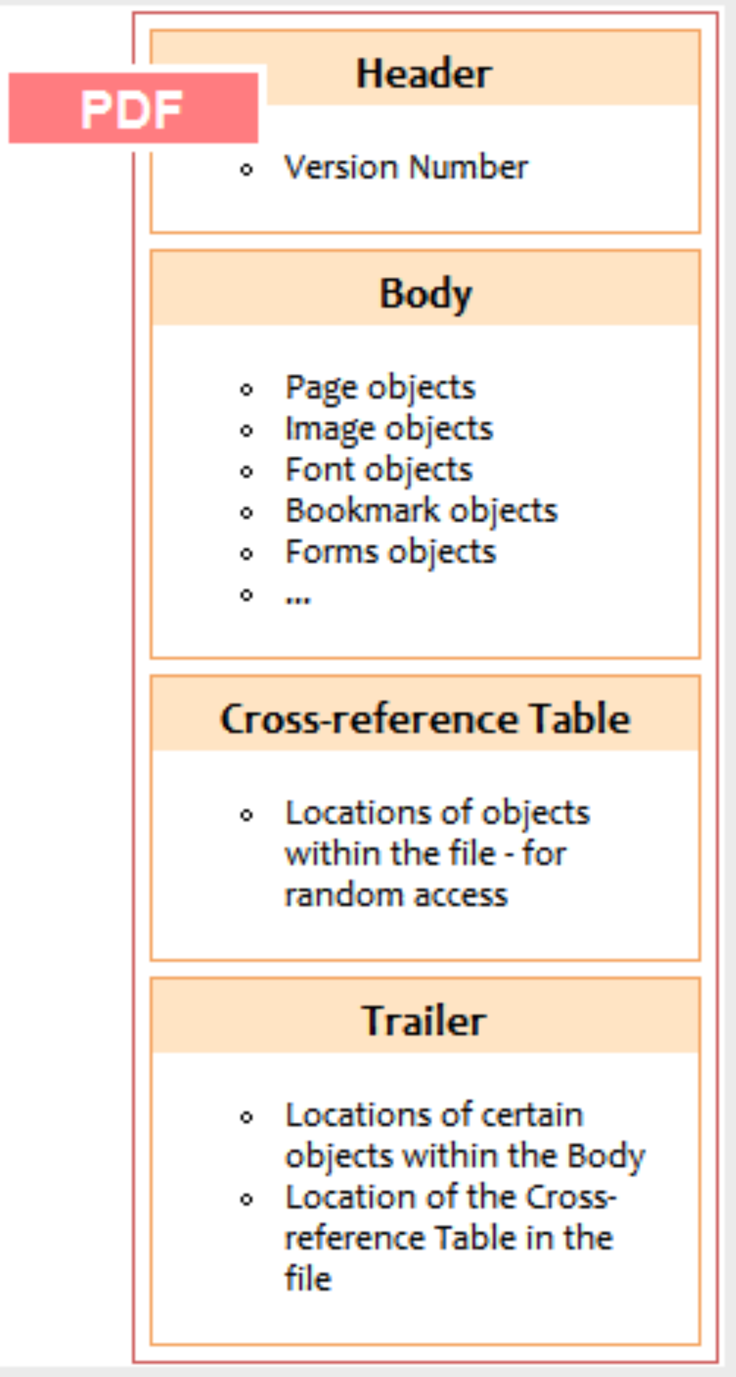
# Structure PDF

In general, a PDF document has fours manly parts .

- One-line header ou Header
- Body
- Cross-reference table
- Trailer

# Structure PDF





Header

- Version Number

Body

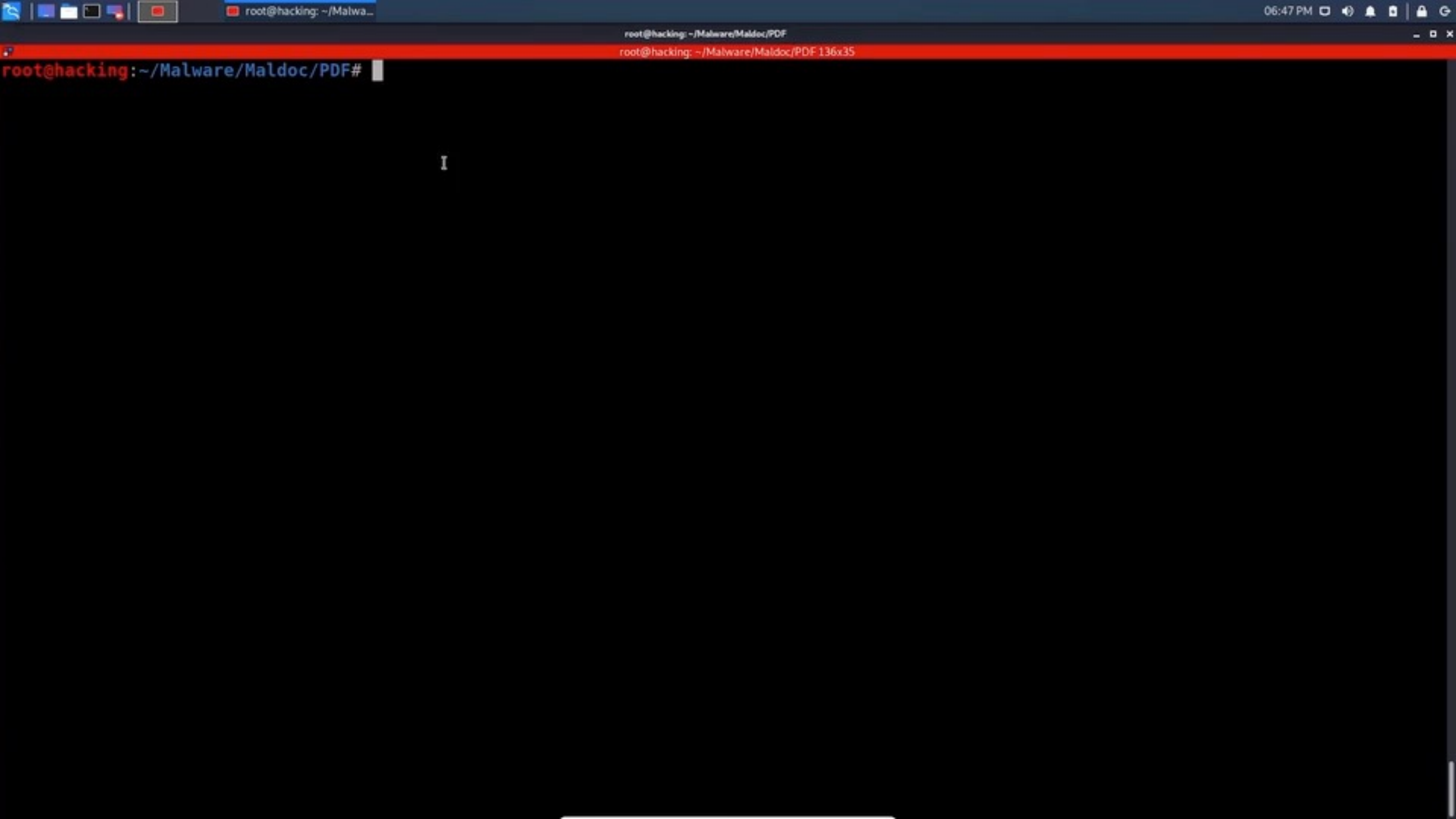
- Page objects
- Image objects
- Font objects
- Bookmark objects
- Forms objects
- ...

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

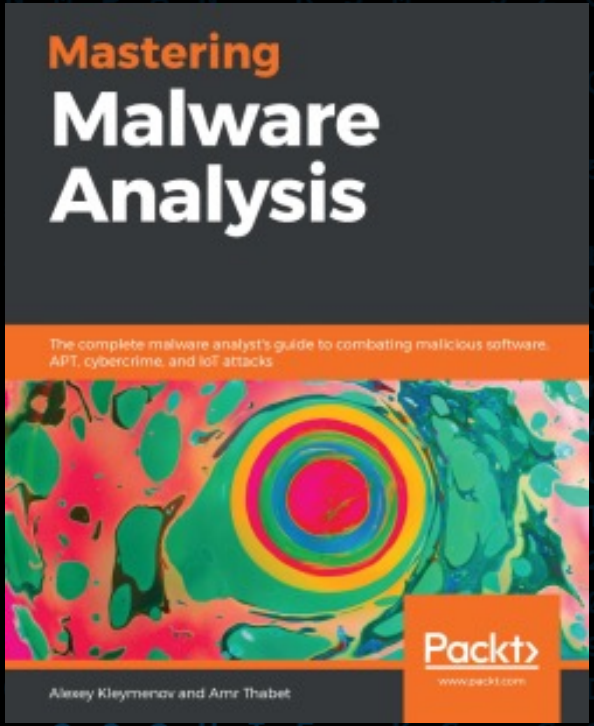


root@hacking: ~/Malwa...
06:47 PM
root@hacking: ~/Malware/Maldoc/PDF
root@hacking: ~/Malware/Maldoc/PDF 136x35

```
root@hacking:~/Malware/Maldoc/PDF# 
```

Recommendation Books

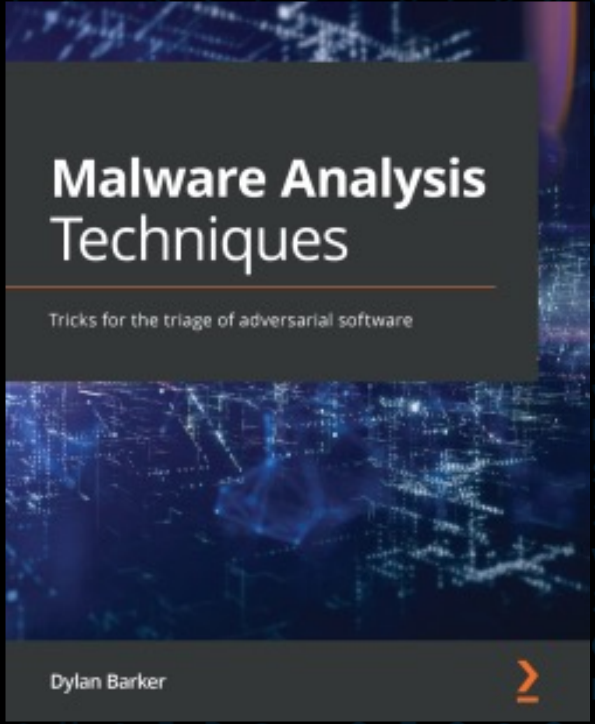
HackInBo®
Spring 2022 Edition
18ª EDIZIONE


Mastering
Malware Analysis

The complete malware analyst's guide to combating malicious software, APT, cybercrime, and IoT attacks

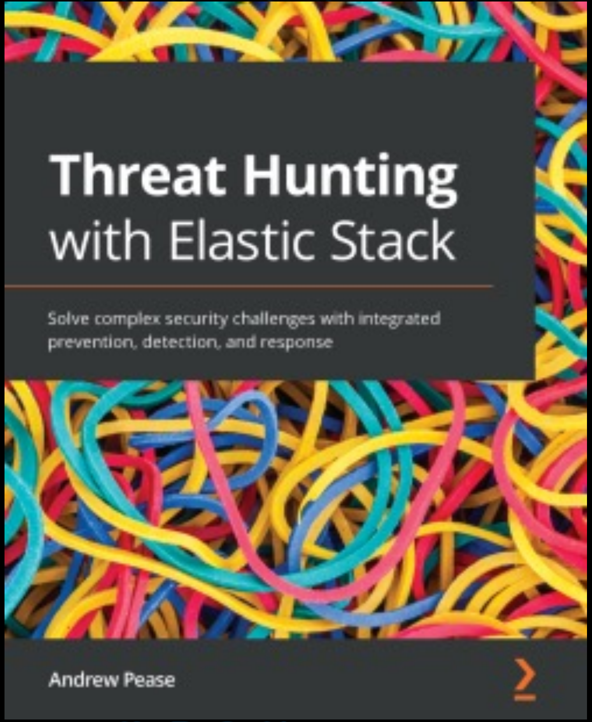
Packt›
www.packt.com

Alexey Kleymenov and Amr Thabet


Malware Analysis Techniques

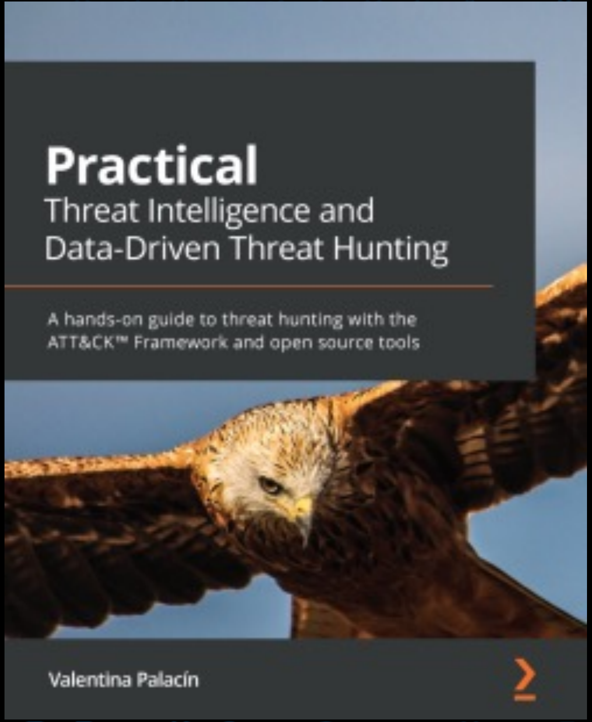
Tricks for the triage of adversarial software

Dylan Barker


Threat Hunting with Elastic Stack

Solve complex security challenges with integrated prevention, detection, and response

Andrew Pease


Practical
Threat Intelligence and Data-Driven Threat Hunting

A hands-on guide to threat hunting with the ATT&CK™ Framework and open source tools

Valentina Palacín

Thank you

HACKINBO®
Spring 2022 Edition
18ª EDIZIONE

- ➢ https://filipipires.com
- ➢ https://twitter.com/FilipiPires
- ➢ https://github.com/filipi86
- ➢ https://www.linkedin.com/in/filipipires/

Filipi Pires

Security Researcher | Cybersecurity Advocate | Snyk Ambassador | Hacking Is Not a Crime Advocate | Speaker | Writer

Talks about #infosec, #malware, #security, #cybersecurity, and #malwareanalysis

Porto Metropolitan Area · Contact info

15,229 followers · 500+ connections

Filipi Pires

Researcher | Security Researcher | Speaker | Writer | Cybersecurity Advoc...