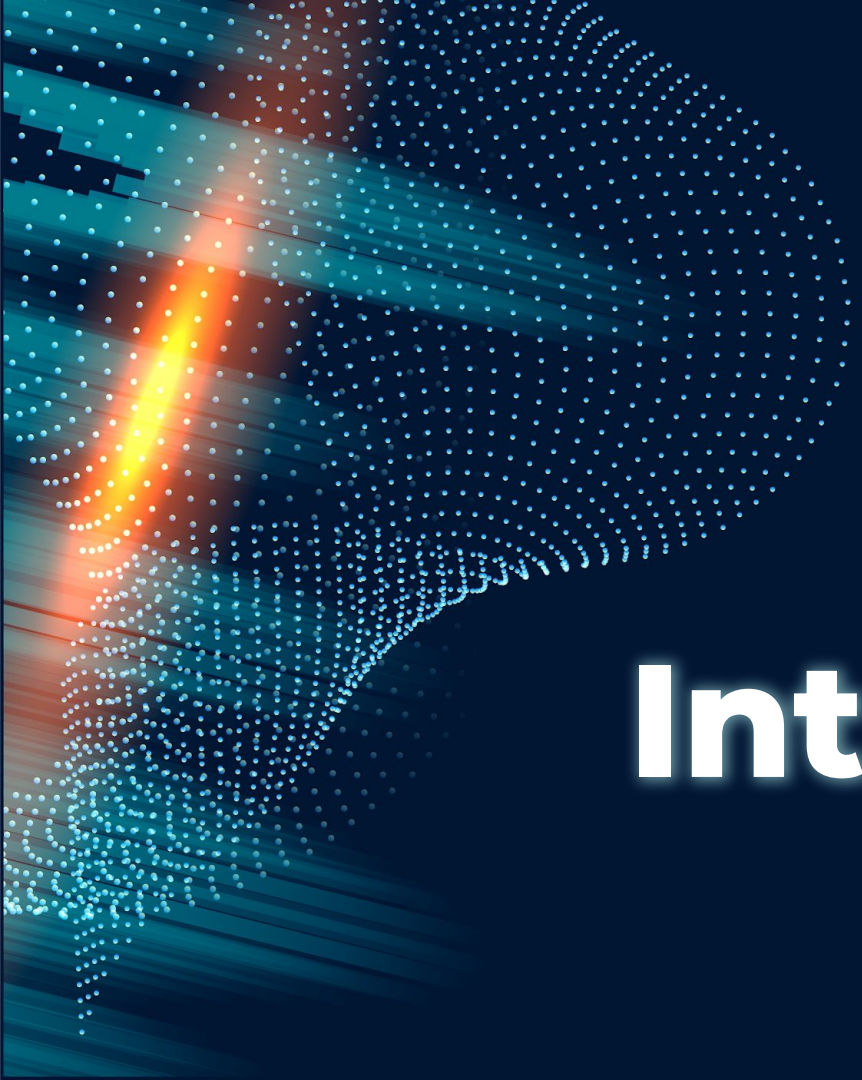
Internship, Stratosphere Laboratory, CTU in Prague, 2024

# Analysis and understanding a malware of the PyRation family

**Tomas Nieponice**
Main advisor: Sebastian Garcia
Co-advisor: Veronica Valeros



# Introduction

# Who am I?

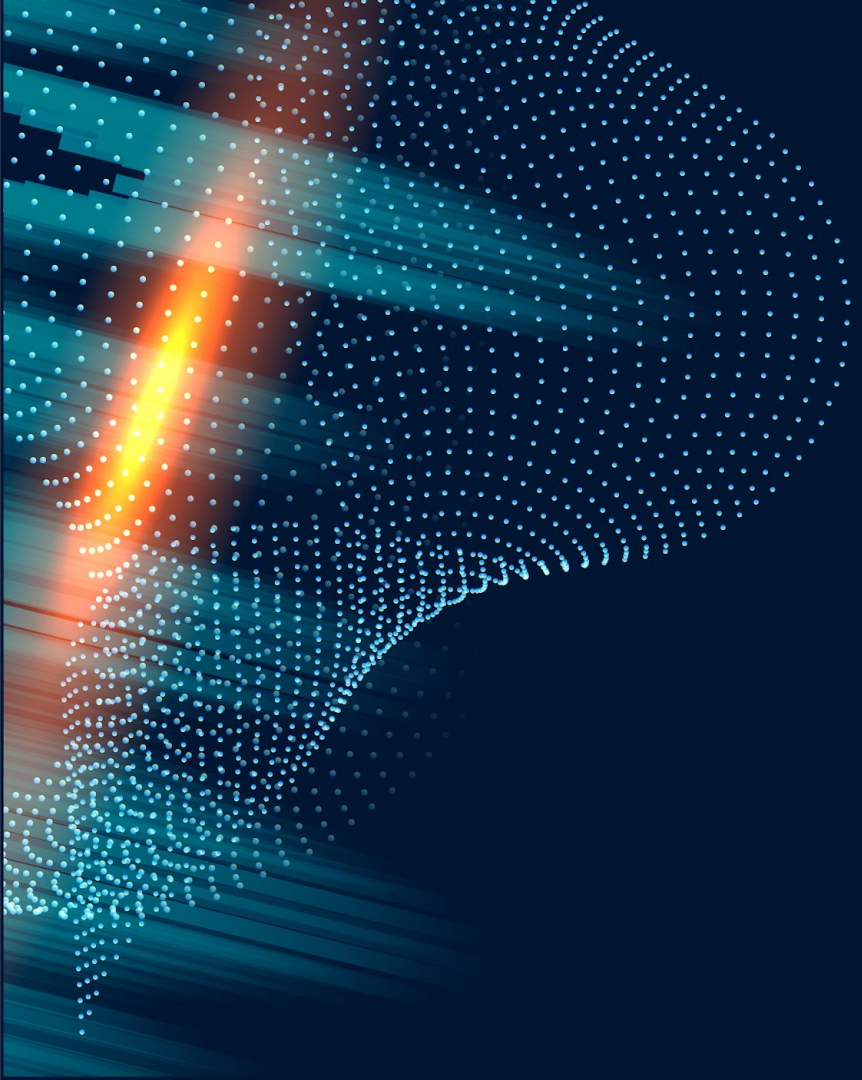
- High school student
- 16 years old
- Tech enthusiast

# Our objective for the internship:

**Understand how a real malware behaves: reversing, coding and network traffic**

# Our process

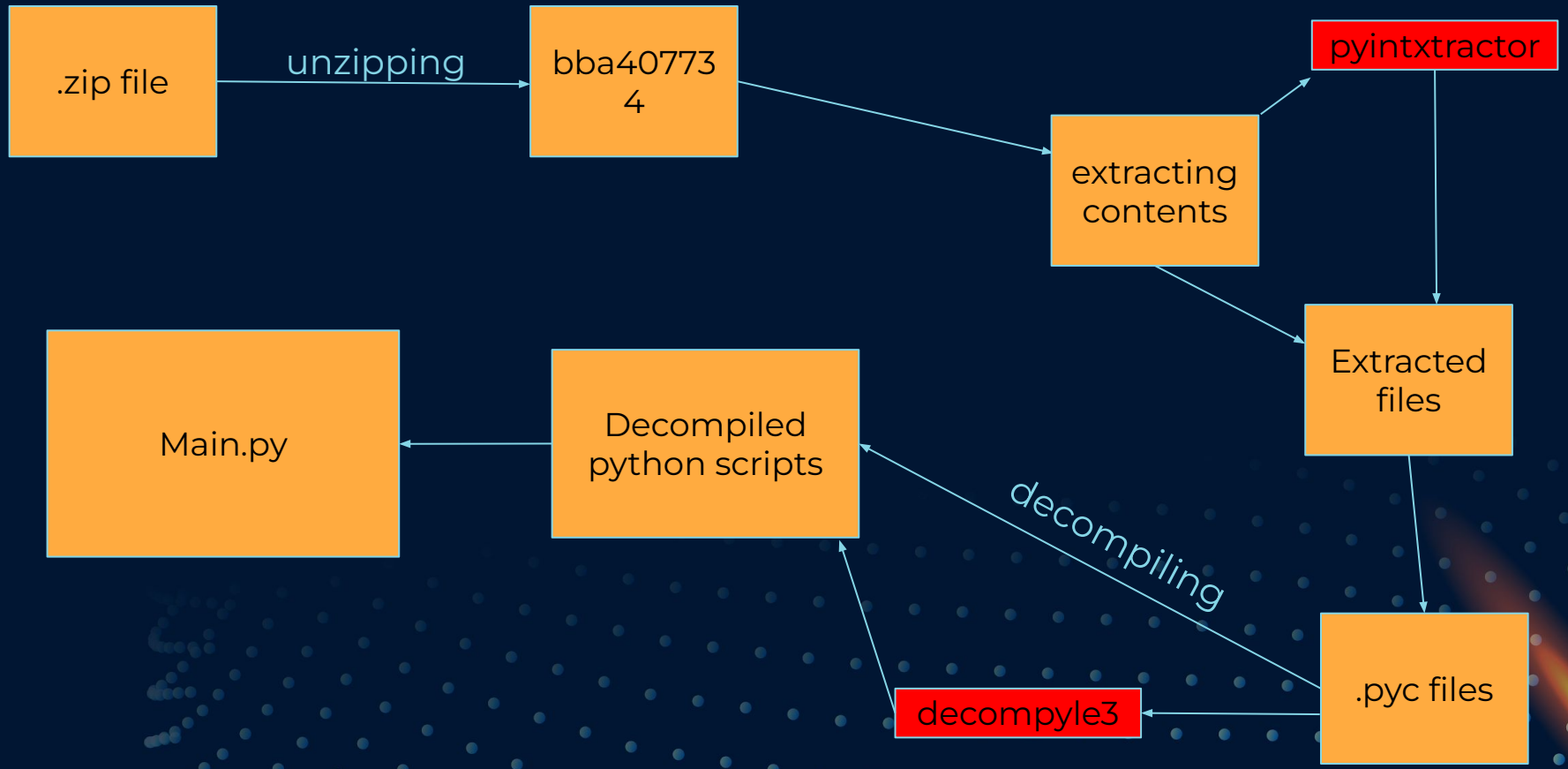
- **Reversing** the malware
- **Understanding** how it’s structured
- **Analyzing** its functionality
- **Reconstructing** the missing components



# Malware reversing

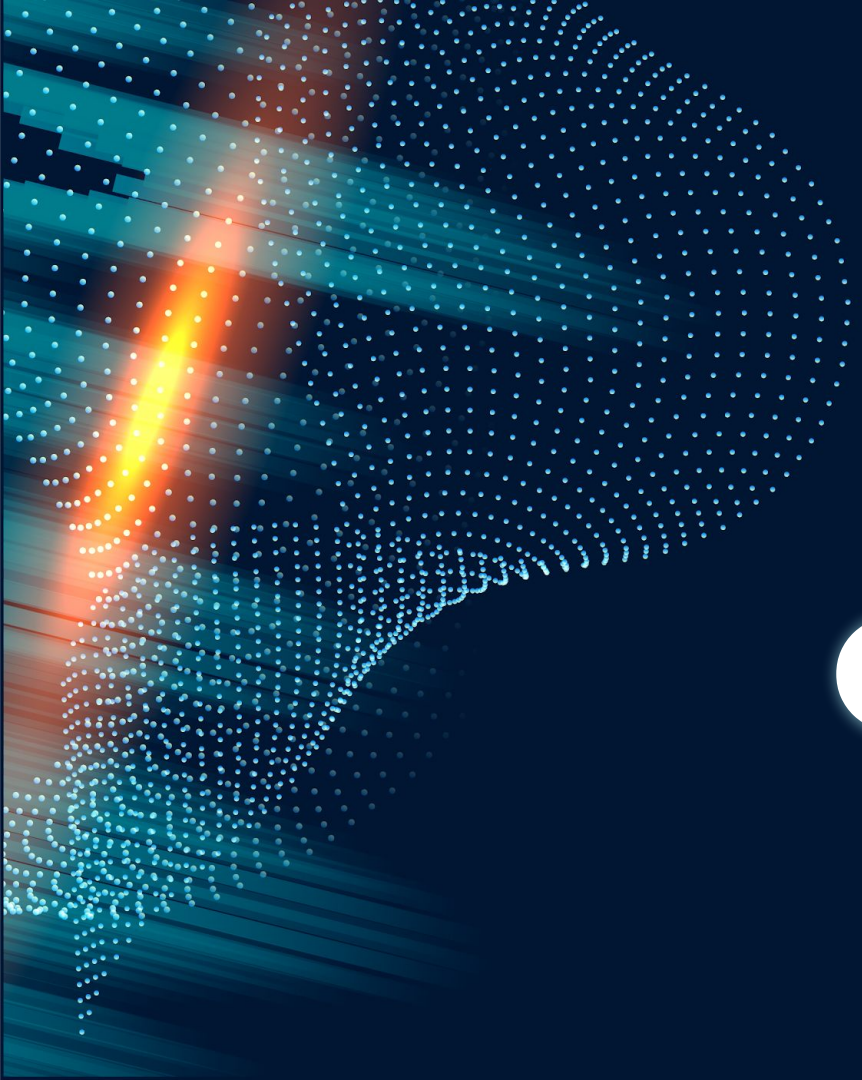
# What we are working with

- PyRation variant
- md5: 67e77dcdbf046a0fd91a0bbb3e807831
- Python executable (Windows PE file)


.zip file
unzipping
bba40773
4
pyintxtractor
extracting
contents
Extracted
files
Main.py
Decompiled
python scripts
decompiling
.pyc files
decompyle3

# socketio

- Socketio is a networking library
- Cornerstone of the malware itself
- In charge of all server-client interactions



# Malware Operation

# Malware operation

- Client
- Server
- Botmaster

# The client

- The result of the reversing the original .exe file
- Has its own unique session id (sid)
- Where all the functionality of the malware is written

# The server

- Can be run locally or remotely
- It broadcasts the instructions given by the bot master
- Updates automatically

# The botmaster

- Connects to the server
- Sends instructions to the server
- Instructions are sent to all clients

# Malware functionality

# Screenshots

- Takes screenshots every 10 minutes*
- Making use of pillow library
- Can only send images of 1MB or less.
- Image size depends on resolution (set to 600x600)

**On MacOS it needs permissions*

# Antivirus detection

- It detects installed antiviruses using windows_tools library*
- It only works on Windows (for now)
- Can detects up to 18 anti viruses

* https://github.com/netinvent/windows_tools

# Keylogging

- Detects key presses across all apps
- Uses the Listener object of the pynput library
- Client sends keylogs to server every minute*
- No local storage of keys is kept

**given that more than 8 seconds passed since the last key press*

# File management functions

- Download file from server (filename given by server)

- Write a new file (content and name given by server)

# Anonymous browsing

- Uses the infected computer’s IP address to browse remotely

- Parameters of the request are given by the server

# Command execution

- Allows remote command execution
- Special command (version check)
- Sends output to server

# Reconstructing Components

# Fixing the client

- Understanding what it does

- Fixing Windows-only function (antivirus detection)

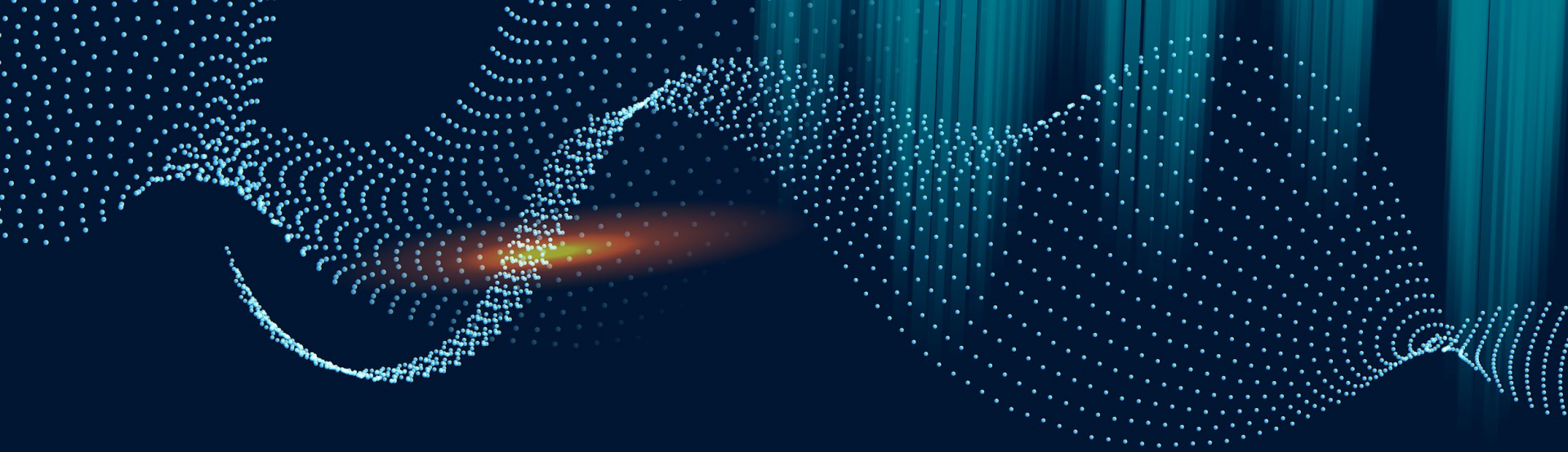
# (Re)creating the server

- From client code and socketio documentation, implement server

- Socketio servers cant take user input -> botmaster

# (Re)creating the botmaster

- Server cant take user input
- Special client with special functions
- May not be the real method



# Conclusion

- We were able to understand and recreate the malware functionality
- We shared the code with the community at: https://github.com/stratosphereips/Malware-CC-Recovery
- Learned the process to reverse, code and execute the malware locally