Malware Development and AV Evasion

Writing Bad Code … On Purpose!

Andrea Costanzo

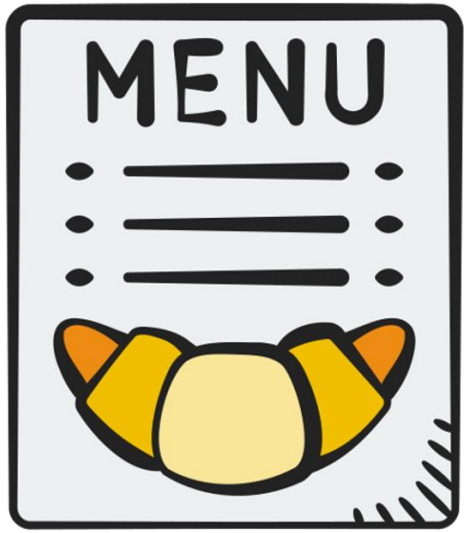
This course is designed solely for educational purposes to teach students about the principles, techniques, and tools of ethical hacking. The knowledge and skills acquired during this course are intended to be used responsibly, legally, and ethically, in compliance with applicable laws and regulations.

Authorized Use Only: Students must only use the methods, techniques, and tools taught in this course on systems and networks for which they have explicit authorization to test and analyze.

Personal Responsibility. Students are personally responsible for ensuring that their actions comply with all relevant laws and ethical guidelines. Neither the instructor nor the institution will be held liable for any misuse of the information or tools taught during this course.

Professional Integrity: Students are expected to uphold the highest standards of integrity and professionalism, refraining from any activity that could harm individuals, organizations, or systems

Summary: malware development and analysis



- Brief recap on malware
- Analyze malware using Python
  - Writing virus code
  - Writing worm code: the AbraWorm
  - Turning a Python videogame into a Trojan
  - Adware
  - Scareware
  - Infostealer
  - Cryptolocker
  - Malicious USB drive
- Advanced techniques
  - Compilation, packing and distribution
  - Persistence
  - Evasion

What is malware?

- **Malware is invasive software or computer code designed to infect, damage, or gain access to systems**
  - Malware is an umbrella term for any type of "**mal**icious soft**ware**"

- Malware isn't a threat only to PC (Windows & Macs): mobile devices are also vulnerable

- There are many different types of malware
  - Adware, spyware, viruses, botnets, trojans, worms, rootkits, and ransomware …
  - Each infects and disrupts devices differently
  - All malware variants are designed to compromise the security and privacy of computer systems

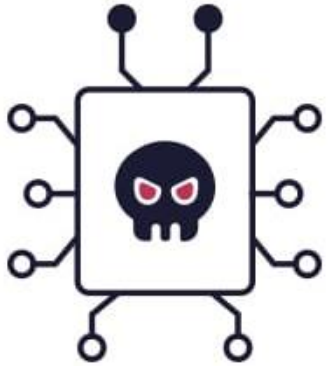
- The use of malicious software:
  - helps hackers evade security protocols more effectively
  - allows them to more easily target large numbers of victims
  - helps them perpetrate a wide range of sophisticated cybercrimes including fraud, extortion, data theft, and denial of service attacks

Why do hackers and cybercriminals use malware?

- Hacking and malware go hand-in-hand, computer hacking means *gaining unauthorized access to a device or network, which is often done through malicious code*
  - With malware source code widely available on the dark web, even pedestrian cybercrooks can get access easily

- All types of malware follow the *same basic pattern*:
  - your device gets infected after you unwittingly download or install malicious software

- How does a device get infected?
  - Often by clicking on a malicious link or visiting an infected website
  - Common sources of malware are peer-to-peer file-sharing services and free software download bundles. **Embedding malicious computer code in a popular torrent or download is an effective way to spread malware across a wide user base**



VIRUS

Spreads between computers

WORM

Spreads between computers in one company or location

TROJAN

Sneaks malware onto your computer

SPYWARE

Steals your data

ADWARE

Spams you with ads

RANSOMWARE

Encrypts files and blackmails you

FILELESS MALWARE

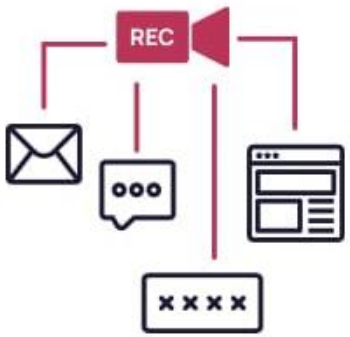
Operates in your system's memory

ROOTKIT

Gives remote access to your device

BOTNET

Turns your PC into a puppet



KEYLOGGER

Records user activity

Source: https://sosafe-awareness.com/sosafe-files/uploads/2023/05/Malware_Glossary_3.jpg

What is an anti-malware?

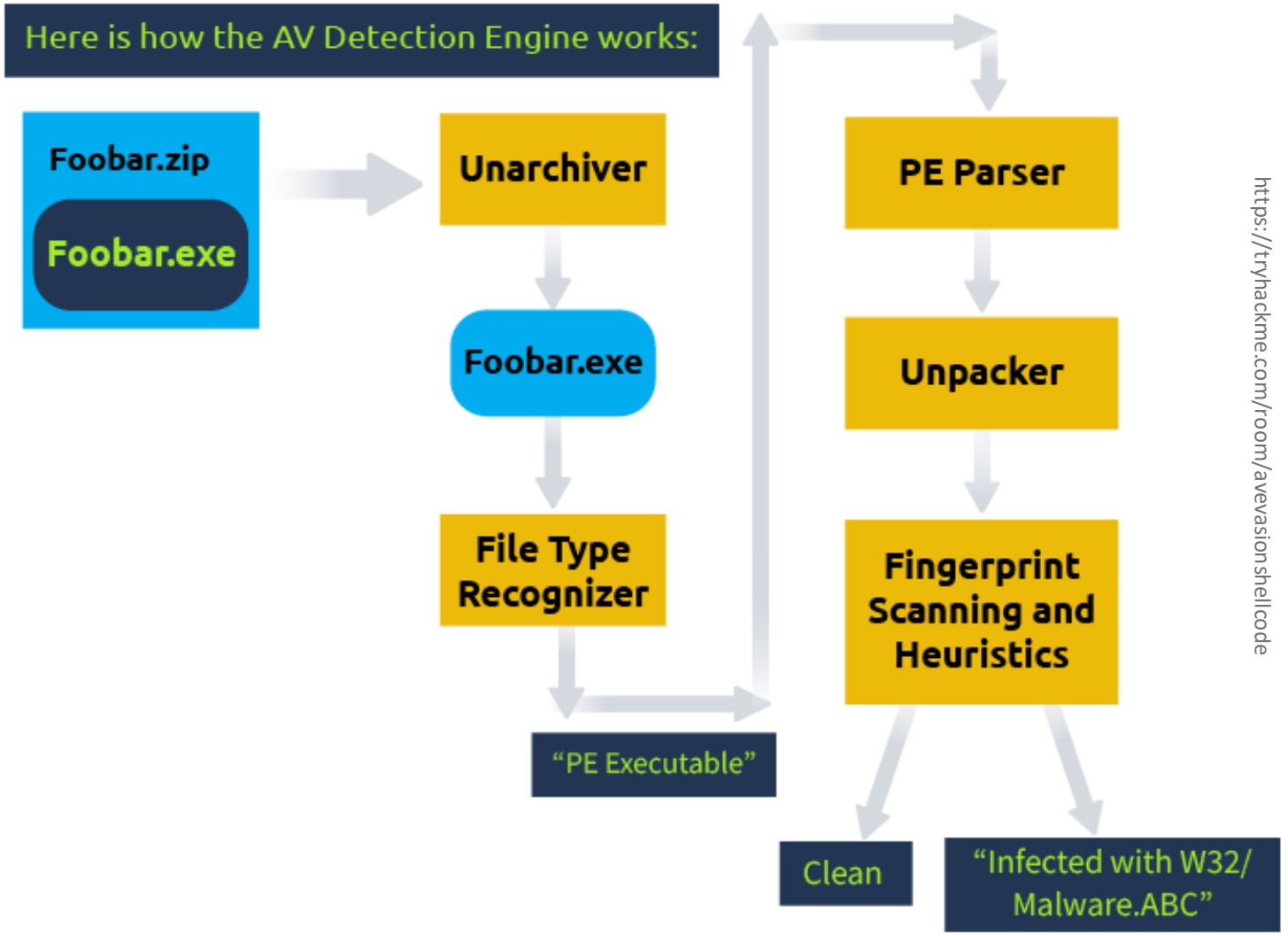
- Antivirus (AV) software is an extra layer of security that aims to detect and prevent the execution and spread of malicious files in a target operating system

- **It is a host-based application that runs in real-time (in the background) to monitor and check the current and newly downloaded files.**
  - The AV software inspects and decides whether files are malicious using different techniques

- AV software looks for malware with predefined malicious patterns or signatures, including but not limited to:
  - Gain full access to a target machine
  - Steal sensitive information such as passwords
  - Encrypt files and cause damage to files
  - Inject other malicious software or unwanted advertisements
  - Used the compromised machine to perform further attacks such as botnet attacks

How does an anti-malware work?

1. A suspicious *Foobar.zip* file is passed to AV software to scan
2. AV software applies an un-archiver feature to extract the files (*Foobar.exe*)
3. It identifies the file type to know which module to work with
   - … suppose it is an executable
4. It performs a PE parsing operation to pull the binary's information and other characteristic features
5. It checks whether the file is packed
   - if it is, it unpacks the code
6. Finally, it passes the collected information and the binary to the AV engine, where it tries to detect if it is malicious



https://tryhackme.com/room/avevasionshellcode

Mitigating malware

- **Update OS**
- **Use a reliable anti-malware and keep it always up-to-date**
- **Update software, including the Web browser**
  - Modern web browsers implement several defenses against malware
    - Alerting for websites that are not safe, blocking dangerous scripts, etc.
- **Regularly back-up your data**
- **Patch/update yourself!**
  - Do not download copyrighted media from shady websites (e.g. torrents).
    - Why would someone who does'nt even know you would give you something valuable for free?
    - Your personal data's value is way higher than the price of the stolen media
  - Be cautious with email and attachments
    - carefully review the sender and the email body
  - Be cautious with the links you are clicking on
    - carefully review the URL, do not trust HTTP
  - Use strong passwords and multi-factor authentication

This laboratory includes examples and discussions of malware-related concepts and potentially harmful techniques

All materials are provided **strictly for educational and defensive purposes**

- The goal is to understand how threats work in order to better detect and prevent them

Any code provided is **partial, simplified, or intentionally altered**

- Examples are designed **not to work** "*as-is*"
- Critical components are omitted or modified to prevent misuse

No actual malicious payloads are included or executed

- Any demonstrated behavior **is simulated or harmless**

Analysis of real-world malware (when discussed) **does not include reusable or operational routines**

- Techniques are shown at a **conceptual level only**

By continuing this lab, you agree to use the provided materials **responsibly, ethically, and only within authorized environments**

Dear Receiver

You have just received an Irish virus.

Since we are not so technologically advanced in Ireland,

This is MANUAL virus.

Please delete all the files on your hard disk yourself

and send this mail to everyone you know.

That'd be grand.

Tanx

Paddy O'Hacker at **paddy@bejaisus.com**