MAURICE LAMBERT

ANTIVIRUS BYPASS

1. IS IT REALLY AN ANTIVIRUS ?

2. WHAT ABOUT UNKNOWN MALWARE ?

3. HOW « ANTIVIRUS » WORKS ?

4. ARE HASHES GOOD SIGNATURES ?

5. GENERIC PATTERNS

6. PACKER

7. OBFUSCATION

8. ENTROPY BYPASS

9. EXECUTABLE FORMAT EXPLOITATION

10. ARE ANTIVIRUSES USELESS ?

ANTIVIRUS BYPASS

DO YOU THINK THAT AN "ANTIVIRUS" IS REALLY A PROTECTION AGAINST VIRUSES ?

IS IT REALLY AN ANTIVIRUS ?

IT’S NOT AN ANTIVIRUS BUT AN ANTIMALWARE

The term "antivirus" is often used instead of "antimalware" due to historical reasons and public familiarity, despite antimalware being a more accurate term. Antivirus software was first developed to combat computer viruses, which were the primary digital threats in the early days of computing. As the landscape of digital threats evolved, the term "antivirus" remained popular even as the software expanded its capabilities.

ANTIVIRUS USAGES

CHECK FILES ON DEMAND

- Check a specific selection of files
- Check the full filesystem
- Check each X time (scheduled tasks)
- Don't check a file when is written

- What about deleted file ?
  - Easy way to bypass basic antivirus: delete malware after execution
    - No persistence
    - Download the malware for each execution

- Role: identify threats (antivirus don't protect, there is no active protection in antivirus, this is the role for EPP)

- Goal: identify and delete malwares (malicious softwares)

ANTIVIRUS BYPASS

DO YOU THINK THAT AN ANTIVIRUS CAN DETECT UNKNOWN MALWARE ?

UNKNOWN MALWARE DETECTION

SHOULD AN ANTIVIRUS DETECT UNKNOWN MALWARE ?

A basic antivirus may struggle to detect unknown malware consistently. While traditional antivirus software primarily relies on signature-based detection, which is effective for known threats, it has limitations when dealing with new, unknown malwares.

HOW « ANTIVIRUS » WORKS ?

SIGNATURES AND REPUTATION

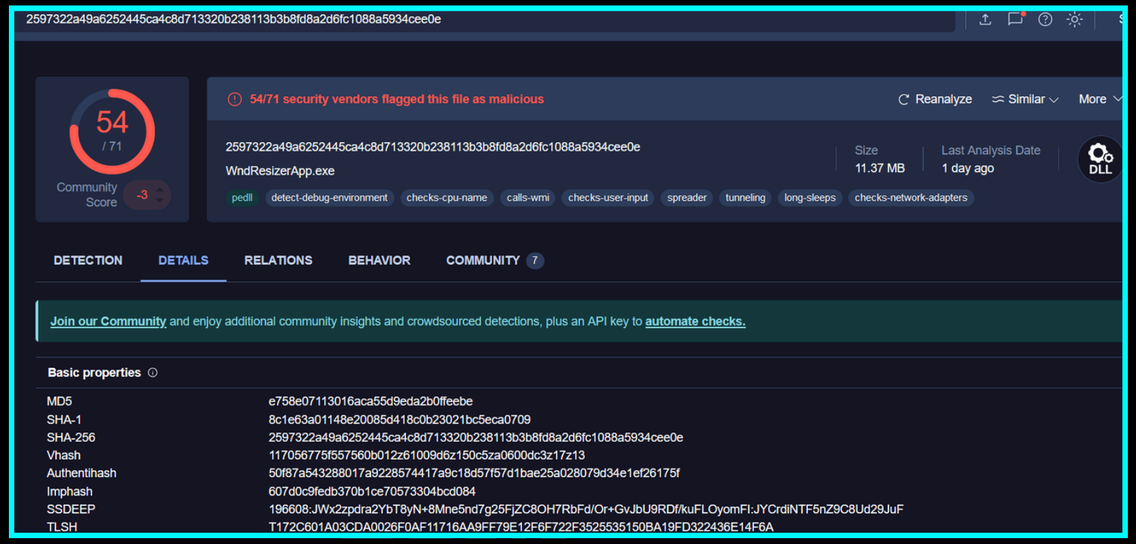
Antivirus software works by scanning files, programs, ~~and network traffic~~ to detect and remove malicious code.

- Signature-based detection
  - Hashes
  - Generic patterns
- Reputation
- Quarantine and removal

ANTIVIRUS BYPASS

DO YOU THINK THAT A HASH SIGNATURE IS A GOOD SIGNATURE ?

ARE HASHES GOOD SIGNATURES ?



HASHES TYPES

- Cryptographic Hashes
  - md5
  - sha1
  - sha256
  - sha512
  - sha3
  - blake2
  - ...
- Imphash (Import Hash)
- SPHF (Similarity Preserving Hash Functions)
  - SSDeep Hash (Context Triggered Piecewise Hashing)
  - TLSH (Trend Micro Locality Sensitive Hash)
  - VHash
- Authentihash
- ...

GENERIC PATTERNS

FUNCTIONS, ENTROPY, STRINGS...

- Imported / exported functions
  - Memory access/permissions
  - Debug functions
  - Network functions
  - Command line functions
  - COM "Interface" functions (DllRegisterServer)
  - ...
- Suspicious shannon entropy
  - Very high (greater than 7.2)
  - Very low (smaller than 2 or 3)
- File size
  - CIA maldev rule: executable smaller than 150KB
  - Lot of malwares use more than 1 GB overlay
- Strings
  - Bitcoin wallet
  - IOC: IP, Domain, URL
  - Number of strings
- Section names and characteristics

SUMMARY OF THE FIRST PART

ANALOGY TO THE ANTIVIRUS BEHAVIOUR

An antivirus behaviour is similar to the following discussion, with a file in the role of the girl and the antivirus in the role of the friend

- You: Do you think she's a good girl?
- Friend: She is not on the list of girls I know as malicious
- You: Okay but you don't know if it's a good girl.
- Friend: Yeah, yes, she's pretty.
- You: Yes but that doesn't answer my question...
- Friend: She is fine because her appearance does not look suspicious.

ANTIVIRUS BYPASS

IT'S TIME TO BYPASS !

PACKER

KNOWN AND TRUSTED PACKERS

- Used in production
- Modify sections name
- Compress
  - Reduce size
  - Greater entropy score
- Best antivirus decompress it and analyse data

CUSTOM PACKER

- Bypass antivirus
- Require access to suspicious calls
  - Can bypass suspicious imports
- Most of the time the entropy increases (encryption)
- Can modify sections name

The maldev CIA posture: don't use packer.

OBFUSCATION

SCRIPTS OBFUSCATION

- Random variables name
- Usage of eval or exec functions
- Hide the code structure
- Encoding or/and encryption
- Add useless code
- Hide constants value

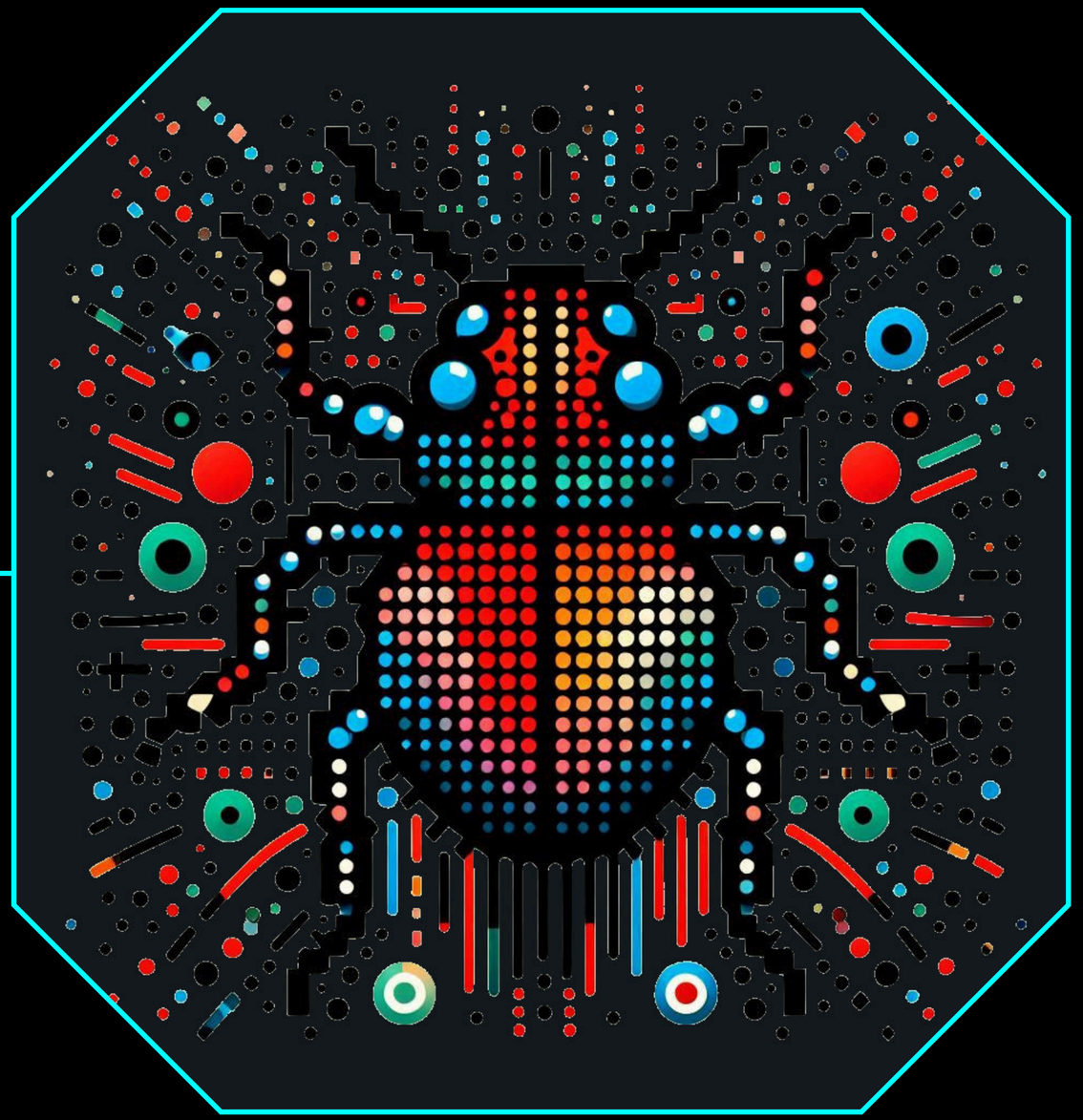
EXECUTABLE OBFUSCATION

- Add useless instructions

The maldev CIA posture: don't use obfuscation in executable.

ANTIVIRUS BYPASS

NOT DOCUMENTED TIPS AND TRICKS



ENTROPY BYPASS

PADDING

- Documented
- Problem: significant increase in file size
- Resolve: global file entropy
- Problem: don't modify the high entropy sector

SPECIFIC ENCODING/ENCRYPTION

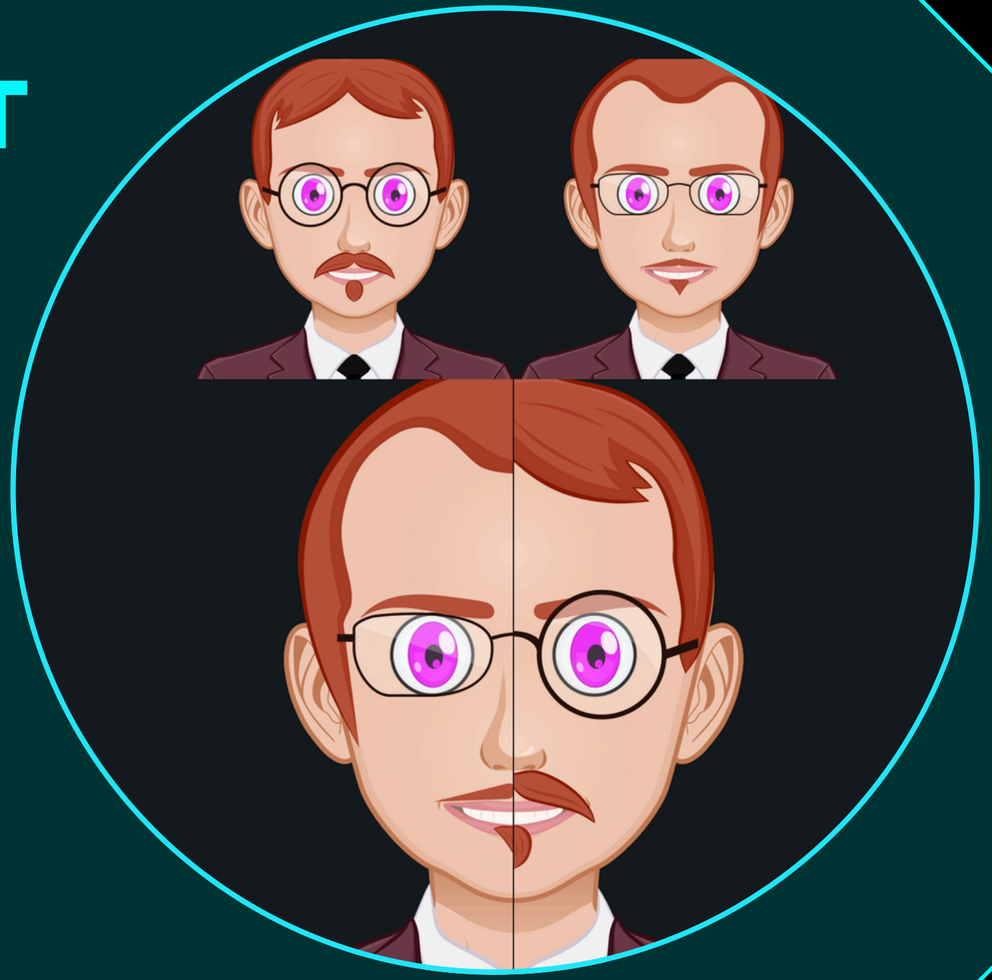
- I have never found any documentation online
- Problem: small increase in file size
- Resolve: high entropy sector

Implementation and POC: EntropyEncoding.

EXECUTABLE FORMAT EXPLOITATION

MODIFY UNUSED FIELDS, "METADATA" FIELDS AND STRINGS

- PE
  - DOS STUB
  - Rich headers
  - Timestamps
  - Fields reserved for future uses
  - Filename
  - Copyright
  - Description
  - ...
- ELF
  - Fields reserved for future uses
  - "Usage" in help message
  - Copyright message
  - ...



ANTIVIRUS BYPASS

TESTS TIME !

VIRUS TEST

BASIC EXECUTABLE INFECTION

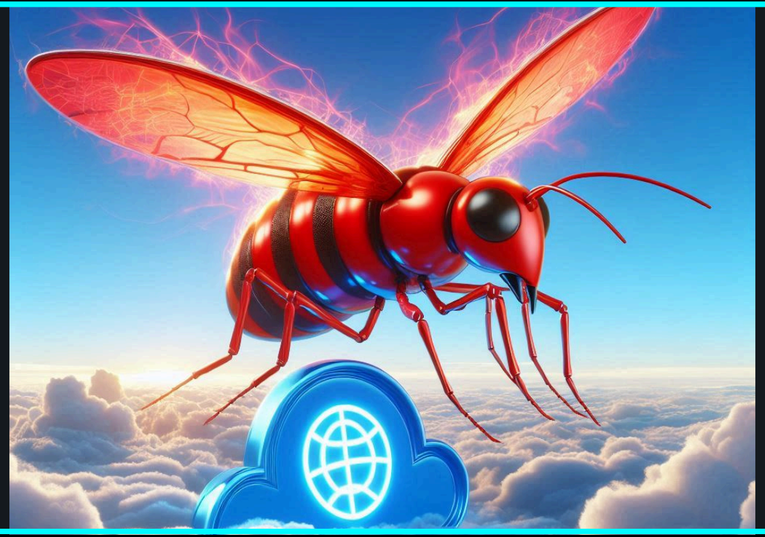
- Payload replication in other files
- Usages
  - Persistence
  - Defense evasion
  - "Analyst evasion"
- Virus type
  - Executable/DLL
  - Script
    - Admin scripts
    - Server scripts
  - Office documents
    - doc/docm and other microsoft office documents
    - PDF
    - RTF
  - System file
    - LNK
  - Archive files (add malicious files in trusted archive)
  - ...
- Infect the file using PeInjector

UNKNOWN MALWARE DETECTION

DOWNLOAD CUSTOM MALWARES

- Download non-obfuscated/non-packed malwares files
  - Spyware
  - Keylogger
  - MbrWiper
  - Ransomware
  - ...

FILELESS MALWARE EXECUTION



PE LOADER

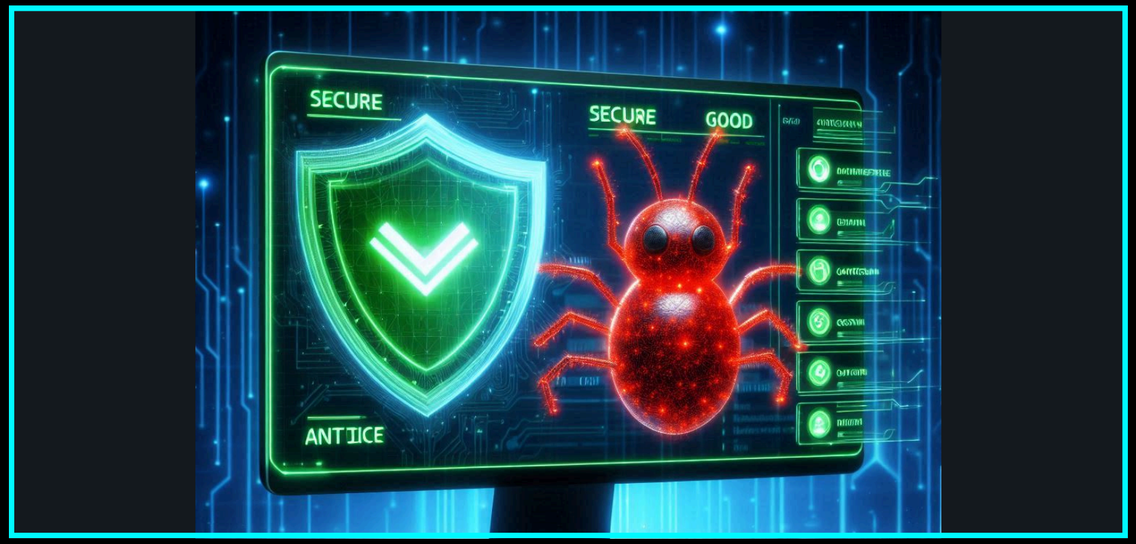
- Python PE Loader (PyPeUrlLoader)
  - Download the malware over HTTP(S)
  - Optional file decryption (useful to bypass firewall)
  - Stock the file in memory (don't write it on the disk)
  - Load it using PyPeLoader as the Windows linker
  - Execute the malware from entry point
- Don't write any malware on the disk
- No problem with entropy detection
- Require an internet/network access
- No persistence

PACKER DETECTION

USING A PYTHON PACKER

- Using PyPePacker
  - Compress
  - Encryption
  - Reduce entropy (using EntropyEncoding)
  - Possible conversion to PE (with high entropy in the overlay)
  - Possible obfuscation using PyObfuscator

KNOWN HACKTOOL FILE DETECTION



BYPASS USING EXE FILE STRUCTURE

- Download ChromePasswordsStealer
  - Antivirus detection
- Download it using BypassHash executable
  - No antivirus detection
  - Run the executbale to verify that it works well
  - Compare hashes
    - Cryptographic hashes
    - ssdeep
  - Compare size

ANTIVIRUS BYPASS

THE END: ARE ANTIVIRUSES USELESS ?

ANTIVIRUS TODAY

USE CASES FOR ANTIVIRUS TODAY

- EPP use antivirus signatures in real time
- EPP use antivirus signatures in memory
- Common antivirus bypass techniques use suspicious items monitored by EDR
- A good signature system generates fewer false positives than newer technologies (like machine learning, correlations, ...)
- A good signature system generates fewer bugs
- A good signature system requires less maintenance
- A good, up-to-date signature system protects you from known attack campaigns

RECOMMENDATION FOR PERSONAL WINDOWS

- Use microsoft defender because there is an EPP integrated (you pay the EPP with the Windows license).

APPENDICES

ImpHash

- Resolving ordinals to function names when they appear
- Converting both DLL names and function names to all lowercase
- Removing the file extensions from imported module names
- Building and storing the lowercased string . in an ordered list
- Generating the MD5 hash of the ordered list

PE format

- IMAGE_DOS_HEADER
- DOS Stub
- Rich headers
- IMAGE_NT_HEADERS
  - IMAGE_FILE_HEADER
  - IMAGE_OPTIONAL_HEADER32 | IMAGE_OPTIONAL_HEADER64
    - IMAGE_DATA_DIRECTORY
- IMAGE_SECTION_HEADER
- <section 1>
- <section 2>
- ...
- <section N>
- Overlay

- Instructions
- Imports (ILT, IAT)
- Exports (EAT)
- Relocations
- Resources
- Initialized data
- Uninitialized data
- ...

ELF headers

- ELF Header
- ELF Section Header
- <section 1>
- <section 2>
- ...
- <section N>
- Overlay
-

Windows loader

- Parse the PE file headers
- Load the PE file sections into memory
- Process the import table
  - Load required DLLs
  - Resolve external function addresses
  - Overwrite function pointers
- Apply base relocations
- Set permissions for each section
- Start execution at entry point address