4. Malware basics

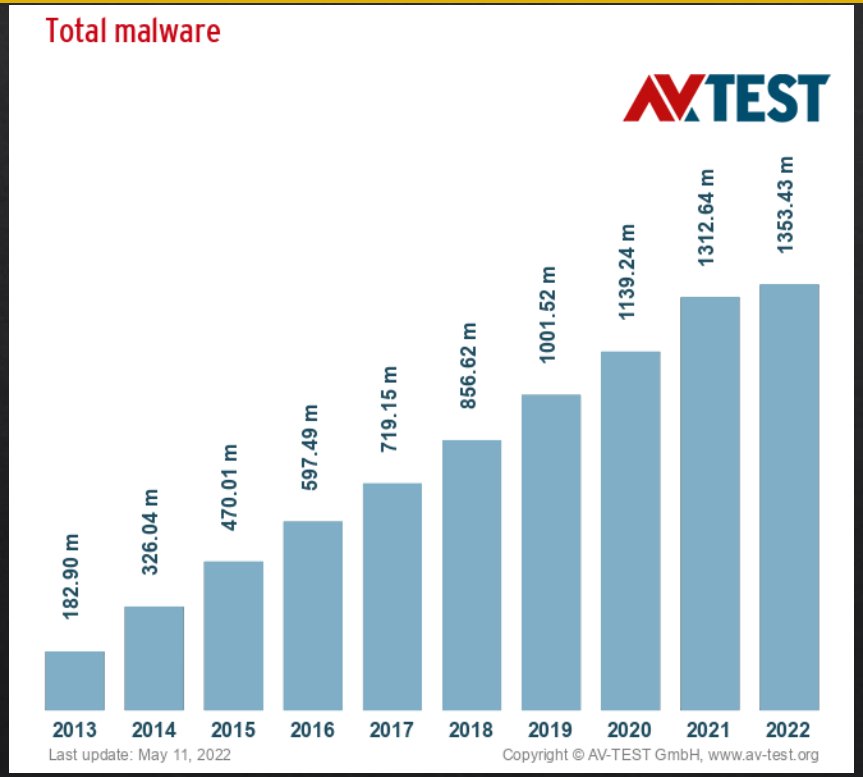
Jin Hong

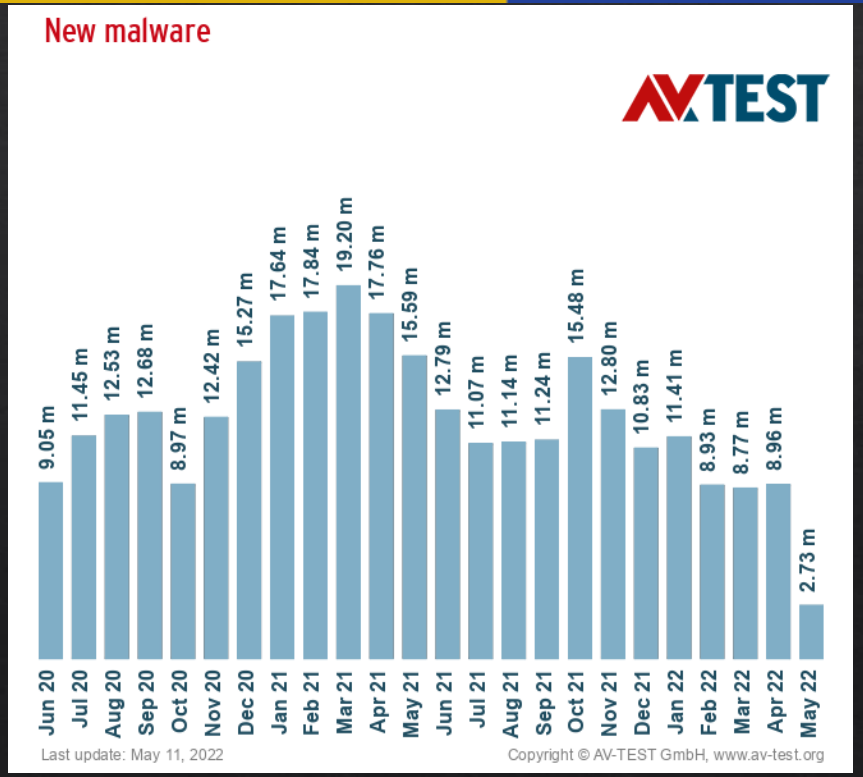
jin.hong@uwa.edu.au

Malware

- Short for malicious software
- Includes
  - Viruses
  - Worms
  - Spyware
  - Trojan Horses
  - Rootkits
  - Ransomware
  - Etc…

Malware stats





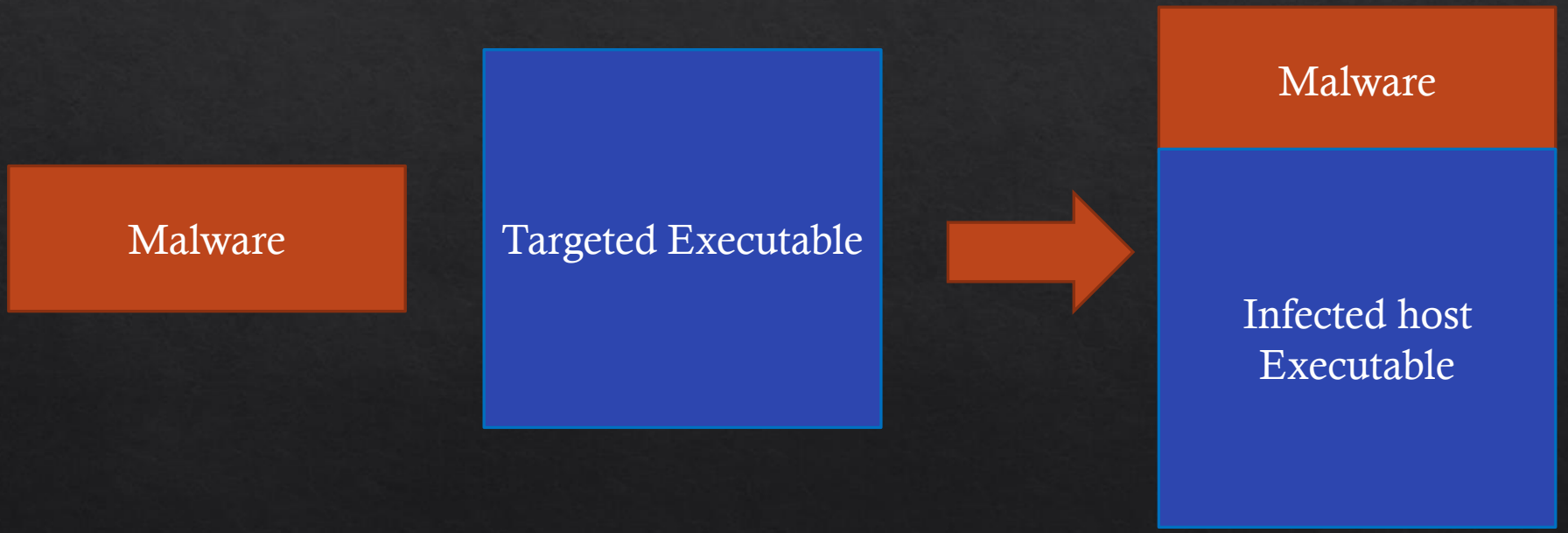
https://www.av-test.org/en/statistics/malware/?utm_source=canva&utm_medium=iframely

Malware

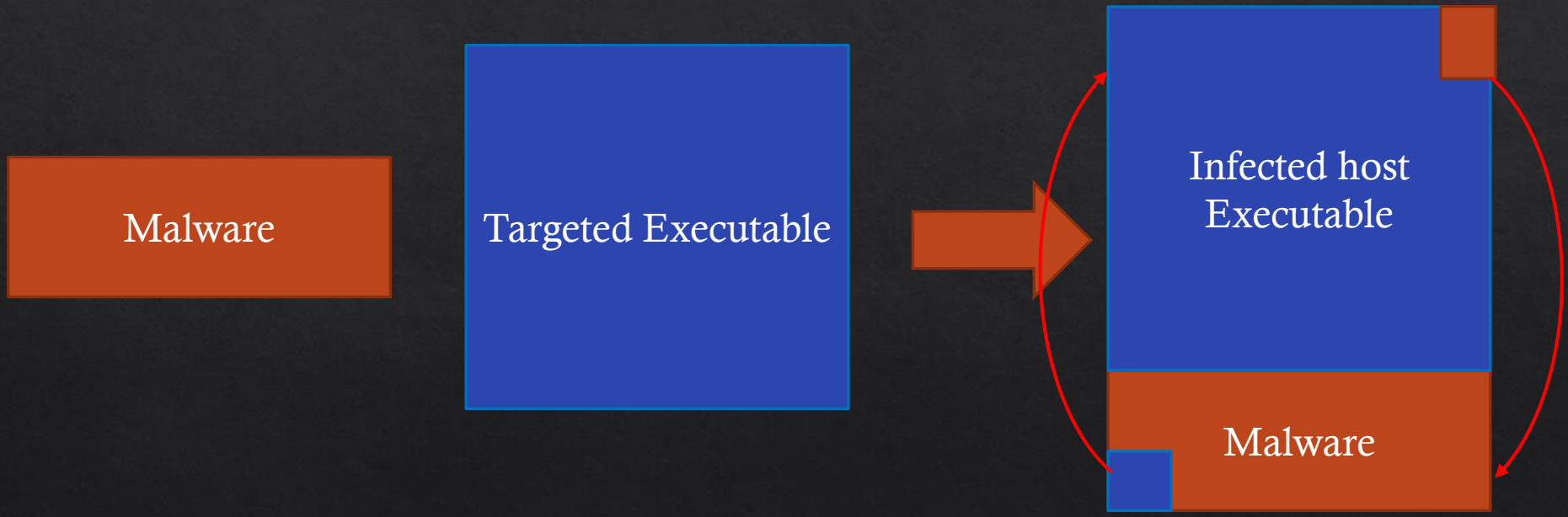
- Malicious Software – harms your system in many ways e.g., virus, worm, trojan etc.
- Spread in various ways:
  - Overwriting
  - Prepending
  - Appending
  - Cavity
- They mutate (Packer):
  - Oligomorphic – using multiple decryptors. E.g., Whale
  - Polymorphic – mutate certain part of itself. E.g., Virut
  - Metamorphic – rewrites all (or most) of itself. E.g., Zmist, Virlock

Malware - Overwriting

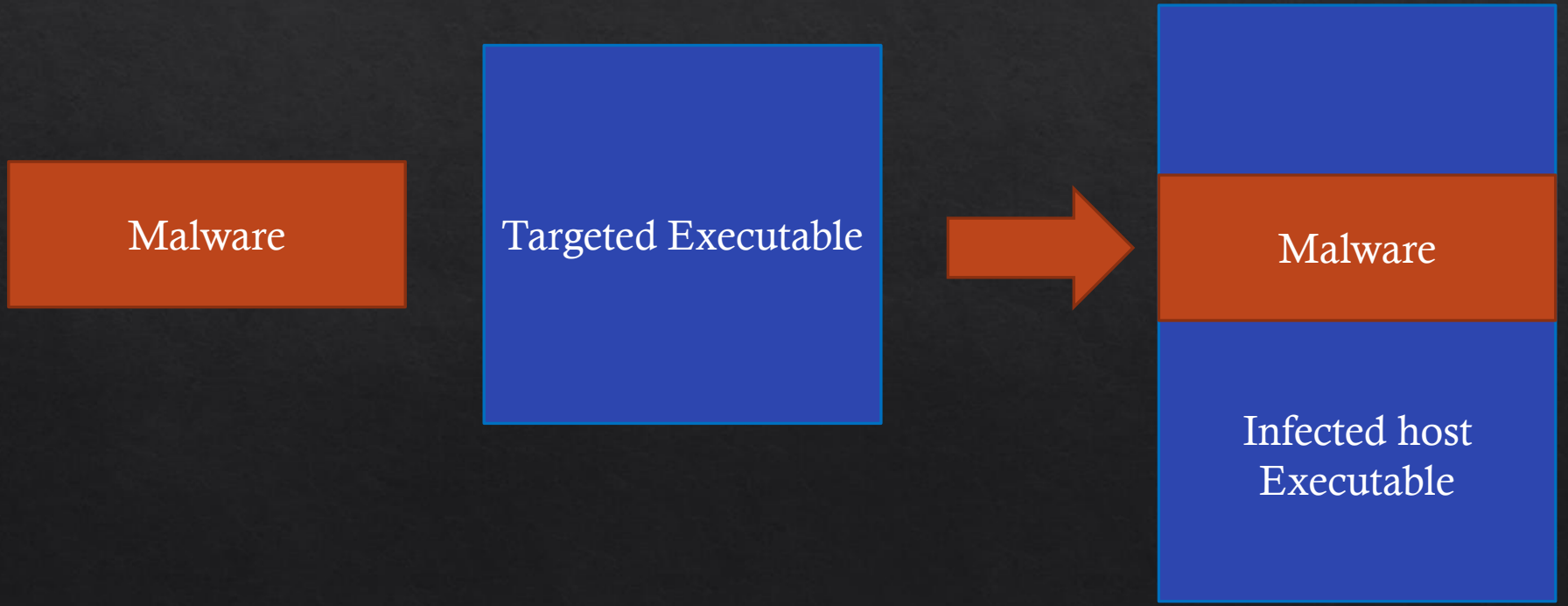
Malware - Prepending



Malware - Appending

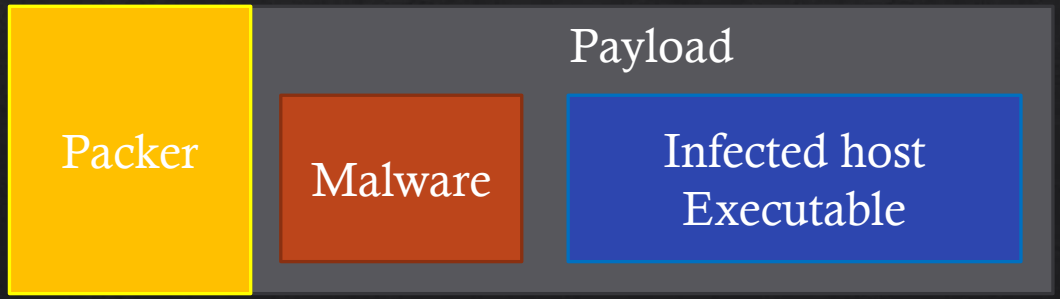


Malware - Cavity



Malware - Packers

- **Compress**
- **Encrypt**
- **Randomize (polymorphism)**
- **Anti-debug technique (int / fake jmp)**
- **Add-junk**
- **Anti-VM**
- **Virtualization**



Auto start

- Folder auto-start : C:\Documents and Settings\[user_name]\Start Menu\Programs\Startup
- Win.ini : run=[backdoor]" or "load=[backdoor]".
- System.ini : shell=”myexplorer.exe”
- Wininit
- Config.sys

Auto start cont.

- Assign know extension (.doc) to the malware
- Add a Registry key such as *HKCU\SOFTWARE\Microsoft\Windows \CurrentVersion\Run*
- Add a task in the task scheduler
- Run as service

Unix autostart

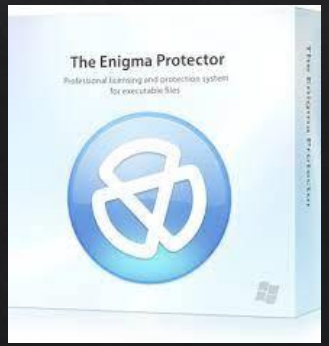
- Init.d
- /etc/rc.local
- .login .xsession
- crontab
  - crontab -e
  - /etc/crontab

Macro virus

- Use the builtin script engine
- Example of call back used (word)
  - AutoExec()
  - AutoClose()
  - AutoOpen()
  - AutoNew()

Malware - Packers

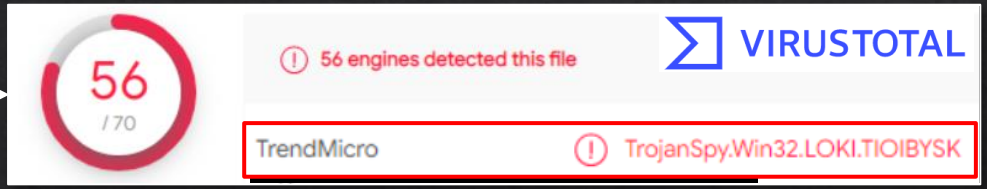
- **Example tools**
  - **UPX**
  - **The Enigma Protector**
  - **MPRESS**
  - **Exe Packer 2.300**
  - **ExeStealth**
  - **Morphine**
  - **Themida**
  - **FSG**
  - **PESpin**
  - **etc…**



Malware - Mutations

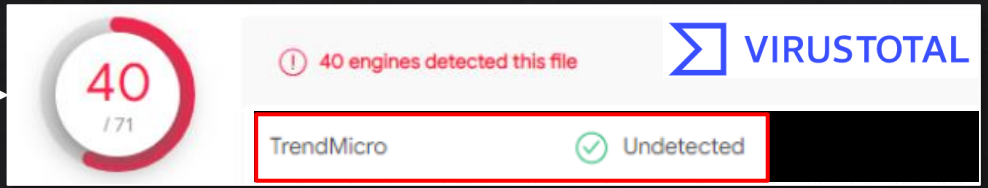
```
...
7b 05 50 9c 57 7d c3 9c 72 7d c2 9c 52 7f c3 9c
0f 04 29 9c 22 7d c3 9c 0f 04 1c 9c 73 7d c3 9c
...
```

Original sample

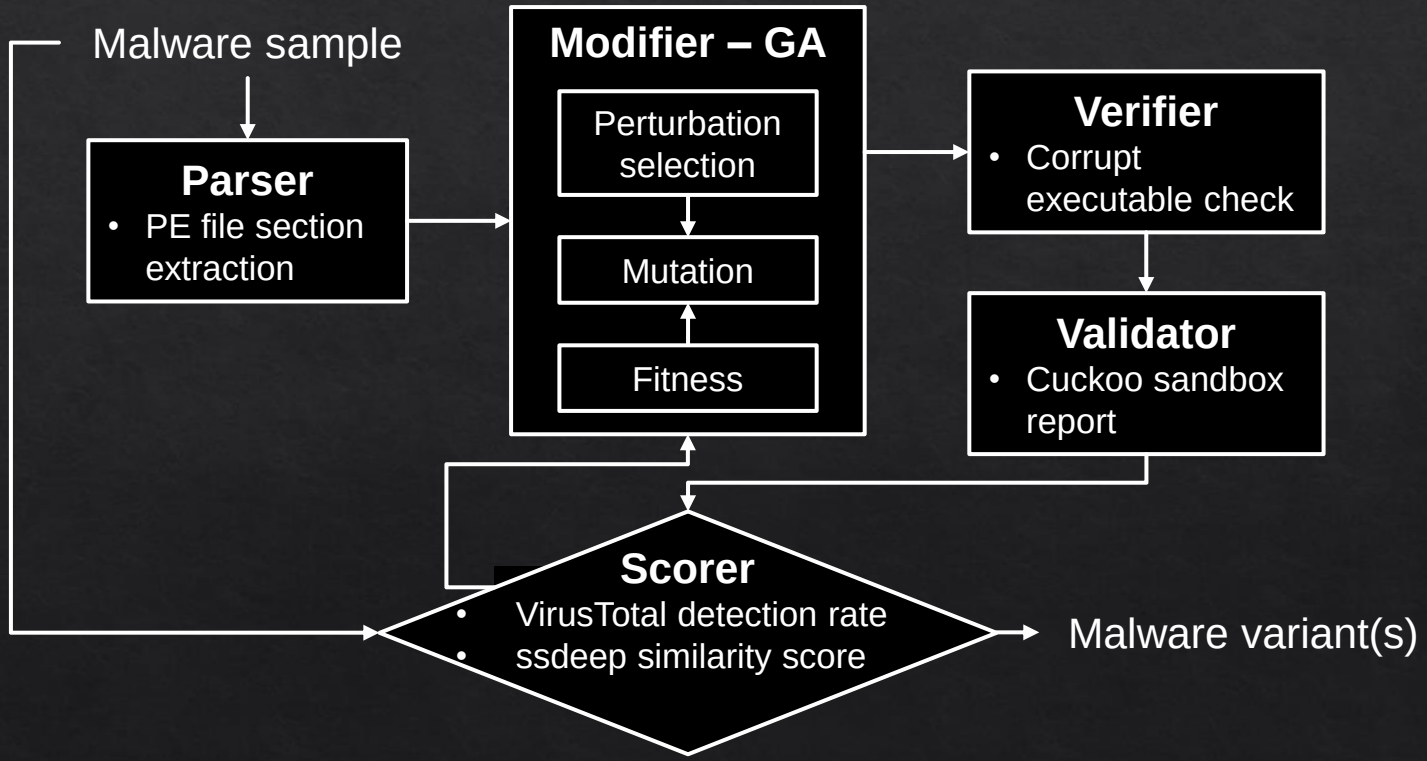



```
...
7b 05 50 9c 57 7d c3 9c 72 7d c2 9c 52 7f c3 9c
0f 04 29 9c 22 7d a4 96 5a 42 66 79 b0 5f c4 8e
...
```

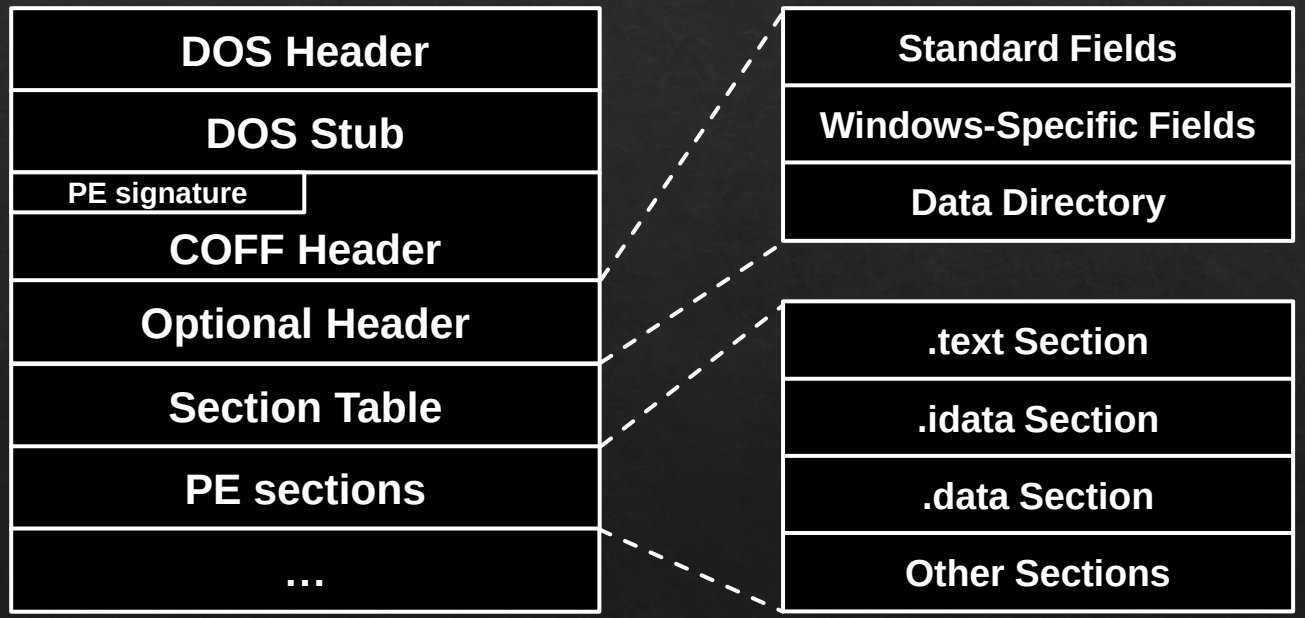
Modified sample



Malware – FUMVar



Malware – FUMVar



Malware – FUMVar

Perturbations	Description
Overlay append	Adds the random length of zeroes to the end of the binary.
DOS header	Change the field values in DOS header.
DOS stub	Change DOS stub to random byte sequence.
Optional header	Change the field values in Optional header.
Rich header	Insert a new content info Rich header.
Section add	Add a new section with sequence of bytes from benign sections.
XOR obfuscation	Encrypt some binary code using XOR operation with a one random byte key.

***a few selected perturbations**

Malware – FUMVar

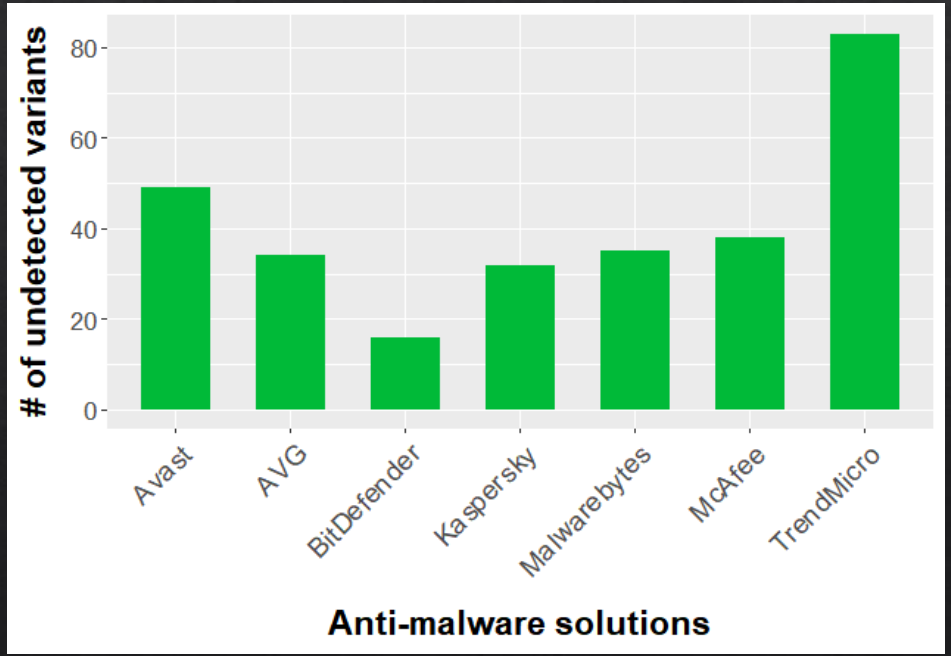
```
Sections
========
.text     1c798     2000     1c800     200     0     6.60167
.reloc    c         20000    200       1ca00   0     1.94734
.rsrc     15d90     22000    15e00     1cc00   0     7.99764
```

```
Sections
========
.text     1c798     2000     1c800     200     0     6.60167
.reloc    c         20000    200       1ca00   0     1.94734
.rsrc     15d90     22000    15e00     1cc00   0     7.99764
.ua       2000      37d90    200       32c00   0     0.63025
```


Section add (SAD) adds a new section with random sequence of bytes

Malware – FUMVar

- Anti-malware solutions have the low capability for detecting malware variants
  - TrendMicro was the worst one of the top 7 solutions, which 83 of 112 variant samples bypassed TrendMicro
  - BitDefender was the best-performing solution



Malware - Detection

- Signature
  - Find a string that can identify the virus
  - Fingerprint like
- Heuristics
  - Analyze program behavior
    - Network access, File open, Attempt to delete file, Attempt to modify the boot sector etc.
- Anomaly
  - Running the executable in a VM and observe
    - File activity, Network, Memory etc.

Most solutions

Expensive

Signatures: A Malware Countermeasure

- Scan compare the analyzed object with a database of signatures
- A signature is a virus fingerprint
  - E.g.,a string with a sequence of instructions specific for each virus
  - Different from a digital signature
- A file is infected if there is a signature inside its code
  - Fast pattern matching techniques to search for signatures
- All the signatures together create the malware database that usually is proprietary

Signatures Database

- Common Malware Enumeration (CME)
  - aims to provide unique, common identifiers to new virus threats
  - Hosted by MITRE
  - http://cme.mitre.org/data/list.html
- Digital Immune System (DIS)
  - Create automatically new signatures

White/Black Listing

- Maintain database of cryptographic hashes for
  - Operating system files
  - Popular applications
  - Known infected files
- Compute hash of each file
- Look up into database
- Needs to protect the integrity of the database

Shield vs. On-demand

- Shield
  - Background process (service/daemon)
  - Scans each time a file is touched (open, copy, execute, etc.)
- On-demand
  - Scan on explicit user request or according to regular schedule
  - On a suspicious file, directory, drive, etc.

Performance test of scan techniques
- Comparative: check the number of already known viruses that are found and the time to perform the scan
- Retrospective: test the proactive detection of the scanner for unknown viruses, to verify which vendor uses better heuristics

Anti-viruses are ranked using both parameters:
http://www.av-comparatives.org/

Online vs Offline Anti Virus Software

Online

- Free browser plug-in
- Authentication through third party certificate (i.e. VeriSign)
- No shielding
- Software and signatures update at each scan
- Poorly configurable
- Scan needs internet connection
- Report collected by the company that offers the service

Offline

- Paid annual subscription
- Installed on the OS
- Software distributed securely by the vendor online or a retailer
- System shielding
- Scheduled software and signatures updates
- Easily configurable
- Scan without internet connection
- Report collected locally and may be sent to vendor

Quarantine

- A suspicious file can be isolated in a folder called quarantine:
  - E.g,. if the result of the heuristic analysis is positive and you are waiting for db signatures update
- The suspicious file is not deleted but made harmless: the user can decide when to remove it or eventually restore for a false positive
  - Interacting with a file in quarantine it is possible only through the antivirus program
- The file in quarantine is harmless because it is encrypted
- Usually the quarantine technique is proprietary, and the details are kept secret

Heuristic Analysis

- Useful to identify new and “zero day” malware
- Code analysis
  - Based on the instructions, the antivirus can determine whether or not the program is malicious, i.e., program contains instruction to delete system files,
- Execution emulation
  - Run code in isolated emulation environment
  - Monitor actions that target file takes
  - If the actions are harmful, mark as virus
- Heuristic methods can trigger false alarms

Static vs. Dynamic Analysis

Static Analysis

- Checks the code without trying to execute it
- Quick scan in whitelist
- Filtering: scan with different antivirus and check if they return same result with different name
- Weeding: remove the correct part of files as junk to better identify the virus
- Code analysis: check binary code to understand if it is an executable, e.g., PE
- Disassembling: check if the byte code shows something unusual

Dynamic Analysis

- Check the execution of codes inside a virtual sandbox
- Monitor
  - File changes
  - Registry changes
  - Processes and threads
  - Networks ports

Additional Materials

(not assessed)

- Assembly programming
  - https://www.tutorialspoint.com/assembly_programming/index.htm
- Packers
  - https://resources.infosecinstitute.com/topic/top-13-popular-packers-used-in-malware/
- FUMVar
  - https://github.com/FUMVar/FUMVar

References

- Materials adopted from
- Stanford
- GMU
- Goodrich and Tamassia