Clean vs Malicious

Malware Verdict

OFTEN EASY

often small samples

often obviously malicious

except when they are not ...

Malware Verdict

CHALLENGING CASES 1

Trojanized software: patched legitimate programs

big code base

most code is clean

Malware Verdict

CHALLENGING CASES 2

Packed program with no indication of anything

but that is an unpacking problem!

will be handled later

Malware Verdict - Differentiation

BEWARE OF GRAYWARE

patched software that is cracked is grayware

Clean Verdict

DIFFICULT

clean software can have huge code base

you cannot analyse everything

Clean Verdict

DIFFICULT

proving absence of malicious code often not possible

--> often you cannot be 100% sure

set a maximum analysis time!

Clean Verdict - Triage

1. **VERSION INFO**
   - program and company name
2. **CERTIFICATE**
   - valid? manipulated?
3. **HOW WIDE-SPREAD**
   - submission numbers and sources
4. **AGE**
   - first submission date
5. **RESEARCH SOFTWARE**
   - website and publisher

Clean Verdict - Main Analysis

1. **SET MAX ANALYSIS TIME**
   - don't analyse forever!
2. **REASON FOR SUBMISSION**
   - submitter may think something is suspicious that is actually not
3. **FIND ITS PURPOSE**
   - no purpose? --> junk
4. **COMPARE WITH ORIGINAL**
   - bin diff tool in disassembler
5. **POINTS OF ENTRY**
   - main function, export functions ...
   - cctor in .NET
6. **SUSPICIOUS ITEMS FROM TRIAGE**

Free tools for binary diffing

VBINDIFF

only for finding small changes
but everything must be at the same offset
use to get first idea

MELD

text comparison, finds also insertions etc
can compare decompiled code, e.g.:

DnSpy --> export to project, then meld

BINDIFF

similarity of disassembled function blocks
for Ghidra use additionally BinExport

PORTEXANALYZER

compare hashes of sections
compare images with your eye
--pdiff option for visualized diff of 2 PE files

Finding certificate manipulation

ANALYZEPESIG BY DIDIER STEVENS

Check these values:

- Bytes after signature: must be 0
- Bytes after PKCS7 signature: must be 0-7
- Bytes after PKCS7 signature not zero: must be 0