So you want to be a Malware Reverse Engineer (RE) ?

A sharing of tips/lessons gathered from a 5 year old malware RE.

Whoami

@peta909

Malware RE for about 5 years at Palo Alto Networks

10 years at SG govt. agency related to defence

Speaking in my PERSONAL capacity!

dir

Tools, Techniques and Procedures (TTP)s I use while RE malware

Demos on some TTPs against a PE sample

How to take care of your most important tool?

QnA

WHY

What is the goal for this RE task ?

- malware or benign, find IOCs, discover bugs in products ?
- deep dive vs quick triage
- 1 hash vs a 1000s hash vs a cluster...

Able to adapt is the key!

- It's not about the tools
- It's not about static vs dynamic analysis
- It's about attaining the goal with minimal effort
- Me vs malware authors

Google is your friend

- Known or unknown ?
- Virus Total, Google ....
- Online sandbox e.g. Joe Sandbox, VMRay, AnyRun, Cuckoo…
- Trust but verify!

Initial Triage

- Gather as much info on the sample(s) as possible without deep analysis
- no debuggers/IDA
- Information can change as more time is spend on the sample(s)
- Don't start by debugging the sample, you maybe debugging some runtime libraries NOT the malware logic
- VB, self extracting Zip, Py2Exe, Innosetup ?

Demo 1 Initial Triage

What is the file format ?

Is it packed ?

Keylogger ? Trojan ? Dropper ?

Quick wins ? e.g. C2 in the strings

Google ?

Unpacking...

Why unpack ?

- could be the packer and/or malware having evasions
- throw away the noise
- easier to patch the sample logic later

automated unpacking vs manual vs hybrid

- full automated fails many times due to anti dumping /analysis
- hybrid can fail too
- prefer manual understand malware internals better

Demo 2 Unpacking

- Unpacking
  - allocate memory-> write into allocated memory-> execute allocated memory
- how to do a proper unpacking ?
  - look for PE loader
  - Setting Breakpoints
  - Is the sample unpacked ?

Anti analysis

Goal of the malware author

Hide the actual malware logic e.g. C2s, config, intent

Slow down the analysis process (automated and/or manual)

Able to adapt is the key!

- It's not about the tools
- It's not about static vs dynamic analysis
- It's about attaining the goal with minimal effort
- Me vs malware authors

Demo 3 Opaque Predicate

- Mess up CFGs or call graphs in IDA Pro
- Automate with scripts!
- Simple technique but it can waste a lot of analysis time!

Demo 4 Anti Debugging

- Don't patching the code e.g. JNZ to JMP
- Modifying the register value is better! e.g. ELF,
- Conditional breakpoint is your friend!

What is your most important tool?

YOU!

Body, Soul and Spirit

- Body - your physical self
  - Ergonomics for back, neck, wrist…
  - Desk bound jobs hazards are REAL!
- Soul - your thoughts
  - Please sleep!
  - Exercise
  - Eat and drink healthy
- Spirit - your inner self
  - Things Takes Time…
  - Do something non tech as hobby!

Thank you.

- Feel free to DM me on twitter @peta909
- Any questions/comments related to malware and/or RE
- I can’t promise I have all the answers :)

Demo 5 x86 + x64 = ?

- Wow64 environment
  - Kernel is x64
- x86 embedded with x64
  - Heaven’s gate
- Debuggers - Windbg for the win!

Demo 6 Using AppCall

- Automate decryption of strings AppCall
  - Easiest to use
  - Need to overcome anti debugging and other anti analysis
  - IDA Pro feature
- Implement the decryption function in python
  - AppCall dont work!
  - Works without IDA Pro
  - Takes time to RE function
- Extract the ASM and reimplement into assemblers like Flat Assembler (FASM)
  - When brute forcing is need!