Malware Analysis with Reverse Engineering

Hands-on

Matjaž Rihtar
Ljubljana, March 2018
Example

• What does this code do?
  ... 0F 31 66 BB FF 00 66 F7 F3 ...

• Disassembly
  
  rdtsc
  mov   bx, 0xFF
  div   bx

• Explanation - a random generator
  
  rdtsc           ; CPU time stamp counter → EDX:EAX
  mov   bx, 0xFF  ; 255 → BX
  div   bx        ; DX:AX % BX → DX (random [0..254])
Code patterns

- Recognizing
  - Architecture
  - Compiler
  - Language
  - Functions
  - Arguments
  - Results of functions
  - System calls
Important fundamentals

• Data structures and storage
  • Memory: byte/word/long/long long
  • CPU registers
  • Logical operators AND/OR/XOR
  • Endianness
    • Intel is little-endian

• CPU instructions
  • 32-bit/64-bit
  • Special: SSEx/AVX/...
Finding interesting stuff in the code

- Analysis of executables
  - EXE header
  - Imported DLLs
    - `LoadLibrary`
  - Strings
    - ASCII and Unicode
  - Constants
    - Precomputed values
      - CRC32, MD5, ...
  - Magic numbers
    - MZ for EXE/DLL files
    - Dates
OS Specifications

• Argument passing
  • Via stack and registers
  • cdecl, stdcall,fastcall

• Returning values
  • Modifying arguments on stack
  • Via pointers
  • Via registers

• Windows NT
  • CRT → main
  • GUI → WinMain
API Function hooks

• Microsoft Detours
  • Pro (x64) version: 10000 USD
• Others
  • madCodeHook
  • PolyHook
• Sandbox isolation
  • Sandboxie
  • Cameyo, Shade Sandbox, Shadow Defender, Cuckoo Sandbox, ...
• Virtual machines
  • VMWare Workstation, VirtualBox
Tools

• Disassemblers
  • IDA Pro

• Decompilers
  • Hex-Rays

• Debuggers
  • OllyDbg, WinDbg, Radare, x64dbg, ...

• System calls tracing
  • Sysinternals’ Process Monitor

• Other tools
  • Hex editor, Wireshark, QEMU, calculator
Example in practice

- Regex Match Tracer
  - IDA Pro
  - OllyDbg
  - Hex editor
  - Process Monitor
Complications

• Code obfuscation
  • Hiding text strings
  • Inserting garbage code

• EXE packers/crypters
  • Armadillo, ASPack, PECompact, UPX, ...
  • Packer detectors: PEiD, DIE (Detect It Easy), RDG Packer Detector, ...

• Code virtualization
  • Reversed code is virtual machine’s byte code

• Anti-debugging measures
  • IsDebuggerPresent, FindWindow, CsrGetProcessId, ...
  • TitanHide (kernel driver)
Literature

• Reversing - Secrets of Reverse Engineering (Eilam, 2005)
• Practical Malware Analysis (Sikorski, 2012)
• Practical Reverse Engineering (Dang, 2014)
• Reverse Engineering for Beginners (Yurichev, 2018)
Questions?

A CRYPTO NERD’S IMAGINATION:

His laptop’s encrypted. Let’s build a million-dollar cluster to crack it.

No good! It’s 4096-bit RSA!

Blast! Our evil plan is foiled!

WHAT WOULD ACTUALLY HAPPEN:

His laptop’s encrypted. Drug him and hit him with this $5 wrench until he tells us the password.

Got it.