Part 4

Advanced Dynamic Analysis

How can a controlled execution of the malware in a debugger (OllyDbg) increase your understanding?

We know a lot, but we want to see actual values

Input: values of parameters/arguments

Output: Values returned from functions

NTNU

Challenge 4

What is the value of inputs to and output from functions?

Need to execute the malware in a controlled fashion and pay attention to content of stack and registers.

Use: Debugger

NB! Why it may fail? Environmental dependencies

NTNU

Suggested Approach

- OllyDbg v2.0 (run as administrator)
- Open spybot in a debugger
  - Stops at 4011CB (OEP)

Hotkeys:

- F2 toggle breakpoint
- F9 run
- F7 step into (single instr)
- F8 step over (execute function)
- Ctrl G – goto address
- Ctrl F2 - restart

Challenges

1. Deobfuscation- function 402B81
2. File copying at 401458
3. Randomizing file name at 4012D8
4. How to get to 401482
    1. Find Mutex
    2. Find IP addresses

Challenge 4.1

Deobfuscation- function 402B81

- Ctrl G – 401280
- Set breakpoint (F2)
- F9 run (to breakpoint)
- F8 step through

- What happens when function 402B81 is called?
  - Look at inputs (push)
  - Return value (aex)
  - Memory location 412598 and 4125CA

Answer 4.1

- Call 402B81 twice, return eax:
  - Input pointer to memory location (global variable)
    - 412598 (first)and 4125CA (second)
  - Input length of string
- AEX contains pointer to deobfuscated string
  - First run 412598 points to
    - SOFTWARE\Microsoft\CurrentVersion\RunOnce
  - Second run 412B81 points to
    - SOFTWARE\Microsoft\CurrentVersion\Run

IOC: persistance

Challenge 4.2 – FileCopy

Study the loop from 40140D-401460

- Purpose?
- Study input arguments and return values for Call functions (main focus on CopyFileA)
- How are variables retrieved and stored?
- Role of esi?
- Exit condition (when is the loop done?)

Challenge 4.2 (continue)

- Goto 40140B (Ctrl+G) – jmp short 401458
- Set breakpoint (F2)
- F9 run to breakpoint
- F7 once (jmp to 401458) – cmp
  - Esi is a counter, incremented at 401457
  - Index for pointer to filenames
  - Filename compared to 0 (continue if zero)
- F2 breakpoint at 401458
- F7 once: check the zero flag it «controls» the loop

Challenge 4.2 (continue)

- F8 mulitple times (x12) until 40143A
  - Notice input on stack
- F8 once: look at edi and eax
- F8 multiple times (x6) until 401452 CopyFile
  - NewFileName and ExistingFileName is on stack
- F8 once
  - Open folder to see file created
- F8 once: increment esi
- Repeat with F8 if wanted otherwise F9

Challenge 4.2 (continue)

- F9 until esi=E
- F7 once: Check zeroflag Z=1
- Loop done

NTNU

Answer 4.2

- As expected from IDA analysis, the loop makes copies of spybot.exe under 14 different filenames
- 401458 cmp point to filenames in memory, loops as long as there is a name, continues when empty

Challenge 4.3 – Randomize

Why do we get a new filename each time we start the malware?

Challenge 4.3 Randomize File Name

- Investigate reandomization of the filename first run
  - Goto 401352 (Ctrl+G)
  - F2 – breakpoint
  - F9 – run
  - Notice aex (did the filecopy succed?)
  - First time: yes
  - Goto 401462
  - F2 break point
  - F9 – run
  - Ctrl F2 - restart

Challenge 4.3 Randomize File Name (cont)

- Investigate randomization of the filename second run
  - F9 – run (breakpoint at 401352 still there)
  - Notice aex (did the filecopy succed?)
  - Second time: no
  - Goto 401314
  - F2 F9
  - First time: F8 pay attention to 4012FC (look at 412088+esi)
  - F9 until esi=7 (length-4)
  - F8 until 401355: Path generation
  - F8 until 40134D: CopyFile
  - F9 (Done)

Answer 4.3

- All letter in the original filename wuaumqr are randomized one by one

Challenge 4.4 – Execution path

How do can we manipulate the execution path, i.e. reach 401482?

Challenge 4.4

How to get to 401482

- The trick
  - Goto 4012AE
  - F2 F9
  - **Manually increment eax (right click)**
  - F7 x2
- Goto + F2 + F9
  - 4014C6: Mutex=krnel
  - 401613: CreateThread startadd=4030E0 (keylogger)
  - 40166C: ip=209.126.201.20
  - F8: keylog.txt created
  - IP changes between 20 and 22 in loop

NTNU

What didn’t we cover

- A lot
- The IRC channel
- Commands to the malware
- Login, PRIVMSG (4132F3)
- …

NTNU

Questions?