המרכז
לחינוך סייבר
CYBER EDUCATION CENTER

Reverse Engineering Course

AntiDebug Techniques

Barak Gonen

המרכז
לחינוך סייבר
CYBER EDUCATION CENTER

Intro

- PE format
- DLL files
- Loader

AntiDebug Techniques

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

- We shall discuss only FEW AntiDebug methods:
  - IsBeingDebugged
  - NtGlobalFlag
  - CheckRemoteDebuggerPresent
  - Check for breakpoints
  - Check code integrity
  - Monitor thread
  - TLS Callback
  - Packed file

PEB

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

- Process Environment Block – windows data structure
  - We shall use 32 bit PEB values
- X32dbg:
  - peb() - view PEB address
- Windbg:
  - dt ntdll!_peb – view PEB structure
  - !peb – view specific process values
  - r $peb – view PEB address
  - eb $peb - edit PEB values

IsBeingDebugged

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

- IsBeingDebugged –at $PEB + 2
- Can be called by IsDebuggerPresent
- How to bypass?
  - Edit the PEB
  - Simply jump over IsDebuggerPresent
  - Patch code (change conditions etc)

NtGlobalFlag

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

- $PEB + 0x68
- A debugger will usually set the flags:
  - FLG_HEAP_ENABLE_TAIL_CHECK (0x10)
  - FLG_HEAP_ENABLE_FREE_CHECK (0x20)
  - FLG_HEAP_VALIDATE_PARAMETERS (0x40)

CheckRemoteDebuggerPresent

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

- Checks if a process has a non zero debug port
- How to bypass?
  - Same idea as IsDebuggerPresent

Monitor Thread

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

- Demo

Hands On

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

- https://data.cyber.org.il/reversing/Inception.exe
- Remove defense using patching

TLS Callback

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

- Thread Local Storage
- TLS callbacks -Mechanism provided by the loader
- Initialize / clean when
  - Thread starts / ends
  - Process starts/ ends
- Demo
- https://data.cyber.org.il/reversing/TLS.exe

Check Breakpoints

המרכז
לחינוך סייבר
CYBER EDUCATION CENTER

- Debuggers replace a byte with “CC” (int 3)
- Search for “CC” opcode in the text section

Check Code Integrity

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

- Pre-Calculate the sum (or other hash function) of all bytes
- Test during runtime that value is same

ClassWork

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

- https://data.cyber.org.il/reversing/BispooKeygen1.exe

Homework

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

- https://data.cyber.org.il/reversing/BispooKeygen2.exe

Packed File

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

- https://data.cyber.org.il/reversing/packed.exe
  - Credit: Polarium
- Demo

Exercise 2

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

- https://data.cyber.org.il/reversing/ShabakSecond.exe
- ONLY solve antidebugging