Topic: Malware Reverse Engineering
Anti-Debugging

Arnur Tokhtabayev, George Mason University
PE packer technologies

- Code
  - Virtualization
    - Anti-crack (prevent debugging/dumping, resist unpacking tools)
      - VMProtect, Enigma, Themida
    - Armadillo, ASProtect, Themida
  - PE packers (multilayer packing)
    - UPX, ASPack, PECompact, Boxed App
Dynamic Unpacking Scheme

Tool chain

1. Identify packer
   - PEiD

2. Trace (debug) unpacking routine
   - OllyDbg

3. Define Original Entry Point (OEP)
   - Signatures (semantics)

4. Dump unpacked image
   - OllyDump plugin

5. Rebuild import table (section)
   - ImportRec

OEP

Process dump, OEP
Unpacked Code Dumping to New PE
ASPack: manual unpacking

Plugins: http://www.openrce.org.downloads/
Anti-Debugging in Packers

Debugger detection

- System API: check for the existence of a debugger using system information (`IsDebuggerPresent()`, `CheckRemoteDebuggerPresent()`).
- System data: check debugger presence in Process/Thread global structures (`NtGlobalFlag`, `PEB.BeingDebugged`).
- Other: code integrity check (INT 3h instruction detection), SEH (INT 3h exception check), hardware breakpoints, execution latency
Anti-Debugging in Packers: Example
(Source: http://www.openrce.org/reference_library/anti_reversing)

**System API:**

```assembly
CALL IsDebuggerPresent ; invoke API
CMP EAX, 1
JE @DebuggerDetected
```

**System data:**

```assembly
MOV EAX, DWORD PTR FS:[18h] ; get TID entry address
MOV EAX, DWORD PTR DS:[EAX+30h] ; get PEB entry address
MOVZX EAX, BYTE PTR DS:[EAX+2h]
CMP EAX, 1
JE @DebuggerDetected
```

**Note:**

FS – segment register
(points to various items in TIB (Tread Information Block))

Example:

FS[0] -> SEH
FS[30h] -> Address of PEB (Process Environment Block) structure

```c
typedef struct _PEB {
    BOOLEAN InheritedAddressSpace;
    BOOLEAN ReadImageFileExecOptions;
    BOOLEAN BeingDebugged;
    BOOLEAN Spare;
    ...
};
```
Anti - anti – debugging: Unpacking robust packers
Dr. Arnur Tokhtabayev,
Center for Secure Information Systems
George Mason University
Computer Science Department
Research I, Rm 435
E-mail:
- atokhtab@gmu.edu
- arnur78@gmail.com