Malware Analysis and Antivirus Technologies: Using Debuggers to Analyze Malware
Agenda

• Debugger basics
  • Introduction
  • Scenarios and tools
• How debuggers work
  • Debug API
  • The debugger loop
  • Underlying mechanisms
• Debugging malware
• Anti-debugging
Debugging and debuggers

- Wikipedia:
  - Debugging is a methodological process of finding and reducing the number of bugs, or defects (…)
  - A debugger is a computer program that is used to test and debug other programs
- Our purpose is different
  - The debugger is just a tool to analyze the behavior of unknown applications
Common Debugger Features

• Create a new process or attach to an existing process
• Control the target process
  • Break the execution
  • Step through code
  • Trace through code
• Set breakpoints
• Read and write memory
• Read and write registers and flags
• View the call stack
• View a disassembly of the code
• (View source code)
User-mode Debugging

Kernel-mode

User-mode

Debugger.exe

Target.exe
Remote Kernel-mode Debugging

- Debugger.exe
- Ntoskrnl.exe
- Debuggee.sys
- Debuggee.exe

Target OS (Guest)

Kernel-mode

User-mode
Local Kernel-mode Debugging

Target OS

Kernel-mode

Ntoskrnl.exe

User-mode

Windbg.exe

No control over target machine!

Vista and beyond: “bcdedit /debug on” and reboot
IDA Pro “Hardware Debugging”
Tools: OllyDbg

- Graphical debugger for 32-bit Windows
- Only for user-mode debugging
- Designed for working without source code
- Lots of useful plugins
Tools: Immunity Debugger

- Similar to OllyDbg, but adds several nice features such as Python scripting
Tools: Windbg

- Graphical 32-bit/64-bit debugger from Microsoft
- For user-mode and kernel-mode debugging
- Also local kernel debugging
Windows Debug API

- Most Windows debuggers are based on the Debug API
  - Implemented by dbghelp.dll
- Interesting functions
  - `DebugActiveProcess()` to attach to an existing process
  - `WaitForDebugEvent()` to get events
  - `DebugBreakProcess()` to break into a running debuggee
Debug loop

```c
while (TRUE) {
    WaitForDebugEvent(event, timeout);
    switch (event->dwDebugEventCode) {
        case EXCEPTION_DEBUG_EVENT:
            switch (event->u.Exception.ExceptionRecord.ExceptionCode) {
                case EXCEPTION_ACCESS_VIOLATION:
                case EXCEPTION_BREAKPOINT:
                    (...)
            }
        case LOAD_DLL_DEBUG_EVENT:
            (...)
    }
}```
Context

- The current state of a thread is described by a CONTEXT structure
- Contains all registers and flags
- Very platform-specific

```c
lkd> dt nt!_CONTEXT
+0x000 ContextFlags : Uint4B
+0x004 Dr0              : Uint4B
...                        
+0x08c SegGs : Uint4B
+0x090 SegFs : Uint4B
...                        
+0x09c Edi              : Uint4B
+0x0a0 Esi : Uint4B
...                        
+0x0b8 Eip : Uint4B
+0xbc SegCs : Uint4B
+0xc0 EFlags : Uint4B
+0xc4 Esp : Uint4B
```
Exceptions

- Exception = an event that occurs during execution of a program that requires execution of code outside the normal execution flow

- Question: what happens when this code executes in user-mode?

```assembly
0042D9B0 xor eax,eax
0042D9B2 push eax
0042D9B3 call dword ptr [myfunc]
0042D9B6 mov ecx,80494678h
0042D9BB mov dword ptr [ecx],eax
0042D9BD push eax
0042D9BE call dword ptr [myfunc2]
```
Handling an Exception (Windows XP on x86)

1. CPU does address translation for 80494678h and sees the supervisor-bit set for this page of virtual memory. A page fault exception (#PF) is raised

   • See “IA-32 Intel Architecture Software Developer’s Manual, Volume 3A” for details on exceptions and interrupts on x86

2. The page fault handler in the kernel, through the Interrupt Descriptor Table (IDT), gets control. It passes control to the exception dispatcher.

3. Since the exception happened in user-mode, the dispatcher looks for a user-mode debugger listening to a debug port.

4. The user-mode debugger gets a “first-chance” exception notification.

5. If the user-mode debugger does not handle the exception, the context is adjusted so that the user-mode exception dispatcher will run next.
Handling an Exception (Continued)

6. The user-mode dispatcher looks for any installed vectored exception handlers (VEH) and calls them.

7. If none of the handlers were prepared to handle the exception, a chain of structured exception handlers (SEH) is also called.

8. If the exception is still not handled, it’s re-raised and execution goes back to the kernel exception dispatcher.

9. The user-mode debugger is sent a “second-chance” exception notification.
Handling an Exception in Application Code

- Structured Exception Handling (SEH)
  - Operating system service for applications to provide mechanism for handling exceptions
  - In code: __try/__except/__finally
  - Exceptions are handled by the thread that caused the exception
  - Many handlers can be registered to a stack-based handler chain

- Vectored Exception Handling (VEH)
  - Expands SEH
  - Not frame-based, more like notification callbacks
  - VEH exception handlers take precedence over SEH chain
  - See AddVectoredExceptionHandler() in MSDN
VEH and SEH

![Diagram showing the relationship between exception handling and VEH/SEH chains](image-url)

1. Exception
2. VEH chain (process-specific)
3. SEH list (thread-specific)
4. Vectored Exception Handler #1
5. Structured Exception Handler #1
6. Vectored Exception Handler #2
7. Structured Exception Handler #2
Debugger Features: Single Stepping

• Single stepping means executing the application one instruction at a time
  • A very typical debugger feature
• Usually implemented using EFLAGS.TF (Trace Flag)
• When TF=1, the processor generates a debug exception for each executed instruction
Debugger Features: SW Breakpoints

- Used to break the execution of the target process at a specific address
- Typically implemented using INT 3
  - Debugger writes a byte with value 0xCC (opcode for INT 3) to the memory address
  - Note: usually the debugger makes this transparent to the user, so the modification is not visible in memory view
- Good:
  - No limitation to the amount of software breakpoints
- Bad:
  - Modifies the actual code bytes
  - Cannot break on reads or write addresses, just execution
Debugger Features: HW Breakpoints

- The CPU debug registers provide support for up to 4 hardware breakpoints
- DR0-3 store the linear addresses to be monitored
- DR7 configures the type of event
  - Break on execution, break on read, break on read/write
  - Length of data item to be monitored (1, 2 or 4 bytes)
- Good:
  - Does not modify code bytes
- Bad:
  - Limited number of breakpoints
  - Limited length of monitored data item (often you would like to break on a range of bytes)
  - Target can read and change the debug register contents through exception handlers
Debugger Features: Reading and Writing Memory

- Debugger must be able read and write the virtual memory space of the debuggee
- Done through normal Windows API functions
  - ReadProcessMemory()
  - WriteProcessMemory()
Debugger Features: Initial Breakpoint

• Initial breakpoint = first time the debugger gets control of the target

• OllyDbg has three options for the initial breakpoint
  • System breakpoint
    • Loader breaks into debugger **before any application code is run**
  • Entrypoint of main module
    • First break is at the entrypoint as defined by the main module PE header
  • WinMain (if known)
    • Attempts to skip compiler-generated stub and break at high-level main

• With anything else than system breakpoint, **application code can run before you get control!**
  • See PE/COFF specification and TLS callbacks
  • Support for TLS callbacks in Ollydbg 2.0
Why Debug Malware?

• Faster to execute and step through code than just read it
  • Especially for beginners it’s more convenient to ”see what the code does”
• Dealing with runtime packers
• A good, free debugger is sometimes all you need
  • They all have a disassembler
  • Ollydbg has pretty good code analysis features
• Also a matter of preference
  • Sometimes a combination of static and dynamic analysis is good
    • Browse through the application in a good interactive disassembler
    • When you’ve spotted the interesting parts, you can see how they are called and what they do in a debugger
  • Tip: use plugin and MAP files to transfer names from IDA to OllyDBG
Note on Debugging and Security

- We are now moving from **reading unknown code into executing it!**
  - Even if you are very careful, eventually your debuggee will escape
- If you ever debug potentially malicious applications, you need a safe environment
  - A machine you don’t care about (a virtual machine running on anything important is not good enough...)
- No Internet connectivity (or very limited)
- Be extra careful with any portable media
Debugging Applications vs. Debugging Malware

• When debugging normal applications, you typically have symbols and/or source code
  • Obviously not the case for malware
• Normal applications don’t actively prevent debugging
  • Malware plays a lot of tricks to avoid dynamic analysis
• Most common reason to debug a normal application: analyze a bug
  • Most common reason to debug malware: analyze functionality

Requirements for the tools are different!
Runtime Packers

• With a runtime packer, the original executable is compressed (or obfuscated/translated) and embedded into a new executable

• In the simple case, the packed executable has a stub that
  • Unpacks the original file
  • Jumps to the original entry point (OEP)

• Direct static analysis of a packed executable is impossible

• One way is to use a debugger and let the executable unpack itself...

• A separate lecture coming up on this!
Anti-Debugging

- Anti-debugging is used to prevent debugging an application or make it less convenient
  - Attempt to prevent a debugger from being attached
  - Attempt to detect an attached debugger and
    - Exit
    - Crash the application
    - Behave differently
    - …
  - Make debugging difficult by clearing breakpoints, causing "noise" with exceptions, jumping to the middle of exported functions to avoid breakpoints, …
Anti-Debugging Techniques

• Documented API’s to check if a debugger is active
  • IsDebuggerPresent()
  • CheckRemoteDebuggerPresent()
  • …

• Debugger-specific tricks
  • Checking for objects created by the debugger
    • Registry keys
    • Files
    • Devices
    • Windows
    • Remote process memory scanning
Anti-Debugging Techniques

- Checking data set in the process by the debugger
  - PEB!IsDebugged
  - PEB!NtGlobalFlags
- Scanning for software breakpoints (0xCC)
- Detecting through timing key points of execution
  - See \textit{rdtsc instruction}
- Detecting virtual machines *)
  - Processes, file system, registry: VMWare tools service, registry settings
  - Memory: look for "VMWare", IDT location
  - Hardware: virtual hardware
  - CPU: non-standard opcodes, non-standard behaviour of existing opcodes
  - Lots and lots more...

*) http://handlers.sans.org/tliston/ThwartingVMDetection_Liston_Skoudis.pdf
Anti-Debugging Techniques

• Playing tricks with exceptions
  • Flooding with exceptions
  • Disabling hardware breakpoints through exception handlers
• Self-debugging
  • Create a child process that attempts to debug the parent
  • Split the execution into parent and child (debuggee), which communicate through exceptions
• Other miscellaneous:
  • NtQueryInformationProcess() with ProcessDebugPort
  • NtSetInformationThread() with ThreadHideFromDebugger
Anti-Debugging: Example 1

; Check from Process Environment Block (PEB)
; if a debugger is attached

mov eax, dword ptr fs:[18h] ; self-pointer to TEB
mov eax, [eax+30h] ; pointer to PEB
movzx eax, byte ptr [eax+2] ; PEB.BeingDebugged

test eax, eax
Anti-Debugging: Example 2

push offset handler
push dword ptr fs:[0]
mov fs:[0],esp
xor eax, eax
div eax ;generate exception
pop fs:[0]
add esp, 4
;continue execution ;...

handler:
mov ecx, [esp+0Ch]
add dword ptr [ecx+0B8h], 2 ;skip div
mov dword ptr [ecx+04h], 0 ;clean dr0
mov dword ptr [ecx+08h], 0 ;clean dr1
mov dword ptr [ecx+0Ch], 0 ;clean dr2
mov dword ptr [ecx+10h], 0 ;clean dr3
mov dword ptr [ecx+14h], 0 ;clean dr6
mov dword ptr [ecx+18h], 0 ;clean dr7
xor eax, eax
ret
SEH Chain

```
fs:[0] Stack
    next_handler
    handler_ptr
    ...
    ...
    next_handler
    handler_ptr
    handler1
    handler2
```
Anti-Debugging: Example 3

.text:004042F7       push 0
.text:004042F9       call dword ptr [eax] ; eax = msvcr60!_CIacos
.text:004042FB       mov edx, eax ; eax = 0x00321EA8
.text:004042FD       imul edx, 10000h ; edx = 0x1EA80000
...                  push 0E1A8A200h
.text:004042DD       pop esi
.text:004042DE       add esi, edx ; esi = 0x0050A200, read-only
.text:004042E0       mov edi, esi
.text:004042E2       loc_4042E2:
.text:004042E2       lodsd
.text:004042E3       xor eax, 0C2EA41h
.text:004042E8       stosd ; access violation!
.text:004042E9       loop loc_4042E2

Source: https://www.openrce.org/blog/view/1043/SpyShredder_Malware_Spammed_on_OpenRCE (Rolf Rolles)
Example 3 Explained

- msvcrtd_Ciacos calculates the arccos of the input
  - Return value in floating point register, not eax!
- After the call to _Ciacos,
  - Eax = 0x00321EA8 if a debugger is present
  - Eax = 0x00321E98 if a debugger is not present
- The value in eax is left there by the _Ciacos function as a side-effect
  - It comes indirectly from an earlier call to calloc()
  - The difference of 0x10 bytes in the pointers is caused by the debugger enabling debug heap settings!
Anti-Debugging: Example 4

Function in original application

Control flow (jumps) replaced with interrupts

Copyright F-Secure 2010. All rights reserved.
Anti-Debugging: Example 4 (continued)

Parent process (debugger)

Child process (debuggee)

- Debug loop
- Encrypted table of jmp destinations

Copyright F-Secure 2010. All rights reserved.
Getting Around Anti-Debugging

- Make the debugger less visible to the target
  - Clear out bits from PEB
  - Disable setting of debug heap flags
  - OllyDbg has extensions to automate this
- Depending on the anti-debugging techniques used, change your methods
  - If hardware breakpoints are cleared, try software breakpoints
  - Attach to the process after it has unpacked itself, but before it exits
- Step through the most problematic parts of code and work around manually
  - Tedious and time-consuming
Process Dumps

• It’s possible to create a dump of the state of a running process
  • The modern format is called a *minidump*
  • Contents are configurable: thread contexts, parts of memory, handle data etc.
  • Use Windbg (.dump) or userdump.exe to create a minidump
• Minidumps can be loaded into Windbg and analyzed
  • Read memory, examine thread state, enumerate open handles
  • Cannot run code at this point
• Sometimes useful for malware analysis
  • Forensic information: a minidump from an infected machine is more valuable than just the sample
  • A dump of the process will have the uncompressed code and data visible
Related Tools: Procmon

- Procmon (from Sysinternals) is a more light-weight tool for dynamic analysis
- A flexible process monitor
  - File system
  - Registry
  - Process/thread activity
- Rich filtering possibilities
Resources

- Ollydbg
  - http://www.ollydbg.de
- Debugging Tools for Windows (Windbg)
  - www.microsoft.com/whdc/devtools/debugging/default.mspx
- Structured Exception Handling, Vectored Exception Handling
  - http://msdn.microsoft.com/msdnmag/issues/01/09/hood/
- Windows Anti-Debug Reference (N. Falliere)
  - http://www.securityfocus.com/infocus/1893
- P. Szor, The Art of Computer Virus Research and Defense
  - Chapter 15.4.4 – Dynamic Analysis Techniques
  - Chapter 6.2.7 – Antidebugging
Protecting the irreplaceable