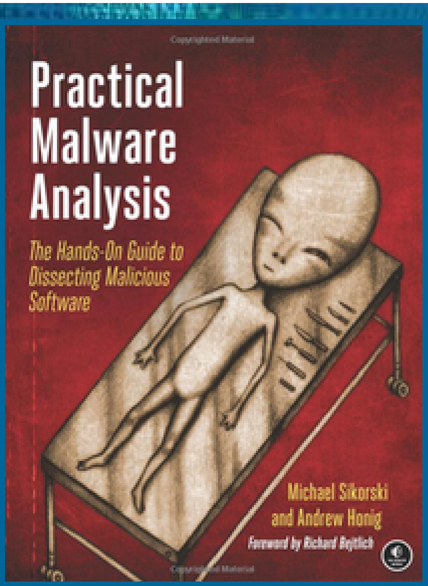
CNIT 126: Practical Malware Analysis

Spring 2017 Sam Bowne

`37184 Mon 6:10 - 9 PM SCIE 200`

Schedule · Lecture Notes · Projects · Links · Training · Home Page

Scores



Catalog Description

Learn how to analyze malware, including computer viruses, trojans, and rootkits, using disassemblers, debuggers, static and dynamic analysis, using IDA Pro, OllyDbg and other tools.

Advisory: CS 110A or equivalent familiarity with programming

Upon successful completion of this course, the student will be able to:

A. **Describe types of malware, including rootkits, Trojans, and viruses.**
B. **Perform basic static analysis with antivirus scanning and strings**
C. **Perform basic dynamic analysis with a sandbox**
D. **Perform advanced static analysis with IDA Pro**
E. **Perform advanced dynamic analysis with a debugger**
F. **Operate a kernel debugger**
G. **Explain malware behavior, including launching, encoding, and network signatures**
H. **Understand anti-reverse-engineering techniques that impede the use of disassemblers, debuggers, and virtual machines**
I. **Recognize common packers and how to unpack them**

Textbook

"Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software", by Michael Sikorski and Andrew Honig; ISBN-10: 1593272901 Buy from Amazon

Quizzes

The quizzes are multiple-choice, online, and open-book. However, you may not ask other people to help you during the quizzes. You will need to study the textbook chapter before the lecture covering it, and take the quiz before that class. Each quiz is available for one week, up till 8:30 am Saturday. Each quiz has 5 questions, you have ten minutes to take it, and you can make two attempts. If you take the quiz twice, the second score is the one that counts, not necessarily the higher score.

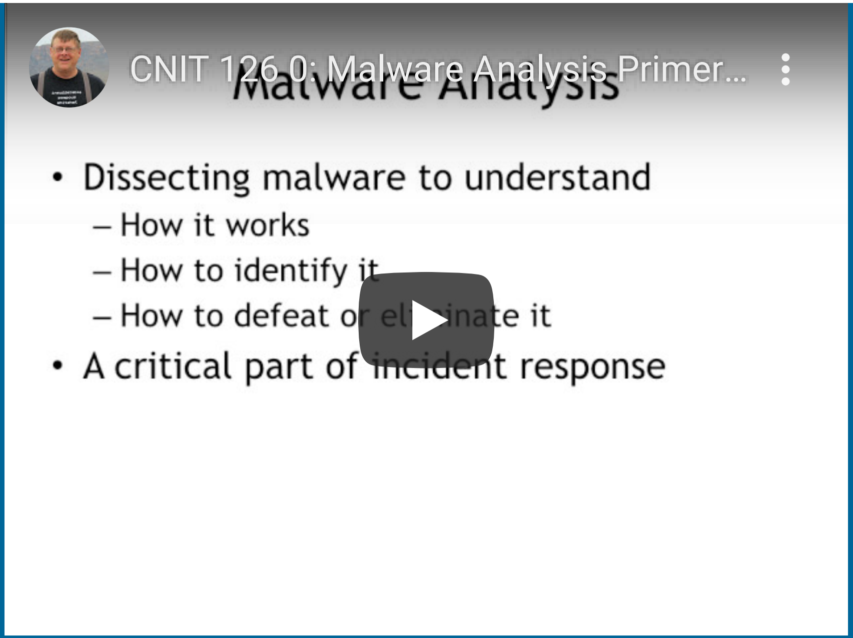
To take quizzes, first claim your RAM ID and then log in to Canvas here:

https://ccsf.instructure.com

Schedule (may be revised)

Note: Chapter Numbers are one too high in the E-Book: Chapter 0 is mislabelled as Chapter 1, etc.

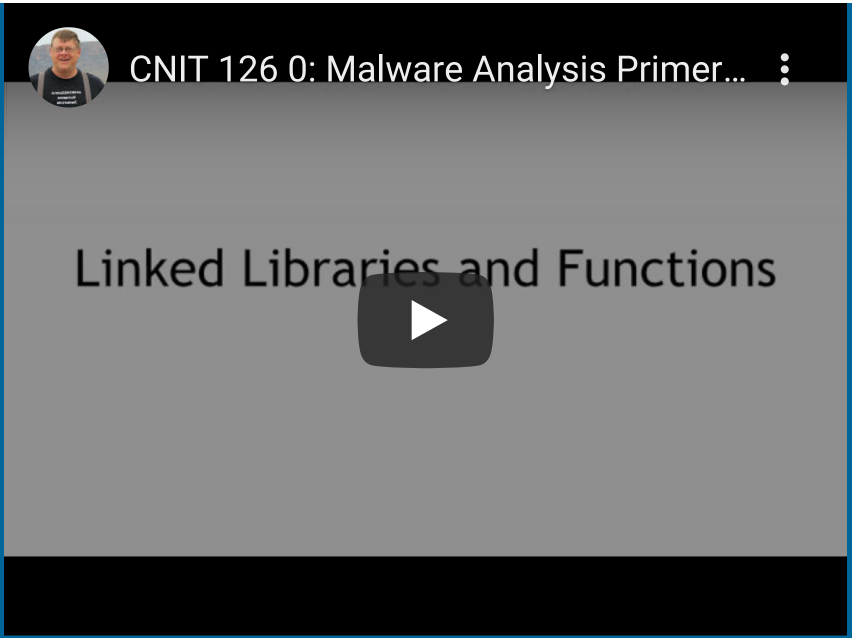
Date	Quiz	Topic
Mon 1-23		0: Malware Analysis Primer & 1: Basic Static Techniques



CNIT 126 0: Malware Analysis Primer...

Malware Analysis

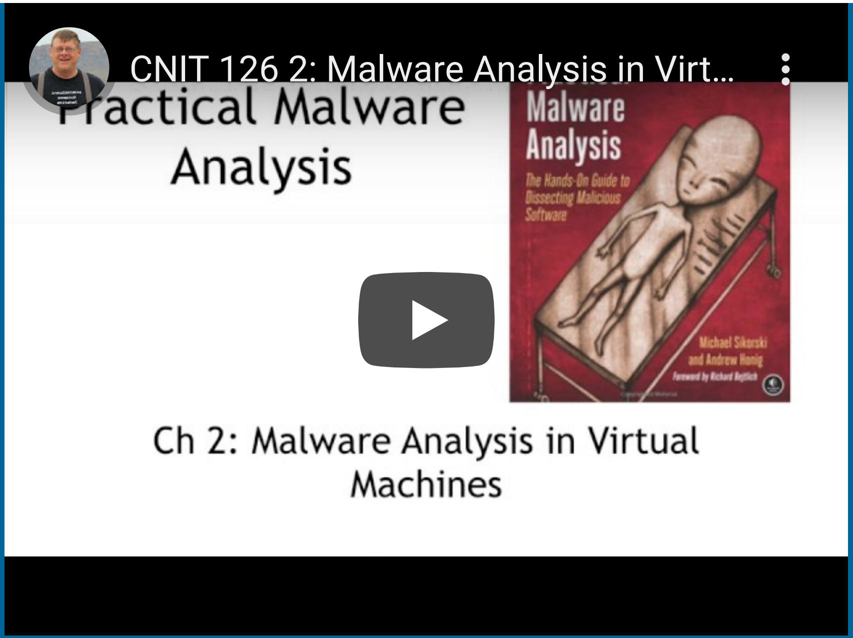
- Dissecting malware to understand
  - How it works
  - How to identify it
  - How to defeat or eliminate it
- A critical part of incident response



CNIT 126 0: Malware Analysis Primer...

Linked Libraries and Functions

Mon 1-30	**2: Malware Analysis in Virtual Machines & 3: Basic Dynamic Analysis**



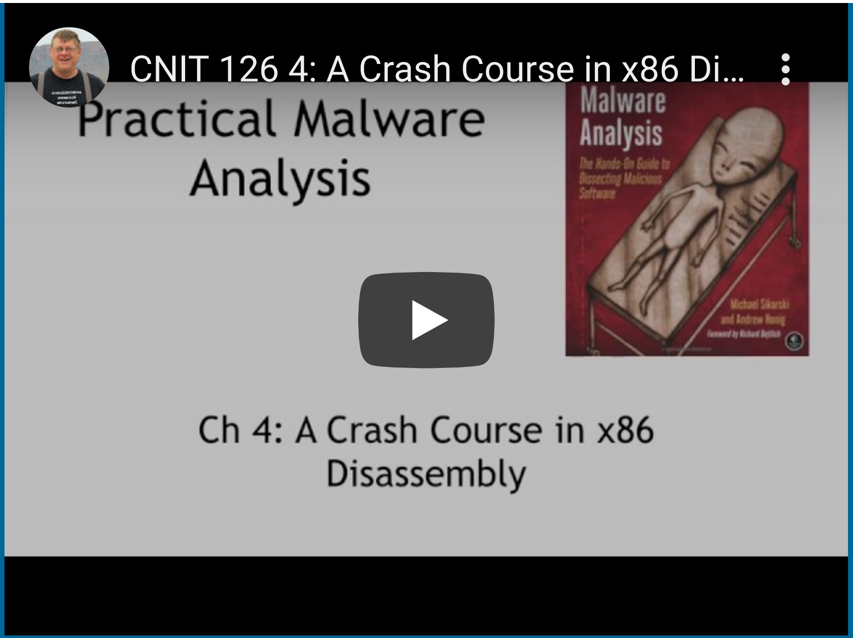
CNIT 126 2: Malware Analysis in Virt...

Practical Malware Analysis

Ch 2: Malware Analysis in Virtual Machines

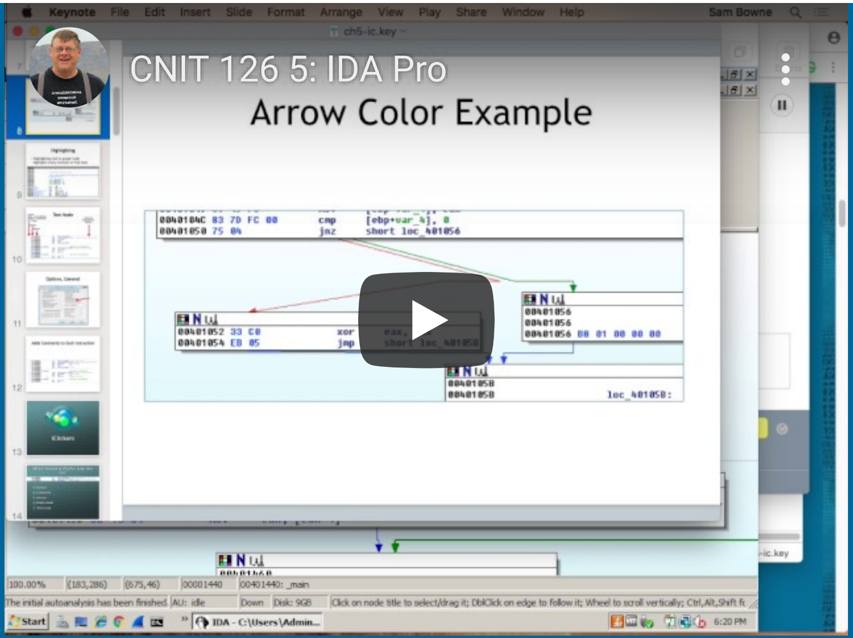
Malware Analysis
The Hands-On Guide to Dissecting Malicious Software
Michael Sikorski and Andrew Honig
Foreword by Richard Bejtlich

Fri 2-3	*Last Day to Add Classes*	
Mon 2-6	**Ch 0-1 Quiz due before class** **Ch 4 Quiz due before class** **Proj 1-2 due**	**4: A Crash Course in x86 Disassembly**



CNIT 126 4: A Crash Course in x86 Di...
Practical Malware Analysis
Malware Analysis
The Hands-On Guide to Dissecting Malicious Software
Michael Sikorski and Andrew Honig
Ch 4: A Crash Course in x86 Disassembly

Mon 2-13	**Ch 2-3 Quiz due before class** **Ch 5 Quiz due before class** **Proj 3 due**	**5: IDA Pro**



CNIT 126 5: IDA Pro

Arrow Color Example

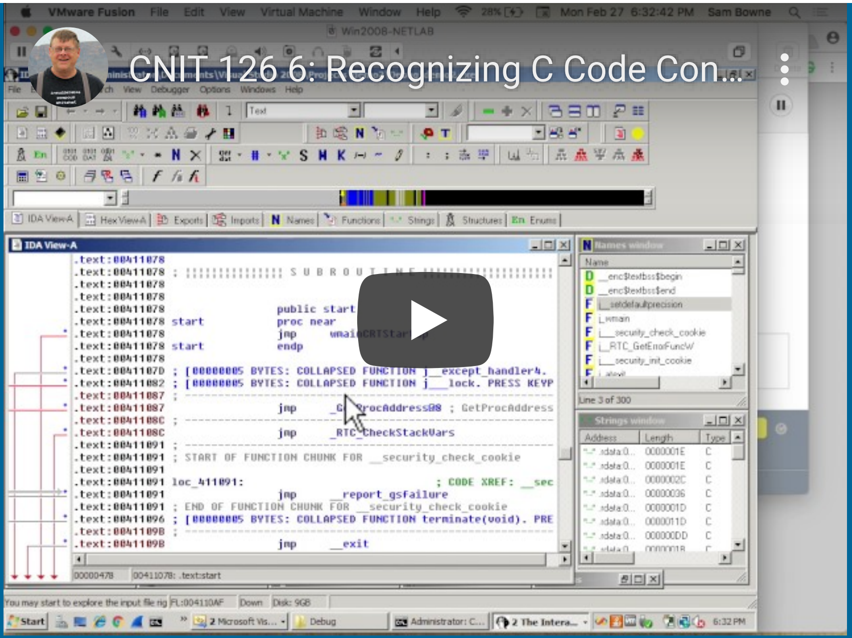
```
0040104C 83 7D FC 00        cmp     [ebp+var_4], 0
00401050 75 04              jnz     short loc_401056

00401052 33 C0              xor     eax,
00401054 EB 05              jmp     short loc_401058

00401056
00401056
00401056 B8 01 00 00 00

00401058
00401058                            loc_401058:
```

Keynote File Edit Insert Slide Format Arrange View Play Share Window Help
Sam Bowne
ch5-ic.key
Start
IDA - C:\Users\Admin...
6:20 PM

```
100.00%  (183,286)  (675,46)  00001440  00401440: _main
The initial autoanalysis has been finished.  AU: idle  Down  Disk: 9GB  Click on node title to select/drag it; DblClick on edge to follow it; Wheel to scroll vertically; Ctrl,Alt,Shift fc
```

Mon 2-20 *Holiday - No Class*

Mon 2-27	**Ch 6 Quiz recommended before class** **Proj 4-5 due**	**6: Recognizing C Code Constructs in Assembly**



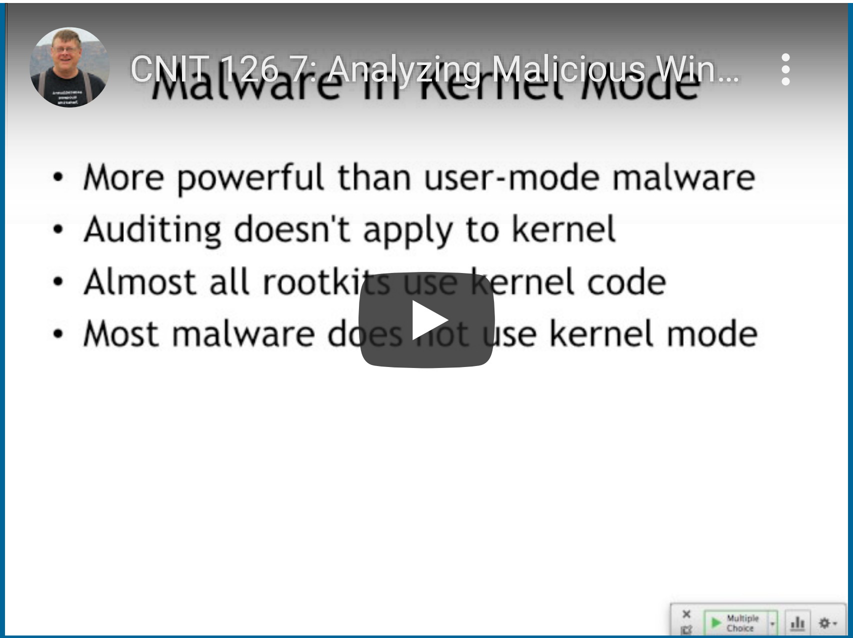
CNIT 126 6: Recognizing C Code Con...

```
.text:00411078
.text:00411078 ; !!!!!!!!!!!!!!! S U B R O U T I N E !!!!!!!!!!!!!!!!!!!!
.text:00411078
.text:00411078
.text:00411078                 public start
.text:00411078 start           proc near
.text:00411078                 jmp     wmainCRTStartup
.text:00411078 start           endp
.text:00411078
.text:0041107D ; [00000005 BYTES: COLLAPSED FUNCTION j__except_handler4.
.text:00411082 ; [00000005 BYTES: COLLAPSED FUNCTION j___lock. PRESS KEYP
.text:00411087 ; ---------------------------------------------------------
.text:00411087                 jmp     _GetProcAddress@8 ; GetProcAddress
.text:0041108C ; ---------------------------------------------------------
.text:0041108C                 jmp     _RTC_CheckStackVars
.text:00411091 ; ---------------------------------------------------------
.text:00411091 ; START OF FUNCTION CHUNK FOR __security_check_cookie
.text:00411091
.text:00411091 loc_411091:                             ; CODE XREF: __sec
.text:00411091                 jmp     __report_gsfailure
.text:00411091 ; END OF FUNCTION CHUNK FOR __security_check_cookie
.text:00411096 ; [00000005 BYTES: COLLAPSED FUNCTION terminate(void). PRE
.text:0041109B ; ---------------------------------------------------------
.text:0041109B                 jmp     __exit
```

Mon 3-6	**Ch 6 & 7 Quiz due before class** **Proj 6 due**	**7: Analyzing Malicious Windows Programs**

CNIT 126 7: Analyzing Malicious Win...

The Windows Registry

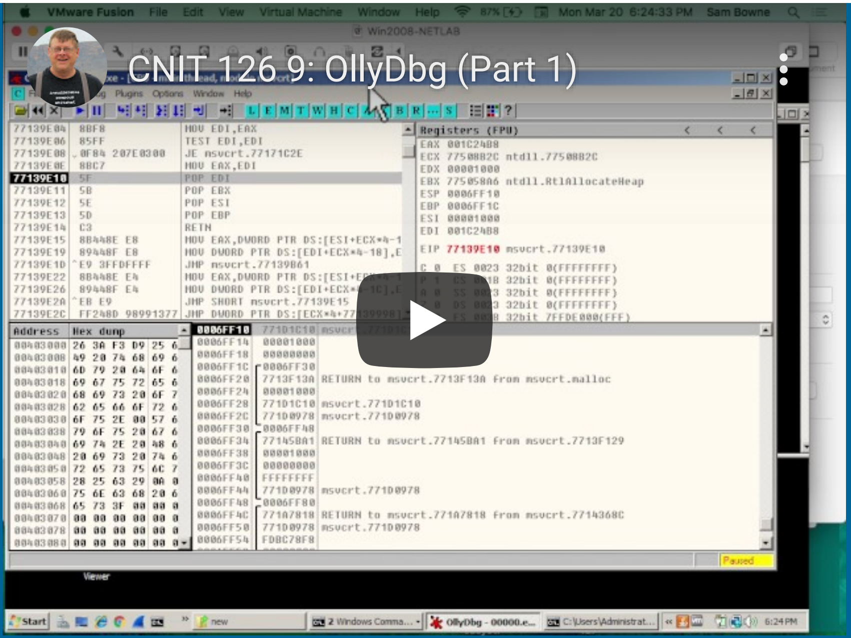

CNIT 126 7: Analyzing Malicious Win...

Malware in Kernel Mode

- More powerful than user-mode malware
- Auditing doesn't apply to kernel
- Almost all rootkits use kernel code
- Most malware does not use kernel mode

Mon 3-13	**Ch 8 Quiz due before class** **Proj 7-8 due**	**8: Debugging**

Mon 3-20	Ch 9 Quiz due before class Proj 9 due	9: OllyDbg



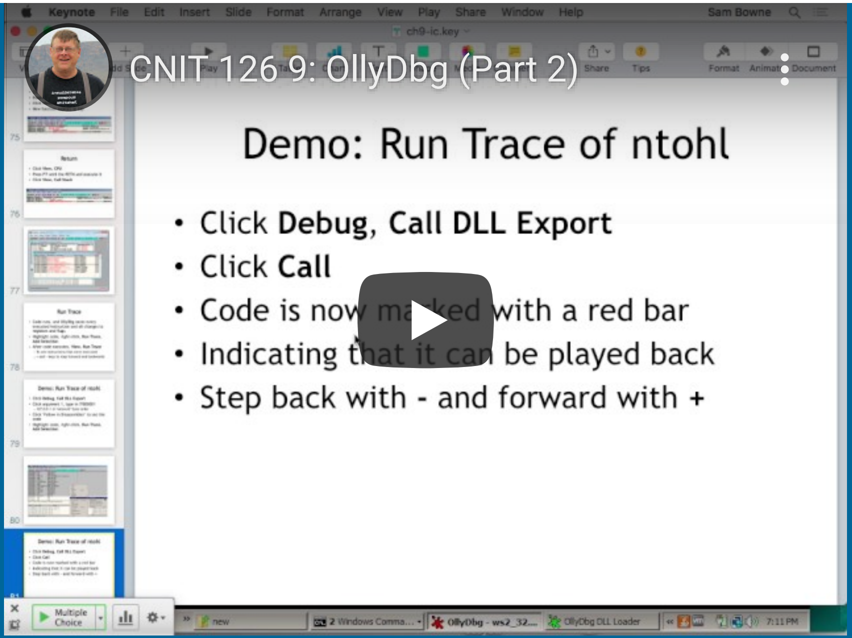
CNIT 126 9: OllyDbg (Part 1)

```
77139E04  8BF8           MOV EDI,EAX
77139E06  85FF           TEST EDI,EDI
77139E08 ,0F84 207E0300  JE msvcrt.77171C2E
77139E0E  8BC7           MOV EAX,EDI
77139E10  5F             POP EDI
77139E11  5B             POP EBX
77139E12  5E             POP ESI
77139E13  5D             POP EBP
77139E14  C3             RETN
77139E15  8B448E E8      MOV EAX,DWORD PTR DS:[ESI+ECX*4-1
77139E19  89448F E8      MOV DWORD PTR DS:[EDI+ECX*4-18],E
77139E1D ^E9 3FFDFFFF    JMP msvcrt.77139B61
77139E22  8B448E E4      MOV EAX,DWORD PTR DS:[ESI+E
77139E26  89448F E4      MOV DWORD PTR DS:[EDI+ECX*
77139E2A ^EB E9          JMP SHORT msvcrt.77139E15
77139E2C  FF248D 98991377 JMP DWORD PTR DS:[ECX*4+77
```

```
Registers (FPU)
EAX 001C24B8
ECX 7750882C ntdll.7750882C
EDX 00001000
EBX 775058A6 ntdll.RtlAllocateHeap
ESP 0006FF10
EBP 0006FF1C
ESI 00001000
EDI 001C24B8

EIP 77139E10 msvcrt.77139E10

C 0  ES 0023 32bit 0(FFFFFFFF)
P 1  CS 0018 32bit 0(FFFFFFFF)
A 0  SS 0023 32bit 0(FFFFFFFF)
Z 0  DS 0023 32bit 0(FFFFFFFF)
     FS 003B 32bit 7FFDE000(FFF)
```

```
Address   Hex dump
00403000  26 3A F3 D9 25 6
00403008  49 20 74 68 69 6
00403010  6D 79 20 64 6F 6
00403018  69 67 75 72 65 6
00403020  68 69 73 20 6F 7
00403028  62 65 66 6F 72 6
00403030  6F 75 2E 00 57 6
00403038  79 6F 75 20 67 6
00403040  69 74 2E 20 48 6
00403048  20 69 73 20 74 6
00403050  72 65 73 75 6C 7
00403058  28 25 63 29 0A 0
00403060  75 6E 63 68 20 6
00403068  65 73 3F 00 00 0
00403070  00 00 00 00 00 0
00403078  00 00 00 00 00 0
00403080  00 00 00 00 00 0
```

```
0006FF10  771D1C10  msvcrt.771D1C
0006FF14  00001000
0006FF18  00000000
0006FF1C  0006FF30
0006FF20  7713F13A  RETURN to msvcrt.7713F13A from msvcrt.malloc
0006FF24  00001000
0006FF28  771D1C10  msvcrt.771D1C10
0006FF2C  771D0978  msvcrt.771D0978
0006FF30  0006FF48
0006FF34  77145BA1  RETURN to msvcrt.77145BA1 from msvcrt.7713F129
0006FF38  00001000
0006FF3C  00000000
0006FF40  FFFFFFFF
0006FF44  771D0978  msvcrt.771D0978
0006FF48  0006FF80
0006FF4C  771A7818  RETURN to msvcrt.771A7818 from msvcrt.7714368C
0006FF50  771D0978  msvcrt.771D0978
0006FF54  FDBC78F8
```



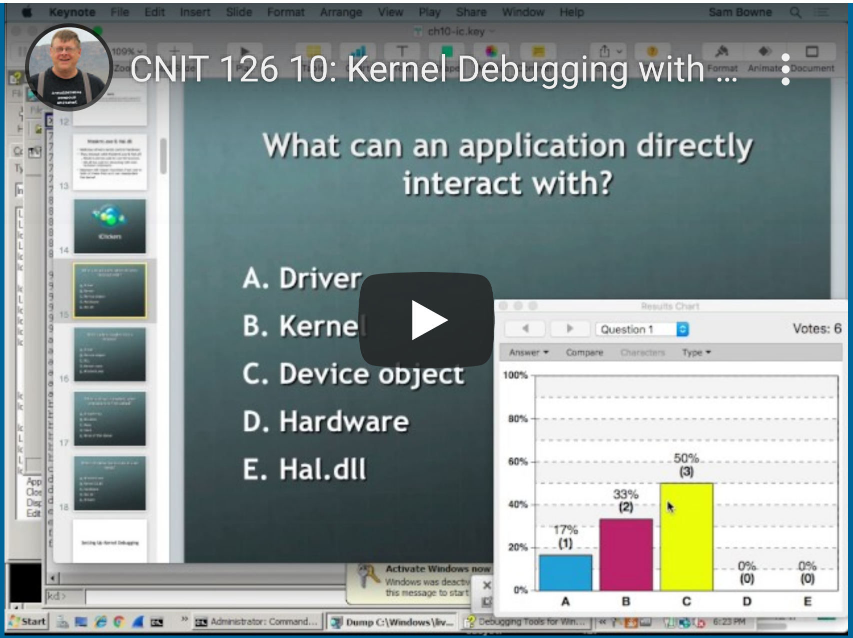
CNIT 126 9: OllyDbg (Part 2)

Demo: Run Trace of ntohl

- Click **Debug**, **Call DLL Export**
- Click **Call**
- Code is now marked with a red bar
- Indicating that it can be played back
- Step back with - and forward with +

Mon 3-27   *Holiday - No Class*

Mon 4-3	**Ch 10 Quiz due before class** **Proj 10-11 due**	**10: Kernel Debugging with WinDbg**

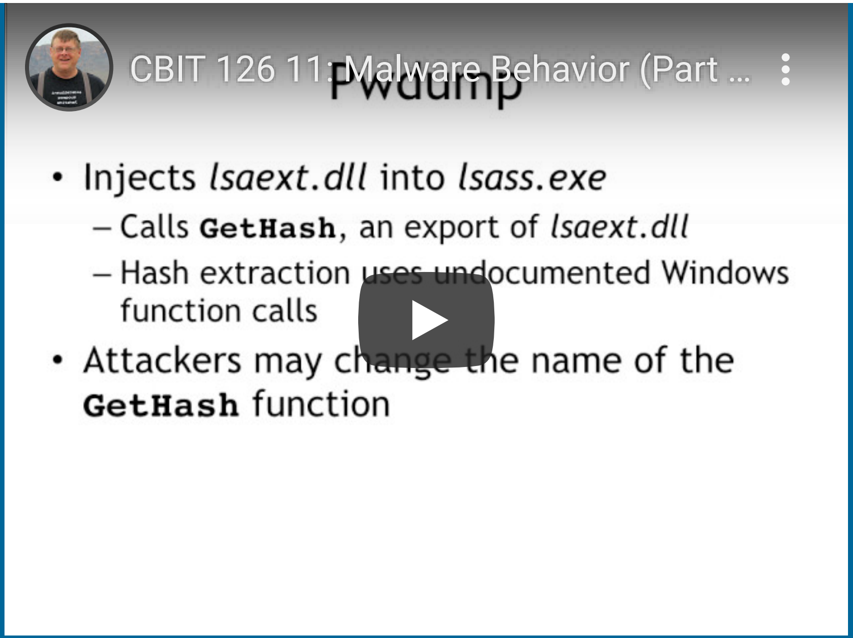


CNIT 126 10: Kernel Debugging with ...

What can an application directly interact with?

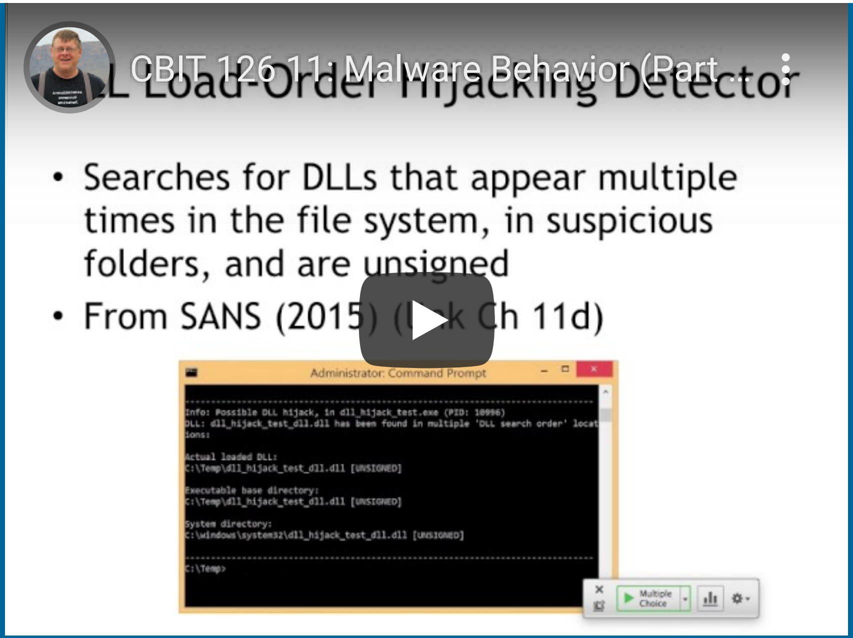
A. Driver
B. Kernel
C. Device object
D. Hardware
E. Hal.dll

Wed 4-6	*Mid-Term Grades Due*	
Mon 4-10	**Ch 11 Quiz due before class** **Proj 12 due**	**11: Malware Behavior**



Pwdump

- Injects *lsaext.dll* into *lsass.exe*
  - Calls **GetHash**, an export of *lsaext.dll*
  - Hash extraction uses undocumented Windows function calls
- Attackers may change the name of the **GetHash** function

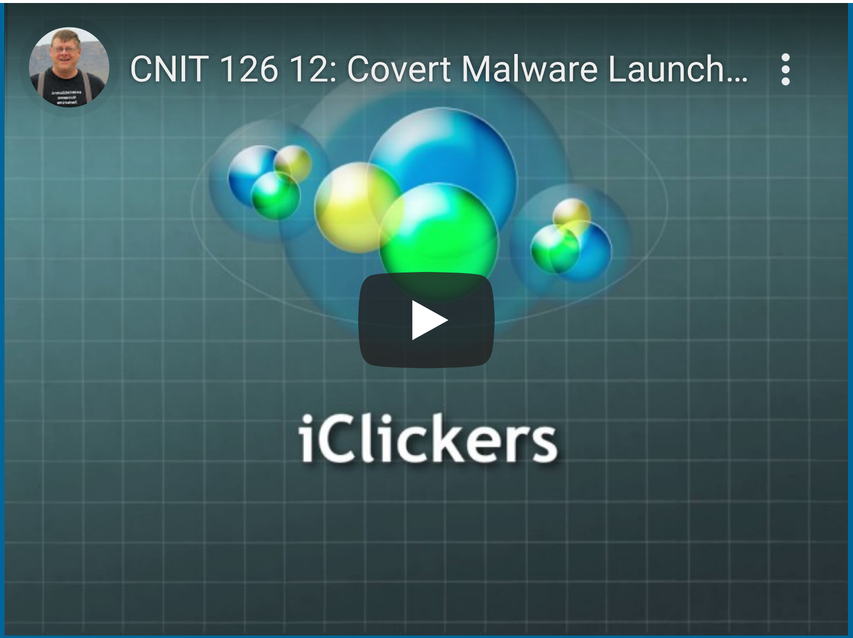

CBIT 126 11: Malware Behavior (Part ...
Administrator: Command Prompt
Multiple Choice

L Load-Order Hijacking Detector

- Searches for DLLs that appear multiple times in the file system, in suspicious folders, and are unsigned
- From SANS (2015) (Link Ch 11d)

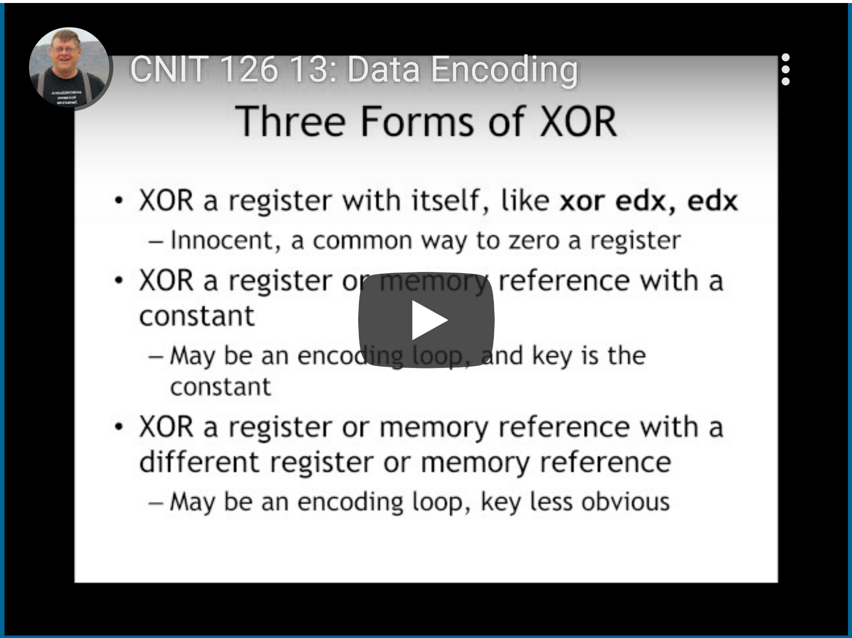
```
--------------------------------------------------------------------------------
Info: Possible DLL hijack, in dll_hijack_test.exe (PID: 10996)
DLL: dll_hijack_test_dll.dll has been found in multiple 'DLL search order' locat
ions:

Actual loaded DLL:
C:\Temp\dll_hijack_test_dll.dll [UNSIGNED]

Executable base directory:
C:\Temp\dll_hijack_test_dll.dll [UNSIGNED]

System directory:
C:\windows\system32\dll_hijack_test_dll.dll [UNSIGNED]

--------------------------------------------------------------------------------
C:\Temp>
```

Mon 4-17	**No Quiz** **No Proj due**	**Guest Speaker: Jason Nelson** **Desktop Support Technician at Child Mind Institute | Digital Advertising/Social Media consultant to lifestyle brands and non-profits**
Mon 4-24	**Ch 12 Quiz due before class** **Proj 13 & 14 due**	**12: Covert Malware Launching**



CNIT 126 12: Covert Malware Launch...

Mon 5-1	**No Quiz due Proj 15 due**	**Technical Sergeant Fernando Borrego Air National Guard Reserve NOTE: DIFFERENT TIME -- 6:30 PM**
Mon 5-8	***Class Cancelled for CyberSecureGov in Washington, DC***	
Mon 5-15	**Last Class · Ch 13 Quiz due before class Proj 16 due All extra credit Proj. due**	**13: Data Encoding**



Three Forms of XOR

- XOR a register with itself, like **xor edx, edx**
  - Innocent, a common way to zero a register
- XOR a register or memory reference with a constant
  - May be an encoding loop, and key is the constant
- XOR a register or memory reference with a different register or memory reference
  - May be an encoding loop, key less obvious

Mon 5-23 ***Final Exam***

Lecture Notes

Policy
Printable Schedule

Basic Analysis

0: Malware Analysis Primer & 1: Basic Static Techniques · KEY · PDF
2: Malware Analysis in Virtual Machines & 3: Basic Dynamic Analysis · KEY · PDF

Advanced Static Analysis

4: A Crash Course in x86 Disassembly · KEY · PDF
5: IDA Pro · KEY · PDF
6: Recognizing C Code Constructs in Assembly · KEY · PDF
7: Analyzing Malicious Windows Programs · KEY · PDF

Advanced Dynamic Analysis

8: Debugging · KEY · PDF
9: OllyDbg · KEY · PDF
10: Kernel Debugging with WinDbg · KEY · PDF

Malware Functionality

11: Malware Behavior KEY PDF
12: Covert Malware Launching KEY PDF
13: Data Encoding KEY PDF

Slides below this line are being updated

14: Malware-Focused Network Signatures KEY

Anti-Reverse-Engineering

15: Anti-Disassembly KEY
16: Anti-Debugging
17: Anti-Virtual Machine Techniques
18: Packers and Unpacking

Special Topics

19: Shellcode Analysis
20: C++ Analysis
21: 64-Bit Malware

Review Questions

Click a lecture name to see it on SlideShare.
If you want to use other formats, you may find this useful:
Cloud Convert.

Back to Top

Projects

Download Textbook Labs Here

Downloading the Virtual Machines

Download VMware Player

Proj 1: Basic Static Techniques (Lab 1-1) (25 pts.)
Proj 2: Basic Static Techniques (Lab 1-2) (20 pts.)
Proj 3: INetSim (20 pts.) (rev. 2-1-16)
Proj 4: Basic Dynamic Techniques (Lab 3-1) (30 pts.) (rev. 2-1-16)
Proj 5: Using Jasmin to run x86 Assembly Code (15 pts.)
Proj 6: IDA Pro (20 pts.) (rev. 2-22-16)
Proj 7: Compiling C on Windows 2008 Server (15 pts.) (rev. 2-27-17)
Proj 8: Disassembling C on Windows (15 pts. + 10 extra credit) (rev. 2-27-17)
Proj 9: Disassembling C on Windows Part 2 (15 pts. + 10 extra credit) (Modified 3-20-17)
Proj 10: Analyzing Malicious Windows Programs (Lab 7-1) (15 pts.) (rev. 3-14-16)
Proj 11: Using OllyDbg to Analyze Lab09-01.exe (rev. 3-21-16) (15 pts.)

Proj 12: Kernel Debugging with Livekd on Windows Server 2008 (20 pts.) (Updated 3-11-17)
Proj 13: Using Kernel Debugging Commands with WinDbg (15 pts.) (rev. 4-19-17)
Proj 14: Malware Behavior (Lab 11-1) (35 pts.) (updated 4-19-17)
Proj 15: Covert Malware Launching (Lab 12-1) (rev. 4-18-16) (25 pts.)
Proj 16: Data Encoding (Lab 13-1) (25 pts.) (rev. 4-24-17)

Extra Credit Projects

Proj 1x: File and Strings (10 pts. extra credit)
121-X11-files.zip (rev. 8-22-13)
Proj 2x: Using IDA Pro Free to Disassemble Executable Files (10 - 40 pts. extra credit)
crackme-121-1.exe crackme-121-2.exe crackme-121-3.exe crackme-121-4.exe
Proj 3x: Harvesting Files from Packet Captures with Wireshark (10 pts.)
pX12-121.pcap (1.2 MB)
Proj 4x: Introduction to Hopper (20 points) (rev. 2-22-16)
Proj 5x: Assembly Code Challenges (30 points) (rev. 2-9-16)
Proj 6x: Disassembling C on Windows Part 3 (15 pts. + 10 extra credit)
Proj 7x: Analyzing Malicious Windows Programs (Lab 7-2) (15 pts.)
Proj 8x: Using WinDbg on a Crash Dump (15 pts.)
Project 12x: Anti-Disassembly (Lab 15-1) (15 pts.)

Back to Top

Links

Lab Files

Download Textbook Labs Here

Chapter Links

Ch 1a: Breach clean-up cost LinkedIn nearly $1 million, another $2-3 million in upgrades (Aug. 2012)
Ch 1b: Fake FBI warning tricks man into surrendering himself for possession of child porn

Ch 2a: VirusTotal - Free Online Virus, Malware and URL Scanner
Ch 2b: UPX NotCompressibleException
Ch 2c: Peering Inside the PE: A Tour of the Win32 Portable Executable File Format
Ch 2d: Dependency Walker (depends.exe) Home Page
Ch 2e: PEview Download
Ch 2f: Resource Hacker
Ch 2g: Download PEiD 0.95
Ch 2h: UPX: the Ultimate Packer for eXecutables - Download Ch 2i: BinText 3.03 McAfee Free Tools

Ch 3a: Process Monitor Download
Ch 3b: Process Explorer Download
Ch 3c: RegShot download
Ch 3d: Regshot user guide
Ch 3e: ApateDNS Download
Ch 3f: 3 Free Tools to Fake DNS Responses for Malware Analysis

Ch 5a: OpenRCE -- Free IDA Scripts

Ch 6a: Entry points for Windows programs

Ch 7b: Autoruns for Windows
Ch 7c: Anatomy of a Program in Memory
Ch 7d: assembly - The point of test eax eax
Ch 7e: CurrentControlSetServices Subkey Entries
Ch 7f: Globally unique identifier - Wikipedia
Ch 7g: SEH in x86 Environments
Ch 7h: assembly - What is the 'FS''GS' register intended for?

Ch 7i: winapi - FS register in Win32
Ch 7j: Ring (computer security) - Wikipedia

Ch 8a: Exploit Development for Mere Mortals Joe McCray - YouTube
Ch 8b: x86 Protected Mode Exceptions
Ch 8c: Enabling Postmortem Debugging - Windows 10 hardware dev
Ch 8d: Using Windows Event Viewer to debug crashes
Ch 8e: LiveKd for Virtual Machine Debugging

Ch 9a: Download OllyDbg 1.10
Ch 9b: OllyDbg v. 2.01 is EVIL; just misses functions found in v. 1.10
Ch 9c: OLLYDBG TUTORIALS! The Legend Of Random
Ch 9d: OpenRCE OllyDbg Plugins (down on 10-14-13)
Ch 9e: shell-storm Shellcodes Database

Ch 10a: Download Windows Symbol Packages
Ch 10b: ntoskrnl.exe - Wikipedia, the free encyclopedia
Ch 10c: Choosing the 32-Bit or 64-Bit Debugging Tools (Windows Debuggers)
Ch 10d: How To: Debug the WRK on Mac OS X Using VMware Fusion
Ch 10e: Assembly Code Debugging in WinDbg (Windows Debuggers)
Ch 10f: Microsoft Windows library files - HAL runs in kernel mode
Ch 10g: Windbg Tutorials
Ch 10h: A word for WinDbg
Ch 10i: Kernel Patch Protection - Wikipedia
Ch 10j: On Windows Syscall Mechanism and Syscall Numbers Extraction Methods
Ch 10k: The Sysenter Instruction and 0x2e Interrupt
Ch 10l: Hooking the System Service Dispatch Table (SSDT)
Ch 10m: Common WinDbg Commands (Thematically Grouped)

Ch 11a: Portable Executable - Wikipedia
Ch 11b: Resource Hacker
Ch 11c: Capturing Windows 7 Credentials at Logon Using a Custom Credential Provider (Replaces MSGINA.DLL)
Ch 11d: Detecting DLL Hijacking on Windows | SANS Institute (2015)
Ch 11e: Windows 10 Hooking Nirvana explained (2016)

Ch 13a: Tools for Examining XOR Obfuscation for Malware Analysis
Ch 13b: Base64 Decode and Encode - Online
Ch 13c:: Download FindCrypt2 (IDA Pro Plug-In)

Ch 13d: Kanal Free Download
Ch 13e: Entropy (information theory) - Wikipedia
Ch 13f: IDA Entropy Plugin
Ch 13g: IDA Entropy Plugin 0.1 -- working download link
Ch 13h: Ent -- entropy visualizer that works on Windows

Ch 15a: The Bastard Linux Disassembler (Linear)
Ch 15b: JUMP and CALL - Stack Overflow

Training Materials

Introductory: Chapter 0

Introduction to Malware Analysis Slides by Lenny Zeltser
Introduction to Malware Analysis - Free Recorded Webcast by Lenny Zeltser
Analysis of Malware Samples -- EXCELLENT TIPS FOR PROCESS MONITOR
Sam's Honeynet "Reverse Engineering Malware" Class Notes (Mar. 2012)

Assembly Language: Chapter 4

Windows Assembly Language Megaprimer -- VIDEO
Introductory Intel x86: Architecture, Assembly --Free class materials!
PE Structure--Excellent Diagram
Download jasmin x86 Assembler Interpreter
Jasmin tutorial - Java Assembler Interpreter

Windows Internals: Chapter 7

Windows 0wn3d By Default Mark Baggett -- VIDEO

Debugging: Chapter 8

Exploit Development for Mere Mortals Joe McCray -- VIDEO OllyDbg Tricks for Exploit Development

OllyDbg: Chapter 9

Exploit Dev Night School Day 2 - YouTube -- HIGHLY RECOMMENDED, MORE DEBUGGER DEMOS
Reverse Engineering 101 on Vimeo

Other Links

Catalog of key Windows kernel data structures
Malware Analysis Resources
Pwning a Spammer's Keylogger - SpiderLabs Anterior
SANS Memory Forensics Cheat Sheet (PDF)
An interesting case of Mac OSX malware
Picking Apart Malware In The Cloud - The business need for malware analysis
FakeNet -- Dynamic malware analysis tool
Static Analysis Talk
Worm 2.0, or LilyJade in action
Pwning the Herpes bothet and it's creator
A technical analysis of Adobe Flash Player CVE-2012-0779 Vulnerability - Microsoft Malware Protection Center - Site Home - TechNet Blogs
Virtual USB Analyzer - Tutorial
PolyPack: An Automated Online Packing Service for Optimal Antivirus Evasion
FileInsight McAfee Free Tools
McAfee FileInsight -- recommended malware analysis tool
CSI:Internet - PDF timebomb
Static Analysis: Following Along at Home with Hopper's Decompiler Feature, Part 1
Deconstructing an ELF File
Malware Analysis Course Lecture Slides
Defeating Flame String Obfuscation with IDAPython
System Forensics: MBR Malware Analysis
Malware Hunting with the Sysinternals Tools
Honeypot Alert PHP-CGI Vuln Targeted For Database Dumping
Th3-0uTl4wS Database -- bot source code
Fuzzy Hashing presentation by Jesse Kornblum
Malware Unpacking Level: Pintool
WireShnork and other Forensics plugins for Wireshark
IntroductionToReverseEngineering
Tweaking Metasploit Modules To Bypass EMET -- Part 1
corkami - reverse engineering experiments and documentations
Modifying VirtualBox settings for malware analysis
What was that Wiper thing? - EXCELLENT MALWARE ANALYSIS

Malware Must Die!: Racing with time to get the latest payload of Blackhole Exploit Kit
Extracting EXE file (in HTTP stream) from captured packets file with Wireshark
Analyzing Unknown Malware: #2 Disclosure of an interesting Botnet - The Executable (Part 1)
Malware Analysis as a Hobby slides --Cuckoo looks great!
Shamoon The Wiper: further details (Part II) - Securelist
Backdoors are Forever: Hacking Team and the Targeting of Dissent
The Case of the Unexplained FTP Connections
Analysis of malware that infects virtual machines
Deobfuscating "PluginDetect"
To Russia With Targeted Attack
Windows DLL Injection Basics
Reverse engineering challenge intended for women
India APT Attack -- Several useful tools demonstrated
MFT vs Super Timeline: Part 1
Stack Smashing On A Modern Linux System -- Good gdb examples
Nothink.org -- EXCELLENT HONEYPOT DATA
Oh, you found a remote OpenSSH 0-day on Pastebin? Don't trust it.
KernelMode.info -- Site to get real malware samples
MalwareURL -- Site to get real malware samples
Malc0de Database -- Site to get real malware samples
PEiD 0.95 Free - Detects packers, cryptors and compilers
QUnpack -- recommended unpacker
ThreatExpert - Automated Threat Analysis
TCPView for Windows -- traffic monitoring
Total Uninstall Analyze, monitor and uninstall programs -- useful for malware analysis
Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code -- recommended book
Volatility Cheat Sheet
Good analysis of the malware at speedtest.net
Free Online Malware Analysis Class
APT #TargetedAttacks within Twitter
How to use MANDIANT Memoryze
contagio: Collection of Pcap files from malware analysis
Malware analysis lab tools
6.25 DNS DDOS Attack In Korea -- Good example of simple dynamic analysis
Mandiant Redline is Free
Windows 8 Server 2012 Memory Forensics
Structured Exception Handler EXPLOITATION

Malware and DLLs
Trojaning antivirus uninstallers with DLL injection
When Malware Meets Rootkits (from 2005)
Process Hiding
Dr. Fu's Security Blog: Malware Analysis Tutorials: a Reverse Engineering Approach -- MORE PROJECTS HERE
Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code -- RECOMMENDED BOOK
SANS Work Study -- Get SANS classes for cheap!
Finding Evil: Automating Autoruns Analysis
Attackers' Toolbox Makes Malware Detection More Difficult
Large botnet cause of recent Tor network overload
Pushdo Botnet detects "FakeNet" analysis tool and spams practicalmalwareanalysis.com (Sept, 2013)
Reverse Engineering a D-Link Backdoor with IDA Pro
Anatomy of an exploit -- inside the CVE-2013-3893 Internet Explorer zero-day -- Part 1
binwalk - Firmware Analysis Tool
Reverse Engineering Videos
How to solve Windows system crashes in minutes --Debugging crash dumps
Kernel Pool Exploitation on Windows 7 (from 2011)
Analysis of a Malware ROP Chain
New Tool: XORStrings
Strings from CSRSS show command-line history on Windows
Reconstructing Master File Table (MFT) Entries with MFTParser.py
The OpenIOC Framework -- for sharing threat intelligence
security-onion - recommended for Snort GUIs
Malware Research -- samples
Barracuda Launches Web-Based Malware Analysis Tool Threatglass
Malware Analysis with pedump
Practical Malware Analysis - Free Download eBook - pdf (works as of 2014-07-16)
What is a mutex? - EPIC EXPLANATION
OfficeMalScanner -- detects malware in Office files
Hopper -- Mac OS X Disassembler, highly recommended by @iamevltwin
fseventer for Mac -- observe filesystem changes
logkext - Freeware keylogger for OS X
contagio: OSX malware and exploit collection (~100 files)
Shellter -- inject Metasploit payloads into PE files to bypass AV
Exeinfo PE Download
How to setup plugins for ollydbg 2.x.x?
Download OllyScript to Automate Packing

Download OllyScript PE Compact Script

QuickUnpack Tool -- Download

Ether: Malware Analysis via Hardware Virtualization Exsensions -- Free online unpacker

MacMemoryForensics - volatility - Instructions on how access and use the Mac OS X support

PEStudio performs the static investigation of Windows executables

Valgrind Tutorial

PEStudio: static malware analysis tool ty @lennyzeltser #S4con

Process Hacker can dump strings from running processes ty @lennyzeltser #S4con

Google mutant names to help identify malware ty @lennyzeltser #S4con

Malware Analysis Database -- search for mutex values & more ty @lennyzeltser #S4con

ProcDOT - Visual Malware Analysis ty @lennyzeltser #S4con

urlvoid.com Website Reputation Checker Tool ty @lennyzeltser #S4con

Exeinfo PE -- Identifies packers ty @lennyzeltser #S4con

Hacker Disassembly Uncovered (free download)

Reversing & Malware Analysis - FREE TRAINING SLIDES

The evolution of OS X malware (Oct. 2014)

Bypassing EMET's EAF with custom shellcode using kernel pointer (from 2011)

Disarming Enhanced Mitigation Experience Toolkit (EMET) v 5.0

Cuckoo Sandbox VM Escape Vulnerability (2014)

Rootkits by Csaba Barta (from 2009)

Malwr - Malware Analysis by Cuckoo Sandbox

Malware Investigator -- from the FBI

Reversing a malvertisment: javascript, regex, and cookie

POWELIKS Levels Up With New Autostart Mechanism

Malicious Flash Files Gain the Upper Hand With New Obfuscation Techniques Security Intelligence Blog

Inside a Kippo honeypot: how the billgates botnet spreads -- PROJECT IDEA

Hook Analyser

Online JavaScript beautifier -- deobfuscates code! -- IMPORTANT FOR MALWARE ANALYSIS

Retrieve the apk signature at runtime for Android

2015-10-07: IOS Application Security Testing Cheat Sheet - OWASP

theZoo · Malware Samples to Analyze ty @the_fire_dog

Malware Researcher\'s Handbook (Demystifying PE File) - InfoSec Resources

RPISEC/Malware: Course materials for Malware Analysis

Malware Analysis by Abstruse Goose

A Crash Course In DLL Hijacking -- EXCELLENT EXPLANATION

x64dbg: An open-source x64/x32 debugger for windows -- ALTERNATIVE TO IDA PRO

REMNUX V6 FOR MALWARE ANALYSIS (PART 2): STATIC FILE ANALYSIS

Microsoft security technology EMET used to disable itself (Feb. 2016)
The Ultimate Disassembly Framework -- Capstone
Malwarebytes 2.2.0.1024 DLL Hijacking (works on Win 2008 Server but not Win 10) -- SHOW TO CLASS
Win32 Assembly Cheat Sheet
Local Kernel-Mode Debugging - Windows 10 hardware dev
WinDbg tools and tutorials
pestudio: Malware Initial Assessment Tool
Identifying malware with PEStudio
A fundamental introduction to x86 assembly programming
Practical Malware Analysis Starter Kit
Introductory Intel x86: Architecture, Assembly, Applications - YouTube
Assembly Primer for Hackers (Part 1) System Organization Tutorial.mp4 - YouTube
Automatically Extracting Obfuscated Strings from Malware using the FireEye Labs Obfuscated String Solver (FLOSS)
GitHub - RPISEC/Malware: Course materials for Malware Analysis by RPISEC
Manalyzer: free online static analysis
WARNING: Tweet to download live Locky malware (BE CAREFUL)
Kwetza: infecting android applications -- MAKE INTO PROJECT
pwning bin2json | psych0tik
Microsoft/binskim: A binary static analysis tool that provides security and correctness results for Windows portable executables.
GitHub - GoSecure/malboxes: Builds malware analysis Windows VMs so that you don't have to.
pev - the PE file analysis toolkit -- MAY BE USEFUL FOR PROJECTS
pev Video Demo
Plasma is an interactive disassembler for x86/ARM/MIPS. It can generates indented pseudo-code with colored syntax. -- TRY FOR PROJECTS
CS7038-Malware-Analysis by ckane
Reverse Engineering Malware 101 -- free online course

New Unsorted Links

My first SSDT hook driver
SSDT Hooking mini-library/example - RaGEZONE - MMO development community
Shadow SSDT Hooking with Windbg
Download Windows Driver Kit Version 7.1.0 from Official Microsoft Download Center
InstDrv plug-in - NSIS
Installing the AWS Command Line Interface
HowTo Export a VM in OVA format in VMware Fusion for OS X with ovftool
FLARE VM: The Windows Malware Analysis Distribution You've Always Needed!
pestudio -- USEFUL FOR MALWARE ANALYSIS

Dropper Analysis -- TEST FOR PROJECT

GUnpacker 0.5 | Generic Unpacker for RE of Malware

wsunpacker -- unpacks many formats

Ether: Online Malware Unpacker

Portable Executable File Corruption Preventing Malware From Running -- USE FOR PROJECTS

fireeye/flare-floss: FireEye Labs Obfuscated String Solver - Automatically extract obfuscated strings from malware.

Practical Malware Analysis Chapter 1 Lab Attempt - YouTube

Kernel Forensics and Rootkits

pestudio: Malware Initial Assessment Tool

Malware Analysis Tutorials: a Reverse Engineering Approach

Reversing Basics - A Practical Approach Using IDA Pro

Ch 8f: LiveKd for Virtual Machine Debugging -- Mark's Blog

ScyllaHide: conceals debuggers from malware

Process Doppelganging Malware Evasion Technique (from 2017) ty @lennyzeltser #IRespondCon

Processhacker: Monitor system resources, debug software and detect malware --ty @lennyzeltser #IRespondCon

Invoke-DOSfuscation: Cmd.exe Command Obfuscation Tool -- ty @lennyzeltser #IRespondCon

olevba -- Extracts VBA Macros from Microsoft Office files -- ty @lennyzeltser #IRespondCon

Malware-Traffic-Analysis.net A source for pcap files and malware samples ty Andrea Kaiser #IRespondCon

MalShare: A free Malware repository providing researchers access to samples, malicous feeds, and Yara results

VirusShare.com - Because Sharing is Caring

Detect It Easy -- Unpacker for Windows malware

CFF Explorer -- Malware Analysis Tool

pestudio -- malware analysis tool

Game Hacking: WinXP Minesweeper - Reverse Engineering

Automated Malware Analysis - Joe Sandbox

Ch 10n: About Dynamic-Link Libraries | Microsoft Docs

Ch 10n: Callback Objects | Microsoft Docs

Ch 10o: Using a Driver-Defined Callback Object | Microsoft Docs

Exeinfo PE by A.S.L - packer - compression detector and data detector

GitHub - horsicq/Detect-It-Easy: Detect it Easy

The Mac Malware of 2018--WITH SAMPLES

OALabs Malware Analysis Virtual Machine

Intro to Cutter for Malware Analysis

Three Heads are Better Than One: Mastering Ghidra

Top 10 Free Keyloggers for Windows

EgeBalci/Keylogger: Simple C Keylogger...

Understanding and Analyzing Carrier Files Workshop

Modern Windows Exploit Development.pdf

Back to Top

Last Updated: 5-16-17 7:05 am