USC Viterbi
School of Engineering

Course ID and Title: ITP 443 – Malware Analysis and Reverse Engineering
Units: 4
Spring 2025: Tuesdays 6-9:50 PM

Location: OHE 542

Instructor: Sean Straw
Office: None
Office Hours: By appointment
Contact Info: straw at usc domain

IT Help: Viterbi Information Technology
Hours of Service: Monday-Friday 8 AM – 9 PM
Contact Info: Phone: 213-740-0517; Email: engrhelp@usc.edu

Catalogue Description
Reverse engineering concepts for Windows malware analysis. Windows APIs, debuggers and decompilers; static and dynamic analysis methods of malicious scripts and binaries.

Course Description
This course is designed to give students a basic understanding of malware analysis and reverse engineering with a focus on Windows-based malware. Students will be exposed to the capabilities of malware and different methods of assessing and understanding its functionality. By the conclusion of the course, students should be able to receive an unknown malware sample and produce technical details (such as atomic indicators of compromise) and analysis in support of incident response, digital forensics, threat intelligence, or security operation center efforts. Students should also begin to develop techniques for researching and understanding techniques they have not seen previously within malware.

Learning Objectives
By the end of this course, students will be able to:
- Set up and use a virtual malware analysis environment;
- Dynamically and statically triage common malware, such as malicious documents;
- Understand basic assembly and compiled code;
- Explain common malware persistence techniques;
- Unpack malware using common packing methods;
- Create detections using YARA;
- Read, understand, and action a sandbox malware analysis report; and
- Summarize findings for other stakeholders.

Prerequisite(s): ITP-325 and ITP-375 (one or both of these prerequisites may be waived with instructor approval).
Recommended Preparation: The course is highly technical and relies on many different aspects of the inner workings of the modern Windows operating system.

Students unfamiliar with programming and programming concepts would benefit from familiarizing themselves with a programming language prior to the course. Experience with a C-style language such as

ITP-165 *Introduction to C++ Programming* is preferred, but experience with other languages such as Python on the level of ITP-115 *Programming in Python* will also provide this background.

Course Notes

Course is letter graded, with materials provided by the USC Learning Platform.

The course is focused on providing students with hands-on experience. The general class format will have students complete prepared reading prior to each section. Class time will be spent on a brief recap of the reading materials, followed by lab time including demonstrations of the assigned lab. Students will then have the remainder of class time to work through the assigned lab.

In all cases, more specific directions supersede broader course policies. For example, though use of outside analysis material (if sourced properly) is permitted, any assignments which specifically exclude their use preclude this permission.

Technological Proficiency and Hardware/Software Required

It is assumed that the student has baseline technical knowledge (basic computer usage, basic internet usage) and foundational cybersecurity concepts (see ITP 125). Malware analysis will be based on Intel architecture, and so students will benefit from having access to an Intel-based system to conduct analysis on. **Newer Apple laptops with M1/M2/M3 processors will not fit this requirement,** but the lab systems will be made available to students as much as possible. Students may be able to complete the assignments on Apple laptops with M1/M2/M3 processors, but this is not supported as part of the course at this time.

Required Readings and Supplementary Materials

Practical Malware Analysis by Michael Sikorski and Andrew Honig

ISBN: 1593272901

Year: 2012

Additional material listed in the assigned week.

Optional Readings and Supplementary Materials

Listed in the assigned week.

Description of Assignments and How They Will Be Assessed

Lab assignments will be provided each week and describe a list of analytical questions and steps to analyze a provided sample. Most of these assignments will analyze the same sample. Often the answers to the assignment will be provided in class as part of the demonstrations. The assignments will be graded on the thoroughness of the explanation of the analysis.

Malware analysis and reverse engineering requires constant discovery of new concepts, so students are expected to research, experiment, and learn proactively.

Final Project

The culmination of the course is a final project analyzing the sample primarily used for most lab work. To complete the final project, you will write a report, typically at least 10-15 pages, in a style of your choosing that describes the process of analyzing the sample and conclusions drawn from the analysis. Throughout the course, students will be exposed to example malware writeups as reference points.

The emphasis for the final project is a report that demonstrates knowledge of a variety of approaches for triaging and analyzing Windows malware. The report should allow other malware analysts to understand the steps the student took and for new analysts to reproduce the results. A report will likely contain the follow sections:

- An executive summary of the analysis and findings.

- A description of initial triage methods to identify and unpack packed files.
- A comparison of the initial triage on the newly unpacked file and how the results differ.
- A demonstration of dynamic analysis techniques to identify malware behavior.
- Examination of the malware's encryption mechanisms using a debugger and disassembler.

Timeline: The lab assignments analyzing the sample will represent components of the topics your final project should address. Each lab assignment submission involving the sample (which will be described as such when provided) can be drafted as a subsection of the final report.

The final two weeks will be set aside to finish compiling the existing subsections and rewriting any portions that require it.

Grading: The final project will account for 20% of the grade. The individual components submitted as lab assignments are graded separately as part of the Lab Assignments portion of the grade.

The following rubric will be used for the evaluation of the final project

Metric	**Evaluates**	**Points**
Breadth of analysis	Coverage of topics discussed throughout the semester. A complete project should cover the analysis of each week using the sample from the semester	8
Details of analysis	Accuracy and description of the analysis steps taken	8
Style and formatting	Persuasiveness, function, grammar, and phrasing of the writeup	4
Total		20

Participation

Malware analysis, like many forms of analysis and investigation, is only useful if someone else can be informed by the results. To that end, students are expected to participate in class by asking and answering questions to increase their comfort with communicating about malware topics.

To fulfill participation, every student will be expected to ask or answer at least one question during each class. If a student anticipates not needing to ask questions for a section, they will have an opportunity at the start of each class to comment briefly on a concept from the reading they enjoyed, considered, or otherwise thought about.

Grading Breakdown

Assessment Tool (assignments)	**% of Grade**
Participation	10
Lab Assignments	55
Quizzes (2)	15
Final Project	20
TOTAL	100

Assignment Submission Policy

The labs will be posted on Brightspace under the "Assignments" or "Labs" section. Each lab will include instructions, a due date, and a link for electronic submission. Labs must be submitted using this link. Do not email your assignments to the instructor, lab assistants, or graders.

Assignments are (typically) due the week following the assignment. Assignments turned in up to 24 hours late will have 25% of the total points deducted from the graded score. Assignments turned in between 24 and 48 hours late will have 50% of the total points deducted from the graded score. After two days, submissions will not be accepted, and students will receive no credit for the assignment barring an exception granted by the professor.

Any exceptions or alternate plans should be documented via e-mail. Even if alternative accommodations are discussed in person, you must follow up via email to confirm.

Should you need an extension for an assignment, please reach out proactively as soon as possible. The sooner issues are raised, the more flexibility available.

Course-Specific Policies

Students are expected to be engaged participants in lectures and demonstrations. Because of the expectation of participation, students are also expected to be supportive of other students and refrain from dismissive comments or other behavior that discourages other students or themselves from participating. Malware analysis can require lots of trial and error, and so students must be able to freely try things that may be wrong.

Attendance

This course is designed to provide the most value through live demonstrations. Consequently, attendance is necessary and expected to get the most out of the course.

Academic Integrity

Unless otherwise noted, this course will follow the expectations for academic integrity as stated in the USC Student Handbook. The general USC guidelines on Academic Integrity and Course Content Distribution are provided in the subsequent "Statement on Academic Conduct and Support Systems" section.

For this class, all students are expected to submit assignments that are original work and prepared specifically for the course/section in this academic term. You may not submit work written by others or "recycle" work prepared for other courses without obtaining written permission from the instructor(s). Students suspected of engaging in academic misconduct will be reported to the Office of Academic Integrity.

Other violations of academic misconduct include, but are not limited to, cheating, plagiarism, fabrication (e.g., falsifying data), knowingly assisting others in acts of academic dishonesty, and any act that gains or is intended to gain an unfair academic advantage.

The impact of academic dishonesty is far-reaching and is considered a serious offense against the university and could result in outcomes such as failure on the assignment, failure in the course, suspension, or even expulsion from the university.

For more information about academic integrity see the student handbook or the Office of Academic Integrity's website, and university policies on Research and Scholarship Misconduct.

Please ask me if you are unsure about what constitutes unauthorized assistance on an exam or assignment, or what information requires citation and/or attribution. In this class, you are expected to submit work that

demonstrates your individual mastery of the course concepts. Unless specifically designated as a 'group project,' all assignments are expected to be completed individually.

In the course of their analysis, student may find existing writeups or descriptions of the samples they are working with. Referencing these materials and even answering questions using the results is fine, but students must not pass off the analysis as their own. When answering questions with material found in existing analysis, students must explain where the conclusion originates from and the source. Lifted material should be quoted.

If found responsible for an academic violation, students may be assigned university outcomes, such as suspension or expulsion from the university, and grade penalties, such as an "F" grade on the assignment, exam, and/or in the course.

Please ask the instructor if you are unsure about what constitutes unauthorized assistance on an exam or assignment, or what information requires citation and/or attribution.

You may not record this class without the express permission of the instructor and all other students in the class. Distribution of any notes, recordings, exams, or other materials from a university class or lectures — other than for individual or class group study — is prohibited without the express permission of the instructor.

Use of Generative AI in this Course

Generative AI permitted but limited as follows: In this course, you are permitted to use artificial intelligence (AI)-powered programs to help you when completing assignments or readings. However:

- You should also be aware that AI text generation tools may present incorrect information, biased responses, and incomplete analyses; thus, their answers may not meet the standards of this course.
- To adhere to our university values, *you must cite any AI-generated material (e.g., text, images, and other content) included or referenced in your work and provide the prompts used to generate the content*. Using an AI tool to generate content without proper attribution will be treated as plagiarism and reported to the Office of Academic Integrity.

Please review the instructions in each assignment for more details on how and when to use AI Generators for your submissions.

Course Evaluations

Course evaluations will be conducted during the last class of the semester. In addition, the instructor will lead an informal mid-semester check in immediately following the first quiz.

Course Schedule

Below is the current projected course schedule. This will be updated as the class progresses. Each week, an announcement will be made confirming or correcting the assigned material for the coming weeks.

	Topics/Daily Activities	Readings/Preparation	Assignment
Week 1	- Class logistics - Goals of malware analysis - Setting up a lab environment	**Practical Malware Analysis** - Chapter 0, Malware Analysis Primer - Chapter 2, Malware Analysis in Virtual Machines	**Lab 1 – Setting Up a Lab Environment**, for week 2. No submission necessary
Week 2	- Windows process fundamentals - Dynamic malware triage	**Processes and Threads** About Processes and Threads **Practical Malware Analysis** - Chapter 1, Basic Static Techniques, page 14, "Portable Executable File Format" to page 18, "Static Analysis in Practice" (non-inclusive) - Chapter 3, Basic Dynamic Analysis - Chapter 7, Analyzing Malicious Windows Programs	**Lab 2 – Basic Malware Triage**
Week 3	Programming concepts and PowerShell Deobfuscation	- Basic Programming Concepts - Simple Data Structures - Objects and Classes - Chapter 8, Debugging, up to "Software Execution Breakpoints" (non-inclusive). Do your best with the assembly but do not fret about it - Using PowerShell ISE to debug - Malicious PowerShell Analysis - (Optional, Funny) wat	**Lab 3 – Debugging and Basic PowerShell Deobfuscation**
Week 4	Assembly and x64dbg	- **PMA** – Chapter 4, A Crash Course in Disassembly - How to use x64dbg - **PMA** – Chapter 21, 64-bit malware (8 pages) - **PMA** – Chapter 6, Recognizing C Constructs in Assembly – Begin - BRBBot analysis	**Lab 4 – Debugging x86/x64 Binaries**
Week 5	Assembly and Ghidra	- Introduction to Ghidra	**Lab 5 – Introduction to Ghidra**

		- Review Chapter 4 - Review Chapter 6	
Week 6	Continued Assembly Analysis and Encoding	- **PMA** – Chapter 13, Data Encoding - Chapter 4, A Crash Course in x86 Disassembly	**Lab 6 – Continued x64 Analysis**
Week 7	Quiz; Stakeholder communication	Review for quiz	None
Week 8	Shellcode analysis	- **PMA** – Chapter 11, ignore or skim the GINA interception - **PMA** – Chapter 19 - Shellcode loader - Encouraged, but optional	**Lab 7 – Shellcode Analysis**
Week 9	Packed malware	- Chapter 18, Packers and Unpacking - Intro up to "Manual Unpacking" (5 pages) - Manual unpacking up to "Let's walk through a simple manual unpacking process" (3 paragraphs) - "Tips and Tricks for Common Packers" - read UPX and Themida (1 page) - "Analyzing without Fully Unpacking" to end (1.5 pages) Choose one (or more!) of the following: - Extracting Embedded Payloads - Cherryloader analysis - Lets Unpack Dridex	**Lab 8 – Triaging Packed Malware**
Week 10	Automated Malware Analysis	- Analysis of DARKGATE - (Optional) Brute forcing DARKGATE Encodings	**Lab 9 – Reviewing Automated Sandbox Reports**
Week 11	Malware Detection	- Intro to YARA Rules - YARA Docs reference – DO NOT read the whole document - YARA Goodware rules - SIGMA Intro - (Optional) SIGMA intro - True/False Classification Matrix - (Optional, but recommended) Lockheed Martin Killchain Whitepaper	**Lab 10 – Writing YARA Rules**

Week 12	Quiz	Prepare for quiz	**Final Project**
Week 13	JavaScript Debugging	Debugging Chrome Analyzing MageCart MallRats: An Analysis of the Natural Fresh Mall Magecart Attack	Work on final project
Week 14	Anti-Analysis techniques; course wrap-up	**Practical Malware Analysis** - Chapter 16, Anti-Debugging - Chapter 17, Anti-Virtual Machine Techniques	Work on final project
Week 15	**Guest Lecture**	**TBA**	
Finals	**Final project due**	**Submit final project**	**Due according to the final exam schedule on the Schedule of Classes https://classes.usc.edu/**

Statement on Academic Conduct and Support Systems

Academic Integrity:
The University of Southern California is a learning community committed to developing successful scholars and researchers dedicated to the pursuit of knowledge and the dissemination of ideas. Academic misconduct, which includes any act of dishonesty in the production or submission of academic work, comprises the integrity of the person who commits the act and can impugn the perceived integrity of the entire university community. It stands in opposition to the university's mission to research, educate, and contribute productively to our community and the world.

All students are expected to submit assignments that represent their own original work, and that have been prepared specifically for the course or section for which they have been submitted. You may not submit work written by others or "recycle" work prepared for other courses without obtaining written permission from the instructor(s).

Other violations of academic integrity include, but are not limited to, cheating, plagiarism, fabrication (e.g., falsifying data), collusion, knowingly assisting others in acts of academic dishonesty, and any act that gains or is intended to gain an unfair academic advantage.

The impact of academic dishonesty is far-reaching and is considered a serious offense against the university. All incidences of academic misconduct will be reported to the Office of Academic Integrity and could result in outcomes such as failure on the assignment, failure in the course, suspension, or even expulsion from the university.

For more information about academic integrity see the student handbook or the Office of Academic Integrity's website, and university policies on Research and Scholarship Misconduct.

Please ask your instructor if you are unsure what constitutes unauthorized assistance on an exam or assignment, or what information requires citation and/or attribution.

Course Content Distribution and Synchronous Session Recordings Policies
USC has policies that prohibit recording and distribution of any synchronous and asynchronous course content outside of the learning environment.

Recording a university class without the express permission of the instructor and announcement to the class, or unless conducted pursuant to an Office of Student Accessibility Services (OSAS) accommodation. Recording can inhibit free discussion in the future, and thus infringe on the academic freedom of other students as well as the instructor. (Living our Unifying Values: The USC Student Handbook, page 13).

Distribution or use of notes, recordings, exams, or other intellectual property, based on university classes or lectures without the express permission of the instructor for purposes other than individual or group study. This includes but is not limited to providing materials for distribution by services publishing course materials. This restriction on unauthorized use also applies to all information, which had been distributed to students or in any way had been displayed for use in relationship to the class, whether obtained in class, via email, on the internet, or via any other media. (Living our Unifying Values: The USC Student Handbook, page 13).

Students and Disability Accommodations:
USC welcomes students with disabilities into all of the University's educational programs. The Office of Student Accessibility Services (OSAS) is responsible for the determination of appropriate accommodations for students who encounter disability-related barriers. Once a student has completed the OSAS process (registration, initial appointment, and submitted documentation) and accommodations are determined to be reasonable and appropriate, a Letter of Accommodation (LOA) will be available to generate for each

course. The LOA must be given to each course instructor by the student and followed up with a discussion. This should be done as early in the semester as possible as accommodations are not retroactive. More information can be found at osas.usc.edu. You may contact OSAS at (213) 740-0776 or via email at osasfrontdesk@usc.edu.

Support Systems:

Counseling and Mental Health - (213) 740-9355 – 24/7 on call
Free and confidential mental health treatment for students, including short-term psychotherapy, group counseling, stress fitness workshops, and crisis intervention.

988 Suicide and Crisis Lifeline - 988 for both calls and text messages – 24/7 on call
The 988 Suicide and Crisis Lifeline (formerly known as the National Suicide Prevention Lifeline) provides free and confidential emotional support to people in suicidal crisis or emotional distress 24 hours a day, 7 days a week, across the United States. The Lifeline is comprised of a national network of over 200 local crisis centers, combining custom local care and resources with national standards and best practices. The new, shorter phone number makes it easier for people to remember and access mental health crisis services (though the previous 1 (800) 273-8255 number will continue to function indefinitely) and represents a continued commitment to those in crisis.

Relationship and Sexual Violence Prevention Services (RSVP) - (213) 740-9355(WELL) – 24/7 on call
Free and confidential therapy services, workshops, and training for situations related to gender- and power-based harm (including sexual assault, intimate partner violence, and stalking).

Office for Equity, Equal Opportunity, and Title IX (EEO-TIX) - (213) 740-5086
Information about how to get help or help someone affected by harassment or discrimination, rights of protected classes, reporting options, and additional resources for students, faculty, staff, visitors, and applicants.

Reporting Incidents of Bias or Harassment - (213) 740-5086 or (213) 821-8298
Avenue to report incidents of bias, hate crimes, and microaggressions to the Office for Equity, Equal Opportunity, and Title for appropriate investigation, supportive measures, and response.

The Office of Student Accessibility Services (OSAS) - (213) 740-0776
OSAS ensures equal access for students with disabilities through providing academic accommodations and auxiliary aids in accordance with federal laws and university policy.

USC Campus Support and Intervention - (213) 740-0411
Assists students and families in resolving complex personal, financial, and academic issues adversely affecting their success as a student.

Diversity, Equity and Inclusion - (213) 740-2101
Information on events, programs and training, the Provost's Diversity and Inclusion Council, Diversity Liaisons for each academic school, chronology, participation, and various resources for students.

USC Emergency - UPC: (213) 740-4321, HSC: (323) 442-1000 – 24/7 on call
Emergency assistance and avenue to report a crime. Latest updates regarding safety, including ways in which instruction will be continued if an officially declared emergency makes travel to campus infeasible.

USC Department of Public Safety - UPC: (213) 740-6000, HSC: (323) 442-1200 – 24/7 on call
Non-emergency assistance or information.

Office of the Ombuds - (213) 821-9556 (UPC) / (323-442-0382 (HSC)
A safe and confidential place to share your USC-related issues with a University Ombuds who will work with you to explore options or paths to manage your concern.

Occupational Therapy Faculty Practice - (323) 442-2850 or otfp@med.usc.edu
Confidential Lifestyle Redesign services for USC students to support health promoting habits and routines that enhance quality of life and academic performance.