Course ID and Title: Intro to Malware Analysis

Units: 4

Spring 2024: Tuesdays 6-10 PM

Location: OHE 542 (Subject to change)

Instructor: Sean Straw

Office: None
Office Hours: By appointment
Contact Info: Email: straw at usc domain
Responses to email

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

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.

Depending on the progress of the course, students may also be able to

- Analyze basic web shells; and
- Reverse engineer JavaScript with a focus on payment card stealing methods.

Prerequisite(s): ITP 125; ITP 375 or ITP 325
Recommended Preparation: Students unfamiliar with programming and programming concepts would benefit from familiarizing themselves with a programming language such as Python prior to the course.

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 a live demonstration of analysis concepts similar to the lab work to be assigned that day. 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 processors will not fit this requirement,** but the lab systems will be made available to students as much as possible.

Required Readings and Supplementary Materials

Practical Malware Analysis by Michael Sikorski and Andrew Honig
Additional material listed in the assigned week.

Optional Readings and Supplementary Materials

Listed in the assigned week.

Description and Assessment of Assignments

Labs will have analysis questions and suggestions on approaches on how to ascertain the questions, but as questions can often be answered many ways, the exact methods and approaches will be up the student unless otherwise specified. The section during which the lab is assigned will include a demonstration of answering the same or similar questions on a different sample to give students one approach to answer the question.

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

Labs will be graded based on the completeness of the answer and the thoroughness of the description of how the student achieved the answer.

Writing Skills

A significant portion of the cyber security and digital forensics curriculum involves communicating by writing professional quality reports. These reports are held to standards that are expected by professionals in industry who are writing reports for clients, attorneys, judges, juries, congresspeople, senators, POTUS, etc.

It is expected that the reports will be written with correct spelling, grammar, and language nuances of the American English language. A component of each report grade will be based on writing style, grammar, and word choice. These reports must be accessible to technical and non-technical readers alike.

If you are not a native English speaker and writer, it is recommended that you visit the USC American Language Institute (http://ali.usc.edu/) for resources to assist you in this course and your professional careers. Writing assistance is also available from the Dornsife Writing Center (https://dornsife.usc.edu/writingcenter/). You do not need to be a Dornsife student to take advantage of the services from the Writing Center. Additional writing assistance is also available from the Viterbi Writing

Center in the form of Writing Consultations (http://viterbi.usc.edu/students/undergrad/varc/writing-consultations.htm). In accordance with University standards, plagiarism of any type will not be tolerated.

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 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

Table 1 Grading Breakdown

Assessment Tool (assignments)	**Points**	**% of Grade**
Participation		10
Lab Assignments		55
Midterm		15
Final Examination		20
TOTAL		

Grading Scale

Course final grades will be determined using the following scale:

Table 2 Course Grading Scale

Letter grade	Corresponding numerical point range
A	93-100
A-	90-92
B+	87-89
B	83-86
B-	80-82
C+	77-79
C	73-76
C-	70-72
D+	67-69
D	63-66
D-	60-62
F	59 and below

Assignment Submission Policy

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, please 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.

Grading Timeline

Assignments submitted on time will be graded within 1-2 weeks of the submission. Late assignments will aim to be graded in the same 1-2 weeks, but the time of the submission may delay it.

Course Specific Policies

Please review the schedule of classes for the Final Exam schedule. Should you have a scheduling conflict with the final exam or per University policy you have more than 2 final exams scheduled on the same day, you must contact the instructor and coordinate an alternative time by the end of Week 3. Any requests made after Week 3 are not guaranteed to be accommodated.

Per USC policy, Final Exams must be scheduled during the assigned final examination schedule. It is your responsibility to arrange your travel after the scheduled date of the final exam.

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.

Classroom norms

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 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.

Academic Integrity

The University of Southern California is foremost a learning community committed to fostering successful scholars and researchers dedicated to the pursuit of knowledge and the transmission of ideas. Academic misconduct is in contrast to the university's mission to educate students through a broad array of first-rank academic, professional, and extracurricular programs and includes any act of dishonesty in the submission of academic work (either in draft or final form).

This course will follow the expectations for academic integrity as stated in the USC Student Handbook. 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.

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).

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.

Table 3 Course schedule

	Topics/Daily Activities	Readings/Preparation	Assignments
Week 1	- Class logistics - Goals of malware analysis - Static vs Dynamic analysis - Setting up a lab environment	**Practical Malware Analysis** - Chapter 0, Malware Analysis Primer - Chapter 2, Malware Analysis in Virtual Machines	Complete **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	Complete **Lab 2 – Dynamic malware triage**
Week 3	- Static malware triage	**Practical Malware Analysis** - Chapter 1, Basic Static Techniques	Complete **Lab 3 – Static malware triage**
Week 4	- Malicious document analysis	**How to Analyze Malicious Office Files** – Focus on everything before DDE's, but read it all **Analyzing Malicious Documents Cheat Sheet**	Complete **Lab 4 – Malicious Macros Analysis**
Week 5	PowerShell analysis and debugging	**Introduction to scripting** **Flow Control** **Practical Malware Analysis** - Chapter 8, Debugging, up to "Software Execution Breakpoints" on page 173 (non-inclusive). Do your best with the Disassembly, but do not fret about it. Optional – **BTLO Malicious PowerShell Analysis**	**C**omplete **Lab 5 – Malicious PowerShell Debugging**
Week 6	x86 Disassembly fundamentals	**Practical Malware Analysis** - Chapter 4, A Crash Course in x86 Disassembly	Complete **Lab 6 – Disassembly puzzles** and finish next week's reading

Week 7	x86 and Ghidra	**Practical Malware Analysis** - Chapter 6, Recognizing C Code Constructs in Assembly - Chapter 21, 64-bit malware	Complete **Lab 7 – Familiarization with Ghidra**
Week 8	Program debugging with x64dbg	**What is x64dbg + How to Use it** **Practical Malware Analysis** - Finish Chapter 8, Debugging (from "Software Execution Breakpoints" - Chapter 9, OllyDbg	Study for Midterm
Week 9	**Midterm**	**Prepare**	Complete next week's reading
Week 10	Using Ghidra and x64dbg	**Practical Malware Analysis** - Chapter 7, Analyzing Malicious Windows Programs	Begin **Lab 8 – Malware Sample Analysis**
Week 11	Summarizing Malware for Stakeholders	**Practical Malware Analysis** - Chapter 11, Malware Behavior **CISA Analysis Report** – Review at a high level, do not get lost in detail. Focus on the structure of how the information is presented. What do you like? **Optional: What to Include in a Malware Analysis Report – Lenny Zeltser**	Finish **Lab 8 – Malware Sample Analysis**
Week 12	Unpacking malware	**Practical Malware Analysis** - Chapter 18, Packers and Unpacking	Complete **Lab 9 – Unpacking malware**
Week 13	Shellcode Analysis	**Practical Malware Analysis** - Chapter 19, Shellcode Analysis	Complete **Lab 10 – Shellcode Analysis**
Week 14	JavaScript Debugging	**Debugging Chrome** **Analyzing MageCart** **MallRats: An Analysis of the Natural Fresh Mall Magecart Attack**	Complete **Lab 11 – Debugging a Scraper**
Week 15	Anti-Analysis techniques; course wrap-up	**Practical Malware Analysis** - Chapter 16, Anti-Debugging - Chapter 17, Anti-Virtual Machine Techniques	Prepare for Final
FINAL			Refer to the final exam schedule in the USC *Schedule of Classes* at 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.

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.