MALICIOUS CODE ANALYSIS

Carnegie Mellon University: Heinz College **Summer 2024**

Instructor: Jason Batchelor
Email: jxbatchelor@gmail.com
Office Hours: By appointment only
Website: http://www.cmu.edu/canvas/

GENERAL INFORMATION

DESCRIPTION

The ability to develop well instrumented networks, policies, and processes are directly correlated to ones understanding of malicious code, such that it has become a requisite for any decision maker operating within a modern enterprise. Just as necessary is the ability to effectively consume and produce actionable intelligence on malicious code. This course aims to provide students with a deeper understanding of the various tactics, techniques, and procedures found when analyzing malware. Students will also develop an appreciation for the technical challenges presented by malware and how to employ strategic detections and mitigations to meet today's threat.

LEARNING OBJECTIVES

Heinz College is a unique place where policy and tech come together and there is a significant gap in industry between those capable of reversing malicious code, and those operating in a managerial capacity to effect change with those results. The outlined course will serve as a bridge to bring these two worlds closer together and afford a better understanding of associated challenges.

Without an understanding of malicious code, the risk it poses to an organization, and techniques used to undermine traditional defense measures; decision makers are ill equipped to meet threats from state sponsored and criminal elements. By taking this course, future leaders are provided a better understanding of adversary tradecraft and how to effectively drive their people, process, and technology to meet modern threat actors.

PREREQUISITES

There are no course prerequisites. However, students are expected to have a working knowledge of both Windows **and** Linux operating systems. Students are also required to be **proficient in at least one** programming language.

Students will need to be able to perform basic troubleshooting exercises for their Lab environment in Windows/Linux environments and should be able to install software via a standalone executable, software repository, or from source code as needed. An understanding of basic command line syntax for both Windows and Linux platforms, such as navigating directories, creating, editing, and removing files is required.

Students are expected to understand basic networking principles to set up a virtual environment between Linux and Windows virtual machines on a virtual network.

Students will be required to be comfortable enough in a programing language to understand how to interpret API documentation, perform basic file I/O operations, basic work with binary data streams, and install/integrate third party modules.

MATERIALS

Optional: Michael Sikorski and Andrew Honig, *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software,* No Starch Press, 2012, ISBN: 978-1593272906

Students are expected to possess or have access to a laptop for completion of course work. The laptop must support the ability to install virtual machines and configure networking using virtualization software such as VMWare, Hyper-V, or VirtualBox.

EVALUATION

GRADING SCALE

A+	**100% - 98%**	**B+**	**89% - 88%**	**C+**	**79% - 78%**
A	**97% - 92%**	**B**	**87% - 82%**	**C**	**77% - 72%**
A-	**91% - 90%**	**B-**	**81% - 80%**	**C-**	**71% - 70%**

WEIGHT

Item	Weight
Assignments	35%
Lab Exercises	40%
Final Exam	25%

ASSIGNMENTS

Nearly every week there will be an **individual** assignment based off the lecture material for the week. Completion of these assignments will greatly assist you on future exams and help to reinforce concepts used in the labs.

LAB EXERCISES

There will be a series of lab exercises which will be **individual** efforts intended to grant students more in-depth exposure to the lecture content. Assigned labs will be less frequent but will require more effort.

FINAL EXAM

The final exam will consist of several multiple choice, fill in the blank, and written answer questions. No one is excused from this exam and there will be no makeup exam. Please ensure you are present.

POLICIES

LATE ASSIGNMENTS

Assignments that are late will face a 50% reduction for the first 24 hours of late time. Once this time has passed the grade cannot earn more than 20%.

The submission timestamp produced by Canvas will be the determining factor in judging if an assignment is late. Ensure you give yourself the requisite time needed to complete each assignment as no leniency will be provided.

CLASSROOM ETIQUETTE

Students are expected to be silent and attentive during lecture. All class members must conduct themselves in a professional and respectful manner both in and outside the classroom to promote an educational environment. Mobile devices are expected to be silent during lecture and are only permitted for use between breaks. Please bring any concerns to your course instructor or any CMU faculty member.

ACADEMIC INTEGRITY

Carnegie Mellon University sets high standards for academic integrity. Those standards are supported and enforced by students, including those who serve as academic integrity hearing panel members and hearing officers. The presumptive sanction for a first offense is course failure, accompanied by the transcript notation "Violation of the Academic Integrity Policy." The standard sanction for a first offense by graduate students is suspension or expulsion. Please see http://www.cmu.edu/academic-integrity/ for any questions.

For any assignment found to be the partial or complete result of cheating or plagiarism, your grade for that assignment will be zero. Cheating is defined as inappropriate collaboration among students on an assignment or failure to cite others work used in the semester paper or in-class presentation. This can include copying someone else's work with or without alteration. When students are found to be collaborating in this way, BOTH will pay the penalty regardless of who originated the work.

STUDENTS WITH DISSABILITIES

Our community values diversity and seeks to promote meaningful access to educational opportunities for all students. CMU and your instructors are committed to your success and to supporting Section 504 of the Rehabilitation Act of 1973 as amended and the Americans with Disabilities Act (1990). This means that in general no individual who is otherwise qualified shall be excluded from participation in, be denied benefits of, or be subjected to discrimination under any program or activity, solely by reason of having a disability.

If you believe that you need accommodations for a disability, please contact us ASAP, and we will work together to ensure that you have the correct access to resources on campus to assist you through your coursework and time at CMU.

TAKE CARE OF YOURSELF

During your time at Carnegie Mellon do your best to maintain a healthy lifestyle by eating well, exercising, avoiding drugs and alcohol, getting enough sleep and taking some time to relax. This will help you achieve your goals and cope with stress.

All of us benefit from support during times of struggle. You are not alone. There are many helpful resources available on campus and an important part of the college experience is learning how to ask for help. Asking for support sooner rather than later is often helpful.

If you or anyone you know experiences any academic stress, difficult life events, or feelings like anxiety or depression, we strongly encourage you to seek support. Counseling and Psychological Services (CaPS) is here to help: call 412-268-2922 and visit their website at http://www.cmu.edu/counseling/. Consider reaching out to a friend, faculty or family member you trust for help getting connected to the support that can help.

COURSE SCHEDULE

Week	Topics	Assigned Reading	Labs	Assignments
1	Analyst Roles and Malware Taxonomy	PDF: Ethics of RE Book: Chapter 0	Lab 1 Assigned	HW 1 Assigned
2	Fundamentals of Malicious Code Analysis	Book: Chapters 1, 2,3 PDF: Capture: A Tool for Behavioral Analysis of Applications and Documents		HW 1 Due HW 2 Assigned
3	Data Obfuscation	Book: Chapter 12 and 13	Lab 1 Due Lab 2 Assigned	HW 2 Due HW 3 Assigned
4	Anti Analysis Techniques	Book: Chapter 15, 16, and 17 PDF: Methods for VM Detection PDF: The "Ultimate" Anti-Debugging Reference		HW 3 Due HW 4 Assigned
5	Economics of Malware Analysis	PDF: Yara User's Manual PDF: The Case for Semantics-Based Methods in Reverse Engineering	Lab 2 Due	HW 4 Due
6	Final Exam			

Any or all of the previous information is subject to change or modification during the quarter.