CSCI 452 – Malware Analysis

COURSE SYLLABUS: Spring 2023

INSTRUCTOR INFORMATION

Instructor	Dr. Srujan Kotikela
Office Location	ACB2 #210
Office Hours	Tu/Thu 9:30 AM -11:30 AM, or by appointment
Email	Srujan. Kotikela **at** tamuc **dot** edu (1-2 business days) Email subject MUST contain CSCI-452-Spring-2023
Communication Response Time	Within 24 hours on weekdays, but any communication after Friday 5pm will be responded to by the following Monday

COURSE INFORMATION

Lectures (Time/Location):

Mon/Wed 2:50 PM - 4:05 PM @ ACB2 #314

Required Textbook:

Practical Malware Analysis, Sikorski and Honig, No Starch Press, 2012. ISBN-13: 978-1-59327-290-6.

Course Description

This class provides insights about the motivations of malware developers and the software weaknesses commonly exploited. In addition, the course will provide students with concepts, tools and methods associated with reverse engineering malicious code. Different attacking methods will be examined and analyzed to defend against malicious code. Safe handling practices for malware analysis will be taught/practiced.

Student Learning Outcomes

Upon completing this course, students should be able to:

- Understand and describe the behavior of typical malware.
- Understand how malware exploits and infects vulnerable systems.
- Perform static and dynamic analysis to study malware behavior.
- Detect and defeat the stealthy techniques used by malware.
- Design countermeasures to handle malware related threats.

COURSE REQUIREMENTS

Prerequisites: Junior Classification, CSCI 310, and Instructor's consent.

Instructional Methods

All materials, projects, and quizzes will be conducted through the D2L MyLeo Online learning system.

Student Responsibilities or Tips for Success in the Course

You own your success in this course, including ensuring you understand the expectations, timelines, policies and learning objectives.

Baseline expectations:

1. Attend weekly meetings and check LMS frequently.
2. Start your work tasks/assignments early.
3. Communicate with the other students in the project regularly and frequently.
4. Communicate with the instructor when you are confused or having course-related difficulties.

GRADING

Final grades in this course will be on the scale: A (>89%), B (80%-89%), C (70%-79%), D (60%-69%), F (<60%).

Assessment Type	Weight of Final Grade
Class participation	10 %
Quizzes	25 %
Mini Projects (executable code and correctness)	40 %
Reports and presentations	25 %

COURSE OUTLINE / CALENDAR

Part I: Malware Analysis Primer
- Malware Reverse Engineering
- Malware Analysis in Virtual Machines
- Mini Project 1

Part II: Advanced Static Analysis
- IDA Pro
- Analyzing Windows Malware
- Mini Project 2

Part III: Advanced Dynamic Analysis
- Debugging
- OllyDbg
- Mini Project 3

Part IV: Malware Functionality
- Malware Behavior
- Stealthy malware techniques

Part V: Anti-Reverse-Engineering
- Anti-Disassembly and Anti-Debugging
- Anit-VM Techniques and Packing
- Mini Project 4

*The schedule is **tentative** and may be adjusted to fit the actual class progress.

TECHNOLOGY REQUIREMENTS LMS

All course sections offered by Texas A&M University-Commerce have a corresponding course shell in the myLeo Online Learning Management System (LMS). Below are technical requirements

LMS Requirements: https://community.brightspace.com/s/article/Brightspace-Platform-Requirements

LMS Browser Support:https://documentation.brightspace.com/EN/brightspace/requirements/all/browser_support.htm

ACCESS AND NAVIGATION

You will need your campus-wide ID (CWID) and password to log into the course. If you do not know your CWID or have forgotten your password, contact the Center for IT Excellence (CITE) at 903.468.6000 or helpdesk@tamuc.edu**.** **Note:** Personal computer and internet connection problems do not excuse the requirement to complete all course work in a timely and satisfactory manner. Each student is expected to have a backup method to deal with these inevitable problems. In case of extreme technology related circumstances, please communicate directly with the instructor to best manage your success in this course.

COMMUNICATION AND SUPPORT

Technical Support

If you are having technical difficulty with any part of Brightspace, please contact Brightspace Technical Support at 1-877-325-7778. Other support options can be found here:

https://community.brightspace.com/support/s/contactsupport

Interaction with Instructor Statement

To communicate with me about this course, kindly use the email address included in this syllabus. During the week, you can generally expect a response to your emails within 1-2 business days. If you do not receive my response in 2 business days, please send a second email to me. To ensure I get your email and respond within indicated timelines above, please make sure that:

- Your email message is sent from your Texas A&M student account.
- Your email message includes a descriptive subject with the indicated prefix: CSCI-452-<semester>-<year>-<descriptive subject>

COURSE AND UNIVERSITY PROCEDURES/POLICIES

Course Specific Procedures/Policies

Attendance is required. Students are expected to do the readings, attend class, and participate in-class discussions. Each student is responsible for managing their own time and workload. Emergency / extreme circumstances causing a student to miss deadlines/exams will need to be supported by official and university approved documentation.

Positive Learning Environment

Your commitment as a student to learning is evidenced by your enrollment at Texas A &M University-Commerce. "All students enrolled at the University shall follow the tenets of common decency and acceptable behavior conducive to a positive learning environment." (See Student's Guide Handbook, Policies and Procedure, Conduct).

Sharing Your Work

All work produced by students may be shared by the instructor with the class for purposes of example and training. Such work will be as anonymous as possible. Finally, the instructor may share your work anonymously with future classes or in her own writing and research.

Submitting Assignments:

Unless special instructions are provided, assignments are NOT to be posted on any discussion board. Your completed work MUST be placed in the appropriate Dropbox in D2L Online. DO NOT EMAIL ME ANY ASSIGNMENTS AS THEY WILL BE DELETED. Please follow the rules for naming and posting assignments.

Late Work Policy

All assignments are due at the date and time specified.

Makeup Policy

There will be NO makeup exams or quizzes. If you shall miss a quiz/exam because of acceptable extreme circumstances (hospitalization, serious injury/sickness, death in the family etc.), you may be offered to choose to receive agrade based on your in-class ranking in the next quiz/exam.

Academic Integrity

Instances of academic dishonesty will not be tolerated. Cheating on exams or plagiarism (presenting the work of another as your own, or the use of another person's ideas without giving proper credit) will result in a failing grade and sanctions by the University. **For this class, all assignments / quizzes / exams / project are to be completed by the individual student unless otherwise specified.**
Any student cheating will receive a zero on the work they are doing, and subsequent cheating will result in a failing grade and potential academic sanctions.

Students at Texas A&M University-Commerce are expected to maintain high standards of integrity and honesty in all of their scholastic work. For more details and the definition of academic dishonesty see the following procedures:
Undergraduate Academic Dishonesty 13.99.99.R0.03
http://www.tamuc.edu/aboutUs/policiesProceduresStandardsStatements/rulesProcedures/13students/undergraduates/13.99.99.R0.03UndergraduateAcademicDishonesty.pdf
Graduate Student Academic Dishonesty 13.99.99.R0.10
http://www.tamuc.edu/aboutUs/policiesProceduresStandardsStatements/rulesProcedures/13students/graduate/13.99.99.R0.10GraduateStudentAcademicDishonesty.pdf

Basic Tenets of Common Decency

"All students enrolled at the University shall follow the tenets of common decency and acceptable behavior conducive to a positive learning environment." (Student's Guide Handbook, Policies and Procedures, Conduct.). This means that rude and/or disruptive behavior will not be tolerated.

Disclaimer

This syllabus is meant to provide general guidance of what to expect from this course. The instructor reserves the right to make changes as appropriate based on the progress of the class. All changes made to this syllabus during the semester will be announced. This document has been posted electronically. If you print a copy of it, please be sure to consult the last modified date of the online version to verify that your printed copy is current.

University Specific Procedures

Student Conduct

All students enrolled at the University shall follow the tenets of common decency and acceptable behavior conducive to a positive learning environment. The Code of Student Conduct is described in detail in the Student Guidebook. http://www.tamuc.edu/Admissions/oneStopShop/undergraduateAdmissions/studentGuidebook.aspx

Students should also consult the Rules of Netiquette for more information regarding how to interact with students in an online forum: https://www.britannica.com/topic/netiquette

TAMUC Attendance

For more information about the attendance policy please visit the Attendance webpage and Procedure 13.99.99.R0.01.

http://www.tamuc.edu/admissions/registrar/generalInformation/attendance.aspx

http://www.tamuc.edu/aboutUs/policiesProceduresStandardsStatements/rulesProcedures/13students/academic/13.99.99.R0.01.p df

Students with Disabilities-- ADA Statement

The Americans with Disabilities Act (ADA) is a federal anti-discrimination statute that provides comprehensive civil rights protection for persons with disabilities. Among other things, this legislation requires that all students with disabilities be guaranteed a learning environment that provides reasonable accommodation for their disabilities. If you have a disability requiring an accommodation, please contact:

Office of Student Disability Resources and Services

Texas A&M University-Commerce
Gee Library- Room 162
Phone (903) 886-5150 or (903) 886-5835, Fax (903) 468-8148

Email: studentdisabilityservices@tamuc.edu

Website: Office of Student Disability Resources and Services
http://www.tamuc.edu/campusLife/campusServices/studentDisabilityResourcesAndServices/

Nondiscrimination Notice

Texas A&M University-Commerce will comply in the classroom, and in online courses, with all federal and state laws prohibiting discrimination and related retaliation on the basis of race, color, religion, sex, national origin, disability, age, genetic information or veteran status. Further, an environment free from discrimination on the basis of sexual orientation, gender identity, or gender expression will be maintained.