Syllabus – Spring 2012

Course: Malware Analysis, 3 credits

CSCI 4972, CSCI 6963

Instructor: Professor Bulent Yener, yener@cs.rpi.edu

Office Hours: TBA, Lally 310

TA: Jeremy White, JWhiteRPI@gmail.com

Office Hours: TBA

Class Meetings: Friday 12:30PM – 2:50PM

Description:

With the increased use of the Internet and injection of computing systems into major industries (including national defense), technology is rapidly becoming a vital part of daily life. Unfortunately, this propagation and improvement of technology has given rise to elaborate malware writing techniques in accordance with a variety of motivations ranging from the relatively harmless Adware to devastating cyber-weaponry, e.g. Stuxnet. As a result, the ability to detect, analyze, reverse-engineer, control and eradicate malware is becoming increasingly important. A standardized analysis methodology is required as a base-line to tackling real-world analysis of malware in the wild.

This course will introduce a practical approach to analyzing malware through reading and hands-on interactive laboratory exercises. The laboratory exercises are to be completed on a weekly basis.

Learning Outcomes: Upon successful completion of this course, students will be able to apply the tools and methodologies used to perform static and dynamic analysis on unknown executables. Students will know how to infer the functionality of a program by analyzing disassembly and observing the changes on the system as it runs; how to extract investigative leads from host and network-based indicators associated with a malicious program; and how to identify specific coding constructs in disassembly. Students will also know the art of dynamic analysis and about Windows APIs most often used by malware authors.

Course Website: http://security.cs.rpi.edu/courses/PracticalMalwareAnalysis/

Required Book: "Practical Malware Analysis" by Michael Sikorski and Andrew Honig.

Free online edition available through Sarfari Tech Books via the RPI library.

http://libproxy.rpi.edu/login?url=http://proquest.safaribooksonline.com/?uicode=rpi.edu

Grading Criteria:

Quizzes.....20%

Malware Analysis #1.....20%

Malware Analysis #2.....20%

Malware Analysis #3 ....20%

Malware Analysis #4 ....20%

Grading Scale: A: 90%, B+: 85%, B: 80%, B-: 75%, C+: 70%, C: 65%, C-: 60%, D: 50%, F: < 50%

Malware Analysis: Each malware analysis will consist of a presentation given to the class, and a write-up to be submitted to the TA. Each presentation is 5% and each write-up is 15%. Sample analyses will be given so there will be no confusion as to what is expected of students.

> **Presentations:** At the end of each section of the book, the student will present an analysis of real malware using the techniques learned up to that current point.
>
> **Write-ups:** To accompany each presentation, a more detailed document will be completed on the malware analysis. Write-ups will utilize all techniques learned up to current point.

Quizzes: A quiz will be given each week, with questions taken directly from the topics presented in that week's lab. The quizzes will be straightforward, with their intended purpose being that students stay on top of completing their labs.

Schedule:

	Week	Chapter/Labs	Topics	Tasks
Part I	Jan 25th	0/1	Introduction to Malware/ Basic Static Analysis	Go through Chapter 1 together
	Feb 1st	2/3	Basic Dyn. Analysis	Chp. 2,3 Quiz
	Feb 8th	Real Malware Analysis		Give Presentations, Submit Write-ups
Part II	Feb 15th	4/5	Disassm., IDA Pro	Chp 4,5 Quiz
	Feb 22nd	6	C Code Constructs	Chp. 6 Quiz
	March 1st	7	Analyzing Win. Programs	Chp. 7 Quiz
	March 8th	Real Malware Analysis		Give Presentations, Submit Write-ups
	March 15th	Spring Break		
Part III	March 22nd	8/9	Debugging, OllyDBG	Chp. 8,9 Quiz
	March 29th	10	WinDBG	Chp. 10 Quiz
	April 5th	11	Malware Behavior	Chp. 11 Quiz
	April 12th	Real Malware Analysis		Give Presentations, Submit Write-ups
Part IV	April 19th	12	Covert Malware Launching	Chp. 12 Quiz
	April 26th	13	Data Encoding	Chp. 13 Quiz
	May 3rd	14	Network Signatures	Chp. 14 Quiz
	TDB (May 13th – May 17th)	Real Malware Analysis		Give Presentations, Submit Write-ups