Course Content	
Course Title (English)	Malware Reverse Engineering and Analysis
Course Title (Chinese)	惡意程式逆向分析
Credit	4
Instructor	Adjunct Assistant Prof. Chin-Wei Tien 田謹維 兼任助理教授
Outline	Malware is the main threat vector in cyber security. Enterprises often need to invest lots of resources in malware detection and defense. However, this offensive and defensive "game" is endless. Attackers will always try to use various attack methods to achieve their desired goals, thus create numerous new variant malwares. Therefore, how to understand and analyze malware programs is the aims of this course. This course is a graduate course developed and run solely by students, to teach skills in reverse engineering, malware behavior analysis and anti-analysis techniques. Topics Description 1 Course Preliminary 2 Basic Analysis 3 Static Analysis • File properties analysis • Behavioral analysis essentials 4 Dynamic Analysis • Code analysis essentials • Interactive behavioral analysis 5 Code Analysis (1)

	• Core reversing concepts • Functions reversing concepts 6 Code Analysis (2) • Control flow reversing • API patterns in malware 7 Midterm 8 Anti-Analysis Techniques (1) • Anti-Disassembly, Anti-VM, Anti-Debugging, Anti-AV 9 Anti-Analysis Techniques (2) • Executable packers and unpacking 10 Memory Forensics 11 Advanced Malware Analysis (optional) • Suspicious Web object (.vb, .js) analysis • Malicious office and pdf document analysis • 64-Bit Malware • Malware analysis using data science techniques 12 Finals
Goal	• Accessing the skills necessary to carry out independent analysis of modern malware reversing techniques using both static analysis, dynamic analysis and anti-analysis. • Familiar with the operation tools (Ghidra, IDA, OllyDbg, PE Explorer, ProcMon etc.) for malware analysis.
English Teaching	☐ YES ■ NO
Teaching Material	■ English ☐ Chinese