MACS H6012: Cyber Crime Malware

Short Title:	Cyber Crime Malware APPROVED
Full Title:	Cyber Crime Malware

Module Code:	MACS H6012

ECTS credits:	10

NFQ Level:	9

Module Delivered in	2 programme(s)

Module Contributor:	Mark Cummins

Module Description:	Module aims include: • Research into criminal activities on the Internet and computer crime legislation. • Learn the tools and techniques used by professional analysts to conduct online investigations, without revealing their identity. • safely analyze, debug, and disassemble malicious software • Reverse engineer common encoding and encryption algorithms • Investigate prevalent malware threats

Learning Outcomes:

On successful completion of this module the learner will be able to

1. Research methods and tools to conduct online investigations without revealing identity
2. Develop skills in reverse engineering common encoding and encryption algorithms
3. Investigate and appraise prevalent malware threats
4. Research criminal activity on the Internet
5. Review and critique legislation regarding computer and cyber criminal activities.

Module Content & Assessment

Indicative Content
Introduction to Malware analysis What is malware analysis? The goals of malware analysis, types of malware, packers and unpackers, general rules for malware analysis.
Static analysis techniques antivirus scanning, fingerprinting malware, detecting packers, file formats, linked libraries, PE file header and sections, X86 disassembly, IDA Pro.
Dynamic analysis techniques Sandboxes, running malware, monitoring with process monitor, viewing processes, Comparing registry snapshots, faking a network, packet sniffing, debugging, OllyDBG.
Malware analysis in virtual machines Sandboxes, the structure of a virtual machine, the risks of using hyper-visors for malware analysis, using your malware analysis machine, record/replay and running your malware.
Malware Functionality Malware behavior, covert malware launching, data encoding, malware focused network signatures.
Anti-Reverse Engineering Anti-disassembly, anti-debugging, anti-virtual machine techniques

Indicative Assessment Breakdown	%
Course Work Assessment %	100.00%

Course Work Assessment %

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Case study	Conduct online investigations to track criminal activity on the internet	1,4	30.00	Week 11
Practical/Skills Evaluation	Demonstrate practical skills to investigate prevalent malware threats.	3	50.00	Every Second Week
Project	Investigate, reverse and track a given piece malicious software and explain what laws are being broken (if any).	2,5	20.00	Week 6

No Final Exam Assessment %

Indicative Reassessment Requirement
Coursework Only *This module is reassessed solely on the basis of re-submitted coursework. There is no repeat written examination.*

ITB reserves the right to alter the nature and timings of assessment

Indicative Module Workload & Resources

Indicative Workload: Full Time	
Frequency	**Indicative Average Weekly Learner Workload**
Every Week	30.00
Every Week	30.00
Every Week	140.00

Resources

Recommended Book Resources

Michael Sikorski 2012, *Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software*, 1 Ed., No Starch Press [ISBN: 978-159327290]

Michael Ligh 2010, *Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code*, Wiley [ISBN: 978-047061303]

Eldad Eilam; [foreward by Elliot Chikofsky] 2005, *Reversing*, Wiley Indianapolis, IN [ISBN: 9780764574818]

Britz, M. J. 2004, *Computer Forensics and Cyber Crime; an Introduction*, Pearson Prentice Hall

Supplementary Book Resources

Christopher L.T. Brown 2005, *Computer Evidence: Collection and Preservation*

Recommended Article/Paper Resources

***1*, International Journal of Digital Crime and Forensics**

***2*, Journal of Digital Investigation**

***3*, International Journal of Digital Evidence**

This module does not have any other resources

Module Delivered in

Programme Code	Programme	Semester	Delivery
BN_KMACS_R	Master of Science in Computing in Applied Cyber Security	2	Elective
BN_KMACS_M	Master of Science in Computing in Applied Cyber Security (Research)	1	Group Elective 2