Assignment Instructions (COMP6236)

UNIVERSITY OF Southampton
School of Electronics and Computer Science

Module:	Software Engineering and Cyber Security	**Lecturer:**	ofb
Assignment:	Malware and Reverse Engineering	**Weighting:**	30%
Deadlines:	15/12/2016 4 p.m		

About the coursework

This coursework will focus on malware and reverse engineering. In this coursework you will investigate the different types of malware and how they work, explore how to analyse malware using static analysis tools and reverse engineering methodologies and make determinations as to the function of unknown executables.

Obtaining the required files

In order to obtain the required virtual machine images, you will need to be on the ECS VPN or using a computer in the ECS network, for example a lab machine. You can find full details on how to connect to the ECS VPN here:
https://secure.ecs.soton.ac.uk/kb/17/

If you are using a Windows machine, once you have connected to the VPN, in an explorer window, navigate to \\weevils.ecs.soton.ac.uk\comp6236 where you will be able to download the virtual machine images and copy the VM images to your local drive.

Once you have copied them, right click and select to open with Virtual Box to get started. If you are using a lab machine, **it is important that you store it locally on the C: drive** and not on your H: drive (which includes your documents and desktop), as the virtual machines do not work across the network.

If you are using a Mac, once you have connected to the VPN, open a new finder window and select 'Go' from the menubar, then 'Connect to server…'. Enter in smb://weevils.ecs.soton.ac.uk/comp6236 where you will be able to copy the virtual machine images.

From here, you can then download the Malware.ova.

Setting up the execution environment

Download the Malware.ova virtual machine and import it in Virtual Box. The virtual machine runs Windows 7 Enterprise Edition.

You MUST NOT enable networking connectivity on the Virtual Machines. You will be handling live samples of malware which will attempt to communicate with other computers on the network and the outside world. Everything you need to perform these tasks is already available on your Virtual Machine. You will not require any additional tools or internet connectivity.

You should take a Snapshot of the clean machine before you begin.

Your Report

It is expected that you will write between 1000-1200 words. In your report, you are expected to write down all the steps that you took to complete each part of the task and what you have learnt and discovered as part of your analysis. You should supplement this with screenshots of the various tools you have used and what you learnt from them. **It is the process that you go through, your justifications of the steps you take and your understanding which will be marked**.

Your Task: Identifying Suspicious Malware

Enter the Suspicious folder on the V: drive, where you will find 10 different suspicious executables. Your task is to attempt to identify which are malicious and which are benign.

1. **Basic static analysis:** To begin with, **without running any of these samples**, you should aim to identify as much information about them as possible using the **static analysis tools** and arrive at a conclusion as to which you believe to be malicious and which are not, justifying your answer.
2. **Reverse engineering:** Using the advanced reverse engineering tools available to supplement your basic static analysis, analyse each sample in further depth to identify what they do, how they work and further support your conclusions.
3. **Dynamic analysis:** Finally, use the dynamic analysis tools to run each sample and attempt to verify your conclusions and make any further observations.

Your report should cover the process you went through for each of these tasks. At the end of the report, you should provide a table for each sample of malware, with a column for what you found under static analysis, reverse engineering and dynamic analysis.

Submission

You will need to submit a **zip file**, containing an **html** report and all associated images through handin.ecs.soton.ac.uk. The .**html** file should describe how you have performed each task and should be no more than 1000-1200 words.

Your report should include screenshots of the tools being used. The top of the `.html` file should contain the username, first name and surname of the students who have worked together for this assignment.

The zip file should be named as follows: Malware_<Username1>_<Username2>.

For late submission, the standard ECS late penalties apply, as detailed in the regulations (para. 4.1 of *http://www.calendar.soton.ac.uk/sectionXII/ecs-ug.html*). They are 10% per working day that a piece of work is overdue, up to a maximum of 5 days, after which the mark becomes zero.

Support

Support will be offered through lectures, the timetabled labs and the tutorial.

Learning Outcomes

1. Understand the different types of malware
2. Utilise static analysis tools to analyse malware
3. Perform basic reverse engineering to identify the behaviour of malware
4. Utilise dynamic analysis tools to analyse malware at runtime

Marking Scheme

Your submission will be marked out of 30. The marking criteria below will be used:

Static analysis	Some use of static analysis tools used, examining some resources in malware samples. Conclusions lacking in justification.	*1,2*	*1-3*
	A reasonable use of static analysis, identifying common resources and using a good set of tools. Some justification of conclusions.		*4-6*
	A strong use of static analysis, making use of all resources and tools available to arrive at well-justified conclusions		*7-9*
Reverse	Some use of reverse engineering, although lacking in identification and understanding of key	*1,3*	*1-3*

Engineering	behaviours. Some observations made, although lacking in detail or justification.		
	A reasonable use of reverse engineering, with good identification and understanding of behaviour demonstrated. Reasonable observations made covering most behaviour.		*4-6*
	A strong use of reverse engineering, with deep identification and understanding shown of behaviour. Observations are accurate, relevant and justified and cover the important behaviour.		*7-9*
Dynamic analysis	Some use of dynamic analysis, although lacking in identification and understanding of key behaviours. Some observations made, although lacking in detail or justification.	*1,4*	*1-3*
	A reasonable use of dynamic analysis, with good identification and understanding of behaviour demonstrated. Reasonable observations made covering most behaviour.		*4-6*
	A strong use of dynamic analysis, with deep identification and understanding shown of behaviour. Observations are accurate, relevant and justified and cover the important behaviour.		*7-9*
Readability	Missing or incomplete report		*0-1*
	Basic report explaining some of the process and questions.		*2*
	Process explained clearly and concisely. Questions answered with explanations and examples. No grammatical/spelling errors		*3*

Please note that the University regulations regarding academic integrity apply (http://www.calendar.soton.ac.uk/sectionIV/academic-integrity-regs.html).