(COMP6016- Malware Analysis)

Coursework 2

Introduction

This coursework is worth 70% of the module. It is due in by Friday 23:59 of week 11. Files should be submitted via Moodle. Feedback will be given in week 14.

This is an individual coursework. Normal university rules on mitigating circumstances and academic conduct apply

Resources

The machine for analysis is an XP virtual machine which you can get at - http://sots.brookes.ac.uk/~p0087449/p00501/XP_Victim_for_students.ova (**NB This is 2GB is size so you probably want to download on campus**).

- The username is - administrator
- The password is - AVictim

A range of tools are pre-installed on the VM. You may install whatever else you need. You may share folders from the VM to a Kali VM if you wish to use any Linux tools

Assignment (What you have to do)

You are required to analyse and identify 4 pieces of the malware on the virtual machine given.

Requirements

You should document the process that you go through to detect and analyse the malware and for each piece of malware, where appropriate, you should determine the following -

- How does the malware affect the computer system?
- Where is the malware located (Note: it may be located in multiple places)
- What, if any, obfuscation techniques does it use?
- What, if any, network communication does it utilise?
- Suggest potential manual removal techniques

Hints

Documenting your process is a key as we are more concerned with how you find and analyse the malware rather than the number of malware that you locate.

Submission

You should submit a report on Moodle documenting –

- The process you went through to identify and analyse the malware
- Any tools that you used
- For each piece of malware, an answer to the questions in the assignment
- A reflection on the process

Mark scheme

The specification for the assignment gives the you lots of freedom to choose which aspect to focus on. You are expected to submit a report which include the process of identifying and analysing the malware.

Things do:

- (a) Good description in determining what the malware does and where it is located (10%)
- (b) Be able to find 4 pieces of malware on the computer (30%)
- (c) Be able to determine if the malware perform any obfuscation techniques and network communication (10%)
- (d) Consideration of manual removal techniques (10%)
- (e) Good report writing which include brief process in finding the malware (15%)
- (f) Good malware analysis which study their impact to the computer (15%)
- (g) Clear presentation with suitable summaries (10%)

Note: This is an individual assignment. You must write the report in your own words (do not copy from the paper) and any evidence of copying will be treated as plagiarism.

Learning Outcomes

This coursework is designed to test your attainment of the following learning outcomes:

2) Utilise appropriate tools, and techniques, for reverse engineering malware, including a critical analysis of local and network activity.

3) Demonstrate a critical understanding of obfuscation techniques and the tools and techniques that can be utilised to de-obfuscate obfuscated code.

4) Demonstrate a detailed understanding of the human factors in malware and
how these can be best defended against