

**REVERSE ENGINEERING MALWARE**

Year 2 (2019/20), Semester 3

## SCHOOL OF INFOCOMM TECHNOLOGY

Diploma in Cybersecurity & Digital Forensics

**ASSIGNMENT**

Weightage: 50%

Deadline: *Refer to Section IV. Deliverables*

# Objective

The aim of the assignment is to test the students’ ability to work in a group and individually, to analyse a malware using IDA Pro and reverse engineer it using OllyDBG.

# Scope

Students will work in teams of 2 members (for individual assignment the student can focus only on IDA Pro).

# Instructions

**Malware Submission Approval**

You will need to identify a malware to be analysed in this assignment.

You can download malwares at the following websites:

<https://zeltser.com/malware-sample-sources/>

<https://github.com/ytisf/theZoo>

<http://www.tekdefense.com/downloads/malware-samples/>

<https://malwaretips.com/forums/malware-vault-samples.104/>

(Make sure the malware is Win32 malware)

You will need to get submit the details of your team members and the malware by **Monday, 27th July 2020, 9.00 AM** before proceeding to analyse your malware (Login using your NP account to submit the form). The team leader can submit the details on <https://forms.gle/p8XTUv3ZiPBXcbx4A> (Note: You need to use the school email for login. No two teams in the same class will be allowed to analyse the same malware. In the event 2 or more teams submit the same malware for analysis preference will be given the first group which submits the details, the other teams need to change the malware. Please check the summary charts of the form results before you can submit the details)

**Report Submission**

After your tutor approves of the malware, you can proceed to analyse the malware and start writing your report (Template available on MeL). Your report should capture the necessary screenshots as evidence of analysis.

# Deliverables

The following are the deliverables, deadlines, and submission modes for this assignment. Only one copy of each deliverable is required.

Table 1 – Deliverables

|  |  |  |  |
| --- | --- | --- | --- |
| **Item** | **Deliverable** | **Deadline** | **Submission Mode** |
| 1 | Malware Submission Approval | **Monday, 27th July 2020, 9.00 AM** | Google Form |
| 2 | Report Submission | **Monday, 17th August 2020, 9.00 AM** | One Submission per team. To be submitted via Safe Assign in MeL. |

# Assessment

Each student in the team shall be graded according to the following components.

Table 2 – Assessment

|  |  |  |  |
| --- | --- | --- | --- |
| **Item** | **Component** | **Marks** | |
| **Team** | **Individual** |
| 1 | **Report Submission** | 20 | 80 |
| 2 | Presentation & Demo (via MS Teams) |  | 20 |
| **Sub-total** | | **20** | **80** |
| **Total** | | **100** | |

# Penalty

**Submission Mode**

For all submission modes, late submissions will be subjected to a penalty of 10% (of the total mark of the submitted component) for each day passed the deadline (including Sunday and public holiday). The last day for late submission is 3 days after the submission deadline, after which the assignment will not be accepted.

**Plagiarism**

If your submission was found to be plagiarised, you will fail the assignment and be put forward to further disciplinary actions.