CS4238 Group Project: Malware Analysis, Draft Description

1 Instructions

This is a group/team assignment. You need to work with your teammates, and submit just one report for your team. Note that your report may be checked by the available anti-plagiarism service.

Please prepare your report in PDF format by using your team number as part of the file name. Upload your report to LumiNUS's Files under the Student Submission / Group-Project folder. Note that your report should also list the name, student number, and email address of all team members at the beginning of it. Please also briefly mention the contributions of each team member in your group. Equal share of contribution is expected for all group members and exceptions should be indicated in the report.

The deadline of submission is **Wednesday, 1 December 2021, 23:59 SGT.**

2 Assignment Mission

2.1 Learning Objective

The **learning objective** of this project is for your team to analyze some real-world Windows malware samples using techniques that are discussed in our lectures and labs. The **following techniques** are thus relevant to be applied on the given malware samples:

- Basic static analysis;
- Basic dynamic analysis;
- Advanced static analysis, e.g. using IDA Pro;
- Advanced dynamic analysis, e.g using a Windows debugger such as OllyDbg;
- Unpacker, e.g using an unpacker such as Un{i}packer;
- Windows malware behavior analysis.

To help you with the tasks given below, several **sample malware analysis reports** are included with this assignment brief for your reference.

If you **run and dynamically-analyze** the malware samples, and be careful and make sure there is no network connection and folder sharing with your host machine and network!! If you are not sure, please have a discussion with TAs before you proceed.

2.2 Provided Malware Samples

You are given a zip file of malware samples, malware-samples.zip in LumiNUS. There are two sub-folders named `Solarwind` and `Olympic Destroyer` with 5 samples each. These samples are named by their respective MD5 hash value in a `zip` file. The password to the `zip` file is `infected`, which is a typical password to protect malicious files. Some of the samples can be executed (i.e. entrypoint), while the other samples are part of the malware workflow. To run some of the samples that can be executed, first rename them to "`.exe`" extension/suffix, and then run them as administrator. Please analyze the samples using any tools you prefer according to the two tasks given below.

3 Assignment Tasks

This group-project assessment component has the possible **25 marks**, which is worth **25%** of your final marks.

Complete the given tasks and write up your report about the malware behaviour by:

- explaining your analysis steps;
- mentioning the employed tools;
- putting necessary screenshots;
- succinctly highlighting important findings;
- making conclusions based on the findings.

3.1 Task 1: Simple Analysis of 3 Selected Malware Samples (15 marks)

Please perform a simple analysis of **any 3 of the 10** given malware samples by considering the features mentioned in the lecture. Additionally, do mention key similarities and differences among the 3 analyzed samples.

Please write up your report based on your analysis. Do put only color screenshots from tools that your team use, and avoid attaching screenshots obtained from external web-based services.

3.2 Task 2: Advance Analysis of 1 Selected Malware Sample (10 marks)

Please perform an advance analysis of **any 1 of the 10** given malware samples. Do write up your report based on your analysis. This advance analysis task is open-ended and **exploration is strongly encouraged**. You may consider performing the following investigation points, but are encouraged to explore additional interesting tasks beyond them:

- Network analysis (using Wireshark): e.g. are there any network-behavior patterns?
- Filesystem behavior analysis: e.g. what files do the malware create/modify/delete? Is there any sequential order/pattern?
- code-analysis with IDA: e.g. locate the code's functions related to your findings on malware behaviors, and make further exploration on these functions.
- Identify the malware's payload and analyze it.

Again, please put only color screenshots from tools that your team use, and avoid including screenshots obtained from external web-based services.

Good luck, and have fun with your group project!

— *End of Brief* —