Université Rennes 1

M2 CSE cybersecurity

Project 1

Real world malware analysis

November 5, 2020

1 Introduction

The role of a malware analyst is to conduct investigations of cyberattacks. Different from the toy examples proposed during this course, in the real world cyberattacks can be more complex and often mounted in multiple stages. This project's goal is to introduce malware analysis in a real world scenario.

2 Instructions

In this project, you will conduct a full analysis of a malware caught in the wild. For this, you will need to:

- prepare your own analysis environment (see 2.1);
- track an ongoing malware campaign[1];
- carry out a full analysis of this campaign[2]
- produce an analysis report and a presentation of your findings (see2.2)

The possibility of tracking an ongoing malware campaign on your own intends to let you to select the samples according to the setup of the analysis environment and, mostly important, to adapt the difficult/maturity level of the campaign. Do *not* hesitate to explore multiple malware campaigns before selecting one that is *active* and display an adequate maturity level[3].

2.1 Analysis environment

It is up to you to prepare your analysis environment, it must follow the following guidelines:

- **ISOLATION**: take the isolation of the analysis environment very seriously. Refer to this document for a detailed discussion about isolation of the lab environment.

[1] Use the slack channel *#malware-analysis* for exchanging information about ongoing malware campaigns with your colleagues

[2] Describe the attack stages, conduct static and dynamic analysis of the artifacts, etc.

[3] More advanced malware campaigns will be taken more into account for the evaluation.

- **PE file**: this project intends to practice the analysis of PE files (i.e. on Windows environment), therefore the chosen malware campaign must include at least on artifact as PE file - additional artifacts of other formats, such as scripts, are also meant to be analyzed.

Do not hesitate contact if any assistance is needed (specially regarding isolation).

2.2 Evaluation

The project will be documented in a *final report* and presented in two occasions: a *mid presentation* and a *final presentation*.

The criteria that will be observed in the project evaluation and the due dates are presented below.

Activity	due date	eval. weight
Report	23/11	40%
Mid presentation	12/11	20%
Final presentation	19/11	40%

Report

The produced report should contain a clear description of the work produced during the project, including details about the setup of the analysis environment, the process for the malware campaign tracking, artifact analysis, findings, additional research about the campaign and/or its artifacts, etc.

The final report must be in *PDF* format and should be pushed in the Github repository assigned for this project. This repository can include additional files, furthermore you are free to organize and use it as you deem most appropriate for your project repository (initially blank), however in this case you should create a readme file for describing the project organization (and where to find the final report).

Use this link for pulling the project repository.

Mid presentation

The *mid presentation* is intended for exposing the state of the ongoing project and engendering valuable discussions for its continuation. Therefore, your participation in the discussions and exchanges about your colleagues' projects will be considered as important as your project exposition in the evaluation.

The presentation will be take place remotely in a video-conference and slides as well as live demo or recorded video can be used. It should be planed to take 30 minutes, where 15 minutes will be dedicated for the project presentation and 15 for questions & answers.

Final presentation

The *final presentation* is intended for exposing the the work produced in the project, detailing its most important aspects and findings. As in the *mid presentation* your participation in the discussions and exchanges is desired and will be taken into account in the final evaluation.

The presentation will be take place remotely and it is expected to contain descriptive slides - supplementary live demo/recorded video is a plus. It should be planed to take 30 minutes, where 25 minutes will be dedicated for the project presentation and 5 for questions & answers.