**Assignment 2 (The Unknown Malware)**

You have been tasked with analyzing a suspicious executable program that has been provided to your company. The program has a picture icon and may potentially be malicious. In order to thoroughly understand the features and characteristics of this executable, you will need to conduct both static and dynamic analysis. This will involve examining the program's host indicators, such as its file structure and internal code, as well as its network indicators, such as its network traffic and communication patterns. As part of your analysis, you will also be required to write Yara Rules to describe the malware and upload them to Github. These rules will help to inform others about the characteristics and behavior of the malware.

Please note that the malware was created by me, so it should not cause any serious damage if it is accidentally run on your computer. However, you should still perform the analysis in an isolated environment to minimize the risk of accidental infection. This is a group assignment that can be completed by a maximum of two students and a minimum of one.

The assignment is worth 10 points. The malware is compressed with a password of "infected", as you learned in class. You will need to use this password to extract the malware before beginning your analysis.

Good luck 😊