# Malware Analysis Project

In this project, you will research a specific malware and create report and presentation that covers the following:

* Overview of the Threat - Etta
* Technical Expose - Megan
* Containment Strategy - Megan
* Awareness Training - Etta

**Note:** This website provides the option of downloading the malware and pcap files for closer study. If you choose to do so, please do so in your virtual environment.

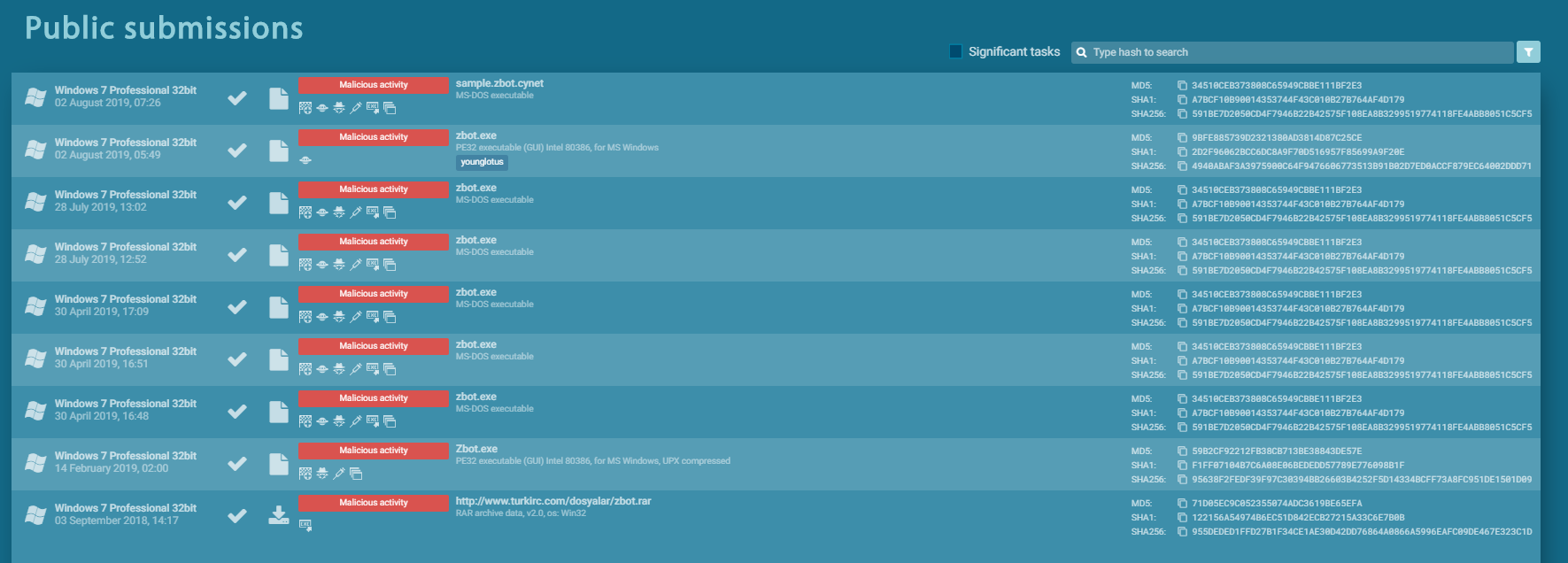
**Important Due Dates**:

* Saturday December 7th
* Written reports will be handed in at the end of the following week.

## **Malware Analysis**

In this project, you and your group will analyze the behavior of a live malware sample running on the Any.Run executable analysis platform.

Access the analyses at the URLs below:



* <https://app.any.run/tasks/8997c8a3-3a1f-43c7-b8fb-a3e6e72b8894/>
* <https://app.any.run/tasks/cbbba64e-2453-4aca-814b-2fd55f8e3e91/>
* <https://app.any.run/tasks/75ef8340-ffa6-4752-9082-96bd61d4201e/>
* <https://app.any.run/tasks/07644b1f-5493-44a1-ac09-ef6bfa5801d1/>
* <https://app.any.run/tasks/fcc008d1-a9d7-4ba0-ad18-b73d898afaa9/>
* <https://app.any.run/tasks/bd8d9316-6ad6-4dc7-a4b1-41786381f436/>
* <https://app.any.run/tasks/c15db619-356d-4e18-8930-da2d422429c5/>
* <https://app.any.run/tasks/208d5390-6d9d-4ec5-8bc7-8e0d8668948e/>
* https://app.any.run/tasks/c15db619-356d-4e18-8930-da2d422429c5/

### 

### **Analyzing Malware with Any.Run**

The Any.Run interface is pleasantly intuitive, but contains quite a lot of information. In the walkthrough below see link: <https://github.com/the-Coding-Boot-Camp-at-UT/UT-MCC-CYBER-PT-10-2019-U-C/blob/master/Lectures/Week%207%20-%20Malware%20Analysis/Project/StudentInstructions.md>

## **Writing the Report**

Your report must meet the following **requirements**:

* At least 4-5 pages, double-spaced.
* Include at least one diagram.
* Report should cover the same theme as your presentation.
* Include works cited at the end of the report.

### **Writing the Overview of the Threat:**

In this section, you will research, source and cite relevant articles and materials. Then, you will answer the required questions.

### **Writing the Technical Expose Section:**

Use the [Technical Expose Template](https://docs.google.com/document/d/1-V77cM1akgVRu5JXuUJZXklKcQayxgSipkUeW_XRfF0/edit) to guide you with this section of the report.

### **Writing the Containment Strategy and Awareness Training Sections:**

Use the [Containment Strategy and Awareness Training Template](https://docs.google.com/document/d/1mX3p3fo1lDUilX3w3g1Xuqw2Bq_BVyNRm3x89wlmSH0/edit) to guide you with these sections of the report.

## **Creating the Presentation**

Your presentation must meet the following requirements:

* Presentations will be given in-class, on the third day of the Malware Analysis Unit.
* Presentations will last 10-12 minutes each.
* Each person in the group must contribute in presenting the project. (Each person should speak for at least 2 minutes each.)
* Be prepared to answer follow-up questions.

Keep in mind the following criteria and tips when creating your presentation:

* Focus on developing clean slides with technical accuracy and depth
* Be as engaging as possible. (This presentation is an opportunity to practice your oral communication skills.)
* Consider what in your 4-5 page report is most relevant to include in your 10-12 minute presentation.