M E M O R A N D U M

15 October 2020

TO: **Agent CSI2334**
FROM: **Agency Director Fry**
RE: **OPERATION Reversing**

This morning our internal servers, while doing some routine history scans, discovered a newly cataloged executable that had no tracking data available. As this raises our Agency's security level to orange, your team has been assigned to determine what this code does.

As new members of the team, let me remind you of a few security items:

- The behavior of this executable is unknown - it should NOT be executed before your team determine what it does.
- Do not share any results with other teams - we suspect that there might be a mole in our organization that allowed this code to mysteriously appear.
- The executable has been compressed and renamed (ECS.2334), but some virus detection software may still be able to identify it as a binary or executable file. You may need to issue an exception for this file on your computer.

The renamed executable is located on Canvas, under "Course Resources" and then "Group Project". To help in your evaluation of this threat, each team can avail themselves of the use of a disassembler (as we have used in class) and any of the freely available online tools. Thanks to the reconnaissance efforts of agency analysts, we have intelligence on the internal structure of ECS.2334. Although not definitive, it is understood that this file could be a calculator tool that was lost in the system, it might be malicious code masquerading as a calculator, or it might be both of these (a functioning calculator with some malicious segments).

You will be selecting your groups of two people per project team. Each team must send an email to me notifying me of the team's composition no later than midnight on October 18, 2020.

The following information is requested as part of your team's final report.

1. In your report, address the following questions:

    a. What is the behavior of the executable?

    b. Is the executable a simple calculator, a malicious piece of code with calculator-like behavior, a combination of both, or neither of these?
        i. If it is a simple calculator, modify its behavior.
        ii. If it is malicious, quarantine the malicious code segment(s).
        iii. If it is both, do both i. and ii. above.
        iv. If it is neither, report on its detailed behavior.

    c. What approach did your team take in attacking this challenge? How did you divide and conquer this challenge given the resources at your disposal?

    d. What are your team milestones (develop a Project Plan)? How will your team ensure you meet those milestones?

    e. As a team, what did you learn from this challenge? What recommendations would you make to new team members coming to the Agency in the future?

2. Your final report to the Agency Director should start with your final Statement of Work, and describe your solution methods in detail. It is appropriate to include a brief summary of what you did, but the bulk of the report should focus on how you approached the problem, why you did what you did. Another agent who reads your report should be able to apply your techniques to any new similar threats, so make sure you document any tools and techniques that you use (describe each one thoroughly, along with its recommended/non-recommended uses and a list of advantages and disadvantages of each – a table format is preferred). The goal is to save time in the future by avoiding the need for slow and potentially dangerous brainstorming, so make sure your final report includes everything mentioned here.

3. As agents-in-training, part of your apprenticeship will include several communication artifacts:

    a. Progress Reports, with updated Statement of Work (SOW) as the changes in your team's specification is updated. These changes must be approved by the Agency Director before changes are implemented. The SOW will be used, in part, to assess the success of your team's efforts.

    b. Final Presentation of Findings will be conducted at the end of the training period. These presentations will be done virtually, since our teams are located across the globe.

    c. You will work with your partner to ensure optimum performance and assessment. To this end, you will complete both a formative and a summative evaluation, and you will be assessed on the thought and deliberation going into both of these evaluations.

Final presentations will be conducted on Tuesday, December 1, 2020, by video link, before 12:30pm CT. All project artifacts (with the exception of the Summative Peer Evaluation) will be due before midnight on Monday, November 30, 2020.