Engineering Interview Homework Assignment

Last Updated: June 2018

Background Information

Red Canary processes telemetry from Endpoint Detection and Response (EDR) agents. This telemetry includes activity such as:

- Process creation
- File creation
- File creation, modification, and deletion
- Registry key creation, modification, and deletion (Windows)
- Registry value creation, modification, and deletion (Windows)

One concern when the EDR agent is updated is if there are regressions in the data it emits. Red Canary needs a way to ensure that our core telemetry is still properly emitted when EDR agents are updated.

Assignment Instructions

Your assignment, should you choose to accept it, is to create a framework that allows us to generate endpoint activity across **at least two of three** supported platforms (Windows, macOS, Linux). This program will allow us to test an EDR agent and ensure it generates the appropriate telemetry.

Your program should trigger the following activity:

- Start a process, given a path to an executable file and the desired (optional) command-line arguments
- Create a file of a specified type at a specified location
- Modify a file
- Delete a file
- Establish a network connection and transmit data

Additionally, your program should keep a log of the activity it triggered. The activity log allows us to correlate what data the test program generated with the actual data recorded by an EDR agent.

This log should be in a machine friendly format (e.g. CSV, TSV, JSON, YAML, etc). Each data type should contain the following information:

- Process start
    - Timestamp of start time
    - Username that started the process
    - Process name
    - Process command line
    - Process ID
- File creation, modification, deletion
    - Timestamp of activity
    - Full path to the file
    - Activity descriptor - e.g. create, modified, delete
    - Username that started the process that created/modified/deleted the file
    - Process name that created/modified/deleted the file
    - Process command line
    - Process ID
- Network connection and data transmission
    - Timestamp of activity
    - Username that started the process that initiated the network activity
    - Destination address and port
    - Source address and port
    - Amount of data sent
    - Protocol of data sent
    - Process name that created/modified/deleted the file
    - Process command line
    - Process ID

You may use any programming language you choose, so long as it supports all three platforms (Windows, macOS, Linux). We understand that not everyone may have access to all platforms and can assist in setting up a test environment for you.

The code should be placed on GitHub so that we can review your changes.

You're free to ask questions and brainstorm with Red Canary engineers. You do not have to solve this in a vacuum but you will have to write all code yourself.