RedEye Tool

October 14, 2022

OVERVIEW

RedEye is an open-source analytic tool developed by CISA and DOE's Pacific Northwest National Laboratory to assist Red Teams with visualizing and reporting command and control activities. This tool, released in October 2022 on GitHub, allows an operator to assess and display complex data, evaluate mitigation strategies, and enable effective decision making in response to a Red Team assessment. The tool parses logs, such as those from Cobalt Strike, and presents the data in an easily digestible format. The users can then tag and add comments to activities displayed within the tool. The operators can use the RedEye's presentation mode to present findings and workflow to stakeholders.

RedEye can assist an operator to efficiently:

- Replay and demonstrate Red Team's assessment activities as they occurred rather than manually pouring through thousands of lines of log text.
- Display and evaluate complex assessment data to enable effective decision making.
- Gain a clearer understanding of the attack path taken and the hosts compromised during a Red Team assessment or penetration test.

GETTING STARTED

To begin,

1. Go to the RedEye section on CISA's GitHub page.
2. Review the `README.md` file.
3. Download the latest `RedEye` binaries for your operating system from the Releases section on GitHub.

RedEye currently supports uploading Cobalt Strike logs and offers both Red Team and Blue Team modes.

- The **Red Team mode** offers the ability to upload campaign logs, explore, and create presentations. This mode is started by running RedEye with the `SERVER_BLUE_TEAM=false` environment variable or the `--redTeam` argument.
- The **Blue Team mode** enables the ability to review a read-only campaign exported by a Red Team. This mode runs by default.

Note: Both Red and Blue Team modes can be started from the same `RedEye` application binary.

ADDITIONAL RESOURCES

For more details about this tool, watch CISA's RedEye tool overview video.