

Shortcomings/Wishlist

Limitations

The payload simulation uses simplified behaviors and does not mimic real malware complexity. The program relies on a single Python script, therefore limits modularity and maintainability. Upon trying to email the .exe file to a group member for a test on their computer, the email provider flagged and blocked the .exe, restricting testing. Also, the simulation currently only runs on Windows and is not cross platform. We attempted to open the file on a macOS device and it failed to open. Lastly, the user interactions are not recorded, including click behavior or engagement tracking

Future Work

Prioritized roadmap items for future iterations include adding more realistic behavior scenarios, improving modular design by splitting components into separate scripts, and expanding compatibility for macOS and Linux. Additions may look like face encryption or keylogging demo.