Demonstration Trojan Horse

Team Orange

What is it?

A **trojan horse** is a seemingly benign application that secretly contains malicious code.

Our trojan horse masquerades as a simple weather app.

Secretly, it will send user keystrokes back to a remote server.

The remote server hosts a web interface, to visualize and search for keystrokes.

Problem to solve

An educational tool for students to learn about trojan horses.

- Raising awareness of what is possible
  - 2.8 billion malware attacks in 2022, +11% from 2021 (Sonicwall, 2022)
- Inspire skepticism of unknown / untrusted applications
  - Encourage caution granting root access to unknown applications
- Identify mechanisms for implementation of malicious code
  - Educate cyber defense professionals on how to properly mitigate attacks
  - Offer mitigation strategies

Source:

https://www.sonicwall.com/medialibrary/en/white-paper/mid-year-2022-cyber-threat-report.pdf

Our implementation

- **Benign Application:** Used as a vehicle to deliver keylogger
- **Keylogger:** Intercepts keystrokes from victim and sends to server
- **Web server:** Displays information on the current keys that have been pressed and any information pulled from it.