**Malware Sandbox Simulator – Project Document**

**Team Members:**

* Member 1 – Simulated Malware Developer
* Member 2 – Sandbox Detector & Logger
* Member 3 – GUI Interface Developer

**Start Date:** [23/07/2025]  
**Repository:** [https://github.com/Night424/sandboxSimulator]

**Project Overview**

The **Malware Sandbox Simulator** is a safe and educational tool that mimics virus-like behaviour and detects it in real-time. It simulates what malicious software might do (file replication, startup injection, hidden files) and monitors the system for those behaviours in a sandboxed environment.

**For educational and portfolio purposes only. No real malware is used or created.**

**Project Goals**

* Simulate real-world malware behaviours (harmlessly)
* Monitor file system and log suspicious activity
* Provide a user-friendly GUI for launching and viewing logs
* Teach malware analysis basics in a controlled, safe environment

**Core Features**

|  |  |
| --- | --- |
| **Feature** | **Description** |
| Simulated Malware | Creates hidden files, copies itself, simulates registry write |
| Sandbox Monitor | Watches directories and logs malware-like actions |
| Logging System | Stores logs to file and displays in console or UI |
| Electron GUI | Interface to launch simulator, view logs, and control sandbox |
| Quarantine Folder | Detected files are optionally moved here |

**🗂 Folder Structure**

**Team Member Responsibilities**

**Member 1 – Simulated Malware Developer (Norytt)**

* Create fake virus scripts (fakevirus.js)
* Simulate behaviors like:
  + Self-replication to startup
  + Hidden file creation
  + Fake "registry" JSON entry
  + Dummy payload (message, countdown, etc.)

**Member 2 – Sandbox Monitor (LilBayBey)**

* Watch system directories using chokidar (Node.js) or watchdog (Python)
* Log detected file activity: create, delete, modify
* Optionally trigger alerts or move suspicious files to quarantine

**Member 3 – GUI Developer (Night)**

* Build an Electron interface:
  + Buttons to launch malware sim
  + View logs in real-time
  + Open folders
* Style app with basic CSS (dark theme or terminal-like look)

**Technology Stack**

|  |  |
| --- | --- |
| **Purpose** | **Tech** |
| Scripting & Monitoring | Node.js (FS module, chokidar) |
| GUI | Electron.js |
| File Handling | Node.js fs Os |
| Logging | Plaintext + console |
| Optional |  |

**Milestones**

|  |  |
| --- | --- |
| **Milestone** | **Deadline** |
| Project Planning & Roles | [Today] |
| Setup Folder Structure & GitHub Repo | [Soon] |
| Finish Simulated Malware Logic | [Date] |
| Build Monitoring Script | [Date] |
| Create GUI and Hook Up Logs | [Date] |
| Testing: Log detection, simulate infection | [Date] |
| Final Packaging (e.g., Windows .exe) | [Optional] |

**README Highlights (for GitHub)**

# Malware Sandbox Simulator 🐛

This is a safe and educational tool that simulates malware behavior and detects it in a sandboxed environment.

> For educational use only. No real malware is used or executed.

## Features

- Simulates self-copying, stealth files, and registry injection

- Monitors file changes and logs events in real-time

- Desktop GUI built with Electron