Dhwanil Raval

20231105060127

Abstract

A safe, browser‑based malware simulator (HTML/CSS/JS, deployed on Netlify) models viruses, worms, and trojans using an in‑memory file system and virtual network graph without executing real malware. Adjustable attack/defense parameters and Python analytics produce infection curves, detection ratios, and R0‑style estimates; results highlight how worms spread quickly in unsegmented networks, viruses rely on user/file activity, and trojans depend on user consent—reinforcing integrity, defense‑in‑depth, and monitoring.

Malware Analyzer: A Safe, Interactive Simulator for Viruses, Worms, and Trojans

ALA‑2 (CNS)

* **Quantum Nexus Cyber — Detailed Case Study Report**

**1.Abstract**

Quantum Nexus Cyber is an interactive, browser-based platform designed to simulate malware behavior and demonstrate cybersecurity defense strategies in a safe, conceptual quantum-secured environment. The project uses HTML, CSS, JavaScript, and Python to provide an intuitive, real-time simulation of viruses, worms, and trojans. It allows users to understand malware propagation, configure defense mechanisms, and visualize system health, all without executing real malware

**2. Project Objectives**

1. Create a safe, educational simulation of malware spread in a networked environment.
2. Provide configurable parameters for malware behavior and defense strategies.
3. Visualize infection propagation, network health, and analytics in real-time.
4. Introduce users to quantum-inspired security concepts in an accessible way.
5. Offer a terminal interface (NEXUS Terminal) for technical interaction.

**3. Technology Stack**

* **Frontend:** HTML5, CSS3, JavaScript (ES6+) for UI, interactivity, and simulation control.
* **Backend / Logic:** Python for handling simulation computations and optional server-side logging.
* **Visualization:** Canvas API and/or SVG for network graph and heatmap visualizations.
* **Hosting:** Netlify for fast, secure, browser-accessible deployment.
* **Simulation Engine:** Custom JS engine to model malware behavior and defense mechanisms.
* **Analytics:** Real-time charts and logs implemented via JS charting libraries.

**4. Features**

* **Malware Simulation:** Interactive modeling of three malware types: viruses, worms, and trojans.
* **NEXUS Terminal v4.0:** Command-line style interface for technical users.
* **Configurable Parameters:** Infection probability, network size, scan rates, patching speed, segmentation options.
* **Real-Time Analytics:** Infection timelines, heatmaps, and system health indicators.
* **Educational Insights:** Helps users learn about malware dynamics, defense strategies, and quantum-inspired security.
* **Safe Environment:** Entire simulation is client-side; no real malware is executed.

**5. Working / Simulation Design**

**5.1 Simulation Model**

* Uses discrete-time ticks to simulate network evolution.
* Each node in the network can be in one of several states: Healthy, Exposed, Infected, Dormant, or Removed.
* Malware spreads probabilistically based on its type and configured parameters.
* Defense mechanisms like antivirus scanning, patching, and network segmentation reduce infection likelihood.

**5.2 Malware Types**

1. **Virus:** Attaches to host files and spreads when files are shared.
2. **Worm:** Self-replicates and spreads across network nodes automatically.
3. **Trojan:** Appears as legitimate software but opens backdoors for malicious activity.

**5.3 Prevention Strategies (Simulated & Real-World)**

* **Network Segmentation:** Limits malware propagation paths.
* **Regular Patching:** Keeps systems updated to reduce vulnerabilities.
* **Antivirus & Endpoint Protection:** Detects and removes malware before it spreads.
* **User Awareness:** Training to avoid executing suspicious files or links.
* **Backup & Recovery:** Maintain offline backups to restore affected systems.

**6. Pros**

* **Highly Interactive:** Engaging visualizations and real-time analytics.
* **Educational:** Demonstrates malware behavior and defense strategies effectively.
* **Safe:** No execution of real malware.
* **Quantum-Inspired Security Concept:** Unique angle that adds depth and originality.
* **Terminal Interface:** Appeals to technical users and makes learning fun.
* **Configurable:** Users can experiment with different parameters and scenarios.

**7. Cons**

* **Limited Advanced Malware Models:** Could include ransomware or botnets in future updates.
* **Browser-Based Performance:** Large networks may run slower in some browsers.
* **Quantum Security Implementation:** Currently conceptual, not fully implemented (still educational).

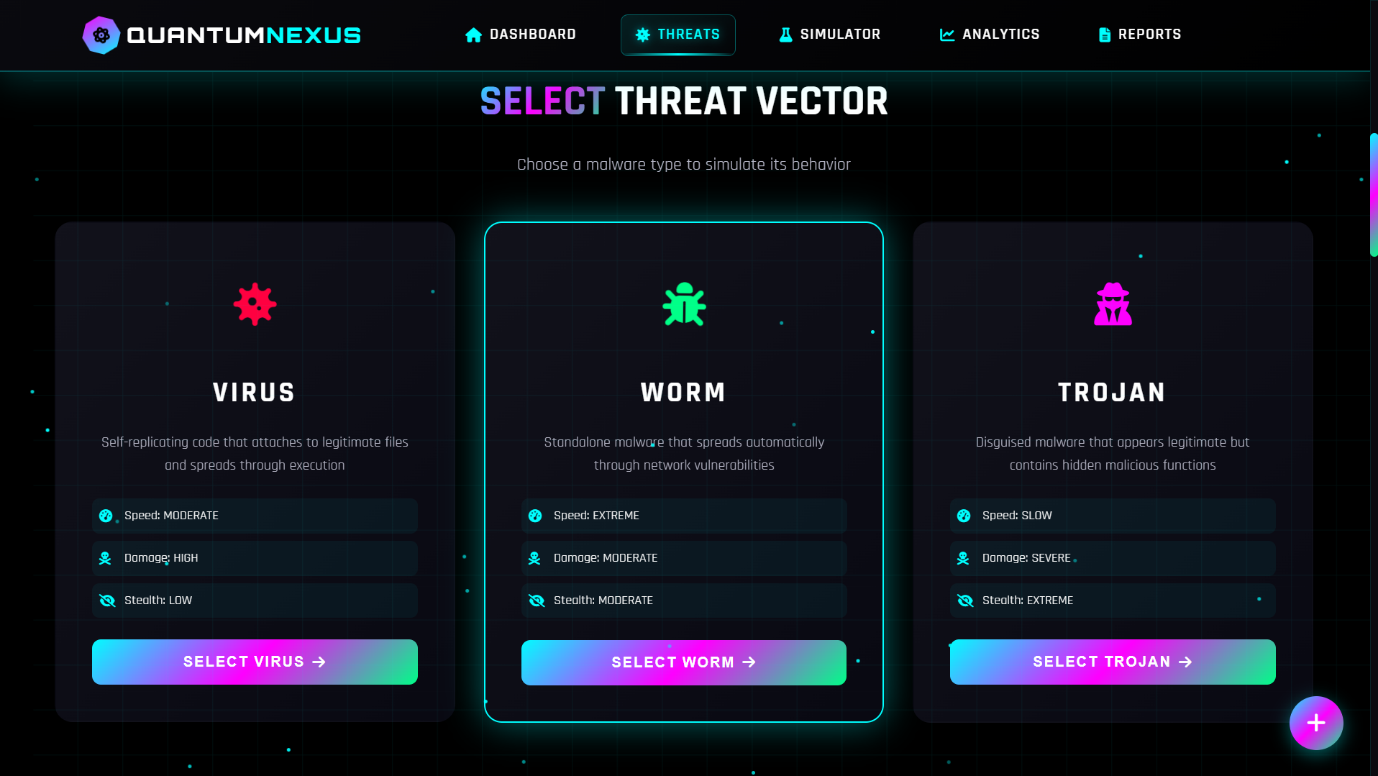
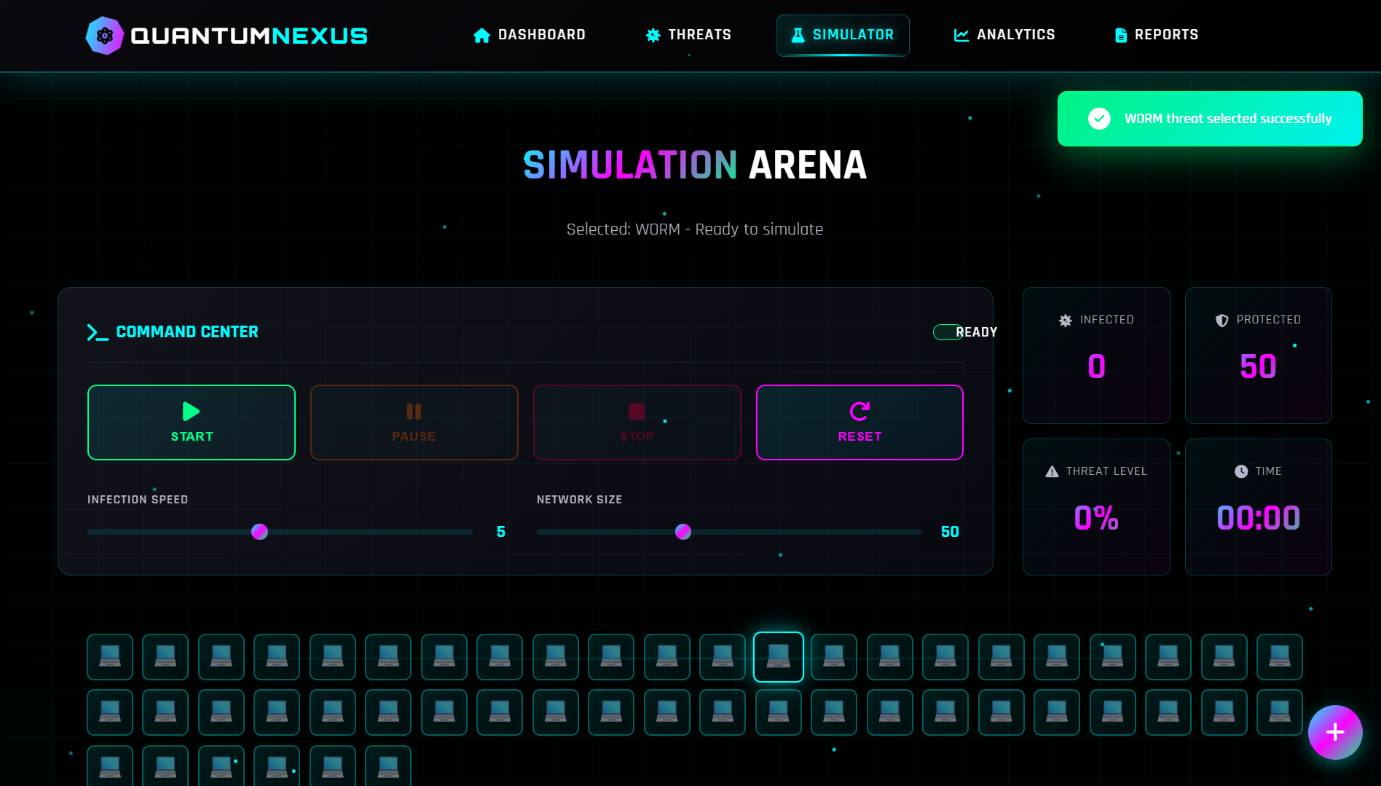
**8. Conclusion**

Quantum Nexus Cyber is a robust educational platform combining interactive malware simulation, configurable defense strategies, and quantum-inspired security concepts. Using HTML, CSS, JavaScript, and Python, it offers real-time analytics, an engaging terminal interface, and safe experimentation. With minimal cons, this project is highly suitable for academic demonstrations, workshops, and cybersecurity training, providing both technical depth and originality

**A screenshot of a computer game

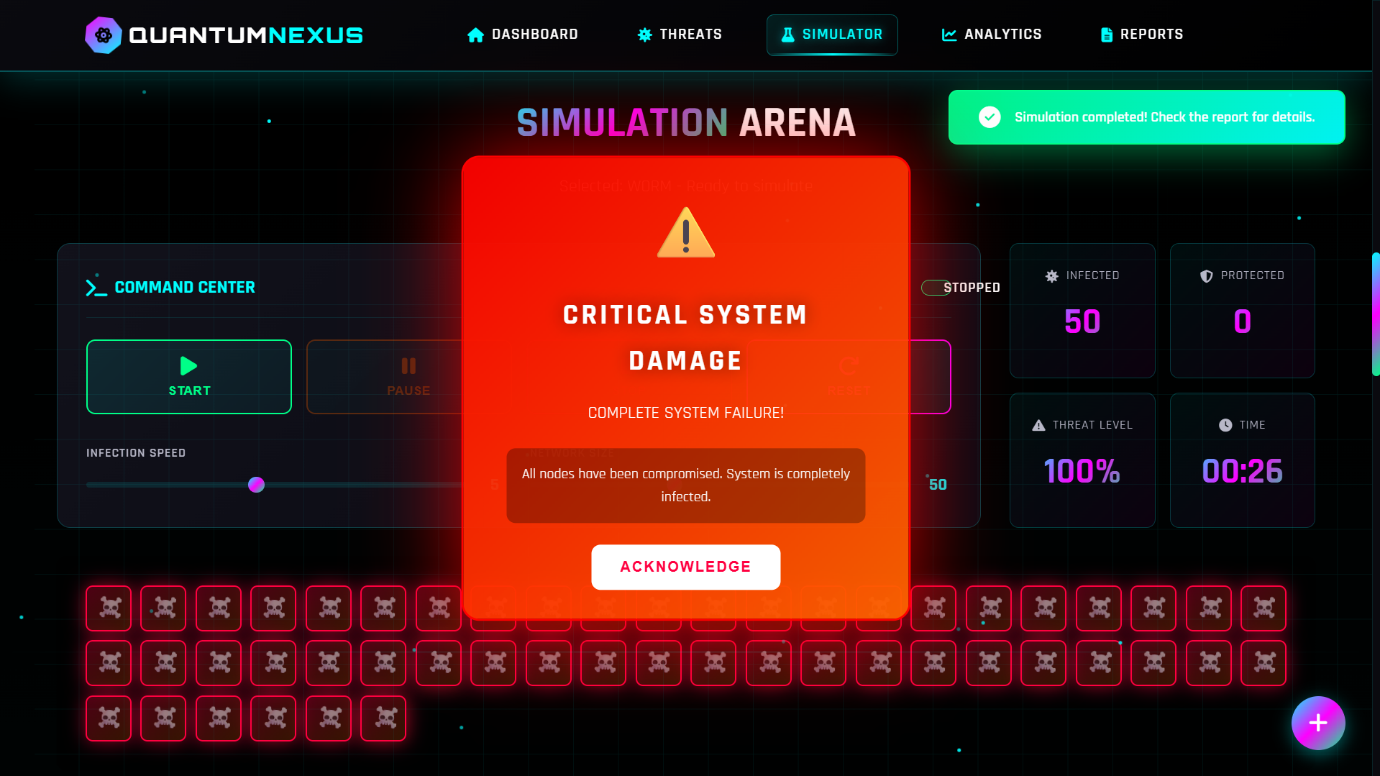
AI-generated content may be incorrect.9. working and output:-**

**Fig 1 Dashboard**

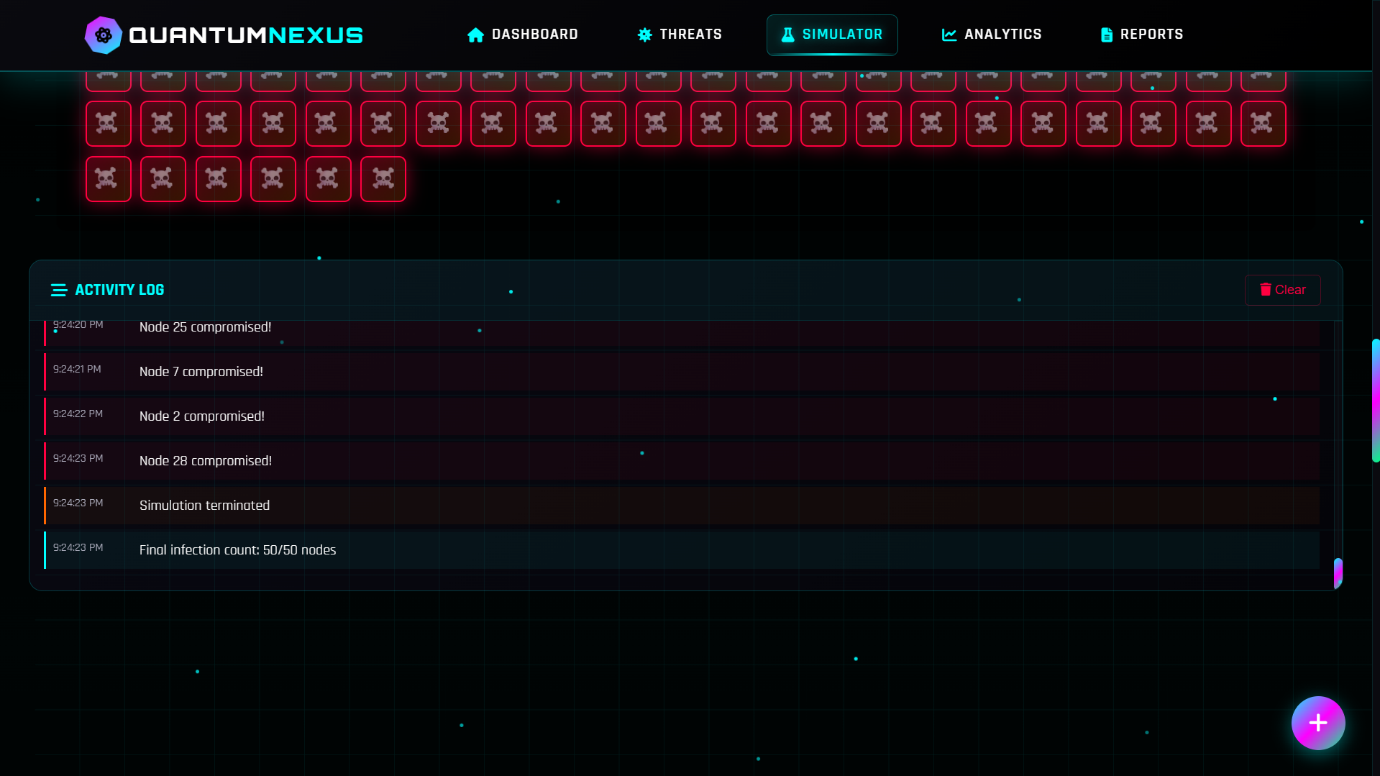
****

**Fig 3 Simulator Arena**

**Fig 2 Threat Vector**

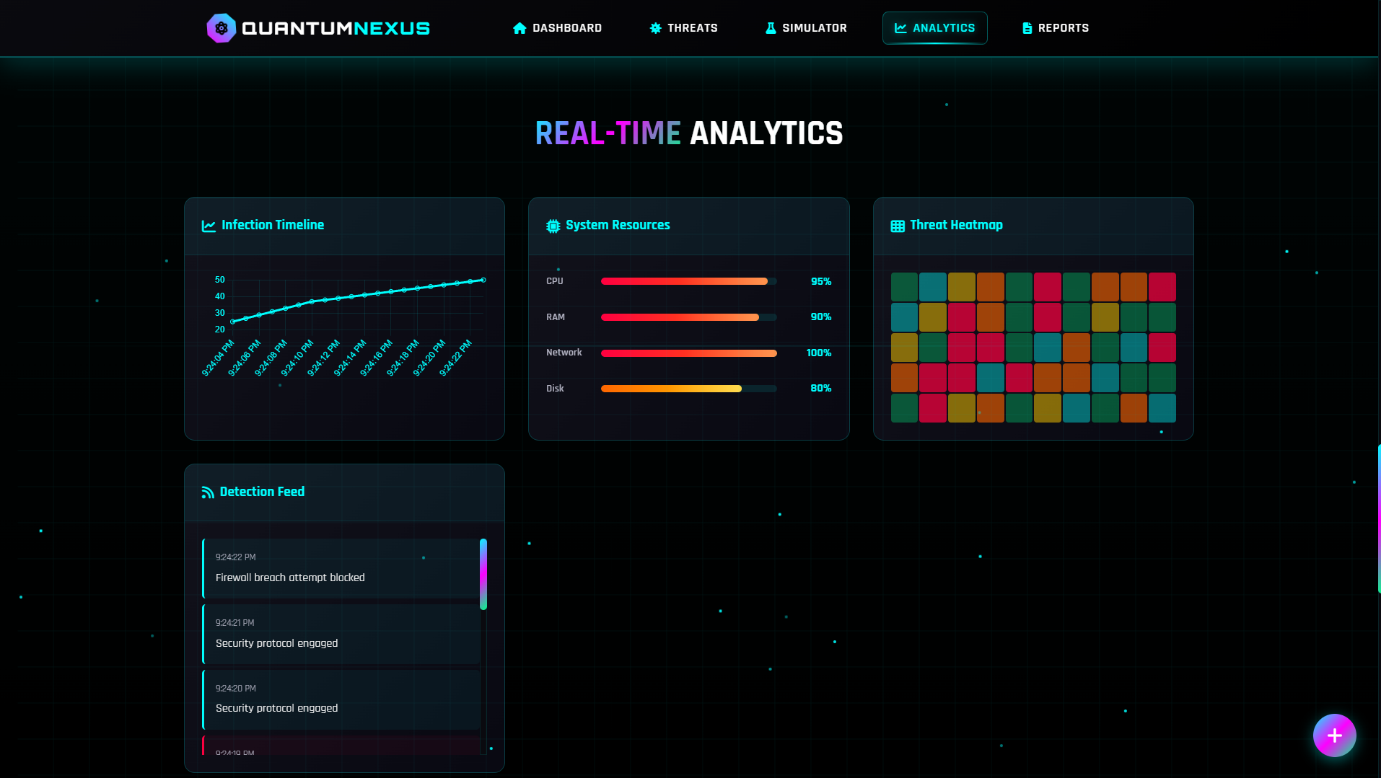
****

**Fig 4 System Damage Pop-Up**



**Fig 5 Activity Log**

**A screenshot of a computer

AI-generated content may be incorrect.**

**Fig 7 Analysis Report**

**Fig 6 Real-Time Analytics**

A screenshot of a game

AI-generated content may be incorrect.

**Fig 8 Quantum Nexus Terminal**