Journal of Posthumanism
2025
Volume: 5, No: 9, pp. 355–372
ISSN: 2634-3576 (Print) | ISSN 2634-3584 (Online)
posthumanism.co.uk

DOI: https://doi.org/10.63332/joph.v5i9.3335

Bridging Theory and Practice: A Hybrid Malware Detection System with 3D Propagation Visualization for Cybersecurity Training

Dino Jhoel Condori-Churata[1], Yarin Nilo Laqui-Huilahuaña[2], Joel Edson Huerta-Barrantes[3], Robert Antonio Romero-Flores[4], Hugo Yosef Gomez-Quispe[5], Giovana Araseli Flores-Turpo[6], Wily Leopoldo Velasquez-Velasquez[7]

Abstract

This study presents an innovative pedagogical approach to cybersecurity education through the development of an interactive malware propagation simulation. The system integrates a hybrid detection model, combining SHA-256 signature analysis, a proprietary heuristic engine, and file verification using the WinTrust API, in addition to system-level monitoring through Microsoft Defender's command-line interface. Its main contribution lies in a dynamic visualization module that represents malware propagation in a virtual network of nodes, displaying states such as healthy, infected, or immune through color-coded graphics. This interactive component allows real-time observation and experimentation with infection dynamics, effectively bridging theory and practice. Tests demonstrated its ability to identify suspicious files and simulate various propagation scenarios, validating its potential as an educational resource in cybersecurity.

Keywords: *Malware Propagation Modeling, Hybrid Threat Detection, Heuristic Analysis, SHA-256 Fingerprinting. Interactive Learning Systems, Visual Learning Tools, Cybersecurity Training.*

Introduction

Cybersecurity has become established as a critical global challenge, whose impact transcends geographic, economic, and sectoral boundaries (Sema Admass, Yayeh Munaye, & Abeshu Diro, 2024; Delaere, Bouillet Carroza, & Armijo Catalán, 2025). It is estimated that the cost of cybercrime will reach between 1.2 and 1.5 trillion U.S. dollars annually by 2025, reflecting the magnitude of both direct and indirect financial losses, including operational disruption and reputational damage (Miliefsky, 2025). This outlook has been worsened by a growing wave of disruptive and destructive attacks, whose frequency has doubled since 2020. In 2024 alone, more than 200 large-scale incidents were recorded, including the devastating "NotPetya" attack, with

[1] National University of Altiplano, Puno, Peru. Email: 75921149@est.unap.edu.pe, ORCID: https://orcid.org/0009-0008-4686-0563.
[2] National University of Altiplano, Puno, Peru. Email: 77022006@est.unap.edu.pe, ORCID: https://orcid.org/0009-0005-9343-2295.
[3] Universidad Nacional del Altiplano, Puno, Peru. Email: 76546319@est.unap.edu.pe, ORCID: https://orcid.org/0009-0006-6384-8174
[4] National University of Altiplano, Puno, Peru. Email: rromero@unap.edu.pe, ORCID: https://orcid.org/0000-0002-6144-9309 (Corresponding Author)
[5] National University of Altiplano, Puno, Peru. Email: hygomez@unap.edu.pe, ORCID: https://orcid.org/0000-0002-8627-412X
[6] National University of Altiplano, Puno, Peru. Email: rgiovana.flores@unap.edu.pe, ORCID: https://orcid.org/ 0000-0003-0240-647X
[7] National University of Juliaca, Puno, Peru. Email: wlvelasquezv.doc@unaj.edu.pe, ORCID: https://orcid.org/ 0000-0001-6945-4260

estimated losses of 10 billion U.S. dollars (QBE, 2024).

The frequency and sophistication of cyber threats are constantly evolving. Globally, an average of 2,200 cyberattacks occur daily, equivalent to one every 39 seconds (Jain, 2025). Among these, ransomware has emerged as the most prevalent threat, representing approximately 70% of global attacks and affecting strategic sectors and essential services (Petrosyan, 2025; VikingCloud, 2025). Likewise, the average cost of a data breach rose to 4.88 million U.S. dollars in 2024, highlighting the growing effectiveness and sophistication of these attacks (VikingCloud, 2025; Fox, 2024). Although this is a global-scale problem, its regional impact is equally significant. In Peru, for example, more than 45 billion cyberattack attempts were reported in 2024 alone (Infobae, 2025). This reality has resulted in high-profile incidents that have severely undermined trust in institutions. A relevant case was the massive data breach in the public sector, which compromised national security by exposing critical vulnerabilities in state infrastructures (Infobae, 2024). Similarly, the leak of personal and financial information of more than three million Interbank customers revealed the fragility of banking systems in the face of current threats (Infobae, 2024).

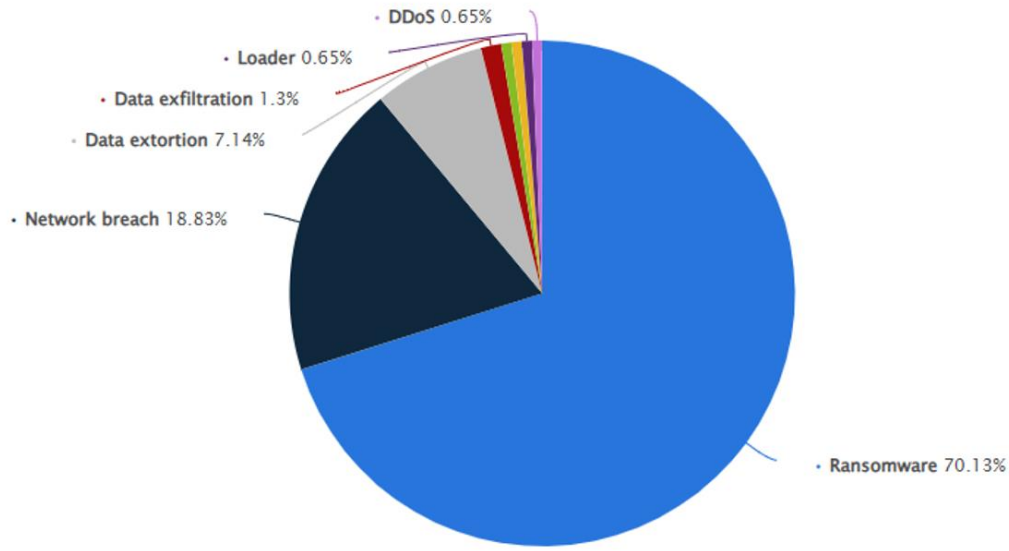

Figure 1 Distribution of Detected Cyberattacks Worldwide In 2023, By Type (Petrosyan, 2025)

This context reveals an urgent gap in specialized cybersecurity training. Despite the growing level of threat, teaching methods often focus on theoretical approaches or virtual environments that lack dynamic visual components (Alnajim, Habib, Islam, Saleh AlRawashdeh, & Wasim, 2023). Such limitations reduce students' ability to understand and anticipate the mechanisms of malware propagation in real networks.

In response to this need, the present study proposes an innovative pedagogical model based on the interactive simulation of malware propagation (Khattak et al., 2024). The main objective of this research is to develop and validate an educational tool that integrates a hybrid threat detection framework with real-time graphical visualization. This tool seeks to strengthen practical cybersecurity training, enabling students not only to identify different types of malware but also to understand their propagation dynamics in simulated network environments.

This approach emphasizes the use of visual and interactive environments as effective resources for teaching, integrating theoretical foundations with observable and practical experiences.

Educational Simulators and Game-Based Environments in Cybersecurity

In both literature and practice, there are numerous serious games and simulators with pedagogical purposes in cybersecurity. For example, the Hackend simulator is presented as a "serious game" in the form of a graphic adventure, where students learn business security concepts while helping a character chase cybercriminals. Similarly, CyberCIEGE —originally developed by the U.S. Navy— is an interactive network simulation video game in which the user must acquire and configure workstations, servers, and network devices in a business environment, balancing budget, productivity, and security.

In CyberCIEGE, players can observe in real time how their decisions —such as installing firewalls, VPNs, or authentication systems— affect the resilience of the network against simulated attacks. These serious games provide visual environments and interactive challenges to illustrate good security practices, although their didactic scope is generally limited to basic concepts of protection and awareness. In particular, they rarely incorporate advanced technical components, such as malware detection algorithms, and instead focus on creating narrative learning situations or game-based mechanics —for example, keeping a network safe— without internally modeling the actual propagation of a threat.

Likewise, there are learning platforms based on wargames and virtual labs that simulate attacks or hacking challenges in a practical way. OverTheWire, for instance, is a free online "wargame" platform where each level presents a different scenario requiring cybersecurity skills to solve sequential challenges. Similarly, TryHackMe offers guided virtual labs where users explore simulated environments —networks, servers, services— and complete step-by-step ethical hacking or cyber defense missions. These platforms emphasize structured practices and controlled tests, ideal for learning attack and defense techniques, but they do not integrate an automatic threat detection system. Instead, the focus is on manual experimentation, such as scanning for vulnerabilities or configuring defenses, rather than observing the behavior of a malware detection algorithm.

Educational games aimed at awareness and the general public have also been developed. Google, for instance, created SpaceShelter and Interland, mini-games designed for young users to promote safe habits, while INCIBE offers CyberScouts, a set of interactive games with different levels of difficulty that assess basic security knowledge. Although these initiatives provide attractive and accessible interfaces aimed at initial training, they are mainly closed learning experiences —organized by levels or missions— and not continuous simulation environments.

References	Year	Domain	Description
Anit-Phishing Phil [42]	2007	Cybersecurity education	An online game for teaching how to notice unusual URLs to avoid phishing cyberattacks
CyberCIEGE [43]	2007	Cybersecurity training	An interactive video game for security training
Hernandez et al. [44]	2011	Cybersecurity training	An advanced simulator for CS training
Control-Alt-Hack [45]	2013	Cybersecurity training	A computer security board game for learning computer security
Le et al. [46]	2015	Cybersecurity training	A serious game for CS training
CyberAware [47]	2015	Cybersecurity training	Cybersecurity mobile game for conveying cybersecurity concepts to K–6 level students
Cyber Security Defender [48]	2015	Teaching about cyberattacks	Cyber Security Defender game is used to teach about cyberattacks caused by viruses and hackers
Gestwicki and Stumbaugh [49]	2015	Cybersecurity education	Reviewed about 20 games on cybersecurity education
Nicho et al. [50]	2017	Cybersecurity training	A serious game model for organizations to substantially enhance computer users' cybersecurity awareness
Sorace et al. [51]	2018	Cybersecurity survey	Survey of 181 games related to cybersecurity
The Cyber Wellness and Cyber Security Awareness [52]	2018	Cybersecurity awareness	The Cyber Wellness and Cyber Security Awareness game is used to teach nine (9) types of security awareness to users
Katsantonis et al. [53]	2019	Cybersecurity training	PeriHack is a board and card game simulating the struggle between a team of attackers and a team of defenders
Hill et al. [54]	2020	Cybersecurity survey	A review of 20 serious games for teaching cyber security at various levels
Jaffray et al. [55]	2021	Cybersecurity training	SHERLOCKED is a serious 2D top-down detective adventure game for supporting further engagement
Van et al. [56]	2021	Cybersecurity training	A serious cybersecurity game applicable for CS training
Filippidis et al. [57]	2022	Cybersecurity training	An interactive book and board game for optimizing learning procedures and understanding in an entertaining way
Cloud Defense [58]		Teaching the security protocols of Amazon Web Services (AWS)	A Cloud Defense game is used to teach the security protocols of Amazon Web Services (AWS)

Figure 2 Cybersecurity Training Games (Alnajim, Habib, Islam, Saleh Alrawashdeh, & Wasim, 2023)

Professional Platforms and Advanced Simulators

Beyond purely educational or gamified environments, there are complex simulators aimed at professional training. A notable example is the simulator developed by Indra in 2011: a sophisticated virtual network for training in prevention, detection, and response to cyberattacks, which includes forensic analysis and "cyberwar" scenarios. Another relevant case is the commercial cyber ranges, such as those from SANS Cyber Ranges, which replicate real networks with servers, devices, and applications in isolated environments for intensive training exercises. These systems allow security teams to practice complex attacks and defense tactics without affecting real systems. While highly comprehensive including realistic network scenarios and updated attacks— their complexity and cost are considerable; they generally require specialized licenses or dedicated infrastructure, making them suitable for companies or military and high-level academic institutions, rather than for everyday use by students.

Another professional example is Infection Monkey (by Akamai/Guardicore), an open-source adversary simulation platform that installs on a networked machine and simulates an attack that automatically "jumps" across the infrastructure, analyzing infection paths and generating detailed vulnerability reports. Infection Monkey visualizes the real propagation of malware in a corporate network —such as credential theft and lateral movement— but its interface and documentation are aimed at security engineers, not as an accessible pedagogical tool for general audiences. In summary, these advanced platforms incorporate detailed simulation of networks and real attacks, but they are specialized modules, not comprehensive educational tools, and they lack explicit pedagogical integration —such as guided tutorials, game-like elements, or learning metrics. This limitation has been similarly highlighted by (Chouliaras, y otros, 2021), who note that while cyber ranges provide realistic environments for research and professional training, their infrastructure requirements often limit accessibility for regular classroom education.

Mathematical models and simulation prototypes of malware propagation in networks have also been developed. For example, (García Reyes, López Chau, Rojas Hernández, & Guevara López, 2016) present a desktop application developed in Java that simulates malware propagation according to realistic parameters —number of users, infected machines, among others. This platform allows step-by-step execution of the infection dynamics and shows graphs of the resulting propagation, which facilitates understanding the epidemic phenomenon of malware. However, it is a research prototype with a basic interface, useful for academic analysis, but not an interactive educational product. Similarly, epidemiological models applied to computer viruses —such as those based on differential equations or agents— have been studied, although they are usually presented in academic papers or through tools not designed for end users. In other words, although propagation simulators exist —some with visualization— none constitute a complete didactic environment that combines a modern interface with guided explanations and a structured pedagogical approach.

System Design

The system developed integrates two main components in a coordinated manner: a hybrid detection module and an interactive visual simulation. The first combines static and dynamic techniques to identify both known malware and emerging threats, while the second reproduces, in a three-dimensional graphical environment, the propagation of attacks across a virtual network.

In the simulation, each node represents a device or server, with color-coded states (green, yellow, red) indicating different levels of exposure or compromise. This environment allows users to dynamically observe how a threat originates, spreads, and is contained, integrating defensive response in real time. The architecture is modular and scalable: both components operate independently but share an event and detection database, ensuring consistency between technical analysis and its visual representation.

From a pedagogical perspective, the design fosters situated and constructivist learning, in which students not only understand the theory but also interact with a context that emulates the real conditions of a cyberattack. This strengthens their ability to interpret, anticipate, and respond to security incidents (Adeboye Popoola, Oladipo Akinsayan, Nzeako, G. Chukwurah, & Okeke, 2024).

Technologies Used

To implement the system, tools were selected that combine efficiency, compatibility, and graphical capability:

C++: chosen for its performance and low-level control, essential for fast analysis and efficient memory management.

WinAPI: to interact directly with the Windows operating system, enabling process monitoring, file system access, and digital signature validation.

OpenGL: for real-time visualization, providing smooth animations and an intuitive graphical representation of the network's state.

This combination allows the system to maintain high performance even during large-scale simulations, without sacrificing interactivity or visual clarity.

Detection Module

The detection module integrates three complementary techniques:

1. SHA-256 Signature Scanning: a widely adopted technique in the cybersecurity industry due to its high accuracy in identifying previously cataloged threats (Rodríguez Galiano, 2015). This method generates a unique digital fingerprint for each file and compares it with a database of malicious samples, enabling fast detection with low computational cost.

2. Heuristic Analysis: allows the identification of anomalous behavior patterns even in previously unknown malware, which increases detection capacity against polymorphic and metamorphic variants (Fortinet, s.f.; Kaspersky, s.f.).

3. WinTrust API Verification: a mechanism provided by Microsoft to validate the integrity and authenticity of executable files, used as a preventive measure against the execution of untrusted binaries (Learn, 2021).

This hybrid approach, widely supported in the literature, balances precision and adaptability, reducing false negatives and improving response capacity against unknown threats.

Visual Simulation Module

The visual simulation module serves as the system's main interface, clearly and dynamically displaying the behavior of an attack within a network. The graphical representation presents a network of interconnected nodes, where each node changes color according to its state: green for secure nodes, yellow for those under observation, and red for compromised nodes.

Malware propagation is modeled through timed events that update the states based on active connections between nodes. This approach allows real-time visualization of how a security incident can rapidly escalate if timely measures are not taken. Additionally, the user can modify key parameters—such as propagation speed, node resistance level, or the introduction of new infections—turning the experience into an interactive exercise of exploration and adaptive analysis.

Various studies have shown that interactive simulations not only enhance conceptual understanding of cybersecurity phenomena but also improve student motivation and knowledge retention (Samir Rane, O. Gupta, & Gowalker, 2025; Sudhakaran, Ambadas More, Meher, & Raj Panakkadan, 2025). In this context, the visual representation transforms technical and abstract processes into an intuitive visual language, facilitating the construction of meaningful knowledge and promoting deeper, applied learning.

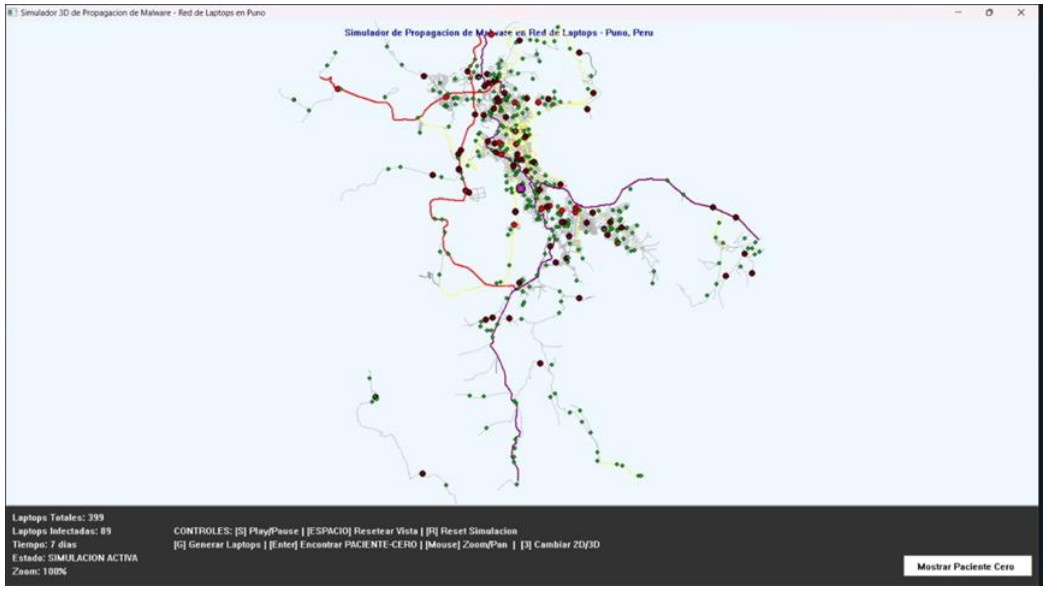

Figure 3: Simulator on a 2D map of Puno, Peru.

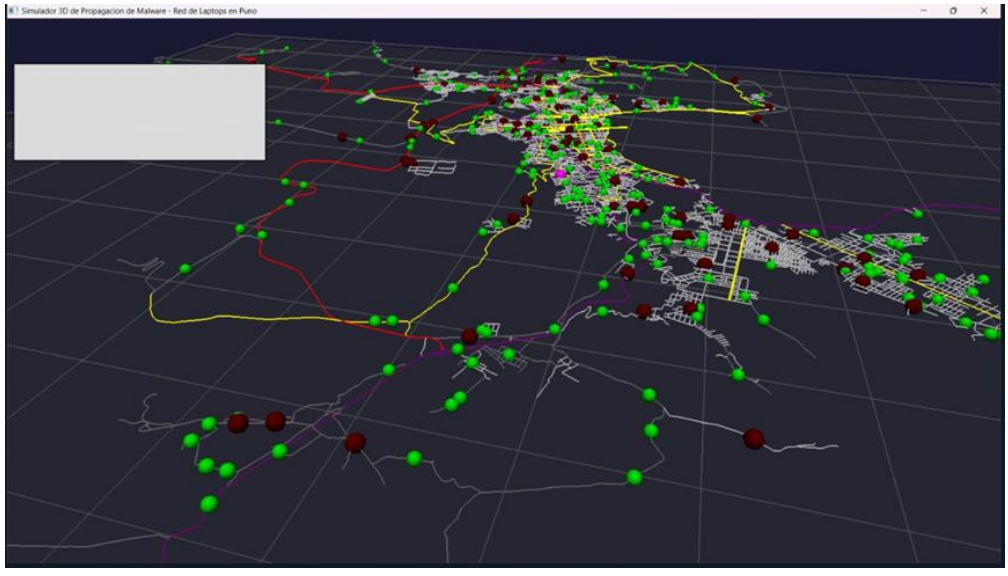

Figure 4: Three-Dimensional View of the Simulator, Showing the Network of Nodes In 3D.

The simulator also incorporates a three-dimensional view that provides a comprehensive perspective of the network topology. This 3D representation allows exploration of the nodes and their interconnections from multiple angles, revealing propagation patterns and critical vulnerability points that may remain hidden in a two-dimensional visualization. This capability is particularly valuable for understanding how connection density and network structure influence the speed and scope of an infection.

The ability to rotate, zoom, and examine the network from different perspectives substantially enriches the analysis, making it easier to identify preferred propagation paths and assess the

overall resilience of the system. This feature reinforces the pedagogical value of the tool, transforming abstract concepts of network topology and infection dynamics into tangible, explorable visual experiences.

Testing and Evaluation

The tests were conducted in a controlled environment, completely isolated from external networks to ensure security and reproducibility of the results. The test set included both benign, commonly used files as well as real malware samples that had been previously deactivated, obtained from specialized educational repositories.

For the evaluation, key metrics such as detection rate, false positive percentage, and response time were measured. The results demonstrated solid performance: a high detection rate, a level of false positives within acceptable parameters, and analysis times that allowed for smooth interaction with the system.

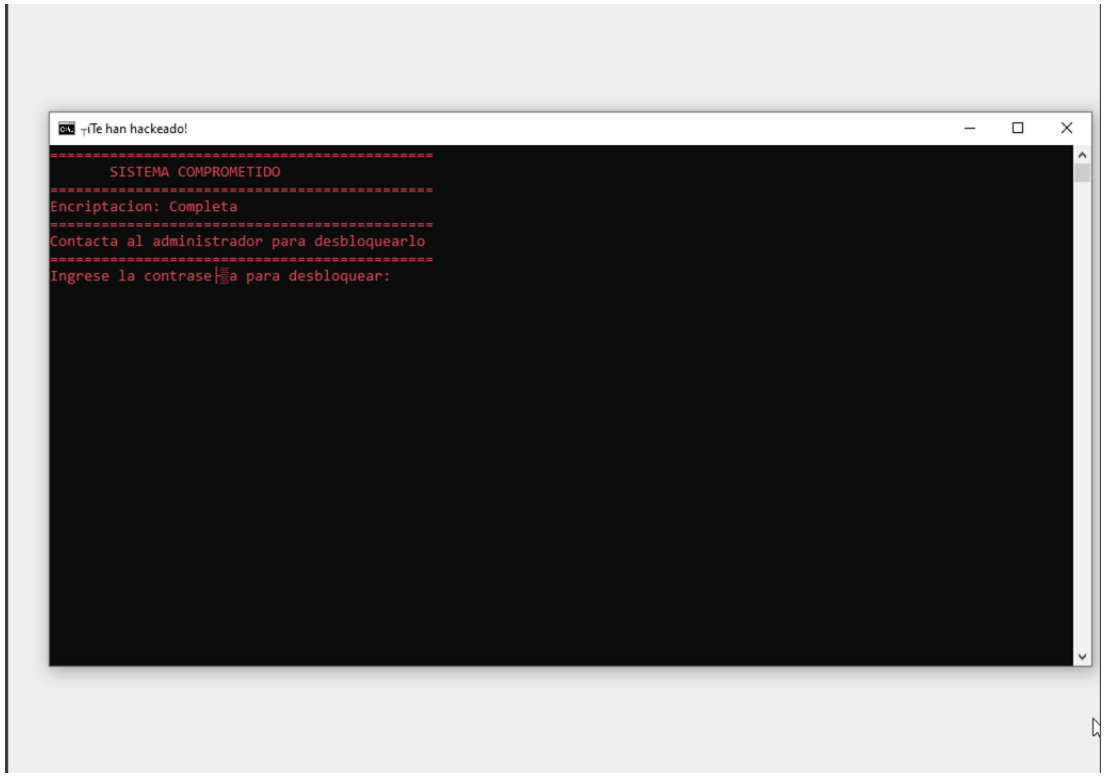

Figure 5: Ransomware Virus Running and Hijacking the System - Executed on A "Virtual Box" Virtual Machine

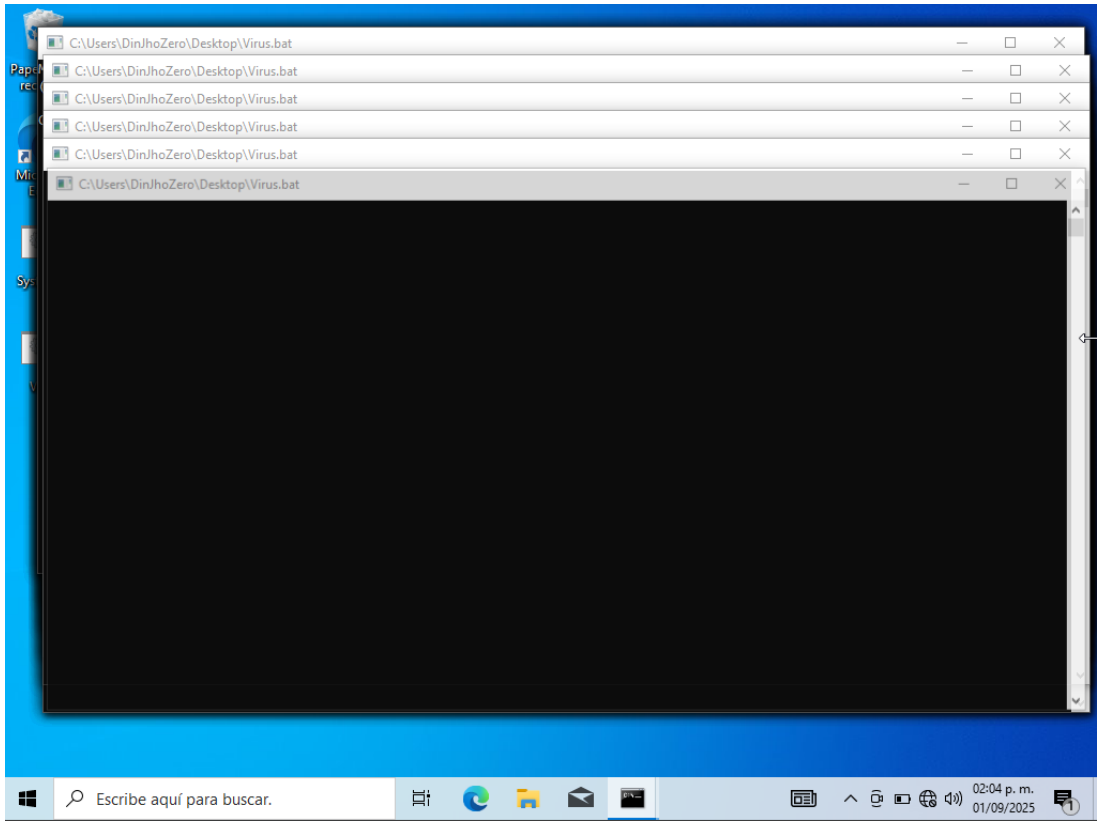

Figure 6: Typical Virus That Creates Multiple Windows Until the Computer Is Saturated, Running - Executed in A "Virtual Box" Virtual Machine.

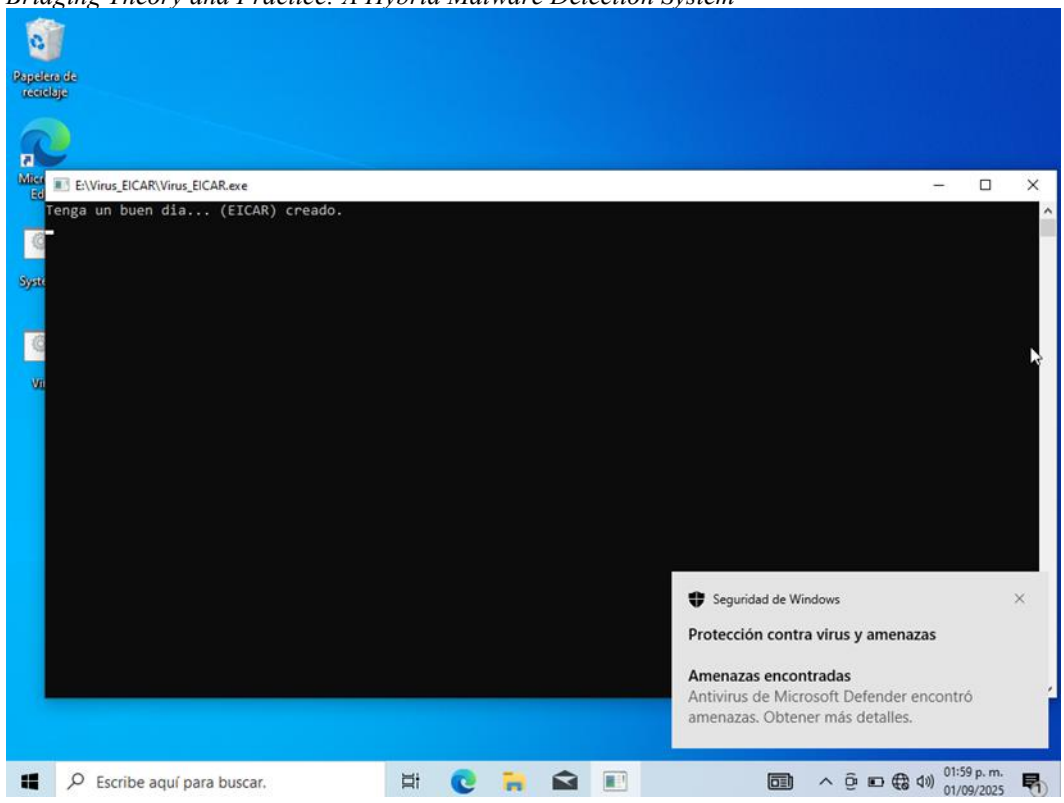

Figure 7: Windows Defender Detects the EICAR Virus Used for Antivirus Testing. It Is Running on the Virtual Machine 'Virtual Box'

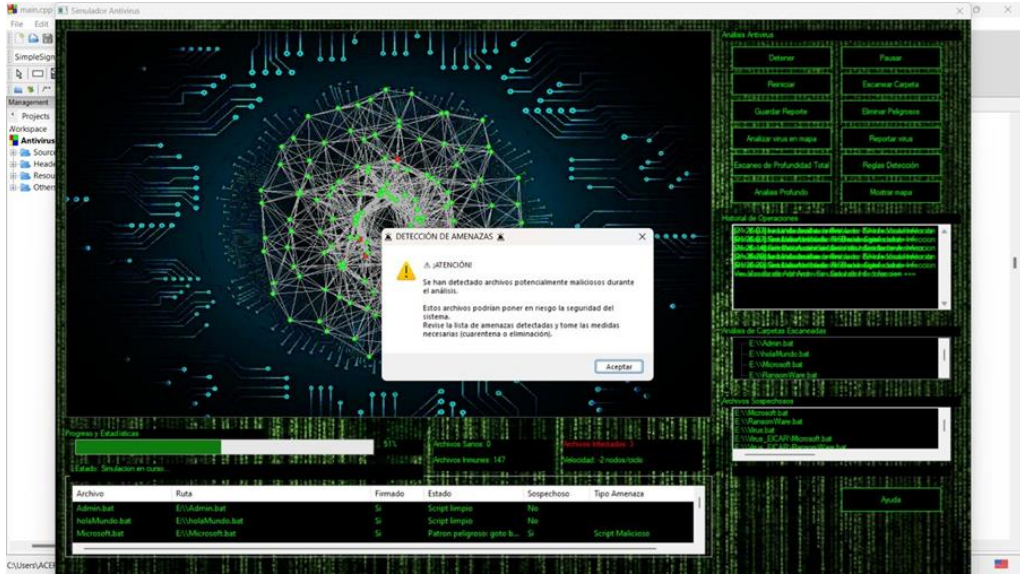

Figure 6: Antivirus Detecting Simulated Threats in Real Time.

Although the initial results are encouraging, it is important to recognize that laboratory tests do not fully replicate the complexity and pressure of real-world environments. In the next phase of research, evaluations are planned in operational scenarios with real traffic and human users, which will allow measurement of scalability, performance under load, and effectiveness against more sophisticated threats. This step is crucial to validate the applicability of the system in professional and high-risk educational contexts.

Parameters Used in the Simulation

The simulation developed in this work was designed with a high degree of flexibility, allowing the adjustment of multiple parameters that control both malware propagation behavior and the user's visual and interactive experience. This configurability ensures that the system can adapt to various contexts, maintaining experiment reproducibility and relevance in different study scenarios.

The main configurable parameters include:

1. Number of nodes in the network: Sets the total number of simulated devices or machines. Increasing this value raises the complexity and realism of the simulation, allowing analysis of malware behavior across networks of different scales.

2. Connection topology: Defines the structure of the network, whether it is a full mesh, star, or with random connections. This variable directly influences the pattern and speed of attack propagation.

3. Propagation speed: Determines the time required for malware to spread from an infected node to its neighbors. Adjusting this makes it possible to simulate extremely fast infections — such as those caused by worms— or more discreet and prolonged attacks.

4. Infection rate: Indicates the probability that a susceptible node will become infected upon contact with a compromised one. This allows modeling of both highly contagious threats and variants with lower propagation capacity.

5. Detection probability: Represents the effectiveness of the simulated defensive system (antivirus, firewall). A higher value translates into greater containment of the threat and a smaller impact on the network.

6. Recovery rate: Defines the percentage of nodes that, after being compromised, successfully eliminate the threat and return to a safe state. This parameter is key to evaluating the effectiveness of mitigation and response measures.

7. Visualization method: Allows switching between different display modes —2D plane, grid, or radial view— using a specific color code for each state: green for safe nodes, red for infected, and yellow for quarantined.

8. Simulation iterations: Controls the duration of the experiment by defining the total number of cycles to be executed before concluding. This value also determines the amount of data collected for subsequent analysis.

9. Random seed: Assigns a numerical value that ensures reproducibility of results, allowing scenarios to be repeated under the same initial conditions.

The interaction between these parameters provides the system with a wide margin of customization, making it valuable both as an educational tool and as a research environment.

Thus, it is particularly useful for studying threat behavior, validating defensive strategies, and training in cybersecurity.

Simulation Procedure

The simulation process was designed to follow a clear and orderly sequence, in which each stage contributes both to visual coherence and to the accuracy of the network behavior representation. Although it is a controlled and simplified environment, the design seeks to realistically emulate how malware might spread. The general flow unfolds in the following stages:

1. IParameter Initialization: The system begins by loading all user-defined values (number of nodes, network topology, infection and recovery rates, among others). If a random seed is set, it is applied to ensure results can be reproduced in subsequent experiments.

2. Network Generation: Based on the chosen topology, the structure of nodes and links is built. Each node is assigned an initial state (safe by default) and is visually represented in the interface.

3. Initial Infection: One or more nodes are designated as the starting point of the attack. This choice can be manual —when a specific scenario is to be simulated— or random, if general behaviors are to be explored.

4. Propagation through Iterations: The contagion dynamics unfold in successive cycles, during which:

a) Infected nodes attempt to transmit malware to their neighbors, according to the infection rate and propagation speed established.

b) Receiving nodes apply the detection probability to decide whether to block the attack or become compromised.

c) Previously infected nodes evaluate their chance of moving to a recovered state, depending on the configured recovery rate.

5. Visual Update: At the end of each iteration, the graphical representation is updated, assigning colors according to the state of each node (safe, infected, quarantined). This enables real-time tracking of the outbreak's evolution.

6. Data Logging: In parallel, metrics such as the number of infected, recovered, and safe nodes in each cycle are collected, providing a quantitative basis for analysis.

7. Termination: The simulation concludes when the maximum number of iterations is reached or when the infection either disappears completely or spreads to all nodes in the network.

8. Result Analysis: As a final step, the system generates graphs and tables summarizing the evolution of the attack, allowing scenario comparison and the extraction of conclusions.

Thanks to this procedure, the simulation not only functions as a visual resource to understand malware propagation dynamics but also becomes a robust tool for controlled experimentation and comparative evaluation of defensive strategies.

Potential and Development

The system was developed following a modular and scalable approach, which made it possible to organize and isolate critical functions, facilitating both its initial implementation and future

expansion. This approach allowed each component to evolve independently and adapt to new requirements. In this process, several key stages were identified and executed:

Propagation model design: A set of mathematical and logical rules was established to define malware behavior within a simulated network. In this phase, variables such as infection speed, identification of vulnerable nodes, and the most probable propagation paths were considered.

Simulation engine implementation: Using a programming language optimized for graph processing, a core engine was developed to dynamically represent the evolution of an attack. This engine updates the state of each node in real time, accurately reflecting the changes caused by propagation.

Graphical User Interface (GUI): An interactive visualization was incorporated to facilitate clear and understandable tracking of the infection. The interface allows users to pause, restart, or modify simulation parameters, offering direct control over the experience.

Validation and testing: Experiments were conducted with various network scenarios and different threat levels, in order to evaluate the accuracy of the system and its ability to reproduce realistic conditions. These tests helped fine-tune parameters and optimize the simulator's performance.

In terms of potential, the system demonstrates remarkable adaptability to different environments and needs. Possible extensions and improvements include:

- Incorporation of artificial intelligence algorithms to anticipate attack patterns.
- Capability to simulate large-scale distributed environments.
- Connection with real-time threat databases.
- Development of modules to evaluate cybersecurity policies.
- Automatic report generation with key metrics.
- Use as a training platform in academies, universities, and research centers.
- Utilization as a testing ground for new detection and response solutions.
- Integration with IoT hardware to evaluate security in physical devices.
- Multi-user support to enable collaborative practice sessions.

These qualities establish the tool as a solid foundation for specialized training in cybersecurity, academic research, digital forensics, and risk assessment. Its relevance is especially significant in contexts where equivalent solutions are not available, as is the case at the national level.

Main Contributions

This work introduces substantial and innovative contributions in the field of malware detection and propagation visualization, combining a hybrid analysis model with an interactive graphical representation. These advances, rarely found in current studies and tools, are described below:

First, a hybrid detection model has been developed that integrates SHA-256 signature scanning, advanced heuristic analysis, and validation through the WinTrust API. This combination makes it possible to identify both known threats and emerging variants, thus overcoming the limitations of systems that rely solely on signatures.

Second, an interactive visual simulation has been implemented, capable of representing malware propagation across a network of interconnected nodes. The visualization displays in real time the state of each node (infected, safe, or quarantined) through an intuitive color-coding system, which facilitates the interpretation of results.

Another key contribution is the educational and formative focus incorporated into the system's design. The tool is oriented toward cybersecurity teaching and malware analysis in academic environments, making it possible to explain complex concepts through practical and visual simulations.

Additionally, lightweight and portable software has been prioritized, developed in C++ with WinAPI and OpenGL, optimizing resource consumption and ensuring high performance even on hardware with limited capacity.

The system also offers notable scalability of scenarios, allowing adjustment of parameters such as the number of nodes, propagation speed, or infection resistance. This makes it adaptable to both small networks and large-scale simulations.

Regarding its local relevance, this is one of the first projects of its kind developed in Peru, where the availability of specialized academic tools in cybersecurity remains limited. Thus, this proposal represents a significant step toward strengthening cybersecurity education at the regional level.

Finally, the system is conceived as a foundation for future research, with an architecture that facilitates the incorporation of new modules, such as AI-based detection, behavioral analysis, or real-time distributed monitoring.

Taken together, these contributions position the proposal not only as an efficient technical solution but also as a comprehensive pedagogical and research tool, capable of combining theory, practice, and visualization for the study of cybersecurity.

Comparison and Relevance of the Proposal

The analysis of existing tools reveals varied approaches, although in most cases they only cover partial aspects compared to what this project proposes. Our proposal integrates, in a comprehensive way, a hybrid malware detection model with a visual simulation of its network propagation, introducing a distinctive value. The main differences can be summarized as follows:

- Educational and technical focus: Many serious games, such as Hackend, CyberCIEGE, or OverTheWire, are oriented toward teaching concepts or solving specific cybersecurity tasks. On the other hand, professional and academic simulators reproduce real network environments but with less emphasis on learning guidance. The proposal integrates both worlds: an interactive and educational space, similar to a game, but with real components of security analysis and response.

- Propagation visualization: Although there are tools such as Infection Monkey that show how malware spreads in a network, they are not designed for everyday didactic use nor do they include guided activities. In this project, pedagogical visualization is key: the student can observe in real time how malware jumps between nodes and how the detection system reacts, all within an interactive environment designed specifically for learning.

- Hybrid detection model: None of the reviewed simulators incorporate an advanced

internal detection engine. Games like CyberCIEGE or wargames focus on defensive configuration, but they do not execute real code or behavior analysis. Even in professional environments, an educational detection module is absent. In contrast, this proposal integrates a hybrid system (static analysis, heuristic analysis, and cryptographic verification) that allows the user to observe and compare malware propagation with its detection in real time.

- Balance between complexity and accessibility: Commercial and research platforms are often complex to install and operate, requiring real networks or specialized software. Educational games, on the other hand, are simpler but less realistic. The proposed system seeks a middle ground: more realistic and interactive than a gamified questionnaire, but more intuitive and faster to use than a professional cyber range, enabling classroom or laboratory iterations without technical barriers.

In summary, there is currently no tool that simultaneously brings together the three key characteristics of this project: hybrid malware detection, visual simulation of network propagation, and didactic orientation for frequent use. Existing solutions are divided among gamification, basic awareness, professional technical simulation, or propagation models for research purposes. This gap validates the relevance and innovation of the proposal, which positions itself as a bridge between traditional educational simulators and advanced cybersecurity training environments.

Results

During the evaluation phase, the system was subjected to tests in three key areas:

1. Effectiveness of the detection module: Initial tests show that the hybrid detection engine —based on signature analysis, advanced heuristics, and cryptographic verification— successfully identifies potentially malicious files with high accuracy. The results are presented in tables and graphs that include metrics such as precision, recall, and F1-score, which allow visualization of the balance between true positives and false positives.

2. Impact of visual simulation: The graphical interface proved effective in representing malware propagation across the network. Screenshots and diagrams included in the appendix show how nodes change state (healthy, infected, immune) in real time, enabling users to understand propagation dynamics that are normally described only in abstract terms.

3. Performance analysis: Measurements of detection speed and resource consumption indicate that the system maintains a balance between accuracy and efficiency. Even in scenarios with multiple infection events, response times remained within acceptable margins for use in educational settings.

Discussion

1. Interpretation of findings: The results confirm that a hybrid detection approach — combining signature analysis, advanced heuristics, and cryptographic verification— can identify potentially malicious files with high accuracy, even in controlled environments. However, the true value of the project becomes evident when incorporating the visual simulation. This component transforms a complex and abstract process into a clear and engaging experience. Seeing how a node transitions from “healthy” to “infected,” and eventually to “immune,” generates an almost instant understanding of propagation dynamics —something difficult to achieve with text or static diagrams.

This type of visual resource aligns with research highlighting how graphical representations enhance knowledge retention and facilitate the assimilation of complex technical processes (Gonzáles Torres, Hernández Campos, González Gómez, L. Byrd, & Parsons, 2020). The experience of "seeing to understand" acts as a bridge between theory and practice, increasing user motivation and their willingness to explore more advanced concepts.

2. Comparison with existing literature: Although the use of simulated and interactive environments in cybersecurity education is not new, it remains an expanding field. Recent studies show that direct interaction with a simulated system increases confidence and reduces anxiety when facing complex problems, especially in beginner students (Raj Panakkadan, Meher, Ambadas Más, & Sudhakaran, 2025). In our case, users not only observe malware propagation but can also modify parameters and trigger new infection events, thus fostering active and experimental learning.

Furthermore, visualization acts as a universal language that transcends technical and linguistic barriers. Regardless of prior knowledge, the visual transitions between states —colors, connections, reaction times— convey the core message without requiring extensive technical explanations. This makes the tool useful both for university students and for non-specialized audiences seeking to acquire basic cybersecurity knowledge.

3. Theoretical and practical implications: From a theoretical perspective, the system represents a solid example of how to apply principles of situated learning and constructivism to cybersecurity education. Situated learning holds that knowledge is more effectively acquired when contextualized in scenarios that mimic real situations. In this case, the user faces an environment simulating a network attack, requiring them to put concepts into practice in a realistic context.

From a practical perspective, the system is scalable and adaptable, making it suitable for use in university courses, graduate programs, corporate training, or even public awareness campaigns. Beyond teaching how to detect malware, the goal is to cultivate a culture of prevention and response to incidents.

4. Study limitations: Although the results are encouraging, the system presents limitations worth noting. The tests were carried out with a small set of files, under controlled conditions, and without the unpredictability of a real attack, which limits the generalization of results. Likewise, the propagation parameters used in the simulation were not based on real statistical data but on arbitrary values. Finally, the lack of testing with students prevents precise evaluation of the educational impact in terms of knowledge retention, motivation, and skill development.

Conclusions

1. Summary of key findings: The system developed represents a significant step toward more visual, interactive, and effective cybersecurity education. The integration of a hybrid detection module with a visual simulation not only facilitates the understanding of complex technical processes but also sparks curiosity and user interest. The results show that, even with limited resources, it is possible to design educational environments that successfully bridge theory and practice in an attractive, intuitive, and accessible way.

2. Future directions: For the next stages, the most promising lines of development include:

- Expanding the test database by incorporating real malware samples and more complex scenarios, in order to assess system robustness.

- Adjusting simulation parameters using empirical data from real incidents, to provide a more representative and realistic experience.
- Conducting field studies with students and professionals to measure real impact on learning, confidence, and response capacity against threats.
- Exploring emerging technologies such as virtual or augmented reality, which could provide a higher level of immersion and realism.
- Integrating artificial intelligence algorithms that dynamically adjust scenarios and difficulty according to user performance, creating personalized learning experiences.

In summary, this project stands as a solid starting point for future initiatives that combine visualization, simulation, and interactive practice in cybersecurity education. In doing so, it contributes to the training of professionals better prepared to face the challenges of an increasingly complex and vulnerable digital environment.

References

Adeboye Popoola, O., Oladipo Akinsayan, M., Nzeako, G., G. Chukwurah, E., & Okeke, C. D. (2024). Exploring theoretical constructs of cybersecurity awareness and training programs: comparative analysis of African and U.S. Initiatives. International Journal of Applied Research in Social Sciences, 819-827.

Alnajim, A. M., Habib, S., Islam, M., Saleh AlRawashdeh, H., & Wasim, M. (2023). Exploring Cybersecurity Education and Training Techniques: A Comprehensive Review of Traditional, Virtual Reality, and Augmented Reality Approaches. MDPI.

Chouliaras, N., Kittes, G., Kantzavelou, I., Maglaras, L., Pantziou, G., & Amine Ferrag, M. (2021). Cyber Ranges and TestBeds for Education, Training, and Research. MDPI.

Delaere, C., Bouillet Carroza, E., & Armijo Catalán, J. (2025). Reporte ciberseguridad. entel digital.

Fortinet. (s.f.). ¿Qué es el análisis heurístico? Obtenido de Fortinet: https://www.fortinet.com/lat/resources/cyberglossary/heuristic-analysis

Fox, J. (23 de Diciembre de 2024). Top Cybersecurity Statistics for 2025. Obtenido de Cobalt: https://www.cobalt.io/blog/top-cybersecurity-statistics-2025

García Reyes, L. A., López Chau, A., Rojas Hernández, R., & Guevara López, P. (2016). Propagaci´on de malware: propuesta de modelo. México: Universidad Autónoma del Estado de México.

Gonzáles Torres, A., Hernández Campos, M., González Gómez, J., L. Byrd, V., & Parsons, P. (2020). Information visualization as a method for cybersecurity education. Innovations in Cybersecurity Education, 55-70.

Infobae. (14 de Noviembre de 2024). Robo de datos en Interbank al descubierto: así operó el hacker para extraer información de clientes del banco. Obtenido de Infobae: https://www.infobae.com/peru/2024/11/11/robo-de-datos-en-interbank-al-descubierto-asi-opero-el-hacker-para-sustraer-informacion-de-clientes-del-banco/

infobae. (22 de Mayo de 2025). Perú registró 45 mil millones de ciberataques en 2024: así puedes proteger tu pyme sin ser experto en tecnología. Obtenido de infobae: https://www.infobae.com/peru/2025/05/22/peru-registro-45-mil-millones-de-ciberataques-en-2024-asi-puedes-proteger-tu-pyme-sin-ser-experto-en-tecnologia

Jain, S. (25 de Junio de 2025). Astra. Obtenido de Astra: https://www.getastra.com/blog/security-audit/cyber-security-statistics/

Kaspersky. (s.f.). ¿Qué es un análisis heurístico? Obtenido de Kaspersky: https://latam.kaspersky.com/resource-center/definitions/heuristic-analysis

Learn, M. (10 de Diciembre de 2021). WinVerifyTrust function (wintrust.h). Obtenido de Windows App Development: https://learn.microsoft.com/en-us/windows/win32/api/wintrust/nf-wintrust-winverifytrust

Miliefsky, G. (13 de Marzo de 2025). The True Cost of Cybercrime: Why Global Damages Could Reach $1.2 – $1.5 Trillion by End of Year 2025. Obtenido de Cyber Defense Magazine: https://www.cyberdefensemagazine.com/the-true-cost-of-cybercrime-why-global-damages-could-reach-1-2-1-5-trillion-by-end-of-year-2025

Nisar Khattak, M., Al-Taie, M. Z., Ahmed, I., & Muhammad, N. (2024). Interplay between servant leadership, leader-member-exchange and perceived organizational support: a moderated mediation model. Journal of Organizational Effectiveness: People and Performance, 11(2), 237-261.

Petrosyan, A. (4 de agosto de 2025). Distribution of detected cyberattacks worldwide in 2023, by type. Obtenido de statista: https://www.statista.com/statistics/1382266/cyber-attacks-worldwide-by-type

QBE. (1 de Octubre de 2024). Annual global cyber-attacks double from 2020 to 2024: QBE. Obtenido de QBE: https://qbeeurope.com/news-and-events/press-releases/annual-global-cyber-attacks-double-from-2020-to-2024-qbe

Raj Panakkadan, R., Meher, P., Ambadas Más, S., & Sudhakaran, S. (2025). MEJORA DE LA EDUCACIÓN EN CIBERSEGURIDAD: EL IMPACTO DEL APRENDIZAJE SIMULADO Y LOS TUTORIALES INTERACTIVOS EN EL RENDIMIENTO ESTUDIANTIL Y LA REDUCCIÓN DE LA ANSIEDAD. 19ª Conferencia Internacional de Tecnología, Educación y Desarrollo, 1775-1784.

Rodríguez Galiano, D. (2015). • Educational and technical focus: Many serious games, such as Hackend, CyberCIEGE, or OverTheWire, are oriented toward teaching concepts or solving specific cybersecurity tasks. On the other hand, professional and academic simulators reproduce real netwo. Madrid: • Educational and technical focus: Many serious games, such as Hackend, CyberCIEGE, or OverTheWire, are oriented toward teaching concepts or solving specific cybersecurity tasks. On the other hand, professional and academic simulators reproduce real netwo.

Samir Rane, A., O. Gupta, R., & Gowalker, N. (2025). INTERACTIVE LEARNING IN CYBERSECURITY: A STUDY ON THE EFECCTIVENESS OF SIMULATION GAMES IN EDUCATING USERS. INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENSE (IJPREMS), 1220-1226.

Sema Admass, W., Yayeh Munaye, Y., & Abeshu Diro, A. (2024). Cyber security: State of the art, challenges and future directions. Cyber Security and Applications, 9.

Sudhakaran, S., Ambadas More, S., Meher, P., & Raj Panakkadan, R. (2025). ENHANCING CYBERSECURITY EDUCATION: THE IMPACT OF SIMULATED LEARNING AND INTERACTIVE TUTORIALS ON STUDENT PERFORMANCE AND ANXIETY REDUCTION. ResearchGate.

VikingCloud. (15 de Junio de 2025). 192 Cybersecurity Stats and Facts for 2025. Obtenido de VikingCloud: https://www.vikingcloud.com/blog/cybersecurity-statistics.