**Cyber Project Report:**

**Interactive Virus Simulator**

**Group Members:**

* Zaryab Ahmed 23K-2044
* Tamseel Khanzada 23K-2063

**Title:**

**Interactive Virus Simulator:**

**Understanding Malware Through Experience**

* **Objective**

This project intends to develop an interactive virus simulator designed to mimic the behavior of various types of malicious software. Its primary objective is to educate users about the potential dangers associated with interacting with unfamiliar pop-up advertisements and notifications. By simulating realistic scenarios, the project will illustrate how seemingly innocuous actions—such as clicking on a harmless-looking link or downloading an attachment—can lead to severe consequences, including data loss, system disruptions, or identity theft.

Through this immersive experience, users will not only witness the immediate effects of their choices but also understand the underlying mechanisms of malware and its various forms. By highlighting different malware behaviors, such as ransomware, spyware, and adware, the simulator aims to foster a deeper awareness of cybersecurity issues. Ultimately, participants will leave with improved skills in recognizing threats and making informed decisions to protect themselves in the digital world.

* **Overview**

The simulator is designed to generate random pop-up messages that closely mimic genuine system alerts, creating an authentic user experience. When users engage with these pop-ups, the simulator randomly activates two distinct virus-like modules, which are engineered to replicate the unpredictable and chaotic behavior commonly associated with real-world malware attacks.

This project serves a dual purpose: it not only aims to showcase the impact of malware on both system performance and user experience but also seeks to underscore the critical importance of maintaining good cyber hygiene practices. By illustrating how easily users can fall victim to deceptive alerts and how such interactions can lead to performance degradation or system compromise, the project highlights the need for awareness and proactive measures in digital security. Through this simulation, participants can better understand the potential threats posed by malware and how to protect themselves in an increasingly digital world.

* **Key features include**
* **Engaging Random Pop-ups:** This feature utilizes carefully crafted random pop-ups to effectively simulate common social engineering tactics, challenging users to recognize and respond to potential security threats.
* **Variety of Virus Modules:** The program includes five distinct virus modules that replicate the behaviors of real malware. These modules create a realistic environment by generating endless pop-ups, causing erratic mouse movements, triggering random application launches, flashing the screen intermittently, and executing keyboard spamming.
* **Windows Compatibility:** Designed specifically for Windows systems, this tool ensures seamless integration and operation across various versions, making it accessible for a wide range of users.

Virus behaviors are implemented through two distinct programs:

* **Virus 2:** Operates on Windows and manages communication with a virtual machine (VM)
* **Virus 3:** Executes specific modules directly on the VM, leveraging randomized activation mechanisms for unique disruptions in each run
* **Features**
* **Initial Virus Modules**

1. **Endless Pop-ups:** Generates continuous alert windows to mimic spam
2. **Random Mouse Movement:** Moves the cursor randomly across the screen
3. **Application Launcher:** Opens system applications (e.g., Notepad, Calculator) at random intervals
4. **Screen Flashing:** Mimics display corruption through rapid color changes
5. **Keyboard Spam:** Simulates input interference by generating random keystrokes

* **Random Activation Mechanism**  
  Each user interaction triggers two random modules, creating unpredictable behavior. This randomness ensures an engaging and chaotic user experience.
* **Technologies and Tools**
* Programming Language: C++
* Operating System: Windows
* Libraries: Windows API (pop-ups, cursor manipulation, app launching), Winsock2 (communication between systems)
* Development Design: Modular, allowing for seamless integration of future virus modules
* **Implementation Details**

**Virus 2: Windows-based Controller**

* Establishes a socket connection utilizing Winsock2 to communicate commands to the virtual machine (VM).
* Please note that the implementation of socket programming is informed by reputable external sources, including GitHub and ChatGPT.
* Prompts the user for input and transmits commands to initiate specific virus modules on the virtual machine.
* Functions as the primary interface for managing the execution of modules on the virtual machine.
* **Key Code Features:**
* Establishes TCP connections with the VM (IP: 192.168.18.245, Port: 8080)
* Handles command input and error detection for seamless communication
* **Sample Interaction:**

1. User enters a command (e.g., "mouse")
2. The command is sent to the VM for execution

**Virus 3: Virtual Machine Executor**

* Executes the virus modules activated by Virus 2, which were independently designed and developed by the project team.
* Incorporates a range of behaviors, including the launching of websites, mouse movement, application initiation, screen flashing, and keyboard input disruption.
* Employs a randomized methodology to maintain an element of unpredictability in the disruptions created.
* **Key Code Features:**
* Functions for each behavior module (e.g., openRandomWebsites, randomMouseMovement)
* Uses Windows API functions (e.g., SetCursorPos, SendInput) for low-level system manipulations
* Handles network communication to receive and execute commands from Virus 2
* **Purpose**
* **Awareness**

1. Provides comprehensive education to users regarding the potential risks associated with engaging with suspicious alerts, helping them recognize signs of phishing or malware threats.
2. Illustrates the severe and disruptive consequences that malware can cause to both individual and organizational systems, thereby emphasizing the critical importance of maintaining cautious online behavior and adhering to cybersecurity best practices.

* **Exploration**

1. Delivers in-depth insights into the behavior of various types of malware, as well as the common vulnerabilities that exist within systems, enabling users to better understand their security landscape.
2. Functions as a hands-on tool that allows users to observe and analyze the impact of cyberattacks on system stability, performance, and overall user experience, fostering a deeper awareness of the importance of cyber hygiene and proactive security measures.

**Expected Outcomes**

* **Engaging Simulator:** This advanced virus simulator is fully functional and features a variety of initial modules that illustrate malware-like behavior. Users can interact with these modules to observe how different types of malware manifest and operate, providing a hands-on approach to understanding cyber threats.
* **Awareness Tool**: Designed as a comprehensive learning experience, this simulator aims to enhance user awareness about the importance of cyber hygiene and the various dangers associated with malicious software. It incorporates informative resources and interactive elements to educate users on identifying, preventing, and responding to potential cyber threats effectively.
* **Extensible Design:** The simulator boasts a modular architecture that is highly customizable. This design allows developers and educators to easily add new virus modules as they are developed. By keeping the content updated and introducing fresh challenges, the simulator ensures that users continue to engage with and learn about the evolving landscape of cybersecurity threats.
* **Conclusion**

This project intricately blends technical innovation with educational insights, offering users a compelling and interactive method to grasp the complexities and dangers of malware. By effectively simulating real-world virus behaviors, it creates an immersive learning experience that enhances user awareness of cybersecurity threats. Participants engage with the project through hands-on activities that demonstrate how various types of malware operate, showcasing their potential impact on systems and networks. This experiential approach not only promotes vigilance but also equips users with essential knowledge and strategies to protect themselves against cyber threats. Ultimately, the initiative aims to foster a culture of cybersecurity consciousness, encouraging individuals to adopt best practices that enhance their digital safety and resilience in an increasingly connected world.