GLA UNIVERSITY

Synopsis

Created By:

Vibhu Yadav: -	2315300033
Dushyant Nagal: -	2315300005
Prem Singh:	2315300018

Mentor:

- Dr. Arvind Prasad

Github: https://github.com/coldman07/HORUS

HORUS: Real-Time Ransomware Canary Detection System

INTRODUCTION

Purpose and Overview

The main goal of this project is to create **HORUS**, a real-time system that detects and stops ransomware on Windows computers.
Instead of using traditional signature or machine learning methods, HORUS uses a **behavior-based deception technique**. It places hidden **canary (fake) files** in important folders like *Documents* and *Desktop*.

If any unknown process tries to open, change, or delete these files, HORUS immediately detects it as suspicious. It then **stops the process**, **disconnects the system from the network**, and **records the incident** for analysis.

The tool is designed to be **lightweight, fast, and easy to use**, giving strong protection against both known and new ransomware attacks.

Objective:-

The project aims to develop a **real-time ransomware detection system** for Windows using **canary (decoy) files**.
It monitors file activities through **Windows Security Logs (Event ID 4663)** to spot suspicious behavior.
On detection, it **terminates malicious processes** and **isolates the system** from the network.
All events are **logged for analysis**, ensuring quick and effective response.
The system is **lightweight, fast, and easy to use**, offering strong protection against ransomware.

Problem Statement:-

Ransomware attacks have become a major threat, encrypting user data and demanding ransom for its recovery.
Traditional detection methods like signatures or machine learning often fail to identify **new or evolving ransomware**.
There is a need for a **real-time, lightweight, and behavior-based system** that can detect attacks early.
Most users, especially non-technical ones, lack tools that provide **automatic response and protection**.
Hence, a system like **HORUS** is required to detect, stop, and prevent ransomware effectively before it causes damage.

Methodology and Design

Canary Files and SACL Configuration

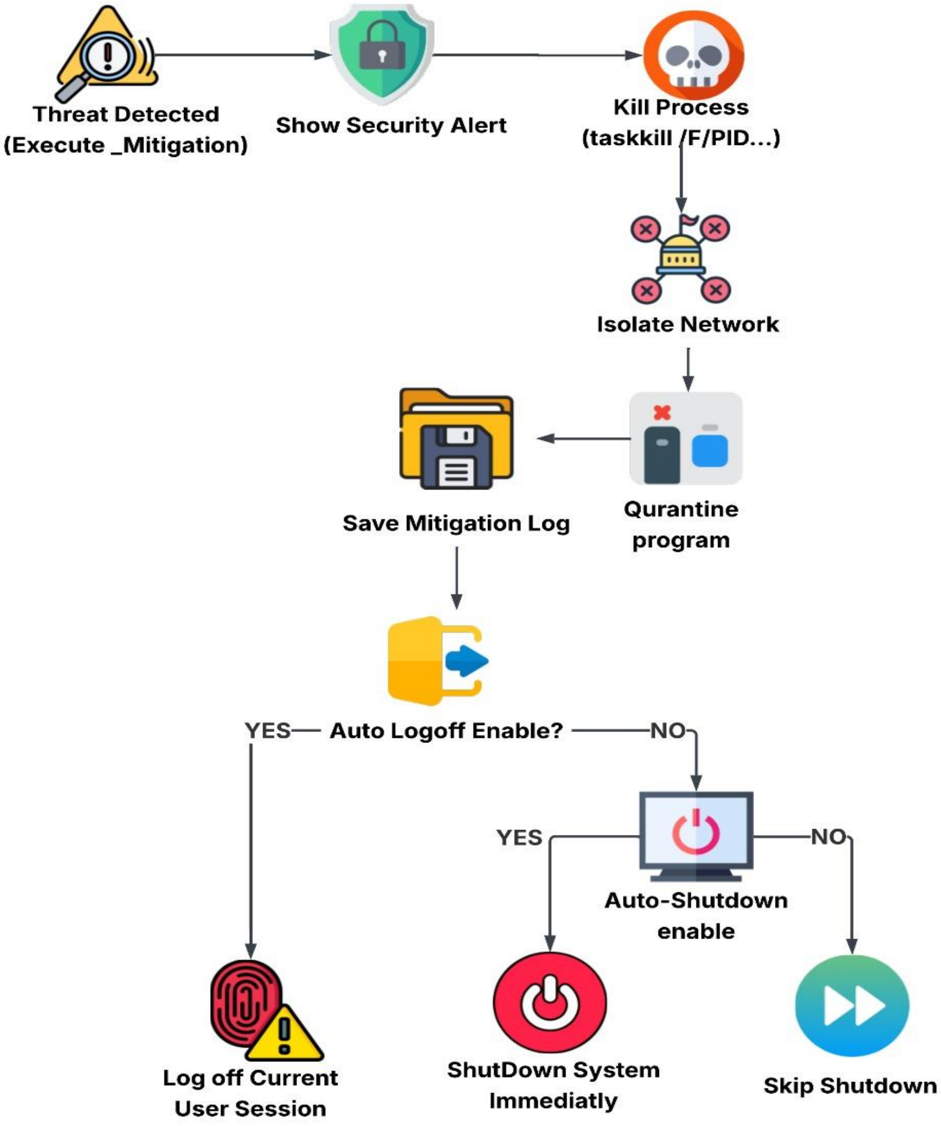
HORUS creates hidden **canary (decoy) files** in key folders like Documents and Desktop.
It enables **auditing through SACL rules**, ensuring any access or modification generates **Windows Event ID 4663**.
This setup allows HORUS to detect suspicious activity the moment a process tries to open, change, or delete a canary file.
Thus, it provides an **early warning system** against ransomware attack.

Monitoring Windows Security Events

HORUS constantly watches the **Windows Security Event Log** for **Event ID 4663** using PyWin32.
Each event provides details like the **file path**, **process name**, and **process ID** of the program accessing the file.
HORUS filters these events to detect access to its **canary files** and quickly identifies the exact malicious process.
This enables **fast and accurate detection** of ransomware activity in real time.

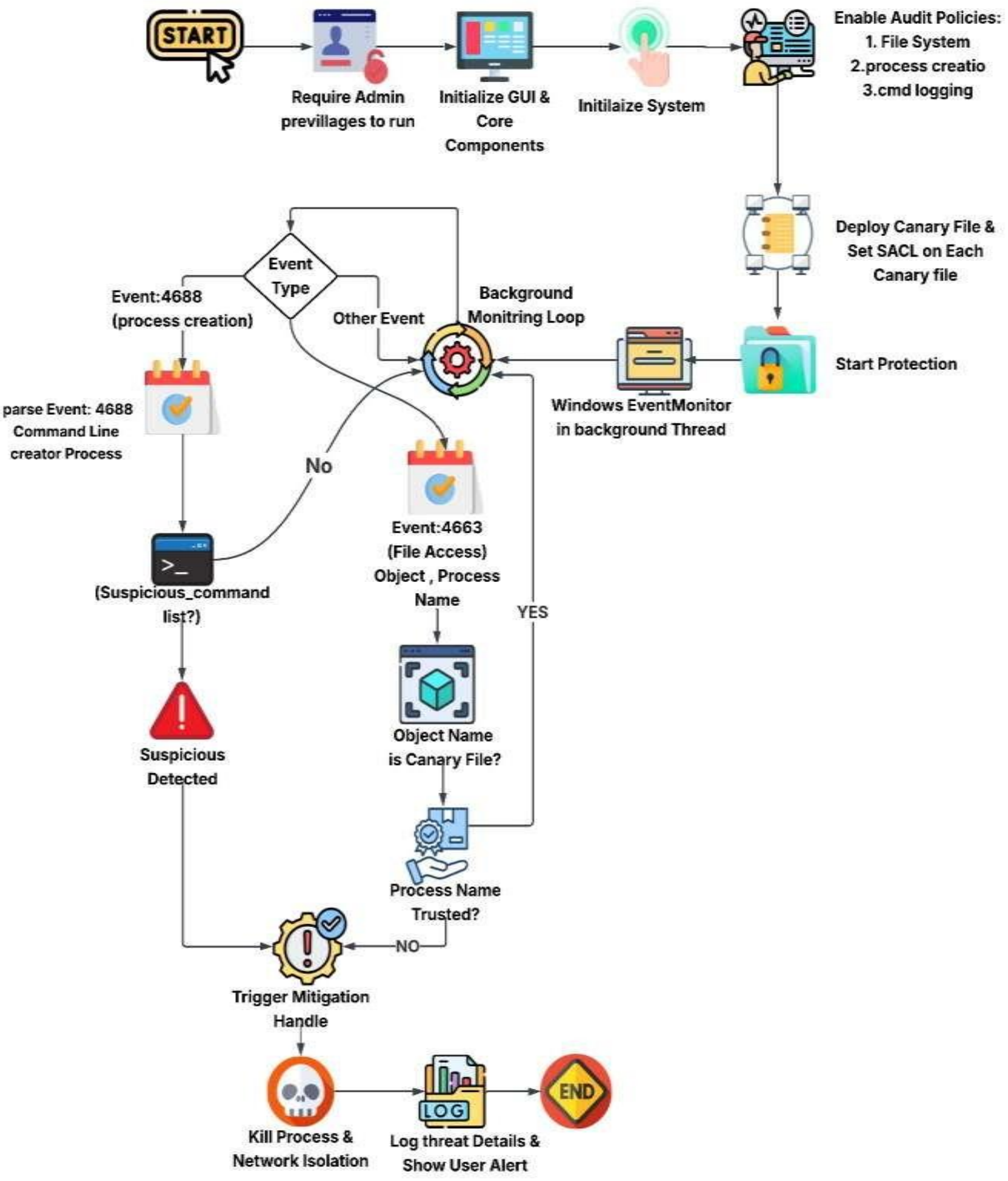
Mitigation Logic:-

When HORUS detects unauthorized access to a canary file, it immediately **terminates the malicious process** using the Win32 API to stop encryption.
Next, it **disables network connections** to prevent the ransomware from spreading or stealing data.
Depending on settings, HORUS can also **shut down or log off** the system for extra safety.
All incidents and actions are **recorded in logs** for later analysis.
This fully automated response ensures **quick containment and minimal user involvement** during an attack.



Evaluation:-

HORUS was tested for **speed, efficiency, and effectiveness** under simulated ransomware conditions.
It detected malicious file access and stopped the process in **under 200 milliseconds**, offering **real-time protection**.
During idle operation, it used only **1–2% CPU**, and even under attack, usage stayed below **5%**, proving it is lightweight.
In ransomware simulations, HORUS **stopped the attack after the first file modification**, preventing further encryption.
Overall, it provides **fast detection, minimal overhead, and strong defense**, matching or exceeding other real-time protection tools.



START
Require Admin previllages to run
Initialize GUI & Core Components
Initilaize System
Enable Audit Policies:
1. File System
2.process creatio
3.cmd logging
Deploy Canary File & Set SACL on Each Canary file
Start Protection
Windows EventMonitor in background Thread
Background Monitring Loop
Event Type
Event:4688 (process creation)
Other Event
parse Event: 4688 Command Line creator Process
No
Event:4663 (File Access) Object , Process Name
>_
(Suspicious_command list?)
YES
Object Name is Canary File?
Suspicious Detected
Process Name Trusted?
NO
Trigger Mitigation Handle
Kill Process & Network Isolation
LOG
Log threat Details & Show User Alert
END

Tools and Technology Required

Programming Language

- Python 3.x: Used for core logic, system control, and GUI development..

Libraries and Modules

- **PyWin32** – For accessing Windows Event Logs, process control, and file auditing (SACL).
- **Subprocess, OS, Time, Hashlib** – For running system commands, timing, and file operations.
- **Tkinter** – To create a simple and interactive desktop GUI.
- **Threading & JSON** – For real-time event handling and structured logging.
- **Dataclasses & Typing** – For organized representation of canary files and events.

Windows Technologies:-

- **Event ID 4663** – Detects file access attempts.
- **SACL** – Enables detailed file auditing.
- **SeSecurityPrivilege & AuditPol** – Used to configure and manage audit settings.

Operating System:-

- **Windows 10/11 (Admin rights needed)** – Main target environment.
- **Linux (optional)** – For testing or future SIEM integration.

Testing Tools:

- **Event Viewer, PowerShell, Task Manager** – To verify logging and monitor behavior.
- **Log files (.log, .json)** – For recording and analyzing detected threats.

Conclusion

HORUS proves that a **behavior-based canary system** can detect and stop ransomware **in real time** with **very low system impact**.
By using **Windows auditing (SACLs and Event ID 4663)**, it quickly identifies suspicious file access and automatically **kills and isolates** the malicious process.
Tests show HORUS reacts **within milliseconds**, uses only **1–2% CPU**, and prevents major file damage.
Unlike traditional antivirus or ML tools, it is **lightweight, fast, and doesn't rely on signature updates**.
With future improvements like **remote alerts and multi-platform support**, HORUS can serve as an effective **last line of defense** against ransomware.