1/3/2025

Ransomware

Defender

Anonymous Defender PUCODE_047

Proof of Concept: Ransomware Defender

Objective: The primary goal of the Ransomware Defender project is to create a comprehensive system to protect against ransomware attacks. This solution targets individual devices and organizational infrastructures and includes a web-based application for broader accessibility.

Concept Overview

The project is divided into three main components:

1. **Tool-Based Protection for Windows Systems**
2. **Organizational-Level Defense Using Splunk**
3. **Web-Based Application**

Technology Stack

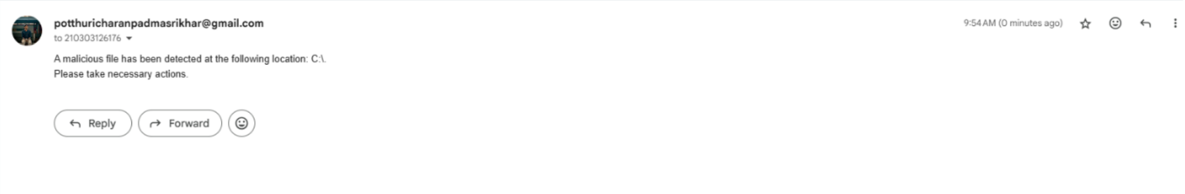
- **Tool-Based Protection:** Python
- **Organizational-Level Defense:** Splunk, Python (for alerts)
- **Web-Based Application:** Flask and Django

Component Details

1. Tool-Based Protection

The Windows tool will perform the following functions:

1. **Email-Based Alerts:**
    - At the initial setup, the user provides their email address.
    - The tool uses this email for all subsequent notifications and does not prompt for it again.

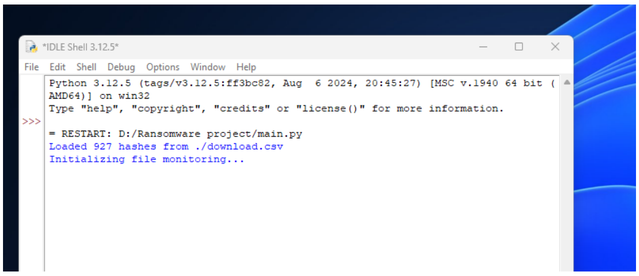


potthuricharanpadmasrikhar@gmail.com
to 210303126176

9:54 AM (0 minutes ago)

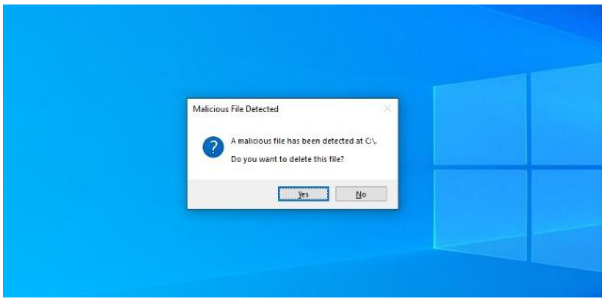
A malicious file has been detected at the following location: C:\.
Please take necessary actions.

2. **Malware Scanning:**
    - The tool scans all drives for malicious files.
    - If malicious files are detected, a popup notifies the user, providing the file path and options to either allow or delete the file.
    - An email alert is sent to the user with details of the malicious file.



```
Python 3.12.5 (tags/v3.12.5:ff3bc82, Aug  6 2024, 20:45:27) [MSC v.1940 64 bit (
AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.
>>>
= RESTART: D:/Ransomware project/main.py
Loaded 927 hashes from ./download.csv
Initializing file monitoring...
```

3. **RDP Port Monitoring:**
   - The tool checks if any file or executable is attempting to access the RDP port.
   - It verifies the presence of malicious scripts or ransomware signatures using datasets from abuse.ch.
4. **Unauthorized File Access Detection:**
   - The tool monitors for any file or executable accessing other files without user permission.
   - If detected, it pops up a notification and sends an email alert.


Malicious File Detected

A malicious file has been detected at C:\.

Do you want to delete this file?

Workflow:

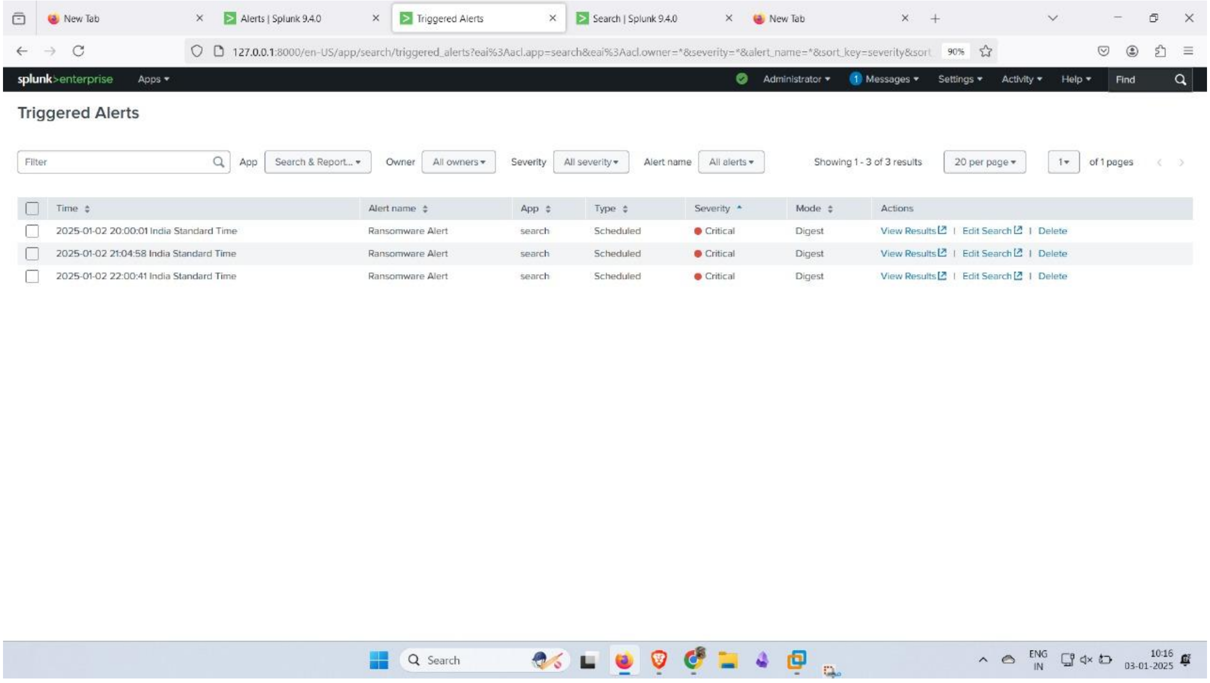
1. Run the tool and provide the email address (one-time setup).
2. Tool scans drives for malicious files and monitors unauthorized access.
3. Alerts and popups guide the user on actions for detected threats.

---

2. Organizational-Level Defense

Using Splunk, the system will:

1. Monitor logs for signs of ransomware or other malicious activity.
2. Generate alerts based on predefined criteria.
3. Display popups to inform the organization of malicious activities detected in the logs.
4. Provide insights for timely action to contain and mitigate ransomware threats.



Triggered Alerts

Filter | App: Search & Report... ▾ | Owner: All owners ▾ | Severity: All severity ▾ | Alert name: All alerts ▾ | Showing 1 - 3 of 3 results | 20 per page ▾ | 1 ▾ of 1 pages

□	Time	Alert name	App	Type	Severity	Mode	Actions
□	2025-01-02 20:00:01 India Standard Time	Ransomware Alert	search	Scheduled	● Critical	Digest	View Results | Edit Search | Delete
□	2025-01-02 21:04:58 India Standard Time	Ransomware Alert	search	Scheduled	● Critical	Digest	View Results | Edit Search | Delete
□	2025-01-02 22:00:41 India Standard Time	Ransomware Alert	search	Scheduled	● Critical	Digest	View Results | Edit Search | Delete

Workflow:

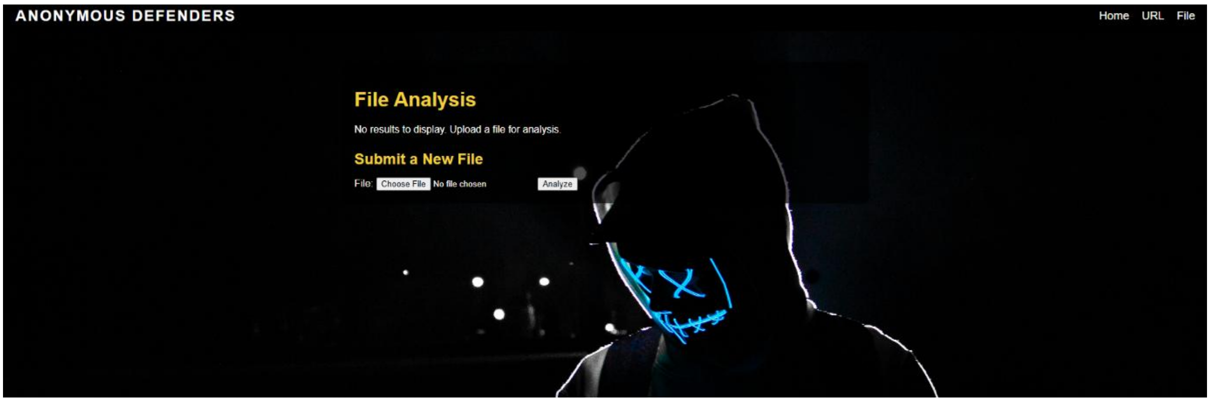
1. Set up Splunk to capture logs.
2. Configure alerts for ransomware-related activities.
3. Display real-time popups for immediate attention.

---

3. Web-Based Application

The web application comprises two main functionalities:

1. **URL Checking:**
   - A user provides a URL via an input field.
   - The system checks the URL against a malicious dataset.
   - Results are displayed, indicating if the URL is safe or malicious.



File Analysis

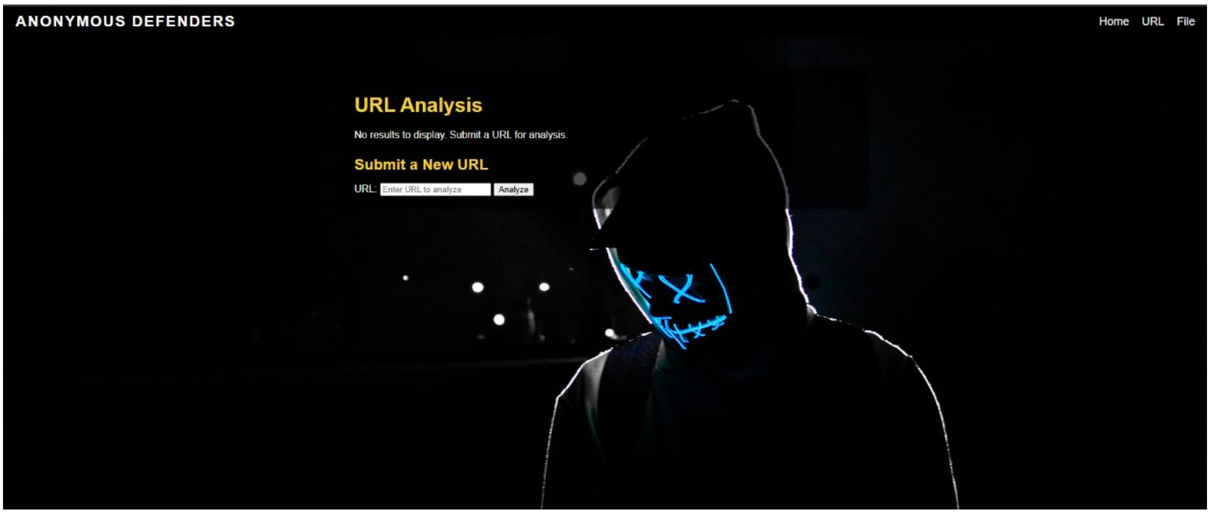
No results to display. Upload a file for analysis.

Submit a New File

File: Choose File No file chosen Analyze

2. **File Upload and Analysis:**

- Users can upload files for analysis.
- The system checks the uploaded file for malicious scripts using a CSV dataset of rules.
- Results are displayed in an easy-to-understand format.



URL Analysis

No results to display. Submit a URL for analysis.

Submit a New URL

URL:

Workflow:

1. User inputs a URL or uploads a file.
2. System processes the input and checks against the datasets.
3. Results are displayed with actionable insights.

Benefits

- **Comprehensive Protection:** Covers individual devices, organizational setups, and online resources.
- **Real-Time Alerts:** Ensures immediate attention to potential threats.
- **Ease of Use:** User-friendly interfaces and actionable notifications.

Implementation Steps:

Tool-Based Protection:

1. Develop email integration for alerts.
2. Implement drive scanning and detection algorithms.
3. Integrate abuse.ch datasets for ransomware signature detection.
4. Add monitoring for unauthorized file access.

Organizational-Level Defense:

1. Configure Splunk for log monitoring.

2. Set up alerts for ransomware-related activities.
3. Develop a popup notification system for real-time alerts..

Web-Based Application:

1. Design the frontend with Flask/Django.
2. Implement URL and file analysis using datasets.
3. Ensure accurate reporting of results.