**Group -3**

**Step6 - Mitigation**

**Memo: Ransomware Simulation and Mitigation Actions**

---

**Subject**: Ransomware Simulation and Mitigation Implementation

---

## Objective

The primary objective was to conduct a risk scenario that attacked a crucial critical file named malicious.pdf while establishing defensive procedures for detection afterward and attack blockage and recovery protocols. The project tested ransomware defense strategies through operations including real-time detection systems along with unauthorized file blocking and backup-restored file retrieval and compromised file isolation to protect operational systems. Following established procedures enabled the project to uncover important information about ransomware performing attacks as well as strategies for system protection. The objectives encompassed testing backup system recovery effectiveness for encrypted files in addition to finding fast breach alerts and putting countermeasures into practice that block file access and shut down malicious processes. The project worked to elevate comprehension of ransomware attacks together with backup strategies and protection methods which reduce both system failures and data loss during ongoing attacks.

---

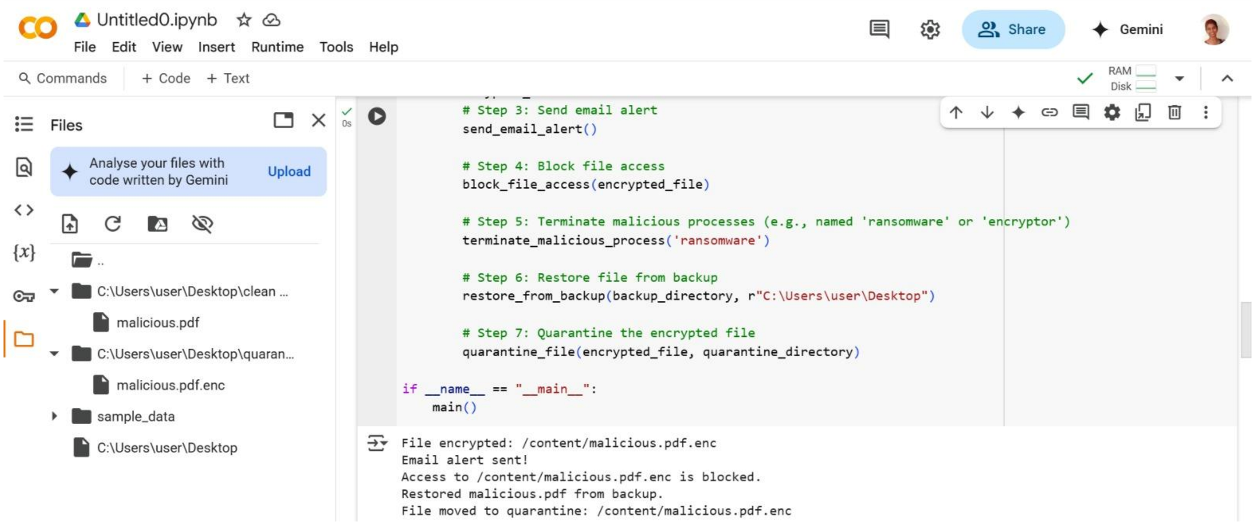
## Action Steps and Implementation

The chosen file for the ransomware simulation test became /content/malicious.pdf which functioned as the victim target. The simulation process activated through encryption required changing the malicious.pdf file to malicious.pdf.enc and modifying its contents to display encrypted data. After encryption of the file the mitigation actions automatically triggered. The system administrator received an email message through the alert system when ransomware activities were detected. A block of access to the infected files became possible by changing their permissions to 0o000 so the ransomware could not make any more modifications. Recovery of the original file was successful by restorating the backup from /content/clean file. The encrypted file received quarantine treatment by transferring its location to the designated directory /content/quarantine to separate it from system resources. The sequence of steps followed in this process showed specifically how different ransomware mitigation practices diminish the overall impact of such attacks.

---

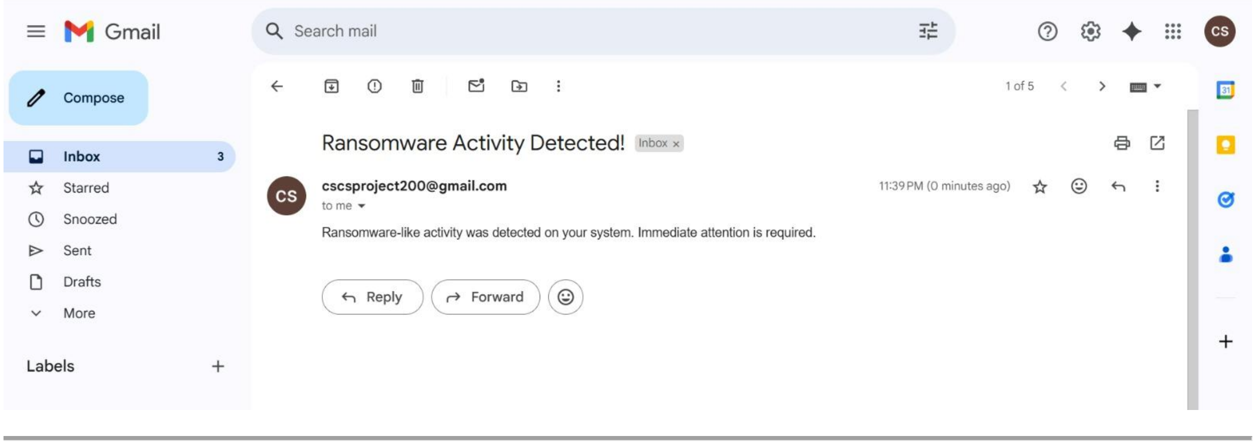
# Results

During the ransomware simulation the target file malicious.pdf successfully went through encryption which involved name change and modification of its data structures to achieve encrypted status. Successfully email alert was sent to the receiver. The system disconnected access to the file to prevent both encryption and any form of alteration. The recovery method within the backup directory showed proper execution thus emphasizing the necessity of backup updates. Successfully quarantining the infected file involved transferring it to a specific directory. The isolation procedure kept the file away from the system making it impossible for it to harm any system components. The developed mitigation procedures successfully stopped the ransomware attack from changing files further while ensuring the recovery of unaffected files. Ransomware mitigation needs immediate detection followed by the prevention of file access and recovery from backups to protect valuable data according to this project's findings.



```
        # Step 3: Send email alert
        send_email_alert()

        # Step 4: Block file access
        block_file_access(encrypted_file)

        # Step 5: Terminate malicious processes (e.g., named 'ransomware' or 'encryptor')
        terminate_malicious_process('ransomware')

        # Step 6: Restore file from backup
        restore_from_backup(backup_directory, r"C:\Users\user\Desktop")

        # Step 7: Quarantine the encrypted file
        quarantine_file(encrypted_file, quarantine_directory)

if __name__ == "__main__":
    main()
```

```
File encrypted: /content/malicious.pdf.enc
Email alert sent!
Access to /content/malicious.pdf.enc is blocked.
Restored malicious.pdf from backup.
File moved to quarantine: /content/malicious.pdf.enc
```



Ransomware Activity Detected!

cscsproject200@gmail.com

to me

11:39 PM (0 minutes ago)

Ransomware-like activity was detected on your system. Immediate attention is required.

## Conclusion

These activities successfully recreated a ransomware attack and depicted the steps for identifying it along with blocking its spread and file recovery operations. The simulation demonstrated how ransomware works by encrypting files while displaying the effective nature of file blocking along with backup recovery and contaminated file containment. The project demonstrated the necessity of complete backup systems as all other countermeasures succeeded in accomplishing their goals while illustrating the value of prepared backup systems for ransomware recovery. The implemented defense strategies proven effective for ransomware attack defense and sensitive data protection by enabling file access control with real-time monitoring as well as data recovery protocols.