SOC101 – Phishing Investigation Report

Challenge 4 – Let'sDefend EventID 8

Student Name: Romaissaa Moftah

Course: Cybersecurity / SOC Analysis

Instructor: Eng. Taha Abouelhgag

1. Executive Summary

On August 29, 2020, at 11:05 PM, a phishing alert was generated by the SOC101 – Phishing Mail Detected rule. The email impersonated a UPS Express notification and attempted to trick the recipient into downloading a compressed file hosted on an external cloud storage service (Amazon S3) via a redirecting download portal. The investigation focused on verifying the sender identity, SMTP source, email content, and endpoint activity to determine whether the malicious file was downloaded or executed and to assess the potential impact on the system.

2. Alert Information

Event ID: 8

Event Time: Aug, 29, 2020 – 11:05 PM

Rule Name: SOC101 – Phishing Mail Detected

Severity Level: Security Analyst

Device Action: Allowed

3. Email Details

Sender Email: info@nexoiberica.com

Recipient Email: mark@letsdefend.io

Subject: UPS Express

Source IP: 63.35.133.186

Protocol: SMTP

Time: Aug, 29, 2020 – 11:00 PM

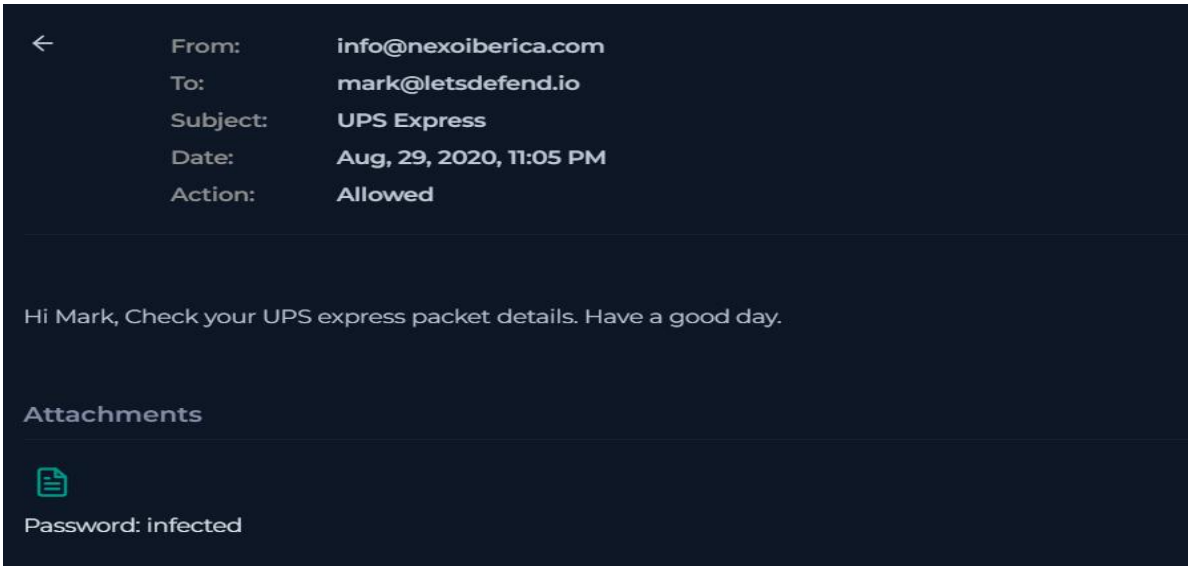
4. Raw Log Analysis

Email Content:

The email claims to be a UPS Express delivery notification and contains a malicious download link. The user is encouraged to access the link to retrieve an attached file related to shipment or invoice information.

Malicious File URL:

https://download.cyberlearn.academy/download/download?url=https://files-ld.s3.us-east-2.amazonaws.com/21b3a9b03027779dc3070481a468b211.zip



Observations:

- The sender domain does not belong to UPS, indicating brand impersonation.

- The file is hosted on a public cloud storage service (Amazon S3), commonly abused for malware delivery.

- The use of a ZIP archive suggests an attempt to bypass email security scanning.

- The email creates urgency by referencing a delivery-related action.

5. Indicator of Compromise (IOC) Analysis

Source IP: 63.35.133.186

Reputation: nexoiberica.com (Not associated with UPS)

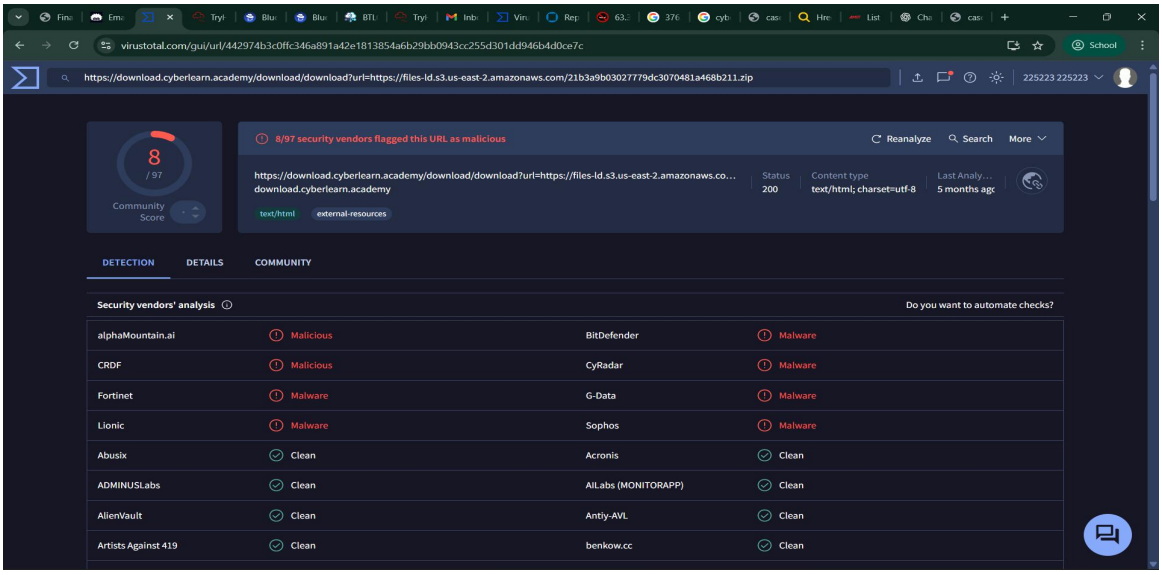
Sender Domain: netflix-payments.com

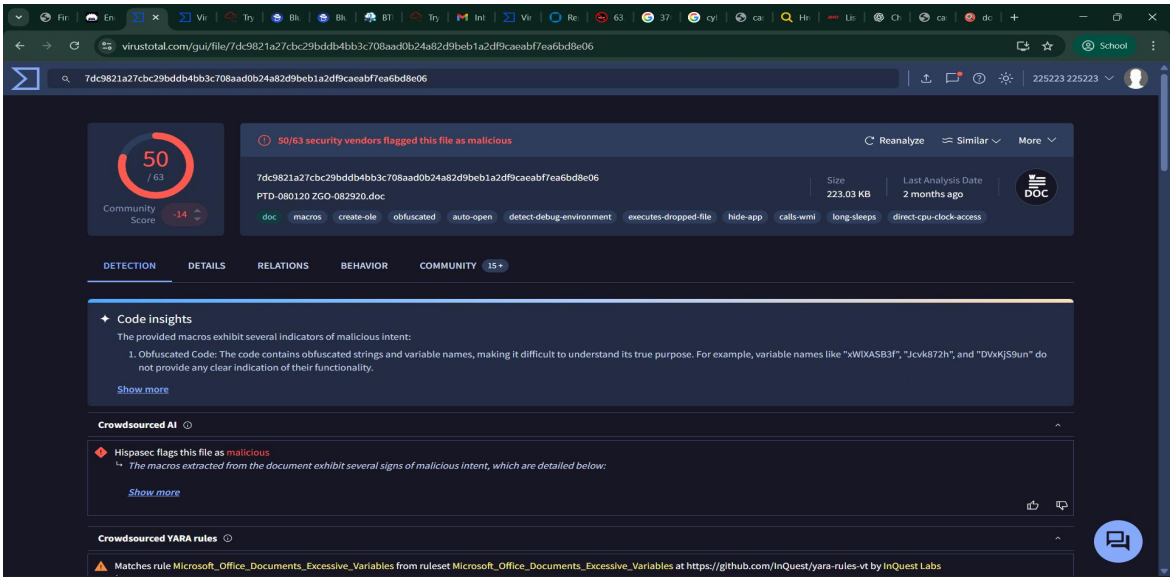
Malicious URL: download.cyberlearn.academy (Redirect)

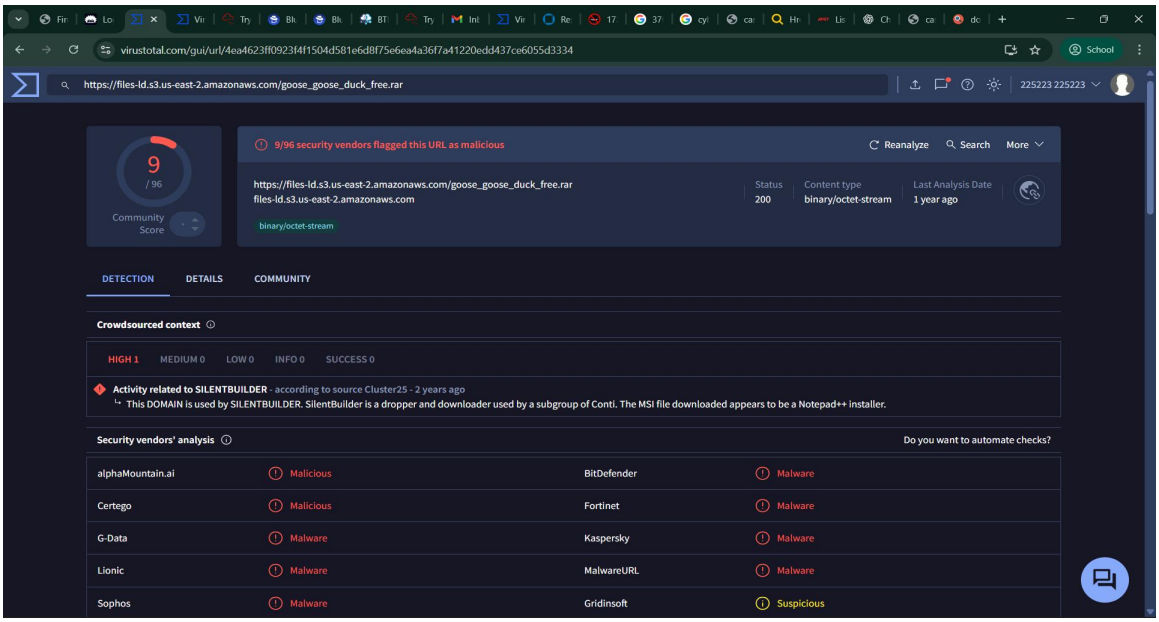
Final File Host: files-ld.s3.us-east-2.amazonaws.com

File Type: ZIP Archive

Risk Level: High





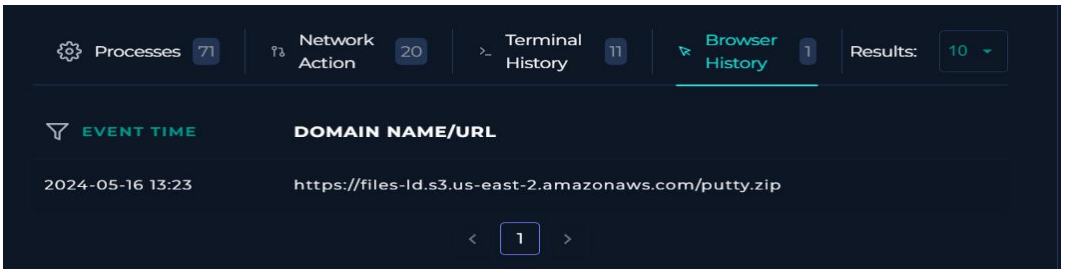


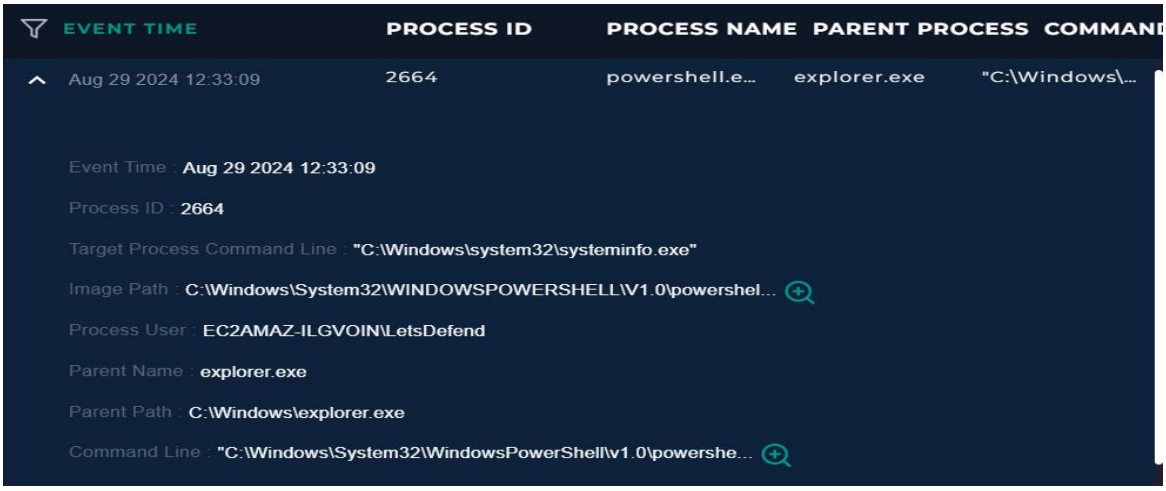
6. Attack Classification

Confirmed Phishing Attempt – Malicious Attachment Delivery

7. Impact Assessment

If the malicious file were opened and executed, it could lead to system compromise, credential theft, malware installation, or unauthorized remote access. Endpoint process logs indicate that a ZIP file was created in the Downloads directory, confirming that the file was successfully downloaded. Subsequent PowerShell and command-line activity suggests potential reconnaissance behavior.





8. Response Actions Taken

- Phishing alert reviewed and validated by SOC analyst.

- Malicious URL and sender domain identified.

- Endpoint logs reviewed for file creation and execution.

- Threat intelligence sources (VirusTotal/URL reputation) consulted.

- Incident documented for escalation and monitoring.

9. Recommendations

- Block sender domain and associated IP address.

- Block the malicious URL and Amazon S3 hosting path.

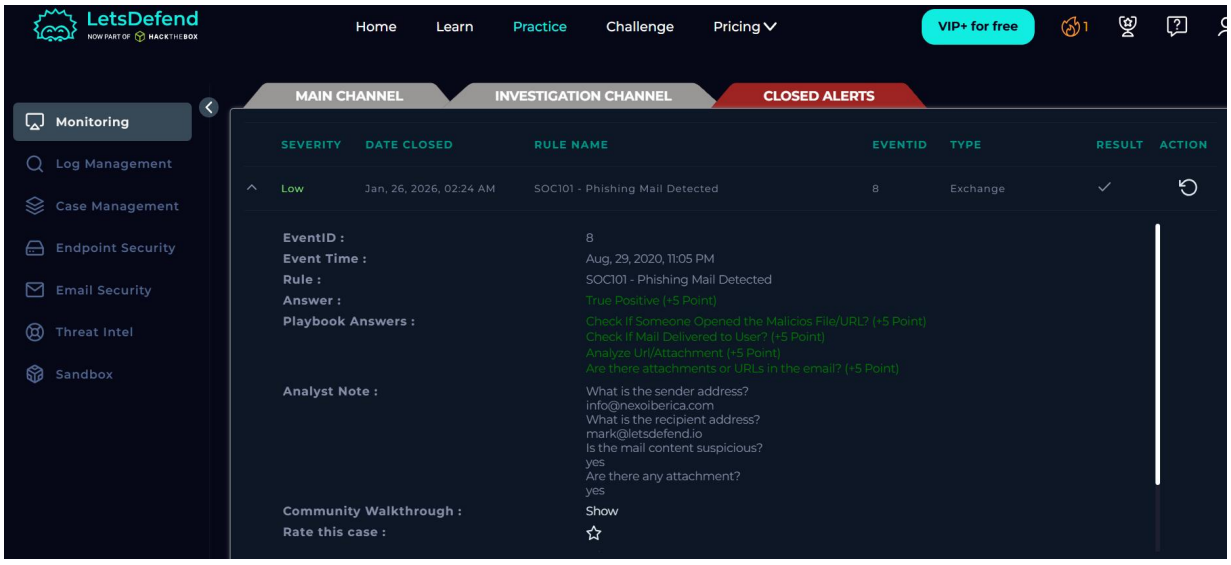
- Enforce email filtering with attachment sandboxing.

- Educate users on identifying fake delivery notifications.

- Enable SPF, DKIM, and DMARC for stronger email authentication.

10. Final Verdict

This incident is classified as a confirmed phishing attack delivering a malicious compressed file. Evidence shows that the file was downloaded to the system, increasing the risk of compromise. Immediate containment and further malware analysis are recommended.



11. Detailed Email Investigation Questions

1. **When was it sent?**

   Aug, 29, 2020 – 11:00 PM

2. **What is the email's SMTP address?**

   63.35.133.186

3. **What is the sender address?**

   info@nexoiberica.com

4. **What is the recipient address?**

   mark@letsdefend.io

5. **Is the mail content suspicious?**

   Yes. The email impersonates UPS Express and delivers a ZIP file through a cloud-hosted malicious link.

6. **Are there any attachments?**

   Yes. A malicious ZIP file is provided via an external download link rather than a direct email attachment.