

# SOC101 – Phishing Investigation Report

Challenge 4 – Let'sDefend EventID 8

**Student Name:** Romaissa 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

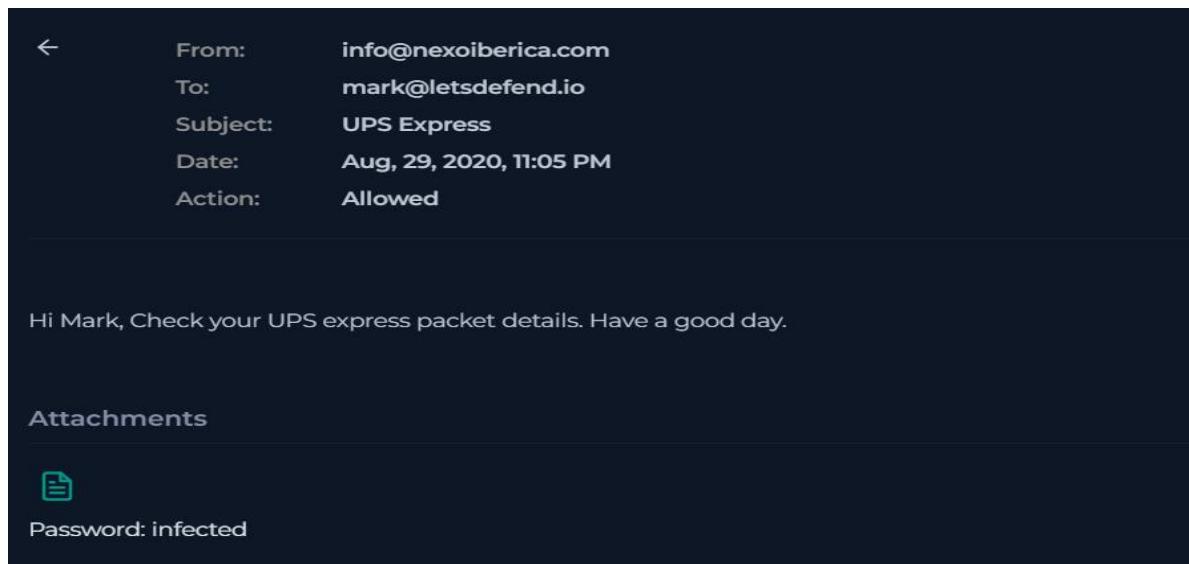
## 4. Raw Log Analysis

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-1d.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

The screenshot shows the VirusTotal analysis interface for the URL <https://download.cyberlearn.academy/download/download?url=https://files-ld.s3.us-east-2.amazonaws.com/21b3a9b03027779dc3070481a468b211.zip>. The page displays a community score of 8/97, indicating 8 out of 97 security vendors flagged it as malicious. The status is 200, and the content type is text/html; charset=utf-8. The last analysis was 5 months ago. Below this, a table lists vendor analysis results:

Vendor	Result	Vendor	Result
alphaMountain.ai	Malicious	BitDefender	Malware
CRDF	Malicious	CyRadar	Malware
Fortinet	Malware	G-Data	Malware
Lionic	Malware	Sophos	Malware
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AllLabs (MONITORAPP)	Clean
AlienVault	Clean	Anti-AVL	Clean
Artists Against 419	Clean	benkow.cc	Clean

The screenshot shows the VirusTotal analysis interface for the file [7dc9821a27cbc29bddb4bb3c708aad0b24a82d9beb1a2df9caeabf7ea6bd8e06](https://vt��.080120.ZG-082920.doc). The page displays a community score of 50/63, indicating 50 out of 63 security vendors flagged it as malicious. The file is a Microsoft Word document (doc). The size is 223.03 KB, and the last analysis date is 2 months ago. Below this, sections include "Code insights" (noting obfuscated code), "Crowdsourced AI" (noting Hispacsec flagged it as malicious), and "Crowdsourced YARA rules" (noting a match with Microsoft\_Office\_Documents\_Excessive\_Variables).

The screenshot shows the VirusTotal analysis interface for the URL [https://files-ld.s3.us-east-2.amazonaws.com/goose\\_goose\\_duck\\_free.rar](https://files-ld.s3.us-east-2.amazonaws.com/goose_goose_duck_free.rar). The main summary indicates a **Community Score** of 9 / 96, with 9/96 security vendors flagged this URL as malicious. The file type is listed as **binary/octet-stream**. Other details include a **Status** of 200, a **Content type** of binary/octet-stream, and a **Last Analysis Date** of 1 year ago. A note in the "Crowdsourced context" section mentions activity related to SILENTBUILDER, which is described as a dropper and downloader used by a subgroup of Conti. The "Security vendors' analysis" table lists results from various engines:

Engine	Result
alphaMountain.ai	Malicious
Certego	Malicious
G-Data	Malware
Lionic	Malware
Sophos	Malware
BitDefender	Malware
Fortinet	Malware
Kaspersky	Malware
MalwareURL	Malware
Gridinsoft	Suspicious

## 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.

The screenshot displays a log viewer interface with the following navigation tabs: Processes (71), Network Action (20), Terminal History (11), Browser History (1), and Results: 10. The results table has columns for EVENT TIME and DOMAIN NAME/URL. One entry is shown: 2024-05-16 13:23 and https://files-ld.s3.us-east-2.amazonaws.com/putty.zip. The page includes a navigation bar with back, forward, and search functions.

▲ May 16 2024 13:24:05	1932	cmd.exe	putty.exe	cmd
Event Time : <b>May 16 2024 13:24:05</b>				
Process ID :	<b>1932</b>			
Target Process Command Line :	\??\C:\Windows\system32\conhost.exe 0xffffffff -For...			
Image Path :	<b>C:\Windows\SysWOW64\cmd.exe</b>			
Process User :	<b>EC2AMAZ-ILGVOIN\LetsDefend</b>			
Parent Name :	<b>putty.exe</b>			
Parent Path :	<b>C:\Users\LetsDefend\Downloads\putty.exe</b>			

Event Time	Process ID	Process Name	Parent Process	Command Line
Aug 29 2024 12:33:09	2664	powershell.e...	explorer.exe	"C:\Windows\...

Event Time : Aug 29 2024 12:33:09

Process ID : 2664

Target Process Command Line : "C:\Windows\system32\systeminfo.exe"

Image Path : C:\Windows\System32\WINDOWSPOWERSHELL\V1.0\powershel... [?](#)

Process User : EC2AMAZ-ILGVOIN\letsdefend

Parent Name : explorer.exe

Parent Path : C:\Windows\explorer.exe

Command Line : "C:\Windows\System32\WindowsPowerShell\v1.0\powershe... [?](#)

## **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.

The screenshot shows the LetsDefend platform interface. On the left, there's a sidebar with navigation links: Monitoring (selected), Log Management, Case Management, Endpoint Security, Email Security, Threat Intel, and Sandbox. The main content area has three tabs at the top: MAIN CHANNEL, INVESTIGATION CHANNEL (selected), and CLOSED ALERTS. The CLOSED ALERTS tab shows a single row of data:

SEVERITY	DATE CLOSED	RULE NAME	EVENTID	TYPE	RESULT	ACTION
Low	Jan, 26, 2026, 02:24 AM	SOC101 - Phishing Mail Detected	8	Exchange	✓	↻

Below this table, there are several expandable sections with details:

- EventID :** 8
- Event Time :** Aug, 29, 2020, 11:05 PM
- Rule :** SOC101 - Phishing Mail Detected
- Answer :** True Positive (+5 Point)
- Playbook Answers :**
  - Check If Someone Opened the Malicious File/URL? (+5 Point)
  - Check If Mail Delivered to User? (+5 Point)
  - Analyze Url/Attachment (+5 Point)
  - Are there attachments or URLs in the email? (+5 Point)
- Analyst Note :**

What is the sender address?  
info@nexolberica.com  
What is the recipient address?  
mark@letsdefend.io  
Is the mail content suspicious?  
yes  
Are there any attachment?  
yes  
Show
- Community Walkthrough :**

Rate this case :

## **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](mailto:info@nexoiberica.com)

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

[mark@letsdefend.io](mailto: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.