

# SOC101 – Phishing Investigation Report

Challenge 4 – Let'sDefend EventID 8

**Student Name:** Romaissaa Moftah

**Course:** Cybersecurity / SOC Analysis

**Instructor:** Eng. Taha Abouelhagag



## 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

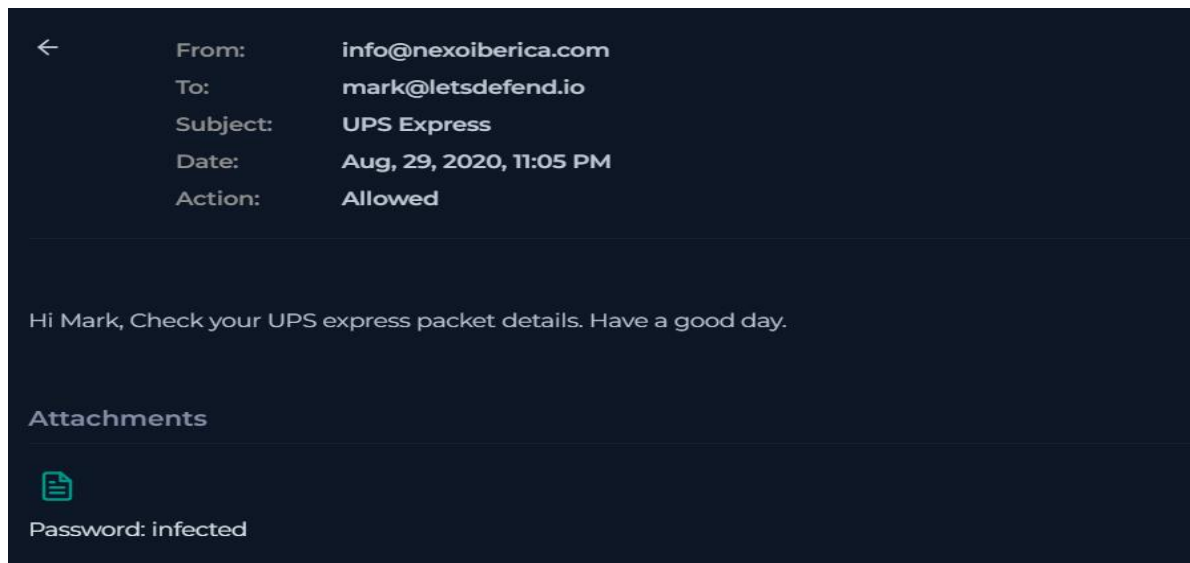
## 4. Raw Log Analysis

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-lid.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

This screenshot shows the VirusTotal interface for a URL. The URL is `https://download.cyberlearn.academy/download/download?url=https://files-ld.s3.us-east-2.amazonaws.com/21b3a9b0302779dc3070481a468b211.zip`. The community score is 8/97. A warning indicates that 8/97 security vendors flagged this URL as malicious. The status is 200, and the content type is text/html. The last analysis was 5 months ago. The detection tab is active, showing a table of security vendors' analysis.

Vendor	Verdict
alphaMountain.ai	Malicious
CRDF	Malicious
Fortinet	Malware
Lionic	Malware
Abusix	Clean
ADMINUSLabs	Clean
AlienVault	Clean
Artists Against 419	Clean
BITDefender	Malware
CyRadar	Malware
G-Data	Malware
Sophos	Malware
Acronis	Clean
AILabs (MONITORAPP)	Clean
Antiy-AVL	Clean
benkow.cc	Clean

This screenshot shows the VirusTotal interface for a file. The file hash is `7dc9821a27cbc29bddb4bb3c708aad0b24a82d9beb1a2df9caeabf7ea6bd8e06`. The community score is 50/63. A warning indicates that 50/63 security vendors flagged this file as malicious. The file size is 223.03 KB, and the last analysis was 2 months ago. The file type is DOC. The detection tab is active, showing code insights and Crowdsourced AI analysis.

**Code insights**

The provided macros exhibit several indicators of malicious intent:

- Obfuscated Code: The code contains obfuscated strings and variable names, making it difficult to understand its true purpose. For example, variable names like "xWIXASB3f", "Jcv4872h", and "DvXkJS9un" do not provide any clear indication of their functionality.

**Crowdsourced AI**

Hispasec flags this file as malicious

The macros extracted from the document exhibit several signs of malicious intent, which are detailed below:

9/96 security vendors flagged this URL as malicious

Community Score: 9 / 96

https://files-ld.s3.us-east-2.amazonaws.com/goose\_goose\_duck\_free.rar

Status: 200 | Content type: binary/octet-stream | Last Analysis Date: 1 year ago

DETECTION DETAILS COMMUNITY

Crowdsourced context

HIGH 1 MEDIUM 0 LOW 0 INFO 0 SUCCESS 0

Activity related to SILENTBUILDER - according to source Cluster25 - 2 years ago  
This DOMAIN is used by SILENTBUILDER. SilentBuilder is a dropper and downloader used by a subgroup of Conti. The MSI file downloaded appears to be a Notepad++ installer.

Security vendors' analysis

Vendor	Verdict	Vendor	Verdict
alphaMountain.ai	Malicious	BitDefender	Malware
Certego	Malicious	Fortinet	Malware
G-Data	Malware	Kaspersky	Malware
Lionic	Malware	MalwareURL	Malware
Sophos	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.

Processes 71 | Network Action 20 | Terminal History 11 | Browser History 1 | Results: 10

EVENT TIME	DOMAIN NAME/URL
2024-05-16 13:23	https://files-ld.s3.us-east-2.amazonaws.com/putty.zip

^ May 16 2024 13:24:05 1932 cmd.exe putty.exe cmd

Event Time : May 16 2024 13:24:05

Process ID : 1932

Target Process Command Line : \??\C:\Windows\system32\conhost.exe 0xffffffff -Forc... 

Image Path : C:\Windows\SysWOW64\cmd.exe

Process User : EC2AMAZ-ILGVOIN\LetsDefend

Parent Name : putty.exe


Parent Path : C:\Users\LetsDefend\Downloads\putty.exe

EVENT TIME	PROCESS ID	PROCESS NAME	PARENT PROCESS	COMMAND
^ 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 displays the LetsDefend web interface, which is part of HackTheBox. The interface features a dark theme with a sidebar on the left containing navigation links: Monitoring, Log Management, Case Management, Endpoint Security, Email Security, Threat Intel, and Sandbox. The main content area is divided into three tabs: MAIN CHANNEL, INVESTIGATION CHANNEL, and CLOSED ALERTS. The CLOSED ALERTS tab is active, showing a table of alerts. The table has columns for SEVERITY, DATE CLOSED, RULE NAME, EVENTID, TYPE, RESULT, and ACTION. A single alert is visible with a severity of 'Low', dated 'Jan. 26, 2026, 02:24 AM', and the rule name 'SOC101 - Phishing Mail Detected'. Below the table, the details of the alert are shown, including the EventID (8), Event Time (Aug. 29, 2020, 11:05 PM), Rule (SOC101 - Phishing Mail Detected), Answer (True Positive (+5 Point)), and Playbook Answers (a list of tasks: Check if Someone Opened the Malicious File/URL? (+5 Point), Check if Mail Delivered to User? (+5 Point), Analyze Uri/Attachment (+5 Point), and Are there attachments or URLs in the email? (+5 Point)). The Analyst Note section contains a list of questions and answers: 'What is the sender address?' (info@nexoiberica.com), 'What is the recipient address?' (mark@letsdefend.io), 'Is the mail content suspicious?' (yes), and 'Are there any attachments?' (yes). The Community Walkthrough section shows a 'Show' button and a 'Rate this case' section with a star icon.

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

**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 Uri/Attachment (+5 Point)  
Are there attachments or URLs in the email? (+5 Point)  
**Analyst Note :** What is the sender address?  
info@nexoiberica.com  
What is the recipient address?  
mark@letsdefend.io  
Is the mail content suspicious?  
yes  
Are there any attachments?  
yes  
**Community Walkthrough :** Show  
**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.