# SOC101 – Phishing Investigation Report

Challenge 3 – Let'sDefend EventID 27

**Student Name:** Romaissaa Moftah

**Course:** Cybersecurity / SOC Analysis

**Instructor:** Eng. Taha Abouelhgag

## 1. Executive Summary

On October 29, 2020, at 07:25 PM, a phishing alert was triggered by the SOC101 – Phishing Mail Detected rule. The email impersonated a shipping service (UPS) and claimed that the recipient had a secure message related to a package status change. The message attempted to lure the user into clicking a suspicious external link and later opening an attachment.

The investigation focused on validating the sender, analyzing the embedded URL, and reviewing the system action to determine whether the threat was successfully blocked and whether any user interaction occurred.

## 2. Alert Information

**Event ID:** 27

**Event Time:** Oct, 29, 2020 – 07:25 PM

**Rule Name:** SOC101 – Phishing Mail Detected

**Severity Level:** Security Analyst

**Device Action:** Blocked

## 3. Email Details

**Sender Email:** ndt@zol.co.zw

**Recipient Email:** susie@letsdefend.io

**Subject:** UPS Your Packages Status Has Changed

**Source IP:** 146.56.209.252

**Protocol:** SMTP

**Time:** Oct, 29, 2020 – 07:25 PM

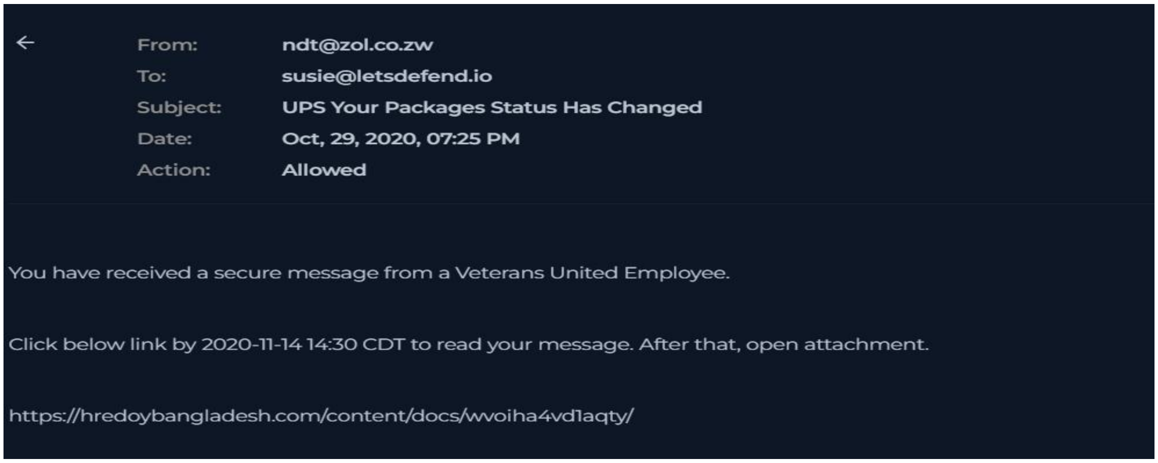
## 4. Raw Log Analysis

Email Content:

"You have received a secure message from a Veterans United Employee.

Click below link by 2020-11-14 14:30 CDT to read your message. After that, open attachment.

https://hredoybangladesh.com/content/docs/wvoiha4vd1aqty/"



From: ndt@zol.co.zw
To: susie@letsdefend.io
Subject: UPS Your Packages Status Has Changed
Date: Oct, 29, 2020, 07:25 PM
Action: Allowed

You have received a secure message from a Veterans United Employee.

Click below link by 2020-11-14 14:30 CDT to read your message. After that, open attachment.

https://hredoybangladesh.com/content/docs/wvoiha4vd1aqty/

### Observations:

- The subject line impersonates UPS, while the body references a Veterans United Employee.

- A suspicious external URL is embedded in the email.

- The domain hredoybangladesh.com is unrelated to UPS.

- The email creates urgency using a deadline.

- The message instructs the user to open an attachment, which is a common malware tactic.

## 5. Indicator of Compromise (IOC) Analysis

**Source IP:** 146.56.209.252

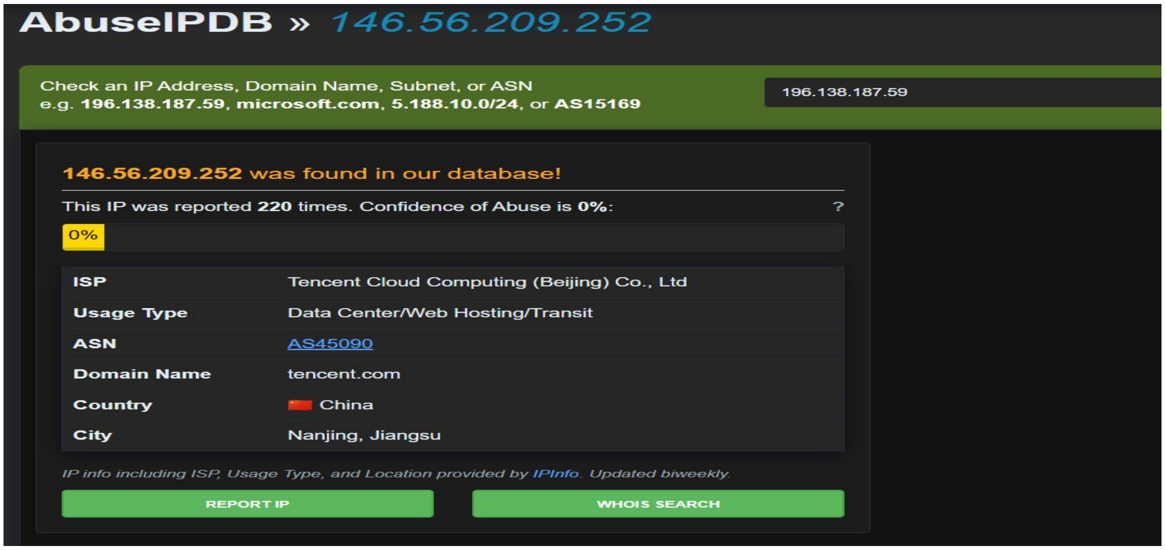
**Reputation:** Potentially suspicious

**Sender Domain:** zol.co.zw

**Analysis:** Does not belong to UPS or any legitimate shipping service.

**Malicious URL:** https://hredoybangladesh.com/content/docs/wvoiha4vd1aqty/

**Risk Level:** High



AbuseIPDB » 146.56.209.252

Check an IP Address, Domain Name, Subnet, or ASN
e.g. **196.138.187.59**, **microsoft.com**, **5.188.10.0/24**, or **AS15169**

196.138.187.59

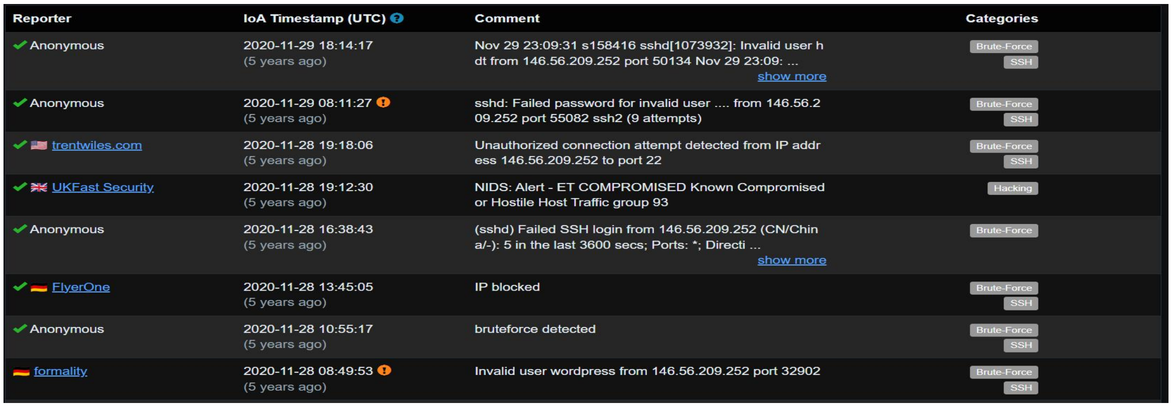
**146.56.209.252** was found in our database!

This IP was reported **220** times. Confidence of Abuse is **0%**: ?

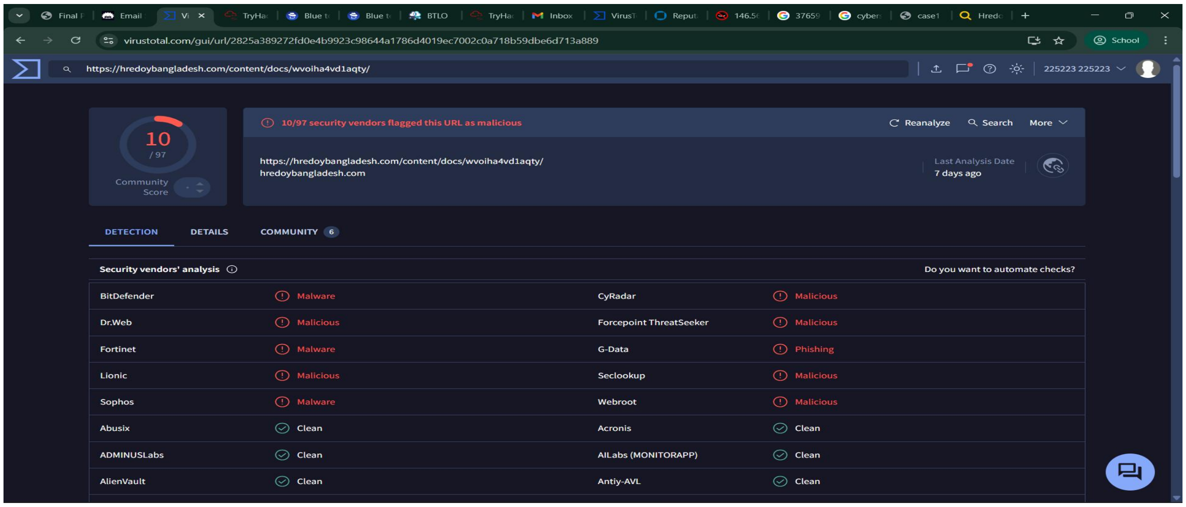
0%

| | |
|---|---|
| **ISP** | Tencent Cloud Computing (Beijing) Co., Ltd |
| **Usage Type** | Data Center/Web Hosting/Transit |
| **ASN** | AS45090 |
| **Domain Name** | tencent.com |
| **Country** | China |
| **City** | Nanjing, Jiangsu |

*IP info including ISP, Usage Type, and Location provided by IPInfo. Updated biweekly.*



| Reporter | IoA Timestamp (UTC) | Comment | Categories |
|---|---|---|---|
| ✓ Anonymous | 2020-11-29 18:14:17<br>(5 years ago) | Nov 29 23:09:31 s158416 sshd[1073932]: Invalid user h dt from 146.56.209.252 port 50134 Nov 29 23:09: ...<br>show more | Brute-Force<br>SSH |
| ✓ Anonymous | 2020-11-29 08:11:27 !<br>(5 years ago) | sshd: Failed password for invalid user .... from 146.56.2 09.252 port 55082 ssh2 (9 attempts) | Brute-Force<br>SSH |
| ✓ trentwiles.com | 2020-11-28 19:18:06<br>(5 years ago) | Unauthorized connection attempt detected from IP addr ess 146.56.209.252 to port 22 | Brute-Force<br>SSH |
| ✓ UKFast Security | 2020-11-28 19:12:30<br>(5 years ago) | NIDS: Alert - ET COMPROMISED Known Compromised or Hostile Host Traffic group 93 | Hacking |
| ✓ Anonymous | 2020-11-28 16:38:43<br>(5 years ago) | (sshd) Failed SSH login from 146.56.209.252 (CN/Chin a/-): 5 in the last 3600 secs; Ports: *; Directi ...<br>show more | Brute-Force |
| ✓ FlyerOne | 2020-11-28 13:45:05<br>(5 years ago) | IP blocked | Brute-Force<br>SSH |
| ✓ Anonymous | 2020-11-28 10:55:17<br>(5 years ago) | bruteforce detected | Brute-Force<br>SSH |
| formality | 2020-11-28 08:49:53 !<br>(5 years ago) | Invalid user wordpress from 146.56.209.252 port 32902 | Brute-Force<br>SSH |



virustotal.com/gui/url/2825a389272fd0e4b9923c98644a1786d4019ec7002c0a718b59dbe6d713a889

https://hredoybangladesh.com/content/docs/wvoiha4vd1aqty/

10/97 security vendors flagged this URL as malicious

https://hredoybangladesh.com/content/docs/wvoiha4vd1aqty/
hredoybangladesh.com

Last Analysis Date
7 days ago

Security vendors' analysis

Do you want to automate checks?

| | | | |
|---|---|---|---|
| BitDefender | Malware | CyRadar | Malicious |
| Dr.Web | Malicious | Forcepoint ThreatSeeker | Malicious |
| Fortinet | Malware | G-Data | Phishing |
| Lionic | Malicious | Seclookup | Malicious |
| Sophos | Malware | Webroot | Malicious |
| Abusix | Clean | Acronis | Clean |
| ADMINUSLabs | Clean | AILabs (MONITORAPP) | Clean |
| AlienVault | Clean | Antiy-AVL | Clean |

## 6. Impact Assessment

If clicked, the link and attachment could result in:

- Malware infection

- Credential theft

- Unauthorized system access

- Data exfiltration

No impact occurred because the email was blocked.

## 7. Response Actions Taken

- Email blocked by the security system

- Alert reviewed by SOC analyst

- URL and sender domain analyzed

- Incident documented

## 8. Recommendations

- Block the domain hredoybangladesh.com

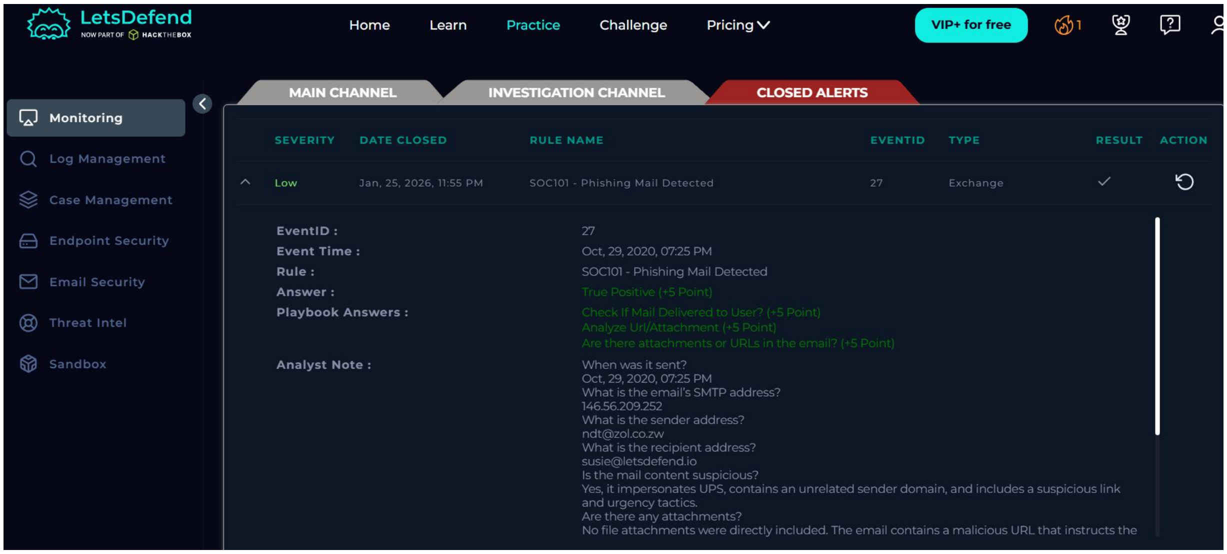
- Monitor or blacklist zol.co.zw

- Enable SPF, DKIM, and DMARC

- Train users on shipping phishing scams

## 9. Final Verdict

This was a confirmed phishing attempt using brand impersonation and a malicious external link. The threat was successfully blocked, and no user interaction occurred.



| SEVERITY | DATE CLOSED | RULE NAME | EVENTID | TYPE | RESULT | ACTION |
|---|---|---|---|---|---|---|
| Low | Jan, 25, 2026, 11:55 PM | SOC101 - Phishing Mail Detected | 27 | Exchange | ✓ | ↺ |

EventID : 27

Event Time : Oct, 29, 2020, 07:25 PM

Rule : SOC101 - Phishing Mail Detected

Answer : True Positive (+5 Point)

Playbook Answers : 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 : When was it sent?
Oct, 29, 2020, 07:25 PM
What is the email's SMTP address?
146.56.209.252
What is the sender address?
ndt@zol.co.zw
What is the recipient address?
susie@letsdefend.io
Is the mail content suspicious?
Yes, it impersonates UPS, contains an unrelated sender domain, and includes a suspicious link and urgency tactics.
Are there any attachments?
No file attachments were directly included. The email contains a malicious URL that instructs the

# 10. Detailed Email Investigation Questions

1. **When was it sent?**

   Oct, 29, 2020, 07:25 PM

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

   146.56.209.252

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

   ndt@zol.co.zw

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

   susie@letsdefend.io

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

   Yes, it impersonates UPS, contains an unrelated sender domain, and includes a suspicious link and urgency tactics.

6. **Are there any attachments?**

   No file attachments were directly included. The email contains a malicious URL that instructs the user to open an attachment.