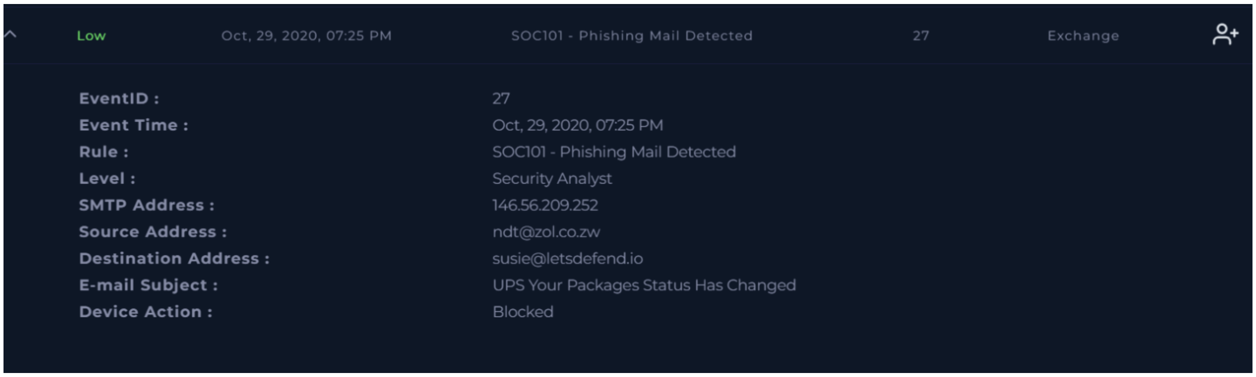
Soc101 – phishing mail Detected
task ID -27



Low	Oct, 29, 2020, 07:25 PM	SOC101 - Phishing Mail Detected	27	Exchange

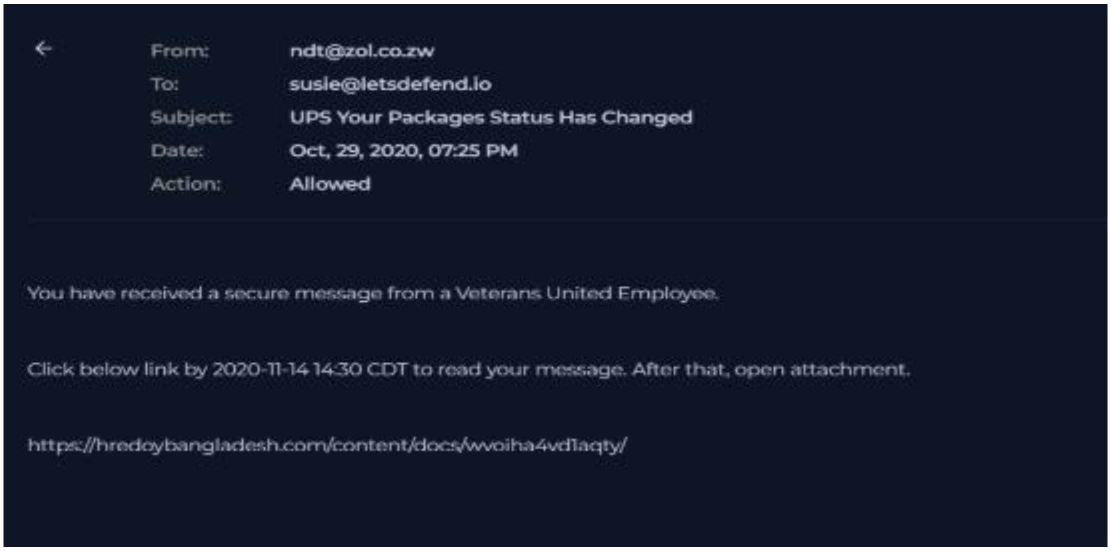
EventID :	27
Event Time :	Oct, 29, 2020, 07:25 PM
Rule :	SOC101 - Phishing Mail Detected
Level :	Security Analyst
SMTP Address :	146.56.209.252
Source Address :	ndt@zol.co.zw
Destination Address :	susie@letsdefend.io
E-mail Subject :	UPS Your Packages Status Has Changed
Device Action :	Blocked

Incident Overview:

A phishing email alert was generated by the security monitoring system under the rule **SOC101 – Phishing Mail Detected**. The investigation identified a malicious URL embedded within the email content, designed to impersonate a legitimate shipping notification. The email was successfully blocked by the email security gateway; however, further analysis revealed additional endpoint visibility concerns due to an EDR agent communication failure.

Email Details

- **SMTP Address: 146.56.209.252**
- **Source Email Address: ndt@zol.co.zw**
- **Destination Email Address: susie@letsdefend.io**
- **Email Subject:** ***UPS Your Packages Status Has Changed***
-



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/

Malicious URL Analysis

Identified Malicious URL:

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

Threat Intelligence Verdict

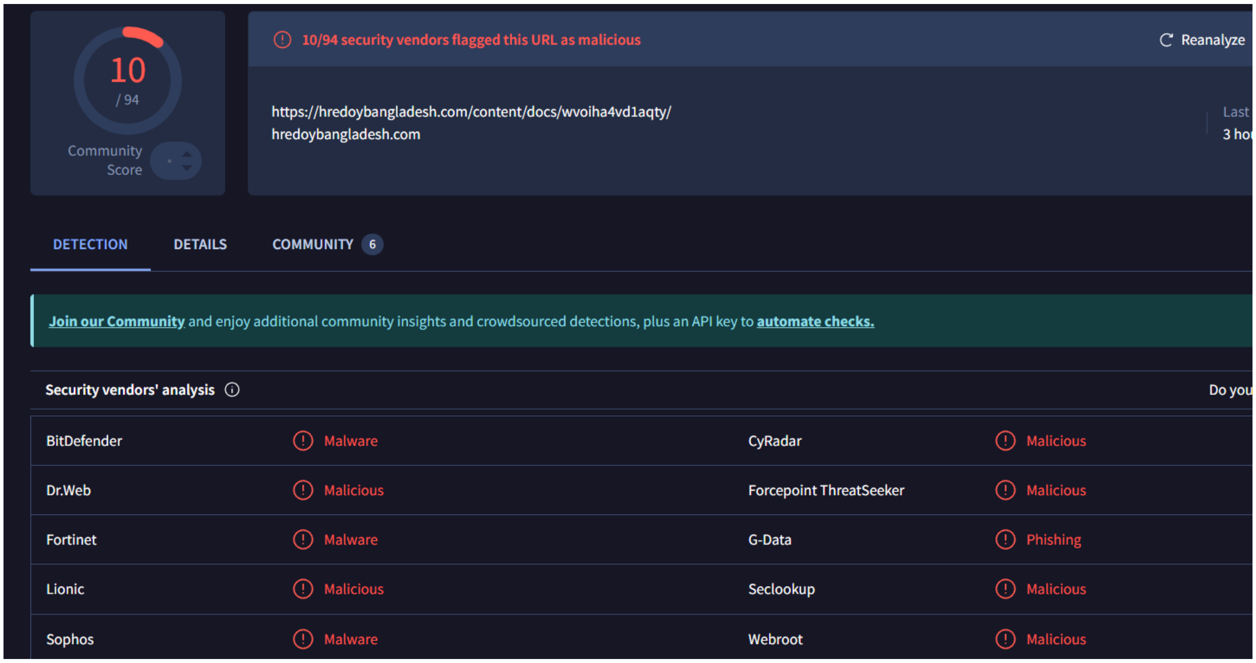
- **Classification: Phishing / Malware**
- **Malware Score: 10 / 10 (High Risk)**
- **File Type: image/png**

- **File Size: 24.12 kB**

Timeline

- **First Submission: 2020-10-16 00:14:11 UTC**
- **Last Submission: 2026-01-29 06:29:00 UTC**
- **Last Analysis: 2026-01-29 06:29:00 UTC**

Multiple security vendors flagged the URL as malicious, confirming its association with phishing and malware distribution campaigns.



10/94 security vendors flagged this URL as malicious

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

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

BitDefender	Malware	CyRadar	Malicious
Dr.Web	Malicious	Forcepoint ThreatSeeker	Malicious
Fortinet	Malware	G-Data	Phishing
Lionic	Malicious	Seclookup	Malicious
Sophos	Malware	Webroot	Malicious

Endpoint Investigation

Endpoint Details

- Hostname: SusieHost
- IP Address: 172.16.17.5
- Operating System: Windows 10
- Primary User: Susie2020
- Client Type: Client
- Last Login: Aug 29, 2020 – 07:58 PM

EDR Status Observation

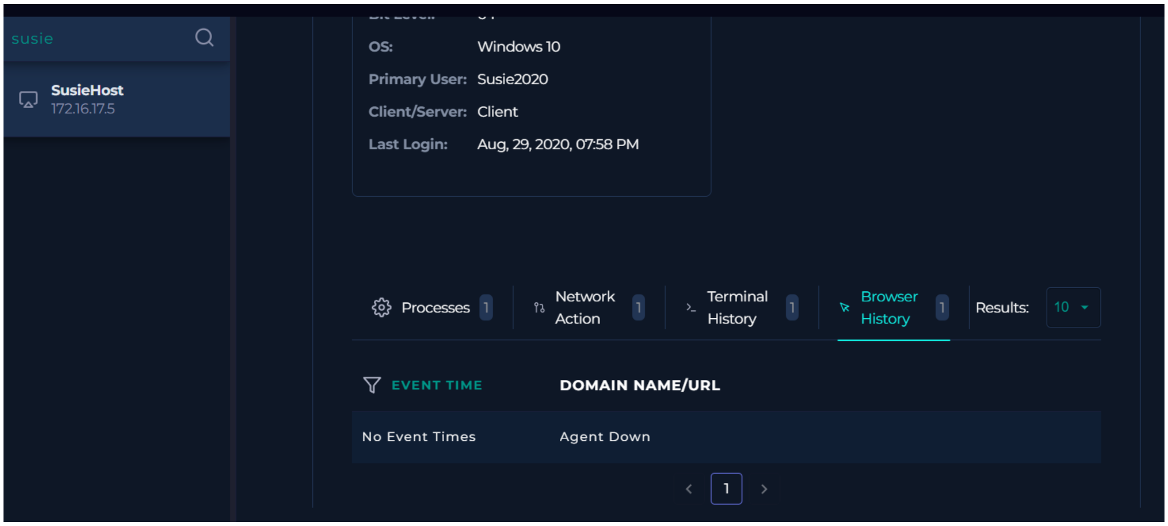
During endpoint analysis, the following condition was observed:

Agent Status:

Agent Down

This indicates that the endpoint security agent was not communicating with the EDR management server, resulting in:

- Loss of real-time telemetry
- Inability to collect behavioral logs
- Reduced endpoint visibility during the incident windo



OS: Windows 10

Primary User: Susie2020

Client/Server: Client

Last Login: Aug, 29, 2020, 07:58 PM

EVENT TIME	DOMAIN NAME/URL
No Event Times	Agent Down

Endpoint Activity Review

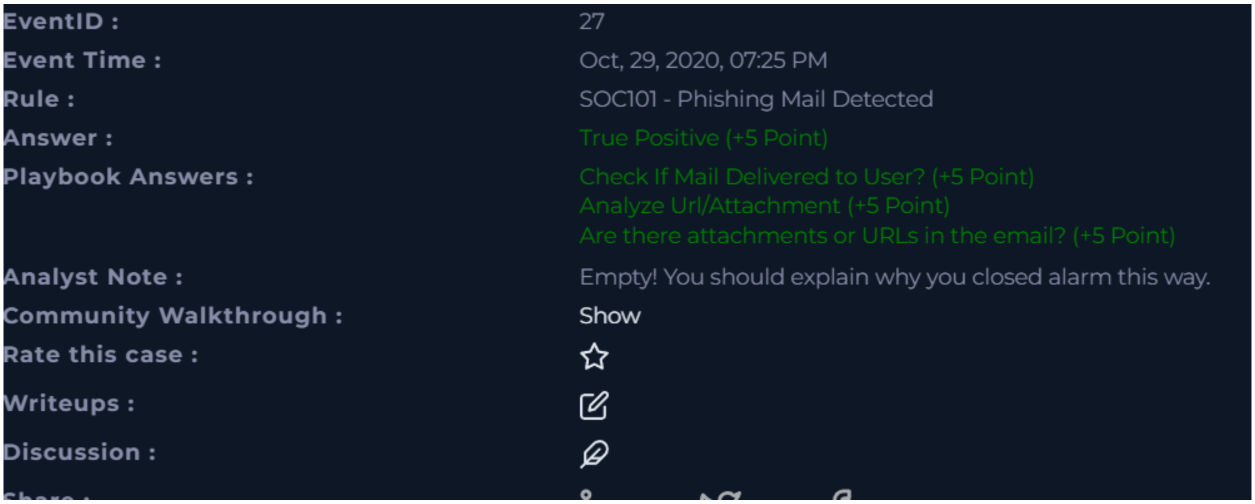
- **Processes:** No confirmed malicious processes observed
- **Network Activity:** No outbound C2 traffic detected
- **Terminal Activity:** No suspicious commands identified
- **Browser History:** No confirmed successful exploitation observed

Due to the EDR agent being offline, historical visibility was limited and could not fully confirm user interaction with the malicious link.

Investigation Questions :

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
- **Are there any attachments?** No



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 :	Empty! You should explain why you closed alarm this way.
Community Walkthrough :	Show
Rate this case :	☆
Writeups :	
Discussion :	
Share :	