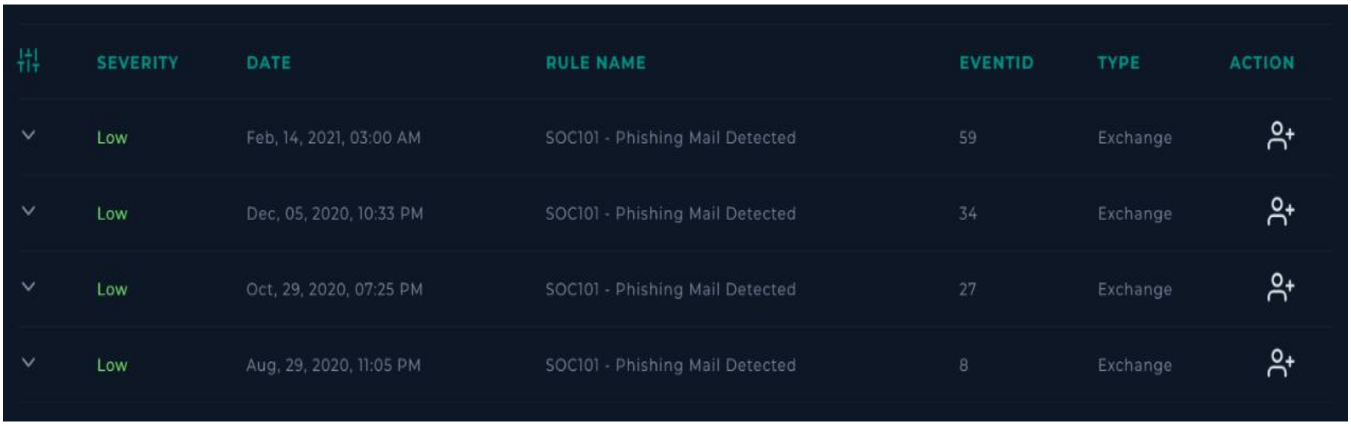
Phishing Alerts Analysis Report

Platform: LetsDefend

Frome: Asem Reda

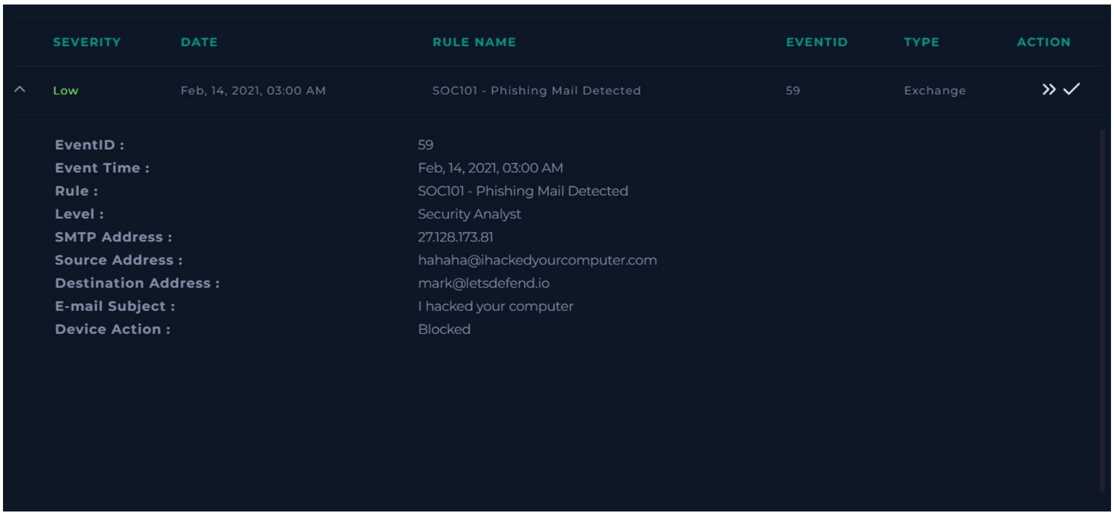
Diploma: Cybersecurity 87

Introduction: This report provides an analysis of four phishing alerts using the 5W1H methodology, discovered through the SOC101 database in LetsDefend. The purpose of this report is to document the threat indicators, methods, and outcomes associated with each alert.



SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
Low	Feb, 14, 2021, 03:00 AM	SOC101 - Phishing Mail Detected	59	Exchange	
Low	Dec, 05, 2020, 10:33 PM	SOC101 - Phishing Mail Detected	34	Exchange	
Low	Oct, 29, 2020, 07:25 PM	SOC101 - Phishing Mail Detected	27	Exchange	
Low	Aug, 29, 2020, 11:05 PM	SOC101 - Phishing Mail Detected	8	Exchange	

First Alert: Event ID 59



SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
Low	Feb, 14, 2021, 03:00 AM	SOC101 - Phishing Mail Detected	59	Exchange	» ✓

EventID :	59
Event Time :	Feb, 14, 2021, 03:00 AM
Rule :	SOC101 - Phishing Mail Detected
Level :	Security Analyst
SMTP Address :	27.128.173.81
Source Address :	hahaha@ihackedyourcomputer.com
Destination Address :	mark@letsdefend.io
E-mail Subject :	I hacked your computer
Device Action :	Blocked

Who:

The sender is a suspicious address (ihackedyourcomputer...) and the recipient is mark@letsdefend.io

What:

A phishing/extortion scam email containing a threatening message with no links or attachments

When:

February 14, 2021 at 03:00 AM

Where:

The email was sent through an SMTP server using the IP address 27.128.173.81

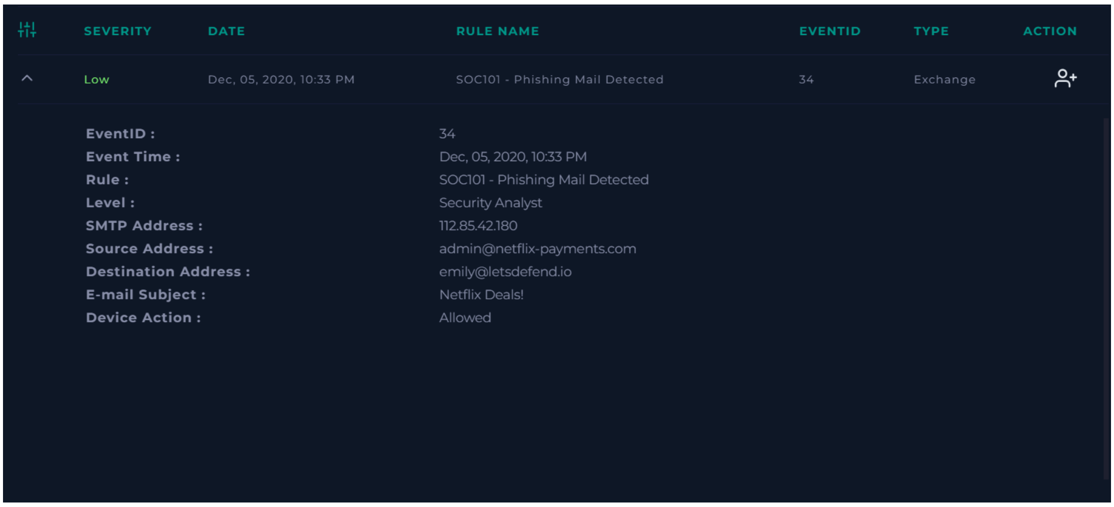
Why:

The attacker attempted to intimidate and extort the user through a threatening message

How:

The email was sent as plain text from an untrusted source. The system automatically blocked the email, preventing it from reaching the user

Second Alert: Event ID 34



SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
Low	Dec, 05, 2020, 10:33 PM	SOC101 - Phishing Mail Detected	34	Exchange	

EventID :	34
Event Time :	Dec, 05, 2020, 10:33 PM
Rule :	SOC101 - Phishing Mail Detected
Level :	Security Analyst
SMTP Address :	112.85.42.180
Source Address :	admin@netflix-payments.com
Destination Address :	emily@letsdefend.io
E-mail Subject :	Netflix Deals!
Device Action :	Allowed

WHO:
The email was sent from **admin@netflix-payments.com**, impersonating Netflix.
The targeted user is **emily@letsdefend.io**.

WHAT:
A phishing email claiming to offer “Netflix Deals!” was detected.
The email attempts to lure the user to click a potentially malicious link.
No malware or attachments were observed in the email.

WHEN:
The phishing email was received on **December 05, 2020 at 10:33 PM**.

WHERE:
The event appeared in the **Email Security system**.
The Log Management records were also checked to identify any connection to the malicious link or C2 address.

WHY:
The attacker impersonates Netflix and uses fake offers to trick the user into interacting with phishing content. This method is usually used to steal login credentials or redirect victims to malicious websites.

HOW:
Records show that the user **clicked on the malicious link**, which could have exposed them to credential theft or redirected them to a malicious site.

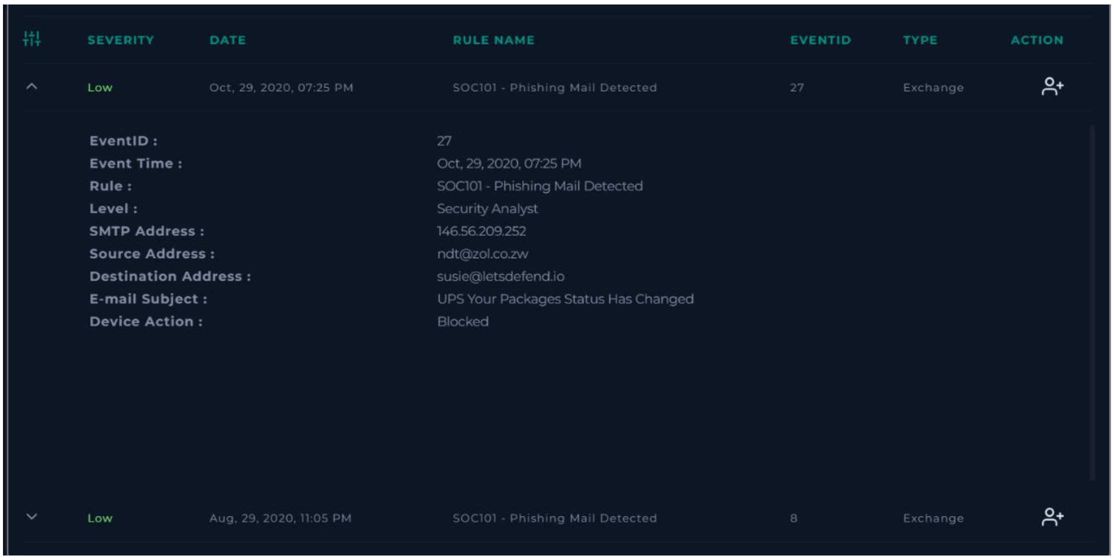
Immediate actions were taken:

The user’s machine was **contained** via EDR to prevent further compromise.

Artifacts including sender email, SMTP IP, subject, and URL were collected for analysis.

Credentials associated with the affected user account were **reset** as a precaution.

Third Alert: Event ID 27



SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
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

SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
Low	Aug, 29, 2020, 11:05 PM	SOC101 - Phishing Mail Detected	8	Exchange	

What:

A phishing email was detected containing a malicious URL impersonating a secure message from "Veterans United." The URL leads to a fraudulent website commonly used in phishing attacks.

Who:

The targeted user is:
susie@letsdefend.io
The email was sent from an untrusted sender:
ndt@zol.co.zw

When:

The alert was generated on:
2020-10-11 14:05:02 (according to the alert details).

Where:

The incident occurred within the organization's email system. The security solution analyzed and flagged the suspicious email.

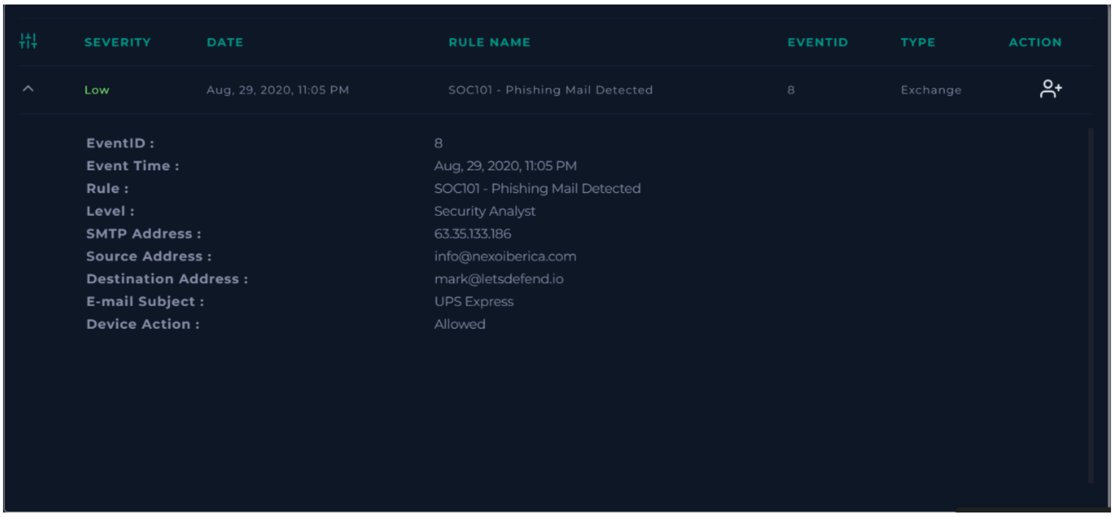
Why:

The attacker attempted to deceive the user into clicking the malicious link, likely aiming to steal credentials or redirect the victim to a phishing page.

How:

The attacker included a malicious URL:
https://hredoybangladesh.com/content/docs/wvoiha4vd1aqty/
The email impersonated Veterans United to appear legitimate.
The system blocked the email before reaching the user (**Device Action: Blocked**) and sandbox analysis confirmed the URL is **malicious**.

fourth Alert: Event ID 8



SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
Low	Aug, 29, 2020, 11:05 PM	SOC101 - Phishing Mail Detected	8	Exchange	

EventID :	8
Event Time :	Aug, 29, 2020, 11:05 PM
Rule :	SOC101 - Phishing Mail Detected
Level :	Security Analyst
SMTP Address :	63.35.133.186
Source Address :	info@nexoiberica.com
Destination Address :	mark@letsdefend.io
E-mail Subject :	UPS Express
Device Action :	Allowed

Who:
The sender is a suspicious address (info@nexoiberica.com) and the recipient is mark@letsdefend.io.

What:
A phishing email pretending to be from UPS Express, attempting to trick the recipient. The email contained a **malicious file** that was opened by the user.

When:
August 29, 2020 at 11:05 PM.

Where:
The email was sent through the SMTP server with IP address 63.35.133.186.

Why:
The attacker attempted to deceive the user into interacting with the content in order to execute malware or steal sensitive information.

How:
The email was sent from an untrusted source and included a malicious attachment. After the user opened the file and malicious activity was detected, **the affected device was isolated and removed from the network to prevent further spread**.