Author: Jack Fitzgerald

Official Incident Report

Date: Oct, 29, 2020, 07:25 PM

Event ID: 27

Rule Name: SOC101 - Phishing Mail Detected

Table of Contents

Alert Details 2
Detection 3
Verify 4
Analysis 5
Containment 6
Summary 7
Lessons Learned 8
Remediation Actions 9
Appendix 9
MITRE ATT&CK 10
Artifacts 10
LetsDefend Playbook 10

Alert Details

Severity: Low

Type: Exchange

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

Based on the information provided in the alert, it appears that a suspicious **phishing email** sent to **susie@letsdefend.io** has been detected. The alert is triggered by rule SOC101 - Phishing Mail Detected.

Upon reviewing the alert, it is observed that an email with the subject **UPS Your Package Status Has Changed** was sent from **ndt@zol.co.zw** with an SMTP of **146.56.209.252**.

The device action is marked **blocked**, indicating that the email was not delivered to the **susie@letsdefend.io** inbox.

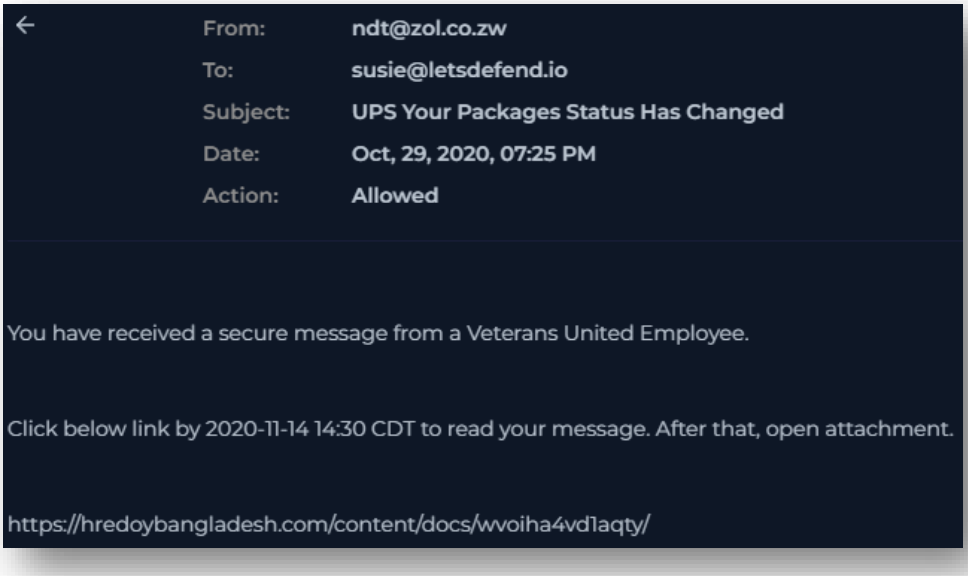
Overall, it appears that the email may be suspicious, and further investigation is needed to identify the extent of the alert and determine if any necessary actions are required to remediate the situation.

Detection

Verify

As a security analyst, one of the first steps we take to verify the alert and determine whether it is a **false positive** or a **true positive** incident is to analyse the logs collected from the host by our security products.

By searching for the email sender of **ndt@zol.co.zw** in Log Management, we can find the email and some further details.



The first step we take when investigating a potential phishing email is to parse the email information.

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's address?

ndt@zol.co.zw

What is the recipient's address?

susie@letsdefend.io

Analysis

The next step is to determine whether there are any **Attachments** or **URLs** in the email. If the email is malicious, the recipient may be exposed to an attack. In this case, there is an identified URL **https://hredoybangladesh.com/content/docs/wvoiha4vd1aqty/**.

We can scan this URL using online analysis tools such as **VirusTotal** and **URLhaus**, to determine its behaviour and whether this link is malicious.

https://www.virustotal.com/gui/url/2825a389272fd0e4b9923c98644a1786d4019ec7002c0a718b59dbe6d713a889

11/98 security vendors flagged this URL as malicious

The link is hosted by **hredoybangladesh.com** domain, and after examining the outputs, it becomes clear that this file is malicious.

https://urlhaus.abuse.ch/url/698975/

While the URL referenced has been used by **bad actors to spread malware** in the past, the **malicious content** has obviously been **removed** around **2022-12-20**. Hence, the website should no longer represent a threat. As a result, URLhaus considers this record historical.

As the email was **blocked** before it could be delivered to **susie@letsdefend.io** mailbox, further analysis of Log Management and Endpoint Security is not required.

Containment

Based on the information gathered during the investigation, it is highly unlikely that the system has been compromised. The system is not required to be isolated from the network to prevent further data loss or unauthorized access.

Summary

The incident does not involve a compromised system. The alert was triggered by the detection of a suspicious **phishing email**, sent to **susie@letsdefend.io**, based on the rule SOC101 - Phishing Mail Detected.

Upon further analysis, it was discovered that the suspicious email contained a malicious URL link **https://hredoybangladesh.com/content/docs/wvoiha4vd1aqty/**. The link requires an attachment download after accessing it and was confirmed as malicious by various security vendors and online analysis tools.

The findings indicate an unsuccessful phishing attempt on our LetsDefend user **susie@letsdefend.io**. The incident does not raise concerns about security protocols.

Lessons Learned

- Email security controls were sufficient this time around, perhaps due to the attacker's Zimbabwe email address or that it referenced UPS, a previous phishing attempt subject

- While our system prevented this attempt, the organization should not be complacent, and phishing awareness and tests should still be applied

Remediation Actions

- Delete the identified email and maintain a block to the email sender and associated IPs and URLs

- Improve email filtering rules, and enable Attachment/URL scanning/sandboxing

- Conduct targeted security awareness training, focusing on social engineering recognition and reporting suspicious emails promptly

- Run simulated phishing campaigns to test and improve readiness

Appendix

MITRE ATT&CK

MITRE Tactics	MITRE Techniques
Reconnaissance	T1598.003 - Spearfishing Link

Artifacts

Value	Comment	Type
https://hredoybangladesh.com/content/docs/wvoiha4vd1aqty/	Found inside email	URL Address
ndt@zol.co.zw		E-mail Sender
zol.co.zw	Zimbabwe domain	E-mail Domain

LetsDefend Playbook

LetsDefend Event ID: 27