Author: Jack Fitzgerald


# Official Incident Report

**Date:** Feb 14, 2021, 03:00 AM

**Event ID:** 59

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

# Table of Contents

# Alert Details

**Severity:** Low

**Type:** Exchange

**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

Based on the information provided in the alert, it appears that a suspicious **phishing email** sent to **mark@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 **I hacked your computer** was sent from **hahaha@ihackedyourcomputer.com** with an SMTP of **27.128.173.81**.

The device action is marked **blocked**, indicating that the email was not delivered to the **mark@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 **hahaha@ihackedyourcomputer.com** in Email Security, 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?**

Feb, 14, 2021, 03:00 AM

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

27.128.173.81

**What is the sender's address?**

hahaha@ihackedyourcomputer.com

**What is the recipient's address?**

mark@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 a URL or Attachment identified.

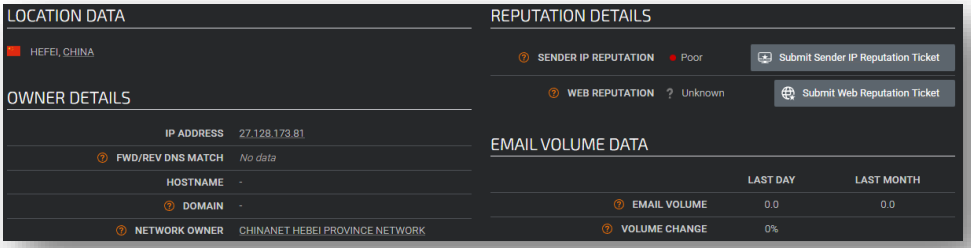
Therefore, the next step we can take is to analyse the SMTP address **27.128.173.81** provided. We upload this to online analysis tools such as **VirusTotal**, **AbuseIPDB**, and **Talos Intelligence** to determine its behaviour and whether this address is malicious.

https://www.virustotal.com/gui/ip-address/27.128.173.81

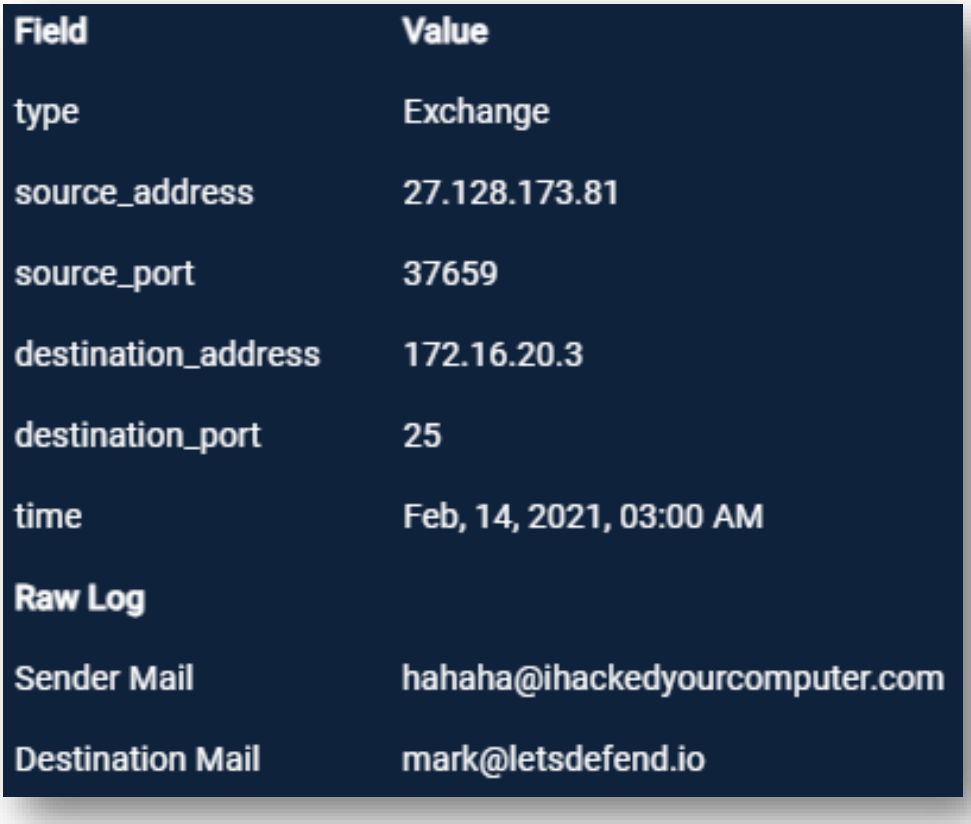
**10+ detected files embedding this IP address**

https://www.abuseipdb.com/check/27.128.173.81


https://talosintelligence.com/reputation_center/lookup?search=27.128.173.81




As part of the analysis, we can investigate deeper by searching for the IP of **27.128.173.81** in Log Management to see if we can find any extra information.




We can see here only the information that we already know, indicating no further activity in this incident.

# Containment

Based on the information gathered during the investigation, it is highly unlikely that the system has been compromised. Isolation of the system from the network is not required.

# Summary

The incident involves no compromised system. The alert was triggered by the detection of a suspicious **phishing email**, sent to **mark@letsdefend.io**, based on the rule SOC101 - Phishing Mail Detected.

Upon further analysis, it was discovered that the suspicious email contained no URL or Attachment, only a message containing boastful language, claiming to have hacked the user's files. The SMTP address was confirmed as suspicious by various security vendors and online analysis tools.

The analysis of Log Management revealed no further activity involved in this incident.

The findings indicate a blocked phishing attempt on our LetsDefend user **mark@letsdefend.io**.

## Lessons Learned

- Email security controls were sufficient in preventing this attack, but email rules and filters should still be applied and improved

## Remediation Actions

- Delete the identified email from the user's inbox and maintain a block to the email sender and associated IPs

- 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 | T1598.001 - Spearfishing Service |

## Artifacts

| Value | Comment | Type |
|---|---|---|
| hahaha@ihackedyourcomputer.com | Clearly malicious, phishing | E-mail Sender |
| ihackedyourcomputer.com | | E-mail Domain |
| 27.128.173.81 | SMTP address | IP Address |

## LetsDefend Playbook

LetsDefend Event ID: 59