SOC101 – Phishing Investigation Report

Challenge 1 – Let'sDefend EventID 59

Student Name: Romaissaa Moftah

Course: Cybersecurity / SOC Analysis

Instructor: Eng. Taha Abouelhgag

1. Executive Summary

On February 14, 2021, at 03:00 AM, a phishing alert was generated by the SOC101 rule on the Exchange email system. The alert indicated a suspicious email attempting to extort the recipient by claiming the sender had compromised the victim's computer and obtained personal files. The email was successfully blocked by the security system before reaching the user's inbox.

The investigation focused on analyzing the sender, source IP address, email content, and associated indicators of compromise (IOCs) to determine whether the event was malicious or a false positive.

2. Alert Information

Event ID: 59

Event Time: Feb 14, 2021 – 03:00 AM

Rule Name: SOC101 – Phishing Mail Detected

Severity Level: Security Analyst

Device: Exchange

Action Taken: Blocked

3. Email Details

Sender Email: hahaha@ihackedyourcomputer.com

Recipient Email: mark@letsdefend.io

Subject: I hacked your computer

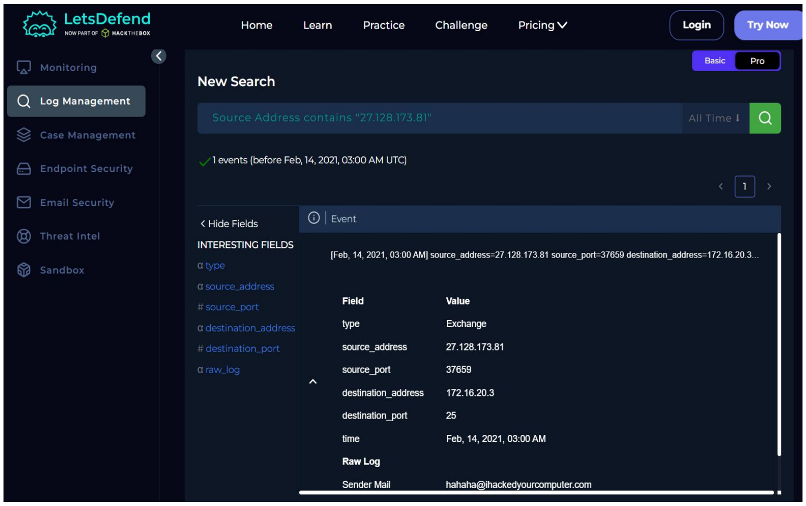
Source IP: 27.128.173.81

Source Port: 37659 (TCP)

Destination IP: 172.16.20.3

Destination Port: 25 (SMTP)

Protocol: SMTP



New Search

Source Address contains "27.128.173.81"

✓ 1 events (before Feb, 14, 2021, 03:00 AM UTC)

```
[Feb, 14, 2021, 03:00 AM] source_address=27.128.173.81 source_port=37659 destination_address=172.16.20.3...
```

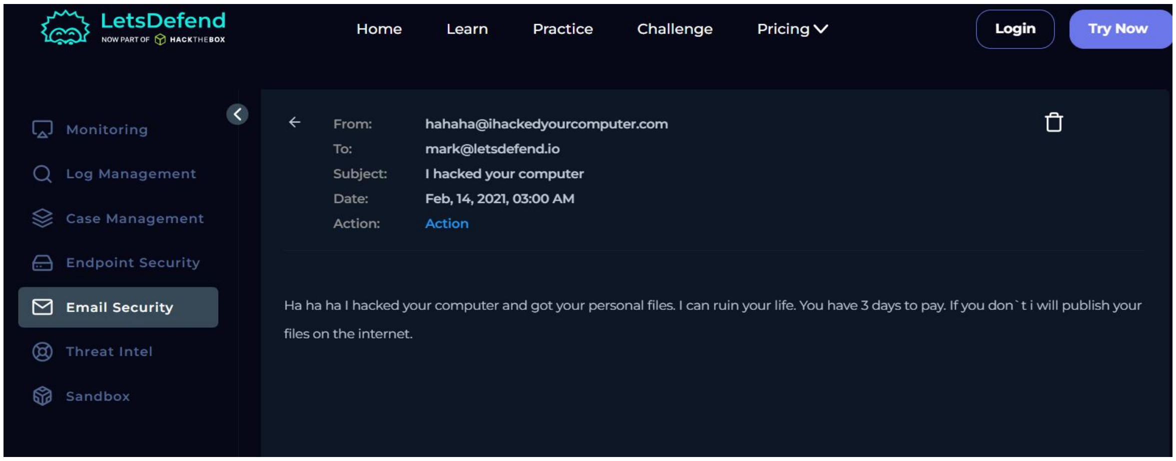
Field	Value
type	Exchange
source_address	27.128.173.81
source_port	37659
destination_address	172.16.20.3
destination_port	25
time	Feb, 14, 2021, 03:00 AM
Raw Log	
Sender Mail	hahaha@ihackedyourcomputer.com

Time: Feb 14, 2021 – 03:00 AM

4. Raw Log Analysis

Email Content:

"Ha ha ha I hacked your computer and got your personal files. I can ruin your life. You have 3 days to pay. If you don’t, I will publish your files on the internet."



From: hahaha@ihackedyourcomputer.com
To: mark@letsdefend.io
Subject: I hacked your computer
Date: Feb, 14, 2021, 03:00 AM
Action: Action

Ha ha ha I hacked your computer and got your personal files. I can ruin your life. You have 3 days to pay. If you don`t i will publish your files on the internet.

Observations:

- The email contains threatening and extortion-based language.

- Claims unauthorized access to the victim’s system.

- Requests payment within a limited time frame.

- Uses psychological pressure and fear tactics.

This behavior is a classic phishing and extortion scam pattern.

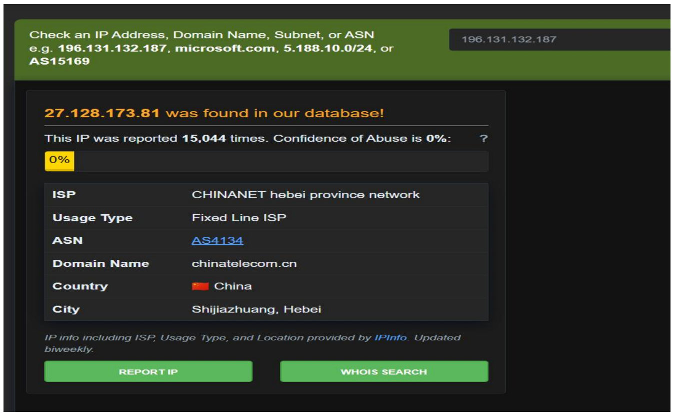
5. Indicator of Compromise (IOC) Analysis

IP Address: 27.128.173.81

Country: China

ASN: AS4134 (China Telecom)

Reported Activity: SSH Brute Force, Web Attacks



Check an IP Address, Domain Name, Subnet, or ASN
e.g. **196.131.132.187**, **microsoft.com**, **5.188.10.0/24**, or **AS15169**

196.131.132.187

27.128.173.81 was found in our database!

This IP was reported **15,044** times. Confidence of Abuse is **0%**: ?

0%

ISP	CHINANET hebei province network
Usage Type	Fixed Line ISP
ASN	AS4134
Domain Name	chinatelecom.cn
Country	China
City	Shijiazhuang, Hebei

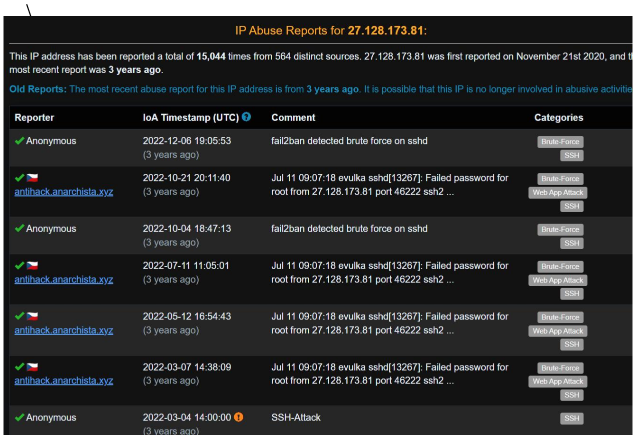
IP info including ISP, Usage Type, and Location provided by IPInfo. Updated biweekly.

Reputation: Historically suspicious

Sender Domain: ihackedyourcomputer.com

This domain is suspicious and not associated with any legitimate organization. It appears to be designed for intimidation and social engineering.

\

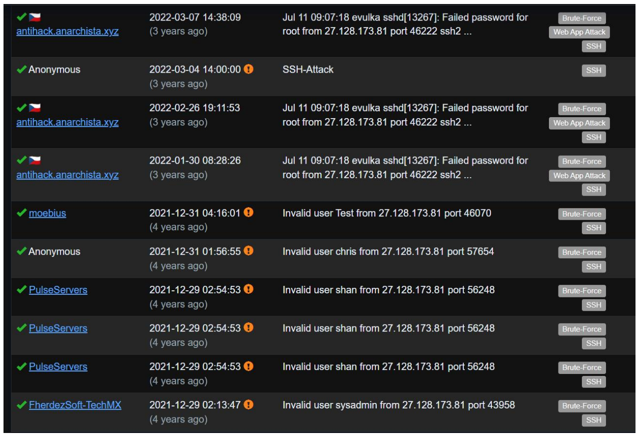


IP Abuse Reports for **27.128.173.81**:

This IP address has been reported a total of **15,044** times from 564 distinct sources. 27.128.173.81 was first reported on November 21st 2020, and t
most recent report was **3 years ago**.

Old Reports: The most recent abuse report for this IP address is from **3 years ago**. It is possible that this IP is no longer involved in abusive activitie

Reporter	IoA Timestamp (UTC)	Comment	Categories
✓ Anonymous	2022-12-06 19:05:53 (3 years ago)	fail2ban detected brute force on sshd	Brute-Force SSH
✓ 🇨🇿 antihack.anarchista.xyz	2022-10-21 20:11:40 (3 years ago)	Jul 11 09:07:18 evulka sshd[13267]: Failed password for root from 27.128.173.81 port 46222 ssh2 ...	Brute-Force Web App Attack SSH
✓ Anonymous	2022-10-04 18:47:13 (3 years ago)	fail2ban detected brute force on sshd	Brute-Force SSH
✓ 🇨🇿 antihack.anarchista.xyz	2022-07-11 11:05:01 (3 years ago)	Jul 11 09:07:18 evulka sshd[13267]: Failed password for root from 27.128.173.81 port 46222 ssh2 ...	Brute-Force Web App Attack SSH
✓ 🇨🇿 antihack.anarchista.xyz	2022-05-12 16:54:43 (3 years ago)	Jul 11 09:07:18 evulka sshd[13267]: Failed password for root from 27.128.173.81 port 46222 ssh2 ...	Brute-Force Web App Attack SSH
✓ 🇨🇿 antihack.anarchista.xyz	2022-03-07 14:38:09 (3 years ago)	Jul 11 09:07:18 evulka sshd[13267]: Failed password for root from 27.128.173.81 port 46222 ssh2 ...	Brute-Force Web App Attack SSH
✓ Anonymous	2022-03-04 14:00:00 ❗ (3 years ago)	SSH-Attack	SSH



✓ 🇨🇿 antihack.anarchista.xyz	2022-03-07 14:38:09 (3 years ago)	Jul 11 09:07:18 evulka sshd[13267]: Failed password for root from 27.128.173.81 port 46222 ssh2 ...	Brute-Force Web App Attack SSH
✓ Anonymous	2022-03-04 14:00:00 ❗ (3 years ago)	SSH-Attack	SSH
✓ 🇨🇿 antihack.anarchista.xyz	2022-02-26 19:11:53 (3 years ago)	Jul 11 09:07:18 evulka sshd[13267]: Failed password for root from 27.128.173.81 port 46222 ssh2 ...	Brute-Force Web App Attack SSH
✓ 🇨🇿 antihack.anarchista.xyz	2022-01-30 08:28:26 (3 years ago)	Jul 11 09:07:18 evulka sshd[13267]: Failed password for root from 27.128.173.81 port 46222 ssh2 ...	Brute-Force Web App Attack SSH
✓ moebius	2021-12-31 04:16:01 ❗ (4 years ago)	Invalid user Test from 27.128.173.81 port 46070	Brute-Force SSH
✓ Anonymous	2021-12-31 01:56:55 ❗ (4 years ago)	Invalid user chris from 27.128.173.81 port 57654	Brute-Force SSH
✓ PulseServers	2021-12-29 02:54:53 ❗ (4 years ago)	Invalid user shan from 27.128.173.81 port 56248	Brute-Force SSH
✓ PulseServers	2021-12-29 02:54:53 ❗ (4 years ago)	Invalid user shan from 27.128.173.81 port 56248	Brute-Force SSH
✓ PulseServers	2021-12-29 02:54:53 ❗ (4 years ago)	Invalid user shan from 27.128.173.81 port 56248	Brute-Force SSH
✓ FherdezSoft-TechMX	2021-12-29 02:13:47 ❗ (4 years ago)	Invalid user sysadmin from 27.128.173.81 port 43958	Brute-Force SSH

6. Attack Classification

This incident is classified as:

Confirmed Phishing and Extortion Attempt

7. Impact Assessment

If the email had reached the recipient, it could have resulted in:

- Financial loss

- Psychological stress

- Risk of further communication with attackers

The threat was successfully blocked, preventing user exposure.

8. Response Actions Taken

- Email blocked by Exchange security system

- Alert logged in SOC platform

- IP and domain investigated using threat intelligence tools

- Incident documented for reporting

9. Recommendations

- Implement advanced spam filtering

- Block high-risk IP ranges

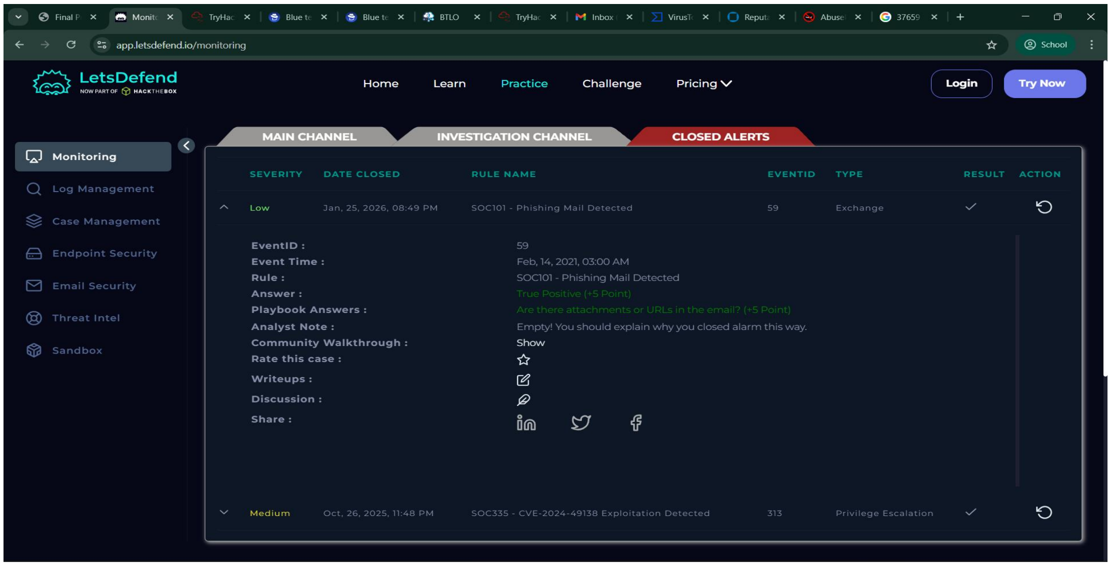
- Enable DMARC, SPF, and DKIM

- Conduct phishing awareness training

- Monitor SMTP traffic continuously

10. Final Verdict

This alert represents a confirmed malicious phishing and extortion attempt. The SOC system successfully detected and blocked the threat before it reached the end user.



SEVERITY	DATE CLOSED	RULE NAME	EVENTID	TYPE	RESULT	ACTION
Low	Jan, 25, 2026, 08:49 PM	SOC101 - Phishing Mail Detected	59	Exchange	✓	↺
Medium	Oct, 26, 2025, 11:48 PM	SOC335 - CVE-2024-49138 Exploitation Detected	313	Privilege Escalation	✓	↺

EventID : 59
Event Time : Feb, 14, 2021, 03:00 AM
Rule : SOC101 - Phishing Mail Detected
Answer : True Positive (+5 Point)
Playbook Answers : 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 :

11. Detailed Email Investigation Questions

1. **When was it sent?**

   The email was sent on February 14, 2021, at 03:00 AM.

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

   27.128.173.81

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

   hahaha@ihackedyourcomputer.com

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

   mark@letsdefend.io

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

   Yes. The content contains threats, extortion demands, and claims of unauthorized access, which align with social engineering attacks.

6. **Are there any attachments?**

   No. The email did not contain any attachments. The attack relies solely on psychological manipulation.