Author: Jack Fitzgerald

Official Incident Report

Date: Apr, 04, 2021, 11:00 PM

Event ID: 87

Rule Name: SOC101 - Phishing Mail Detected

Table of Contents

Alert Details 2
Detection 3
Verify 4
Analysis 5
Containment 8
Summary 9
Lessons Learned 10
Remediation Actions 11
Appendix 11
MITRE ATT&CK 12
Artifacts 12
LetsDefend Playbook 12

Alert Details

Severity: Medium

Type: Exchange

SMTP Address: 146.56.195.192

Source Address: lethuyan852@gmail.com

Destination Address: mark@letsdefend.io

E-mail Subject: Its a Must have for your Phone

Device Action: Allowed

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 **Its a Must have for your Phone** was sent from **lethuyan852@gmail.com** with an SMTP of **146.56.195.192**.

The device action is marked **allowed**, indicating that the email was delivered to the **mark@letsdefend.io** inbox.

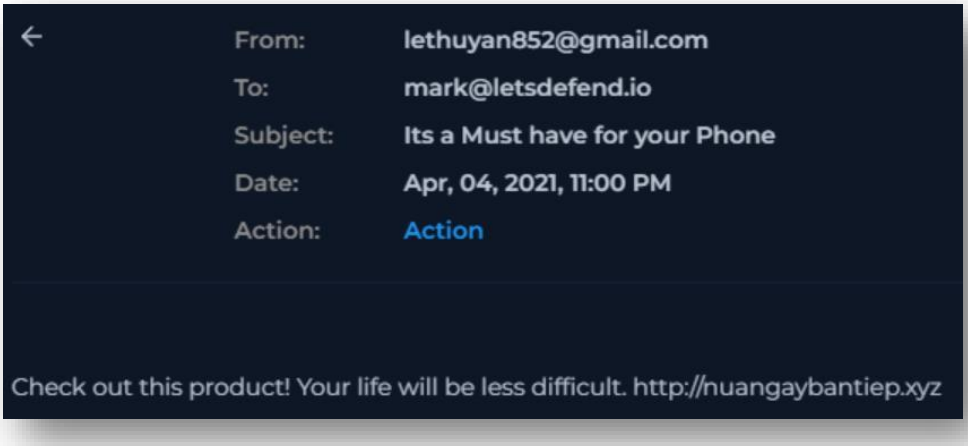
Overall, it appears that the email may be suspicious, and further investigation is needed to identify the extent of the alert and determine if any necessary actions are required to remediate the situation.

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 **lethuyan852@gmail.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?

Apr, 04, 2021, 11:00 PM

What is the email's SMTP address?

146.56.195.192

What is the sender's address?

lethuyan852@gmail.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 **http://nuangaybantiep.xyz** identified.

The first step is to analyse the SMTP address **146.56.195.192** provided. We upload this to online analysis tools such as **VirusTotal** and **AbuseIPDB** to determine its behaviour and whether this address is malicious.

https://www.virustotal.com/gui/ip-address/146.56.195.192

1/95 security vendor flagged this IP address as malicious

https://www.abuseipdb.com/check/146.56.195.192

This address originates from Nanjing, Jiangsu, China. The provider is Shenzhen Tencent Computer Systems Company Limited, which is clearly not related to Gmail's SMTP services. It is understood that the attacker is spoofing their email address to appear as coming from a Gmail address to look legitimate.

The next step we want to perform is to analyse the URL **http://nuangaybantiep.xyz** contained within the email.

https://www.virustotal.com/gui/url/8aa638d1cea36f48c06fc55e532bafbc39cd66ba5ccde7f6ac004a70fb3cec00

No security vendors flagged this URL as malicious

As part of the analysis, we can investigate deeper by searching for the IP of **172.16.17.88** in Log Management to see if we can find any extra information. We know this IP is assigned to **mike@letsdefend.io** due to previous incident reports.

source_port	39483
destination_address	192.64.119.190
destination_port	80
time	Apr, 04, 2021, 11:10 PM
Raw Log	
Request URL	http://nuangaybantiep.xyz
Request Method	GET
Device Action	Allowed
Process	chrome.exe
Parent Process	explorer.exe
Parent Process MD5	8b88ebbb05a0e56b7dcc708498c02b3e

We can see here new information we did not have previously. This log indicates that the **MarkPRD** host accessed the **http://nuangaybantiep.xyz** link that was identified in the

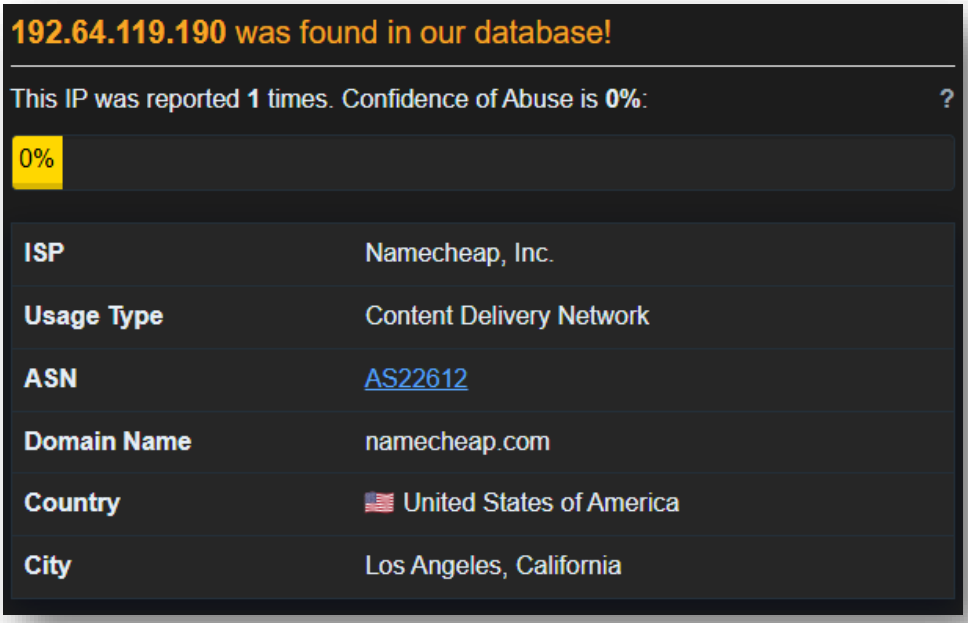
email. The request was allowed on port 80 using the HTTP protocol (unsecure) and identified with the IP address **192.64.119.190** associated with the URL.

Our next step is to analyse this newly found URL.

https://www.virustotal.com/gui/ip-address/192.64.119.190

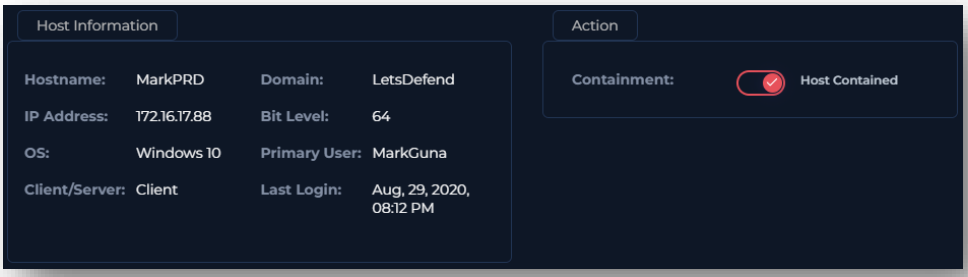
10+ detected files communicating with this IP address

https://www.abuseipdb.com/check/192.64.119.190



Containment

Based on the information gathered during the investigation, it is highly likely that the system has been compromised. Immediate isolation of the system from the network is required to prevent further spread of malicious content.



Summary

The incident involves a compromised system called **MarkPRD**. 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 URL **http://nuangaybantiep.xyz**. The SMTP address was confirmed as suspicious by various security vendors and online analysis tools.

The analysis of Log Management revealed that the user of **MarkPRD** accessed the URL in the email on port 80 using http protocol (unsecure). No further activity was found, however; the findings indicate a malicious phishing attempt on our LetsDefend user **mark@letsdefend.io**.

Lessons Learned

- Don’t access the web through port 80 as the http protocol is used, which is unsecure, allowing attackers to see all the data and information that goes through that channel

- Suspicious sender addresses, such as personal Gmail accounts should be watched for

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	T1598.003 - Spearfishing Link
Defense Evasion	T1672 - Email Spoofing

Artifacts

Value	Comment	Type
http://nuangaybantiep.xyz	Unsecure link found in phishing email	URL Address
lethuyan852@gmail.com	Personal email address	E-mail Sender
gmail.com	Spoofed domain	E-mail Domain
146.56.195.192	SMTP address	IP Address
192.64.119.190	Accessed by MarkPRD when requesting URL	IP Address

LetsDefend Playbook

LetsDefend Event ID: 87