Author: Jack Fitzgerald

LetsDefend

Official Incident Report

Date: Dec, 05, 2020, 10:33 PM

Event ID: 34

Rule Name: SOC101 - Phishing Mail Detected

Table of Contents

Alert Details

Severity: Low

Type: Exchange

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

Based on the information provided in the alert, it appears that a suspicious **phishing email** sent to **emily@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 **Netflix Deals!** was sent from **admin@netflix-payments.com** with an SMTP of **112.85.42.180**.

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

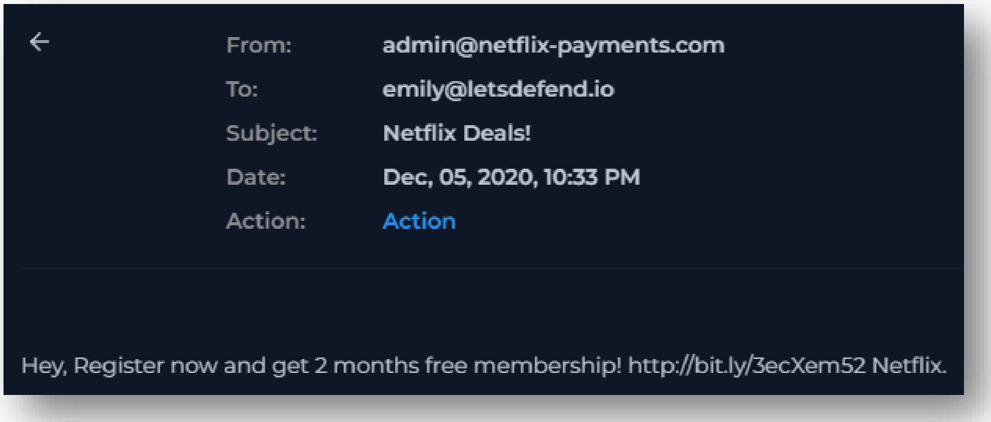
Overall, it appears that the email may be suspicious, and further investigation is needed to identify the extent of the alert and determine if any necessary actions are required to remediate the situation.

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 **admin@netflix-payments.com** in Email Security, we can find the email and some further details.



From: admin@netflix-payments.com
To: emily@letsdefend.io
Subject: Netflix Deals!
Date: Dec, 05, 2020, 10:33 PM
Action: Action

Hey, Register now and get 2 months free membership! http://bit.ly/3ecXem52 Netflix.

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

When was it sent?

Dec, 05, 2020, 10:33 PM

What is the email’s SMTP address?

112.85.42.180

What is the sender's address?

admin@netflix-payments.com

What is the recipient's address?

emily@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://bit.ly/3ecXem52** identified.

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

https://www.virustotal.com/gui/url/e913403221120948995f6609fe7ce52bf3407b06c62db94dfdffcc9aeede3c3f

1/98 security vendor flagged this URL as malicious

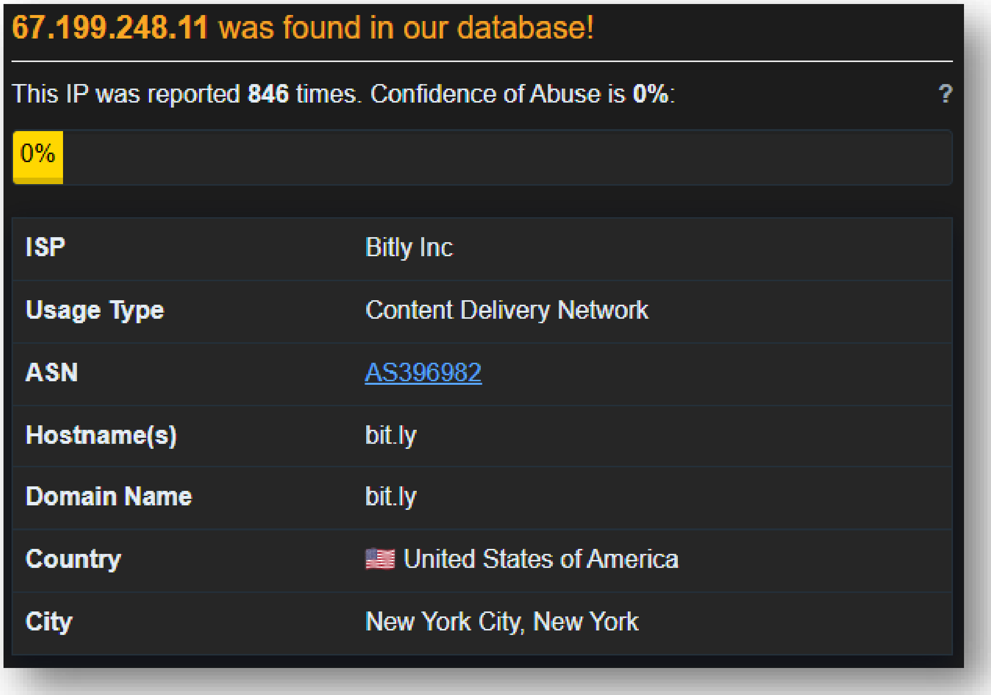
The link contains a serving IP address of **67.199.248.11**, and after examining the outputs, it becomes clear that this file is malicious.

https://www.virustotal.com/gui/ip-address/67.199.248.11

1/95 security vendor flagged this IP address as malicious

We can further analyse the IP **67.199.248.11**, which happens to be the serving IP address of the link.

https://www.abuseipdb.com/check/67.199.248.11



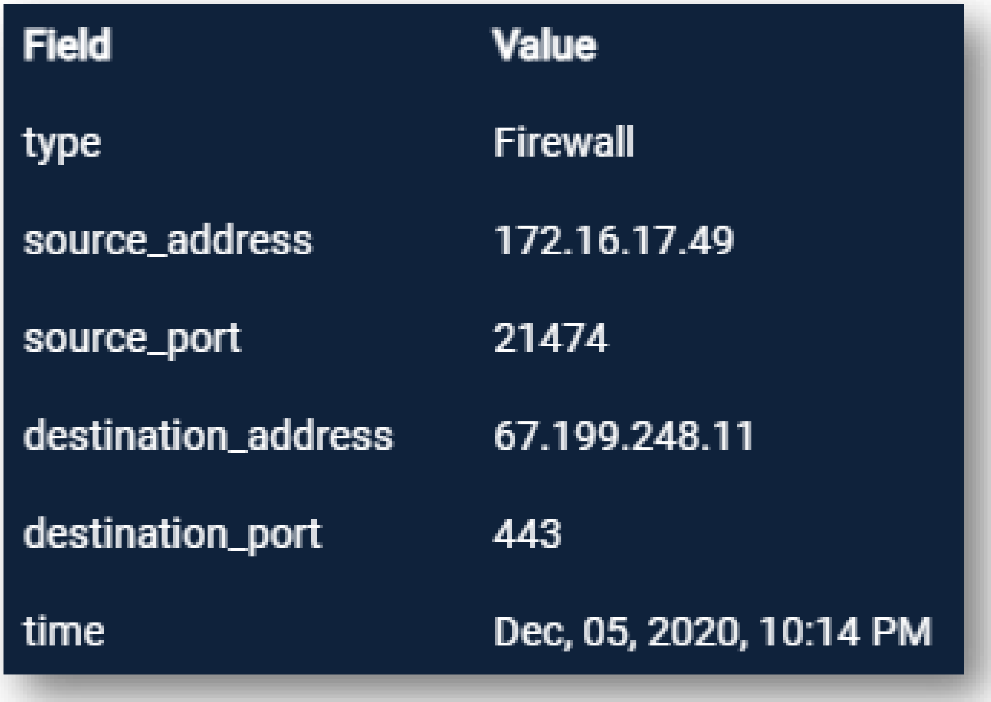
67.199.248.11 was found in our database!

This IP was reported **846** times. Confidence of Abuse is **0%**: ?

0%

ISP	Bitly Inc
Usage Type	Content Delivery Network
ASN	AS396982
Hostname(s)	bit.ly
Domain Name	bit.ly
Country	🇺🇸 United States of America
City	New York City, New York

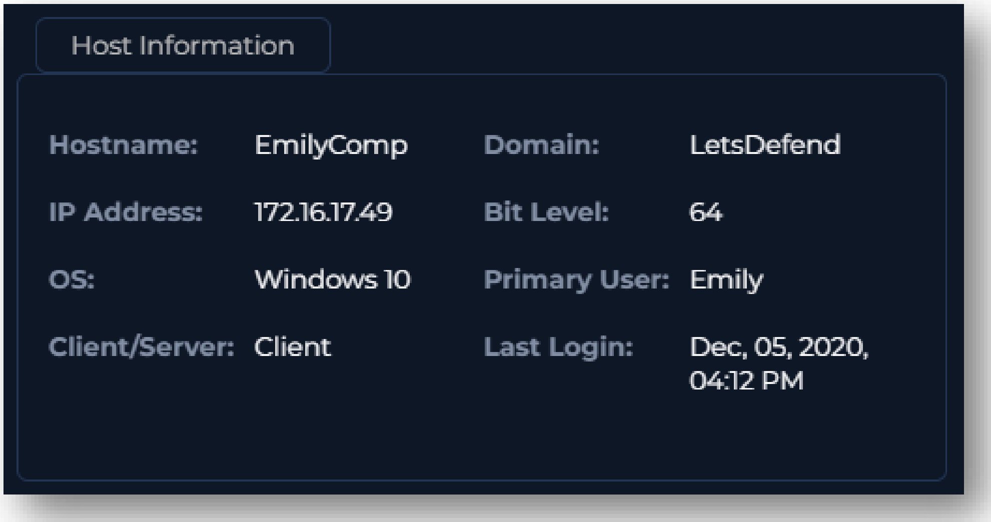
As part of the analysis, we can investigate deeper by searching for the IP of **67.199.248.11** in Log Management to determine whether the serving IP address was accessed.



Field	Value
type	Firewall
source_address	172.16.17.49
source_port	21474
destination_address	67.199.248.11
destination_port	443
time	Dec, 05, 2020, 10:14 PM

We can see here that the serving IP address was accessed at Dec, 05, 2020, 10:14 PM by device **172.16.17.49**.

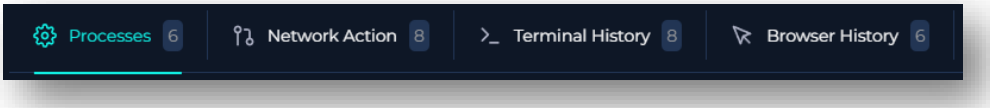
Further analysis requires us to dive into Endpoint Security, where we search for the device with the IP of **172.16.17.49**.



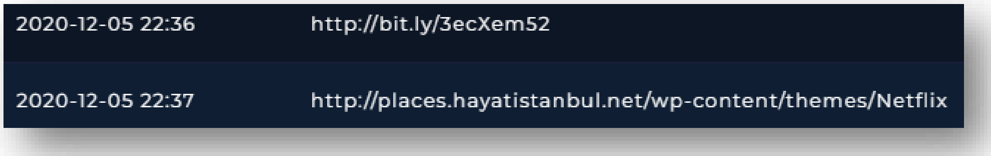
Host Information

Hostname:	EmilyComp	Domain:	LetsDefend
IP Address:	172.16.17.49	Bit Level:	64
OS:	Windows 10	Primary User:	Emily
Client/Server:	Client	Last Login:	Dec, 05, 2020, 04:12 PM

We can determine some host information from here, such as Hostname, IP Address, OS, Client/Server, Domain, Bit Level, Primary User, and Last Login.



We can also investigate Processes, Network Action, Terminal History, and Browser History.



2020-12-05 22:36	http://bit.ly/3ecXem52
2020-12-05 22:37	http://places.hayatistanbul.net/wp-content/themes/Netflix

We have identified the website sent in the email to **emily@letsdefend.io** was accessed, which brings the user to **http://places.hayatistanbul.net/wp-content/themes/Netflix**.

https://www.virustotal.com/gui/url/2098e60d4aafdbd8ca2c50621f3fe7964ae779f16d7241278f08af30dac4ac0a

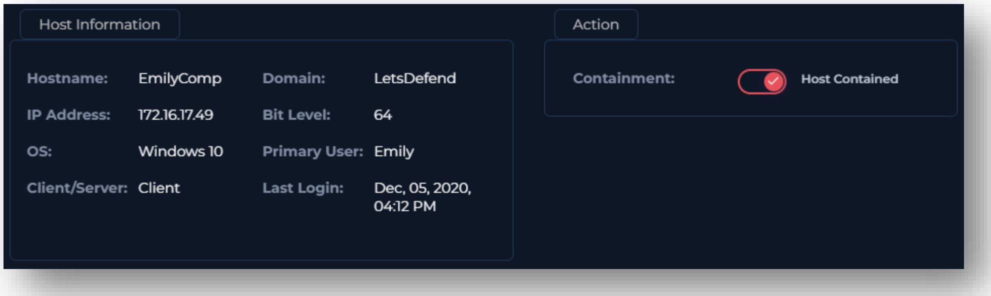
3/97 security vendors flagged this URL as malicious

Containment

Based on the information gathered during the investigation, it is highly likely that the system has been compromised. To prevent further data loss or unauthorized access, it is recommended to isolate the system from the network immediately.

Isolation of the host can be made from the endpoint security tab.

Hostname	EmilyComp
IP Address	172.16.17.49



Host Information

Hostname: EmilyComp

Domain: LetsDefend

IP Address: 172.16.17.49

Bit Level: 64

OS: Windows 10

Primary User: Emily

Client/Server: Client

Last Login: Dec, 05, 2020, 04:12 PM

Action

Containment: Host Contained

Summary

The incident involves a compromised system named **EmilyComp** with an IP address of **172.16.17.49**. The alert was triggered by the detection of a suspicious **phishing email**, sent to **emily@letsdefend.io**, based on the rule SOC101 - Phishing Mail Detected.

Upon further analysis, it was discovered that the suspicious email contained a malicious URL **http://bit.ly/3ecXem52**, with a serving IP address of **67.199.248.11**. The URL and IP were confirmed as malicious by various security vendors and online analysis tools.

The analysis of Log Management revealed that the serving IP address **67.199.248.11** was accessed by **172.16.17.49**, indicating that the user of **EmilyComp** clicked on the URL in the email.

The analysis of **EmilyComp's** browser history revealed access to **http://bit.ly/3ecXem52**, followed by access to **http://places.hayatistanbul.net/wp-content/themes/Netflix**, both being identified as malicious, matching the alert creation date, further substantiating the alert's authenticity.

The findings indicate a successful phishing attempt on our LetsDefend user **emily@letsdefend.io**. The incident raises concerns about user awareness and security protocols.

Based on the findings of the incident, immediate action was taken to isolate the compromised system, named **EmilyComp** with the IP address **172.16.17.49**. Isolation is a critical step to prevent further unauthorized access and potential spread of the compromise to other systems within the network.

Lessons Learned

- Users may always be the weakest point of security within your organisation, therefore you should always allocate resources towards educating your users on security awareness and training modules

- Email security controls may be insufficient due to attackers referencing legitimate businesses, organizations, events, etc. in their subjects and message bodies

- Privilege and access management may be too permissive, as a single compromised account may grant excessive internal access

Remediation Actions

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

- Identify and remove any malicious files downloaded during the incident

- Isolate the compromised machine from the network to prevent the attacker from accessing other resources and systems within the domain

- 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
http://bit.ly/3ecXem52	URL from email	URL Address
http://places.hayatistanbul.net/wp-content/themes/Netflix	URL accessed following bit.ly	URL Address
admin@netflix-payments.com	Non-legit, phishing	E-mail Sender
netflix-payments.com		E-mail Domain
112.85.42.180	SMTP address	IP Address
67.199.248.11	Serving IP address accessed	IP Address

LetsDefend Playbook

LetsDefend Event ID: 34