

SOC101 – Phishing Investigation Report

Challenge 2 – Let'sDefend EventID 34

Student Name: Romaissa Moftah

Course: Cybersecurity / SOC Analysis

Instructor: Eng. Taha Abouelhgag



1. Executive Summary

On December 05, 2020, at 10:33 PM, a phishing alert was generated by the SOC101 – Phishing Mail Detected rule. The alert indicated a suspicious email impersonating Netflix and offering a fake promotional deal (“2 months free membership”) to lure the recipient into clicking a shortened URL.

The investigation focused on analyzing the sender’s email address, SMTP source IP, email content, and network logs to determine whether the malicious URL was accessed and to assess the overall risk to the user and the organization.

2. Alert Information

Event ID: 34

Event Time: Dec, 05, 2020 – 10:33 PM

Rule Name: SOC101 – Phishing Mail Detected

Severity Level: Security Analyst

Device Action: Allowed

The screenshot shows the LetsDefend Endpoint Security interface. The left sidebar has navigation links: Monitoring, Log Management, Case Management, Endpoint Security (which is selected), Email Security, Threat Intel, and Sandbox. The main area displays endpoint information for a host named 'EmilyComp' with IP address '172.36.174.9'. The 'Endpoint Information' panel on the right contains the following details:

Host Information	
Hostname:	EmilyComp
Domain:	Let'sDefend
IP Address:	172.36.174.9
Bit Level:	64
OS:	Windows 10
Primary User:	Emily
Client/Server:	Client
Last Login:	Dec. 05, 2020, 04:12 PM

Below the host information is an 'Action' section with a toggle switch labeled 'Containment'.

3. Email Details

Sender Email: admin@netflix-payments.com

Recipient Email: emily@letsdefend.io

Subject: Netflix Deals!

Source IP: 112.85.42.180

Destination IP: 172.16.20.3

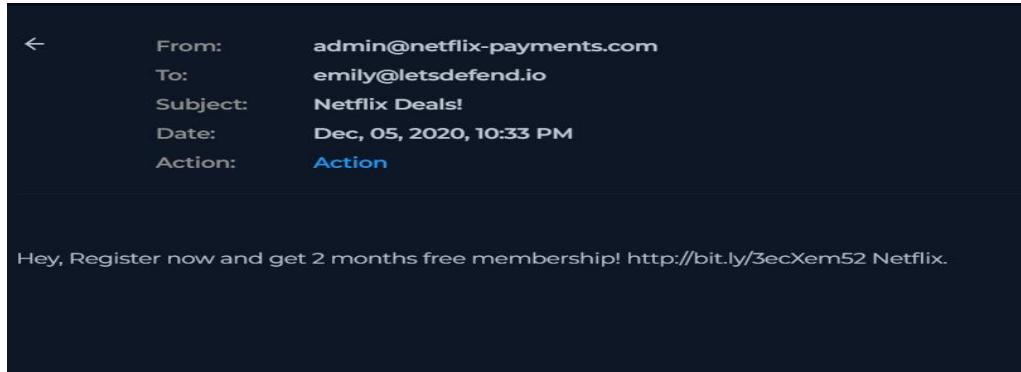
Protocol: SMTP

Time: Dec, 05, 2020 – 10:33 PM

4. Raw Log Analysis

Email Content:

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



Observations:

- The email uses brand impersonation (Netflix) to gain user trust.
- A shortened URL (bit.ly) is used to hide the final destination.
- The message promotes a too-good-to-be-true offer.
- The sender domain is not an official Netflix domain.

Network Log Findings:

No HTTP/HTTPS requests or browser activity were found related to the malicious URL. This indicates that the malicious link was not accessed.

The screenshot shows the LetsDefend network log interface. The left sidebar has a navigation menu with "Endpoint Security" selected. The main area displays a search bar with the URL "http://bit.ly/3ecXem52". Below the search bar, there are tabs for "Processes", "Network Action", "Terminal History", and "Browser History". The "Browser History" tab is active, showing a table with the following data:

EVENT TIME	DOMAIN NAME/URL
2020-12-05 14:13	https://github.com/SecurityRiskAdvisors/VECTR/blob/master/VECTREndUserLicenseAgreement.pdf
2020-12-05 14:14	https://github.com/SecurityRiskAdvisors
2020-12-05 14:15	https://github.com/SecurityRiskAdvisors/VECTR
2020-12-05 14:16	https://github.com/SecurityRiskAdvisors/VECTR/blob/master/README.md
2020-12-05 22:36	http://bit.ly/3ecXem52
2020-12-05 22:37	http://places.hayatistanbul.net/wp-content/themes/Netflix

New Search

Raw Log contains "3ecXem52"

All Time

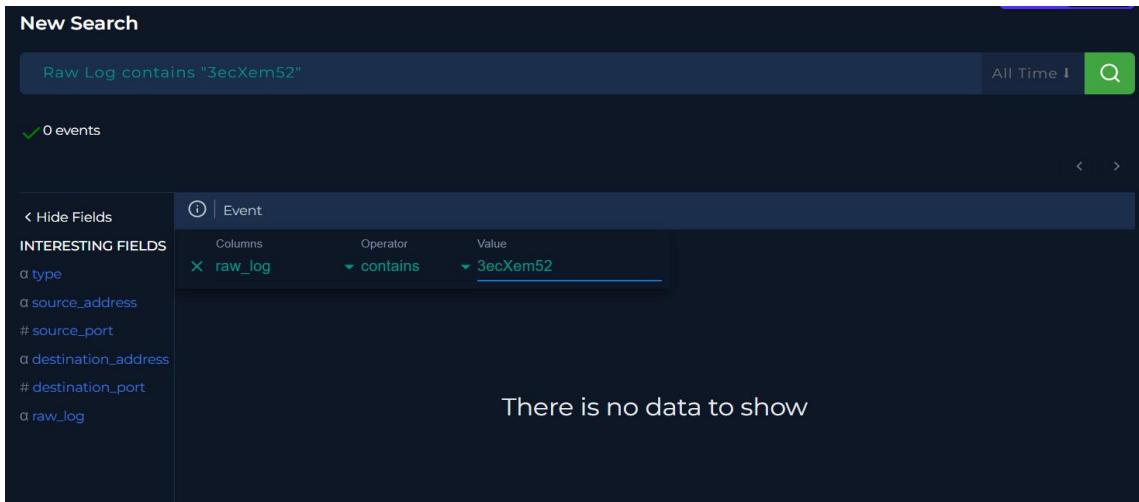
0 events

INTERESTING FIELDS

Columns	Operator	Value
X raw_log	contains	3ecXem52

Event

There is no data to show



5. Indicator of Compromise (IOC) Analysis

Source IP: 112.85.42.180

Reputation: Potentially suspicious

Sender Domain: netflix-payments.com

Analysis: Domain mimics a legitimate Netflix service.

Malicious URL: http://bit.ly/3ecXem52

Risk Level: High

AbuseIPDB » 112.85.42.180

Check an IP Address, Domain Name, Subnet, or ASN
e.g. 196.138.187.59, microsoft.com, 5.188.10.0/24, or AS15169

196.138.187.59

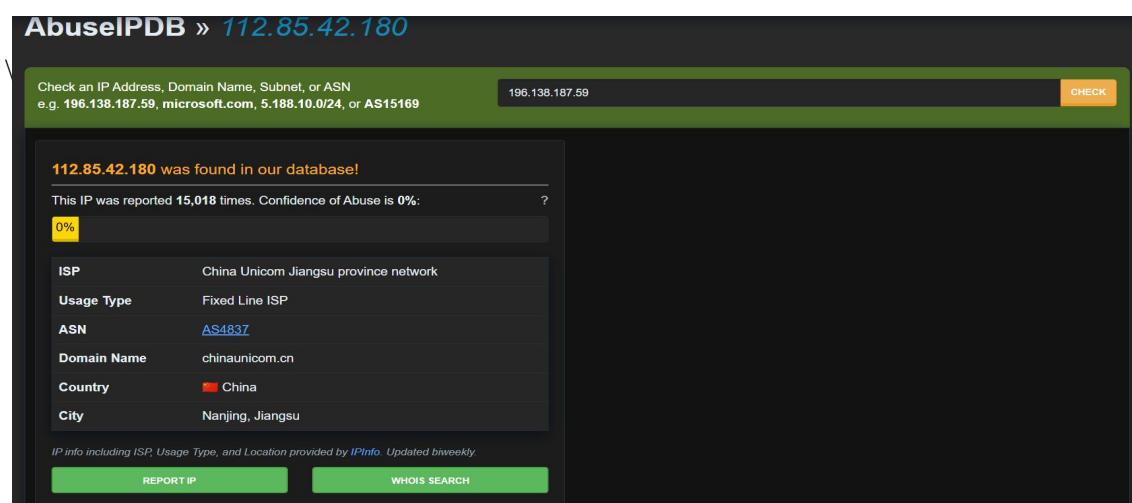
112.85.42.180 was found in our database!

This IP was reported 15,018 times. Confidence of Abuse is 0%: ?

0%

ISP	China Unicom Jiangsu province network
Usage Type	Fixed Line ISP
ASN	AS4837
Domain Name	chinaunicom.cn
Country	China
City	Nanjing, Jiangsu

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



✓ Anonymous	2022-11-16 10:48:38 (3 years ago)	fail2ban detected brute force on sshd	Brute Force SSH
✓ Anonymous	2022-11-13 21:42:33 (3 years ago)	fail2ban detected brute force on sshd	Brute Force SSH
✓ Anonymous	2022-10-04 16:59:09 (3 years ago)	fail2ban detected brute force on sshd	Brute Force SSH
✓ Anonymous	2022-08-22 15:31:06 (3 years ago)	fail2ban detected brute force on sshd	Brute Force SSH
🇯🇵 _Anonymous	2022-01-31 15:15:53 ⓘ (3 years ago)	SSH attacks in a short period.	Brute Force SSH
✓ Anonymous	2021-11-20 21:45:06 (4 years ago)	fail2ban detected brute force on sshd	Brute Force SSH
✓ 🇺🇸 Mashpot	2021-11-09 23:04:45 (4 years ago)	Multiple SSH authentication failures from 112.85.42.180	Brute Force SSH
✓ 🇺🇸 Mashpot	2021-11-07 23:55:49 (4 years ago)	Multiple SSH authentication failures from 112.85.42.180	Brute Force SSH
✓ 🇺🇸 Mashpot	2021-11-06 04:08:52 (4 years ago)	Multiple SSH authentication failures from 112.85.42.180	Brute Force SSH

Final Pr | Log Ma | TryHackMe | Blue te | Blue te | BTLO | TryHackMe | Vir | Reputa | 112.85 | 37659 | cybers | case1 | New Ta | School | +

virustotal.com/gui/url/e913403221120948995f6609fe7ce52bf3407b06c62db94dfdfcc9aeede3e3f

http://bit.ly/3ecXem52

4 / 97 security vendors flagged this URL as malicious

Community Score

http://bit.ly/3ecXem52 bit.ly Status 404 Content type text/html Last Analysis Date 15 days ago

text/html trackers external-resources

DETECTION DETAILS COMMUNITY 1

Security vendors' analysis

				Do you want to automate checks?
CRDF	Malicious	Gridinsoft	Phishing	
Phishing Database	Phishing	PrecisionSec	Malicious	
Abusix	Clean	Acronis	Clean	
ADMINUSLabs	Clean	AI Labs (MONITORAPP)	Clean	
AlienVault	Clean	Antly-AVL	Clean	
Artists Against 419	Clean	benkow.cc	Clean	
BitDefender	Clean	BlockList	Clean	
Blueliv	Clean	Certego	Clean	

Final Pr | Log Ma | TryHackMe | Blue te | Blue te | BTLO | TryHackMe | Vir | Reputa | 112.85 | 37659 | cybers | case1 | New Ta | School | +

virustotal.com/gui/domain/netflix-payments.com

netflix-payments.com

Did you intend to search across the file corpus instead? Click here

Community Score

Registrar GMO Internet Group, Inc. d/b/a Onamae.com Creation Date 1 year ago Last Analysis Date 3 days ago

suspicious content phishing and fraud Phishing and Other Frauds top-1M

DETECTION DETAILS RELATIONS COMMUNITY

Security vendors' analysis

				Do you want to automate checks?
alphaMountain.ai	Phishing	BitDefender	Phishing	
CRDF	Malicious	CyRadar	Phishing	
ESET	Phishing	Forcepoint ThreatSeeker	Malicious	
Fortinet	Phishing	G-Data	Phishing	
Lionic	Phishing	Seclookup	Malicious	
SOCRadar	Malware	Sophos	Phishing	
VIPRE	Malware	Webroot	Malicious	
Abusix	Clean	Acronis	Clean	

6. Attack Classification

Confirmed Phishing Attempt (Brand Impersonation)

7. Impact Assessment

If clicked, the link could result in:

- Credential theft
- Malware infection
- Financial fraud

No impact occurred because the link was not opened.

8. Response Actions Taken

- Alert reviewed by SOC analyst
- Sender domain analyzed
- Logs checked for URL access
- Incident documented

9. Recommendations

- Block sender domain
- Monitor URL shortener traffic
- Enable SPF, DKIM, DMARC
- Conduct phishing awareness training

10. Final Verdict

This was a confirmed phishing attempt. The user did not access the malicious link, preventing any compromise.

The screenshot shows the LetsDefend interface. On the left, there's a sidebar with icons for Monitoring, Log Management, Case Management, Endpoint Security, Email Security, Threat Intel, and Sandbox. The main area has tabs for MAIN CHANNEL, INVESTIGATION CHANNEL, and CLOSED ALERTS. The CLOSED ALERTS tab is active, showing a single row for a closed alert. The alert details are as follows:

SEVERITY	DATE CLOSED	RULE NAME	EVENTID	TYPE	RESULT	ACTION
Low	Jan, 25, 2026, 11:05 PM	SOC101 - Phishing Mail Detected	34	Exchange	✓	View
EventID : 34 Event Time : Dec, 05, 2020, 10:33 PM Rule : SOC101 - Phishing Mail Detected Answer : True Positive (+5 Point) Playbook Answers : Check If Someone Opened the Malicious File/URL? (+5 Point) Check If Mail Delivered to User? (+5 Point) Analyze Url/Attachment (+5 Point) Are there attachments or URLs in the email? (+5 Point) Analyst Note : What is the email's SMTP address? 112.85.42.180 What is the sender address? admin@netflix-payments.com What is the recipient address? emily@letsdefend.io Is the mail content suspicious? yes Are there any attachments?						

11. Detailed Email Investigation Questions

1. When was it sent?

The email was sent on Dec, 05, 2020, 10:33 PM

2. What is the email's SMTP address?

112.85.42.180

3. What is the sender address?

admin@netflix-payments.com

4. What is the recipient address?

emily@letsdefend.io

5. Is the mail content suspicious?

Yes, it impersonates Netflix and uses a shortened link.

6. Are there any attachments?

No. There are no file attachments, only a malicious URL in the email body.