

SOC101 – Phishing Investigation Report

Challenge 2 – Let'sDefend EventID 34

Student Name: Romaissaa Moftah

Course: Cybersecurity / SOC Analysis

Instructor: Eng. Taha Abouelhagag



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

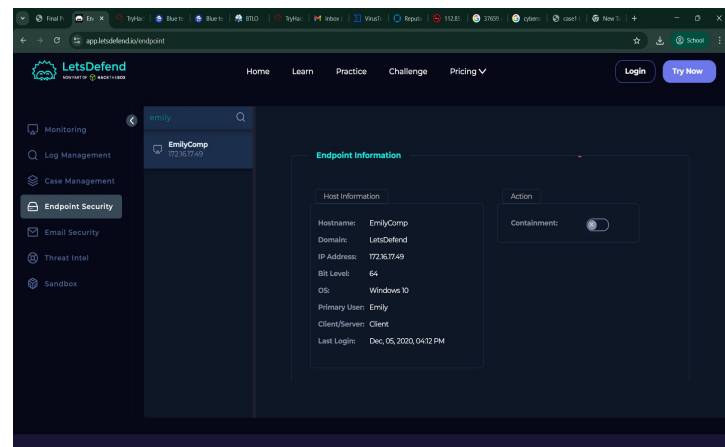
Event ID: 34

Event Time: Dec, 05, 2020 – 10:33 PM

Rule Name: SOC101 – Phishing Mail Detected

Severity Level: Security Analyst

Device Action: Allowed



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."

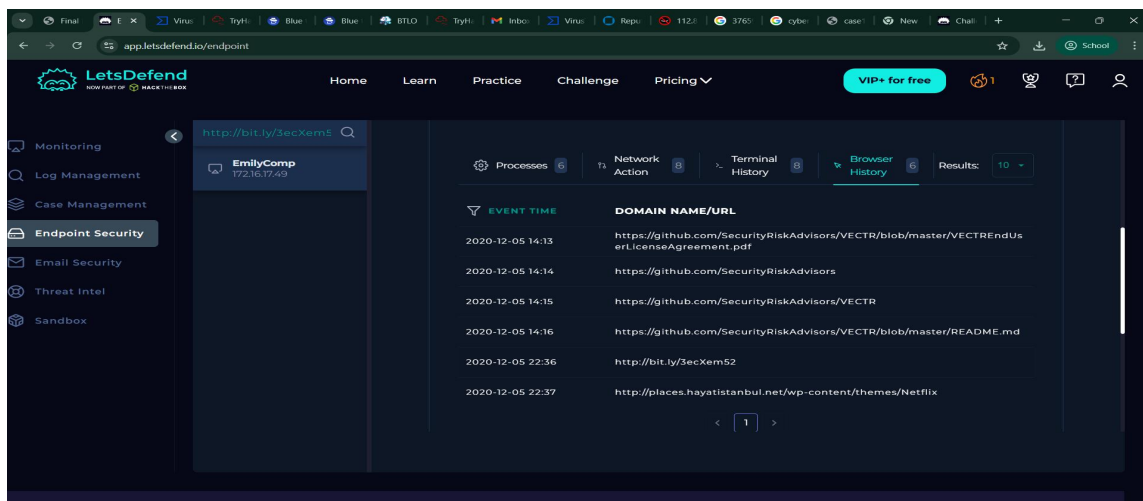


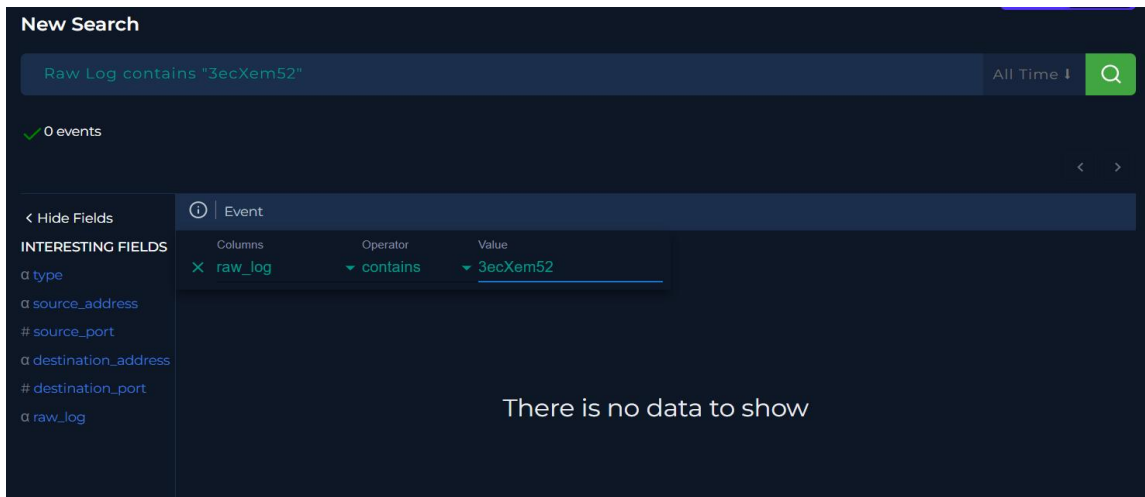
Observations:

- 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.





5. Indicator of Compromise (IOC) Analysis

Source IP: 112.85.42.180

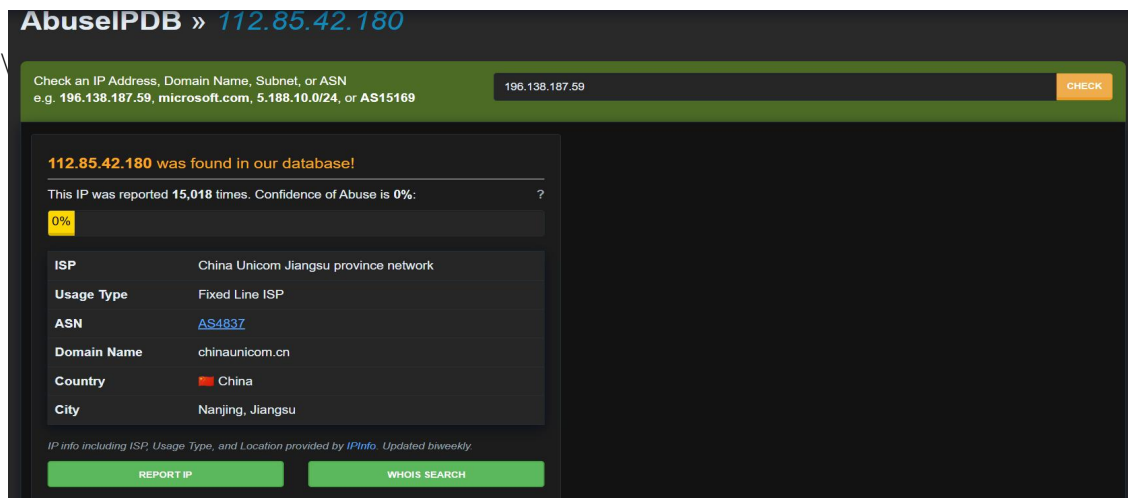
Reputation: Potentially suspicious

Sender Domain: netflix-payments.com

Analysis: Domain mimics a legitimate Netflix service.

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

Risk Level: High



✓ 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
✓ 🇺🇸 Mashpoot	2021-11-09 23:04:45 (4 years ago)	Multiple SSH authentication failures from 112.85.42.180	Brute-Force SSH
✓ 🇺🇸 Mashpoot	2021-11-07 23:55:49 (4 years ago)	Multiple SSH authentication failures from 112.85.42.180	Brute-Force SSH
✓ 🇺🇸 Mashpoot	2021-11-06 04:08:52 (4 years ago)	Multiple SSH authentication failures from 112.85.42.180	Brute-Force SSH

virustotal.com/gui/url/e913403221120948995f6609fe7ce52bf3407b06c62db94dfdffc9aeede3c3f

http://bit.ly/3ecXem52

Community Score: 4 / 97

4/97 security vendors flagged this URL as malicious

Reanalyze Search More

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	AILabs (MONITORAPP)	Clean
AlienVault	Clean	Antiy-AVL	Clean
Artists Against 419	Clean	benkow.cc	Clean
BitDefender	Clean	BlockList	Clean
Blueliv	Clean	Certego	Clean

virustotal.com/domain/netflix-payments.com

netflix-payments.com

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

Community Score: 14 / 92

14/92 security vendors flagged this domain as malicious

Reanalyze More

netflix-payments.com

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

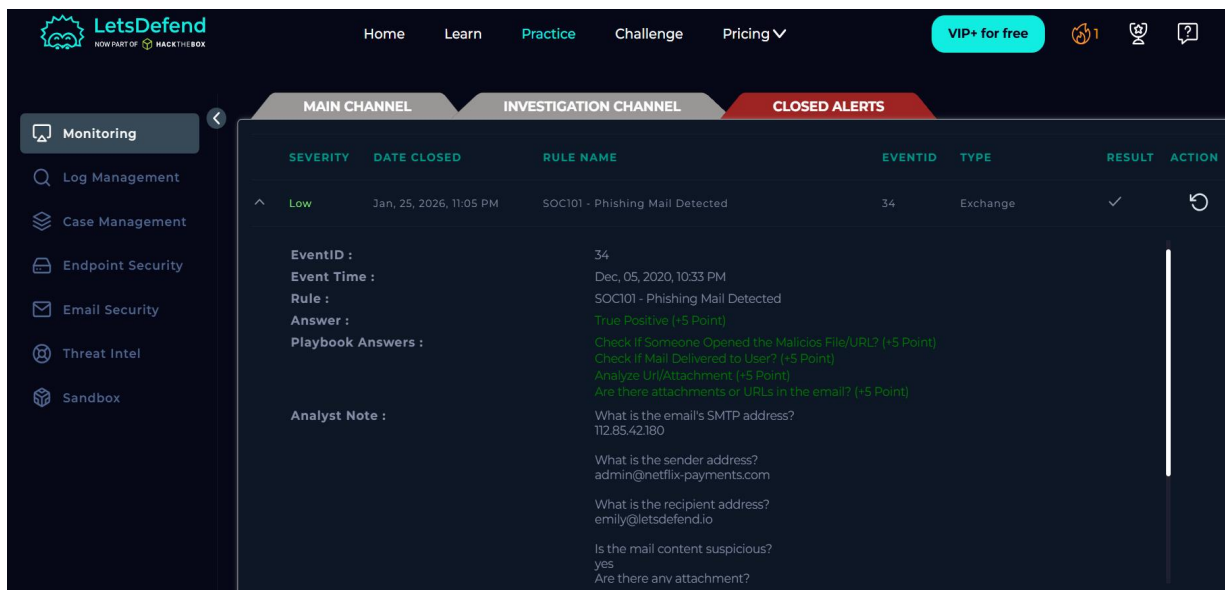
- Alert reviewed by SOC analyst
- Sender domain analyzed
- Logs checked for URL access
- Incident documented

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.



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.