Cyber Threat Intelligence Report

Project Title: OSINT-Based Threat Intelligence Assessment Target Organization: Netflix Inc.

Industry Sector: Technology/Media & Entertainment

Analyst: Remi Adeparusi

Date: January 22nd 2026

Confidentiality Notice

This report contains defensive Cyber threat intelligence derived exclusively from publicly available open-source information (OSINT). It is prepared strictly for educational and analytical purposes and does not include exploitation, intrusion, or unauthorized access activities.

1. Executive Summary

This report presents an Open-Source Intelligence (OSINT) threat intelligence assessment of Netflix, Inc. It focuses on phishing, brand impersonation, and credential harvesting threats. By using only passive and ethical intelligence collection techniques, the analysis reveals how threat actors exploit publicly available information and trusted cloud services to deceive Netflix customers. The active phishing pages, exposed subdomains, and legitimate cloud infrastructure (AWS) that attackers use to get around security filters. Even though Netflix has strong email authentication and security controls, attackers continue to adapt through social engineering, which remains a constant high business risk. This is because attackers often use trusted cloud infrastructure for phishing, making it more likely that they will successfully collect credentials. This could lead to financial loss from account takeovers, damage to reputation from brand abuse, and a decrease in customer trust. Primary **Recommendation:**
Organizations should use improved domain monitoring and automated take-down services for look-alike domains.

2.1 Organization Profile/Overview

Netflix, Inc. is a global streaming service that offers video on demand in over 190 countries. Some of its core services include film/television production, streaming media, and mobile gaming. Its wide online presence, which includes login portals, billing systems, customer support platforms, and mobile apps, makes the brand a common target for phishing and fraud-related Cybercrime.

2.2 Netflix Digital Footprint

Netflix has a high digital footprint globally as it provides a platform where customers can carry out their online services. The digital footprint raises the visibility and trust that the firm enjoys, and despite that, it presents an enablement target and a platform where driven reconnaissance and brand impersonation can take place. Its huge digital footprint is characterized by wide subdomains such as netflix.com (main site for customers login in, managing account, handle billing, and password rest), help.netflix.com, aboutnetflix.com, Instagram is @netflix, waernetflix.

3.1 Intelligence Objectives

The main objective of this assessment is to understand how the information made public can be utilized in conducting phishing activities, brand impersonation, credential harvesting, and other fraudulent activities against Netflix and its customers. Through the application of ethical and passive OSINT approaches, the assessment aims to identify the risks from the public digital footprint of Netflix and explore ways through which these risks can create a potential impact on its customers and its daily business operations.

This project aims to:

- Determine phishing and impersonation campaigns targeting Netflix by examining indexed pages of Netflix logins, account recovery mechanisms, and popular Netflix-themed content often used in social engineering attacks.
- To find exposed or observable assets, including domains, subdomains, email formats, and past web page content that can be used as leverage by the attacker when creating a campaign of phishing or simply gathering information.

- Measure the degree of brand abuse for fraud involving look-alike domains, replicated web pages, and third-party infrastructures with the intent to trick Netflix subscribers into giving their credentials and payment details.

- Obtain attacker intents and methods by combining results from the correlation of OSINT with the MITRE ATTACK reference and identifying the ways the attacker can advance from reconnaissance to credential theft and takeover.

- Explain and translate technical observations into a business-relevant risk regarding what it means to their reputation, customer trust, and possible loss as opposed to the exploitability of the system.

3.2 Scope & Limitations

The Netflix OSINT project is based solely on open-source intelligence with no active scanning, penetration testing, or exploitation of systems whatsoever. Only information gathered from public sources is considered for this project, while ensuring that all activities were done within ethical and legal bounds to make this project information-based only.

4. Methodology & Tools Used

4.1 OSINT Methodology

The assessment planning phase started with explaining intelligence requirements, such as identification of Phishing, brand Impersonation, and fraud risks to Netflix. Assessment only considered publicly available information related to the external digital footprint of Netflix, and no scanning or exploitation was performed.

Processing phase: Publicly available and accessible data was collected through ethical OSINT practices like the use of search engines, domain enumeration, online reputation information, and web archiving. Emphasis is placed on domains, subdomains, email patterns, login pages, account-related pages, and phishing indicators often exploited by attackers.

For the processing phase, we utilized the data that was previously collected, reviewed, filtered, and validated to reduce the occurrence of false positives while removing any extra information that was not required. Indicators were also enriched using ‘Reputation Services’ to verify their legitimacy while checking their abuse history in an accurate manner.

Validated information was analyzed to understand the attacker's intent, technique, or potential scope. Observations were also correlated with the MITRE ATTACK framework to understand the potential capabilities that attackers could utilize while

moving from reconnaissance stages, credential theft, fraud, and leveraging the brand name Netflix.

The results were disseminated and documented in a structured threat intelligence report designed for a SOC and CTI audience. Findings were translated into business-relevant risks supported by evidence, with actionable mitigation recommendations provided to reduce exposure.

4.2 Tools utilized

Google Dorks: This was used to find publicly indexed content related to Netflix login portals, password reset mechanisms, security documents, etc. This was used to imitate the behavior of attackers looking for high-value user space content that often ends up being cloned to perform phishing attacks.

The Harvester: It was used to make a passive enumeration of email patterns and subdomain names associated with Netflix from publicly available information. This illustrates how attackers gather legitimate-looking forms of emails and web content that could be used to impersonate and social engineer.

Shodan: It was used at a high level to verify the presence of publicly identifiable services associated with Netflix. No host selection, port, or vulnerability identification was made. The tool allows for the comprehension of the outside view of the system on the part of the attacker.

Wayback Machine: This was used to investigate different historical designs of Netflix's online web pages, such as their login page and support page designs, in terms of how they might have been utilized by malicious actors to phish unsuspecting visitors to these websites.

MXToolbox: Used to assess the e-mail authentication posture of Netflix, including SPF, DKIM, and DMARC. Results show that it has great protections in place to prevent direct domain spoofing. Explain to the students why bad actors rely on look-alike domains and third-party infrastructure.

VirusTotal: Used to evaluate the reputation of Netflix-themed URLs and phishing indicators: the tool helps confirm if the suspicious link has been previously flagged by security vendors or the community.

URLScan.io: This was used to safely observe the behavior of suspected phishing URLs without direct interaction. This gives context on page structure, redirection behavior, and the loading of external resources.

AbuseIP: This is used to evaluate the historical reputation of IP addresses used to host phishing infrastructure. This also enables the identification of frequently misused cloud-based services by criminals.

WHOIS: Used in validating and ensuring domain ownership, registration details, and age. This is done to identify genuine Netflix properties from recently registered, similarly named domains usually used in phishing.

Have I Been Pwned: This is used for checking if the publicly disclosed email addresses related to Netflix were present in any data breaches. This step assists with the verification of indicators as well as the minimization of false positive occurrences.

5. OSINT Collection Summary

This assessment went through a different collection of several openly sourced data, through ethical OSINT techniques, to assess phishing campaigns, brand impersonation, credential harvesting, and fraud risks against Netflix. The focus of this collection phase was on identifying information that could be used by threat actors in reconnaissance and social engineering activities.

Below are the data types collected:

Domains and look-alike domains like Netflix branding, including publicly observable login, billing, and support-related URLs. These were studied to understand how attackers could build domains that look very similar for phishing and impersonation campaigns.

Information regarding Email addresses and Email pattern identification concerning Netflix and publicly available Internet services. This information illustrates ways an attacker can develop legitimate mail address formats to send phishing emails.

IP addresses and related providers of web hosting services are used to conduct suspicious phishing activities. These indicators were referenced at a high level to focus on the use of third-party or cloud-hosted services usually misused by attackers.

URLs related to phishing, brand Impersonation, fraudulent and credentialing activity attacks, like URLs found in phishing messages themed on Netflix and other phishing pages disguised as Netflix.

Historical web content, like old login and account-related content, demonstrates how attackers reuse old legitimate designs to add credibility to phishing campaigns.

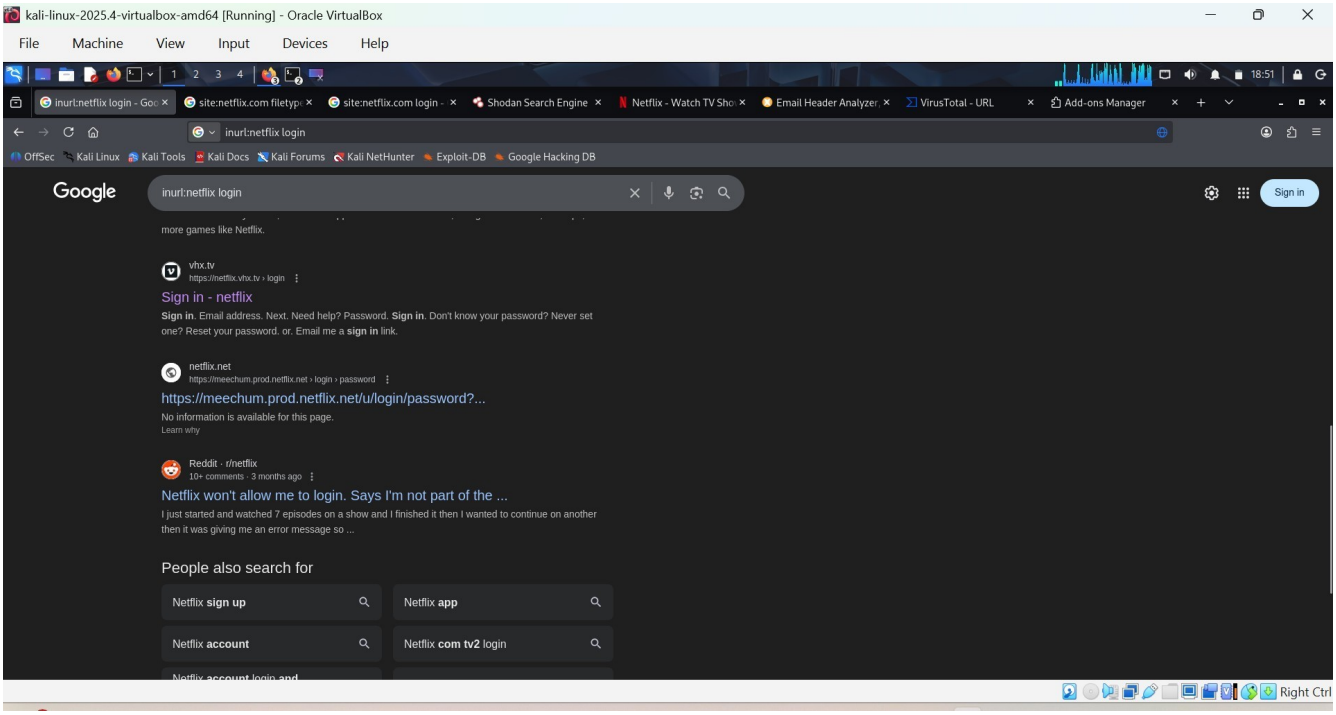
Email authentication information, as well as reputation metadata, including SPF, DKIM, DMARC, and public reputation, helps assess the organization’s immunity towards domain spoofing, as well as the attacker using alternative delivery methods.

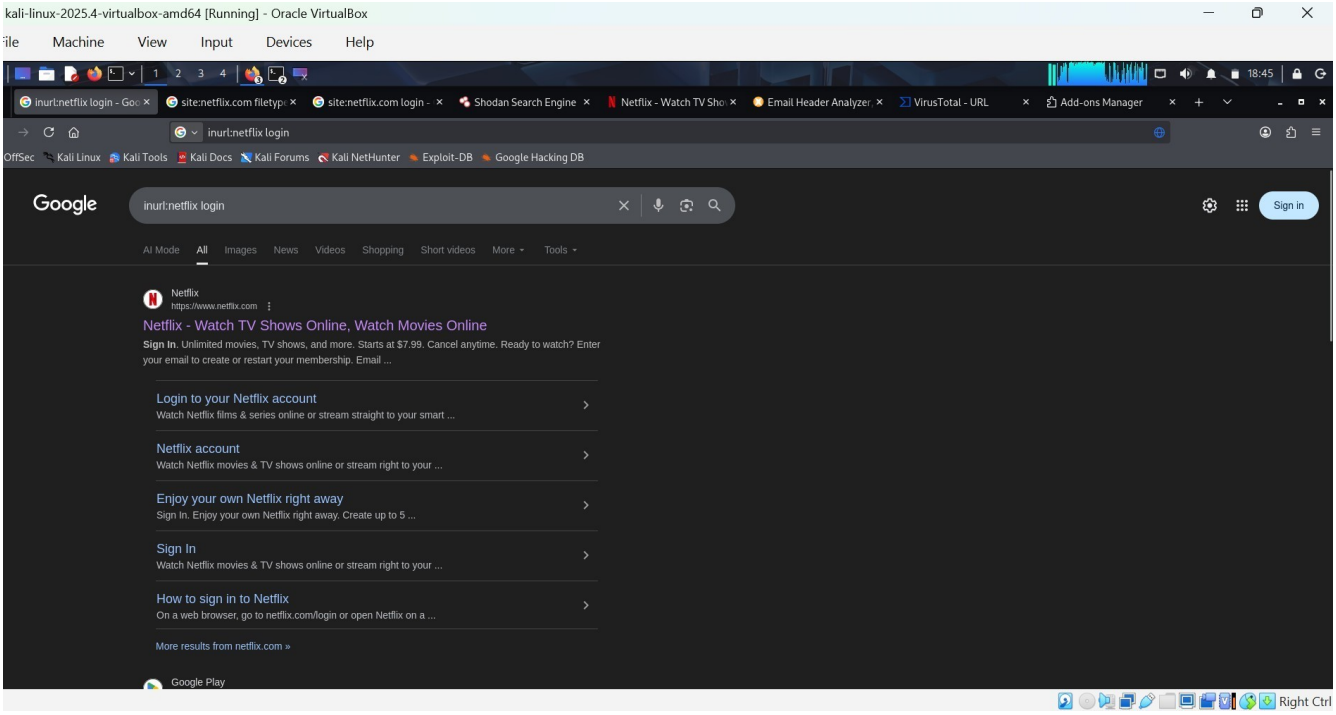
6. Key Findings & Exposure

6.1 Phishing and Brand Impersonation: This part highlights the observation of threat actors using the trusted brand name of Netflix to swindle its end-users for their own financial benefit. Financial Gain and Payment Fraud is the most noticeable theme in the emails, which is a phishing attempt to deceive customers into committing financial fraud. Attackers often launch a spear phishing attack where they encourage the user to click on malicious links to verify their account or change payment details. All campaigns employ electronically mediated social engineering tactics to induce a sense of legitimacy.

6.1.1 Google Dorks

Commands: inurl: Netflix login



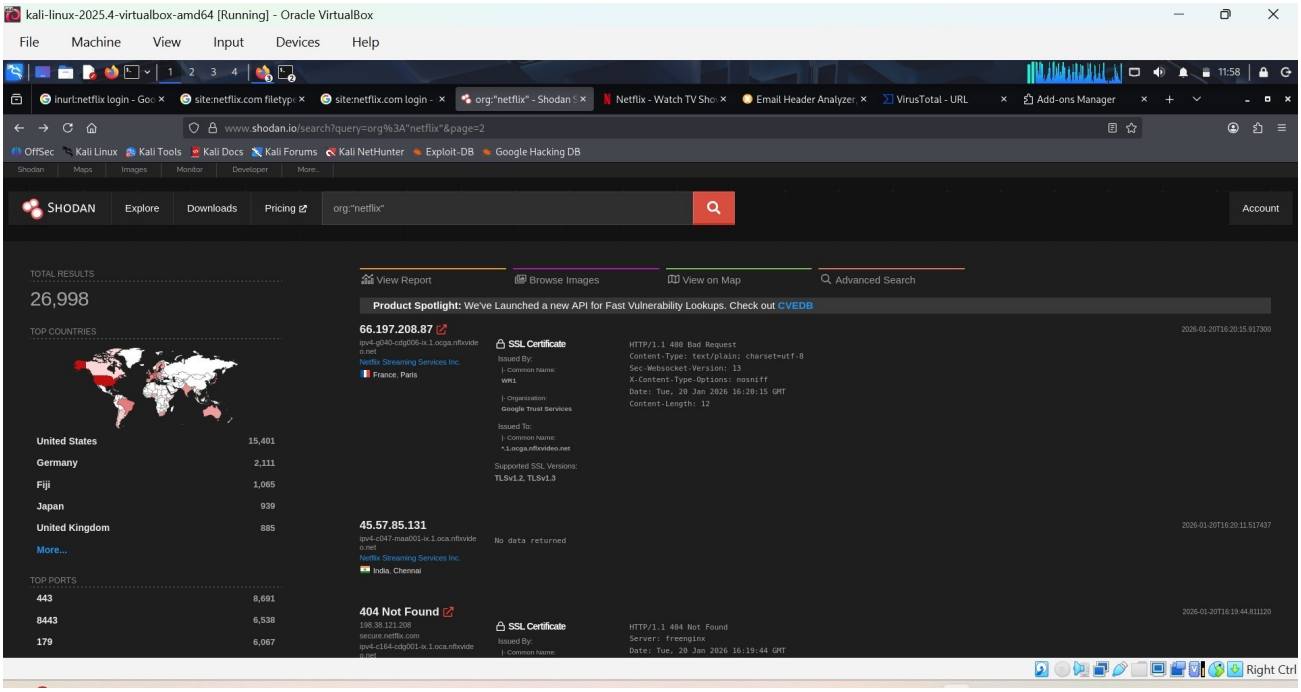


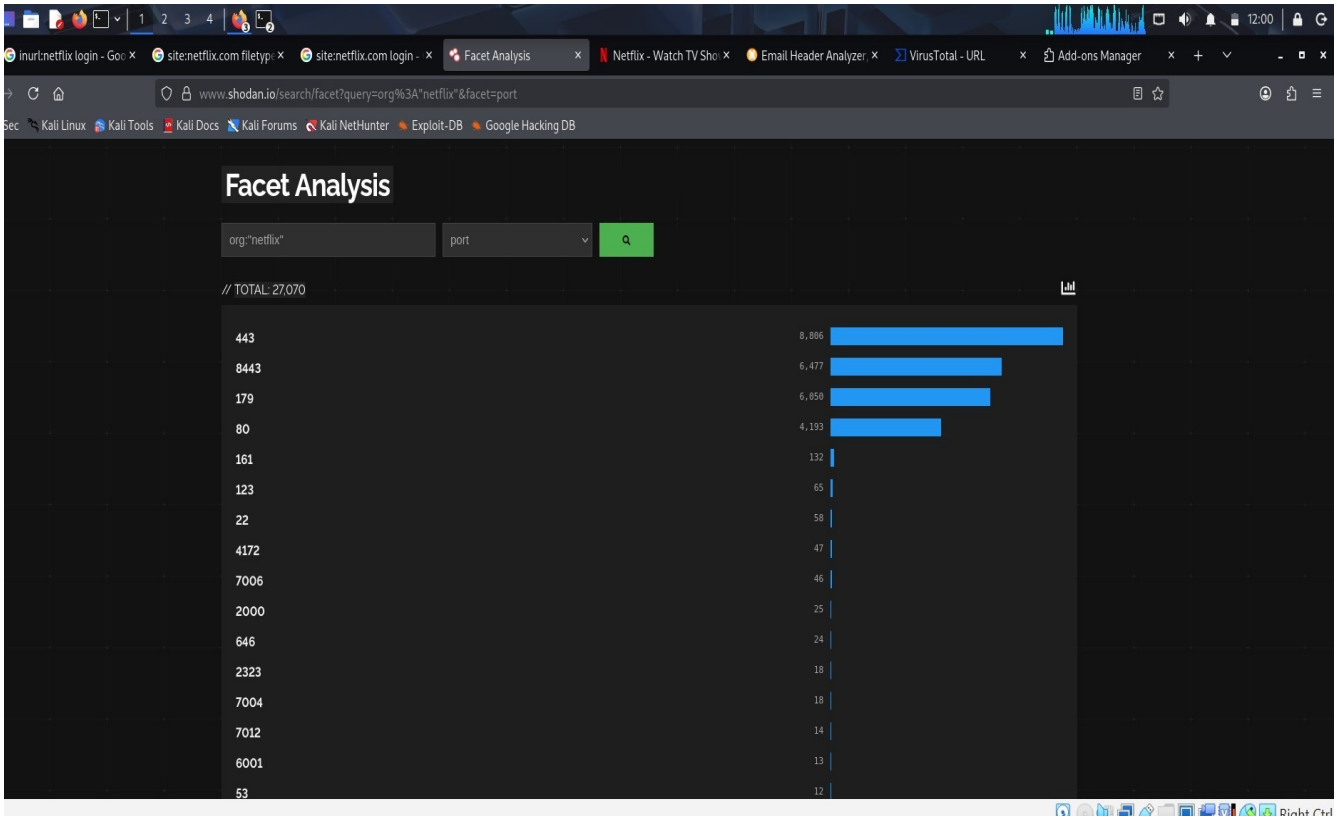
Google dork search on inurl:netflix login, revealing some phishing page Netflix login

- **Look-alike domains and infrastructure identified:** The adversaries were found to utilize the email delivery system of the popular online cloud service, Amazon Web Services, which is a safe delivery platform. By doing so, the adversaries can avoid detection by other threat intelligence tools that will flag the mail as being "clean" due to the source reputation. The attackers, during the reconnaissance stage, have been observed to use third-party domains to carry out their attack lifecycle. A particular IP address, 54.240.4.22, was found and processed through the tool AbuseIPDB as part of the infrastructure for the attacks.

6.1.2 Shodan

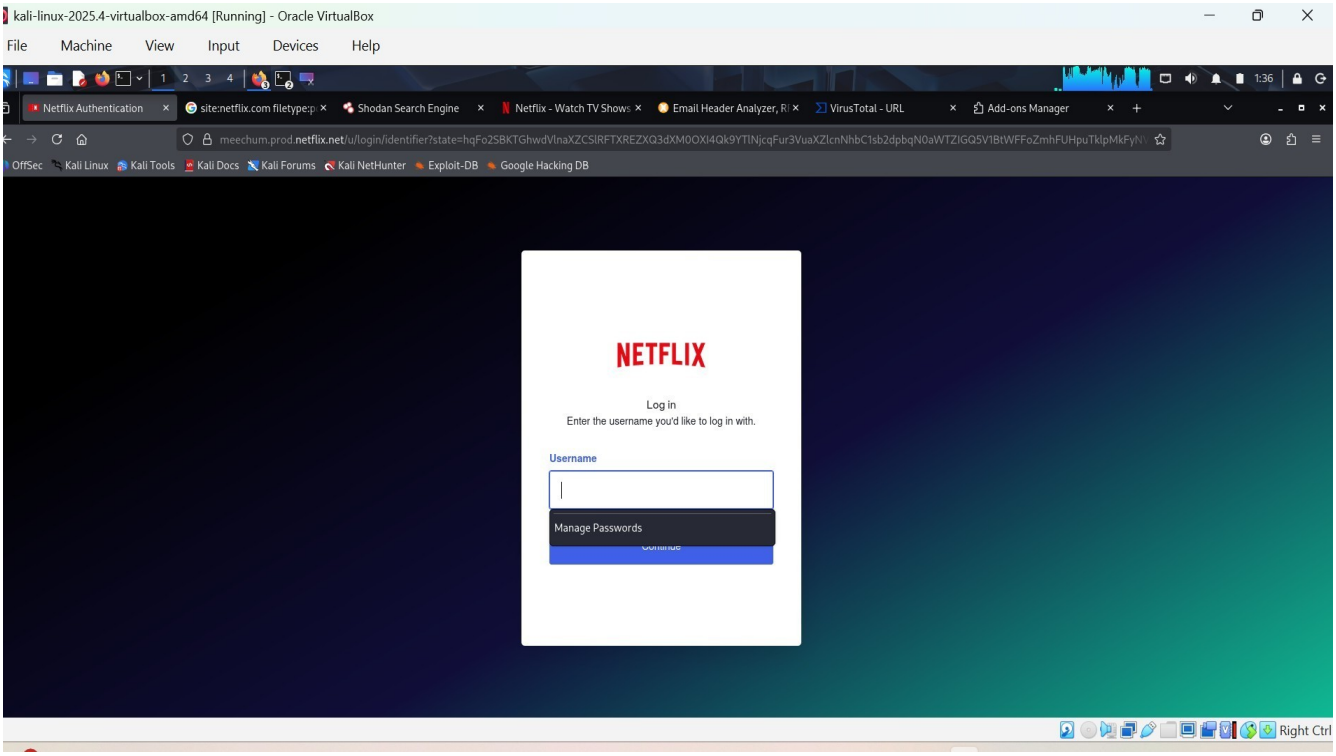
Command: shodan.io search on org:"netflix."





shodan.io search on org:"netflix" organization report

- **Fake login pages and cloned content:** using Google dork inurl:netflix login, reveals the active phishing pages that look like the official network login portal. Threat actors were successful at cloning the Netflix logo to deceive customers about its authenticity. The fake pages were designed to accept input, allowing attackers to harvest users' credentials when entered.



Google dork search on inurl:netflix login revealing some phishing page netflix login.

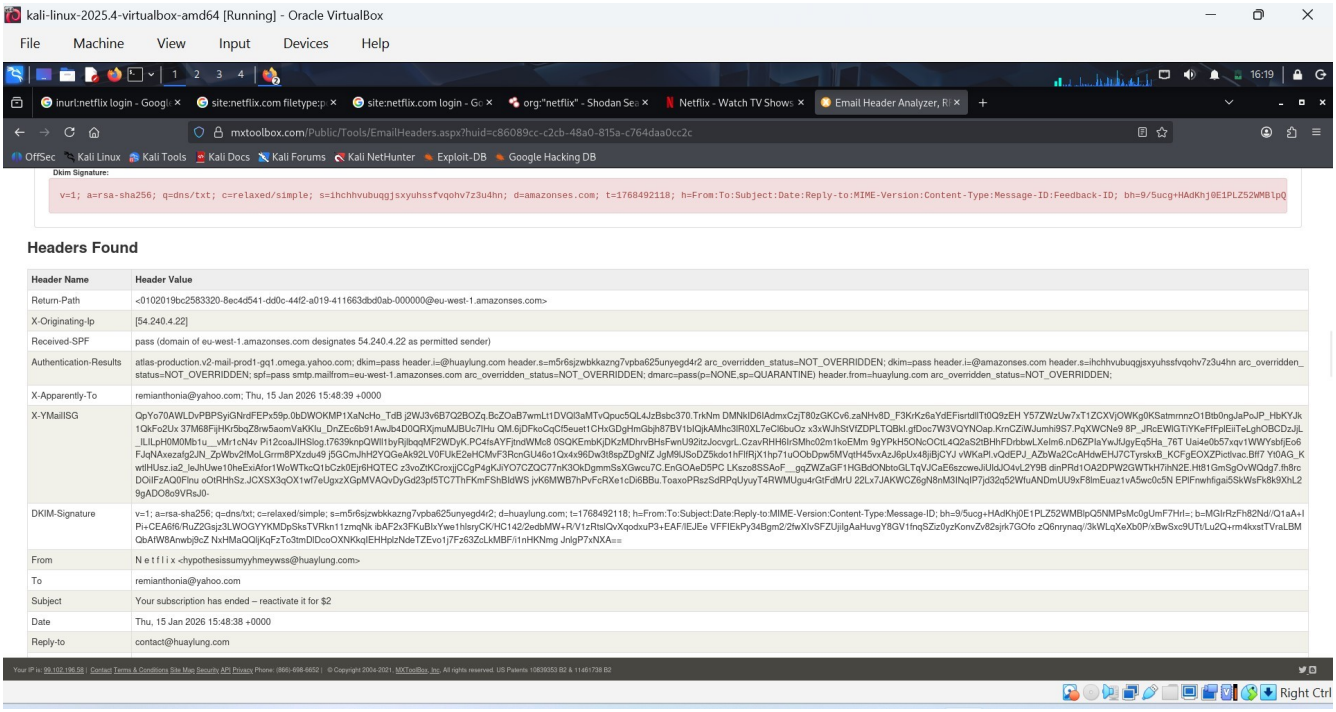
6.2 Infrastructure Exposure: This project reviews the technical assets and cloud techniques and patterns that reveal Netflix's digital presence and exposure to potential exploitation.
Researching the public visible service, based on the result of Shodan.io searches (org:" Netflix") and theharvester result, there was an exposure of some subdomains. Shodan.io reports some open ports associated with the Netflix organization, with a detailed report on port configuration and their organization service maps. Wayback Machine history revealed how Netflix's web design has evolved, which helped threat actors build clones for phishing.

Regarding cloud or hosting patterns abused by attackers, attackers do not simply carry out attacks against Netflix; instead, they utilize trusted cloud ecosystems to remain under the cover of their ill practices.

The analysis of phishing samples collected via MxToolbox showed that the cyberattacks are taking advantage of the Amazon Web Services (AWS) infrastructure. This reveals the abuse of trusted infrastructure.
Since AWS is a 'trusted cloud email delivery infrastructure,' threat intelligence tools or services like VirusTotal have labeled the emails as "clean," which impacted the result.

Cybercriminals were discovered to be acquiring, renting, or leasing third-party domains to host and hence support their activities, mimicking Netflix's hosting infrastructure, logos, etc. Cybercriminals employ different solutions, including physical or virtual infrastructure hosting via relaying information to and from compromised systems through legitimate public web services.

Mxtoolbox Report

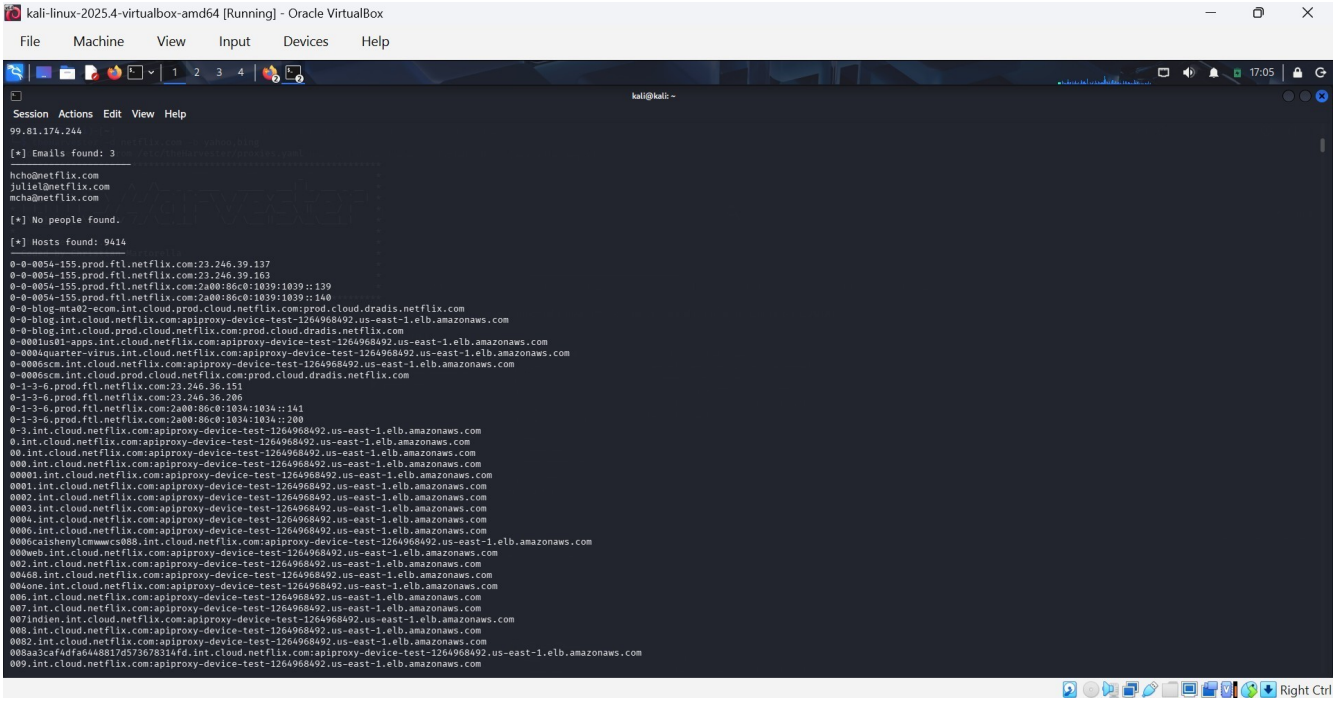


Mxtoolbox analysis of the phishing email reveals AWS

6.3 Data Leakage Indicators: Publicly accessible documents related to Netflix, including policy and security materials, were found using passive search methods. This matters because even if documents don't include sensitive information, they can give attackers Legitimate branding, logos, and formatting. They can also expose the official language used in customer communications and provide insight into account recovery or security processes.
These can be reused to create convincing phishing emails and cloned web pages, increasing the chance of user interaction.

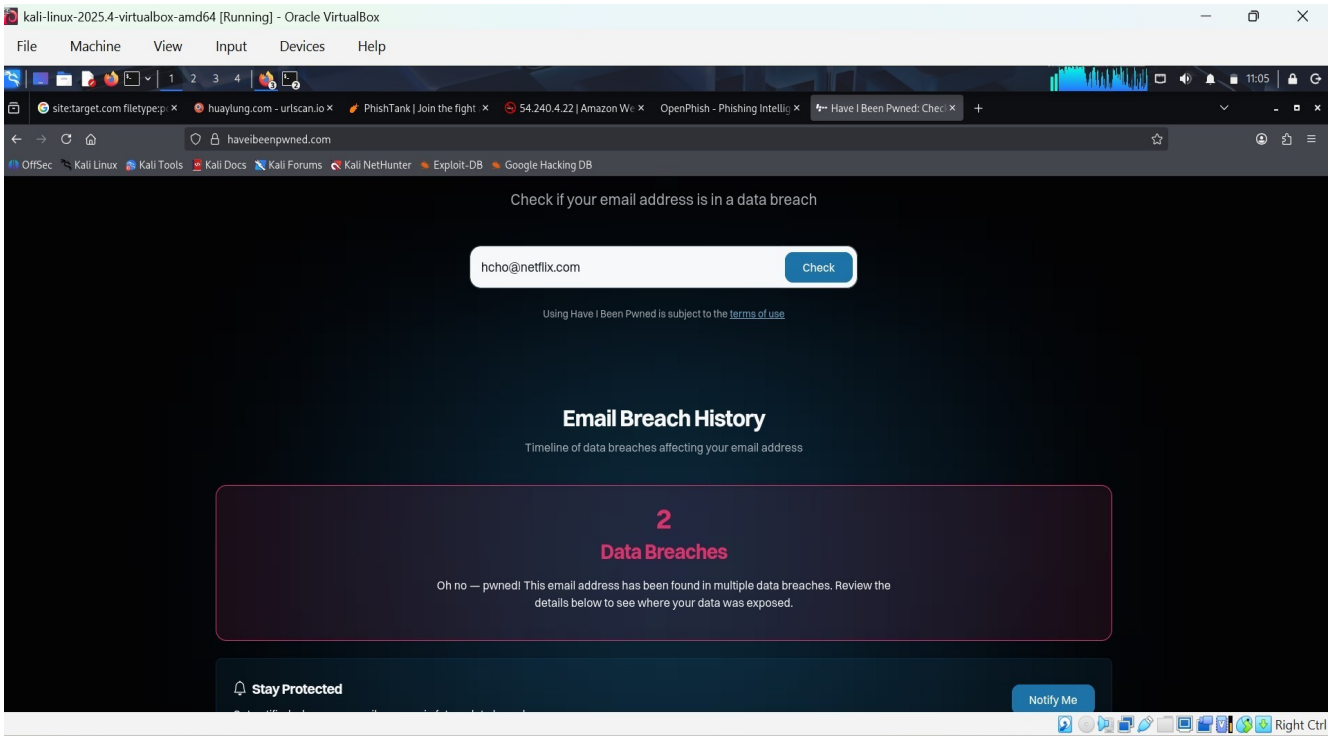
Under the breached or Leaked Email Addresses (No Credentials), publicly discovered Netflix-related email addresses were found and checked against known breach databases. No exposed credentials were observed. This matters because, though no credentials were discovered, exposing valid email addresses or patterns allows attackers to create realistic sender or recipient addresses. Target spear-phishing campaigns more effectively and boost trust by mimicking legitimate Netflix communication formats. This information makes it easier for attackers during reconnaissance and raises their chances of successful phishing. The email hcho@netflix was identified via theHarvester and was revealed to have appeared in historical data breaches using haveibeenpwned.com.

theHarvester -d netflix.com -b all

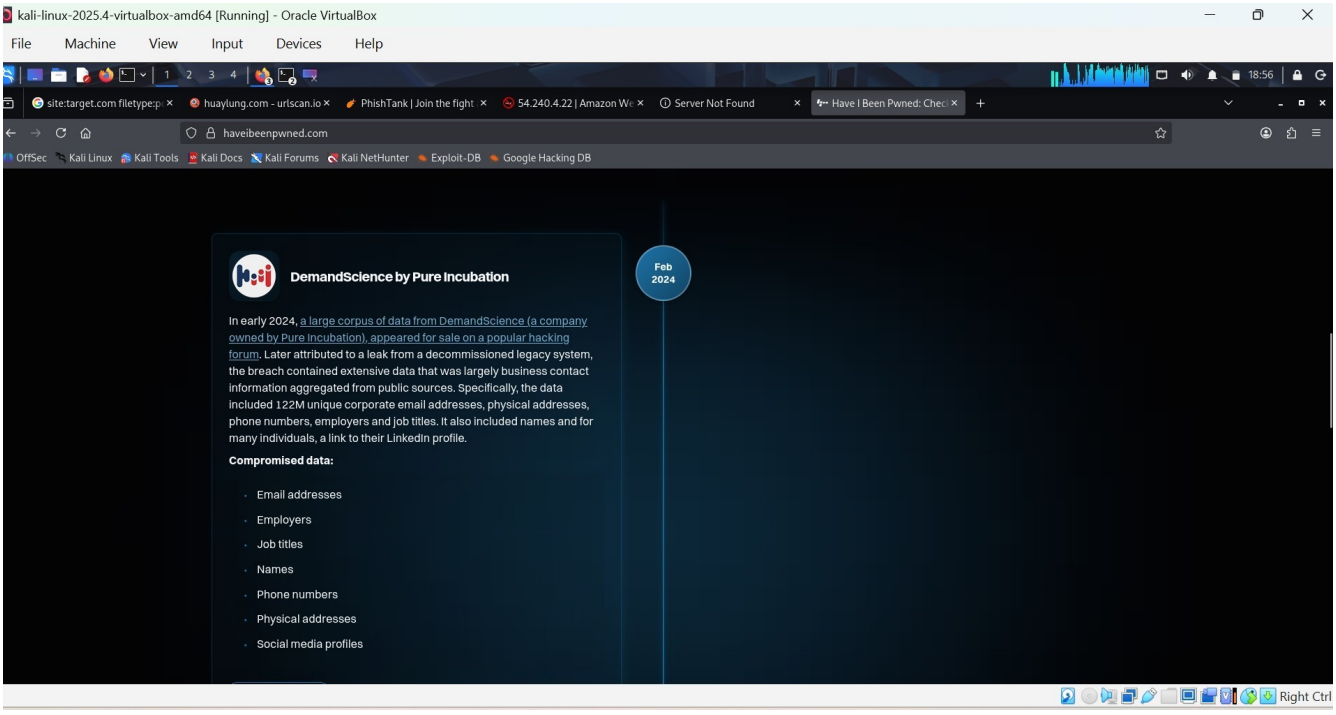


This reveals the email [hcho@netflix]

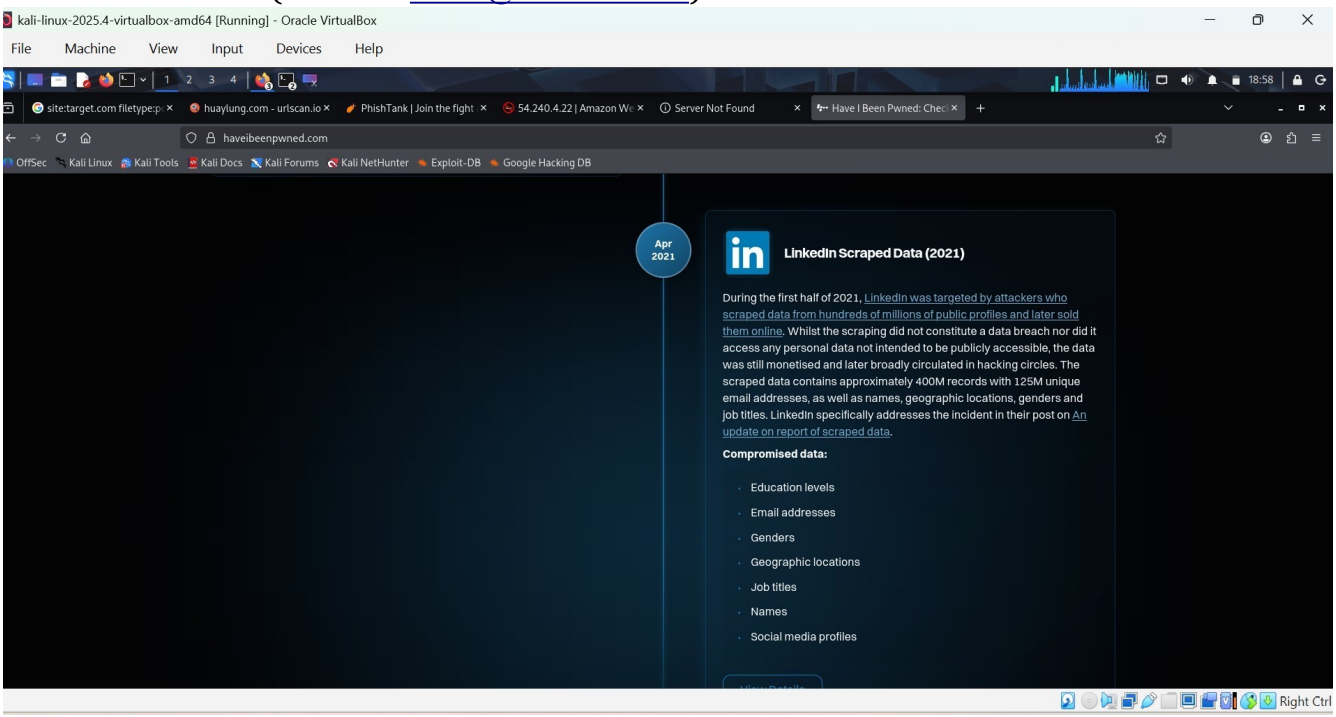
haveibeenpwned.com Report



haveibeenpwned.com report on an email address found on theHarvester -d netflix.com -b all (email is hcho@netflix.com)



haveibeenpwned.com report on an email address found on theHarvester -d netflix.com -b all (email is hcho@netflix.com)



haveibeenpwned.com report on an email address found on theHarvester -d netflix.com -b all (email is hcho@netflix.com)

7.1. Threat Analysis & Risk Assessment

From the threat actor's perspective, the collected OSINT gives enough information to support phishing and brand impersonation campaigns without needing to compromise systems directly.

Likely Attack Paths are as follows:

- Reconnaissance: Attackers collect publicly available Netflix login pages, email formats, and past web designs.
- Resource Development: They create look-alike domains and cloned login pages using Netflix branding and language.
- Delivery: Phishing emails are sent from third-party or cloud-hosted systems to avoid detection and appear more legitimate.
- Credential Harvesting: Victims are redirected to fake login or billing pages where their credentials or payment details are captured.
- Exploitation and Impact: Compromised accounts are used for subscription fraud, resale, or further social engineering.

Below are the Common Attacker Techniques:

➔ Brand impersonation with look-alike domains.
➔ Social engineering through urgent messaging.

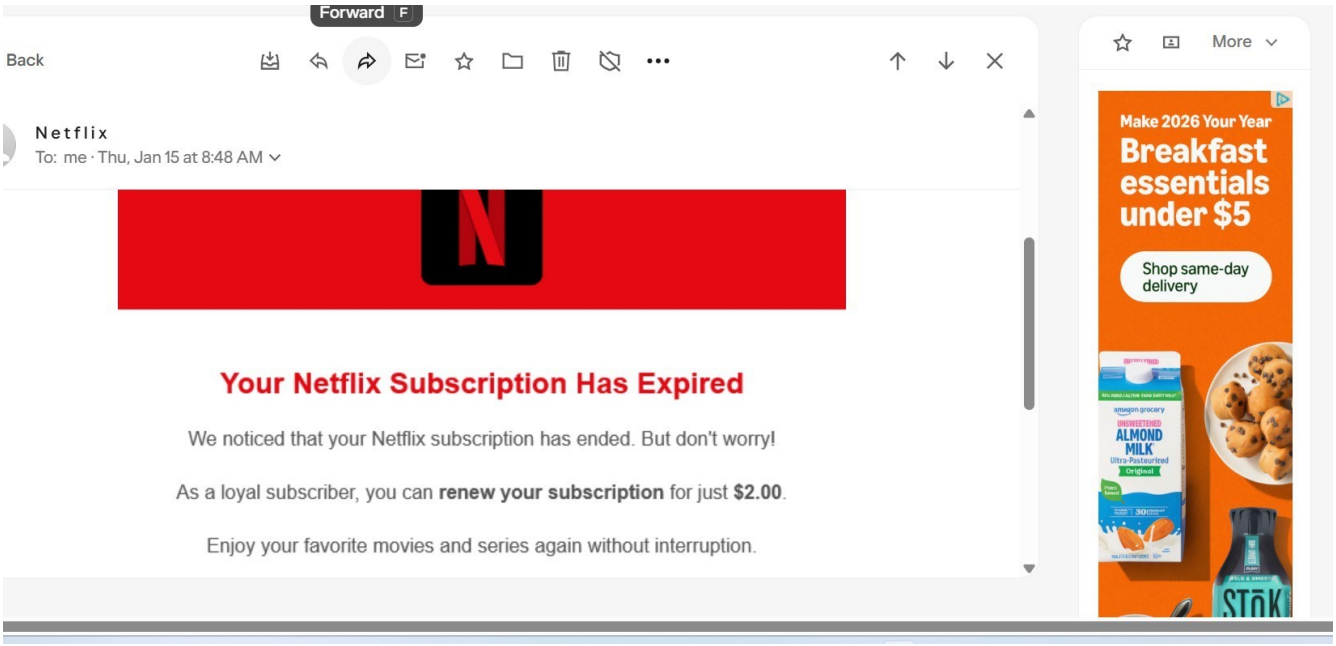
➔ Credential harvesting using cloned login pages.
➔ Use of trusted cloud services to lower the chances of detection.

Alignment With Known Threat Behaviors (MITRE ATTACK). The observed activity matches established adversary techniques, listed as follows:

- Reconnaissance – Phishing for Information (T1598): Collecting user and organization information to aid targeting.
- Resource Development – Acquire Infrastructure (T1583): Registering domains and using third-party hosting services.
- Initial Access – Phishing (T1566): Delivering malicious links through impersonation emails. Credential Access Input Capture (T1056): Harvesting credentials using fake web forms.
- Command and Control – Web Services (T1102): Sending captured data through legitimate external services.

Risk Impact

Brand Reputation- High
Customer Trust- High
Financial fraud- Medium-high
Operational Impact- Medium



sample email of phishing email sent by cybercriminals.

7.2. **Business Risk Impact**

The identified threat activities mainly involve phishing, brand impersonation, and misuse of trusted infrastructure rather than direct attacks on Netflix systems. Still, these activities present measurable business risks.

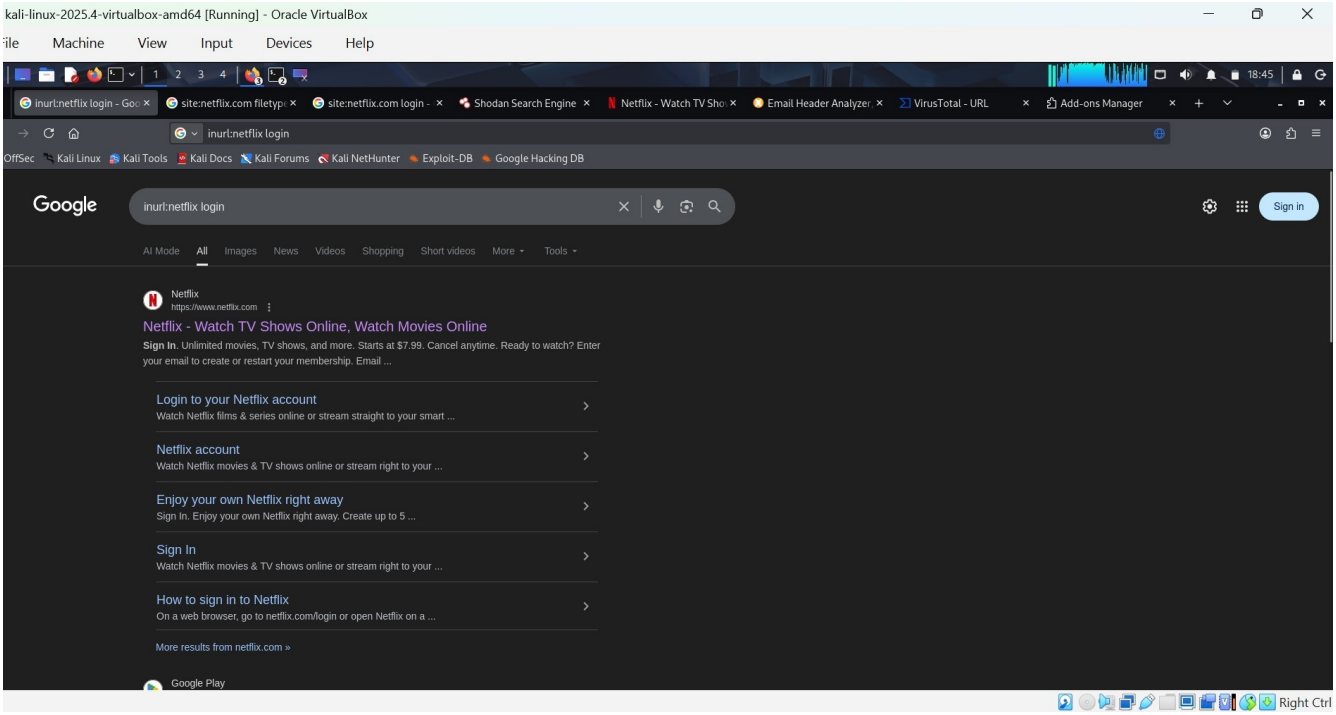
- **Financial Risk is considered Medium** as phishing and account takeover campaigns targeting Netflix customers can lead to the below; Subscription fraud and unauthorized account access, costs for customer support, refunds, and fraud prevention, and higher spending on monitoring and take-down efforts. While Netflix's core infrastructure remains secure, the size of the user base increases the financial impact of even low-cost phishing operations.
- **Reputational Damage is considered High** as brand impersonation and phishing directly influence public perception because customers link fraudulent communications to Netflix. Ongoing phishing campaigns weaken confidence in official communications. Negative experiences are often shared publicly, increasing reputation harm.
- **Customer Trust is considered high.** Trust is crucial for subscription-based services. Successful phishing lowers confidence in account security. Users may hesitate to engage with legitimate Netflix emails. Loss of trust can lead to account cancellations or decreased engagement. Even unsuccessful phishing attempts harm customer trust over time.

- **Regulatory Exposure is considered Low to Medium.** There was no evidence of internal data breaches or regulatory violations. However, Misuse of customer data through phishing may lead to regulatory scrutiny. Areas with strict consumer protection laws may demand notification or investigation. Regulatory exposure is limited but could grow if phishing activity increases or causes widespread consumer harm.

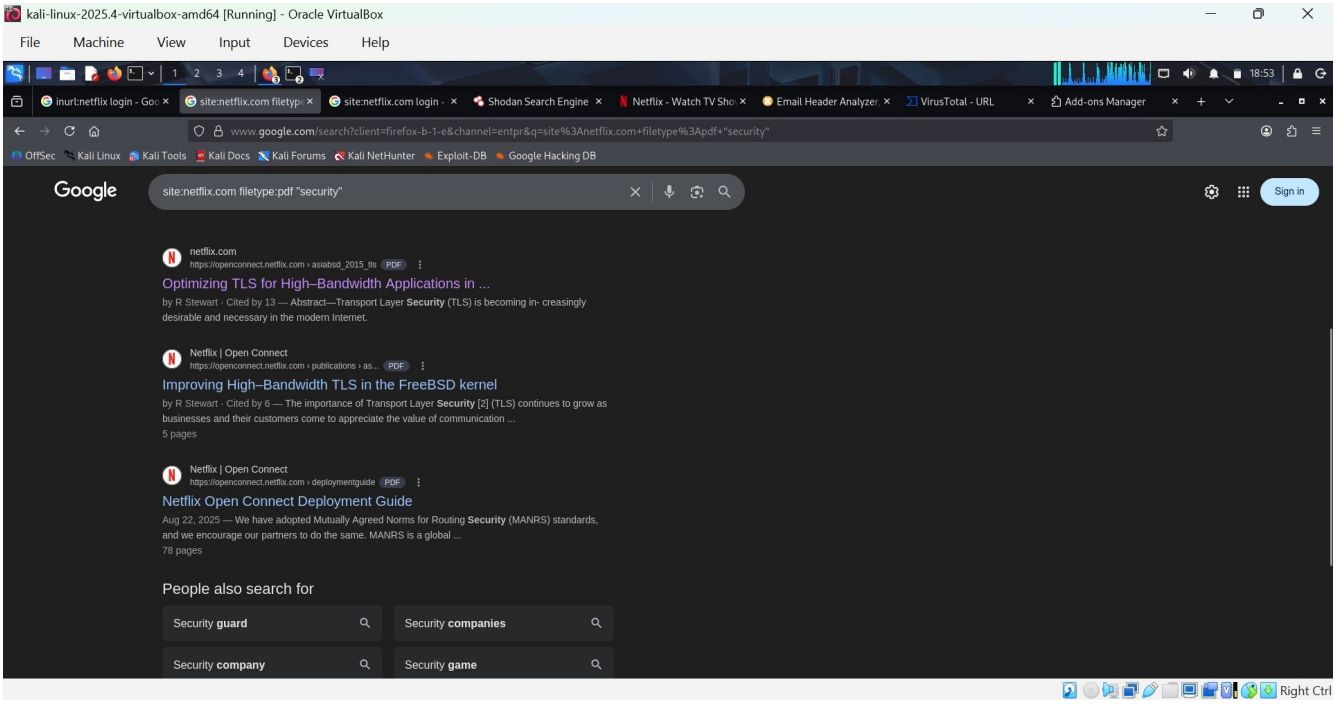
8. **Evidence Log**

The evidence provided below supports the findings presented in this report. All evidence was collected through passive OSINT methods. No exploitation, active scanning, or interaction with internal systems was conducted.

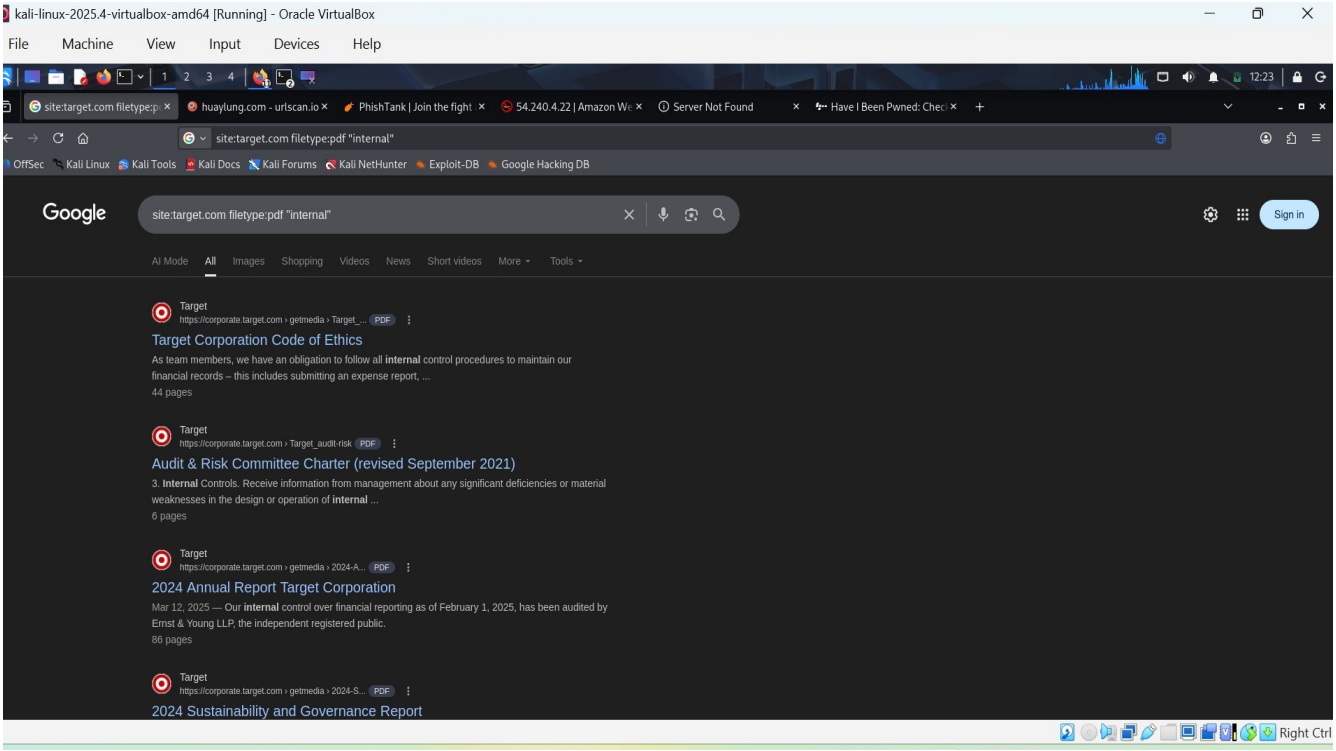
8.1 Google dork Search



Command: inurl:netflix login

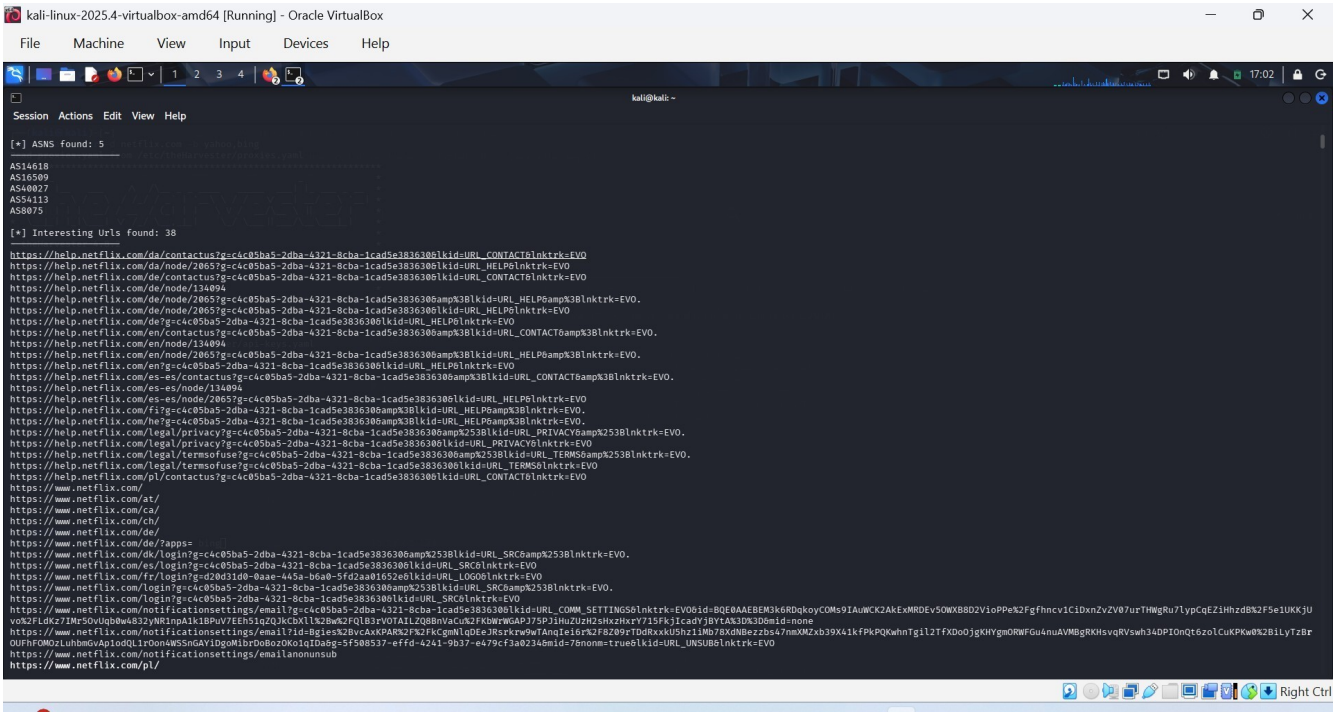


Command: site:netflix.com filetype:pdf "security"



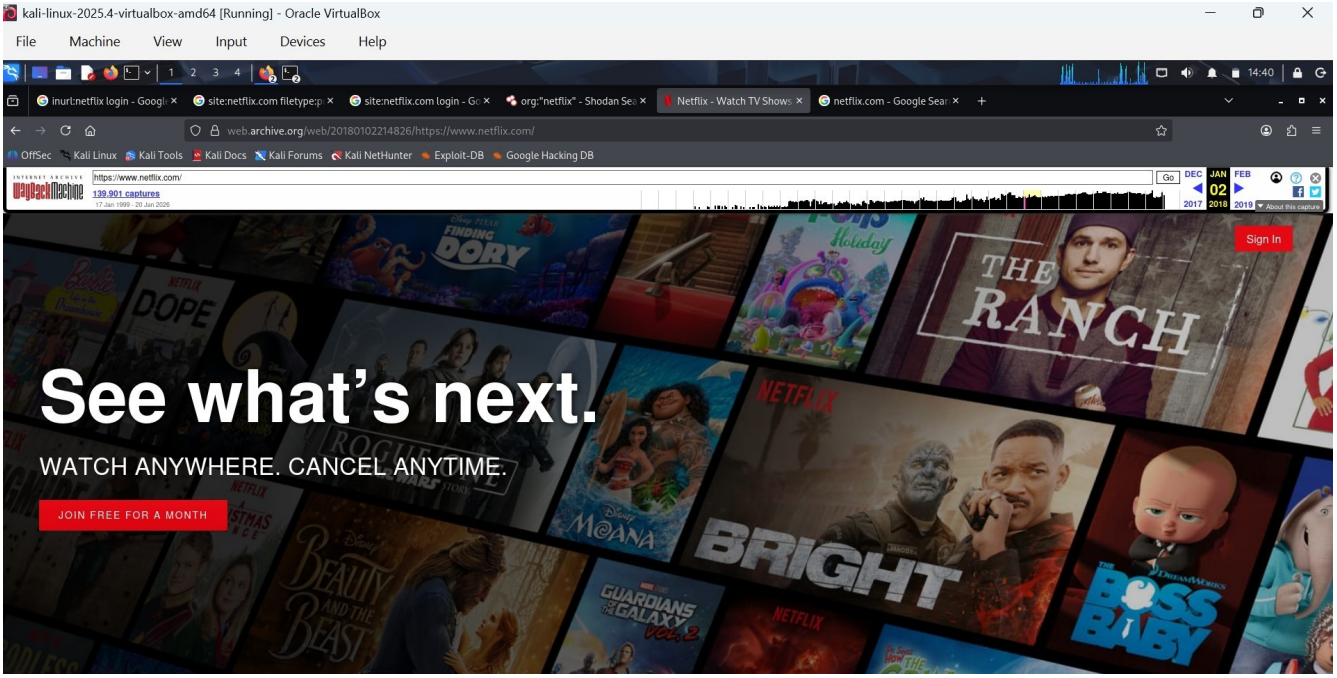
Command: site: target.com filetype:pdf "internal".
This is to help analysts see the organization from the attacker's perspective.

8.1.2. theHarvester Search



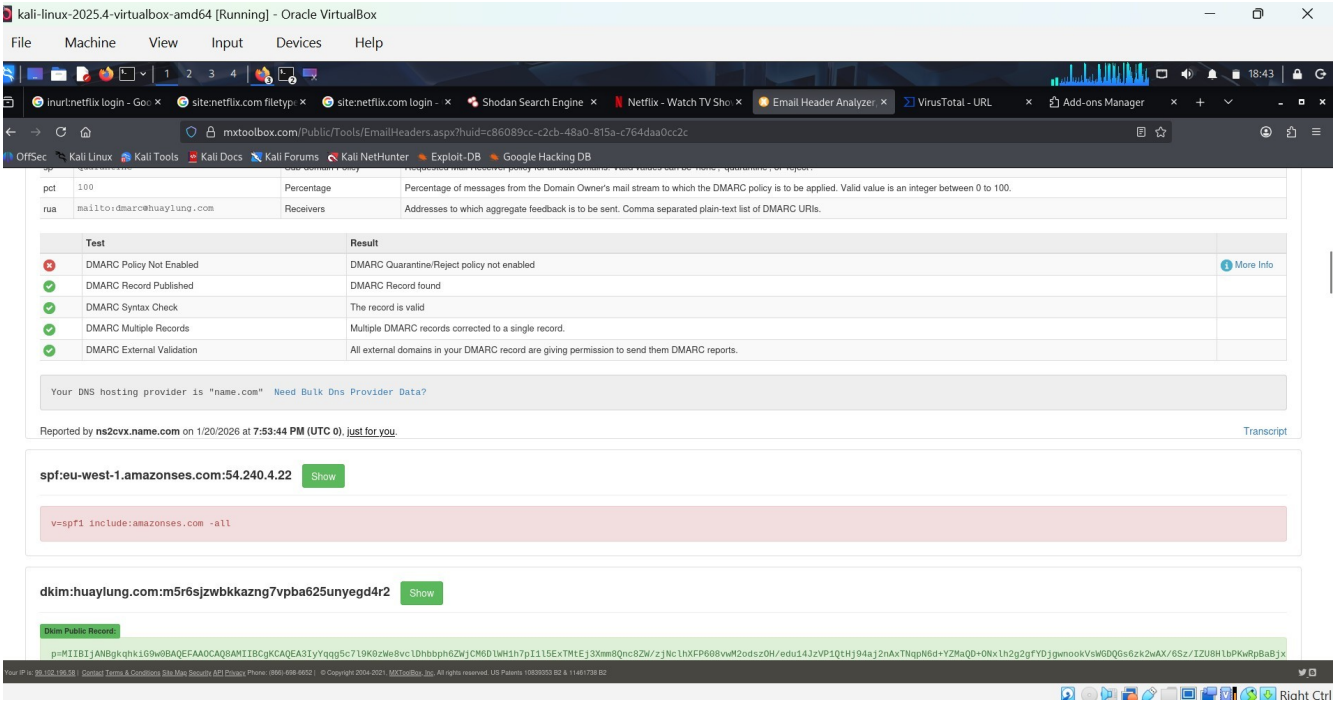
Command: theHarvester -d netflix.com -b all

8.1.3. WaybackMachine



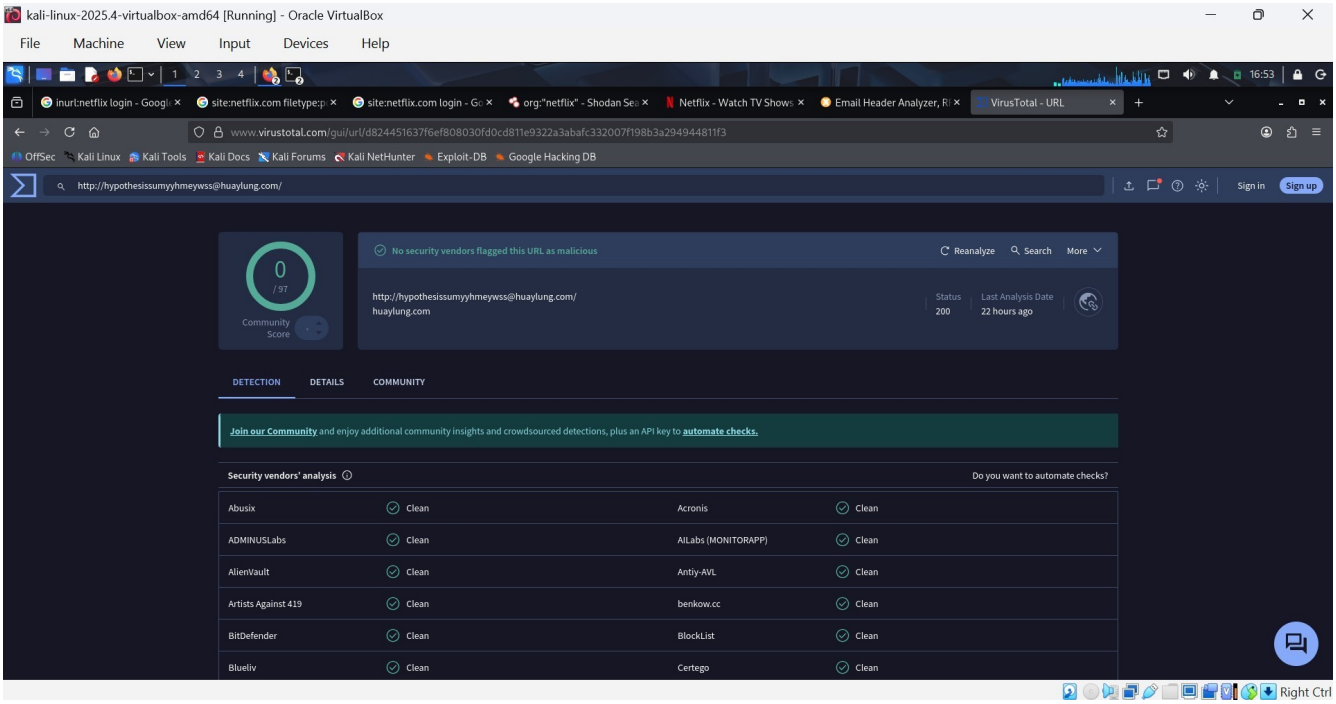
waybackmachine search on netflix.com from 2018

8.1.4. Mxtoolbox Report



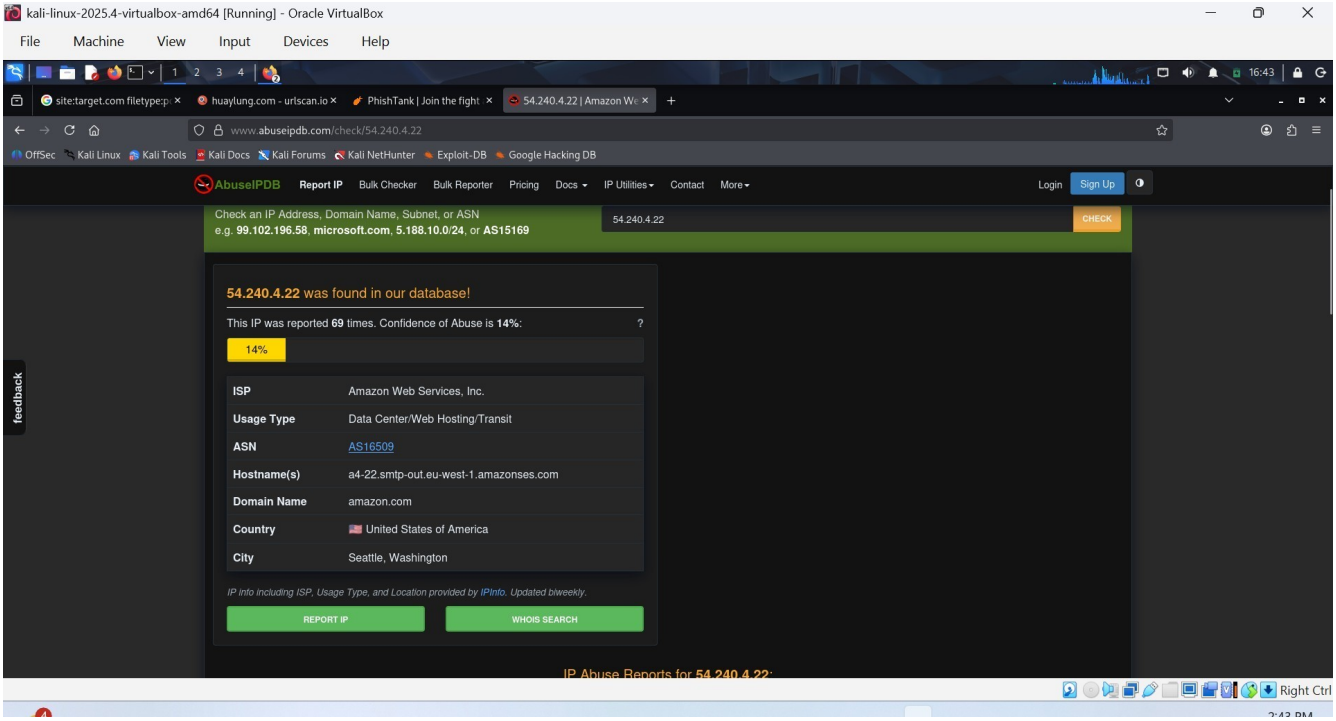
Mxtoolbox analysis of the phishing email reveals AWS

8.1.5. Virustotal Report



VirusTotal report on phishing email. The report came out clean due to the attacker's use of a third-party cloud service, “AWS.”

8.1.6. Abuseipdb report



Abuseipdb report on the Ip address 54.240.4.22 reported from a phishing email.

9. **Mitigation AND Recommendations**

Brand Monitoring and Takedown Processes: There should be continuous brand monitoring to find look-alike domains, fake websites, and impersonation campaigns that target Netflix. This should be done by closely monitoring newly registered domains that look like Netflix branding, setting up quick takedown processes with registrars and hosting providers, and working with threat intelligence vendors to detect brand abuse. Finding issues early shortens the lifespan of phishing campaigns and limits customer exposure. Below are the recommendations suggested:

Email Security Improvements (SPF, DKIM, DMARC): There should be maintenance and enforcement of strong email authentication policies to prevent domain spoofing and impersonation. Continue enforcing DMARC with a strict policy. There should be regular SPF and DKIM settings for third-party services. DMARC reports for spoofing attempts and trends in abuse should be monitored. This action taken will force attackers into relying on less trusted infrastructure, which increases detection and reduces the effectiveness of their campaigns.

User Awareness and Phishing Education: There should be strengthened customer awareness programs that focus on identifying phishing and fraudulent

communications. This can be achieved by publishing clear guidance on official Netflix communication practices, regularly reminding users to verify URLs before entering their credentials. Providing simple ways for users to report suspected phishing attempts. An informed user base greatly reduces the success rate of social engineering attacks.

Continuous OSINT and Threat Monitoring: There should be integration of continuous OSINT monitoring into the threat process to identify emerging threats early. This should be done by monitoring phishing feeds, breach notifications, and abuse databases. Track trends in attacker infrastructure and their delivery methods. Periodically reassess exposure using passive OSINT techniques. Proactive monitoring will allow for early warnings, trend analysis, and quicker responses to changing threats.

10. Conclusion

This OSINT-based threat intelligence assessment focused on and looked at Netflix's external digital presence, focusing on phishing, brand impersonation, credential harvesting, fraud-driven social engineering attacks, and misuse of trusted infrastructure. The findings show that, despite Netflix having strong internal security measures and effective email authentication, its global brand visibility attracts threats driven by social engineering that target customers instead of core systems. Publicly accessible branding elements, login workflows, and communication patterns give attackers enough information to carry out convincing phishing campaigns. This poses risks of financial loss, reputation harm, and loss of customer trust. The assessment highlights the need for ongoing OSINT-driven monitoring to catch emerging threats early, support quick responses, and guide risk-based decision-making. Proactive threat intelligence, along with solid brand protection and user awareness, is crucial for minimizing the impact of external threats and ensuring long-term organizational strength.

11. Ethical Considerations & Disclaimer

All the data used in this assessment was obtained from publicly available sources of open-source intelligence (OSINT) information. No active scanning or exploitation of the Netflix infrastructure was performed. The examination was done solely for academic purposes to assess the exposure to external threats. No confidential data was used or maintained.

References

AbuseIPDB. *Abuseipdb: IP address reputation and abuse reporting*. www.abuseipdb.com_

Google. *Google search*. http: www.google.com

Internet Archive. *Wayback machine*. http://web.archive.org

MXToolbox. *MXToolbox: DNS, blacklist, and email diagnostics*. https: mxtoolbox.com

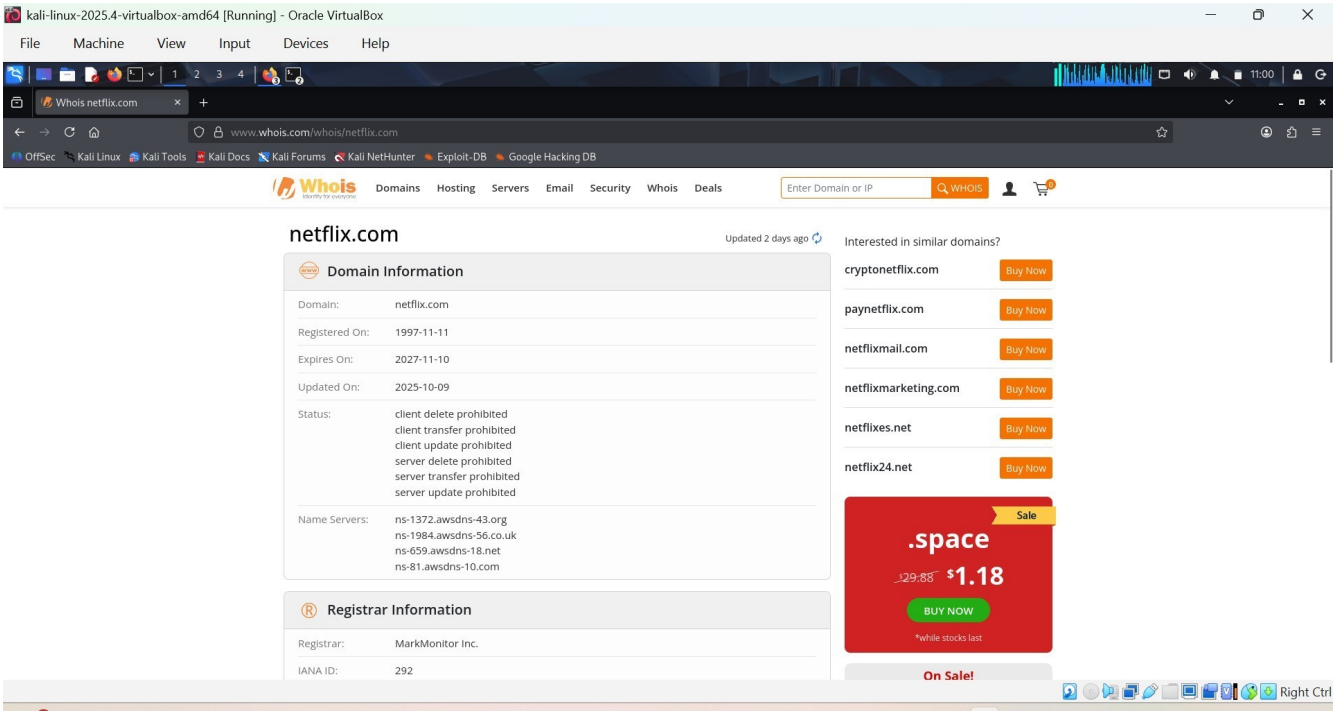
Shodan. *Shodan search engine*. https: www.shodan.io

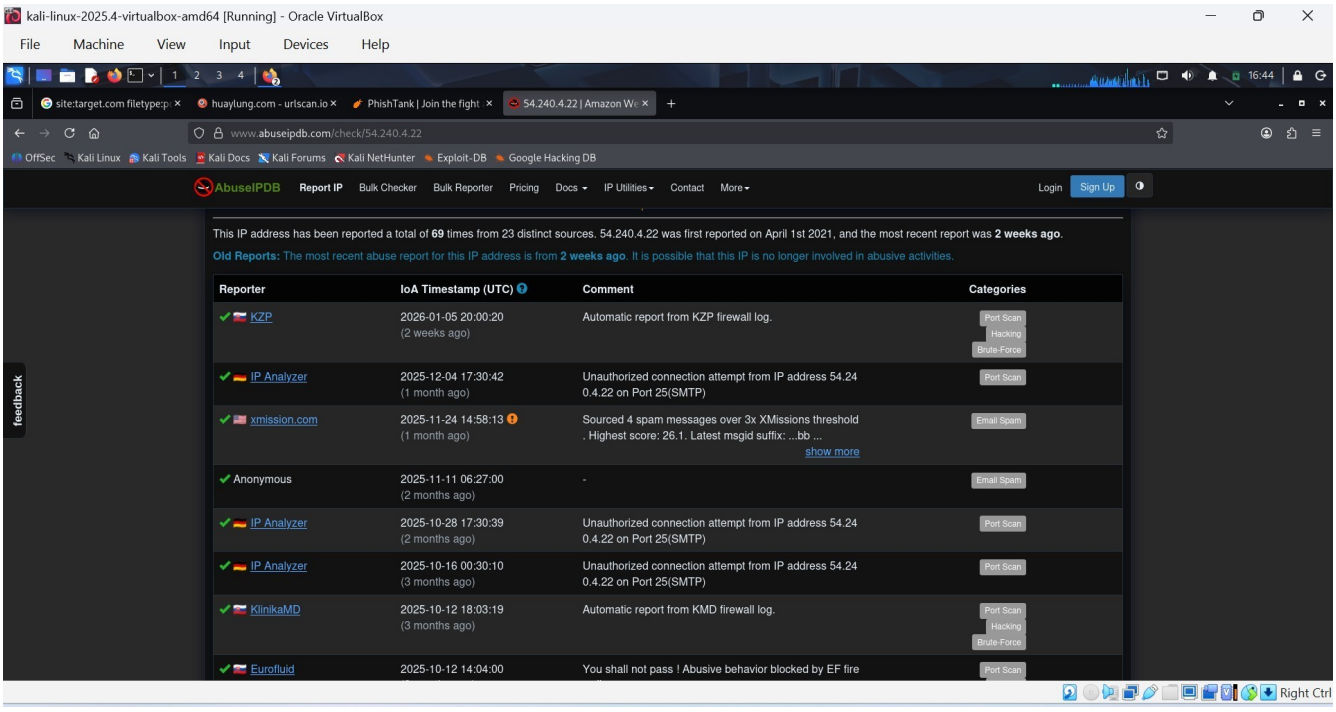
VirusTotal. *VirusTotal: Analyzing suspicious files and URLs*. https:

www.virustotal.com

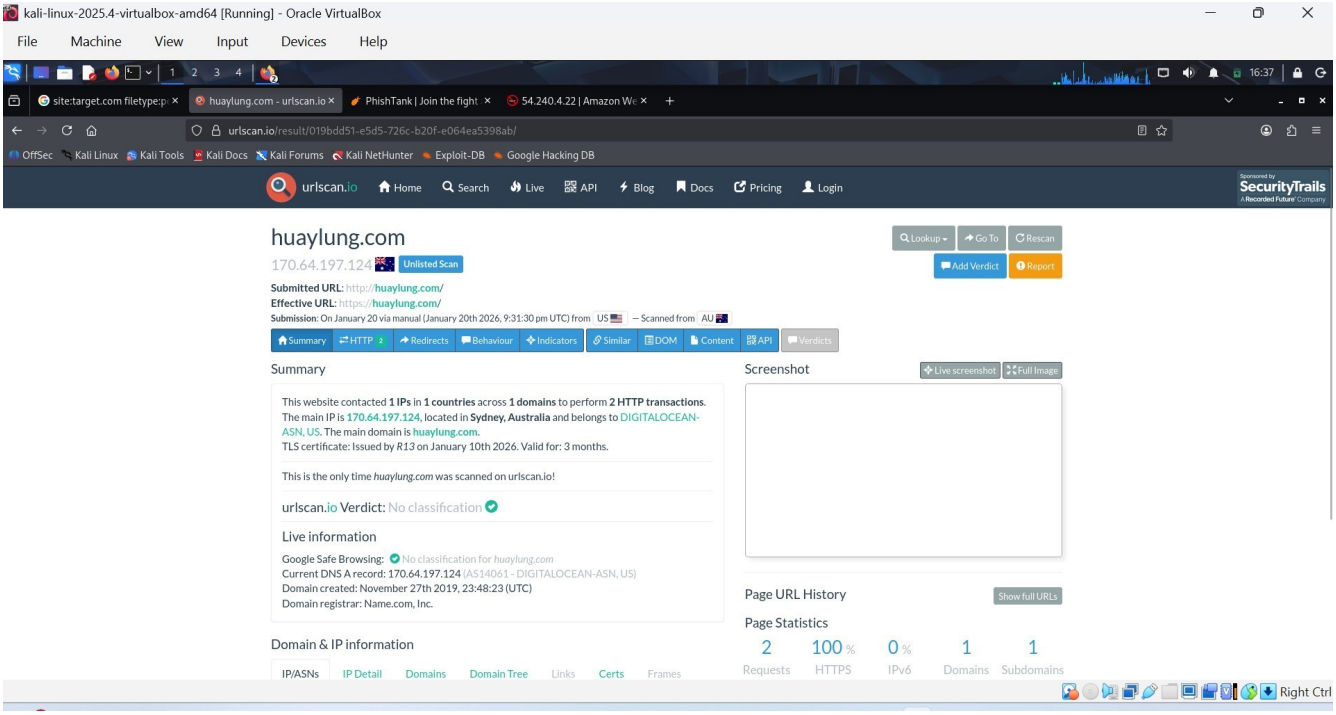
MITRE. *MITRE ATT&CK: Adversary tactics and techniques knowledge base*. https: attack.mitre.org

Appendix

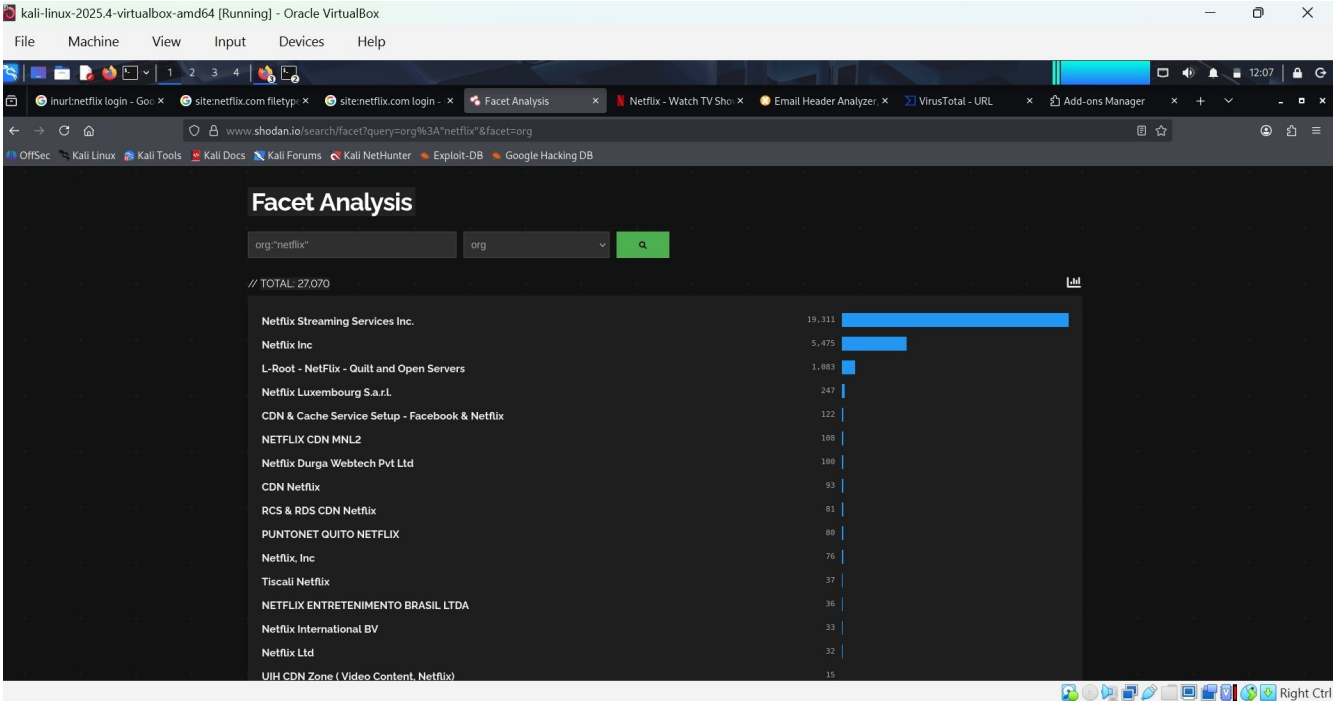




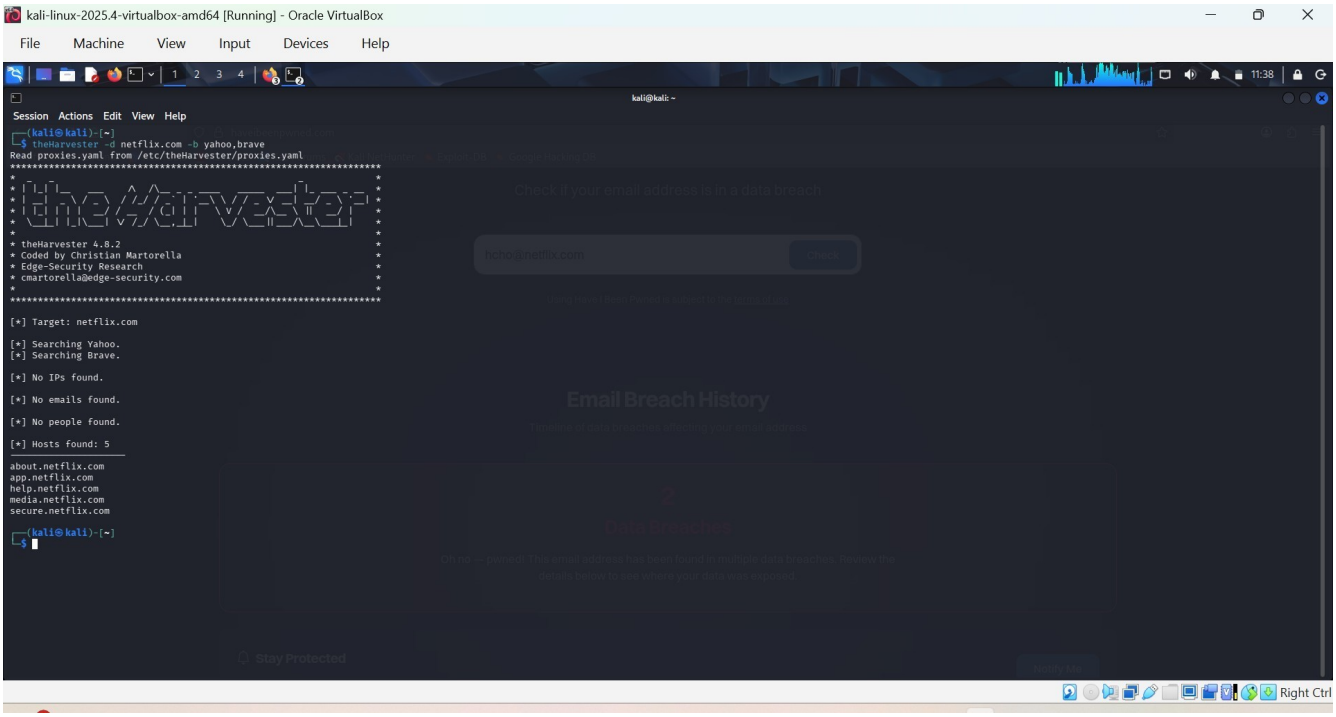
Abuse ipdb re[port on the ip 54.240.4.22



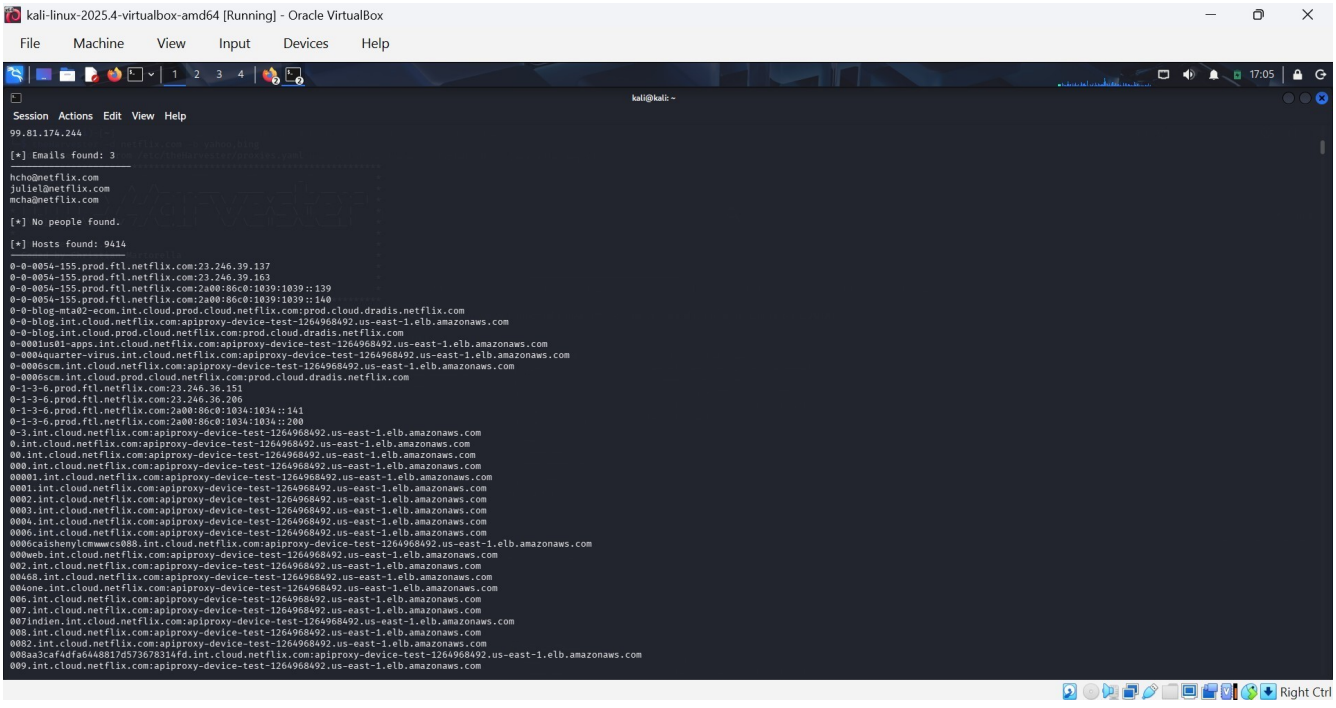
urlscan.io report on phishing email



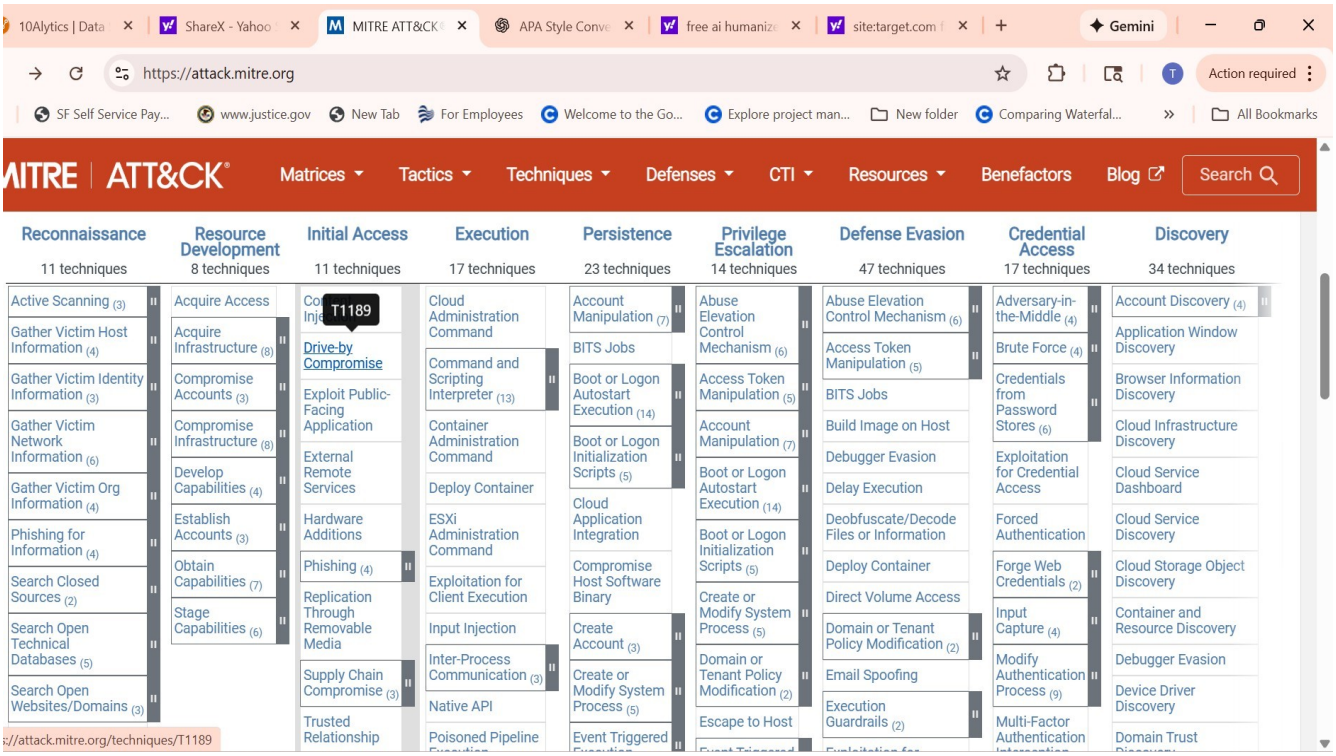
shodan.io search on org:"netflix" organization report



theHarvester -d netflix.com -b yahoo, brave



theHarvester -d netflix.com -b all



Attack Mitre screenshot https://attack.mitre.org

Prepared by: Remi Adeparusi

Cohort: Oct Cohort

Submission Date: January 22nd, 2026 Capstone Project