Phishing Domain Investigation

By: Ziv Kaufman

QUESTION 1

To complete this assignment, I followed a structured process to analyze and assess the risk level of several suspicious URLs provided by the client. Initially, I attempted to access the URLs directly but quickly realized they were inaccessible or formatted to prevent accidental clicks. In cybersecurity, it is standard practice to "defang" malicious URLs to avoid harm during analysis. I used Linux tools and online threat intelligence platforms to evaluate the domains without visiting them directly.

A. https[://]www[.]allsaintsfrance[.]fr/

WHOIS Analysis (Kali Linux):

- Creation Date: May 16, 2025 (5 months old) – suspiciously recent
- Registrant Name: "Ano Nymous" – a red flag, as legitimate brands rarely hide ownership entirely
- Contact Email: avisfosnough01@hotmail.com – appears fake
- Phone/Location Mismatch: Germany (+49), Netherlands (+31), domain uses .fr (France)
- Geographic mismatches are commonly seen in phishing or fraudulent domains

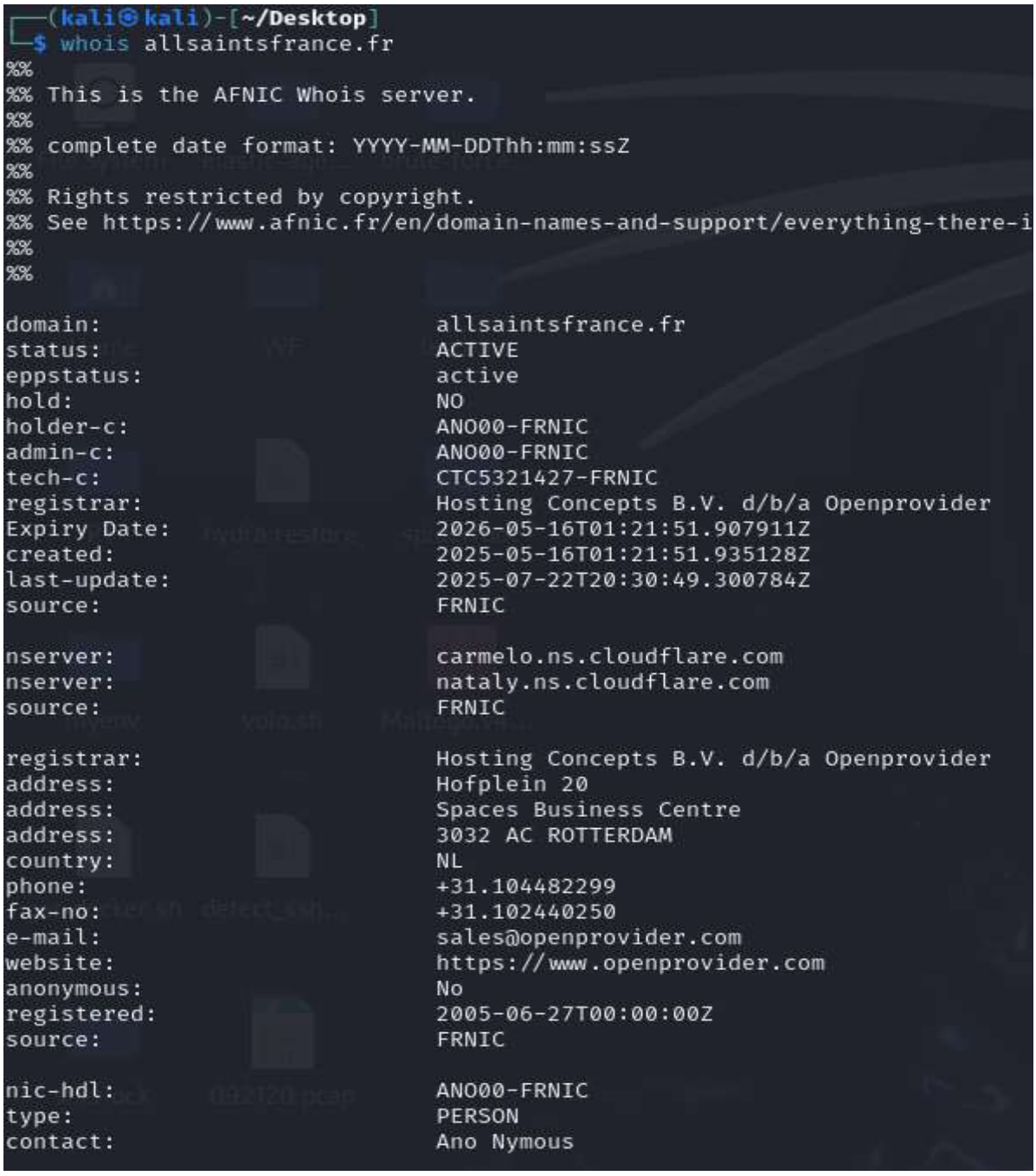

Figure 1: Screenshot or evidence from Kali Linux

Figure 2: Screenshot or evidence from Kali Linux

VirusTotal:

- Flagged as “Phishing” by AlphaMountain.ai
- Flagged as “Malware” by CyRadar, Lionic, Netcraft, and Seclookup
- Multiple detections strongly indicate high risk

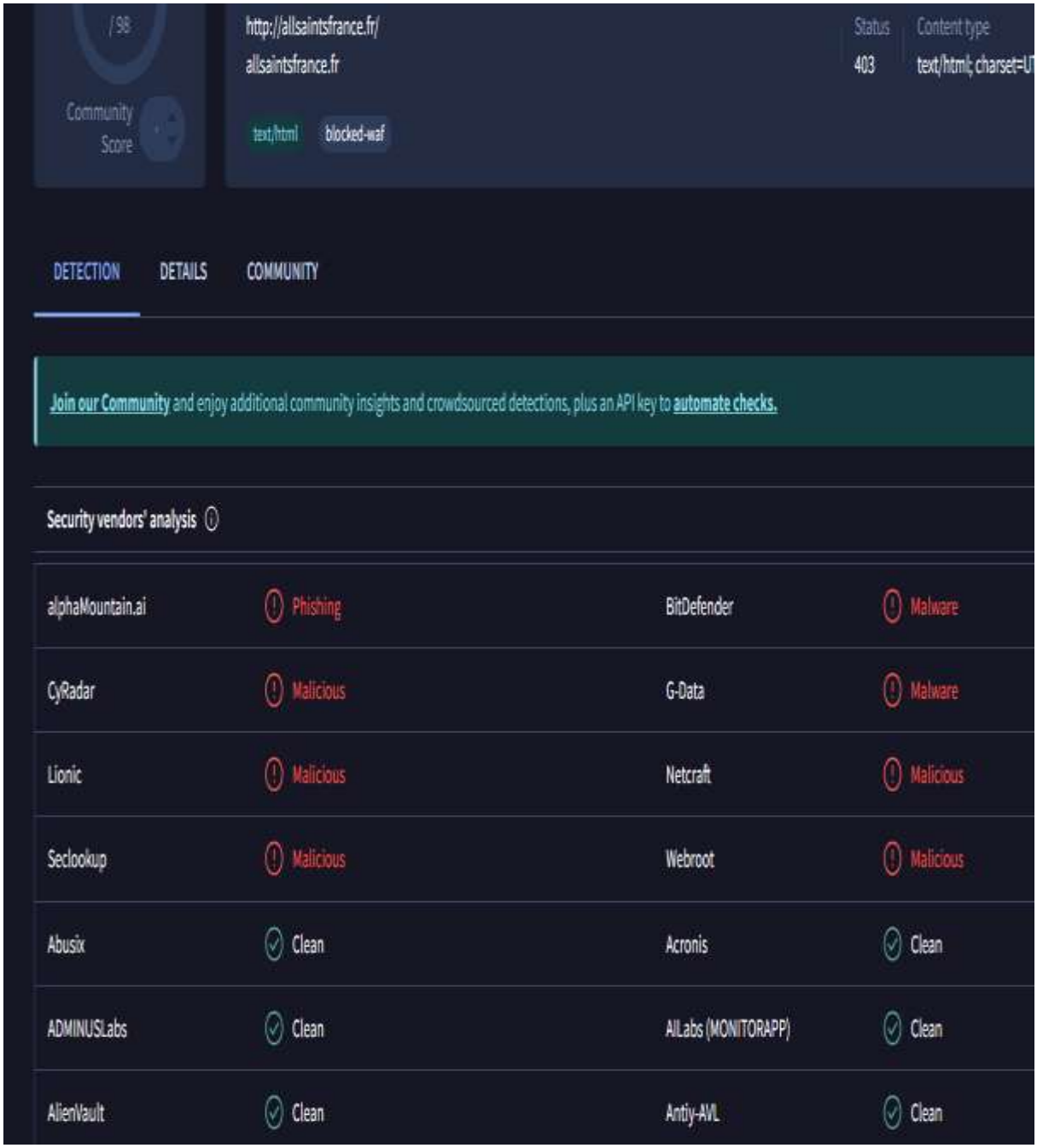

Figure 3: Screenshot or evidence from Virus Total.

Google Search:

- Search in quotation marks to avoid visiting directly
- Advertises ALLSaints leather jackets in French
- Mimics a legitimate online store using authentic-looking imagery

Risk Level: HIGH

B. https[://]careers[.]allsaints[.]com/

WHOIS Analysis (Kali Linux):

- Checked main domain allsaints.com
- Creation Date: 1996 (long-established)
- Expiration: 2027
- Organization: All Saints Retail Limited (matches legitimate brand)
- Country: United Kingdom (matches HQ)

VirusTotal:

- No vendors flagged the domain; all engines marked it as clean

DNS Lookup:

- IP addresses: 104.16.216.130 and 104.16.217.130
- Hosted by Cloudflare, which is common for legitimate companies

Manual Verification:

- Navigating the official AllSaints homepage and clicking “Careers” leads to this URL
- Part of the official corporate website

Risk Level: LOW

C. https[://]allsaintsstore[.]shop/

WHOIS Analysis:

- Creation Date: August 20, 2025 (very recent)
- Expiration Date: August 20, 2026

- Registrar: Chengdu West Dimension Digital Technology Co., LTD (China)
- Recent registration and Chinese registrar are red flags

VirusTotal:

- Flagged as “Malicious” by Netcraft
- Other engines marked it clean

Google Search:

- Website appears “under construction”

ScamAdviser & URLScan.io:

- ScamAdviser labeled as safe (often lacks context)
- URLScan.io flagged as potentially malicious

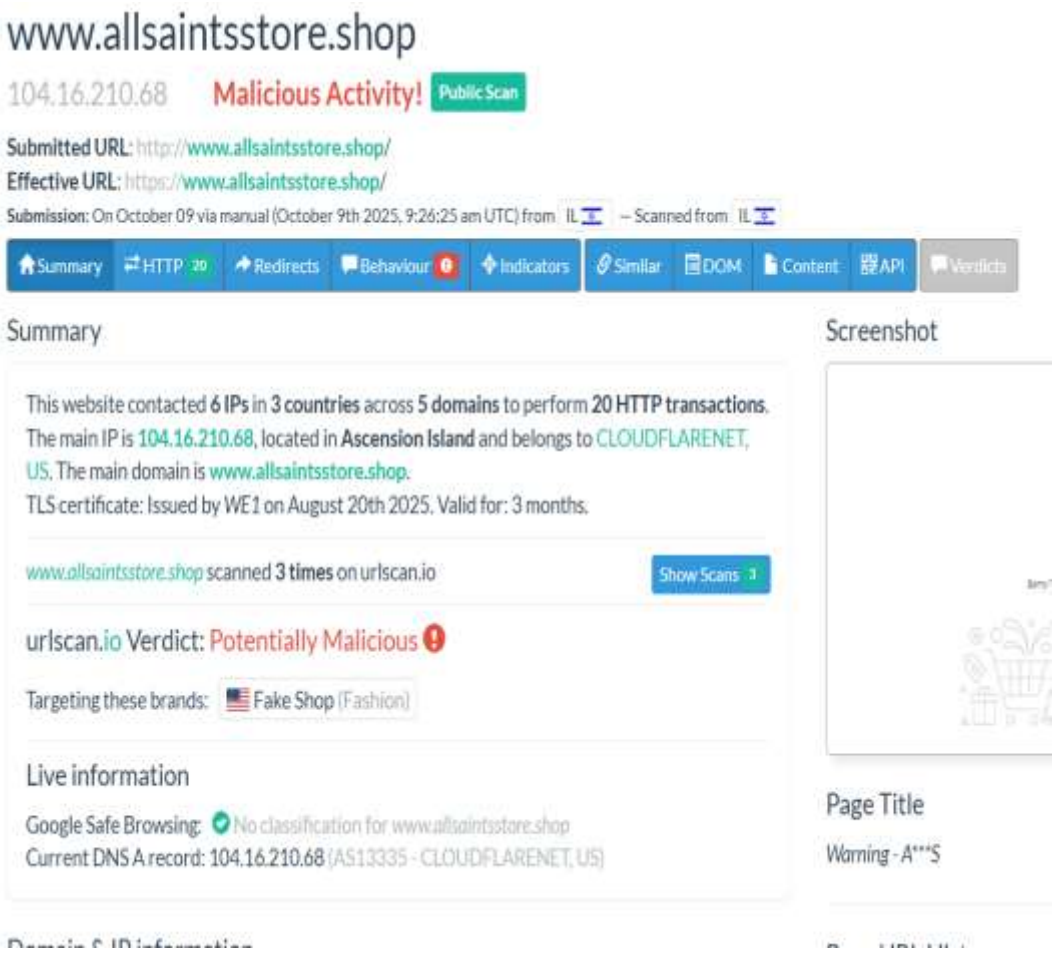

Figure 4: Screenshot or evidence from URLScan.io

Risk Level: MEDIUM

Client Response

Hi Joe,

Thank you for contacting Memcyco.

My name is Ziv Kaufman, and I conducted the investigation regarding the suspicious URLs you reported. Below is a summary of my findings:

• https[://]www[.]allsaintsfrance[.]fr/
This is a high-risk phishing website. Multiple vendors flagged it as malware/phishing. It impersonates a French apparel store to lure victims. Do not click on it or share any personal information. I recommend alerting your French customers that this site is fraudulent.

• https[://]careers[.]allsaints[.]com/
This is a legitimate corporate domain belonging to AllSaints. It is the company's career portal. No malicious activity was detected.

• https[://]allsaintsstore[.]shop/
This domain is not owned by AllSaints. While only one vendor flagged it as malicious, several risk indicators are present (new registration, foreign registrar). Given its inactive state and conflicting reports, I assess it as medium risk.

I hope this provides clarity regarding the risks associated with these URLs. If you have any additional questions or require further support, please don't hesitate to contact me.

Best regards,

Ziv Kaufman
Cybersecurity Analyst

QUESTION 2

For the second question, I evaluated a set of confirmed phishing domains while avoiding direct interaction. I used WHOIS and online tools to extract registration, hosting, and name-server information.

A. https[://]imqoken[.]im/pc/index.html

ViewDNS.info:

- Expiration Date: 07 May 2026 → suggests creation around May 2025
- Name Servers: jillian.ns.cloudflare.com and mcgrory.ns.cloudflare.com

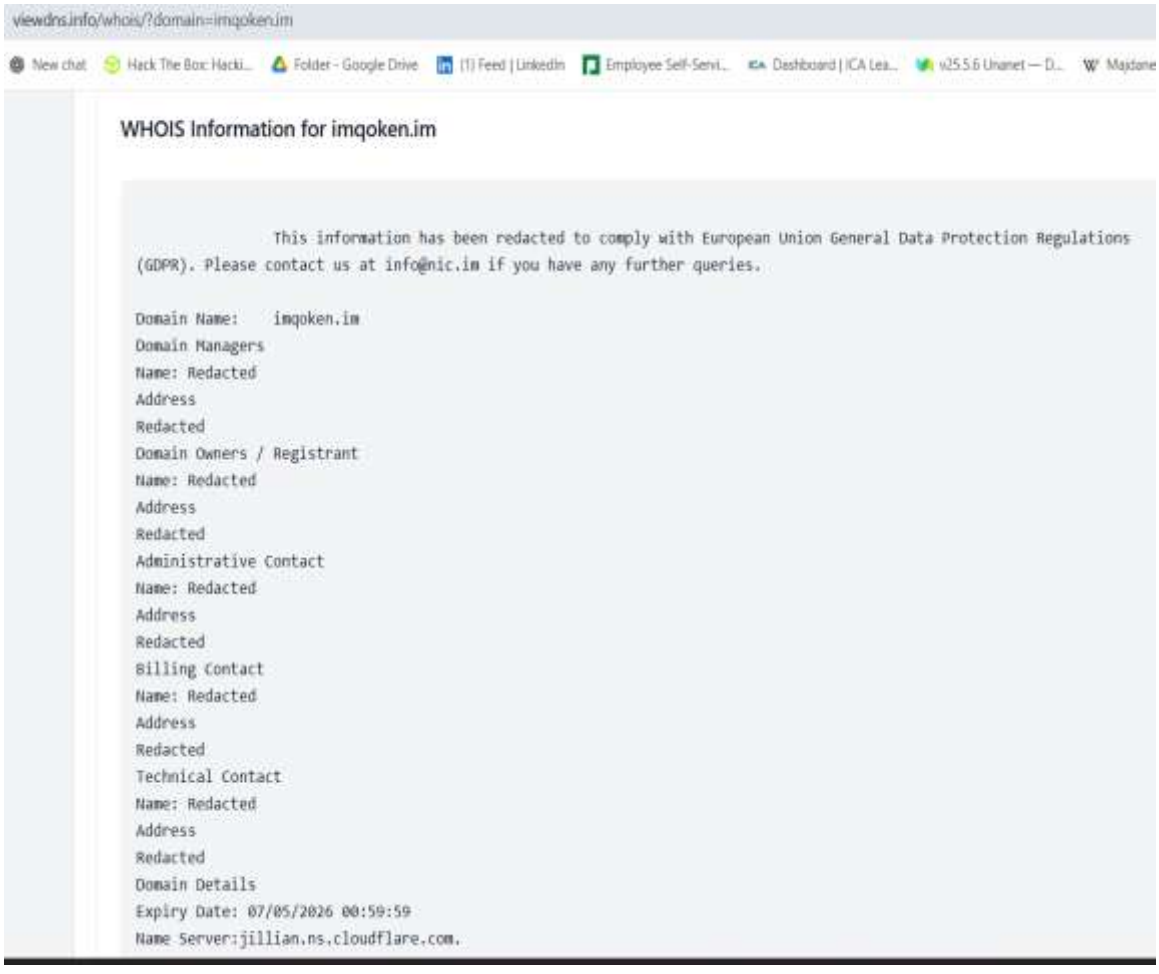

Figure 5: Screenshot or evidence from Viewdns.info

B. https[://]imtakem[.]im/pc/index.html

- Registrar contact: Redacted (GDPR)
- Expiry Date: 07 May 2026 (same as imqoken.im)
- Name Servers: jillian.ns.cloudflare.com / mcgrory.ns.cloudflare.com

Analysis:

- Same TLD (.im), expiry date, and Cloudflare NS
- Likely registered simultaneously
- Strong indication both domains are controlled by the same phishing actor

---

C. https[://]token-de[.]shop/

- Registrar: Chengdu West Dimension Digital Technology Co., LTD (China)
- Creation Date: 10 Sep 2025
- Expiry Date: 10 Sep 2026
- Name Servers: ns5.myhostadmin.net / ns6.myhostadmin.net
- Abuse Contact: abuse@west.cn

Observation:

- Different infrastructure from .im domains
- Likely a different phishing cluster, though the “token” theme may indicate a larger coordinated campaign

---

D. https[://]im-au[.]shop/index.html

- Registrar: Chengdu West Dimension Digital Technology Co., LTD (China)
- Creation Date: 13 Aug 2025
- Expiry Date: 13 Aug 2026
- Name Servers: ns1.myhostadmin.net / ns2.myhostadmin.net
- Registrant Location: Sichuan Province, China

Comparison with token-de.shop:

- Same registrar, country, and hosting family (MyHostAdmin)
- Likely same phishing infrastructure cluster

E. https[://]im-itoken[.]top/

- Registrar: DNSPod, Inc. (China)
- Creation Date: 14 Sep 2025
- Expiry Date: 14 Sep 2026
- Name Servers: cotangent.dnspod.net / group.dnspod.net
- Registrant Country: Anhui Province, China

Observation:

- Different TLD, registrar, and name servers
- Likely a separate phishing cluster

F. https[://]token-mx[.]shop/

- Registrar: Chengdu West Dimension Digital Technology Co., LTD (China)
- Creation Date: 10 Sep 2025
- Expiry Date: 10 Sep 2026
- Name Servers: NS3.MYHOSTADMIN.NET / NS4.MYHOSTADMIN.NET
- Registrant Country: Guangdong Province, China

Observation:

- Fits within the .shop cluster
- Same registrar and hosting provider family

Conclusion:

- Two main phishing clusters plus one standalone domain
- Cluster 1 uses Cloudflare to hide hosting
- Cluster 2 uses Chinese registrar/host infrastructure
- im-itoken.top may represent a separate actor, but geographically still China

---

Additional Notes on Methodology

I primarily relied on `whois` commands in Kali Linux for reliable information. Domains with non-standard TLDs (.top, .shop) were highly suspicious from the outset and I most likely would have figured out they were malicious by myself. Isle of Man (.im) domains were interesting; even if the TLD is legitimate, registration and hosting patterns can indicate malicious activity, as I saw in Question1 with the website supposedly from

France Country of registration, creation dates, registrar, and name servers were used to identify potential patterns and clusters. I focused particularly on domains connected to China or other states associated with cyber threats, as historical data shows high phishing activity from these regions. This structured approach allowed me to determine patterns and assess risk levels without interacting directly with the malicious sites.