

# 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

```
(kali㉿kali)-[~/Desktop]
$ whois allsaintsfrance.fr
%%
%% This is the AFNIC Whois server.
%%
%% complete date format: YYYY-MM-DDThh:mm:ssZ
%%
%% Rights restricted by copyright.
%% See https://www.afnic.fr/en/domain-names-and-support/everything-there-i
%%
%%
domain:                allsaintsfrance.fr
status:                ACTIVE
eppstatus:            active
hold:                 NO
holder-c:              ANO00-FRNIC
admin-c:              ANO00-FRNIC
tech-c:               CTC5321427-FRNIC
registrar:            Hosting Concepts B.V. d/b/a Openprovider
Expiry Date:          2026-05-16T01:21:51.907911Z
created:              2025-05-16T01:21:51.935128Z
last-update:          2025-07-22T20:30:49.300784Z
source:              FRNIC

nserver:              carmelo.ns.cloudflare.com
nserver:              nataly.ns.cloudflare.com
source:              FRNIC

registrar:            Hosting Concepts B.V. d/b/a Openprovider
address:              Hofplein 20
address:              Spaces Business Centre
address:              3032 AC ROTTERDAM
country:              NL
phone:               +31.104482299
fax-no:              +31.102440250
e-mail:              sales@openprovider.com
website:              https://www.openprovider.com
anonymous:           No
registered:          2005-06-27T00:00:00Z
source:              FRNIC

nic-hdl:              ANO00-FRNIC
type:                 PERSON
contact:              Ano Nymous
```

Figure 1: Screenshot or evidence from Kali Linux

```
File Actions Edit View Help
registrar: Hosting Concepts B.V. d/b/a Openprovider
anonymous: YES
remarks: ----- WARNING -----
remarks: While the registrar knows him/her,
remarks: this person chose to restrict access
remarks: to his/her personal data. So PLEASE,
remarks: don't send emails to Ano Nymous. This
remarks: address is bogus and there is no hope
remarks: of a reply.
remarks: ----- WARNING -----
obsoleted: NO
eppstatus: associated
eppstatus: active
eligstatus: ok
eligsource: REGISTRAR
eligdate: 2025-05-16T01:21:51.008766Z
reachstatus: ok
reachmedia: email
reachsource: REGISTRAR
reachdate: 2025-05-16T01:21:51.008766Z
source: FRNIC

nic-hdl: CTC5321427-FRNIC
type: PERSON
contact: douglas s keeton
address: WildermannstraBe 86B
address: 53859 Niederkassel
address: Niederkassel
country: DE
phone: +49.15166204477
fax-no: +49.15166204477
e-mail: avisfosnough01@hotmail.com
registrar: Hosting Concepts B.V. d/b/a Openprovider
changed: 2025-05-16T01:21:51.474539Z
anonymous: NO
obsoleted: NO
eppstatus: associated
eppstatus: active
eligstatus: ok
eligsource: REGISTRAR
eligdate: 2025-05-16T01:21:51.222417Z
reachstatus: ok
reachmedia: email
reachsource: REGISTRAR
reachdate: 2025-05-16T01:21:51.222417Z
source: FRNIC

>>> Last update of WHOIS database: 2025-10-09T09:12:03.655093Z <<<
```

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

The screenshot shows the VirusTotal interface for the URL `http://allsaintsfrance.fr/`. The status is 403 and the content type is `text/html; charset=UTF-8`. The community score is 98. The analysis shows several security vendors' results:

Vendor	Detection	Vendor	Detection
alphaMountain.ai	Phishing	BitDefender	Malware
CyRadar	Malicious	G-Data	Malware
Lionic	Malicious	Netcraft	Malicious
Seclookup	Malicious	Webroot	Malicious
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	ALLabs (MONITORAPP)	Clean
AlienVault	Clean	Antiy-AVL	Clean

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:

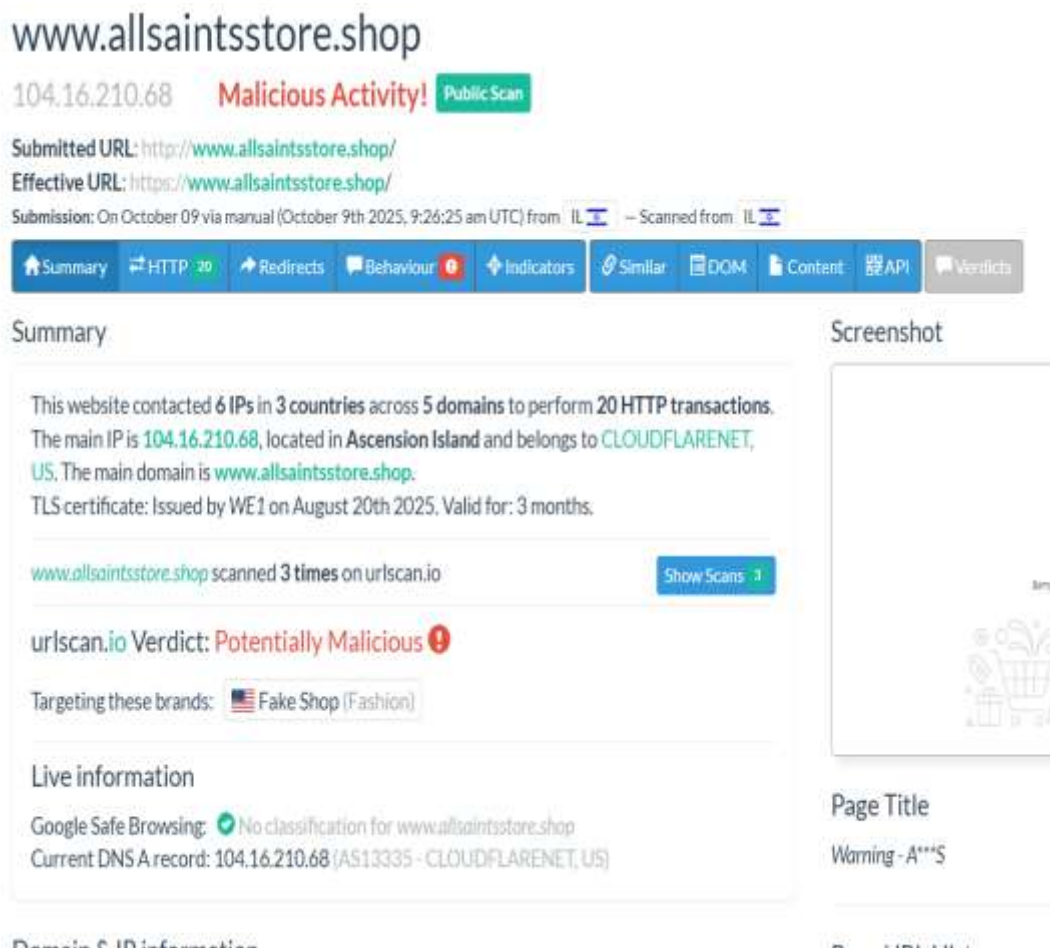
- Flagged as “Malicious” by Netcraft
- Other engines marked it clean

### Google Search:

- Website appears “under construction”

### ScamAdviser & URLScan.io:

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



The screenshot displays the URLScan.io analysis interface for the website **www.allsaintsstore.shop**. At the top, the IP address **104.16.210.68** is shown with a red **Malicious Activity!** warning and a **Public Scan** button. Below this, the submitted and effective URLs are listed as **http://www.allsaintsstore.shop/** and **https://www.allsaintsstore.shop/** respectively. The submission details indicate it was made on October 09 via manual on October 9th 2025, 9:26:25 am UTC from IL, scanned from IL.

A navigation bar contains various analysis tabs: Summary, HTTP (20), Redirects, Behaviour (0), Indicators, Similar, DOM, Content, API, and Verdicts. The **Summary** tab is active, showing a detailed report. The summary text states: "This website contacted 6 IPs in 3 countries across 5 domains to perform 20 HTTP transactions. The main IP is 104.16.210.68, located in Ascension Island and belongs to CLOUDFLARENET, US. The main domain is www.allsaintsstore.shop. TLS certificate: Issued by WE1 on August 20th 2025. Valid for: 3 months." Below this, it notes that the website was scanned 3 times on urlscan.io, with a **Show Scans** button. The **urlscan.io Verdict** is **Potentially Malicious** with a red warning icon. It also indicates the website is **Targeting these brands: Fake Shop (Fashion)**.

The **Live information** section shows **Google Safe Browsing** with a green checkmark and "No classification for www.allsaintsstore.shop". The **Current DNS A record** is **104.16.210.68 (AS13335 - CLOUDFLARENET, US)**. To the right of the summary, a **Screenshot** placeholder is visible, and below it, the **Page Title** is listed as **Warning - A\*\*\*S**.

**Figure 4: Screenshot of 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](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

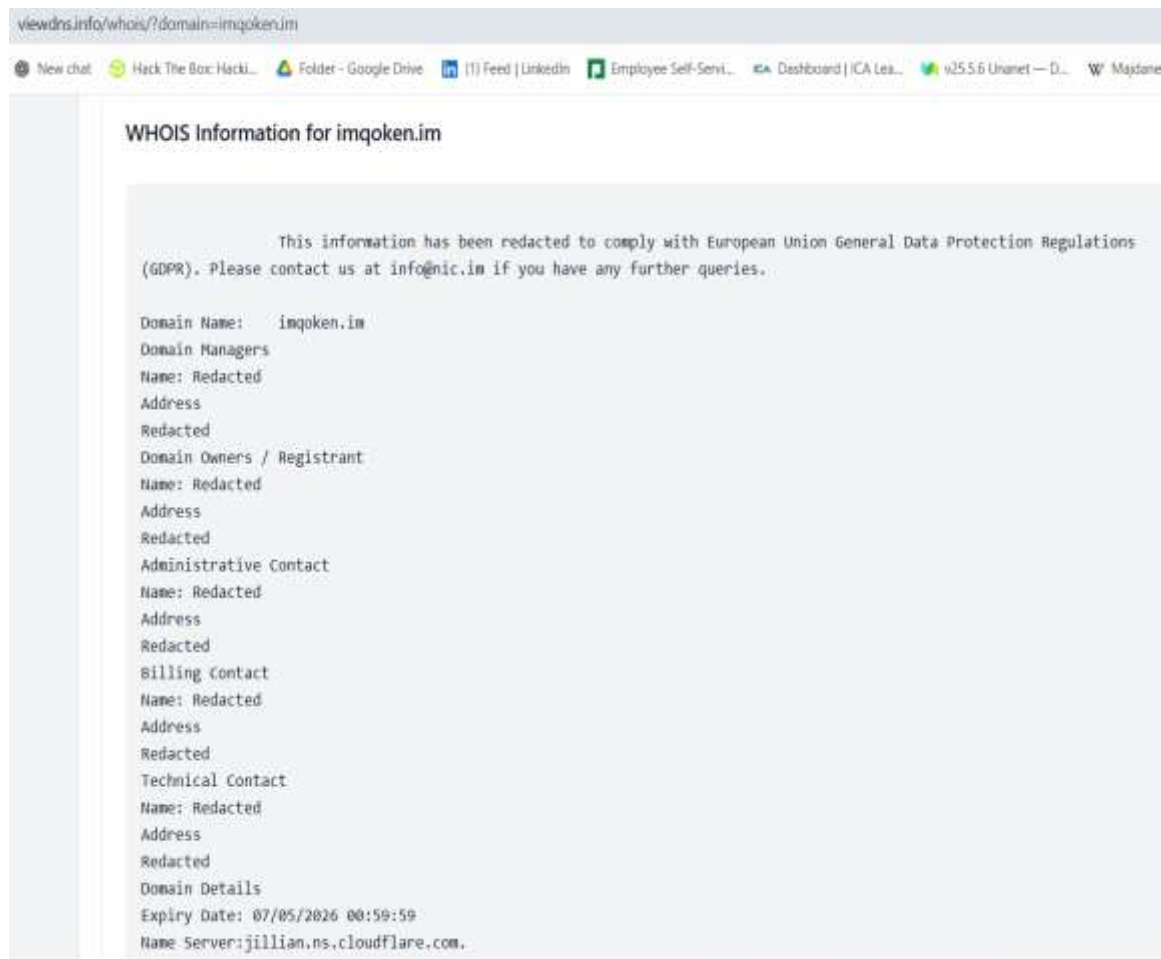


Figure 5: Screenshot or evidence from Viewdns.info



## **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.