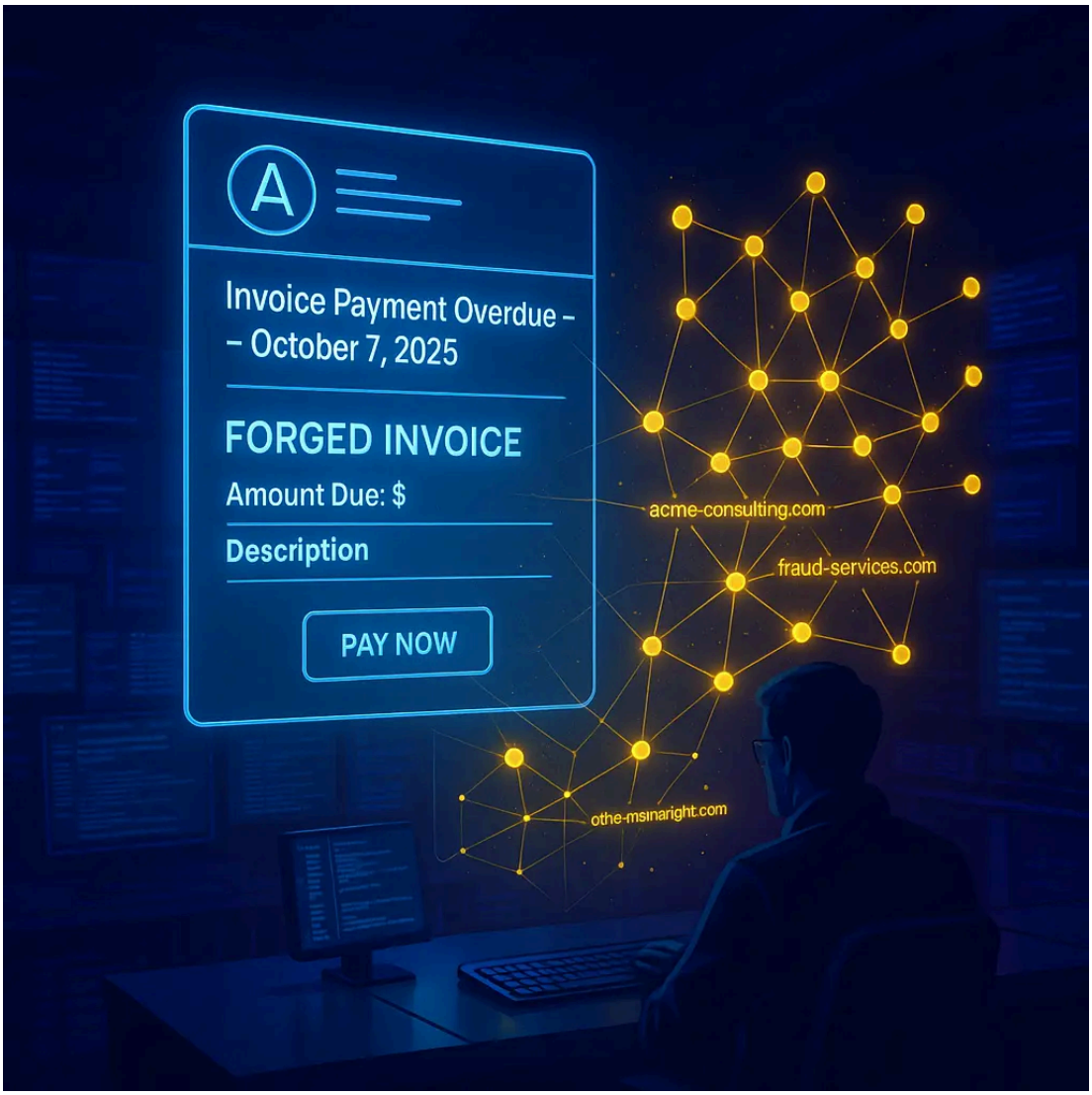
Exploring Invoice Fraud Email Attempts with Validin

⋮ 10/8/2025



By: Kenneth Kinion

2025-10-09

general

Investigating a surprisingly well-crafted scam directed at a Validin employee

It’s fair to say that we see a lot of phishing and fraud emails at Validin. On Tuesday, October 7, 2025, someone on the Validin team received an email that was so convincing that they had to ask if it was real. In this post, we’ll show you how we dove into the breadcrumbs left by this email to identify dozens of domains likely related to this surprisingly sophisticated and intricate campaign. We’ll also show you everything we uncovered in the hope that it helps others identify this type of fraud to limit its effectiveness. Finally, we blocked the complete list of related domain names and I encourage you to do the same with the list of indicators at the end of this blog post.

Fraud Email

The email that Validin received appeared well-structured and was designed to show a realistic and plausible exchange of emails between me and someone at a consulting services company. As a company executive, I was likely chosen as the authority on the Validin side to provide authority to the fake exchange.

One detail I want to address: my name has been used in phishing and fraud attempts against my employees for years in “boss/CEO” gift card scams, direct deposit update scams, and other scams. In fact, these fraud attempts started almost immediately after my first employees advertised in public (e.g., on LinkedIn) that they were employees of Validin. With data brokers, data breaches, and easy access to generative AI tools, it is now incredibly easy and low-cost to map employee-employer relationships, find working contact details, and craft convincing fraud emails targeting companies of virtually any size. If you’re big enough to have employees, you’re big enough to be targeted.

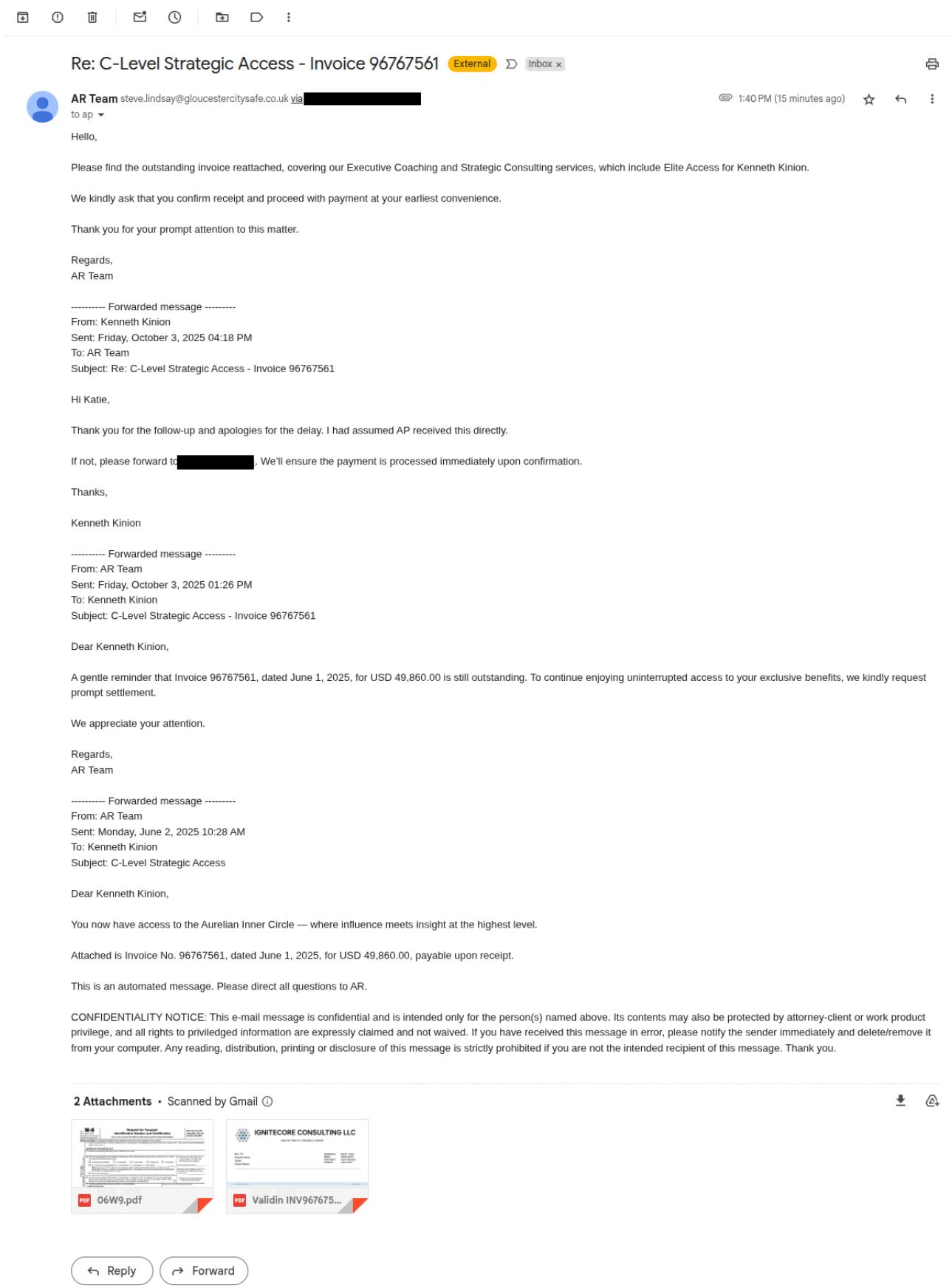


Figure 1. Fraud email requesting payment to invoices, complete with an invoice and a W9 attachment.

The email also included a W9 with an EIN and a company name that matched the domain name in the reply-to address, and an invoice address to me/Validin and remittance details. I'll note that the reply-to header in the email ensures that most mail clients will direct replies to a different email address than the one used to send the email.

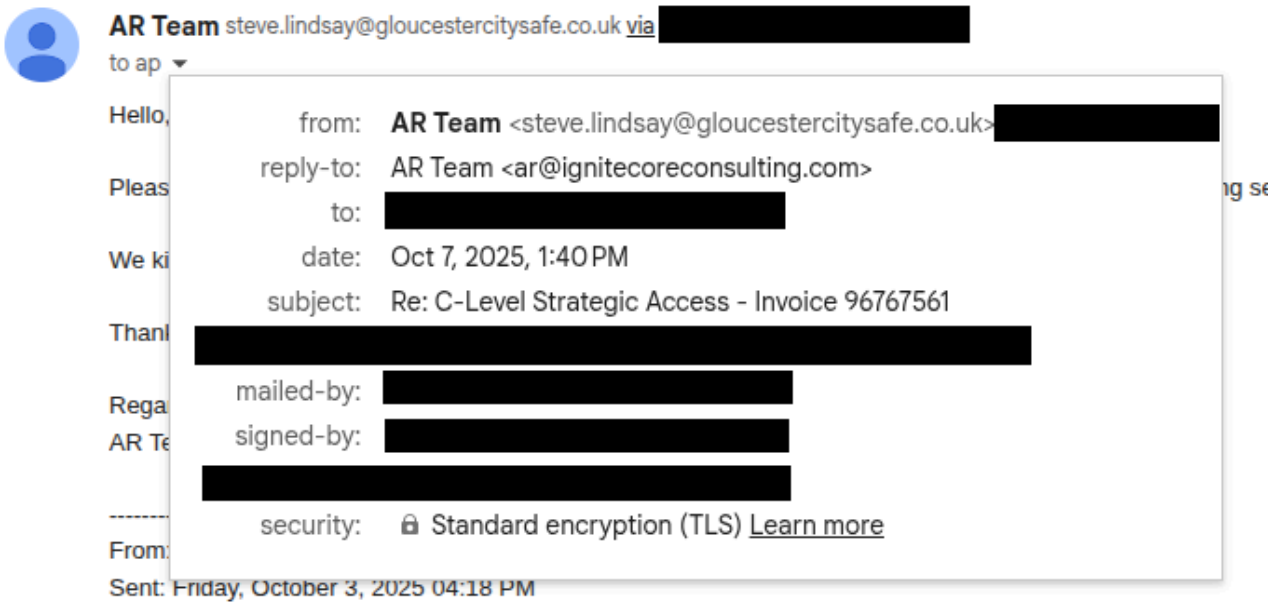


Figure 2. Headers for fraud email.

Company Details

The company on the invoice we received was "Ignitecore Consulting LLC" and presents the address 1400 W 72nd, Chicago, IL 60636 (one that Google Maps is unable to pinpoint). There is also a bank account number and valid ACH and wire routing numbers that direct to Bank of America (note: the Bank of America abuse team received original versions of these documents).

Since the company advertised an Illinois address, I decided to check the Illinois Secretary of State website to see if there was an actual registered entity for "Ignirecore Consulting LLC." To my great surprise, there was!

Form **LLC-5.5**

Illinois
Limited Liability Company Act
Articles of Organization

FILE # 16673714

Secretary of State Alexi Giannoulias
Department of Business Services Limited Liability Division
www.ilsos.gov

Filing Fee: $150

Approved By: GPC

FILED
AUG 17 2025
Alexi Giannoulias
Secretary of State

1. Limited Liability Company Name: IGNITECORE CONSULTING LLC

2. Address of Principal Place of Business where records of the company will be kept:
1400 W 72ND ST
CHICAGO, IL 60636

3. The Limited Liability Company has one or more members on the filing date.

4. Registered Agent's Name and Registered Office Address:
[redacted]
1400 W 72ND ST
CHICAGO, IL 60636-4002

5. Purpose for which the Limited Liability Company is organized:
"The transaction of any or all lawful business for which Limited Liability Companies may be organized under this Act."

6. The LLC is to have perpetual existence.

7. Name and business addresses of all the managers and any member having the authority of manager:
[redacted]
1400 W 72ND ST
CHICAGO, IL 60636

8. **Name and Address of Organizer**
I affirm, under penalties of perjury, having authority to sign hereto, that these Articles of Organization are to the best of my knowledge and belief, true, correct and complete.

Dated: AUGUST 17, 2025 [redacted]
1400 W 72ND ST
CHICAGO, IL 60636

This document was generated electronically at www.ilsos.gov

Figure 3. The registration for "IGNITECORE CONSULTING LLC" was less than two months old according to the Illinois Secretary of State website.

This company was registered as an LLC on August 17, 2025. It's unclear if the registration is directly tied to this scam, or if it's simply being commandeered to facilitate fraud.

Landing Page

The domain `igniteconsulting[.]com` hosts a single-page landing page with a relatively simplistic attempt to appear like a legitimate consulting service. It has the basics: a services section, about section, team section, and even provides a contact form.

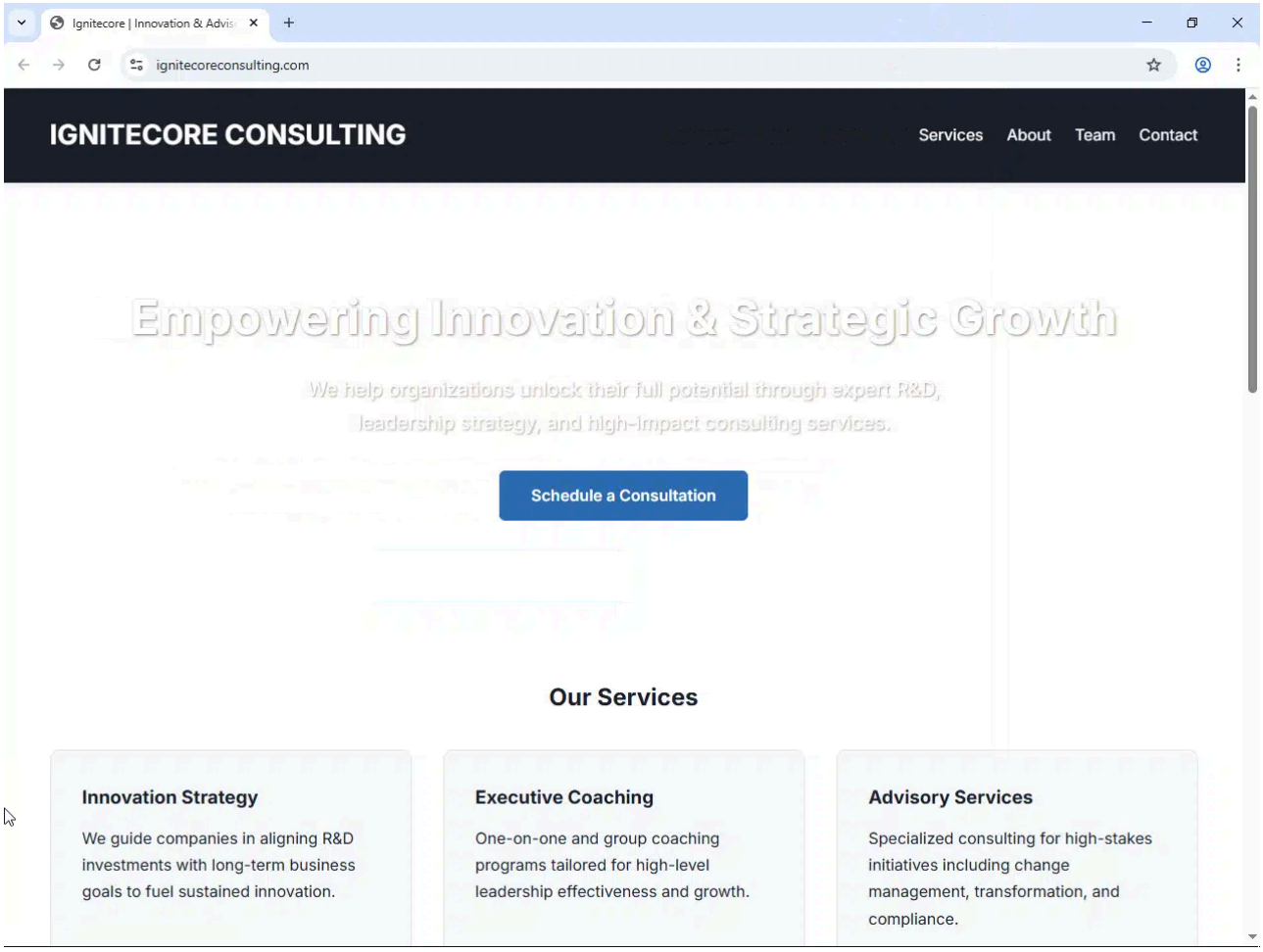


Figure 4. Screenshot of the HTML page served at the reply-to domain from the fraud email.

Note: I always advise to visit suspicious websites using services like URLScan that can safely visit websites in sandboxes.

Domain Enrichment

At this point, I want to learn more about the domain name in the reply-to field, `igniteconsulting[.]com`, to find other domain names that are being used in similar ways.

Searching for this domain in Validin, I found key details like registration date, host response history (how the domain responded when we visited the domain over HTTP/S), and DNS history. The first thing that stood out

is that the domain was less than 3 days old.

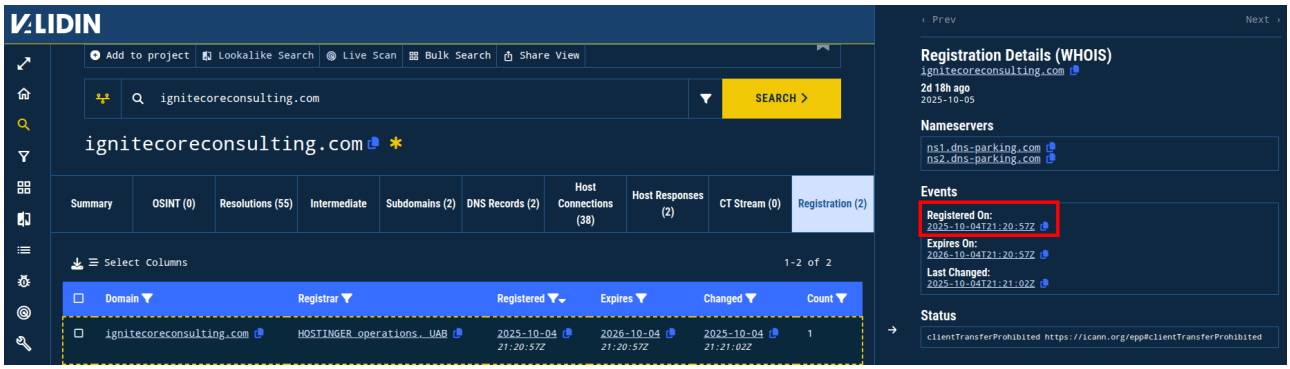


Figure 5. Initial enrichment shows that the reply-to domain was very recently registered (less than 3 days old as of the time of the investigation).

Additionally, I saw from the host responses that there's a webpage claiming to provide "Innovation & Advisory Services," which matches the services claimed on the invoice and the screenshot from the landing page.

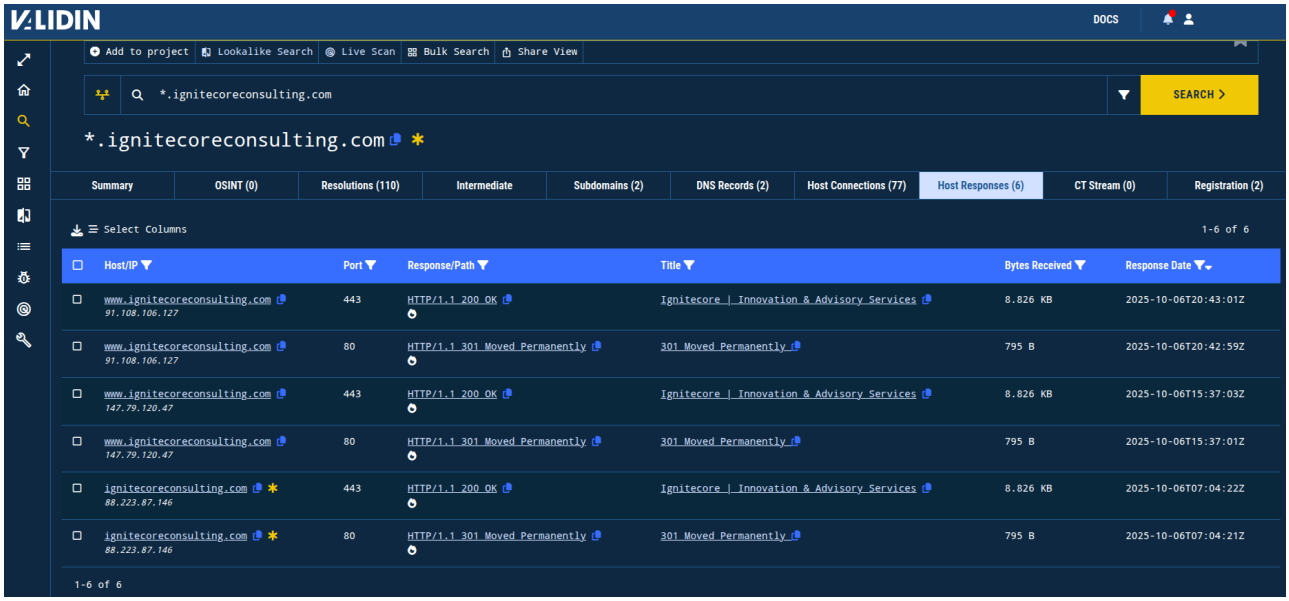


Figure 6. Host responses show a response with a title tag value "Ignitecore | Innovation & Advisory Services."

On Validin's "Host Connections" tab, I find pivotable features that Validin extracted out of the responses from the domain name. These features can help me find other domain names that have the same features which can help discover related domain names.

Using the result filters, I filtered out features that had high pivot counts (more than 20k estimated connections) and focused on header, banner, and CSS class hashes. Among these, the HOST-CLASS_0_HASH and HOST-CLASS_1_HASH (two variations of hashes of the CSS classes used in the HTML responses) linked to a small number of domains that all have consulting, finance, and LLC themes in

their domain names. This would indicate both a common HTML theme and a common domain naming convention.

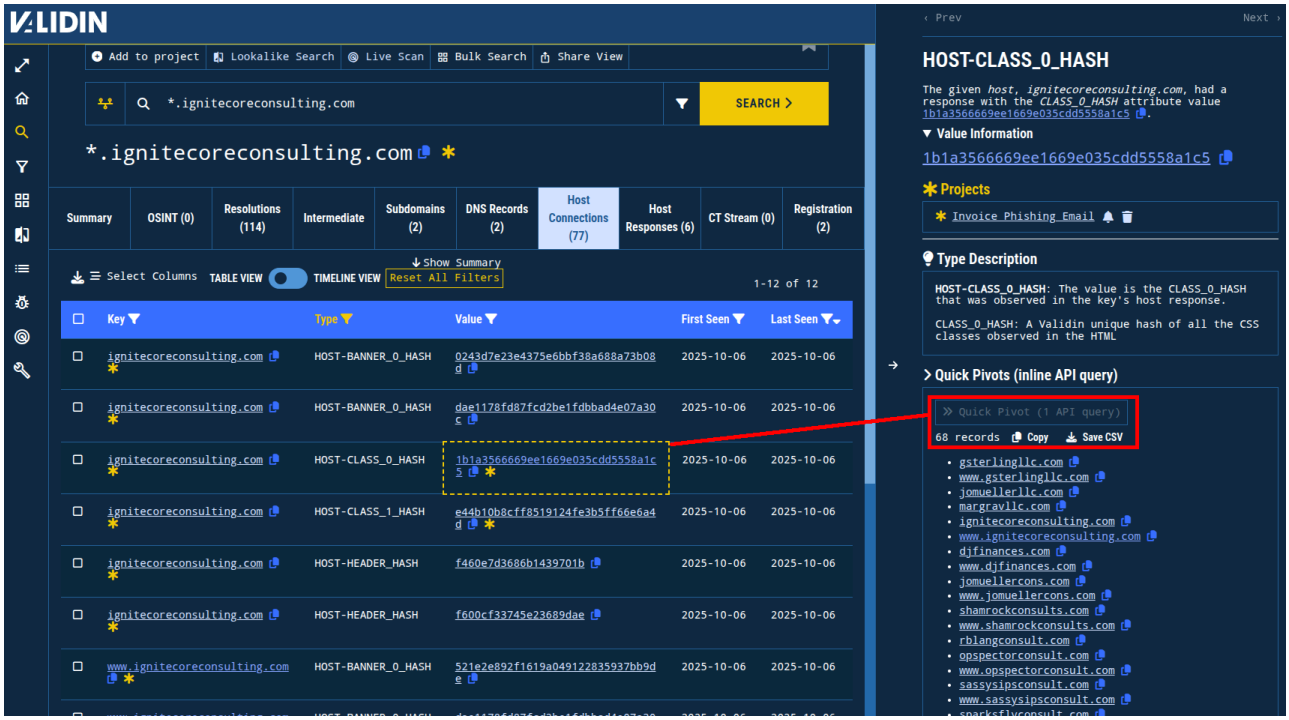


Figure 7. Using the “Quick Pivots” feature to find good pivots for discovering related infrastructure.

CSS Hash Pivot

Pivoting on `1b1a3566669ee1669e035cdd5558a1c5`, I find the 68 connections use a number of unique HTML titles in the web pages returned from the HTTP(S) requests. Note that all of them include the phrase “Innovation & Advisory Services.”

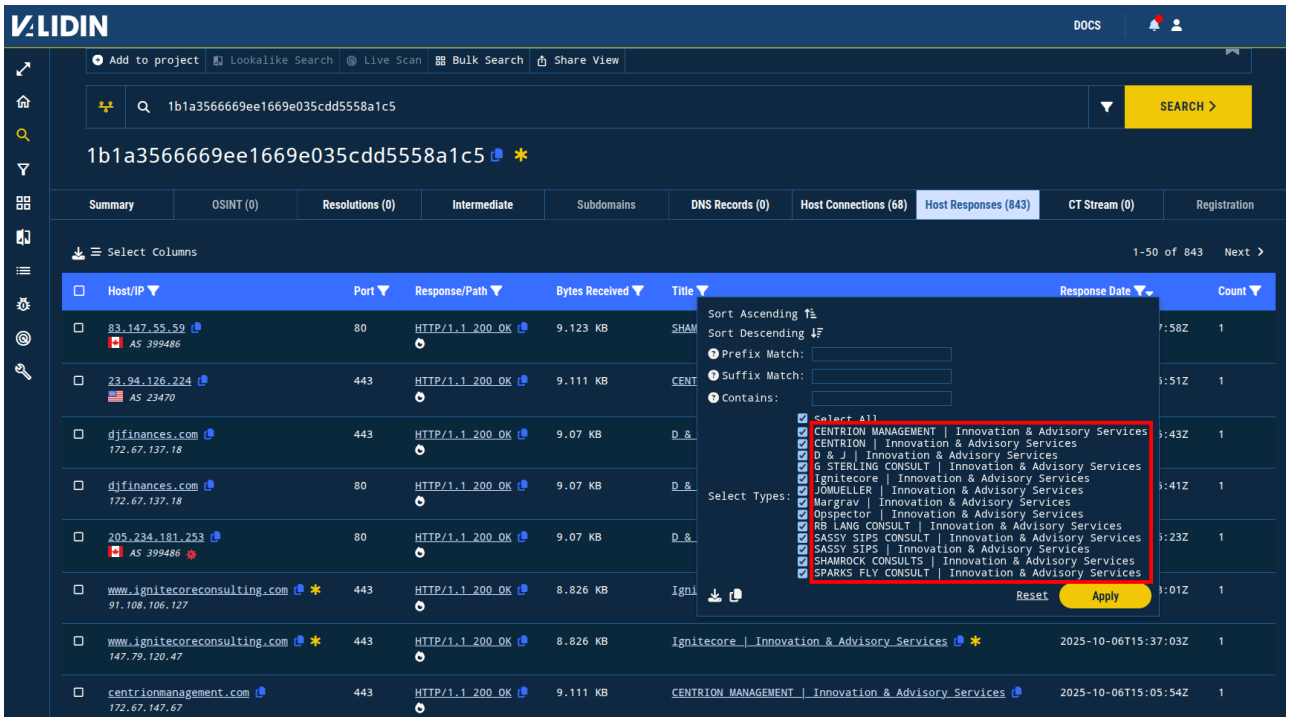


Figure 8. Unique title tags for the CLASS hash, which was used to identify a template that appears to have been used by this campaign a number of times.

I see from the history of this pivot that Validin didn't observe the first domains/IPs with this template until late July.

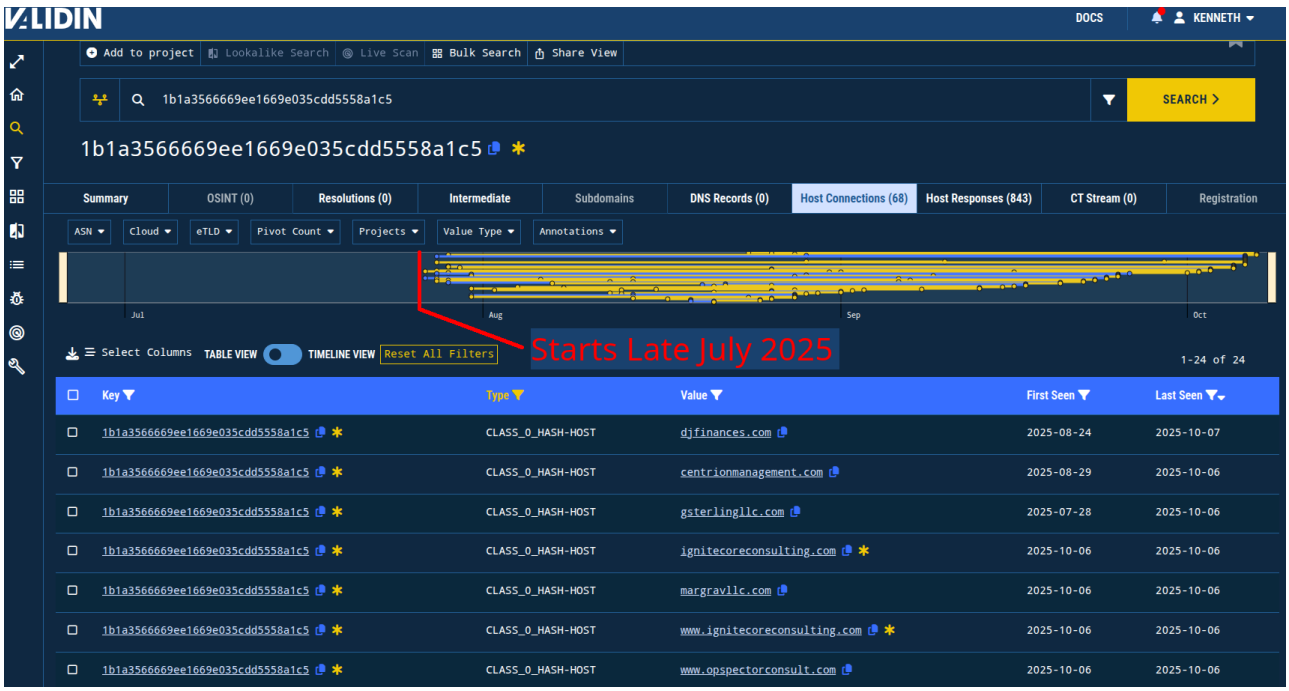


Figure 9. Observing the first observed time for the template in this campaign.

I also noted that many of the IPs that returned this template are on Cloudflare, but 16 IP addresses across 5 ASNs are not on Cloudflare. Of these remaining ASNs, AS 47583 (HOSTINGER) likely only has shared

hosting, as indicated by the white “flame” icon next to the ASN. So, I’ll add the non-Cloudflare, non-Hostinger IP addresses to my project.

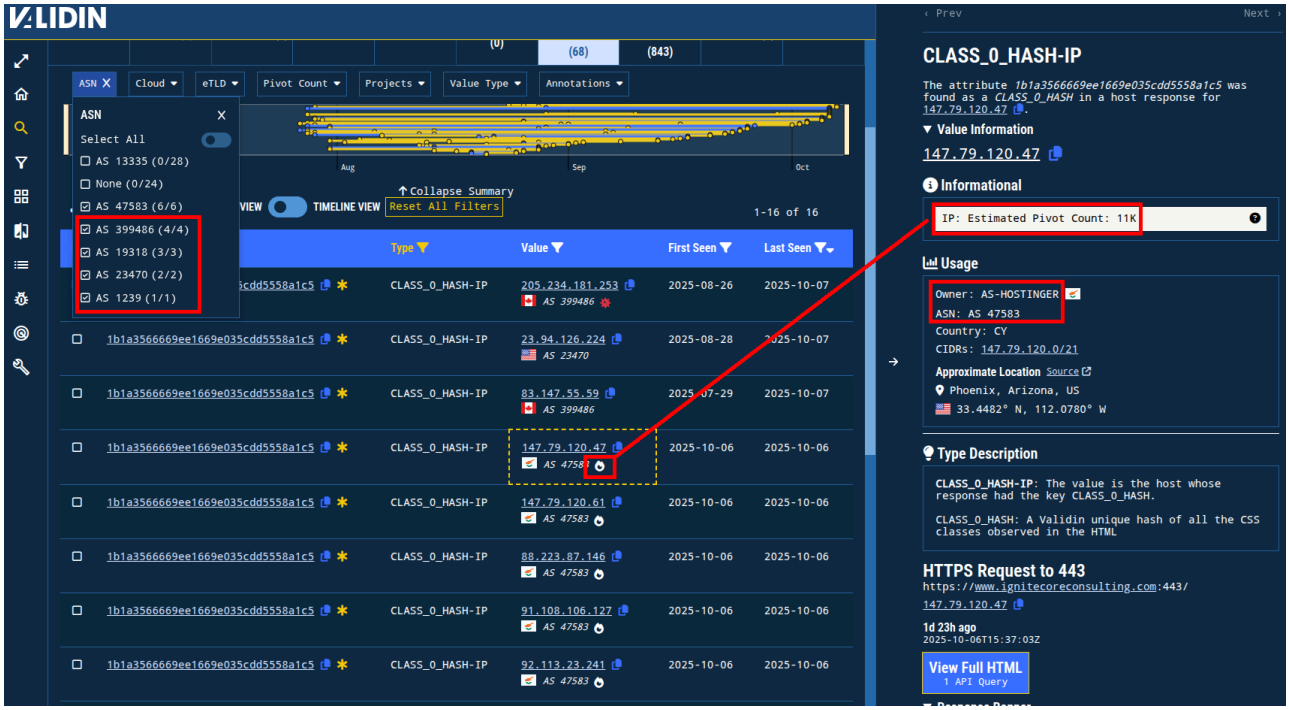


Figure 10. Showing the ASN distribution for the IPs returning the template for this campaign. Note the “popular pivot” icon next to the Hostinger ASNs.

Additional CSS Hash Pivot

The earliest connection to the first CSS class hash, `1b1a3566669ee1669e035cdd5558a1c5`, was in late July 2025. I was curious if any of the domain names had templates that were modified at some point before then and could lead to the discovery of additional domain names, so I started looking at the connection history for the CSS class hashes on all of the domain names.

I found three (3) other domains that had CSS class hashes with identical title tags prior to using the hash `1b1a3566669ee1669e035cdd5558a1c5`:

- `www[.]sparksflyconsult[.]com`
- `rblangconsult[.]com`
- `shamrockconsults[.]com`

These 3 domains all shared a second CSS class hash, `a5b6e03734433ff58dbe3c80f00bcda2`, before changing to `1b1a3566669ee1669e035cdd5558a1c5`. This indicates that the template was modified at some point and replaced with a newer version.

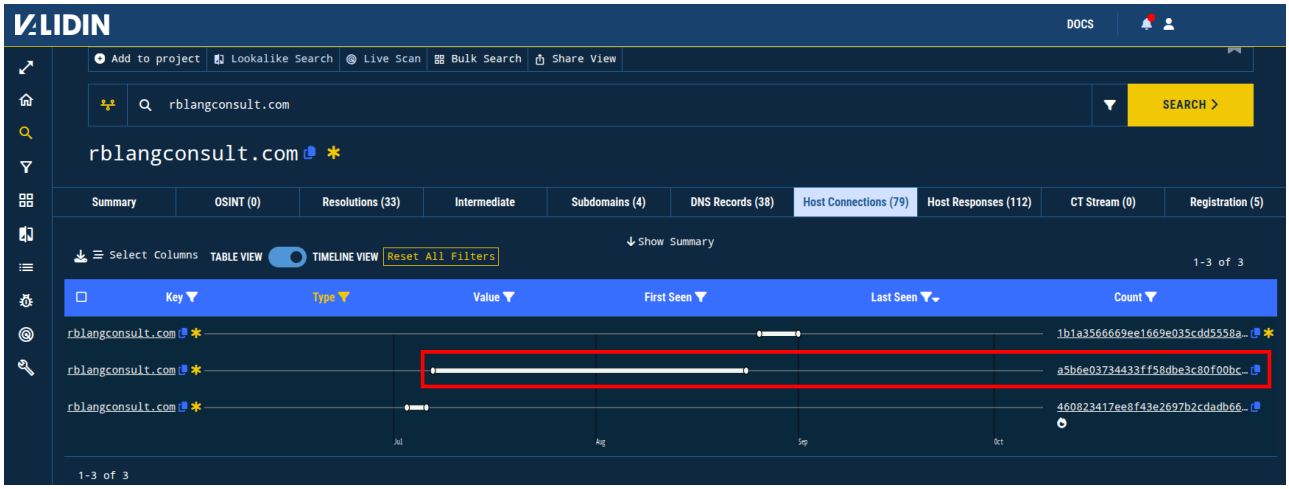


Figure 11. The timeline of the use of another template configuration that resulted in a different CSS class hash.

Pivoting on the CSS class hash `a5b6e03734433ff58dbe3c80f00bcda2`, I observed over 100 distinct domain names that served content matching this hash. This pivot netted a dozen more domain names that had the “consult” or “llc” theme but didn’t also have the CSS class hash already identified, expanding the total number of tracked domain names to 40 (22 apex domains).

Unrelated Domains

Validating candidates and eliminating unrelated domain names is an important part of the threat intelligence gathering process. I suspect that many of the domain names linked by the second CSS class hash (`a5b6e03734433ff58dbe3c80f00bcda2`) are not related due to significant differences in patterns used in the domain name itself. This is highlighted in the figure below.

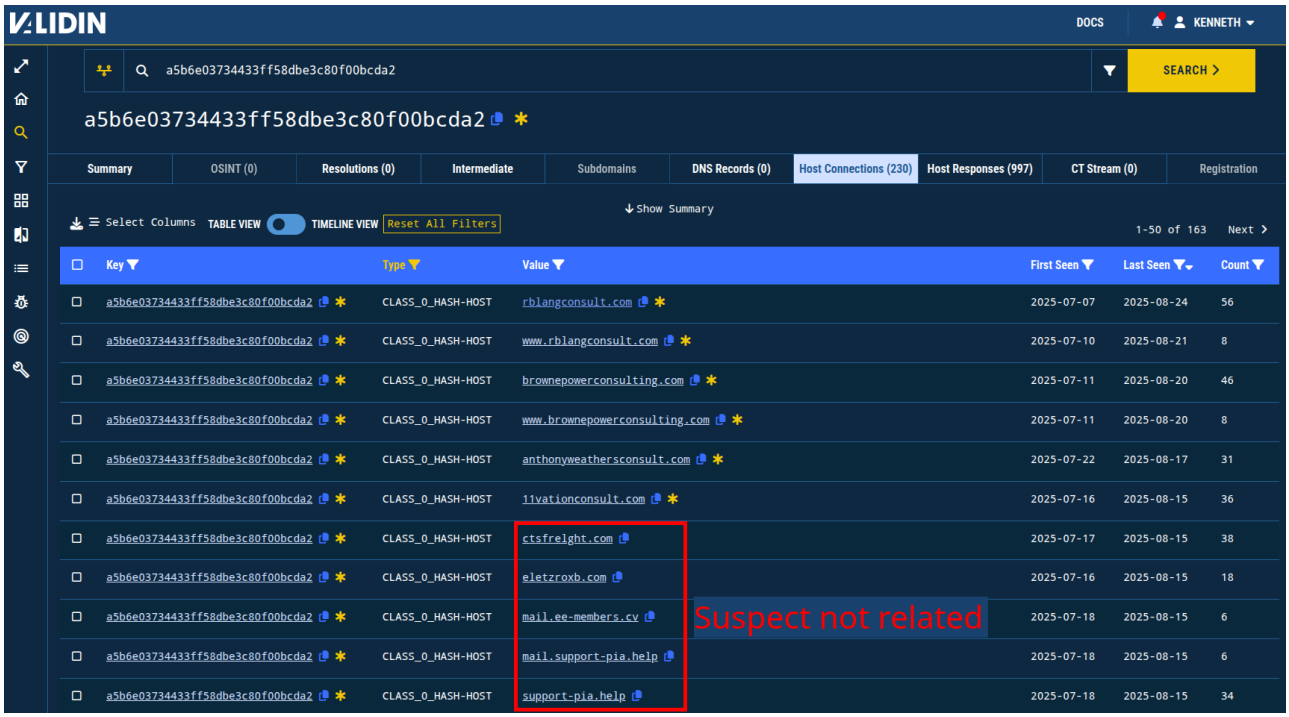


Figure 12. Highlighting domain names that share the CSS class hash attribute but do not have lexicographic similarities to the original set (indicated with a yellow asterisk).

What does this validation process look like?

First, explore the domains currently in our working set to see which non-host response attributes they have in common, including DNS history and registration details.

First observation: most domains are briefly hosted on Hostinger before switching to Cloudflare name servers and IP addresses (and specifically, `paloma[.]ns[.]cloudflare[.]com` and `rob[.]ns[.]cloudflare[.]com`).

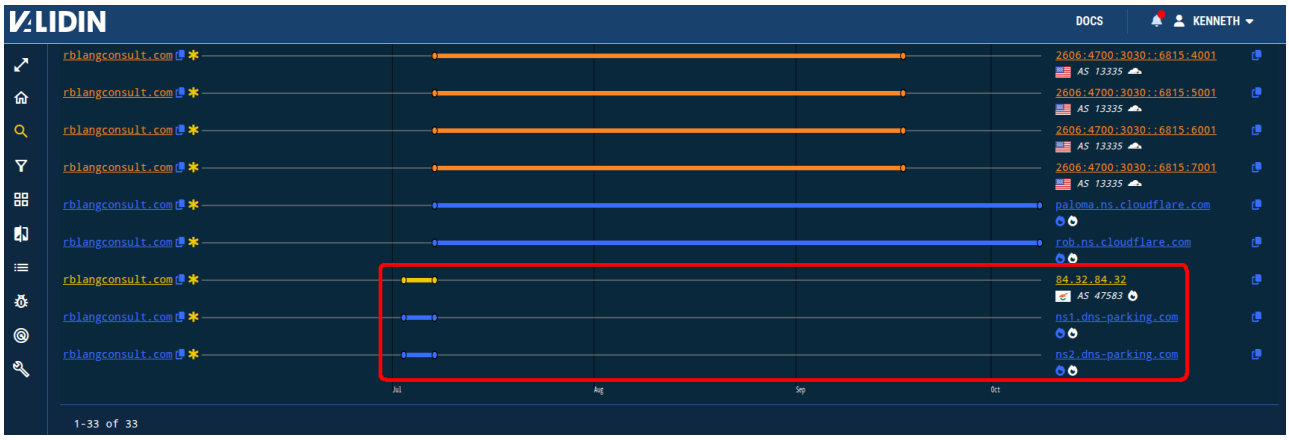


Figure 13. DNS history observations showing the initial use of Hostinger hosting infrastructure quickly followed by a switch to Cloudflare for one of the domains associated with this fraud campaign.

Second observation: most domains are registered with Hostinger, but at least one domain (`anthonyweathersconsult[.]com`) is registered with Tucows instead.

At this point, there are 30 E2LDs associated with the CSS class hash `a5b6e03734433ff58dbe3c80f00bcda2` that I haven't yet confirmed as being part of this cluster of activity. Many of these domains are associated with a specific variant that uses the title tag "GHOUSECOMP LTD | Innovation & Advisory Services". If I exclude every domain that uses this title tag except for `ghousecompltd[.]com`, I'm left with a much smaller set of domains and can quickly add `teamjandm[.]com` as related (associated with title tag "J & M CONSULTS | Innovation & Advisory Services") and eliminate the others.

Cloudflare Shadow

Why do the other "eliminated" domains still return content identical to those that were convicted? I suspect they are a dangling Cloudflare proxy, something the Validin team looked at earlier this year. In this case, these domains may have been configured in Cloudflare to use an origin IP that the domain owners abandoned or lost control over.

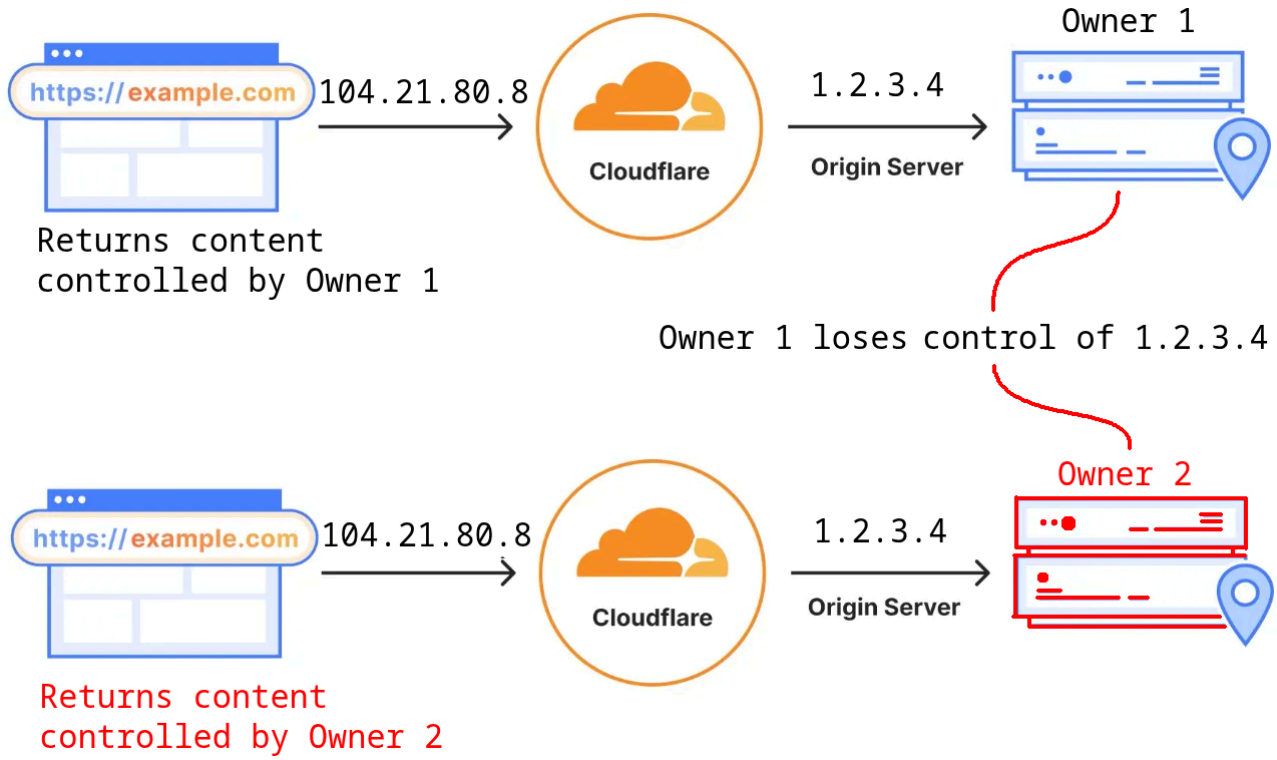


Figure 14. Explanation of “dangling Cloudflare Proxies” as a concept.

Origin IPs

Using Validin’s combination of virtual host responses and direct measurements to individual IP addresses, I can uncover many of the origin IP addresses behind Cloudflare. I can pivot on the unique HTML title tags and HTML hash to find IP addresses returning these values and deduce that these are the IP addresses serving as origin IP addresses behind the Cloudflare proxy.

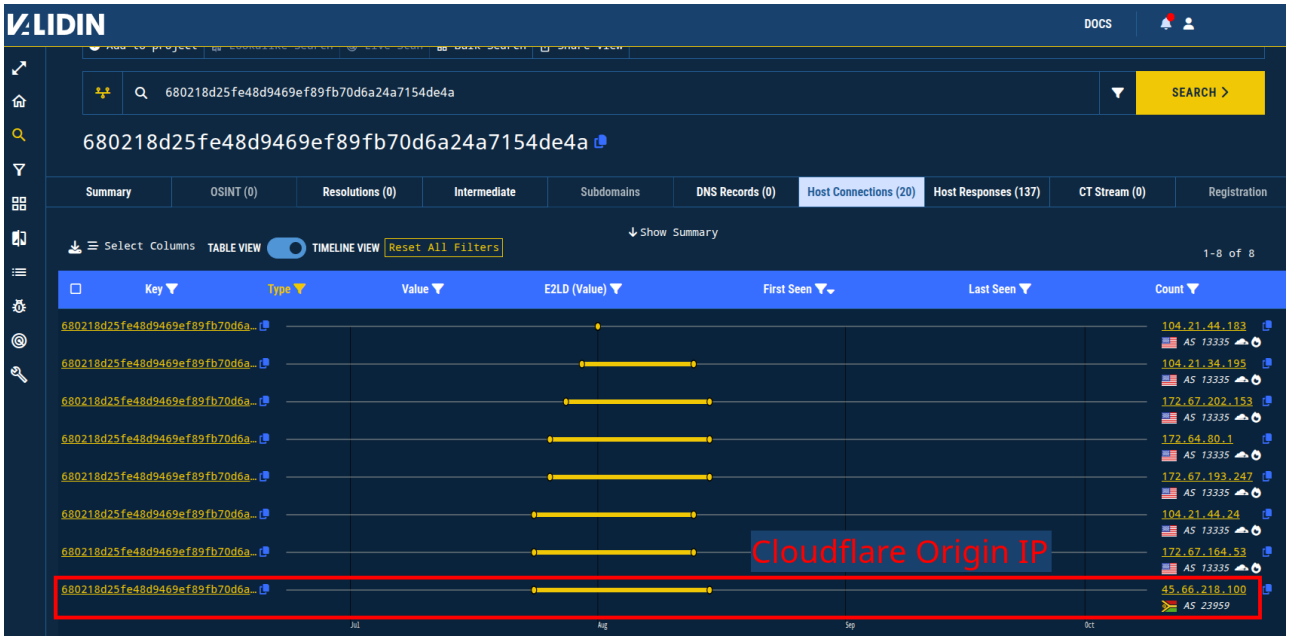


Figure 15. Showing one technique for identifying Cloudflare origin IPs.

Going through the above process, I uncover the following Cloudflare origin IP addresses:

```
107.172.232[.]108
107.172.232[.]107
78.142.229[.]127
146.103.11[.]215
162.244.210[.]60
151.242.58[.]88
45.66.218[.]100
205.234.144[.]59
151.243.254[.]12
50.114.115[.]185
162.244.210[.]104
83.147.53[.]52
23.95.162[.]188
151.243.254[.]131
83.147.55[.]59
23.94.126[.]224
205.234.181[.]253
```

Note: this IP appears to have directly hosted virtual hosts without a Cloudflare proxy: `92.112.189[.]95`

Self-Signed Certificates

The content origin IPs all appear to use a self-signed certificate with the same placeholder values in the Issuer field. In Validin, you can search for certificates with this issuer using this search query:

```
/C=US/ST=New York/L=New York/O=Company Inc/OU=Organization/CN=localhost
```

Here's an example certificate, for with the certificate SHA1 `92d8c45fd06cdd0e23ab07b072a47d65e046c7ab` (SHA256: `2aef3c5058052a97960594e71dec36f2cafc7960bad241b57186df5296ea83c2`), serving content for `elitemindmgmtllc[.]com`:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            37:d9:6f:68:f2:ff:87:59:d9:c8:60:0b:e9:a6:45:14:0a:df:2a:ad
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, ST = New York, L = New York, O = Company Inc, OU =
Organization, CN = localhost
        Validity
```

```
            Not Before: Jun 20 18:21:57 2025 GMT
            Not After : Jun 20 18:21:57 2026 GMT
        Subject: C = US, ST = New York, L = New York, O = Company Inc, OU =
Organization, CN = localhost
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:e9:cc:f8:d7:d1:0d:38:6a:62:1d:aa:56:64:05:
                    7e:1a:49:53:72:33:1c:10:84:81:82:f7:81:ae:fb:
                    05:79:2b:db:cc:29:51:e4:75:f5:d6:c2:c0:20:45:
                    57:84:b7:a6:5b:05:61:c7:9f:fe:6a:23:68:de:2b:
                    62:f8:c0:40:ed:29:7c:b8:85:b2:16:0a:74:5f:38:
                    ad:49:7d:f2:24:93:cd:49:0b:df:d3:49:51:55:cc:
                    2e:10:79:51:6d:3d:41:59:09:b4:bc:06:48:69:89:
                    3c:4d:04:d6:f0:78:94:c6:40:01:dd:1a:53:23:28:
                    9d:13:a1:b7:ff:63:db:a6:13:6d:18:31:46:40:c6:
                    5a:9c:92:de:02:90:09:ac:30:16:ca:8d:cf:de:3e:
                    45:be:6a:98:d2:77:0a:81:0e:2b:46:25:63:e4:72:
                    07:80:0d:8a:73:af:36:18:2e:5f:25:b0:5f:66:ac:
                    75:b0:f7:ec:2a:f5:b3:53:bb:3b:6a:77:70:b3:8d:
                    e2:81:da:02:f9:b2:b1:1a:ee:3d:72:80:ec:3c:62:
                    6f:c0:23:bd:7a:fb:0e:f6:d3:44:d3:fc:f1:62:5c:
                    95:b1:f1:e2:03:d1:89:2d:4e:15:6f:03:34:1e:c3:
                    58:6f:9a:49:82:c9:2f:d5:3d:63:fc:d5:d8:fc:f1:
                    98:3f
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                A9:75:23:81:B7:E4:0C:FF:F2:F6:A8:76:65:D9:B2:18:D0:8A:DE:25
            X509v3 Authority Key Identifier:
                A9:75:23:81:B7:E4:0C:FF:F2:F6:A8:76:65:D9:B2:18:D0:8A:DE:25
            X509v3 Basic Constraints: critical
                CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
    Signature Value:
        77:3a:7d:09:5e:a9:9f:f2:d0:a8:fa:76:a4:dc:12:1d:44:c8:
        07:71:2f:0d:8d:c4:7b:f8:8b:ee:5d:f7:e3:dc:76:d9:67:be:
        e1:08:ba:0f:2b:ed:7a:09:f1:41:b0:d3:9d:1d:a6:a8:1d:8f:
        af:7f:65:3a:9a:a5:dc:99:15:23:04:44:71:06:43:66:4b:ef:
        9a:ad:22:b3:b1:c6:1a:fd:4f:f9:d0:1d:72:5d:3e:0b:89:36:
```

```
        0e:8b:32:d7:46:2e:00:ab:24:b0:e8:b0:4b:bf:b2:49:ea:0c:
        22:bd:e6:0d:68:48:62:68:83:09:9d:38:d9:55:be:a2:8a:e7:
        97:80:b9:d1:af:fd:9b:f2:7b:f9:10:5f:68:ba:bd:cc:f2:49:
        49:54:32:92:56:d4:7f:e3:2b:9c:d9:e4:59:32:2b:ab:b8:ad:
        34:c2:2f:70:68:9b:98:51:76:49:35:fd:20:d0:da:ba:96:e6:
        1d:c8:8d:44:49:b4:49:f8:7c:90:ce:0e:a9:4d:fe:86:53:dd:
        bd:8c:d7:ae:d7:bd:62:b3:2b:ee:f1:d4:aa:42:0f:da:63:9e:
        41:df:d8:98:dd:e3:d1:36:e8:87:ee:09:a6:3c:12:03:60:5e:
        25:c6:94:f4:c0:59:f2:f1:ad:cc:7b:af:10:22:84:59:d8:be:
        14:48:4a:28
```

Unique Servers

The “Server:” header in the origin IP responses advertise very specific apache, OpenSSL, and PHP versions that might be unique enough to be pivotable. Some of the observed server versions include:

```
Apache/2.4.63 (Win64) OpenSSL/3.4.0 PHP/8.2.28
Apache/2.4.63 (Win64) OpenSSL/3.4.0 PHP/8.2.29
Apache/2.4.64 (Win64) OpenSSL/3.5.1 PHP/8.2.29
Apache/2.4.65 (Win64) OpenSSL/3.5.1 PHP/8.2.29
```

Using a few additional filters, I can create a candidate pool for IP addresses to monitor:

- JARM: `2ad2ad16d2ad2ad00042d42d00000061256d32ed7779c14686ad100544dc8d`
- Header Hash: `f400115bf3326edba086`
- Certificate Issuer: `/C=US/ST=New York/L=New York/O=Company Inc/OU=Organization/CN=localhost`

As an advanced search in Validin:

```
server = "Apache/2.4.64 (Win64) OpenSSL/3.5.1 PHP/8.2.29" AND jarm = "2ad2ad16d2ad2ad00042d42d00000061256d32ed7779c14686ad100544dc8d" AND header_hash = "f400115bf3326edba086" AND cert.issuer = "/C=US/ST=New York/L=New York/O=Company Inc/OU=Organization/CN=localhost"
```

Pre-Op Behavior

By tracking the certificate hash, I can pin some inner bounds on when the origin IP addresses were under control by the operator of this campaign. For example, the IP address `78.142.229[.]127` only returned the title tag “ELITEMIND MANAGEMENT LLC | Innovation & Advisory Services” for about 10 days in mid-July. However, the certificate with SHA1 `92d8c45fd06cdd0e23ab07b072a47d65e046c7ab` was used by this IP no later than June 22, 2025, weeks before the placeholder website was configured.

Figure 16. Showing distinct progress of staging and setup phases of the IP address used to host a fake advisory services website.

In that first phase, I observed two IP addresses redirect several popular websites:

- `https[:]//en.wikipedia[.]org/wiki/Main_Page`
- `https[:]//fb[.]com`
- `https[:]//www[.]google[.]com`

There are also potential opportunities to capture more details in the occasional exposed open directory as seen in “Phase 2” above.

Conclusion

Highly targeted scams used to take a lot of resources to pull off convincingly, but the barrier has never been lower for attackers. I built Validin to provide defenders the tools they need to investigate, detect, and proactively block countless varieties of threats on the public internet and the Validin team is dedicated to providing the best possible platform to defenders in service of that core mission.

Ready to elevate your threat hunting, threat attribution, and incident response efforts? Whether you’re an individual analyst or part of a larger enterprise team, Validin offers solutions that meet your needs. Individual users can create a free account and self-upgrade to access more advanced features and data.

Part of a team? Contact us today to explore our enterprise options and discover how Validin can power your organizations with powerful tools and unparalleled data. Let Validin help you work smarter, faster, and more effectively in the fight against cyber threats.

Indicators

```
107.172.232[.]108
107.172.232[.]107
78.142.229[.]127
146.103.11[.]215
162.244.210[.]60
151.242.58[.]88
45.66.218[.]100
92.112.189[.]95
205.234.144[.]59
151.243.254[.]12
50.114.115[.]185
162.244.210[.]104
83.147.53[.]52
23.95.162[.]188
151.243.254[.]131
83.147.55[.]59
23.94.126[.]224
205.234.181[.]253
```

```
johnstonahvec[.]com
betaric[.]com
www[.]betaric[.]com
gsterlingllc[.]com
www[.]gsterlingllc[.]com
jomuellerllc[.]com
elitemindmgmtllc[.]com
www[.]elitemindmgmtllc[.]com
margravllc[.]com
www[.]margravllc[.]com
ignitecoreconsulting[.]com
www[.]ignitecoreconsulting[.]com
brownepowerconsulting[.]com
www[.]brownepowerconsulting[.]com
teamjandm[.]com
djfinances[.]com
www[.]djfinances[.]com
jomuellercons[.]com
www[.]jomuellercons[.]com
shamrockconsults[.]com
```

```
www[.]shamrockconsults[.]com
jandmconsults[.]com
www[.]jandmconsults[.]com
rblangconsult[.]com
www[.]rblangconsult[.]com
jandmconsult[.]com
www[.]jandmconsult[.]com
11vationconsult[.]com
www[.]11vationconsult[.]com
opspectorconsult[.]com
www[.]opspectorconsult[.]com
sassysipsconsult[.]com
www[.]sassysipsconsult[.]com
anthonyweathersconsult[.]com
www[.]anthonyweathersconsult[.]com
sparksflyconsult[.]com
www[.]sparksflyconsult[.]com
centrionmgmt[.]com
www[.]centrionmgmt[.]com
centrionmanagement[.]com
www[.]centrionmanagement[.]com
teamsparksfly[.]com
```