Iranian APT Infrastructure in Focus: Mapping State-Aligned Clusters During Geopolitical Escalation

Published: 2026-03-04 · Archived: 2026-04-29 02:11:16 UTC

Tensions between the United States, Israel, and Iran have reached a critical point following a series of diplomatic breakdowns, which led to escalating military exchanges and proxy engagements across the Middle East. History has shown that when hostilities rise to this degree, cyber operations do not lag far behind kinetic activity. They precede it.

These operations, whether infrastructure reconnaissance, pre-positioning, or network intrusion, are part of the operational groundwork of modern conflict. Disrupting communications and compromising critical systems can weaken response capabilities long before physical engagement begins. Iranian state-aligned actors have historically targeted energy, financial services, government networks, and defense-related organizations across the U.S., Israel, and allied regions.

This post does not attempt to assess the political dimensions of the conflict. Instead, it focuses on infrastructure-level intelligence such as ASN patterns, TLS fingerprints, and hosting clusters derived from Hunt.io. While many indicators originate from public reporting, infrastructure scanning and behavioral clustering can expand them into wider operational patterns.

Understanding these patterns is what enables proactive defense to see the threat coming before it hits. To illustrate how this plays out in real operations, we first examine several Iranian-linked threat actors currently tracked within Hunt.io.

Iranian Threat Actors Currently Tracked in Hunt.io

Hunt.io continuously extracts high-value IOCs such as IP addresses, hosts, and SHA-256 hashes from a wide range of OSINT sources and consolidates them into a single, structured view. 19 threat groups linked to Iran are currently tracked by Hunt.

By normalizing and linking this data at the threat actor level, analysts can quickly pivot between infrastructure, artifacts, and campaigns, reducing the time needed to move from attribution to actionable hunting and detection.

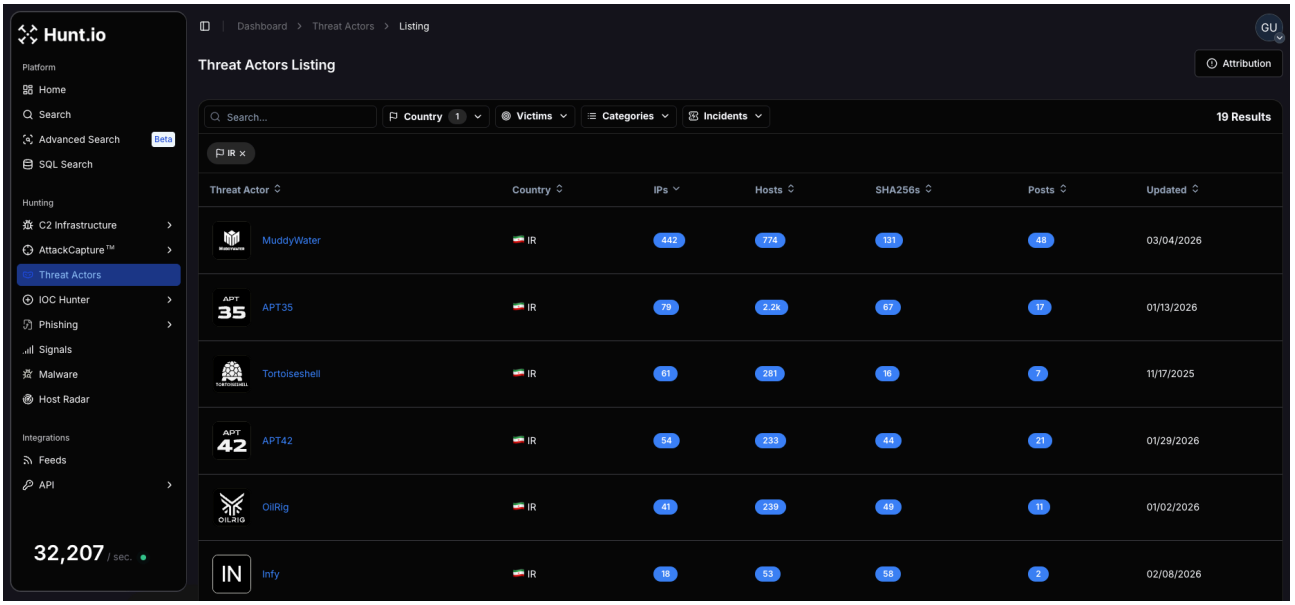

Figure 1: Overview of Iranian threat actor profiles containing IPs, hosts, and sample hashes

These actors represent a mix of state-aligned and hacktivist-motivated operations, with campaigns ranging from espionage and credential harvesting to ransomware and attacks targeting critical infrastructure.

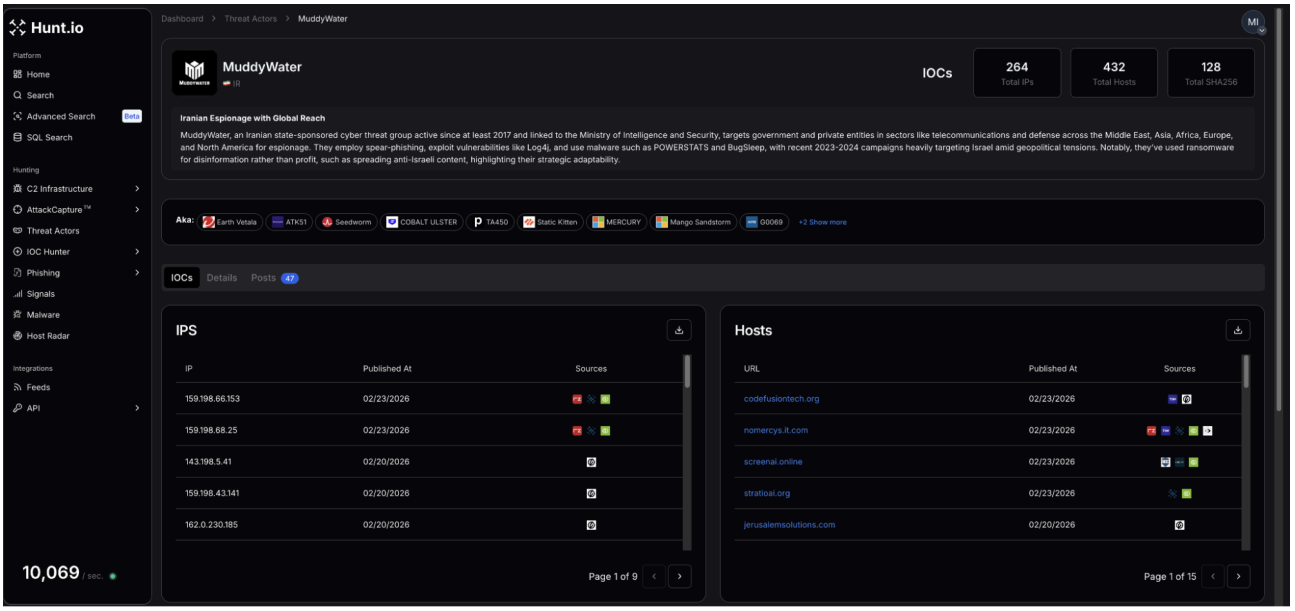

Figure 2: Profile for MuddyWater APT group

Current infrastructure intelligence identifies **264 total IPs**, **432 hosts**, and **128 related SHA-256 hashes** attributed to MuddyWater. Activity observed as recently as the end of January highlighted a persistent campaign targeting organizations in the Middle East and North Africa (MENA). Research also suggested domain reuse dating back to October 2025.

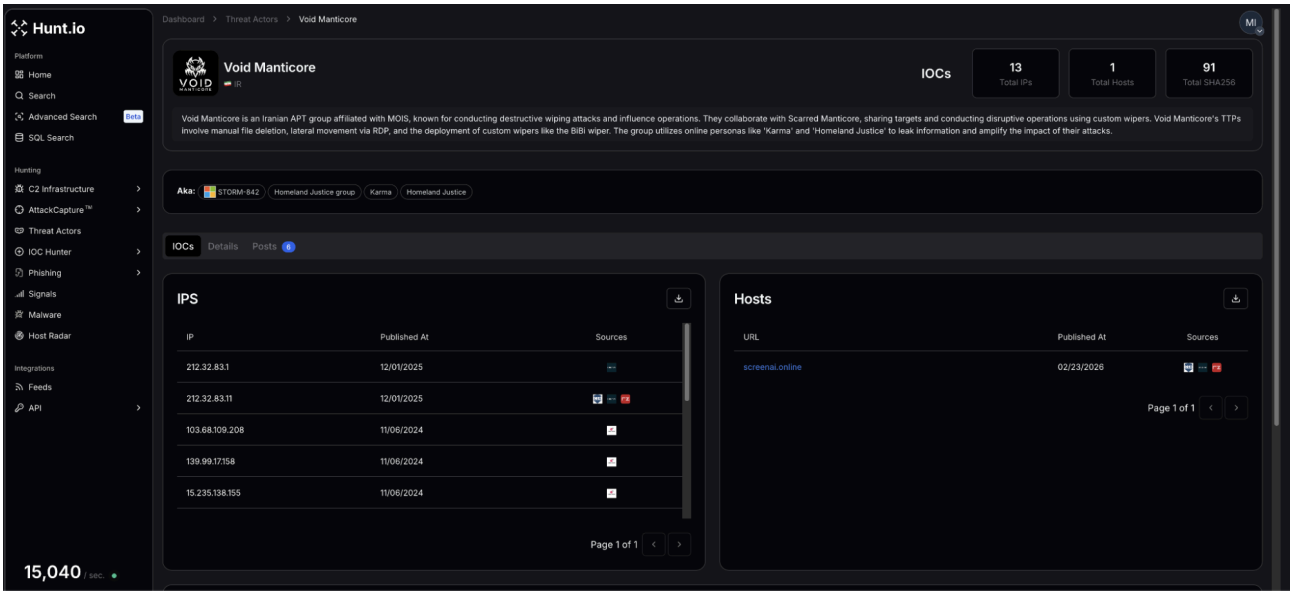

Figure 3: VoidManticore profile showing the most recent IPs and hosts

VoidManticore includes a footprint of **13 tracked IPs**, **1 associated host**, and **91 SHA-256 hashes**. Recent reporting involves the exploitation of an **Omani government mailbox** to facilitate the delivery of malicious Microsoft Word documents focusing on critical infrastructure and government entities worldwide.

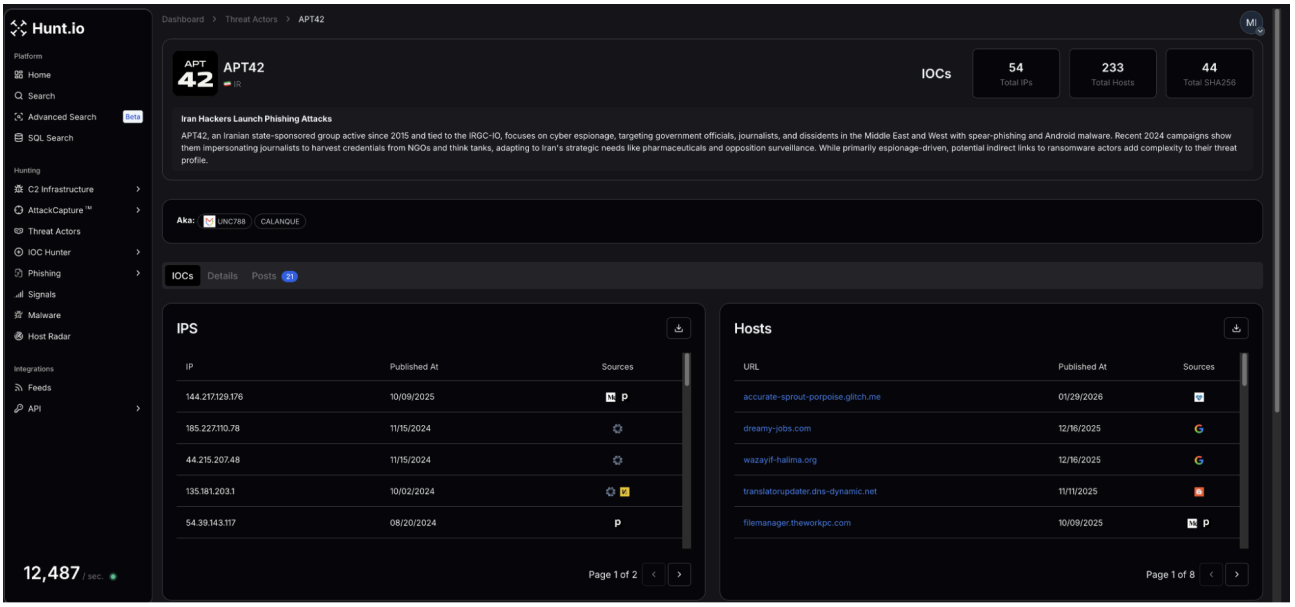

Figure 4: Screenshot of APT42 profile page

APT42, also known as Charming Cypress or Mint Sandstorm, links to **54 IPs**, **233 total hosts**, and **44 SHA-256 hashes**. Analysis of recent campaigns introduces TameCat, a modular, PowerShell-based backdoor used to target **senior defense and government officials**.

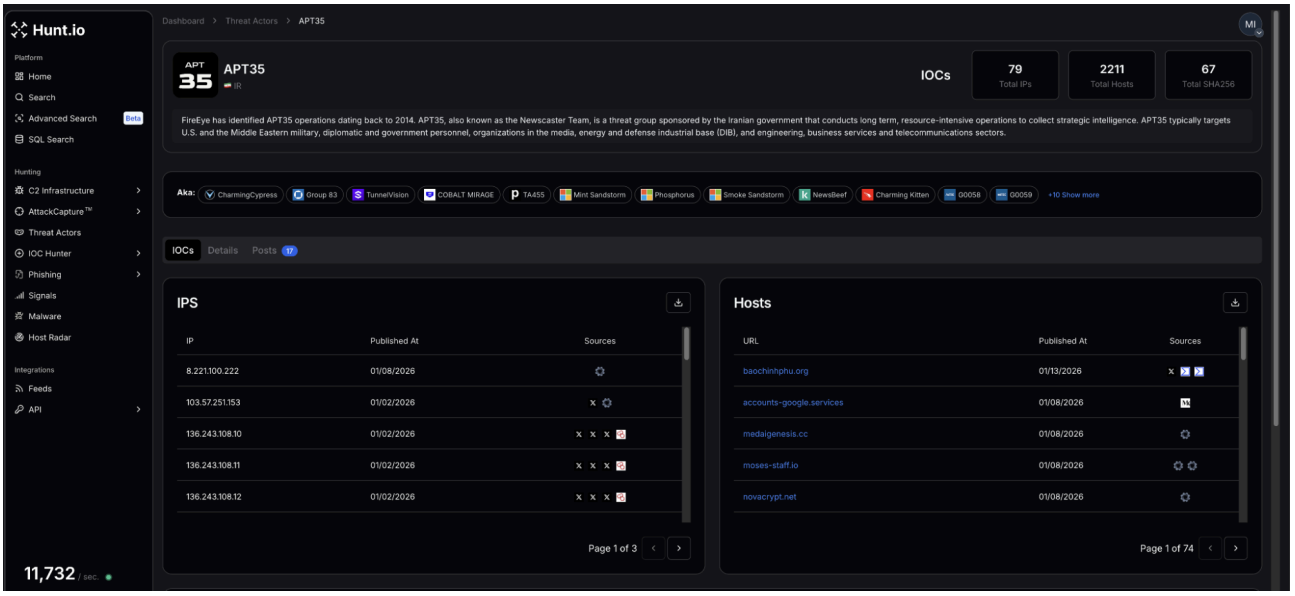

Figure 5: Most recent activity linked to APT35 as identified by Hunt

High-value IOCs revealed **79 IPs**, **2,211 hosts**, and **67 SHA-256 hashes** attributed to APT35. This threat actor has used WhatsApp to distribute spear-phishing messages using spoofed websites to steal the credentials of security and defense-related individuals. In late 2025, a trove of documents and information linked to APT35 was leaked, including C2 infrastructure IPs, usernames, and passwords, and more.

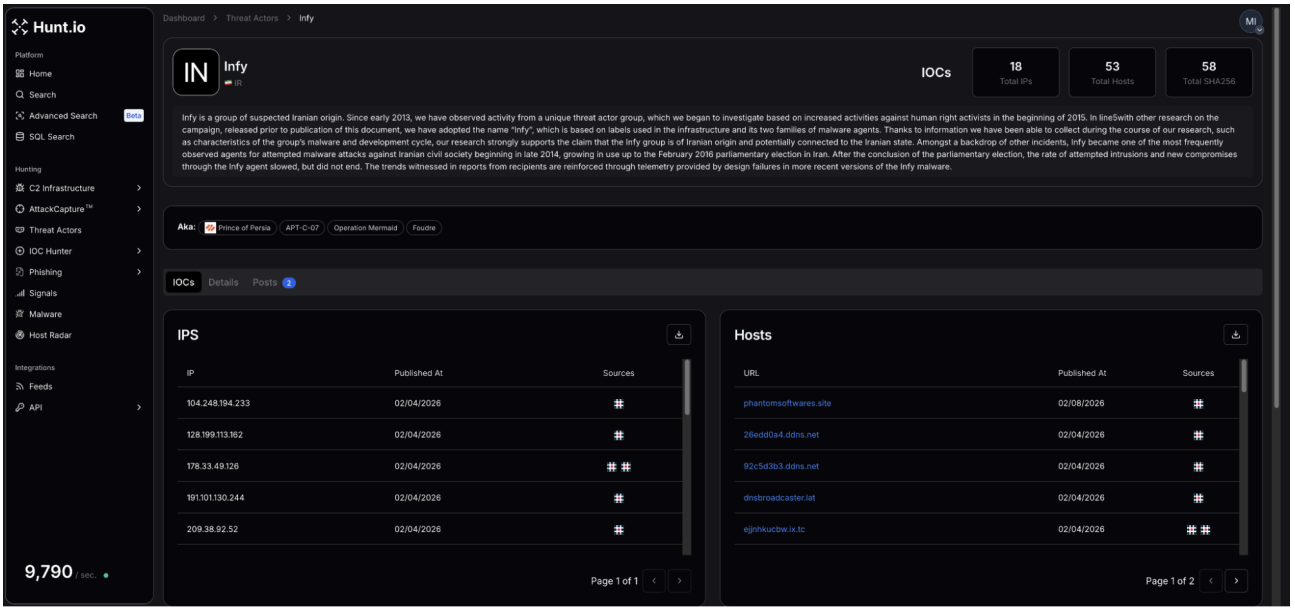

Figure 6: Infy group actor profile page

Infy has a footprint of **18 IPs**, **53 associated hosts**, and **58 SHA-256 hashes**. Following recent campaign shifts, the group has been observed using updated Foudre and Tonnerre variants to target **Iranian dissidents** and **regional government entities**, leveraging Telegram-based C2 to bypass defenses.

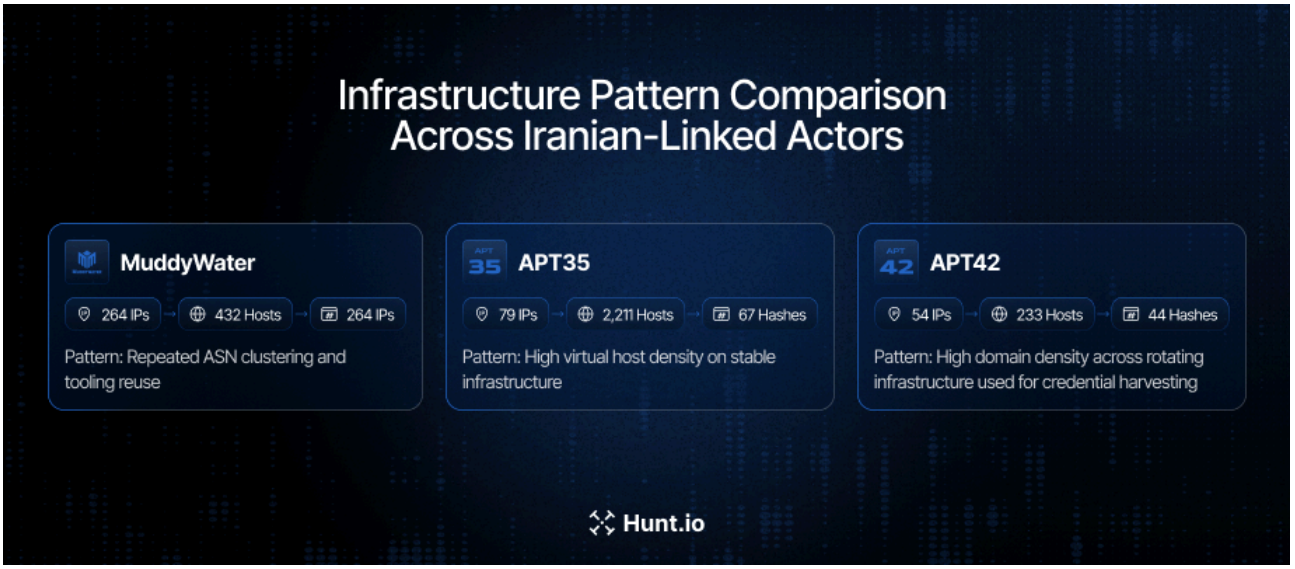

Figure 7: Infrastructure Pattern Comparison Across Iranian-Linked Actors

Infrastructure Patterns Observed

Across intrusion campaigns, network infrastructure is an operational requirement for any threat actor communicating with target systems. While provisioning that infrastructure, actors frequently, sometimes unknowingly, leave behind patterns that defenders can fingerprint and track in real-time.

Clustering on behaviors such as repeated use of specific autonomous systems (AS), hosting providers, certificate authorities, and domain registrars can enable C2/threat group tracking well beyond reported indicators of compromise.

The following examines these patterns as observed through Hunt.io's Attack Capture feature, beginning with a known MuddyWater IP identified in the above threat actor profile page.

Also referred to as Mango Sandstorm, MuddyWater APT, and other Iranian state-linked groups have displayed a preference for including NameCheap and Hosterdaddy Private Limited (AS136557).

Although additional ASNs have appeared in historical reporting, these two providers recur with enough frequency to serve as high-confidence infrastructure clustering pivots. This is particularly valuable when combined with recurring use of offensive tools unique to Iranian APTs like remote monitoring and management (RMM), PowerShell scripts, etc.

Open directory listings are among the highest-value findings in infrastructure hunting. A misconfigured server offers not only an inventory of attacker tooling, but a window into the mindset of how network intrusions are conducted. In Attack Capture, file hashes can be pivoted to find if any other servers are hosting the same file.

Hosted on NameCheap, 209.74.87[.]100 is present in the MuddyWater threat actor profile page on 20 February.

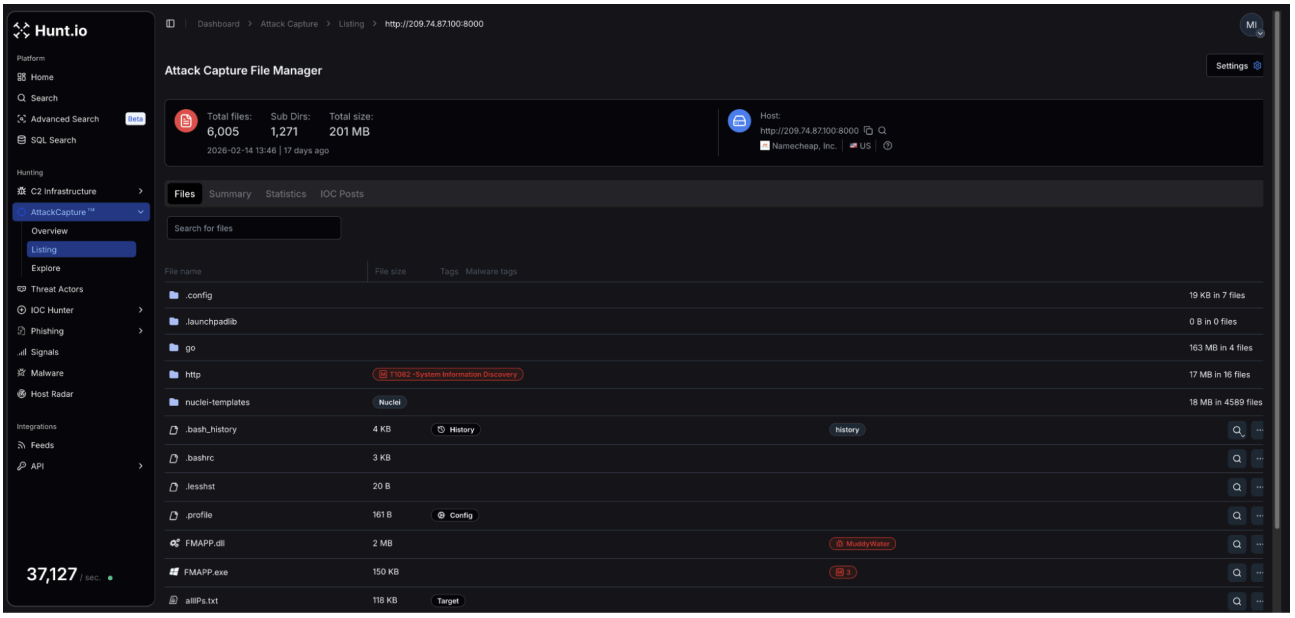

Figure 8: Attack Capture file manager for open directory hosted at 209.74.87[.]100

Among the thousands of exposed artifacts on the server was FMAPP.exe, a proxy binary used as a tunneling component.

Pivoting on the file hash (SHA-256: e25892603c42e34bd7ba0d8ea73be600d898cadc290e3417a82c04d6281b743b) resulted in a single IP not previously reported, [157.20.182[.]49](157.20.182[.]49).

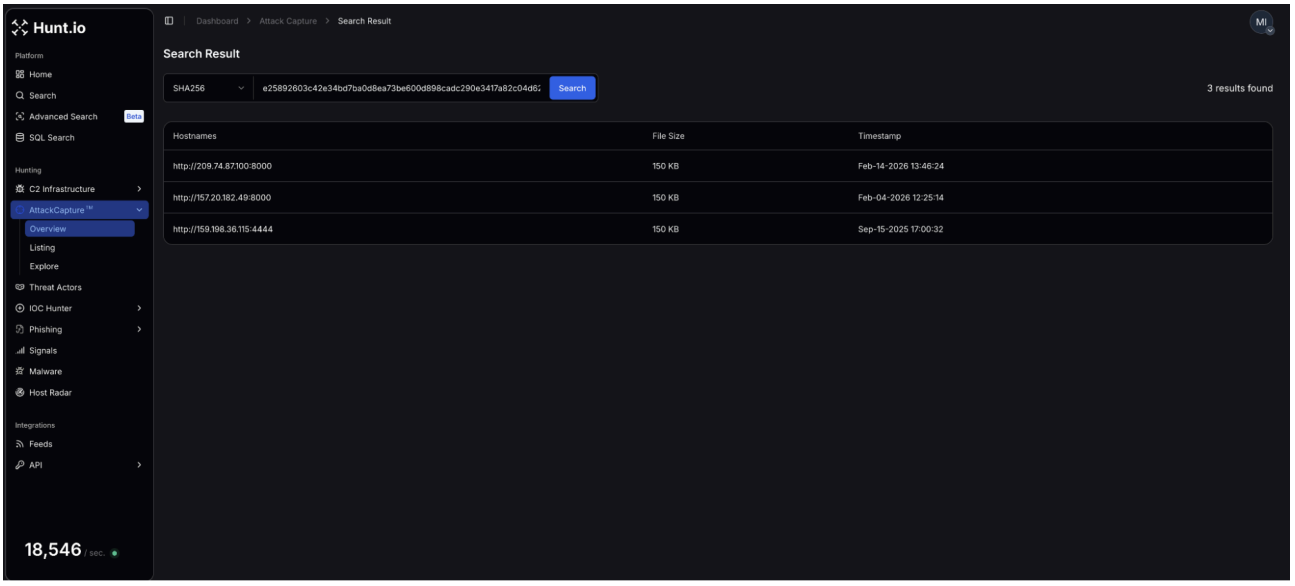

Figure 9: SHA-256 hash pivot result on FMAPP.exe, showing an additional IP

Consistent with MuddyWater's established AS pattern, the above IP is hosted on the Hosterdaddy Private Limited network and is another server within this wider cluster. Similar to the initial directory, many of the exposed files consisted of offensive tooling.

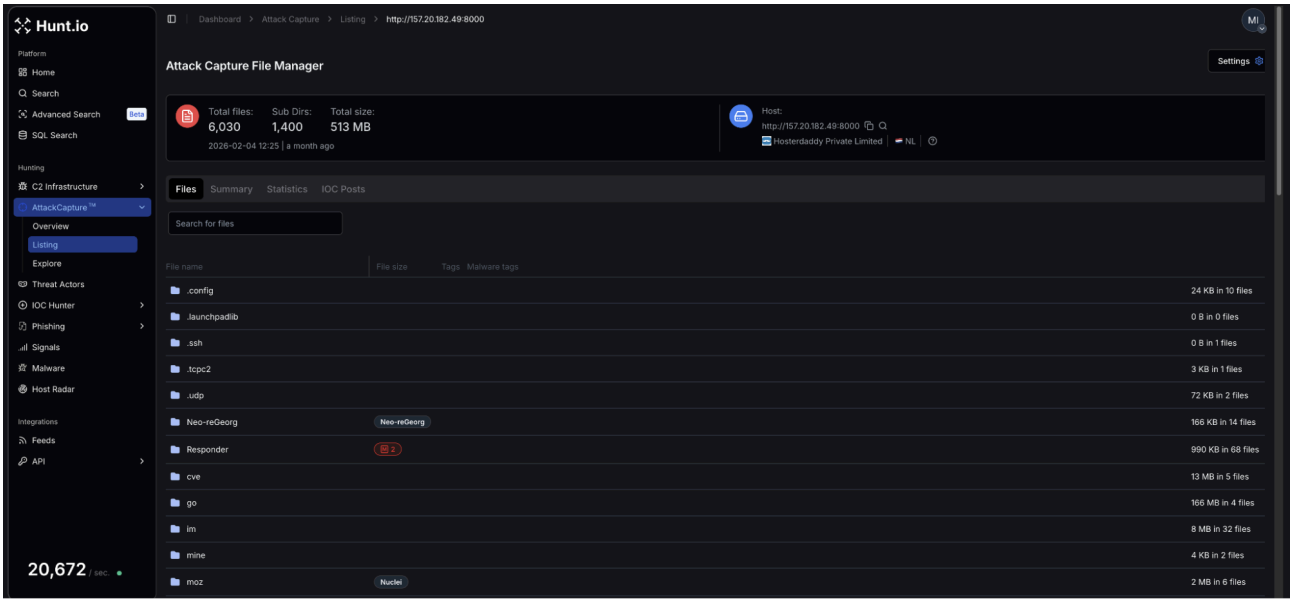

Figure 10: Snippet of the files available for download from 157.20.182[.]49

The directory remained accessible until February 26. Several days later, on March 2, our network scans identified a Sliver C2 server on port 31337. The C2's presence was only captured for a single day. It remains unclear whether MuddyWater is actively operating the Sliver C2 instance, but as the below will explain, it appears the group may be using openly available tooling to blend in with cybercriminals and other actors.

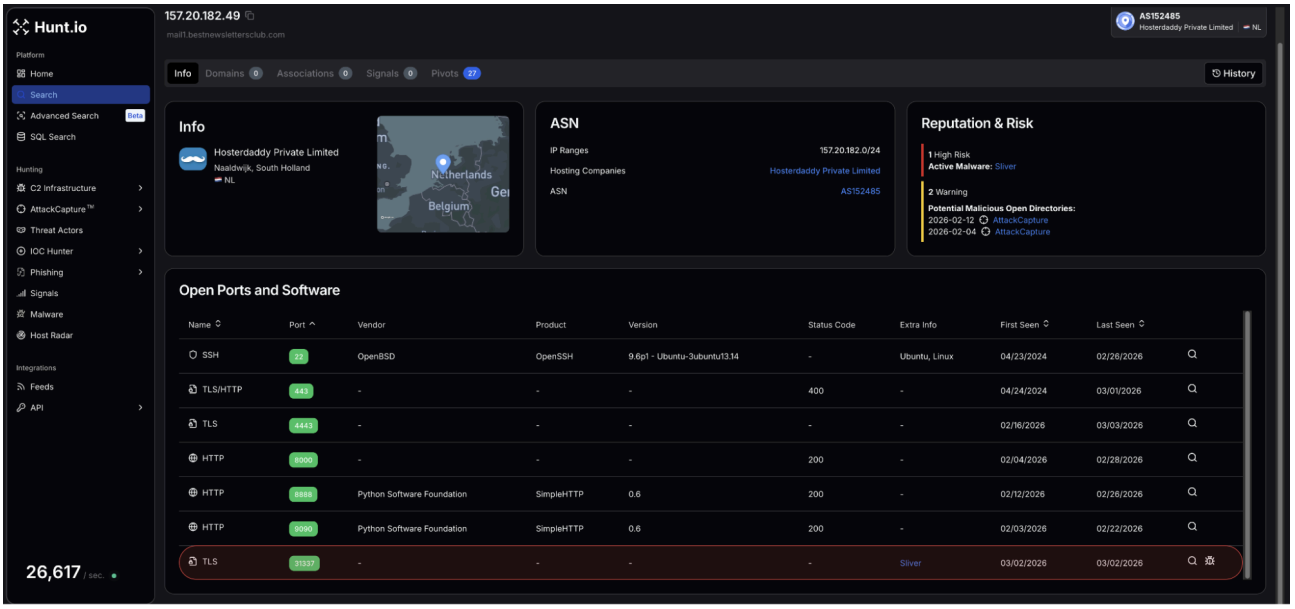

Figure 11: Identification of Sliver C2 on port 31337 on 157.20.182[.]49

Of note, two files from the directory jumped out as interesting/suspicious and required further analysis:

- udp_3.0.py: A custom Python-based UDP command and control server using a lightweight symmetric cipher for communications over port 1269.
- reset.ps1: Multi-stage PowerShell dropper and installer, responsible for downloading JavaScript payloads, including Node.js runtime dependencies.

Particularly interesting was the dropper's explicit dependency on ethers.js and the WebSocket library, indicating Ethereum-based infrastructure as a communications component. Upon execution, reset.ps1 communicates with [185.236.25[.]119:3001](185.236.25[.]119:3001) using websockets. This IP is identified as high risk in Hunt due to login to Tsundere botnet panels on ports 80 and 3000.

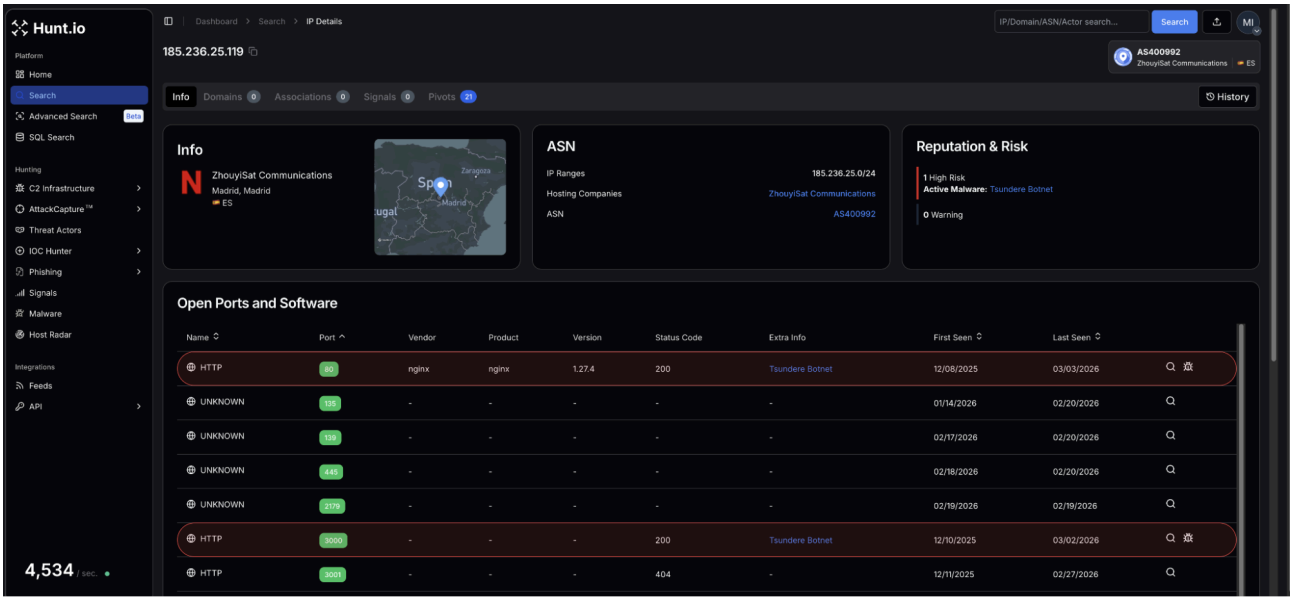

Figure 12: C2 is linked to reset.ps1 is also identified as hosting Tsundere botnet panels

Starting with a single IP address, infrastructure pivoting uncovered two additional servers within the same hosting cluster, including a node potentially leveraging blockchain-related libraries for command-and-control communications.

Additionally, it appears MuddyWater is using publicly available malware likely to blend in with cybercriminals. Target-referenced files related to a UAE engineering company found within the .49 directory further strengthened the assessment of campaign alignment.

This activity is consistent with previously documented MuddyWater infrastructure patterns and overlaps known hosting and tooling behaviors attributed to the group.

How to Track These Actors with Hunt.io

The earlier MuddyWater example demonstrated how pivoting from IP to hash to ASN can expose wider infrastructure clusters tied to an actor. The same clustering logic applies across other Iranian-linked groups.

In this section, we extend that approach using HuntSQL and examine Dark Scepter, a recently identified actor overlapping APT34 (OilRig).

Reviewing C2 domains linked to Dark Scepter showed Cloudflare being used to proxy infrastructure and obscure origin IP addresses. Cloudflare fronting is common among Iranian-aligned operators, which makes certificate Subject Alternative Name (SAN) pivoting especially valuable for revealing backend servers.

While CDN fronting can delay direct attribution, the underlying domain frequently appears as a SAN entry on certificates issued elsewhere. Pivoting on certificate hostnames often exposes the real infrastructure behind the

proxy.

Using the C2 domain web14[.]info as an example, we pivot on certificate hostnames to identify the likely backend server.

Example Query:

```
  SELECT
  ip,
  port,
  hostnames
FROM
  certificates
WHERE
  hostnames RLIKE 'web[0-9]{2}.info[^a-zA-Z0-9.]'
  AND timestamp > '2026-02-01'
group by
  ip,
  port,
  hostnames
```

Copy

Example Output:

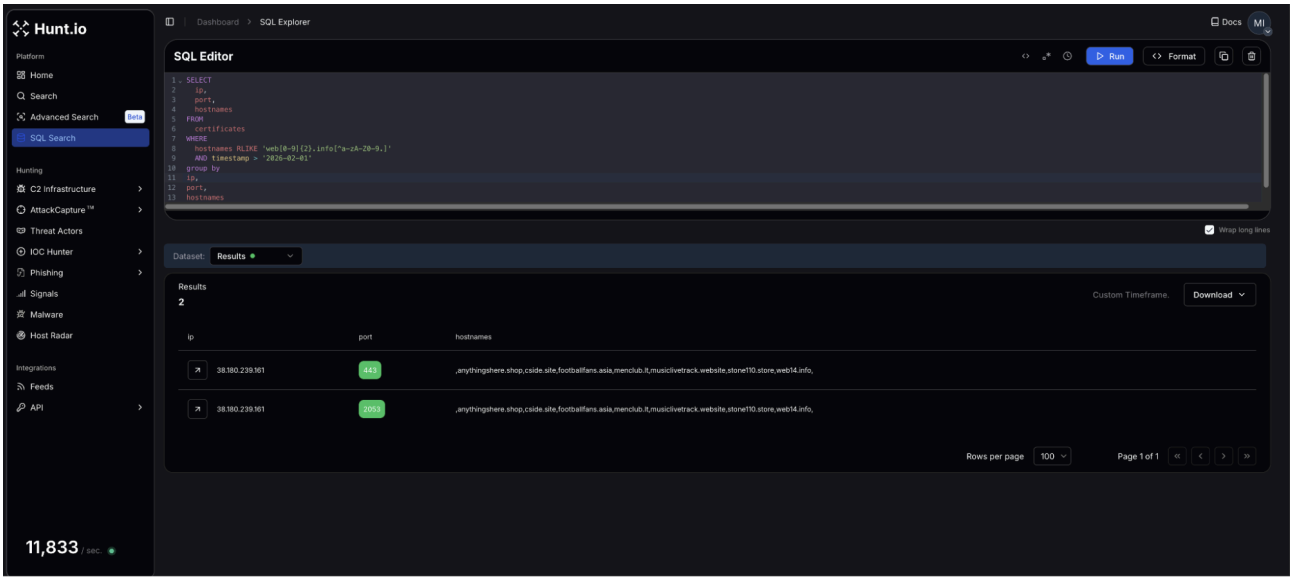

Figure 13: HuntSQL query to locate the real IP used by Dark Scepter

The query, which uses regex to look for all occurrences of web*.info, identifies actor-controlled infrastructure hosted on M247 Europe SRL at 38.180.239[.]161. From the results, we also see several domains listed as hostnames. Some of these domains have previously appeared in public reporting, including Maltrail.

- anythingshere[.]shop
- cside[.]site
- footballfans[.]asia
- menclub[.]lt
- musiclivetrack[.]website
- stone110[.]store
- web14[.]info

A review of the webpage details on 38.180.239[.]161 reveals a unique title, "Wonders Above". To further pivot on these new findings, we can build an additional HuntSQL query to determine how prevalent this title is across the internet and whether it is a solid hunting query.

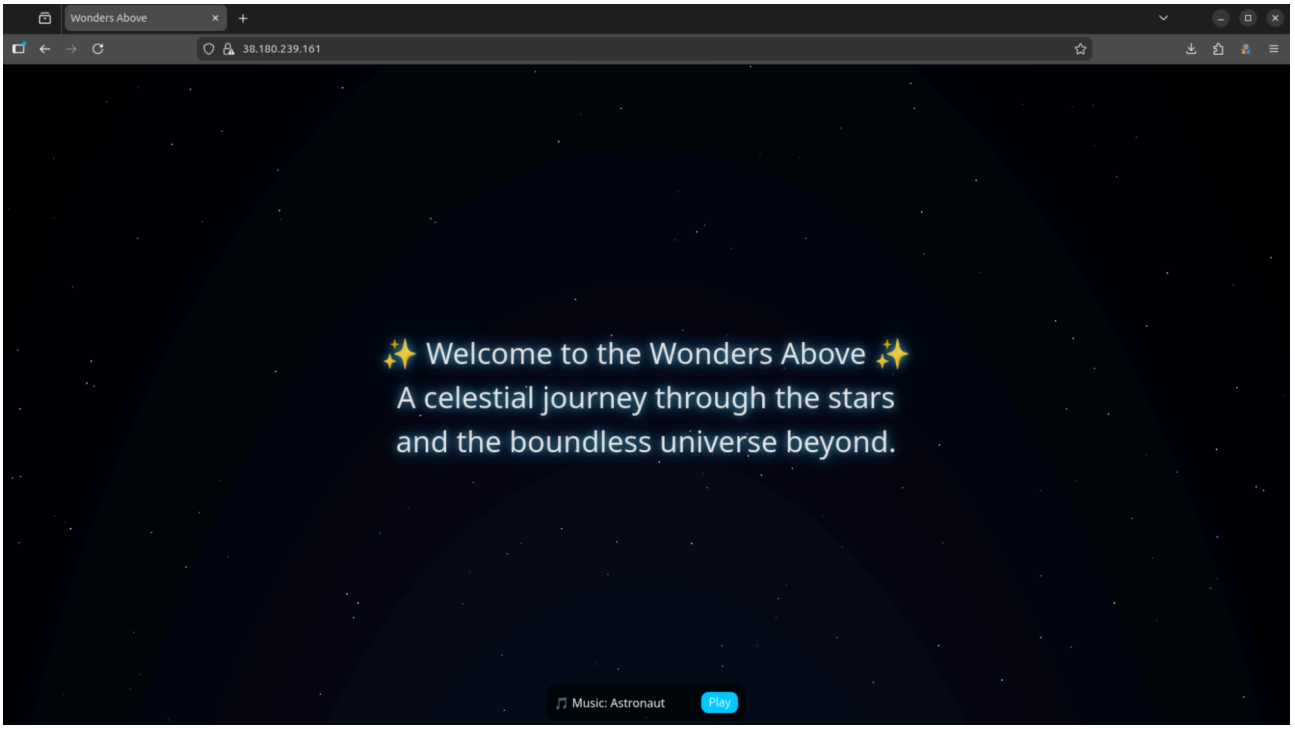

Figure 14: Example webpage when making a GET request to the attacker-controlled IP, 38.180.239[.]161

Example Query:

```
  SELECT
  ip,
  port
FROM
```

```
  httpv2
WHERE
  html.head.title LIKE '%Wonders Above%'
group by
  ip,
  port
```

Copy

Example Output:

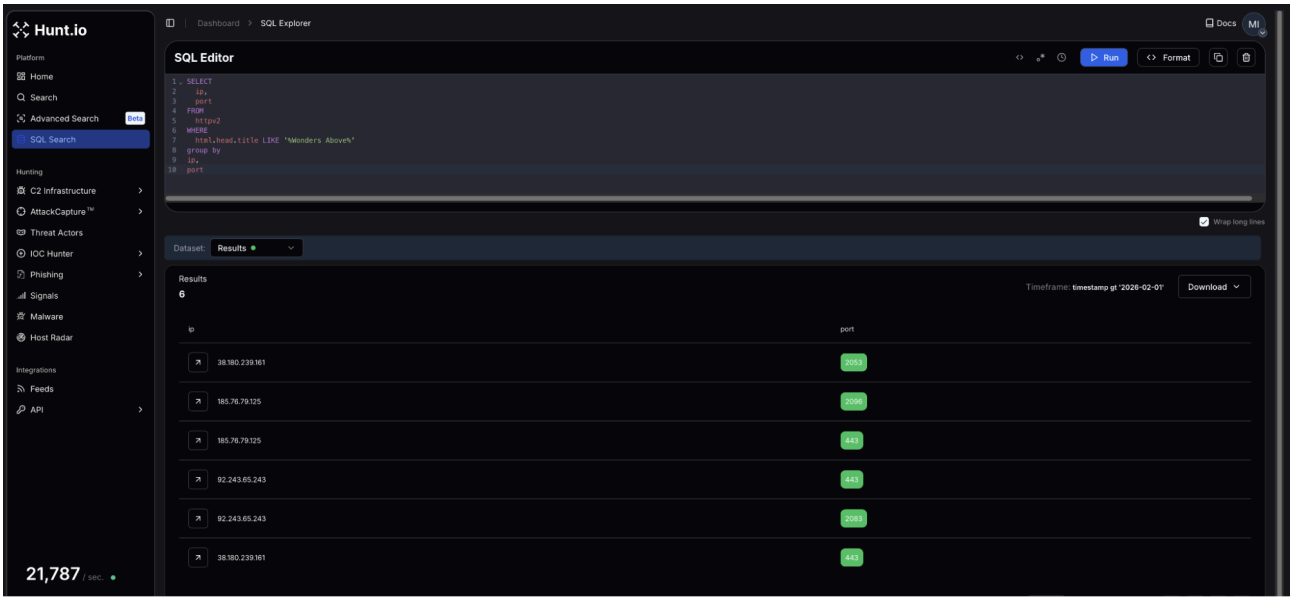

Figure 15: HuntSQL query results for servers hosting the 'Wonders Above' page

The results returned two additional IP addresses using either port 443, 2053, 2083, or 2096, plus the server we started with in the previous query. The new servers share the same webpage and Let's Encrypt certificates with multiple hostnames as seen below:

- 92.243.65[.]243
- 185.76.79[.]125

The virtual servers are hosted on Akton d.o.o. (AS25467), and EDIS GmbH (AS57169), respectively. Observed domain names: justweb[.]click, girlsbags[.]shop, lecturegenieltd[.]pro, ntcx[.]pro, and retseptik[.]info.

Pivoting on reused webpages and certificate hostnames is a reliable way to track not only Dark Scepter and other Iranian groups, but a majority of threat actors who think simply moving their C2 infrastructure behind Cloudflare will deter defenders.

What U.S. and Israeli Organizations Should Monitor

Iranian state-linked actors have consistently targeted organizations aligned with national intelligence priorities and those deemed as a threat. For U.S. and Israeli entities, the sectors of greatest exposure are government agencies, defense contractors, energy and utilities operators, university and policy institutions, and financial services.

Monitoring Recommendations

Defenders should prioritize monitoring the following:

- VPN and remote access appliances: Monitor for anomalous geolocation shifts, ASN changes, and authentication attempts tied to high-risk hosting networks.
- Suspicious emails: Enforce MFA across all users and monitor for OAuth abuse, token replay, and credential harvesting patterns.
- Spoofed domains: Continuously scan for typosquatting domains and certificate reuse tied to defense, energy, and government keywords.
- ASN-based monitoring: Track infrastructure originating from repeatedly observed Iranian-linked ASNs such as Hosterdaddy Private Limited (AS136557).
- TLS fingerprinting: Leverage JARM and JA4x fingerprint clustering within HuntSQL to detect backend infrastructure reuse behind CDN proxies.

Indicators of Compromise (IOCs)

The infrastructure uncovered throughout this investigation reveals several previously unreported hosts, domains, and servers linked to Iranian-aligned operations.

The indicators below represent a subset of the infrastructure identified during this analysis. Additional indicators and actor infrastructure can be explored directly through Hunt.io threat actor profiles.

IP addresses	Details
209.74.87[.]100	Open directory IP found in MuddyWater threat actor profile
157.20.182[.]49	Additional IP/open directory sharing the same file (FMAPP.exe) as 209.74.87[.]100
185.236.25[.]119	C2 for reset.ps1, a PowerShell loader found in 157.20.182[.]49
38.180.239[.]161	Attacker-controlled IP linked to Dark Scepter hidden behind Cloudflare
92.243.65[.]243	Secondary IP linked to 38.180.239[.]161 when pivoting on web page titles.
185.76.79[.]125	Tertiary IP linked to the two above sharing the same web titles and TLS certificates

Domains	Details
anythingshere[.]shop	Dark Scepter C2 domain
cside[.]site	Dark Scepter C2 domain
footballfans[.]asia	Dark Scepter C2 domain
menclub[.]lt	Dark Scepter C2 domain
musiclivetrack[.]website	Dark Scepter C2 domain
stone110[.]store	Dark Scepter C2 domain
web14[.]info	Initial C2 domain linked to Dark Scepter
justweb[.]click	Dark Scepter C2 domain
girlsbags[.]shop	Dark Scepter C2 domain
lecturegenieltd[.]pro	Dark Scepter C2 domain
ntcx[.]pro	Dark Scepter C2 domain
retseptik[.]info	Dark Scepter C2 domain

Conclusion

Network intrusions rarely begin with exploitation. They begin with infrastructure provisioning, staging, and reconnaissance that often occurs weeks before any direct interaction with a target. The indicators documented in this assessment surfaced through proactive infrastructure clustering and behavioral pivoting, not reactive post-incident reporting.

Once an IP address or domain becomes widely published, operators have typically already rotated infrastructure. Monitoring ASN patterns, certificate reuse, hosting clusters, and hash overlaps shifts detection earlier in the intrusion lifecycle, where disruption is still possible. Infrastructure intelligence is not about reacting faster. It is about seeing earlier.

If your organization, industry, or national infrastructure is exposed to these types of campaigns, Hunt.io can help you identify and track the infrastructure behind them.

Get in touch with our team to learn how Hunt.io supports proactive threat hunting and infrastructure monitoring.
