Alexander Ticket

Note: This report has been sanitized for public sharing.

All internal IPs, hostnames, and Splunk URLs have been redacted or replaced with simulated values.

Report was originally prepared for Jira; internal console links are not publicly accessible. Query references shown for context

QRadar ID: 55292

Description

ET WEB_SERVER Likely Malicious Request for `/proc/self/environ` — probe attempting to read process environment (possible LFI/CGI abuse or reconnaissance for environment disclosure)

Victim:

[internal web server] - redacted-domain.local

* Encoded log:*

"\/@fs\/proc\/self\/environ?raw??"

* Decoded log:*

"/@fs/proc/self/environ?raw??"

ATTACKER INFO:

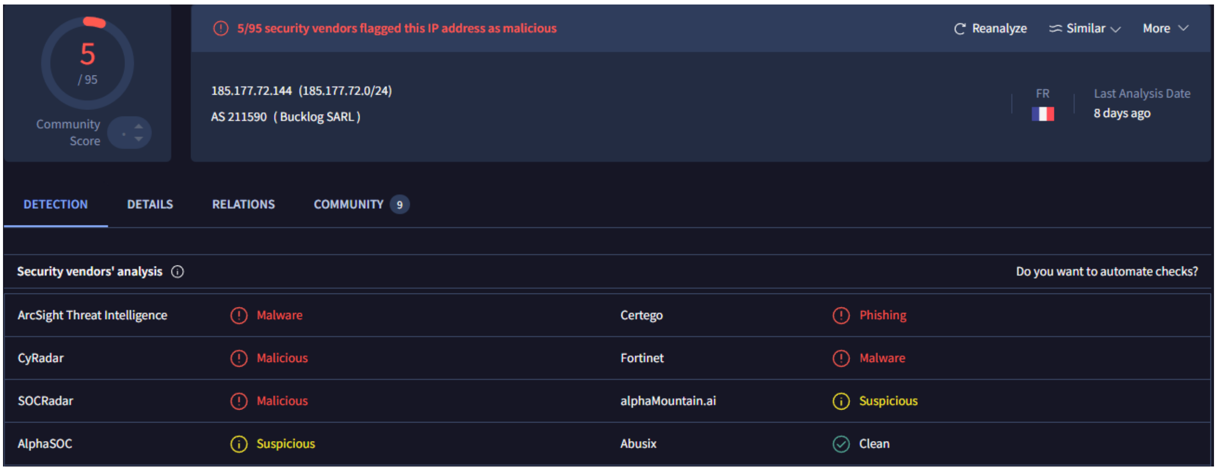
IP: `185.177.72.144` on port `59706`

User Agent: "`"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36"` — this string matches a desktop Chrome 91 on Windows 10, but User-Agent headers are trivially spoofable. Treat this UA as **not** proof of a human browser; automated scanners and exploit tools commonly impersonate popular browsers to blend in "

ANALYST INVESTIGATION:

Virus Total Result: **[here|https://www.virustotal.com/gui/ip-address/185.177.72.144]**

Security Vendors' Analysis from Virus Total: **5/95 security vendors flagged this IP address as malicious and 2 flagged as suspicious**



5/95 security vendors flagged this IP address as malicious

185.177.72.144 (185.177.72.0/24)
AS 211590 (Bucklog SARL)

FR

Last Analysis Date
8 days ago

Security vendors' analysis

Do you want to automate checks?

ArcSight Threat Intelligence	Malware	Certego	Phishing
CyRadar	Malicious	Fortinet	Malware
SOCRadar	Malicious	alphaMountain.ai	Suspicious
AlphaSOC	Suspicious	Abusix	Clean

Talos Intelligence:

REPUTATION DETAILS:

Email Reputation: *Poor*

Web Reputation: *Questionable*

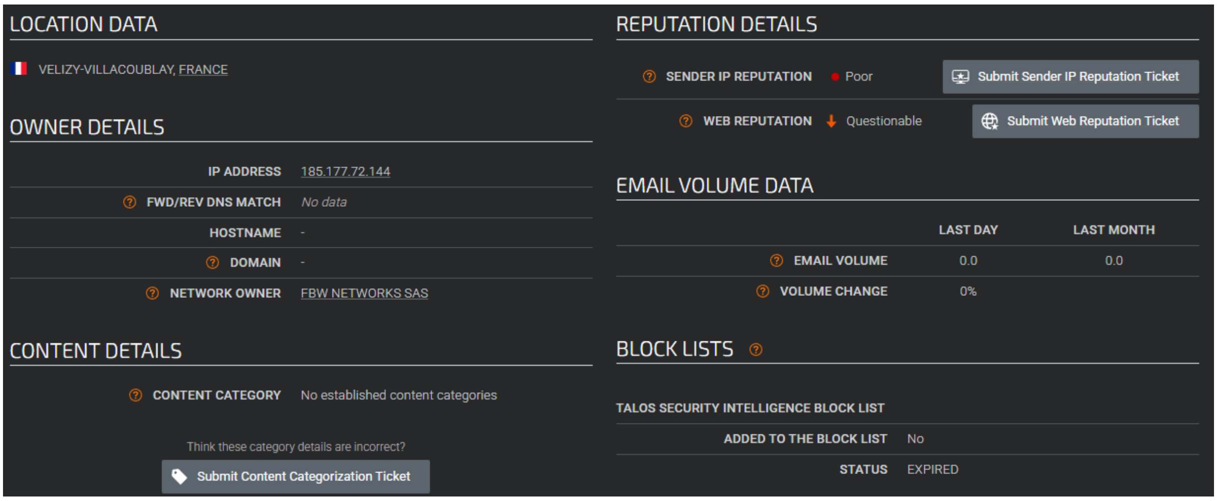
BLOCK LISTS:

Talos Security Intelligence Block List

Added to the Block List = No

Status = EXPIRED

Talos Result:
[here|https://talosintelligence.com/reputation_center/lookup?search=185.177.72.144]



LOCATION DATA

VELIZY-VILLACOUBLAY, FRANCE

OWNER DETAILS

IP ADDRESS	185.177.72.144
FWD/REV DNS MATCH	No data
HOSTNAME	-
DOMAIN	-
NETWORK OWNER	FBW NETWORKS SAS

CONTENT DETAILS

CONTENT CATEGORY	No established content categories

Think these category details are incorrect?

Submit Content Categorization Ticket

REPUTATION DETAILS

SENDER IP REPUTATION	● Poor
WEB REPUTATION	↓ Questionable

Submit Sender IP Reputation Ticket
Submit Web Reputation Ticket

EMAIL VOLUME DATA

	LAST DAY	LAST MONTH
EMAIL VOLUME	0.0	0.0
VOLUME CHANGE	0%	

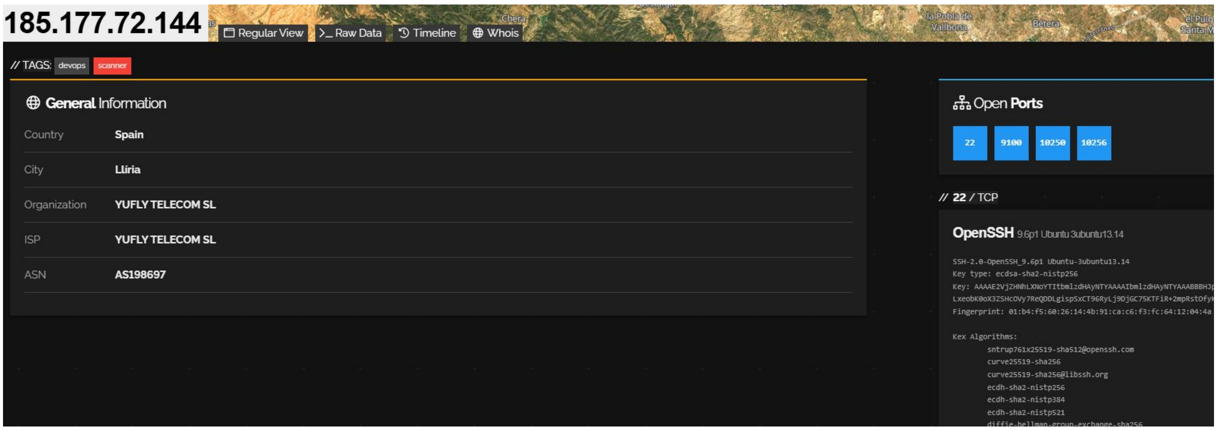
BLOCK LISTS

TALOS SECURITY INTELLIGENCE BLOCK LIST

ADDED TO THE BLOCK LIST	No
STATUS	EXPIRED

ShodanResult: [here|https://www.shodan.io/host/185.177.72.144]

Open Ports: 22, 9100, 10250, 10256



185.177.72.144

// TAGS: devops scanner

General Information

Country	Spain
City	Llíria
Organization	YUFLY TELECOM SL
ISP	YUFLY TELECOM SL
ASN	AS198697

Open Ports

22 9100 10250 10256

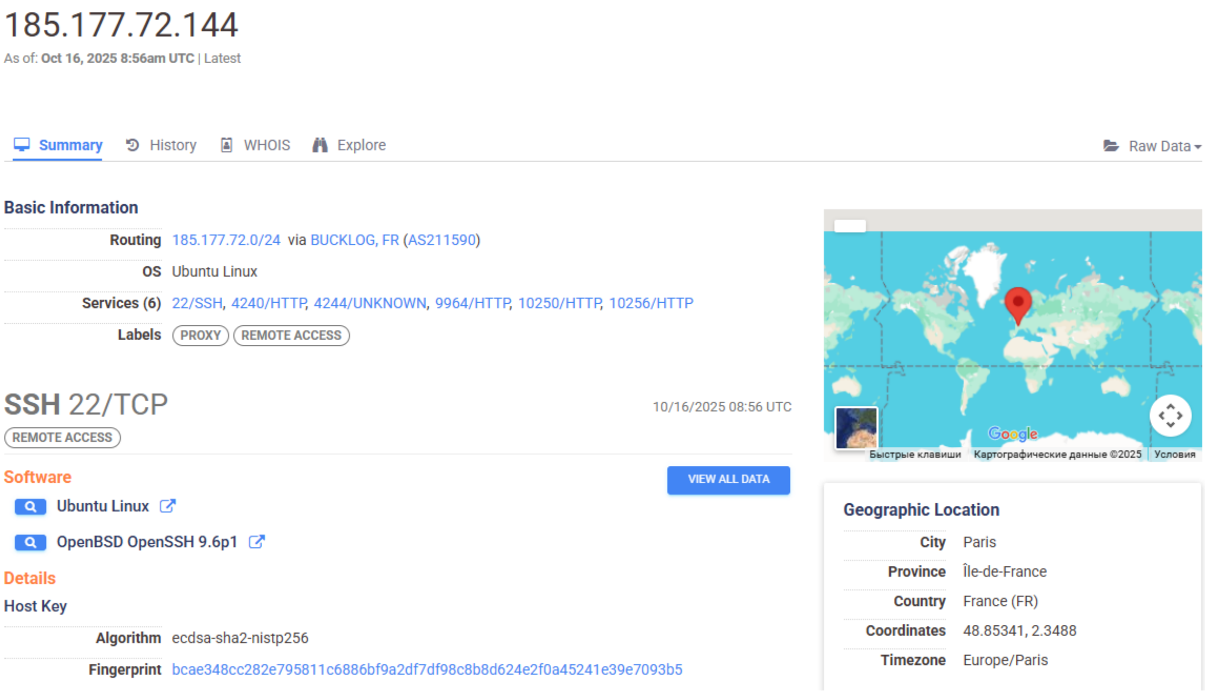
// 22 / TCP

OpenSSH 9.6p1 Ubuntu 3ubuntu13.14

```
SSH-2.0-OpenSSH_9.6p1 Ubuntu-3ubuntu13.14
Key type: ecdsa-sha2-nistp256
Key: AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBHJp
LxeobK0oX3ZSHcOVy7ReQDDLgispSxCT96RyLj9DjGC75KTFiR+2mpRstOfy
Fingerprint: 01:b4:f5:60:26:14:4b:91:ca:c6:f3:fc:64:12:04:4a

Kex Algorithms:
        sntrup761x25519-sha512@openssh.com
        curve25519-sha256
        curve25519-sha256@libssh.org
        ecdh-sha2-nistp256
        ecdh-sha2-nistp384
        ecdh-sha2-nistp521
        diffie-hellman-group-exchange-sha256
```

CensysResult: **[here|https://search.censys.io/hosts/185.177.72.144]**



185.177.72.144

As of: **Oct 16, 2025 8:56am UTC** | Latest

Basic Information

Routing	185.177.72.0/24 via BUCKLOG, FR (AS211590)
OS	Ubuntu Linux
Services (6)	22/SSH, 4240/HTTP, 4244/UNKNOWN, 9964/HTTP, 10250/HTTP, 10256/HTTP
Labels	PROXY REMOTE ACCESS

SSH 22/TCP

10/16/2025 08:56 UTC

REMOTE ACCESS

Software

Ubuntu Linux

OpenBSD OpenSSH 9.6p1

Details

Host Key

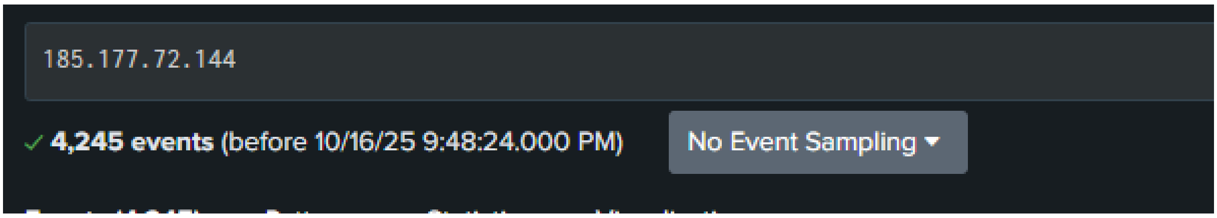
Algorithm	ecdsa-sha2-nistp256
Fingerprint	bcae348cc282e795811c6886bf9a2df7df98c8b8d624e2f0a45241e39e7093b5

Geographic Location

City	Paris
Province	Île-de-France
Country	France (FR)
Coordinates	48.85341, 2.3488
Timezone	Europe/Paris

*Splunk Investigation:*A total of **4,245 events** were identified for source IP **185.177.72.144**.

After applying the key URI filter `/@fs/proc/self/environ?raw?`, the dataset was reduced to **3 events**, all returning **HTTP 403 (Forbidden)** responses — indicating the access attempts were blocked

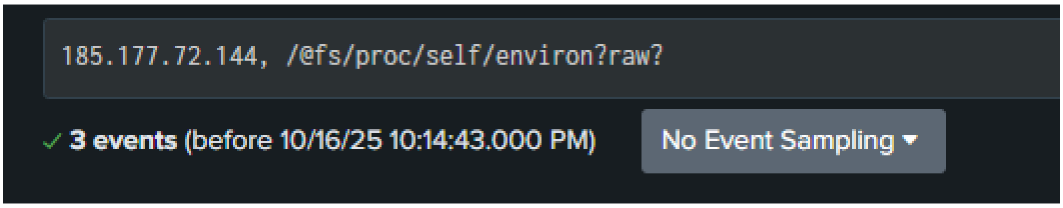


```
185.177.72.144
```

✓ **4,245 events** (before 10/16/25 9:48:24.000 PM)

↑ ↑ ↑

Result 1: Splunk search — internal link (not accessible)

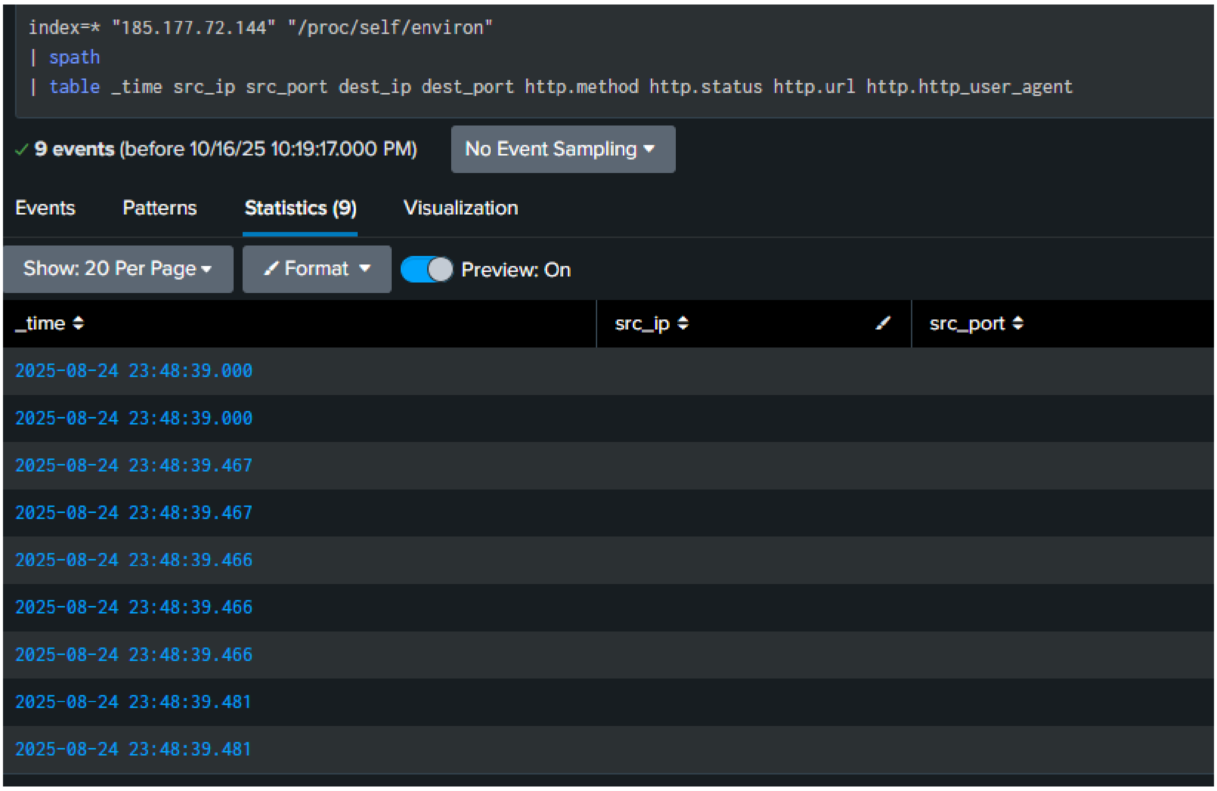


```
185.177.72.144, /@fs/proc/self/environ?raw?
```

✓ **3 events** (before 10/16/25 10:14:43.000 PM)

↑ ↑ ↑

Result 2: Splunk search — internal link (not accessible)



```
index=* "185.177.72.144" "/proc/self/environ"
| spath
| table _time src_ip src_port dest_ip dest_port http.method http.status http.url http.http_user_agent
```

✓ 9 events (before 10/16/25 10:19:17.000 PM) No Event Sampling ▾

Preview: On

_time	src_ip	src_port
2025-08-24 23:48:39.000		
2025-08-24 23:48:39.000		
2025-08-24 23:48:39.467		
2025-08-24 23:48:39.467		
2025-08-24 23:48:39.466		
2025-08-24 23:48:39.466		
2025-08-24 23:48:39.466		
2025-08-24 23:48:39.481		
2025-08-24 23:48:39.481		

↑↑↑

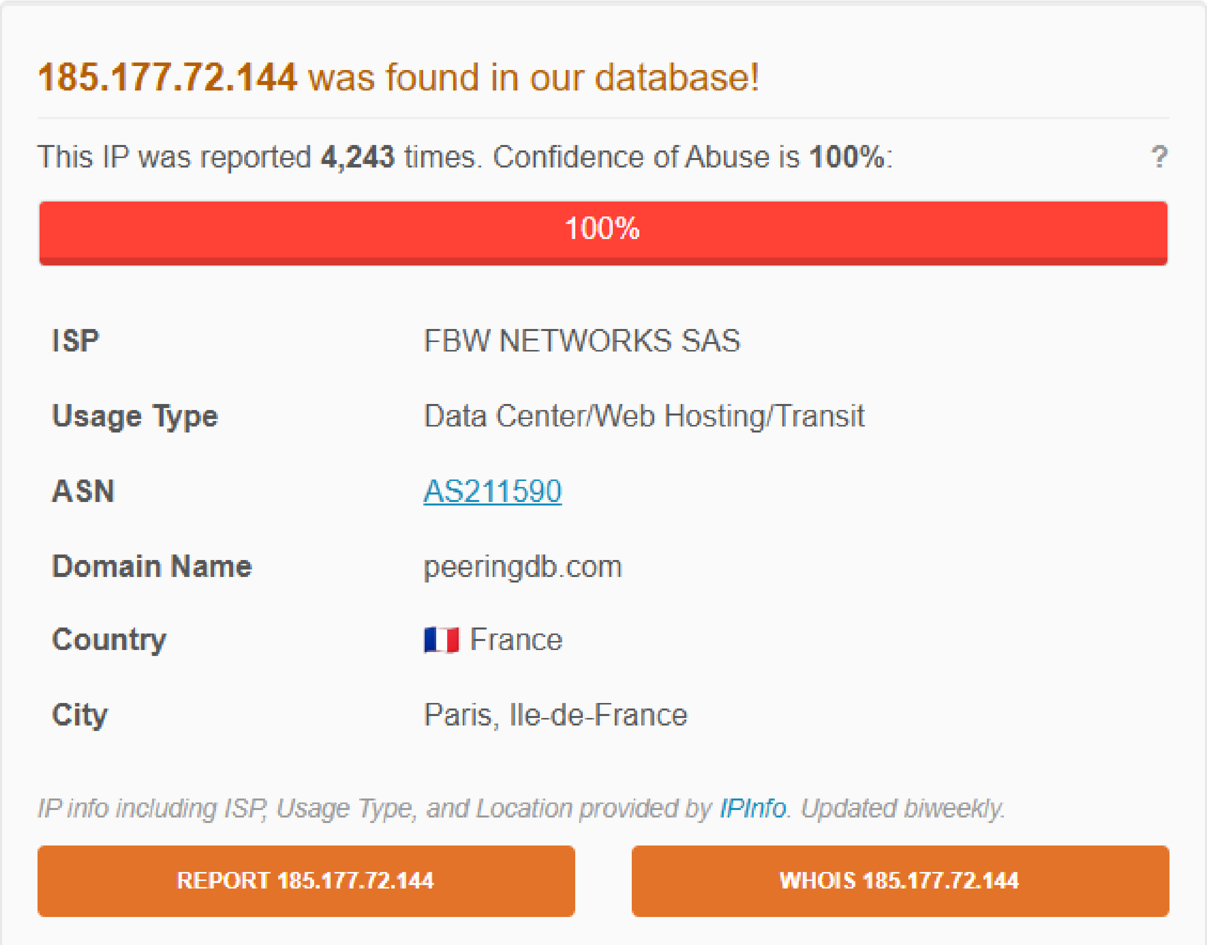
Executed the query, to verify parsed fields. The search returned 9 events, all occurring within one second (*2025-08-24 23:48:39*).
Each request targeted `/@fs/proc/self/environ` and received HTTP 403, confirming automated probing with no successful access.

Result 3: Splunk search — internal link (not accessible)

* Raw Data:*

```
<168>suricata[8969]: {"timestamp":"2025-08-24T22:48:39.481713-
0400","flow_id":2021455601025622,"in_iface":"eth0","event_type":"alert","src_ip":"185.177.72.144","src_port":59706,"
dest_ip":" [internal web
server]","dest_port":80,"proto":"TCP","tx_id":7,"alert":{"action":"allowed","gid":1,"signature_id":2012230,"rev":4,"si
gnature":"ET WEB_SERVER Likely Malicious Request for \/proc\/self\/environ","category":"Web Application
Attack","severity":1},"http":{"hostname":" [internal web server]
","url":"\/@fs\/proc\/self\/environ?raw??","http_user_agent":"Mozilla\/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/91.0.4472.124
Safari\/537.36","http_content_type":"text\/html","http_method":"GET","protocol":"HTTP\/1.1","status":403,"length":279}
}
```

Additional Findings:



185.177.72.144 was found in our database!

This IP was reported **4,243** times. Confidence of Abuse is **100%**:

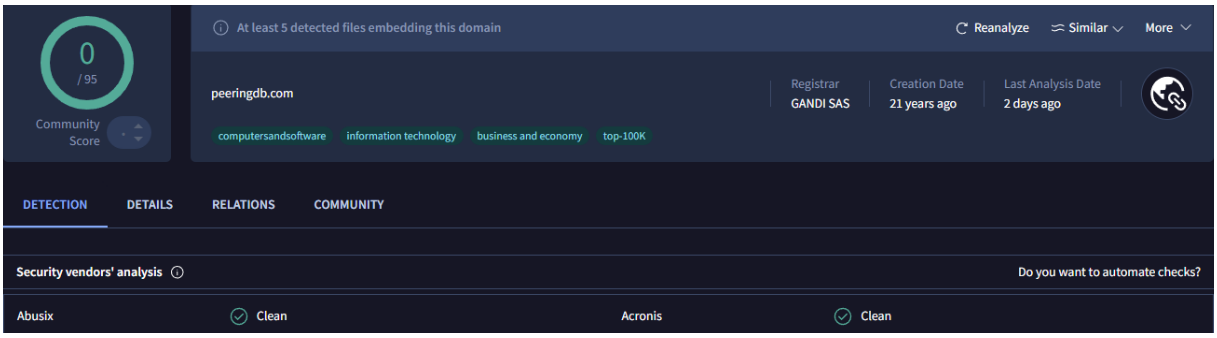
ISP	FBW NETWORKS SAS
Usage Type	Data Center/Web Hosting/Transit
ASN	AS211590
Domain Name	peeringdb.com
Country	🇫🇷 France
City	Paris, Ile-de-France

IP info including ISP, Usage Type, and Location provided by IPInfo. Updated biweekly.

This IP address has been reported a total of **4,243** times from 830 distinct sources. 185.177.72.144 was first reported on May 27th 2025, and the most recent report was **5 hours ago**.

ResultAbuseIPDB: **[here|https://www.abuseipdb.com/check/185.177.72.144]**

The domain `peeringdb.com` associated with this ASN was checked on **VirusTotal** — **0/95 security vendors** flagged it as malicious or suspicious, indicating **no direct compromise** linked to the domain itself.



0 / 95 Community Score

At least 5 detected files embedding this domain

peeringdb.com

computersandsoftware information technology business and economy top-100K

Registrar: GANDI SAS

Creation Date: 21 years ago

Last Analysis Date: 2 days ago

Security vendors' analysis

Abusix	Clean	Acronis	Clean

[here|https://www.virustotal.com/gui/domain/peeringdb.com/detection]

ANALYST ASSESSMENT

Summary:
Suricata triggered `ET WEB_SERVER Likely Malicious Request for /proc/self/environ` from source **185.177.72.144** against [internal web server] (redacted-domain.local**)**. Splunk shows **4,245** total events from this IP. Applying the URI filter for `"/@fs/proc/self/environ?raw?"` produced **3 matching events** in the basic search; an additional parsed-check using `spath` surfaced **9 raw occurrences** with identical timestamps (likely duplicate/raw vs parsed indexing differences). All observed attempts returned **HTTP 403 (Forbidden)** — no successful disclosure observed.

Attack details:

Source: 185.177.72.144 (src port 59706) → **Destination:** [internal web server]
Targeted path: `/@fs/proc/self/environ?raw??` (attempt to read `/proc/self/environ`)

Events: 3 (filtered) / 9 (parsed raw occurrences) — burst within one second (2025-08-24 23:48:39).
HTTP method / status: GET — all responses **403** (no access).

User-Agent: `Mozilla/5.0 (...) Chrome/91.0.4472.124` (spoofable; not proof of human).
Suricata signature: `ET WEB_SERVER Likely Malicious Request for /proc/self/environ` (sid:2012230 rev:4).

Path breakdown / what it means:

- `/CFIDE/` — ColdFusion administrative/utility components commonly probed by attackers.
- `componentutils` — frequently targeted ColdFusion component; existence may allow remote actions or information disclosure if vulnerable.
- Observed requests appear to be **probes** to detect presence of ColdFusion endpoints; 404 responses indicate the path was not present/accessible.

Method / Indicators:

- **HTTP method:** `GET` — passive probing attempt to access `/proc/self/environ` and read environment variables.
- **User-Agent:** `Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36` — matches a legitimate Chrome 91 browser on Windows 10, but User-Agent strings are trivially spoofable. Treat as likely automated scanner traffic rather than human browsing.
- **Timing/volume:** High overall activity (**4,245 events** from the same IP), but only **3 direct hits** to `/@fs/proc/self/environ?raw?` (and 9 raw duplicates in parsed view).This selective, high-frequency pattern within one second is typical of **automated reconnaissance tools** probing for environment disclosure or Local File Inclusion (LFI) vulnerabilities.

Threat Intelligence enrichment :

AbuseIPDB: 185.177.72.144 — reported **~4,243** times (830 reporters); high historical abuse.

VirusTotal (IP): multiple vendors flagging (as recorded in ticket: 5/95 flagged; 2 suspicious).

ASN / Domain: ASN `AS211590` (FBW NETWORKS SAS); domain `peeringdb.com` associated with ASN — domain checked on VirusTotal: **0/95** detections (no malicious flags for the domain itself).

Shodan / Censys: host shows open services (e.g., 22, 9100, 10250, 10256) — increases attack surface.

TI posture: discordant (IP has many abuse reports; associated domain appears clean). Treat IP as **high-risk** while the domain itself is not flagged.

Detection context:

- Pattern (many events from same IP; 3–9 rapid hits to the same sensitive path) is consistent with **automated reconnaissance / scripted probing** for environment disclosure or CGI misconfiguration.

- All attempts returned 403 — **no evidence of successful disclosure or exploitation** in observed telemetry.

- Discrepancy between “3” and “9” is likely due to search semantics (literal-filter vs parsed/raw extraction); both are included in ticket as supporting evidence.

Impact if successful :

Reading `/proc/self/environ` could reveal environment variables (API keys, credentials, paths) leading to data leakage, RCE via crafted CGI handlers, webshell insertion, or follow-on compromise and lateral movement.

attacker could obtain environment secrets → credential leakage → possible RCE / follow-on compromise

Mini Attack Visualization:

[Attacker 185.177.72.144 probes target — [internal web server]**]**

↓

[Connection made from src port 59706 → dest [internal web server]]

↓

[Automated HTTP GET requests sent to `"/@fs/proc/self/environ?raw??"`]

↓

[Requests attempt to read `/proc/self/environ` (environment variables disclosure probe)]

↓

[Burst behavior: 3–9 identical requests observed within one second (2025-08-24 23:48:39)]

↓

[Server response: HTTP 403 (Forbidden) to every request — no file contents returned]

↓

[Probe failed — no environment disclosure, no command execution, no webshell or payload observed]

ACTION

1. **Host Verification** – [internal web server]

Confirm host ownership and business use (redacted-domain.local).
Ensure no exposed `/proc` or CGI handlers are accessible.

2. Evidence Preservation
Export Suricata alert and 3–9 Splunk events (CSV/JSON).
Save access/error logs around *2025-08-24 23:48:39 UTC-4*.

3. Containment
Block or rate-limit **185.177.72.144** for 24–72 h via firewall/WAF.
Add IP/ASN 211590 to watchlist and monitor for recurrence.

4. Web Server & WAF Hardening
Block access to `/proc` and `@fs` paths.
Add WAF rule for `/proc/self/environ` and encoded variants.
Throttle repeated identical requests from a single IP.

5. Logging & Detection
Verify full request/headers logging.
Enable proper JSON field extraction in Splunk (`src_ip`, `http.url`, `status`).
Create saved search for future hits on `/@fs/proc/self/environ`.

6. Threat Hunting
Search last 30–90 days for similar URIs or related IPs in ASN 211590.

7. Escalation
Notify system owner; escalate to IR if any **non-403** responses or abnormal outbound activity appear.