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: 55309

Description

ET WEB_SERVER /bin/sh Detected in URI – Potential Shell Execution Attempt

Victim:

[internal web server] - redacted-domain.local

1 Encoded log:

"/cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh"

1 Decoded log:

"/cgi-bin/../../../../../../../../../../bin/sh"

2 Encoded log:

"/cgi-bin/%%32%65%%32%65/%%32%65%%32%65/%%32%65%%32%65/%%32%65%%32%65/%%32%65%%32%65/%%32%65%%32%65/%%32%65%%32%65/%%32%65%%32%65/bin/sh"

2 Decoded log:

"/cgi-bin/../../../../../../bin/sh"

ATTACKER INFO:

IP: `1.95.121.46` on port `53206 and 57338`

User Agent: "The User-Agent string identifies as libredtail-http, which is not a typical browser.

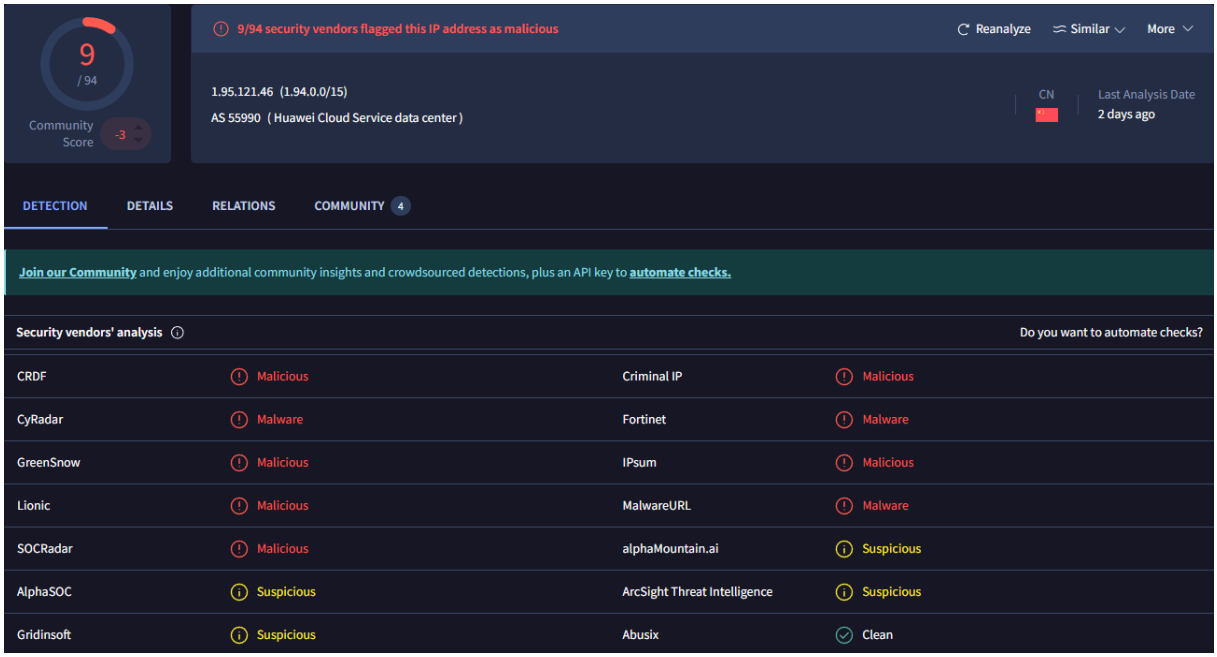
This suggests the request was generated by an automated script or custom tool,

likely used for reconnaissance or exploitation attempts rather than normal user activity."

ANALYST INVESTIGATION:

Virus Total Result: **[here|https://www.virustotal.com/gui/ip-address/1.95.121.46]**

Security Vendors' Analysis from Virus Total: **9/94 security vendors flagged this IP address as malicious**



Talos Intelligence:

REPUTATION DETAILS:

Email Reputation: *Poor*

Web Reputation: *Untrusted*

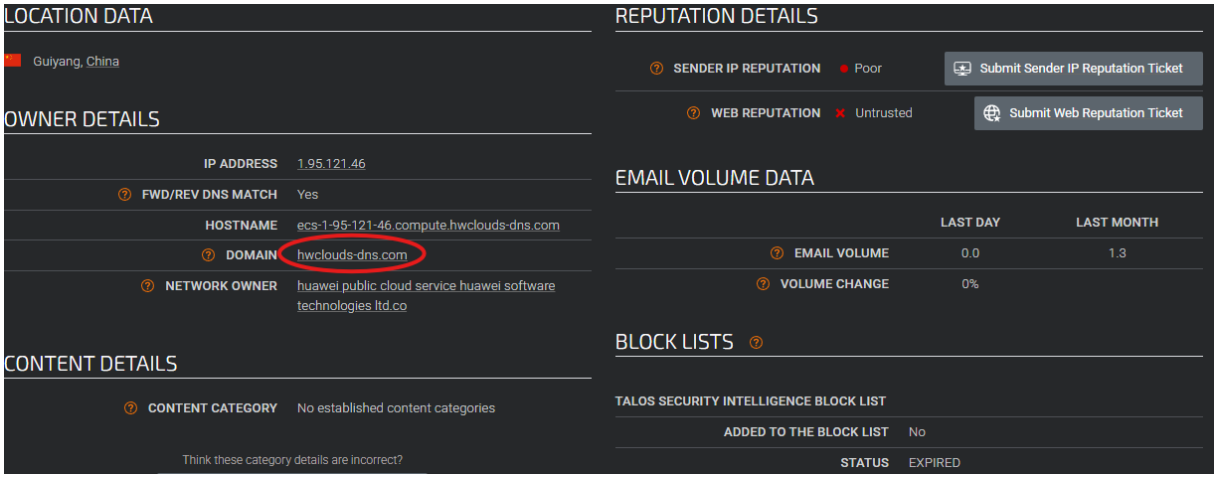
BLOCK LISTS:

Talos Security Intelligence Block List

Added to the Block List = No

Status = EXPIRED

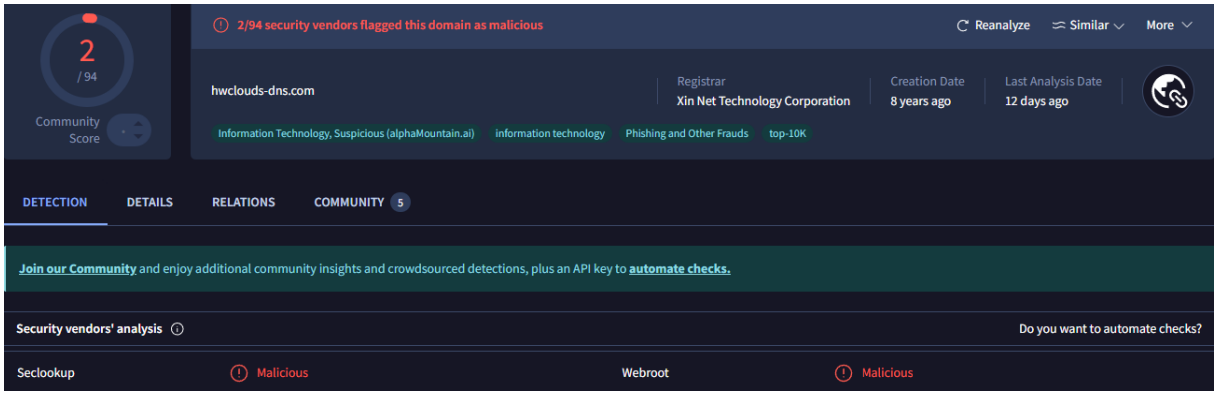
Talos Result:
[here|https://talosintelligence.com/reputation_center/lookup?search=1.95.121.46]



The source IP **1.95.121.46 was checked in Cisco Talos, which resolved to the domain **hwclouds-dns.com**.**

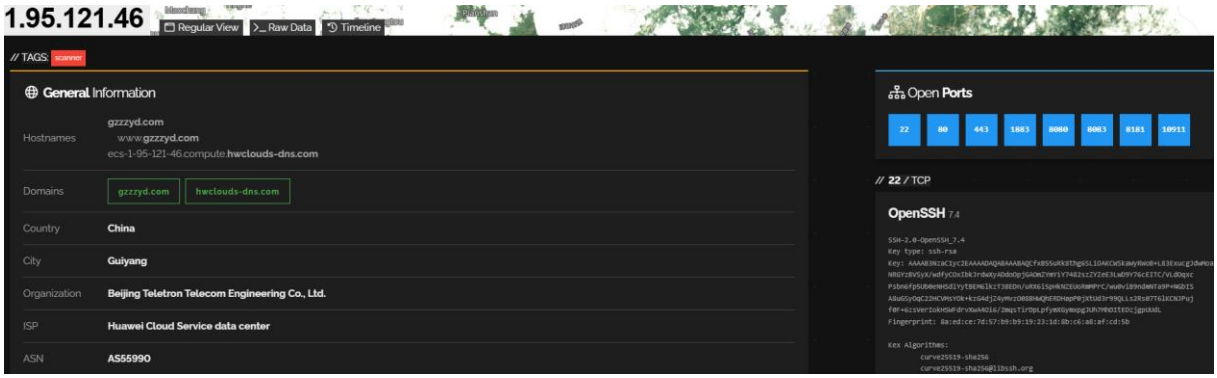
A lookup of this domain in VirusTotal showed **2/94 security vendors flagged it as malicious, indicating suspicious or potentially harmful activity.**


2 / 94 ecs-1-95-121-46.compute.hwclouds-dns.com
Resolution date 2025-08-17 07:43:31
Name ecs-1-95-121-46.compute.hwclouds-dns.com
Creation date 2017-03-28 02:53:26
Last update 2023-06-26 00:59:46
Detections
Webroot malicious
Seclookup malicious
Acronis Undetected
0xSI_f33d Undetected
Abusix Undetected
... and 89 items more
Click to select
Double click to expand

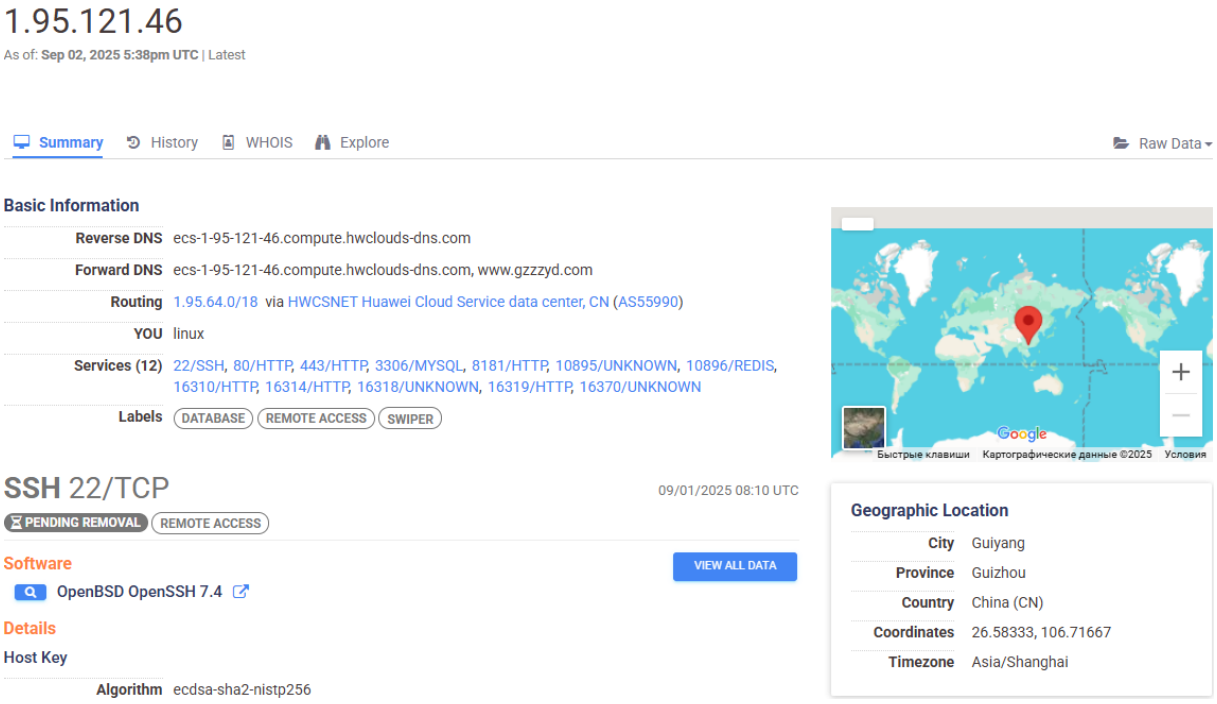

2 / 94
Community Score
2/94 security vendors flagged this domain as malicious
Reanalyze
Similar
More
hwclouds-dns.com
Registrar
Xin Net Technology Corporation
Creation Date
8 years ago
Last Analysis Date
12 days ago
Information Technology, Suspicious (alphaMountain.ai)
information technology
Phishing and Other Frauds
top-10K
DETECTION
DETAILS
RELATIONS
COMMUNITY 5
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Security vendors' analysis
Do you want to automate checks?
Seclookup
Malicious
Webroot
Malicious

ShodanResult: **[here|https://www.shodan.io/host/1.95.121.46]**

Open Ports: 22, 80, 443, 1883, 8080, 8083, 8181, 10911



CensysResult: **[here|https://www.shodan.io/host/1.95.121.46]**



GreyNoise Result: **[here|https://viz.greynoise.io/query/hwclouds-dns.com]**

The IP 1.95.121.46 was checked in GreyNoise and did not show any unusual activity.

However, this IP is associated with the domain hwclouds-dns.com.

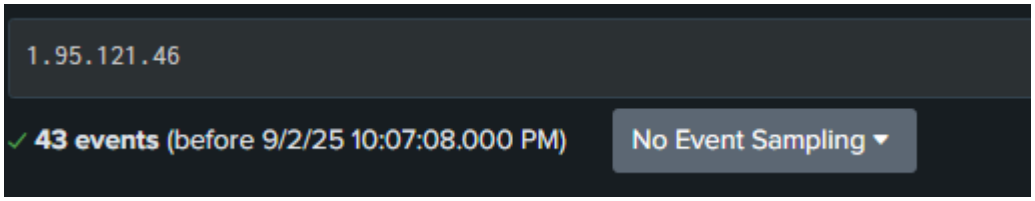
Analysis of this domain revealed 5 related IP addresses that are flagged as malicious in threat intelligence feeds.

These IPs were observed performing SSH brute force attacks and connection attempts against multiple destinations.

Splunk Investigation: A total of 43 events were identified during the analysis.

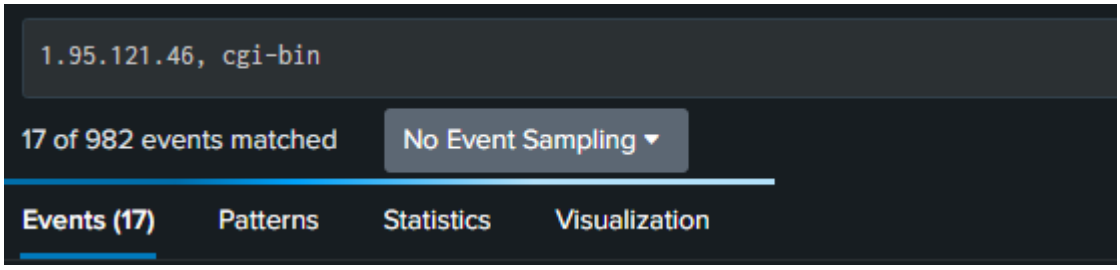
To structure the investigation, two key identifiers were applied: "cgi-bin" and "/bin/sh".

This helped highlight specific activity patterns and potential exploitation attempts involving command execution through web server paths.



↑ ↑ ↑

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

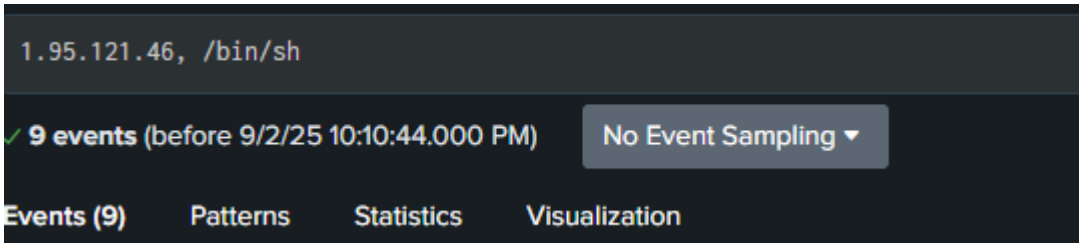


↑ ↑ ↑

A total of 17 events were identified by applying the indicator "cgi-bin".

This filter allowed narrowing down the activity and focusing on requests that may indicate attempts to exploit web server components.

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



↑ ↑ ↑

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

After introducing an additional identifier "/bin/sh", the dataset was further reduced to 9 events.

This refinement highlighted activity consistent with path traversal and possible command execution attempts.

1 Raw Data:

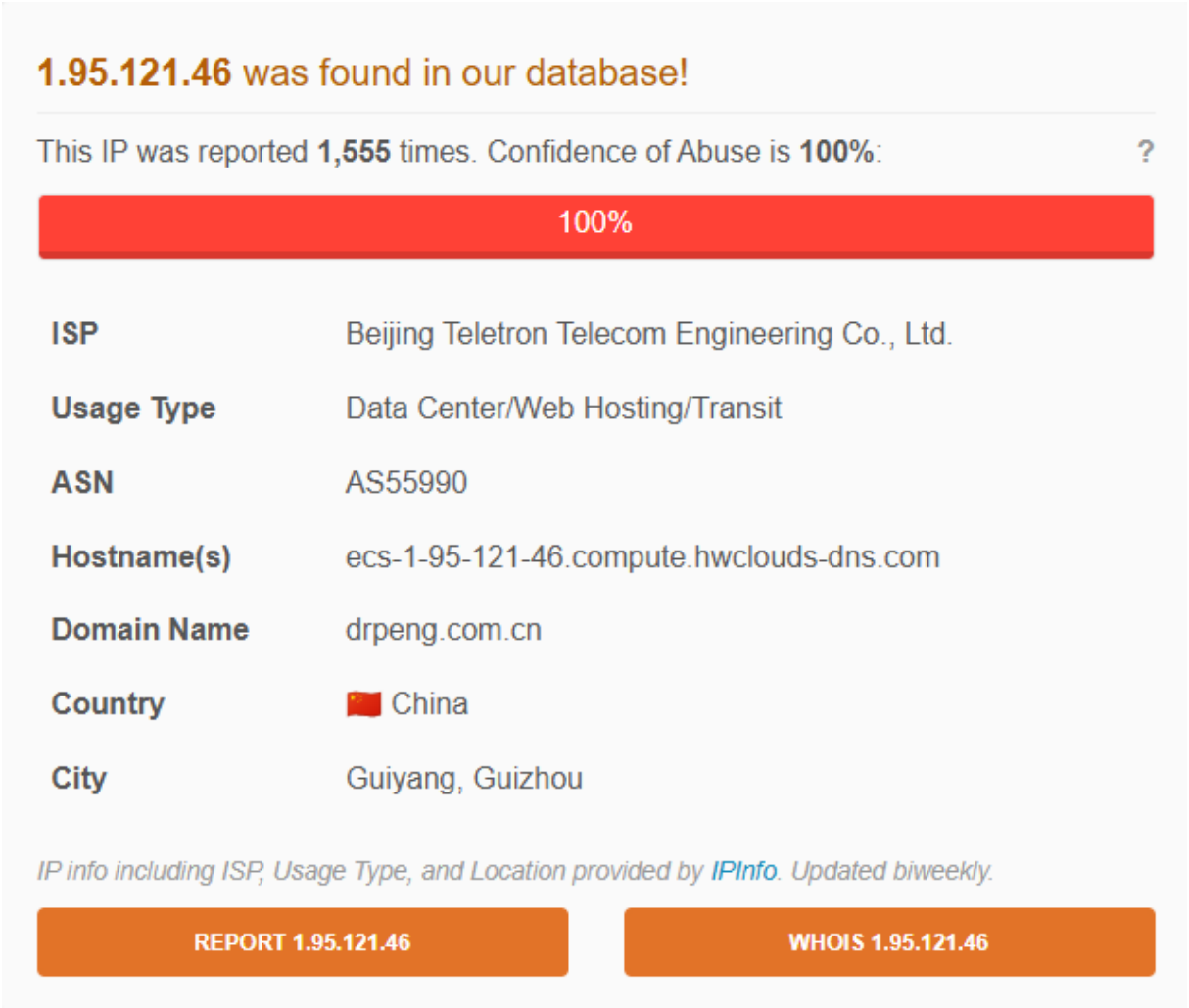
<168>suricata[8969]: {"timestamp":"2025-08-30T17:32:31.345857-0400","flow_id":141905416244629,"in_iface":"eth0","event_type":"alert","src_ip":"1.95.121.46","src_port":53206,"dest_ip":" [internal web server]*","dest_port":80,"proto":"TCP","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_id":2011465,"rev":7,"signature":"ET WEB_SERVER \/bin\/sh In URI Possible Shell Command Execution Attempt","category":"Web Application Attack","severity":1},"http":{"hostname":"* [internal web server]*","url":"\/cgi-*

bin\/.%2e\/.%2e\/.%2e\/.%2e\/.%2e\/.%2e\/.%2e\/.%2e\/.%2e\/.%2e\/bin\/sh","http_user_agent":"libredtail-http","http_content_type":"text\/html","http_method":"POST","protocol":"HTTP\/1.1","status":400,"length":306}}

2 Raw Dat:

<168>suricata[8969]: {"timestamp":"2025-08-30T17:34:44.000154-0400","flow_id":1704341504225759,"event_type":"alert","src_ip":"1.95.121.46","src_port":57338,"dest_ip":" [internal web server]*","dest_port":80,"proto":"TCP","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_id":2011465,"rev":7,"signature":"ET WEB_SERVER \/bin\/sh In URI Possible Shell Command Execution Attempt","category":"Web Application Attack","severity":1},"http":{"hostname":"* [internal web server]*","url":"\/cgi-bin\/%%32%65%%32%65\/%%32%65%%32%65\/%%32%65%%32%65\/%%32%65%%32%65\/%%32%65%%32%65\/%%32%65%%32%65\/%%32%65%%32%65\/bin\/sh","http_user_agent":"libredtail-http","http_content_type":"text\/html","http_method":"POST","protocol":"HTTP\/1.1","status":400,"length":306}}*

Additional Findings:



This IP address has been reported a total of **1,555** times from 357 distinct sources. 1.95.121.46 was first reported on August 16th 2025, and the most recent report was **2 hours ago**.

__ResultAbuseIPDB:__ **[here|https://www.abuseipdb.com/check/1.95.121.46]**

ANALYST ASSESSMENT

The analysis of Suricata network alerts and subsequent log review reveals that the IP address 1.95.121.46 attempted a web application attack targeting a web server over HTTP. The activity specifically involved path traversal sequences and attempts to invoke `/bin/sh` via `/cgi-bin/`, which strongly suggests efforts to execute arbitrary shell commands on the target host. The attacker relied on obfuscation through double-encoded payloads (e.g., `%2e` and `%%32%65`) in the request URI to bypass detection.

Attack Details

The attacker from IP 1.95.121.46, using ports 53206 and 57338, sent crafted HTTP `POST` requests with suspicious paths such as:

- **`/cgi-bin/../../../../../../../../../../bin/sh`**
- **`/cgi-bin/../../../../../../bin/sh`**

These requests are consistent with attempts to exploit CGI-based services and execute commands through the system shell.

Path Breakdown

- **`/cgi-bin/` – The default directory where executable CGI scripts are stored. Attackers often probe this path for vulnerabilities.**
- **`..` (path traversal) – Encoded directory traversal used to escape the intended web root and access restricted system binaries.**
- **`/bin/sh` – The Unix shell, targeted here for direct execution of arbitrary commands if reachable.**

Method

POST – Indicates that data could be sent to the server for execution, not just retrieved, suggesting an attempt at active exploitation.

User-Agent

`libredtail-http` – This is not a standard browser identifier. The User-Agent suggests the request was generated by a custom script or automated tool, not human browsing activity. Such signatures are typical of reconnaissance or mass-exploitation frameworks.

Content Type

`text/html` – Suggests that the attacker expected a normal HTML response, consistent with probing for an exposed CGI binary.

HTTP Status

400 Bad Request – The server rejected the malformed request. While the exploitation attempt was unsuccessful, the activity itself indicates hostile intent and automated probing behavior.

Detection Context

- **Signature Triggered: *ET WEB_SERVER /bin/sh In URI Possible Shell Command Execution Attempt***
- **Unusual URI Access: Requests attempting traversal outside of `/cgi-bin/` to reach `/bin/sh`.**
- **Encoded Payloads: Use of double-encoding (`.%2e` and `%%32%65`) highlights attempts to evade detection filters.**
- **Suspicious User-Agent: The use of *libredtail-http* confirms scripted or automated exploitation activity.**

Threat Intelligence Enrichment

- **VirusTotal: 9/94 vendors flagged the IP as malicious.**
- **Talos Intelligence: The IP resolves to hwclouds-dns.com, a domain with malicious reputation.**
- **GreyNoise: Direct activity for this IP was minimal, but the associated domain links to 5 additional malicious IPs conducting SSH brute force attacks.**

- **Shodan: Multiple open services were discovered (22, 80, 443, 1883, 8080, 8083, 8181, 10911), expanding the attack surface.**

Impact if Successful

- **Remote Command Execution (RCE): Execution of arbitrary shell commands via `/bin/sh`.**
- **Privilege Escalation: Potential for root-level access if the server was misconfigured.**
- **System Compromise: Full server takeover, data leakage, or staging point for lateral movement.**
- **Persistence: Attacker could install backdoors or web shells to maintain long-term access.**

Mini Attack Visualization:

[QRadar SIEM detects suspicious offense with Severity 9]

↓

[Analyst pivots into offense details – source IP 1.95.121.46]

↓

[Attacker initiates connection on ports 53206 / 57338]

↓

[HTTP POST requests sent with encoded traversal payloads]

↓

[Suspicious URIs targeting /cgi-bin/ with /bin/sh execution]

↓

[Request sent via automated tool (User-Agent: libredtail-http)]

↓

[Server receives path traversal attempts to reach /bin/sh]

↓

[Server responds with HTTP 400 Bad Request]

↓

[Suricata triggers ET WEB_SERVER /bin/sh In URI Possible Shell Command Execution Attempt alert]

↓

[Activity correlated in Splunk – 43 events reduced to 9 with identifiers]

↓

[Threat intelligence links IP to hwclouds-dns.com and related malicious infrastructure]

↓

[Activity flagged as exploitation attempt and documented for escalation]

ACTION

1. **Block the Source IP (1.95.121.46)**
   Block the attacker's IP address at the perimeter firewall, IDS/IPS, or WAF to prevent further exploitation attempts.

2. **Restrict Access to /cgi-bin/**
   Limit or disable public access to `/cgi-bin/` directories if not required. Consider removing or hardening legacy CGI scripts to reduce the attack surface.

3. **Harden Against Path Traversal**
   Ensure web servers are configured to properly sanitize and reject encoded traversal sequences (`.%2e`, `%2e`, `%%32%65`). Patch or disable vulnerable CGI handlers.

4. **Enable or Tune WAF Rules**
   Configure the Web Application Firewall to detect and block:

- Path traversal attempts (`../`, `%2e`, double-encoded payloads)
- Requests containing `/bin/sh` or other system binaries
- Suspicious User-Agent strings like `libredtail-http`

5. **Investigate Suspicious User-Agent (libredtail-http)**
   Search logs for other HTTP requests using `libredtail-http`. This User-Agent suggests automated exploitation tools or custom scripts.

6. **Expand Threat Hunting via Threat Intelligence**
   Monitor for related activity from domain **hwclouds-dns.com** and associated malicious IPs performing SSH brute force attacks. Add them to block/monitor lists.

7. **Correlate in Historical Logs**
   Search Splunk/QRadar for additional requests to `/cgi-bin/` or `/bin/sh`, especially from hosting providers and suspicious networks. Identify repeat patterns or campaigns.

8. **Validate QRadar SIEM Offense**
   The detection was initially triggered in **QRadar (Severity 9 offense)**. Verify that correlation rules are tuned to generate alerts for similar exploitation attempts.

9. **Continuous Monitoring**
   Set up alerting for future exploitation attempts involving `/cgi-bin/` and encoded traversal payloads. Monitor for reoccurrence from related infrastructure or other hosting providers.