Finding compromised `upl.php` devices

A use case from yesterday's QBot conference

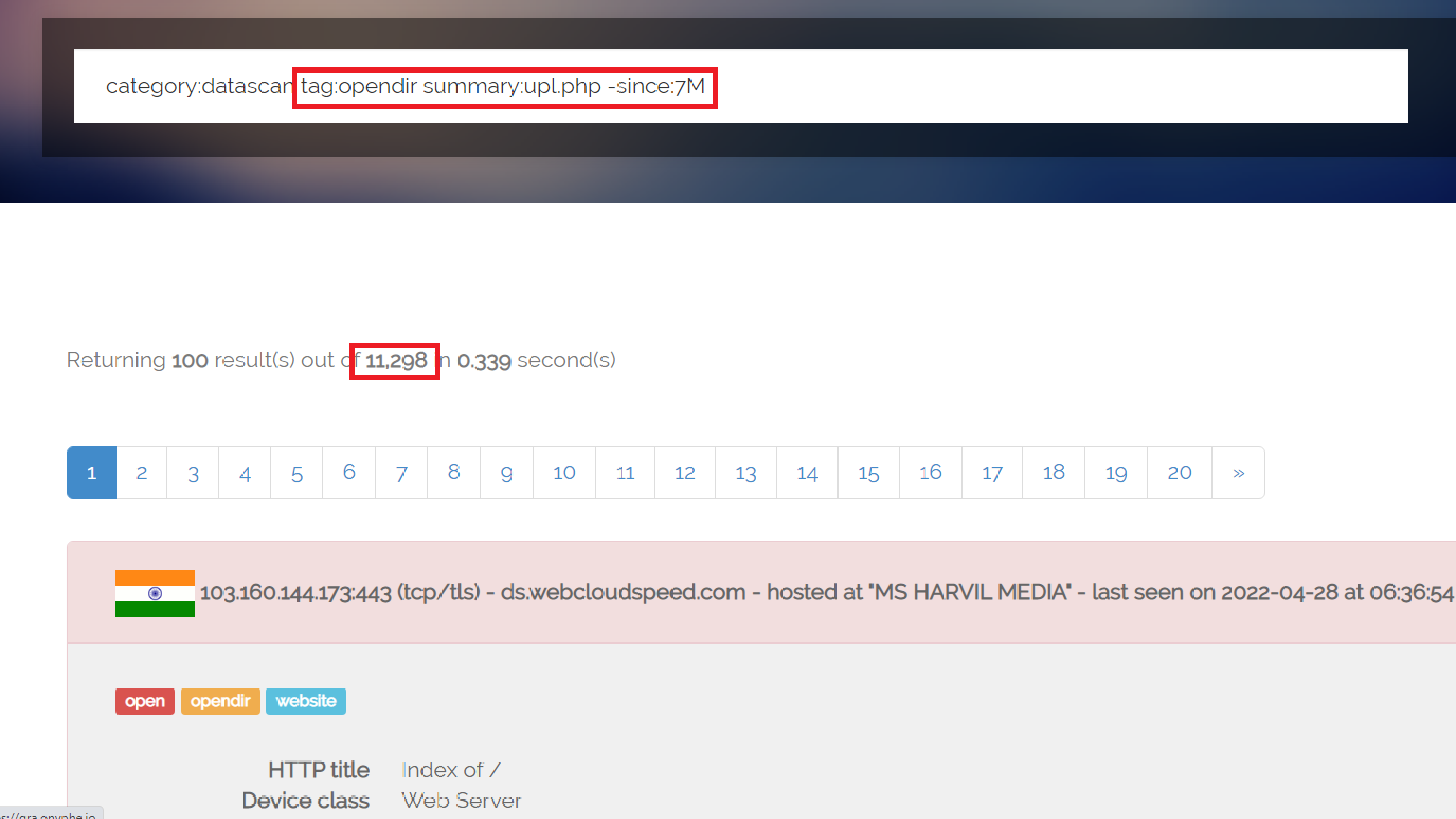
ONYPHE

What ONYPHE does?

- Internet scanning
  - Full IPv4 space
  - **200+ ports** scanned monthly
- URL scanning
  - Like a Web search engine
  - **300,000,000+ URLs** monthly
- **Tagging** and **classification**

- Detections used for this LT
  - **Open Web directories**
  - **Exposed filenames**

ONYPHE



category:datascan tag:opendir summary:upl.php -since:7M

Returning **100** result(s) out of **11,298** in **0.339** second(s)

103.160.144.173:443 (tcp/tls) - ds.webcloudspeed.com - hosted at "MS HARVIL MEDIA" - last seen on 2022-04-28 at 06:36:54

HTTP title	Index of /
Device class	Web Server

ONYPHE CLI tool to query the API

- What about searching for unique hostnames?
  - ONYPHE Command Line Interface tool
  - Splunk-like syntax

- **Demo**: listing unique hostnames exposing `upl.php` file

```
onyphe     'category:datascan tag:opendir summary:upl.php
           | uniq hostname'
```

https://asciinema.org/a/mMkMZJuaNE67CfjFGhb74RDGS

ONYPHE

Devices exposing `upl.php`

- **10,445** unique hostnames found

- How many of them are compromised?
  - Well, having `upl.php` is already a bad sign ☹

- Easy to get that answer with a correlation search
  - Splunk-like syntax for the win

ONYPHE

Correlation search

- Searching within 7-month of data

```
category:datascan tag:opendir summary:upl.php
| dedup ip
| search category:datascan tag:compromised ip:$ip
| uniq hostname
```

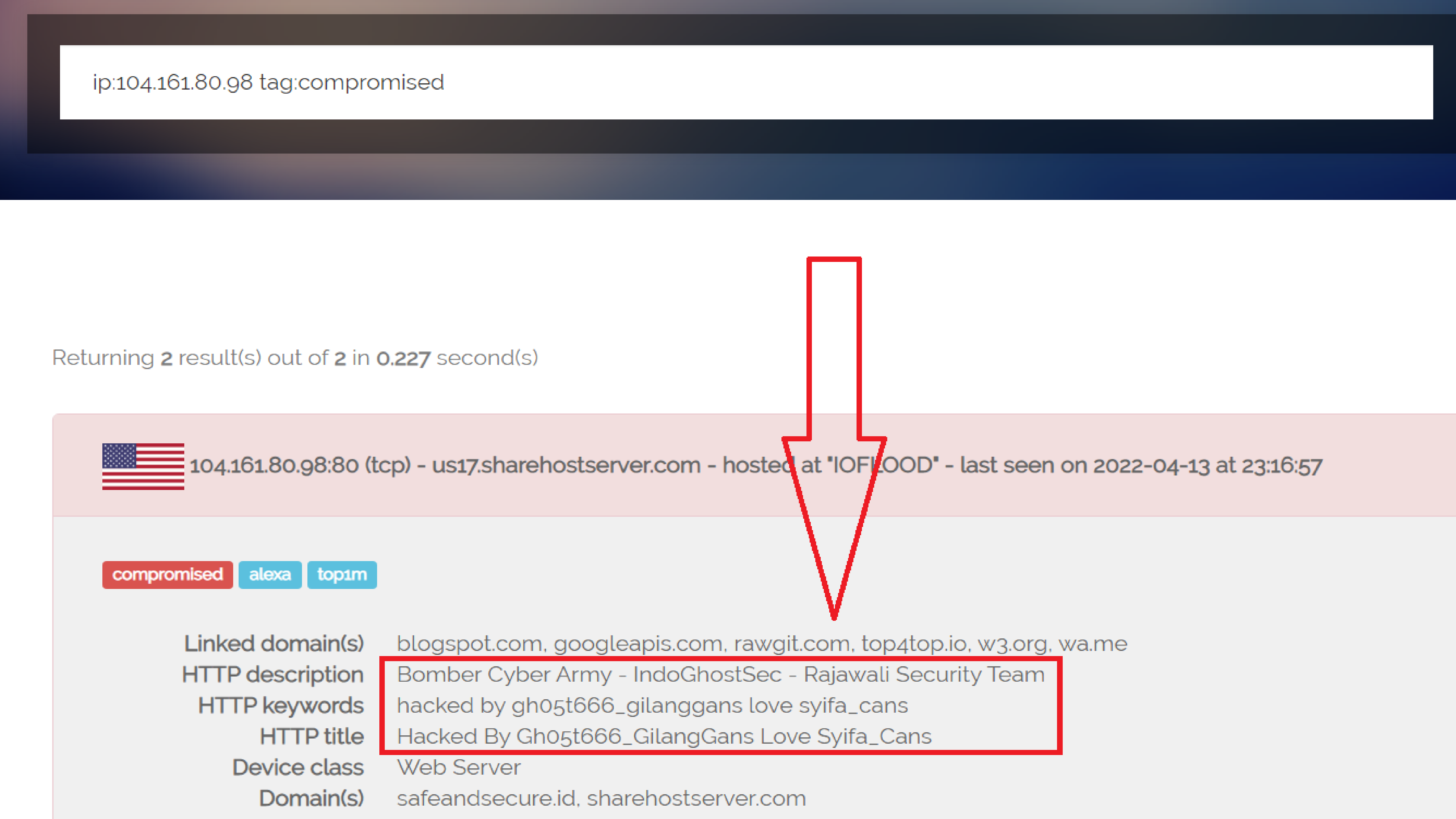
Detected as compromised

- **1,649** unique hostnames found

- But we should consider all of them as compromised

- How were they detected as compromised?
  - Pattern matching in HTML content
  - And other heuristics

ONYPHE



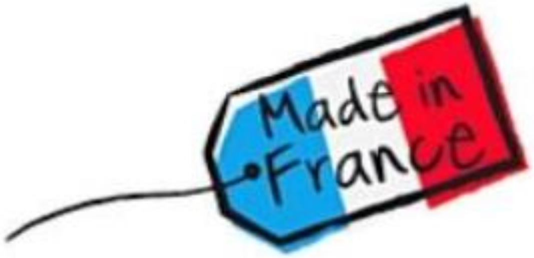
ip:104.161.80.98 tag:compromised

Returning **2** result(s) out of **2** in **0.227** second(s)

104.161.80.98:80 (tcp) - us17.sharehostserver.com - hosted at "IOFLOOD" - last seen on 2022-04-13 at 23:16:57

Linked domain(s)	blogspot.com, googleapis.com, rawgit.com, top4top.io, w3.org, wa.me
HTTP description	Bomber Cyber Army - IndoGhostSec - Rajawali Security Team
HTTP keywords	hacked by gh05t666_gilanggans love syifa_cans
HTTP title	Hacked By Gh05t666_GilangGans Love Syifa_Cans
Device class	Web Server
Domain(s)	safeandsecure.id, sharehostserver.com

Thank you



Twitter:	@ONYPHE
Register:	https://www.onyphe.io/login/#register
Pricing:	https://www.onyphe.io/pricing

ONYPHE