

Bypassare i Content Delivery Network (CDN)

Cosa sono i Content Delivery Network?

A livello di performance

I CDN sono reti di server distribuiti geograficamente che collaborano per fornire contenuti web e altri servizi su Internet in modo più efficiente e veloce.

A livello di sicurezza

Molte volte le reti CDN contengono soluzioni WAF che permettono di proteggere le applicazioni web da minacce informatiche.

Inoltre queste soluzioni fanno sì che l'indirizzo IP del server di origine non sia raggiungibile grazie all'utilizzo di server DNS proprietari costringendo l'utente a effettuare la richiesta attraverso la rete CDN.

Quali sono le soluzioni in commercio?

- CLOUDFLARE
- Amazon CloudFront
- Google Cloud CDN

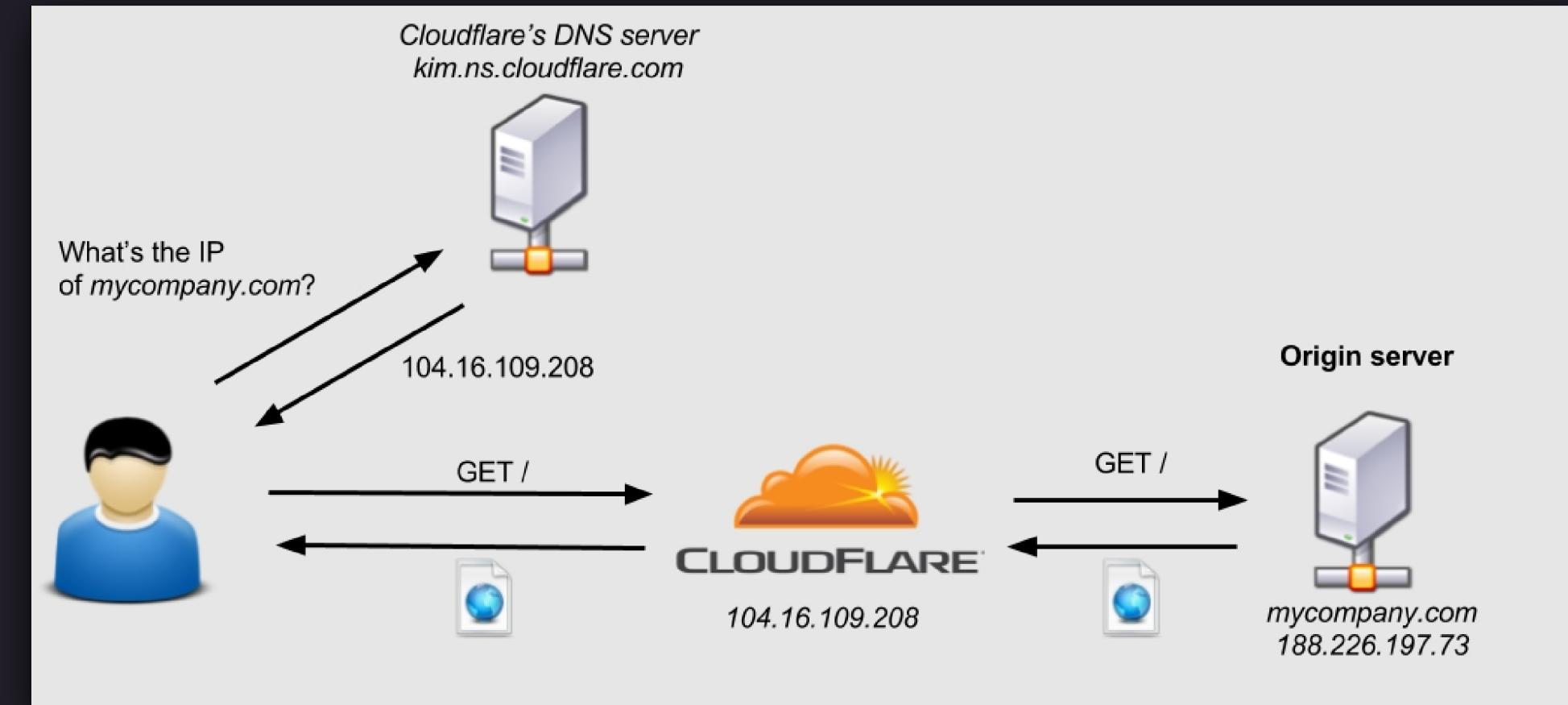
Cosa significa e perché bypassare un CDN per un attaccante?

Bypassare un CDN

Significa conoscere l'indirizzo IP del server origine

Perché bypassare un CDN

Se un attaccante riesce a individuare l'IP del server di origine dietro il CDN, potrebbe tentare di bypassare il CDN per colpire direttamente il server. Questo potrebbe rendere più facile per l'attaccante lanciare attacchi come DDoS (Distributed Denial of Service), exploit di vulnerabilità del server o tentativi di accesso non autorizzato.



Quali sono i blocchi di IPv4 assegnati ai vari vendor CDN?

Conoscere i blocchi assegnati dalla IANA ai vari vendor è importante per capire quali applicazioni web sono protette (se sono protette) da quale rete CDN.

- CLOUDFLARE ⇒ 104.16.0.0/13 , 172.64.0.0/13 , 141.101.64.0/22 ,
Lista disponibile a <https://www.cloudflare.com/it-it/ips/>
- Amazon CloudFront ⇒ 120.52.22.98/27 , 54.192.0.0/16 , 3.165.0.0/16 ,
Lista disponibile a <https://d7uri8nf7uskq.cloudfront.net/tools/list-cloudfront-ips>
- Google Cloud CDN ⇒ 34.125.0.0/16 , 34.64.0.0/11 , 35.216.0.0/15 ,
Lista disponibile effettuando un nslookup:
`nslookup -q=TXT _cloud-netblocks.googleusercontent.com 8.8.8.8`

Tecniche utilizzate per trovare l' indirizzo IP del Sever Origine

1. Brute-Force sui sottodomini
2. Query DNS sui record MX (Mail), SPF, TXT
3. Controllo della DNS History
4. Controllo dei server che usano il certificato SSL assegnato al dominio
5. Brute-Force sui range ipv4 probabili
6. Utilizzo di motori di ricerca come Shodan e Censys

Brute-Force sui sottodomini

Query DNS ad un nome protetto da un CDN

Una volta che la query DNS per il nome del server protetto viene risolta da un server DNS del CDN, è probabile che l'attaccante venga reindirizzato a un server nella rete CDN, e di conseguenza l'indirizzo IP del server di origine sarà offuscato.

Query DNS ad un sottodominio di un nome protetto da un CDN

Nel caso in cui il sottodominio non sia anche esso protetto dal CDN la query sarà gestita da un altro server DNS che risolverà il nome. In questo caso, se il sottodominio viene risolto con l'indirizzo IP dello stesso server, quest'ultimo sarà effettivamente l'IP del server di origine.

Esempio di utilizzo del tool cloudIP per trovare come vengono risolti i sottodomini di nabcosmetic.com utilizzando una wordlist con 7 entry:

```
> nabcosmetic.com selected
Attempting to check IPs with nslookup..
104.31.71.204 --> CLOUDFLARENET
104.31.70.204 --> CLOUDFLARENET

> Resolve Attempt 1 of 7 [ FTP ] ----> 109.234.164.18
NetName of 109.234.164.18 --> 02SWITCH

> Resolve Attempt 2 of 7 [ Cpanel ] --> 109.234.165.77
NetName of 109.234.165.77 --> 02SWITCH

> Resolve Attempt 3 of 7 [ Mail ] ----> 109.234.165.77
NetName of 109.234.165.77 --> 02SWITCH

> Resolve Attempt 4 of 7 [ Direct ] --> Failed to resolve

> Resolve Attempt 5 of 7 [ Direct-Connect ] --> Failed to resolve

> Resolve Attempt 6 of 7 [ Webmail ] --> $
NetName of 109.234.165.77 --> 02SWITCH
```

Query DNS sui record MX, SPF, TXT

Query DNS ad un record MX, SPF, TXT di un nome protetto da un CDN

Anche in questo caso è possibile che non tutti questi record siano stati protetti dalla rete CDN e quindi che la query venga gestita da un server DNS che non fa parte della rete CDN e che conosce il vero indirizzo del server origine.

Nel caso del record MX, ad esempio, è possibile conoscere l'IP del server SMTP che gestisce le mail inviate dal dominio e nel caso esso sia lo stesso server che contiene il servizio web l'offuscamento viene meno.

Nel caso del record TXT, alcune volte è possibile trovare informazioni sensibili che possono contenere l'indirizzo IP del server di origine.

Pezzo di output del tool dnsrecon sul nome hackersploit.org.

Il server SMTP non è protetto da CLOUDFLARE in quanto l'IP restituito dal campo MX non appartiene al range IP di CLOUDFLARE

```
[*]      NS jim.ns.cloudflare.com 173.245.59.125
[*]      NS jim.ns.cloudflare.com 172.64.33.125
[*]      NS jim.ns.cloudflare.com 108.162.193.125
[*]      NS jim.ns.cloudflare.com 2606:4700:58::adf5:3b7d
[*]      NS jim.ns.cloudflare.com 2a06:98c1:50::ac40:217d
[*]      NS jim.ns.cloudflare.com 2803:f800:50::6ca2:c17d
[*]      MX _dc-mx.2c2a3526b376.hackersploit.org 198.54.120.212
[*]      A  hackersploit.org 172.67.202.99
[*]      A  hackersploit.org 104.21.44.180
```

Controllo della DNS History

La DNS History potrebbe essere utilizzata da un attaccante per ricostruire la cronologia degli indirizzi IP associati a un dominio nel tempo.

Questo potrebbe includere informazioni su tutti gli indirizzi IP a cui il dominio è stato associato nel corso del tempo, compresi quelli utilizzati prima che il dominio fosse protetto da un CDN.

Questo è il motivo per cui molti vendor consigliano ai propri clienti di cambiare il proprio indirizzo IP dopo che hanno effettuato la migrazione su una soluzione CDN.

Esempio di HistoryDNS di pastebin.org da ViewDNS.

Notare che è presente l'IP del server prima di passare a CLOUDFLARE.

Viewdns.info

Tools API Research Data

[ViewDNS.info](#) > Tools > IP History

Shows a historical list of IP addresses a given domain name has been hosted on as well as where that IP address is geographically owner of that IP address.

Domain (e.g. `domain.com`): GO

IP history results for `pastebin.org`.
=====

| IP Address | Location | IP Address Owner | Last seen on this IP |
|-----------------|--------------------------|---------------------------|----------------------|
| 192.64.119.87 | United States | NAMECHEAP-NET | 2024-03-02 |
| 104.28.25.81 | United States | CLOUDFLARENET | 2019-01-23 |
| 104.28.24.81 | United States | CLOUDFLARENET | 2019-01-23 |
| 192.64.119.87 | United States | NAMECHEAP-NET | 2018-08-03 |
| 192.64.119.92 | United States | NAMECHEAP-NET | 2017-07-16 |
| 68.65.123.253 | United States | NAMECHEAP-NET | 2017-02-07 |
| 162.255.119.254 | United States | NAMECHEAP-NET | 2015-04-10 |
| 192.64.119.68 | United States | NAMECHEAP-NET | 2014-07-04 |
| 198.187.31.144 | United States | NAMECHEAP-NET | 2012-12-29 |
| 38.101.213.238 | Marietta - United States | COGENT-174 | 2012-11-24 |
| 199.188.207.38 | United States | NAMECHEAP-NET | 2012-10-26 |
| 38.101.213.231 | Marietta - United States | COGENT-174 | 2012-04-27 |
| 38.101.213.226 | Marietta - United States | COGENT-174 | 2012-03-09 |
| 208.64.126.194 | United States | BLCC | 2012-03-02 |
| 38.101.213.251 | Marietta - United States | COGENT-174 | 2012-02-10 |
| 208.64.126.194 | United States | BLCC | 2012-01-13 |
| 208.64.127.93 | United States | BLCC | 2011-12-30 |
| 64.202.189.170 | Ashburn - United States | AS-26496-GO-DADDY-COM-LLC | 2011-12-23 |
| 184.154.125.14 | United States | SINGLEHOP-LLC | 2011-11-18 |
| 173.236.33.165 | United States | SINGLEHOP-LLC | 2011-06-26 |

Controllo dei server che usano il certificato SSL assegnato al dominio

Un attaccante conoscendo il certificato SSL associato al dominio protetto dal CDN può effettuare una ricerca, tramite l'utilizzo di alcuni tool come Censys, per farsi restituire tutti gli indirizzi IP che hanno associato quel certificato SSL.

I 3 passaggi effettuati sono:

1. Fare una ricerca per i certificati rilasciati al dominio protetto dal CDN (Ad esempio con Censys)
2. Trovare tutti gli Indirizzi IP che utilizzano quel certificato (Sempre con Censys)
3. Controllare se gli host identificati da quegli IP sono il server web di origine

```
[*] Looking for IPv4 hosts presenting these certificates...
[*] 10 IPv4 hosts presenting a certificate issued to "myvulnerable.site" were found.
- 51.194.77.1
- 223.172.21.75
- 18.136.111.24
- 127.200.220.231
- 177.67.208.72
- 137.67.239.174
- 182.102.141.194
- 8.154.231.164
- 37.184.84.44
- 78.25.205.83

[*] Retrieving target homepage at https://myvulnerable.site
```



```
[*] Testing candidate origin servers
- 51.194.77.1
- 223.172.21.75
- 18.136.111.24
    responded with an unexpected HTTP status code 404
- 127.200.220.231
    timed out after 3 seconds
- 177.67.208.72
- 137.67.239.174
- 182.102.141.194
- 8.154.231.164
- 37.184.84.44
- 78.25.205.83

[*] Found 2 likely origin servers of myvulnerable.site!
- 177.67.208.72 (HTML content identical to myvulnerable.site)
- 182.102.141.194 (HTML 98 % structurally identical to myvulnerable.site)
```

Brute-Force sui range ipv4 probabili

Quando le tecniche precedenti non forniscono informazioni utili, gli attaccanti possono ricorrere a un metodo di brute force su un probabile range di indirizzi IPv4. In questo processo, gli attaccanti provano a scansionare una vasta gamma di indirizzi IP per identificare eventuali host che potrebbero essere collegati al dominio di destinazione. Una volta identificati questi host, gli attaccanti possono eseguire ulteriori controlli per determinare se uno di essi è l'origin server desiderato.

Determinare un buon range di indirizzi IP

Visto che l'organizzazione che hosta il server web origine è spesso identificabile facilmente essi utilizzano come range il blocco di IP che è stato assegnato dalla IANA a quella organizzazione.

Esempio di utilizzo di real_ip_discover.py per trovare il serverweb di cisco sul range 72.163.4.0/24:

Utilizzo di motori di ricerca come Shodan e Censys

Una tecnica spesso utilizzata per integrare le strategie precedenti è l'impiego di motori di ricerca di dispositivi in rete come Shodan o Censys.

Questi strumenti forniscono informazioni preziose e costantemente aggiornate, consentendo agli attaccanti di ottenere dettagli sui dispositivi delle organizzazioni che sono accessibili pubblicamente su Internet.

Esempio di ricerca di google.com su censys:

Notare che la lista di host può essere filtrata per Autonomous System, Location e anche per Organizzazione.

The screenshot shows the Censys search interface with the query 'google.com' entered in the search bar. The results page displays a list of hosts found, each with detailed information about the device's platform, location, and open ports. The interface includes filters for Host Filters (Labels, Autonomous System, Location), a sidebar with a 'Host Filters' section, and navigation links for Report, Docs, and Subscriptions.

Host Filters

Labels:

- 2.22M remote-access
- 448.52K login-page
- 212.47K file-sharing
- 175.23K database
- 125.35K email
- More

Autonomous System:

- 4.42M GOOGLE-CLOUD-PLATFORM
- 262.66K GOOGLE
- 80.72K CHINANET-BACKBONE
- No.31,Jin-rong Street
- 75.06K KIXS-AS-KR Korea Telecom
- 57.03K DTAG Internet service provider operations
- More

Location:

- 3.25M United States
- 380.40K Belgium
- 265.35K Germany
- 200.94K Netherlands
- 171.11K Taiwan

Results

Hosts

Results: 5,840,867 Time: 1.10s

45.135.132.113 (google.com)

Linux BITWEB-AS (57271) Moscow, Russia
open-dir remote-access email file-sharing

| Port | Protocol | Service | Ports |
|-----------|----------|----------|-----------|
| 21/FTP | SSH | 22/SSH | 22/SSH |
| 110/POP3 | IMAP | 143/IMAP | 443/HTTP |
| 993/IMAP | POP3 | 995/POP3 | 1500/HTTP |
| 53/DNS | | | 80/HTTP |
| 465/SMTP | | | 587/SMTP |
| 1501/HTTP | | | |

51.159.16.92 (51-159-16-92.rev.poneytelecom.eu)

Linux Online SAS (12876) Île-de-France, France
web.control-panel.hosting login-page email file-sharing remote-access

| Port | Protocol | Service | Ports |
|-----------|----------|-----------|-----------|
| 21/FTP | SMTP | 25/SMTP | 53/DNS |
| 143/IMAP | HTTP | 443/HTTP | 465/SMTP |
| 995/POP3 | HTTP | 2077/HTTP | 587/SMTP |
| 2086/HTTP | HTTP | 2087/HTTP | 2082/HTTP |
| 2087/HTTP | HTTP | 2095/HTTP | 2083/HTTP |
| | | | 2096/HTTP |
| | | | 12141/SSH |

82.146.45.104 (vesthost.ru)

Linux RU-JSCIOT (29182) Moscow, Russia
email remote-access file-sharing

| Port | Protocol | Service | Ports |
|-----------|----------|----------|-----------|
| 21/FTP | SSH | 22/SSH | 25/SMTP |
| 110/POP3 | IMAP | 143/IMAP | 443/HTTP |
| 993/IMAP | POP3 | 995/POP3 | 2525/SMTP |
| 53/DNS | | | 80/HTTP |
| 465/SMTP | | | 587/SMTP |
| 8083/HTTP | | | |

DEMO su HLTV.org

Questo sito rappresenta il punto di riferimento globale per monitorare le classifiche dei migliori giocatori impegnati negli e-sports competitivi.

Come vedremo è protetto da un CDN.

The screenshot shows the HLTV.org homepage. At the top left, there's a sidebar with "RANKING BY" and "EVENTS". The main content area features a "Player of the week" section for Djoko with a rating of 1.44. Below it is a "THUNDERPICK" section showing BOSS at 7.00 and Liquid at 1.06. The central part of the page displays the "PGL CS2 Major Copenhagen 2024 Americas RMR" tournament, with tabs for Overview, Matches, Results, and Stats. A large banner for the tournament is present. On the right side, there's a "TODAY'S MATCHES" list and a "RECENT ACTIVITY" sidebar. The "RECENT ACTIVITY" sidebar lists various esports-related events and comments from users like saffee and NEKIZ.

AWARD BY 1XBET

Djoko
Player of the week

1.44 Rating

THUNDERPICK

BOSS 7.00

Liquid 1.06

RANKING BY 1XBET

1. FaZe

2. Vitality

3. Spirit

4. MOUZ

5. Natus Vincere

Complete ranking Last updated: 26th of Feb

EVENTS

PGL Major AM RMR

HLTV

AWARD BY 1XBET

Djoko
Player of the week

1.44 Rating

THUNDERPICK

BOSS 7.00

Liquid 1.06

RANKING BY 1XBET

1. FaZe

2. Vitality

3. Spirit

4. MOUZ

5. Natus Vincere

Complete ranking Last updated: 26th of Feb

EVENTS

PGL Major AM RMR

PGL RMR 2024

PGL CS2 Major Copenhagen 2024 Americas RMR

Overview Matches Results Stats

LIVE

ASTRALIS SIGN BRO AS DEVICE TAKES OVER AS IGL

LIVE: PGL Major Americas RMR

saffee: "We have to keep our feet on the ground" 11 minutes ago 12 comments

Today's news

NEKIZ: "Brazilian teams try to be the best in Brazil, not in the world; it doesn't help the scene" an hour ago 28 comments

Grayhound cease operations after Major failure 3 hours ago 132 comments

Sonic: "Once M80 came to fruition, a lot of teams in NA popped up and put in the work" 10 hours ago 27 comments

EURIA and Complexity to square off for Major

TODAY'S MATCHES

fnatic 9 (0)

Preasy 11 (0)

Metizport 12 (0)

ECLOT 10 (0)

FTW 15:00

Rhyno

BOSS 17:00

Liquid

M80 17:00

Wildcard

Sangal 17:00

Rebels

BetBoom 18:00

Sprout

Preasy 18:00

ex-ENEIDA

fnatic 18:00

GODSENT

ECSTATIC 18:00

SINNERS

KOI 18:00

The Chosen F...

TSM 18:00

Nexus

ILIN 18:00

9INE

RUSH B 18:00

RECENT ACTIVITY

Grayhound cease o... 132

some highlights 9

fnatic vs Preasy 62

proof that Pimp is goat 3

Live Draft BLAST 4

Poland Tragedy High ... 66

Metizport vs ECLOT 32

Indian Men 76

s1mple before/after 11

SPUNJ new project 39

Great job volvo 79

knife + glove combo 137

NEKIZ: "Brazilian tea... 28

ECSTATIC vs Monte 58

zywoo weeb??? 121

liquid out today? 21

LaLiga racist issues 173

India 158

Got something huge ... 36

New hobby 56

TOP 30 TRANSFERS

Try Pitch

Quali NameServer gestiscono questo Dominio?

Con nslookup è possibile controllare quali DNS server risolvono il nome hltv.org

Notare che gli indirizzi restituiti fanno parte del blocco ipv4 assegnato a CLOUDFLARE.

```
$ nslookup hltv.org
Server: 10.0.0.1
Address: 10.0.0.1#53

Non-authoritative answer:
Name: hltv.org
Address: 172.64.146.44
Name: hltv.org
Address: 104.18.41.212
```

Con dnsrecon invece si ottengono più informazioni su questi DNS server che confermano il fatto che il dominio sia protetto da CLOUDFLARE.

```
$ dnsrecon -d hltv.org
[*] Performing General Enumeration of Domain: hltv.org
[!] Wildcard resolution is enabled on this domain
[!] It is resolving to 148.251.125.51
[!] All queries will resolve to this address!!
[-] DNSSEC is not configured for hltv.org
[*] SOA edna.ns.cloudflare.com 173.245.58.109
[*] SOA edna.ns.cloudflare.com 108.162.192.109
[*] SOA edna.ns.cloudflare.com 172.64.32.109
[*] NS jack.ns.cloudflare.com 173.245.59.121
[-] Recursion enabled on NS Server 173.245.59.121 in thi
```

Chi gestiva HLTV.org prima di CLOUDFLARE?

Adesso che si sa che il dominio è protetto da CLOUDFLARE, utilizzando History di ViewDNS è possibile sapere a quali vendor era assegnato il dominio e con quale indirizzo IPv4.

Prima di utilizzare CLOUDFLARE nel 2013 il dominio era legato ad Hetzer Online GmbH, ovvero un operatore di data center specializzato nel gaming e negli e-sports.

| | | | |
|-----------------|--------------------|---------------------|------------|
| 162.159.241.196 | Unknown | Cloudflare, Inc | 2014-10-29 |
| 162.159.240.196 | Unknown | Cloudflare, Inc | 2014-10-29 |
| 162.159.241.196 | Unknown | Cloudflare, Inc | 2014-10-28 |
| 162.159.240.196 | Unknown | Cloudflare, Inc | 2014-10-28 |
| 144.76.157.147 | Solingen - Germany | Hetzner Online GmbH | 2014-10-02 |
| 162.159.240.196 | Unknown | Cloudflare, Inc | 2014-10-01 |
| 141.101.125.220 | Unknown | Cloudflare, Inc | 2014-01-08 |
| 144.76.157.147 | Solingen - Germany | Hetzner Online GmbH | 2013-11-20 |
| 141.101.125.220 | Unknown | Cloudflare, Inc | 2013-11-17 |
| 141.101.116.103 | Unknown | Cloudflare, Inc | 2013-09-29 |
| 144.76.157.147 | Solingen - Germany | Hetzner Online GmbH | 2013-09-23 |
| 88.198.27.51 | Germany | Hetzner Online GmbH | 2013-09-21 |
| 78.46.22.209 | Germany | Hetzner Online GmbH | 2012-08-18 |

Integriamo con Censys e Shodan

Cercando su Internet è possibile conoscere l' Autonomous System di HETZNER così da raffinare le nostre query su Censys e Shodan. AS (24940) I risultati restituiti sono diversi ma entrambi hanno un host in comune su cui è possibile concentrarci:

213.239.193.16

Questo host sembra essere un SMTP server che appartiene alla rete di HETZNER e riceve tutte le mail inviate dal dominio web6.hltv.org.

Si sa quindi che l'host potrebbe appartenere alla stessa rete del web server origine.

Host Filters
Labels:
7 remote-access
2 default-landing-page
2 email
2 login-page
1 database
More
Autonomous System:
9 HETZNER-AS
Location:
8 Germany
1 Finland
Service Filters
Service Names:
12 HTTP
7 SSH
2 NTP
2 SMTP
1 MySQL
More

Hosts
Results: 9 Time: 0.32s

- 148.251.125.51 (static.51.125.251.148.clients.your-server.de)**
Linux HETZNER-AS (24940) Saxony, Germany
remote-access email
22/SSH 25/SMTP 80/HTTP
- 213.239.193.16 (static.213-239-193-16.clients.your-server.de)**
Debian Linux HETZNER-AS (24940) Saxony, Germany
email
25/SMTP 123/NTP
- 5.9.158.200 (greenfield.hltv.org)**
Linux HETZNER-AS (24940) Saxony, Germany
remote-access
22/SSH 80/HTTP
- 136.243.53.2 (static.2.53.243.136.clients.your-server.de)**
Debian Linux 8.0 HETZNER-AS (24940) Saxony, Germany
database remote-access
22/SSH 3306/MySQL

TOTAL RESULTS
3

TOP PORTS
25 2
443 1

TOP ORGANIZATIONS
Hetzner Online AG 1
Hetzner Online GmbH 1
M-net Telekommunikations G... 1

View Report View on Map

Access Granted: Want to get more out of your existing Shodan account? Check out [everything you have access to](#).

213.239.193.16
static.213-239-193-16.clients.your-server.de
Hetzner Online AG
Germany, Falkenstein
starttls self-signed

SSL Certificate
Issued By:
- Common Name: web6.hltv.org
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
Supported SSL
Versions:
SSLv3, TLSv1,
TLSv1.1, TLSv1.2

93.104.116.53
ppp-93-104-116-53.dynamic.mnet-online.de
M-net Telekommunikations GmbH
Germany, Munich
self-signed

SSL Certificate
Issued By:
- Common Name: Zoraxy Self-host
X-Proxy-By: zoraxy/3.0.0
Date: Mon, 26 Feb 2024 20:34:42 GMT
Content-Length: 52

Quale è il probabile blocco IPv4 del server web origine?

Su Internet è sempre possibile consultare i blocchi Ipv4 assegnati alle varie organizzazioni.

Nel nostro caso basta consultare quelli assegnati a HETZNER Online GmbH.

Tramite l'host trovato in precedenza è possibile controllare a quale dei blocchi assegnati esso appartiene.

E quindi →

| | | |
|----------------------------------|---|--------|
| 213.239.192.0/18 |  Hetzner Online GmbH | 16,384 |
|----------------------------------|---|--------|

è la rete che cercavamo, e contiene solo 16,384 host

Quale è il server web origine?

Disponiamo di una rete comprendente 16.384 host, tra cui potrebbe essere presente il server web che stiamo cercando. Utilizzando lo strumento `real_ip_discover.py`, possiamo verificare se nella rete ci sono host con le porte HTTP o HTTPS aperte e se il loro contenuto corrisponde a una stringa che abbiamo specificato.

Possiamo specificare il dominio da cercare nell'URL, la sottorete su cui condurre la ricerca e la stringa da confrontare. Nel nostro scenario, la stringa da cercare è "HLTV.org", presunta essere contenuta nel campo `<title>` della risposta HTML.

Visto che il tool accetta solo sottoreti da massimo 256 host si deve suddividere la ricerca in più iterazioni.

Quando si arriva alla sottorete **213.239.228.0/24**

l'output del tool trova un match con l'host:

213.239.228.130

```
$ python3 real_ip_discover.py "www.hltv.org" 213.239.228.0/24 "HLTV.org" -t50
Not Found
1:476fec7849af8d574ea4dbace7d5cb2fab08329
V... The search space is composed of 256 subnets, each containing 2^12 hosts.
Efrén Diaz @elefr3n

[[![[HLTV.org]](/img/static/TopSmallLogo2x.png)]()]
Host: www.hltv.org [Results] [/results] [Events] [/events]
IPv4: 213.239.228.0/24 (256 addresses) (512 requests)
Match: HLTV.org
Uri: /
Threads: 50 [/img/static/TopSmallLogo2x.png]]()
Timeout: 3 [matches] [Results] [/results]

13:46:32: STARTING ...
13:47:00: http request to 213.239.228.130 matchs (191kb)
Events [/events] check it: "curl -H 'Host: www.hltv.org' http://213.239.228.130/ -k"
13:47:10: FINISHED WITH 1 MATCHES
* [ All events ] [/events]
```

Abbiamo trovato l' IP del Web Server Origine!

```
$ curl -H 'Host: www.hltv.org' http://213.239.228.130/ -k | head -n 35
% Total    % Received % Xferd  Average Speed   Time     Time   Current
          Dload  Upload   Total   Spent    Left  Speed
0       0     0      0      0      0 --:--:-- --:--:-- 0<!DOCTYPE html>
<html lang="en" data-client-country-iso="" data-ads-api-url="https://www.hltv.org/api/ads/rendered/[%7B%22key%22:%7B%22id%22:%22page%22%7D,%22value%22:%7B%22id%22:%22Front%22%7D%7D]" data-ad-rewriter-version="1" data-bc-content-allowed="true" data-impression-tracking-endpoint="https://ncuxt.hltv.org">
<head>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1" id="metaViewport">
  <meta property="fb:admins" content="1004164229">
  <meta property="fb:pages" content="249997999009">
  <meta property="fb:app_id" content="1460388157605817">
  <meta name="google-site-verification" content="DcypRFLQvgYQL5Acx7feoGWbbLSsmKv6HpPI7mM_1uw">
  <meta name="google-site-verification" content="50triQwtVytxCNrtDRVt0gtjmAN81BJ9Z6ZLLCXEYwQ">
  <meta name="yandex-verification" content="00ed04feb3ede037">
  <link rel="apple-touch-icon" sizes="180×180" href="/img/static/favicon/apple-touch-icon.png">
  <link rel="icon" type="image/png" sizes="32×32" href="/img/static/favicon/favicon-32×32.png">
  <link rel="icon" type="image/png" sizes="16×16" href="/img/static/favicon/favicon-16×16.png">
  <link rel="manifest" href="/img/static/favicon/manifest.json">
  <link rel="mask-icon" href="/img/static/favicon/safari-pinned-tab.svg" color="#5bbad5">
  <meta name="theme-color" content="#ffffff">
  <link href="https://fonts.googleapis.com/css?family=Open+Sans:400,400i,700,700i|Oswald:700&subset=latin-ext" rel="stylesheet">
  <link rel="stylesheet" href="/vendor/font-awesome-4.7.0/css/font-awesome.min.css" type="text/css">
  <script type="text/javascript" src="/scripts/hltv-csstheme.js?hash=d7f7aa3242d687f1bd5fd5865c277983" data-day-css="163138b6eefeb96c023a49c1c3879e9d" data-night-css="4a45fc1c
c26f3163522f7c817c75679b"></script>
  <script type="text/javascript" src="/scripts/hltv.js?hash=38d8c8a70a9bc7f9e3e4f7ec413f9f25"></script>
  <script type="text/javascript" src="/js/ht.js" data-domain="hltv.org" data-api="/ht/event" defer="defer"></script>
  <title>Counter-Strike News & Coverage | HLTV.org</title>
  <meta name="description" content="Welcome to the leading Counter-Strike site in the world, featuring news, demos, pictures, statistics, on-site coverage and much much more!">
  <meta property="og:title" content="HLTV.org – The home of competitive Counter-Strike">
  <meta property="og:image" content="https://www.hltv.org/img/static/openGraphHltvLogo.png">
  <meta property="og:site_name" content="HLTV.org">
  <script type="application/ld+json">{
    "@context": "http://schema.org",
    "@type": "Organization",
    "name": "HLTV.org",
    "url": "https://www.hltv.org/",
    "description": "Welcome to the leading Counter-Strike site in the world, featuring news, demos, pictures, statistics, on-site coverage and much much more!",
    "parentOrganization": "Better Collective A/S",
    "sameAs": [
      "https://www.hltv.org"
    ]
  </script>
100 7025      0 7025      0 108k      0 --:--:-- --:--:-- --:--:-- 110k
curl: (23) Failure writing output to destination
```

→ 213.239.228.130

Fonti

- <https://infosecwriteups.com/find-real-website-ip-bruteforcing-ipv4-ranges-c1e9ab2941e7>
- <https://www.zenrows.com/blog/bypass-cloudflare#calling-origin-server>
- <https://blog.christophetd.fr/bypassing-cloudflare-using-internet-wide-scan-data/>
- <https://blog.cloudflare.com/ddos-prevention-protecting-the-origin/>

Fine

Lorenzo Fallani

Pitch

**Want to make a presentation
like this one?**

Start with a fully customizable template, create a beautiful deck in minutes, then easily share it with anyone.

[Create a presentation \(It's free\)](#)