

Threat Hunting

HW05

Name: 劉定睿 ID: M11409313

Date: 2025-10-19

目錄

- [目錄](#)
 - [whois](#)
 - [DNS](#)
 - [Certificate Transparency](#)
 - [NameDroppers](#)
 - [Whoisology](#)
 - [Wayback Machine](#)

whois

First of all, I use `whois` to check the information of this domain name. The information shows that this domain is host in cloudflare server. So I can't obtain the correct information of the personal and server.

```
└─$ whois flockfilmseries.com
Domain Name: FLOCKFILMSERIES.COM
Registry Domain ID: 1851414881_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.cloudflare.com
Registrar URL: http://www.cloudflare.com
Updated Date: 2024-09-11T16:44:22Z
Creation Date: 2014-03-21T16:31:24Z
Registry Expiry Date: 2026-03-21T16:31:24Z
Registrar: Cloudflare, Inc.
Registrar IANA ID: 1910
Registrar Abuse Contact Email: registrar-abuse@cloudflare.com
Registrar Abuse Contact Phone: +1.6503198930
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: DAMON.NS.CLOUDFLARE.COM
Name Server: ZELDA.NS.CLOUDFLARE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-10-18T07:00:20Z <<<
```

DNS

Use `dig` command digging into DNS Record.

```
└─$ dig flockfilmseries.com

; <<>> DiG 9.20.11-4+b1-Debian <<>> flockfilmseries.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23275
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;flockfilmseries.com.      IN      A

;; ANSWER SECTION:
flockfilmseries.com.      377     IN      A       104.21.31.199
flockfilmseries.com.      377     IN      A       172.67.179.168

;; Query time: 99 msec
;; SERVER: 10.255.255.254#53(10.255.255.254) (UDP)
;; WHEN: Sat Oct 18 15:01:12 CST 2025
;; MSG SIZE rcvd: 80
```

Then I check the DNS record via `dnsdumpster`.

A Records (subdomains from dataset)

Host	IP	ASN	ASN Name	Open Services (from DB)	RevIP
flockfilmseries.com	172.67.179.168	ASN: 13335 172.67.176.0/20	CLOUDFLARENET	http: cloudflare title: Direct IP access not allowed tech: Cloudflare http8080: cloudflare title: Direct IP access not allowed tech: Cloudflare	708
flockfilmseries.com	104.21.31.199	ASN: 13335 104.21.16.0/20	CLOUDFLARENET	http: cloudflare title: Direct IP access not allowed tech: Cloudflare http8080: cloudflare title: Direct IP access not allowed tech: Cloudflare	664

MX Records

Host	IP	ASN	ASN Name	Open Services (from DB)	RevIP
0 flockfilmseries-com.mail.protection.outlook.com	52.101.41.0	ASN: 8075 52.96.0.0/12	MICROSOFT-CORP-MSN-AS-BLOCK United States		

NS Records




Host	IP	ASN	ASN Name	Open Services (from DB)	RevIP
damon.ns.cloudflare.com	173.245.59.96	ASN: 13335 173.245.59.0/24	CLOUDFLARENET	http: cloudflare title: Direct IP access not allowed tech: Cloudflare http8080: cloudflare title: Direct IP access not allowed tech: Cloudflare	
zelda.ns.cloudflare.com	173.245.58.242	ASN: 13335 173.245.58.0/24	CLOUDFLARENET	http: cloudflare title: Direct IP access not allowed tech: Cloudflare http8080: cloudflare title: Direct IP access not allowed tech: Cloudflare	

TXT Records

"v=spf1 ip4:198.246.200.0/24 ip4:66.119.29.0/26 include:spf.protection.outlook.com -all"

Certificate Transparency

After that. I search the certificate transparency record data via `crt.sh`.

crt.sh Identity Search    [Group by Issuer](#)

Criteria Type: Identity Match: ILIKE Search: 'flockfilmseries.com'

Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
	21568190592	2025-10-08	2025-10-08	2026-01-06	flockfilmseries.com	*.flockfilmseries.com flockfilmseries.com	C=US,O=Google Trust Services,CN=WE1
	21073029211	2025-09-17	2025-09-17	2025-12-13	flockfilmseries.com	*.flockfilmseries.com flockfilmseries.com	C=GB,O=Sectigo Limited,CN=Sectigo Public Server Authentication CA DV E36
	21073028653	2025-09-17	2025-09-17	2025-12-13	flockfilmseries.com	*.flockfilmseries.com flockfilmseries.com	C=GB,O=Sectigo Limited,CN=Sectigo Public Server Authentication CA DV E36
	20239651171	2025-08-10	2025-08-10	2025-11-08	flockfilmseries.com	*.flockfilmseries.com flockfilmseries.com	C=US,O=Google Trust Services,CN=WE1
	20238593130	2025-08-10	2025-08-10	2025-11-08	flockfilmseries.com	*.flockfilmseries.com flockfilmseries.com	C=US,O=Google Trust Services,CN=WE1
	19653669424	2025-07-14	2025-07-14	2025-10-11	flockfilmseries.com	*.flockfilmseries.com flockfilmseries.com	C=GB,O=Sectigo Limited,CN=Sectigo Public Server Authentication CA DV E36
	19653669208	2025-07-14	2025-07-14	2025-10-11	flockfilmseries.com	*.flockfilmseries.com flockfilmseries.com	C=GB,O=Sectigo Limited,CN=Sectigo Public Server Authentication CA DV E36
	18971344678	2025-06-12	2025-06-12	2025-09-10	flockfilmseries.com	*.flockfilmseries.com flockfilmseries.com	C=US,O=Google Trust Services,CN=WE1
	18970730598	2025-06-12	2025-06-12	2025-09-10	flockfilmseries.com	*.flockfilmseries.com flockfilmseries.com	C=US,O=Google Trust Services,CN=WE1
	18423244857	2025-05-15	2025-05-15	2025-08-13	flockfilmseries.com	*.flockfilmseries.com flockfilmseries.com	C=GB,ST=Greater Manchester,L=Salford,O=Sectigo Limited,CN=Sectigo ECC Domain Validation Secure Server CA
	18423244904	2025-05-15	2025-05-15	2025-08-13	flockfilmseries.com	*.flockfilmseries.com flockfilmseries.com	C=GB,ST=Greater Manchester,L=Salford,O=Sectigo Limited,CN=Sectigo ECC Domain Validation Secure Server CA
	17833311095	2025-04-14	2025-04-14	2025-07-13	flockfilmseries.com	*.flockfilmseries.com flockfilmseries.com	C=US,O=Google Trust Services,CN=WE1

NameDroppers

NameDroppers shows that this Domain name is already expired.

Manage Your Account
How To
Dictionary
Advertise
Embed On Your Site
Business Partnerships
Comments & Questions
Purchase Domain Reports
Monitor Domain Changes

SEARCH and REGISTER Domain Names Quickly and Easily!
All Domain Registrations Using Namedroppers.com® Receive Free Domain Parking !

flockfilmseries **Drop Em!**

Search Parameters (More Options)
 Any Order Exact Order
 com net org edu biz us info name

Purchase Domain:
flockfilmseries
After reviewing your search results to find an available domain name, enter your desired name in the input box above to purchase it.

Registered Domain Names
Matched 1 domain names out of 187,891,579 active records!

1. [WHOIS] flockfilmseries.com

Whoisology

Same as whois. Can't investigate the real IP / Registration information.

Domain, Email, or Keyword

Expanded Advanced Keyword Bulk

flockfilmseries.com

This is Whoisology's most current historical whois lookup for the domain name flockfilmseries.com. Click any of the records below (address, phone, email, etc) to perform a reverse lookup.

Admin Contact		Other Details	
The Admin Contact is the person or organization who controls the domain.		These are technical details & related, connected to the domain.	
Name	DATA REDACTED (2,222,621) Changes: +229,438 ccTLD: 10,314	Registrar Name	Cloudflare, Inc.(2,631,215) Changes: +215,658 ccTLD: 98,233
Org.	DATA REDACTED (2,222,454) Changes: +229,386 ccTLD: 10,313	Created Date	2014-03-21(15,720) Changes: -1,400 ccTLD: 6,753
Email	-	Whois Servers	whois.cloudflare.com(2,376,129) Changes: +160,189 ccTLD: 98,232

Wayback Machine

Check the history of this website. And there's a lot of server-side error between at 2023~2025.

INTERNET ARCHIVE **WayBackMachine** Explore more than 946 billion web pages saved over time

DONATE flockfilmseries.com

Calendar · Collections · Changes · Summary · Site Map · URLs

Saved 28 times between September 27, 2015 and March 17, 2025.

Year	Captures
2002	0
2003	0
2004	0
2005	0
2006	0
2007	0
2008	0
2009	0
2010	0
2011	0
2012	0
2013	0
2014	0
2015	1
2016	2
2017	1
2018	1
2019	1
2020	0
2021	0
2022	0
2023	1
2024	1
2025	28

Calendar view showing captures on Feb 5, May 16, and Mar 17.

Browser address bar: <http://flockfilmseries.com/cgi-sys/defaultwebpage.cgi> | 2 captures | 10 Jan 2019 - 20 Jan 2019

SORRY!

If you are the owner of this website, please contact your hosting provider: webmaster@flockfilmseries.com

It is possible you have reached this page because:

- The IP address has changed.**
The IP address for this domain may have changed recently. Check your DNS settings to verify that the domain is set up correctly. It may take 8-24 hours for DNS changes to propagate. It may be
- There has been a server misconfiguration.**
You must verify that your hosting provider has the correct IP address configured for your Apache settings and DNS records. A restart of Apache may be
- The site may have moved to a different server.**
The URL for this domain may have changed or the hosting provider may have moved the account to a different server.

After checking, this domain/website is in full swing in 2015 to 2016.

Calendar · Collections · Changes · Summary · Site Map · **URLs**

180 URLs have been captured for this URL prefix.

Filter results

URL ↑	MIME Type	From	To	Captures
http://flockfilmseries.com/	text/html	Sep 27, 2015	Mar 17, 2025	20
http://flockfilmseries.com/?p=104	text/html	Apr 22, 2016	Nov 2, 2018	4
http://flockfilmseries.com/?p=12	text/html	Apr 21, 2016	Nov 2, 2018	4
http://flockfilmseries.com/?p=16	text/html	Apr 22, 2016	Nov 2, 2018	3
http://flockfilmseries.com/?p=177	text/html	Apr 22, 2016	Nov 2, 2018	3
http://flockfilmseries.com/?p=189	text/html	Apr 22, 2016	Nov 2, 2018	3
http://flockfilmseries.com/?p=20	text/html	Jul 11, 2016	Jul 11, 2016	1
http://flockfilmseries.com/?p=55	text/html	Apr 21, 2016	Nov 2, 2018	3
http://flockfilmseries.com/?p=57	text/html	Apr 22, 2016	Nov 2, 2018	3
http://flockfilmseries.com/?p=76	text/html	Apr 21, 2016	Nov 2, 2018	3
http://flockfilmseries.com/?p=78	text/html	Apr 22, 2016	Nov 2, 2018	3
http://flockfilmseries.com/?p=81	text/html	Apr 22, 2016	Nov 2, 2018	3
http://flockfilmseries.com/?p=91	text/html	Apr 22, 2016	Nov 2, 2018	3
http://flockfilmseries.com/?p=94	text/html	Apr 21, 2016	Nov 2, 2018	3
http://flockfilmseries.com/?p=98	text/html	Apr 22, 2016	Nov 2, 2018	3
http://flockfilmseries.com/apple-touch-icon-114x114.png	image/png	Mar 7, 2016	Aug 23, 2018	10
http://flockfilmseries.com/apple-touch-icon-120x120.png	image/png	Mar 7, 2016	Aug 23, 2018	10
http://flockfilmseries.com/apple-touch-icon-144x144.png	image/png	Mar 7, 2016	Aug 23, 2018	10
http://flockfilmseries.com/apple-touch-icon-152x152.png	image/png	Mar 7, 2016	Aug 23, 2018	10