



UNLEASHING THE DIGITAL SPY: EXPLORING OFFENSIVE OSINT STRATEGIES



About CyberWarFare Labs

CyberWarFare Labs is an Ed-Tech Cyber Security Focused Platform which is totally engrossed in solving the problem of Cybersecurity by providing them real-time hands-on manner solutions to problems of B2C & B2B Audience.

We provide Practical Labs [Simulation of critical infrastructure] like Healthcare, Nuclear Facility etc.



About Speaker

Abhijeet Kumar
(Security Researcher)

Abhijeet Kumar works at CyberWarFare Labs as a Red Team Intern. His areas of interests includes Red Team Operations, Network Security, Cloud Infrastructure, and Linux Systems. Apart from this, he enjoys researching Adversarial TTPs and experimenting in his homelab.

Disclaimer

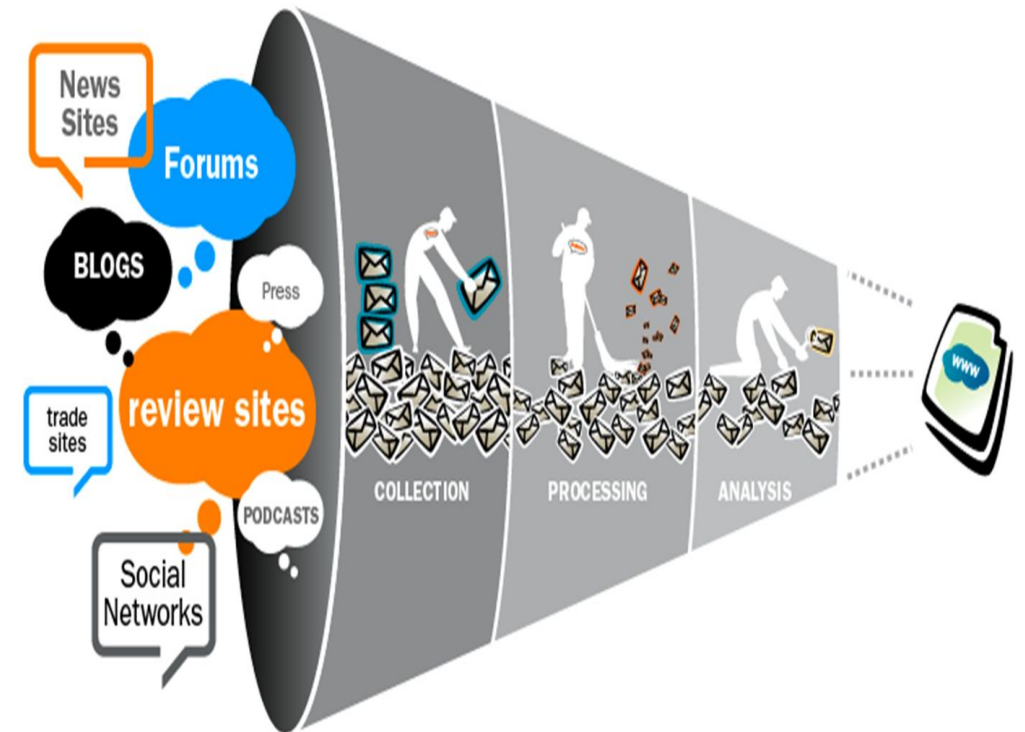
- Be mindful of your local laws
- Make sure to do your due diligence beforehand
- Use the tools and techniques mentioned as your own risk
- We (Speaker and CyberWarFare Labs) are not liable for any damage caused by the presented material(s)

Before we begin

- This is my very first webinar, kindly provide feedback if possible
- I have tried my hands on PowerPoint after a long time, do pardon my rusty skills
- Also not a native English speaker, please bear with me

What is OSINT?

- Stands for Open Source **Intelligence**
- Extracting **actionable intel** from publicly available sources



Why OSINT?

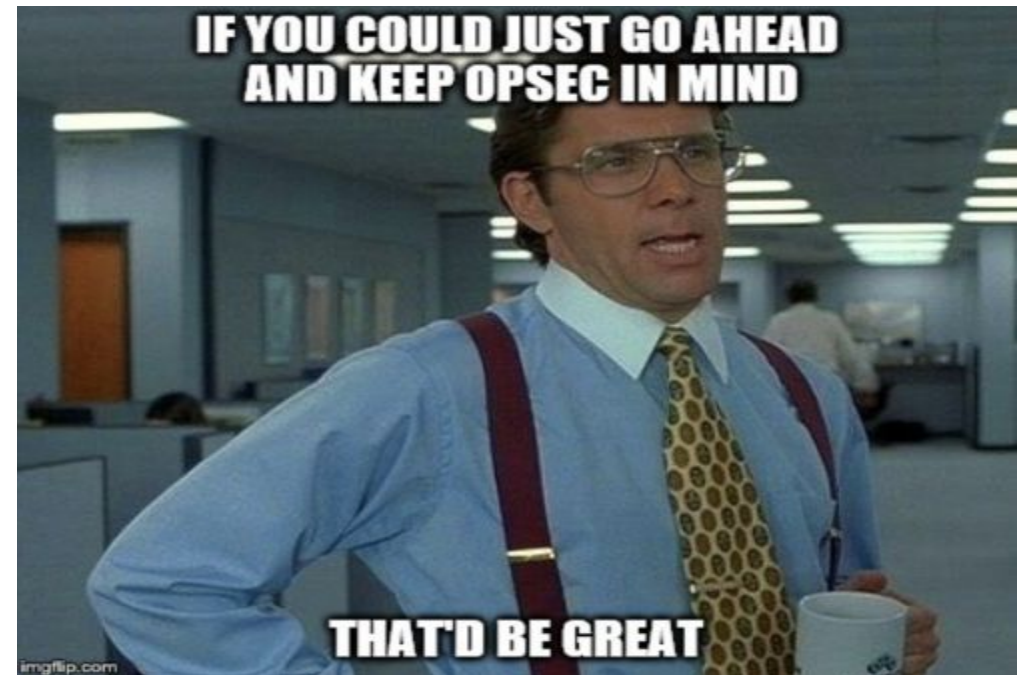
- People love to share details online, sometimes too much
- Governments and other institutions make data available online
- Helps connect dots between data points
- It would be a shame not to use Internet properly

What to watch out for?

- Misinformation is a real thing, verify before trust
- Always double (or triple) check facts
- Use **multiple sources** to verify something, don't rely on just one

OPSEC

- Stands for Operational security
- Protecting internal operations and critical information
- Preventing disclosure of unnecessary information



Device

- **Don't** use personal device for OSINT, use a **seperate** one
- Encrypt the drives and harden the OS
- Implement anti-tampering measures



One for the wenches and one for the dough

VPN

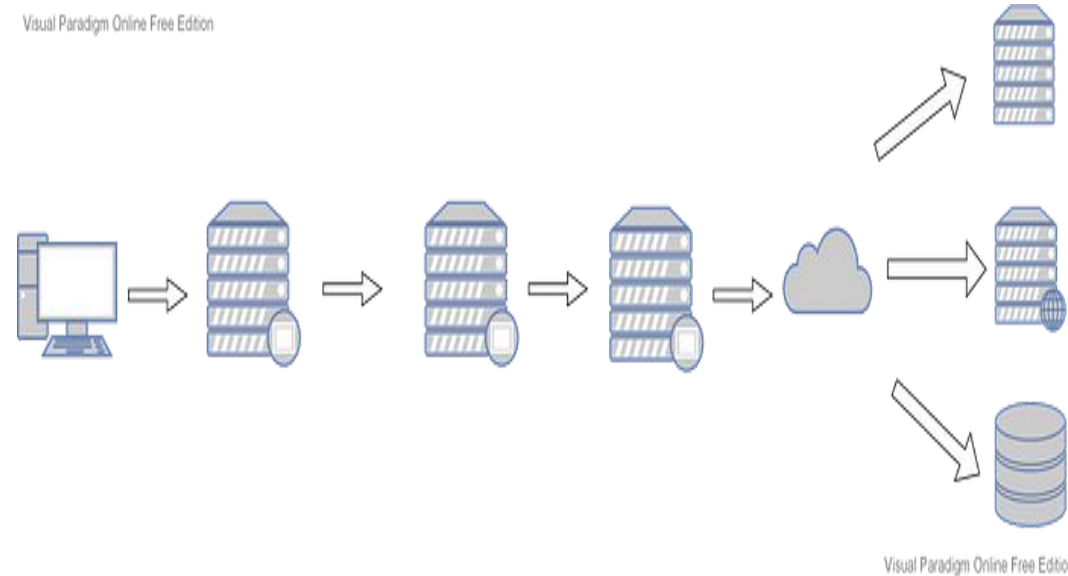
- Stands for Virtual Private Network
- Creates an encrypted tunnel between user and VPN server
- Masks user's domestic IP address



Client → ISP → VPN Server → Internet → Different Servers

TOR

- Stands for The Onion Router
- Routes user traffic between different tor nodes
- Can help user evade tracking to some extent



Client → TOR entry node → TOR middle node → TOR exit node →
Internet → Different servers

VPN + TOR


- Best of both worlds
- Combining both technologies can be more effective
- **Start VPN → Connect TOR → Browse Internet**



Browser(s)

- Customizing browser(s) for investigation purposes
- Disabling telemetry, stopping trackers, isolating cookies
- Hardening security configurations and normalize fingerprint
- Firefox, TOR, and Brave are well suited for research purposes

Tab Containers



By Firefox

270,547 Users
5,659 Reviews
4.6 Stars

5 ★
4 ★
3 ★
2 ★
1 ★

Firefox Multi-Account Containers lets you keep parts of your online life separated into color-coded tabs that preserve your privacy. Cookies are separated by container, allowing you to use the web with multiple identities or accounts simultaneously.

Add to Firefox

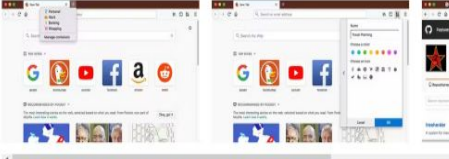
Rate your experience

How are you enjoying Firefox Multi-Account Containers?

Log in to rate this extension

Report this add-on for abuse

Screenshots




Multi-Account Containers

- Apri nuova scheda in...
- Riapri questo sito in...
- Ordina schede per contenitore
- Apri sempre questo sito in...

Contenitori

Personal	1	>
Work	1	>
Banking	1	>
Shopping	1	>
Facebook		>

Gestisci contenitori



Open this site in your assigned container?

You asked Firefox to always open **Test** for this site:

<https://www.mozilla.org/>

Would you still like to open in this current container?

☒ Remember my decision for this site

Open in **Current** Container

Open in **Test** Container

User Agent Changer

Firefox Browser ADD-ONS Explore Extensions Themes More...

Find add-ons

User-Agent Switcher and Manager by Ray

66,162 Users 325 Reviews 4.3 Stars

Recommended

5 stars 271
4 stars 53
3 stars 25
2 stars 16
1 star 30

Spooft websites trying to gather information about your web navigation—like your browser type and operating system—to deliver distinct content you may not want.

+ Add to Firefox

Rate your experience

How are you enjoying User-Agent Switcher and Manager?

Log in to rate this extension

Report this add-on for abuse

Screenshots

User-Agent Switcher

What's My User Agent? - UserAgent Switcher (enabled)

User-Agent String: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0

What's My User Agent?

Your User Agent is:

Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0

Your IP Address is:

49.213.19.59

Browser Information:

JavaScript Enabled: Yes

Cookies Enabled: Yes

Device Pixel Ratio: 1

Screen Resolution: 2560px x 1080px

We earn a referral fee when you buy services from many of the hosts on our site. Learn more...

Browser	OS	User-Agent String
<input type="radio"/> Firefox 56.0	Windows 10	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0
<input type="radio"/> Firefox 55.0	Windows 10	Mozilla/5.0 (Windows NT 10.0; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0
<input type="radio"/> Firefox 55.0	Windows 10	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:55.0) Gecko/20100101 Firefox/55.0
<input type="radio"/> Firefox 55.0	Windows 7	Mozilla/5.0 (Windows NT 6.1; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0
<input type="radio"/> Firefox 55.0	Windows 7	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:55.0) Gecko/20100101 Firefox/55.0
<input type="radio"/> Firefox 55.0	Windows 7	Mozilla/5.0 (Windows NT 6.1; rv:55.0) Gecko/20100101 Firefox/55.0
<input type="radio"/> Firefox 55.0	Windows 8.1	Mozilla/5.0 (Windows NT 6.3; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0
<input type="radio"/> Firefox 54.0	Windows 10	Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0
<input type="radio"/> Firefox 54.0	Windows 7	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:54.0) Gecko/20100101 Firefox/54.0

Filter

User-Agent String: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0

Apply Reset

Sock Puppet

- Identities made solely for investigation
- Comprised of fake details
- Help protect real individual
- Reduces attack surface



Using Sock Puppet

- Aim is to blend with regular traffic/users
- Disposable email addresses and phone numbers
- Different devices, browsers, and ISPs

*“All human actions have one or more of these seven causes: **chance, nature, compulsion, habit, reason, passion, and desire.**”*

— Aristotle

Intro to Offensive OSINT

- Using OSINT to identify relevant information for pentesting and red team activities
- Analyzing client's online presence thoroughly, in order to identify weakness (human or otherwise)
- Thinking like an adversary while determining relevance of information

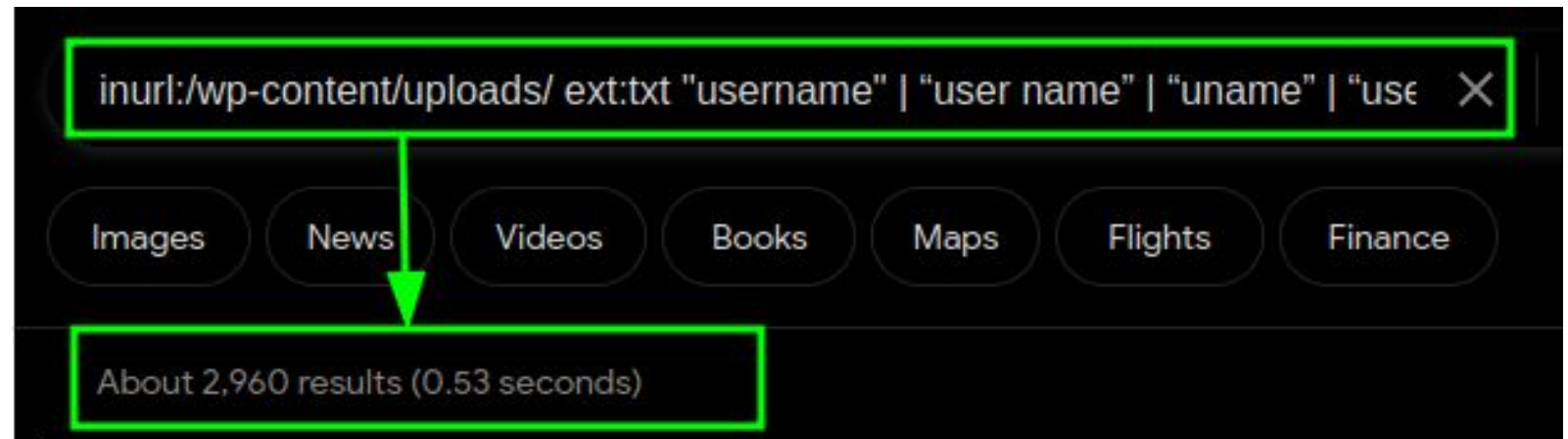
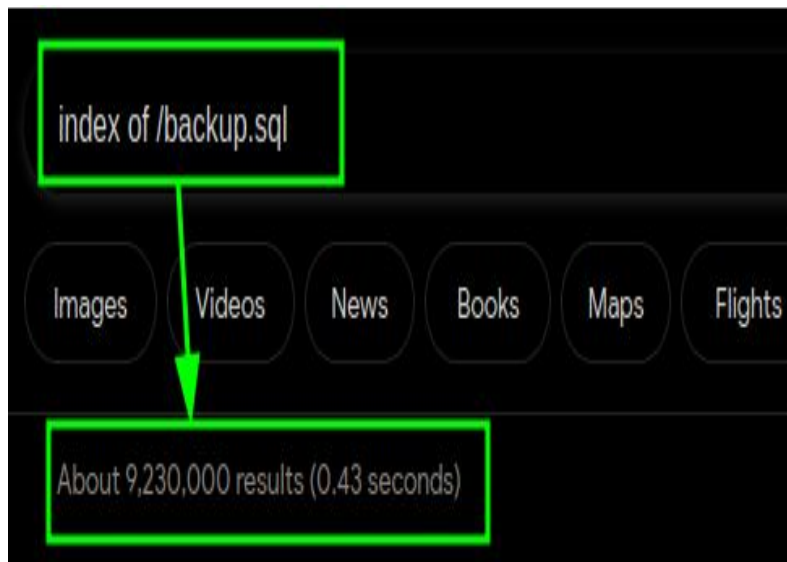
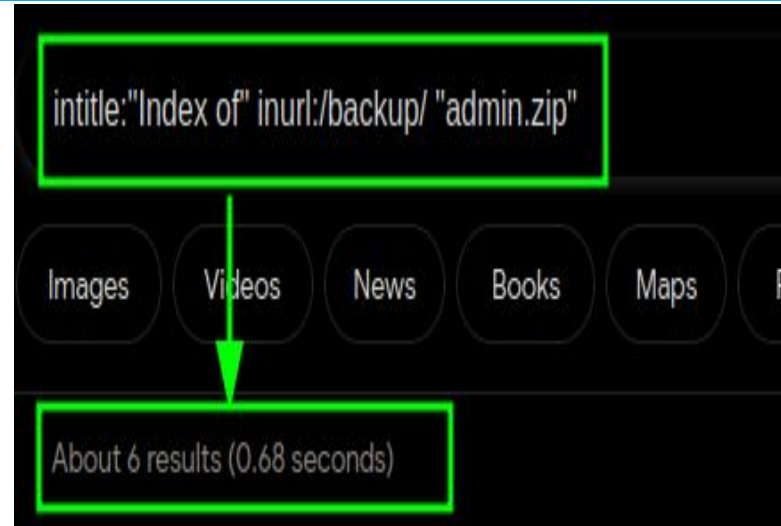
Data Breaches

- Scenario when sensitive data is exfiltrated from an organization by threat actors
- Lots and lots of sensitive information related to users and organization
- Dark web marketplaces are where distribution and sale happens



Google Dorking

- Extracting information using Google's powerful search operators
- From simple few word queries to complex piped (|) queries
- **Google Hacking Database (GHDB)** is one of the largest collection of publicly available queries



LinkedIn

- Professional version of FaceBook
- High chances of target(s) having a regular presence here
- Has suffered data breaches in past
- Excellent platform for mining data





- Employee list can be extracted from company page
- Employees sometimes reveal sensitive information on LinkedIn
 - E.g:- Office images, tech stack(s), welcome kits, certificates, etc
- Employees often comment on each other's posts.
- And **#hashtags** are a thing



[Home](#) [My Network](#) [Jobs](#) [Messaging](#) [Notificati](#)



ENHANCE CYBER SECURITY SKILLS WITH
CYBERWARFARE LABS
A REAL WORLD ADVERSARY SIMULATION LAB



CyberWarFare Labs
A Real World Adversary Simulated Lab
Computer and Network Security · Bengaluru, Karnataka · 7,319 followers · 7 employees

[+ Follow](#) [Register](#) [More](#)

[Home](#) [About](#) [Posts](#) [Jobs](#) [People](#) [Events](#)

7 employees

Where they live + Add

7 | India

4 | Karnataka, India

Where they studied + Add

1 | Arena Animation

1 | First Step School

[Home](#) [About](#) [Posts](#) [Jobs](#) [People](#) [Events](#)

2 employees

Python X

[Clear all](#)

Where they live + Add

2 | Karnataka, India

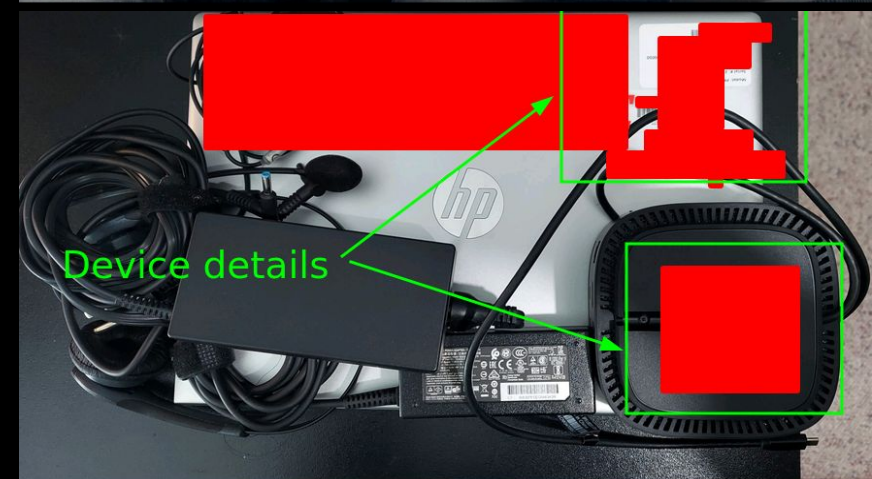
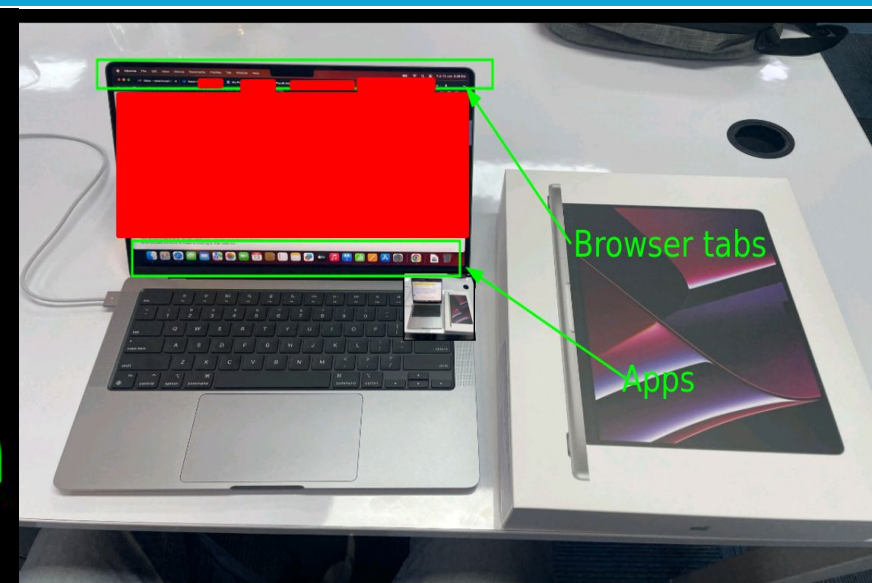
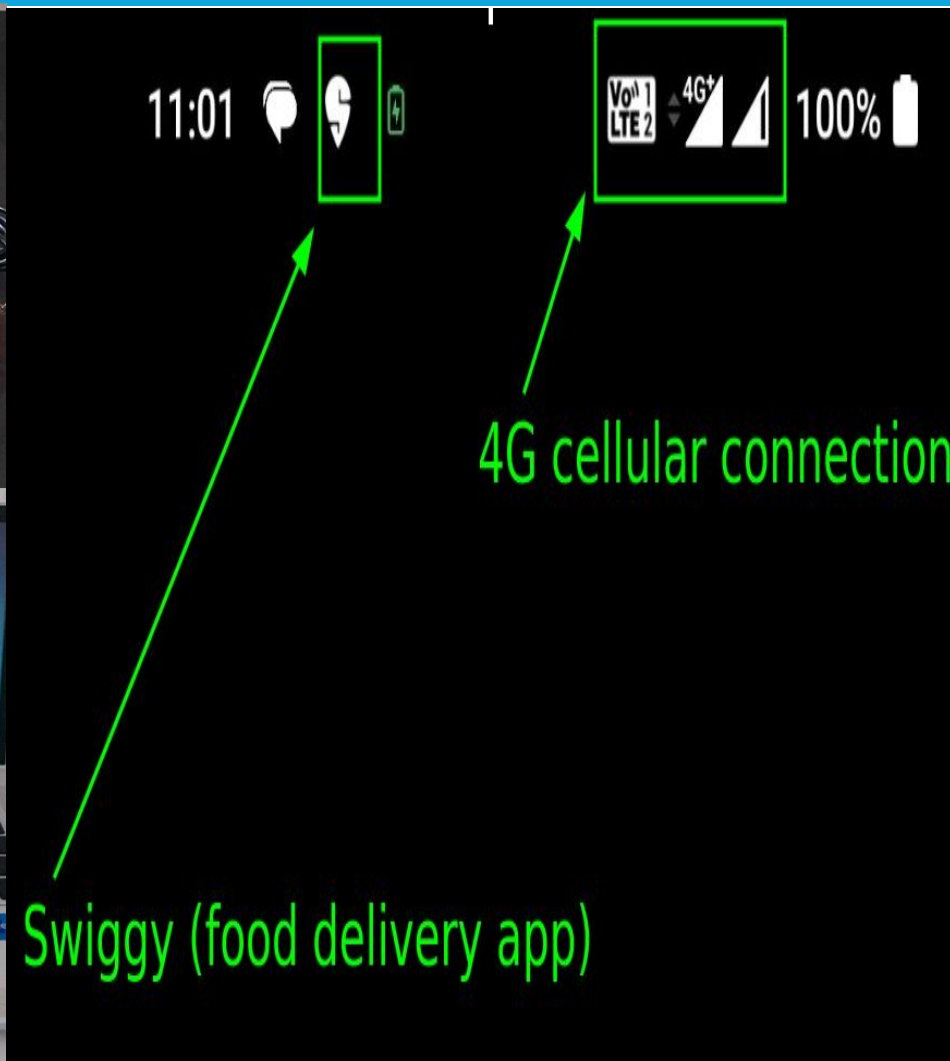
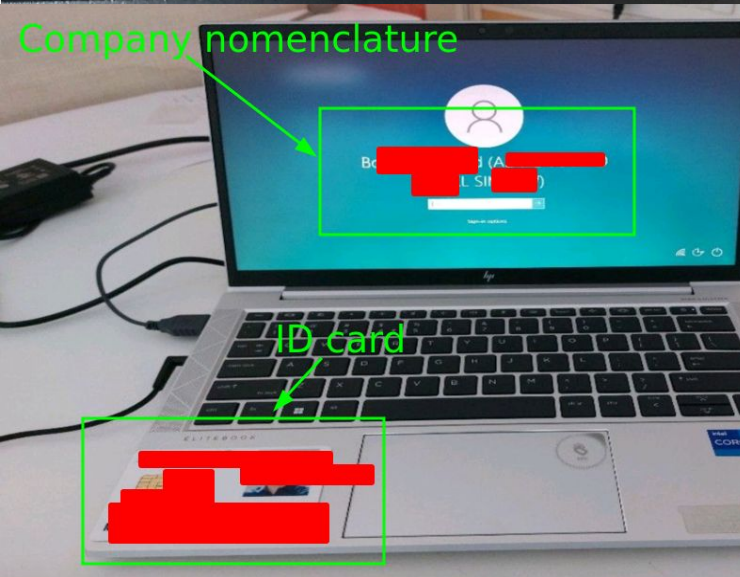
2 | India

2 | Bengaluru

2 | Greater Bengaluru Area

Where they studied + Add

1 | REVA University



Discord

- Popular communication application
- Used by lots of tech communities and individuals alike
- People also **connect** their **other accounts** here
- And, they write status too

LISTENING TO SPOTIFY



Showdown
by Jonathan Belle
on Cruising in the Grid

0:00

Play on

CONNECTIONS



CONNECTIONS



CONNECTIONS



Member since
Tweets Followers

CONNECTIONS



CONNECTIONS



Member since
3 Games

Followers Following Likes

WHOIS

- Query-Response protocol
- Can lookup domain names and IP addresses, and ASNs
- Provides ownership and other registration data



cyberwarfare.live

whois information

- Whois
- DNS Records
- Diagnostics

cache expires in 23 hours, 59 minutes and 59 seconds

Registrar Info

Name	GoDaddy.com, LLC
Whois Server	whois.godaddy.com/
Referral URL	http://www.godaddy.com/domains/search.aspx?ci=8990
Status	clientDeleteProhibited https://icann.org/epp#clientDeleteP clientRenewProhibited https://icann.org/epp#clientRenew clientTransferProhibited https://icann.org/epp#clientTransf clientUpdateProhibited https://icann.org/epp#clientUpdate

Important Dates

Expires On	2024-04-26
Registered On	2020-04-26
Updated On	2022-04-05

Name Servers

jermaine.ns.cloudflare.com	172.64.35.157
joyce.ns.cloudflare.com	162.159.38.14

Registrant Contact Information:

Name	REDACTED FOR PRIVACY
Organization	Domains By Proxy, LLC
Address	REDACTED FOR PRIVACY
City	REDACTED FOR PRIVACY
State / Province	Arizona
Postal Code	REDACTED FOR PRIVACY
Country	US
Phone	REDACTED FOR PRIVACY
Fax	REDACTED FOR PRIVACY
Email	Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Reg.

Administrative Contact Information:

Name	REDACTED FOR PRIVACY
Organization	Domains By Proxy, LLC
Address	REDACTED FOR PRIVACY
City	REDACTED FOR PRIVACY
State / Province	Arizona
Postal Code	REDACTED FOR PRIVACY
Country	US
Phone	REDACTED FOR PRIVACY
Fax	REDACTED FOR PRIVACY
Email	Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Reg.

Technical Contact Information:

Name	REDACTED FOR PRIVACY
Organization	Domains By Proxy, LLC
Address	REDACTED FOR PRIVACY
City	REDACTED FOR PRIVACY
State / Province	Arizona
Postal Code	REDACTED FOR PRIVACY
Country	US
Phone	REDACTED FOR PRIVACY
Fax	REDACTED FOR PRIVACY
Email	Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Reg.

Subdomains

- Provide additional targets
- Often act as an initial entry point
- Could be used for integrating third party services



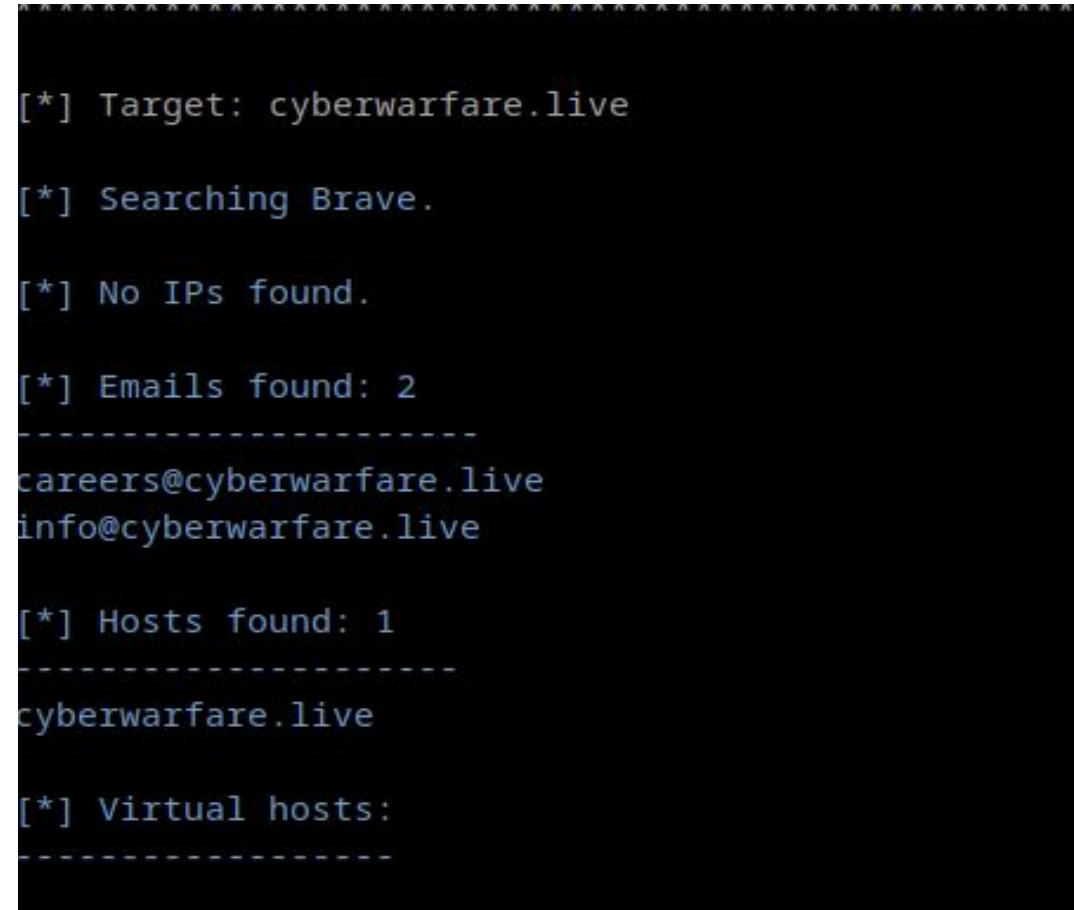
crt.sh Identity Search



Group by Issuer

Criteria Type: Identity Match: ILIKE Search: 'cyberwarfare.live'

	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
	9638350347	2023-06-12	2023-06-12	2023-09-10	cyberwarfare.live	*.cyberwarfare.live cyberwarfare.live	G=US, O=Google Trust Services LLC, CN=GTS CA 1P5
	9591730791	2023-06-05	2023-06-05	2023-09-03	air.cyberwarfare.live	air.cyberwarfare.live	G=US, O=Let's Encrypt, CN=R3
	9576289007	2023-06-05	2023-06-05	2023-09-03	air.cyberwarfare.live	air.cyberwarfare.live	G=US, O=Let's Encrypt, CN=R3
	9345352712	2023-05-08	2023-05-08	2023-08-06	email.kjbm.cyberwarfare.live	email.kjbm.cyberwarfare.live	G=US, O=Let's Encrypt, CN=R3
	9338676756	2023-05-08	2023-05-08	2023-08-06	email.kjbm.cyberwarfare.live	email.kjbm.cyberwarfare.live	G=US, O=Let's Encrypt, CN=R3
	9171165033	2023-04-17	2023-04-17	2023-07-16	test.cyberwarfare.live	test.cyberwarfare.live	G=US, O=Let's Encrypt, CN=R3
	9171154830	2023-04-17	2023-04-17	2023-07-16	test.cyberwarfare.live	test.cyberwarfare.live	G=US, O=Let's Encrypt, CN=R3
	9145962490	2023-04-14	2023-04-14	2023-07-13	cyberwarfare.live	*.cyberwarfare.live cyberwarfare.live	G=US, O=Google Trust Services LLC, CN=GTS CA 1P5
	9086245743	2023-04-05	2023-04-05	2023-07-04	air.cyberwarfare.live	air.cyberwarfare.live	G=US, O=Let's Encrypt, CN=R3
	9065665848	2023-04-05	2023-04-05	2023-07-04	air.cyberwarfare.live	air.cyberwarfare.live	G=US, O=Let's Encrypt, CN=R3
	8880628135	2023-03-09	2023-03-09	2023-06-07	email.kjbm.cyberwarfare.live	email.kjbm.cyberwarfare.live	G=US, O=Let's Encrypt, CN=R3
	8845624871	2023-03-09	2023-03-09	2023-06-07	email.kjbm.cyberwarfare.live	email.kjbm.cyberwarfare.live	G=US, O=Let's Encrypt, CN=R3
	8865137851	2023-03-07	2023-03-07	2023-06-05	cwlab.cyberwarfare.live	cwlab.cyberwarfare.live	G=US, O=Let's Encrypt, CN=R3
	8828802080	2023-03-07	2023-03-07	2023-06-05	cwlab.cyberwarfare.live	cwlab.cyberwarfare.live	G=US, O=Let's Encrypt, CN=R3
	8860331554	2023-03-06	2023-03-06	2023-06-04	cwlab.cyberwarfare.live	cwlab.cyberwarfare.live	G=US, O=Let's Encrypt, CN=R3
	8820640358	2023-03-06	2023-03-06	2023-06-04	cwlab.cyberwarfare.live	cwlab.cyberwarfare.live	G=US, O=Let's Encrypt, CN=R3
	8817328924	2023-03-06	2023-03-06	2023-06-04	rt.cyberwarfare.live	rt.cyberwarfare.live	G=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
	8817328671	2023-03-06	2023-03-06	2023-06-04	rt.cyberwarfare.live	rt.cyberwarfare.live	G=AT, O=ZeroSSL, CN=ZeroSSL RSA Domain Secure Site CA
	8854476746	2023-03-05	2023-03-05	2023-06-03	rt.cyberwarfare.live	rt.cyberwarfare.live	G=US, O=Let's Encrypt, CN=R3
	8811059115	2023-03-05	2023-03-05	2023-06-03	rt.cyberwarfare.live	rt.cyberwarfare.live	G=US, O=Let's Encrypt, CN=R3
	8853555439	2023-03-05	2023-03-05	2023-06-03	fluke.cyberwarfare.live	fluke.cyberwarfare.live	G=US, O=Let's Encrypt, CN=R3
	8809525712	2023-03-05	2023-03-05	2023-06-03	fluke.cyberwarfare.live	fluke.cyberwarfare.live	G=US, O=Let's Encrypt, CN=R3
	8706348368	2023-02-21	2023-02-21	2024-02-21	*.cyberwarfare.live	*.cyberwarfare.live cyberwarfare.live	G=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo ECC Domain Validation Secure Server CA
	8706347102	2023-02-21	2023-02-21	2024-02-21	*.cyberwarfare.live	*.cyberwarfare.live cyberwarfare.live	G=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo ECC Domain Validation Secure Server CA
	8655542156	2023-02-14	2023-02-14	2023-05-15	*.cyberwarfare.live	*.cyberwarfare.live cyberwarfare.live	G=US, O=Google Trust Services LLC, CN=GTS CA 1P5
	8465014181	2023-01-13	2023-01-13	2023-04-13	defense.cyberwarfare.live	defense.cyberwarfare.live	G=US, O=Let's Encrypt, CN=R3
	8428271593	2023-01-13	2023-01-13	2023-04-13	defense.cyberwarfare.live	defense.cyberwarfare.live	G=US, O=Let's Encrypt, CN=R3
	8456443785	2023-01-12	2023-01-12	2023-04-12	nuclear.cyberwarfare.live	nuclear.cyberwarfare.live	G=US, O=Let's Encrypt, CN=R3
	8397560310	2023-01-12	2023-01-12	2023-04-12	nuclear.cyberwarfare.live	nuclear.cyberwarfare.live	G=US, O=Let's Encrypt, CN=R3
	8456059295	2023-01-12	2023-01-12	2023-04-12	flopster.cyberwarfare.live	flopster.cyberwarfare.live	G=US, O=Let's Encrypt, CN=R3
	8397331679	2023-01-12	2023-01-12	2023-04-12	flopster.cyberwarfare.live	flopster.cyberwarfare.live	G=US, O=Let's Encrypt, CN=R3
	8222527062	2022-12-17	2022-12-17	2023-12-17	*.cyberwarfare.live	*.cyberwarfare.live	G=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo ECC Domain Validation Secure Server CA



DNS Records

- Naming system of Internet
- Maps IP addresses to domains and vice versa
- Provides critical insights into client's attack surface

















Whois **DNS Records** Diagnostics
















DNS Records for cyberwarfare.live

Hostname	Type	TTL	Priority	Content
cyberwarfare.live	SOA	1800		jermaine.ns.cloudflare.com dns.cloudflare.com 2312053932 10000 2400 604800 1800
cyberwarfare.live	NS	21600		jermaine.ns.cloudflare.com
cyberwarfare.live	NS	21600		joyce.ns.cloudflare.com
cyberwarfare.live	A	300		172.67.197.22
cyberwarfare.live	A	300		104.21.92.181
cyberwarfare.live	AAAA	300		2606:4700:3030::6815:5cb5
cyberwarfare.live	AAAA	300		2606:4700:3030::ac43:c516
cyberwarfare.live	MX	300	1	aspmx.l.google.com
cyberwarfare.live	MX	300	10	alt3.aspmx.l.google.com
cyberwarfare.live	MX	300	10	alt4.aspmx.l.google.com
cyberwarfare.live	MX	300	5	alt1.aspmx.l.google.com
cyberwarfare.live	MX	300	5	alt2.aspmx.l.google.com
www.cyberwarfare.live	A	282		172.64.80.1
www.cyberwarfare.live	AAAA	300		2606:4700:3030::6815:5cb5
www.cyberwarfare.live	AAAA	300		2606:4700:3030::ac43:c516

DNS Servers

jermaine.ns.cloudflare.com.     	172.64.35.157 jermaine.ns.cloudflare.com	CLOUDFLARENET United States	   
joyce.ns.cloudflare.com.     	172.64.34.14 joyce.ns.cloudflare.com	CLOUDFLARENET United States	

MX Records ** This is where email for the domain goes...

1 aspmx.l.google.com.   	74.125.205.26 le-in-f26.1e100.net	GOOGLE United States	
10 alt3.aspmx.l.google.com.   	142.250.141.26 dd-in-f26.1e100.net	GOOGLE United States	
10 alt4.aspmx.l.google.com.   	142.250.115.26 rq-in-f26.1e100.net	GOOGLE United States	
5 alt1.aspmx.l.google.com.   	142.250.157.26 ta-in-f26.1e100.net	GOOGLE United States	
5 alt2.aspmx.l.google.com.   	173.194.202.26 pf-in-f26.1e100.net	GOOGLE United States	

TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations

"MS=ms41957772"
"google-site-verification=f-7oucGuCtckXn0R4v6zNpFNxQQBBV4r1Ls0aHuoKdQ"
"v=spf1 include:_spf.google.com ~all"

Host Records (A) ** this data may not be current as it uses a static database (updated monthly)

www.cyberwarfare.live      HTTP: cloudflare	104.21.92.181	CLOUDFLARENET unknown	
cwlab.cyberwarfare.live    	4.193.141.23	MICROSOFT-CORP-MSN-AS-BLOCK Singapore	

Tech Stack

- Technologies implemented in client's infrastructure
- Provide deep insight while planning attack paths
- Ranges from software products to hardware appliances

Analytics and Tracking

[View Global Trends](#)

Google Analytics

[Google Analytics Usage Statistics](#) · [Download List of All Websites using Google Analytics](#)

Google Analytics offers a host of compelling features and benefits for everyone from senior executives and advertising and marketing professionals to site owners and content developers.

Application Performance · Audience Measurement · Visitor Count Tracking

Google Analytics 4

[Google Analytics 4 Usage Statistics](#) · [Download List of All Websites using Google Analytics 4](#)

Google Analytics 4 formerly known as App + Web is a new version of Google Analytics that was released in October 2020.

Global Site Tag

[Global Site Tag Usage Statistics](#) · [Download List of All Websites using Global Site Tag](#)

Google's primary tag for Google Measurement/Conversion Tracking, Adwords and DoubleClick.

Widgets

[View Global Trends](#)

Zoho SalesIQ

[Zoho SalesIQ Usage Statistics](#) · [Download List of All Websites using Zoho SalesIQ](#)

Website visitor tracking and live chat, integrates with Zoho's CRM and other apps

Live Chat

Kajabi

[Kajabi Usage Statistics](#) · [Download List of All Websites using Kajabi](#)

Sell Your Content Online

eCommerce

Font Awesome



Google Analytics GA4

CDN



jsDelivr



Cloudflare

Font scripts



Google Font API

JavaScript libraries



Moment.js 2.24.0



jQuery 3.5.1



AOS



Fancybox 3.5.7



core-js 3.22.8

Live chat



WhatsApp Business Chat



Tawk.to

WayBack Machine

- The actual, living, capturing, **Time Machine of World Wide Web**
- Anyone can captures a site's snapshots
- Can track a website's evolution
- And the statistics it gives, real awesome



URL	MIME Type	From	To	Captures	Duplicates	Uniques
http://cyberwarfare.live	text/html	Jun 19, 2020	Jun 6, 2023	59	27	32
http://cyberwarfare.live/CyberWarfare/	text/html	Jun 19, 2020	Oct 23, 2020	4	2	2
http://cyberwarfare.live/index.php	warc/revisit	Nov 1, 2020	Feb 28, 2021	10	4	6
http://cyberwarfare.live/robots.txt	text/html	Sep 9, 2020	Jun 6, 2023	79	69	10
http://www.cyberwarfare.live/trainings/certified-	unk	Jun 6, 2023	Jun 6, 2023	1	0	1
https://cyberwarfare.live/404	text/html	May 8, 2021	May 11, 2021	2	1	1
https://cyberwarfare.live/_next/static/chunks/28df9282f51634b867431184c26287a4538504a85ac24ad59f130e83c22b.js	application/javascript	May 12, 2021	Jul 27, 2021	4	2	2
https://cyberwarfare.live/_next/static/chunks/7803c8f9b1dde1d08121b84b9671ca29503c7f815c32b6c10ba8910001.js	application/javascript	Sep 3, 2021	Sep 3, 2021	1	0	1
https://cyberwarfare.live/_next/static/chunks/82847670.d032408e2471bd10a140.js	application/javascript	Oct 20, 2021	Oct 20, 2021	1	0	1
https://cyberwarfare.live/_next/static/chunks/8ff16a13bbe0b847493f8b6181.js	application/javascript	May 19, 2021	Jul 27, 2021	4	3	1
https://cyberwarfare.live/_next/static/chunks/c0273303a7470349e5eb26119c9eb148803eadd5720bba8f0e00993cd56.js	application/javascript	Sep 3, 2021	Sep 3, 2021	1	0	1
https://cyberwarfare.live/_next/static/chunks/c184d2103bbe0b847493f8b6181.js	application/javascript	Sep 3, 2021	Sep 3, 2021	1	0	1
https://cyberwarfare.live/_next/static/chunks/ea6579d9f962ebac6823aeff92973dbef5edc5ae404159d6ba09c4d74b120.js	application/javascript	Sep 3, 2021	Sep 3, 2021	1	0	1
https://cyberwarfare.live/_next/static/chunks/framework.7039e9be771a2513c407.js	application/javascript	Sep 3, 2021	Sep 3, 2021	1	0	1
https://cyberwarfare.live/_next/static/chunks/framework.d93d6172e8226ca70dc1.js	application/javascript	May 12, 2021	Jul 27, 2021	4	2	2
https://cyberwarfare.live/_next/static/chunks/main-7d35e8e56333122be82b.js	application/javascript	Sep 3, 2021	Sep 3, 2021	1	0	1
https://cyberwarfare.live/_next/static/chunks/main-cbb84a0e138d09798141.js	application/javascript	May 12, 2021	Jul 27, 2021	4	2	2
https://cyberwarfare.live/_next/static/chunks/pages/_app-d8b9ad568a70be7eb16.js	application/javascript	Sep 3, 2021	Sep 3, 2021	1	0	1

host www.cyberwarfare.live

Indexed on January 21, 2023.

Saved - times -

MIME-types

Any MIME-types

Year Start

2020

Year End

2023

All text image application font

Summary on MIME-types Count

Quick search on MIME-types...

<< < 1 2 > >>

	Captures	URLs	New URLs
text/html	394	148	130
image/png	93	54	52
text/css	38	29	29
image/vnd.microsoft.icon	22	3	0
image/jpeg	19	14	14
font/woff2	13	10	10
application/pdf	10	8	7
application/xml	6	2	1
image/svg+xml	2	1	1

Captures

Last 10 Captures

Capture	Captures	URLs	New URLs
Tue, 06 Jun 2023 05:34:37 GMT	200	154,111,111	15,000
Fri, 02 Jun 2023 16:20:56 GMT	301	unk	462
Tue, 23 May 2023 06:18:28 GMT	301	unk	442
Sun, 07 May 2023 14:09:10 GMT	200	text/html	18,697
Sat, 22 Apr 2023 23:51:42 GMT	-	warc/revisit	968
Sat, 22 Apr 2023 23:50:34 GMT	200	text/html	18,573
Thu, 23 Mar 2023 11:22:18 GMT	200	text/html	15,129
Fri, 24 Feb 2023 01:55:51 GMT			
Mon, 30 Jan 2023 01:40:29 GMT			
Mon, 02 Jan 2023 17:35:02 GMT			

Shodan

- Records of almost every device with an IP address
- Publicly exposed devices with vulnerable components
- Can find IP cameras to Industrial systems, and everything in between
- Queries are welcome here with an account

General Information

Hostnames

[REDACTED]

Domains

CLOUDFLARE.COM

Country

United States

City

San Francisco

Organization

Cloudflare, Inc.

ISP

Cloudflare, Inc.

ASN

AS13335

Open Ports



ATTENTION!!! Read Before L

Your system has been hacked !!! Your system recover files on your own will result in their notify the management of your company at communication: helpforyou@gmx.com or h have the recovery keys, before agreeing on companies, ask OUR price

OK

Applications 2,930

Boa Web Server 1,477

D-Link/Airlink IP webcam http config 1,090

[More...](#)

TOP OPERATING SYSTEMS

Windows Server 2012 R2 246,093

Windows (Build 10.0.14393) 119,044

Windows (Build 10.0.17763) 116,024

Windows (Build 10.0.19041) 55,631

Windows (Build 10.0.20348) 53,961

[More...](#)



Censys

- Attack Surface Monitoring
- Large database of Internet connected devices
- Provides high quality information
- Supports queries without signing up



Hosts Search

Results

Host Filters

Labels:

Hosts

Results: 219 Time: 0.14s

Summary Explore History WHOIS

Raw Data

Basic Information

Network CLOUDFLARENET (US)

Routing

Protocols 80/HTTP, 443/HTTP, 2052/HTTP, 2053/HTTP, 2082/HTTP, 2083/HTTP, 2086/HTTP, 2087/HTTP, 2095/HTTP, 2096/HTTP, 8080/HTTP, 8443/HTTP, 8880/HTTP

80/HTTP TCP

Observed Jun 13, 2023 at 8

Software

CloudFlare Load Balancer

Details

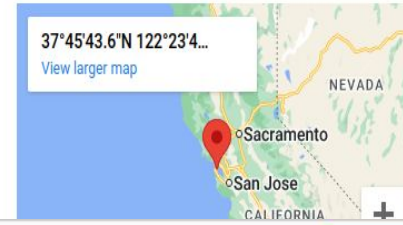
http://172.67.197.22

Request GET /

Protocol HTTP/1.1

Status Code 403

Status Reason Forbidden



VIEW ALL DATA



Hosts x

Results

Host Filters

Labels:

Hosts

Results: 13,228 Time: 0.08s

Automating OSINT

- Efficient by reducing workload
- More time analyzing data
- First learn manual, then move to automation

How To Automate OSINT

- Use software like Maltego, Recon-ng, etc
- Use websites like OSINT Framework, Intel Techniques, etc
- Write custom tools as per use case

Bonus: Twitch

- Find all **NightBot** commands of a Twitch streamer:-

<https://nightbot.tv/t/<username>/commands>

Nobody:

NightBot as soon as i chat something on live stream:



Channel Commands

Show
100
entries
Search:

Command	Message	Userlevel
!academy	Get your hackin' knowledge on: https://academy.tcm-sec.com	everyone
!discord	Come hang out and chat: https://tcm-sec.com/discord	everyone
!donate	If you want to support the channel, you can donate at: https://streamlabs.com/the cybermentor	everyone
!howtohack	https://tcm-sec.com/so-you-want-to-be-a-hacker-2022-edition/	everyone
!instagram	Follow me on Instagram: https://instagram.com/the cybermentor Follow TCM Security on Instagram: https://instagram.com/tcmsecurity	everyone
!linkedin	Follow me on LinkedIn: https://linkedin.com/in/the cybermentor Follow TCM Security on LinkedIn: https://linkedin.com/company/tcm-security-inc	everyone
!merch	Get awesome TCM merch at https://merch.tcm-sec.com	everyone
!patreon	If you'd like to support the channel, get exclusive access to content, and even some cool swag: https://www.patreon.com/the cybermentor	everyone
!pnpt	Get PNPT certified: https://certifications.tcm-sec.com/pnpt	everyone
!pnptlive	Join our free class: https://academy.tcm-sec.com/p/pnpt-live	everyone
!socials	Add us on social media! https://pastebin.com/y9S5MbXt	everyone
!specs	https://pastebin.com/EQFYJLX5	everyone
!sub	Love the content? Please consider supporting with a sub on Twitch: https://subs.twitch.tv/the cybermentor	everyone
!twitter	Tweet tweet: https://www.twitter.com/tcmsecurity	everyone
!uptime	Stream uptime: [twitch]	everyone
!youtube	Subscribe to my YouTube: https://www.youtube.com/c/the cybermentor	everyone

Showing 1 to 16 of 16 entries
First
Previous
1
Next
Last

<https://nightbot.tv/t/the cybermentor/commands>

Resources

- **OSINT Collections** →
 - <https://start.me/p/DPYPMz/the-ultimate-osint-collection>
 - <https://start.me/p/rx6Qj8/nixintel-s-osint-resource-list>
 - <https://cheatsheet.haax.fr/resources/osint/>
 - <https://osintframework.com/>
 - <https://map.malfrats.industries/>
 - <https://inteltechniques.com/tools/index.html>
- **Google Dorking** →
 - <https://www.googleguide.com/>
 - <https://www.exploit-db.com/google-hacking-database>
 - <https://pentest-tools.com/information-gathering/google-hacking>
 - <https://dorkgpt.com/>

Resources

- **Other Dorks** →

- <https://techofide.com/blogs/uncovering-vulnerabilities-shodan-github-dorks-and-linkedin-osint-tools-for-bug-hunting/>
- <https://github.com/cipher387/Dorks-collections-list>
- <https://github.com/mathis2001/Dorking>

- **Domain** →

- <https://who.is/>
- <https://lookup.icann.org/>

- **IP** →

- <https://www.shodan.io/>
- <https://search.censys.io/>
- <https://app.netlas.io/>
- <https://pulsedive.com/>

Resources

- **DNS** →

- <https://www.osintme.com/index.php/2021/01/16/ultimate-osint-with-shodan-100-great-shodan-queries/>
- <https://nasniconsultants.com/top-40-shodan-dorks-for-finding-sensitive-iot-data/cybersecurity/2021/05/27/diran/>
- <https://github.com/mr-exo/shodan-dorks>

- **Subdomain** →

- <https://dnsdumpster.com>
- <https://crt.sh/>

THANK YOU :)