

20

CyberSecurity Search Engines



RajihSalim



<https://www.shodan.io/>



The screenshot shows the Shodan website interface. At the top, there are navigation tabs: Maps, Images, Monitor, Developer, and More... Below these are links for DAN, Explore, and Pricing. A search bar with a magnifying glass icon is present. The main content area features the heading "Search Engine for the Internet of Everything" and a world map with colored data points. A green "SIGN UP NOW" button is visible. Below the main content, there is a section titled "EXPLORE THE PLATFORM" with three cards: "Beyond the Web", "Monitor Network Exposure", and "Internet Intelligence".

Maps Images Monitor Developer More...

DAN Explore Pricing Search...

Search Engine for the Internet of Everything

Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.

[SIGN UP NOW](#)

EXPLORE THE PLATFORM

- Beyond the Web**
Websites are just one part of the Internet. Use
- Monitor Network Exposure**
Keep track of all your devices that are directly
- Internet Intelligence**
Learn more about who is using various

2

<https://www.wigle.net/>

The screenshot displays the Wigle.net website interface. At the top, there is a navigation bar with icons and labels for 'View', 'Uploads', 'Info', 'Stats', and 'Tools'. Below this is the main header with the 'WIGLE.NET' logo and the tagline 'All the networks. Found by Everyone.'.

Below the header, there are five statistics cards:

STUMBLERS	WIFI NETWORKS	WIFI OBSERVATIONS	WIFI TODAY	BT DEVICES
385,613	933,641,928	13,238,152,321	425,296	1,078,672,591

On the left side, there are three news items:

- DEF CON 30**
Wed, 10 Aug 2022 06:01:25 GMT
DC30 is happening this week, and bobzilla and arkasha will be there!
Find us and say "hi" for swag!
-arkasha
- Highway to the...**
Wed, 03 Aug 2022 04:25:06 GMT
... #WWWD2022
read more...
-arkasha
- World-Wide War Drive, RFHS and DEF CON 30**
Fri, 29 Jul 2022 21:51:17 GMT
Greetings WIFriends! The fine folks at the RFHS have invited us to hold a World-Wide War Drive in conjunction with the DEF CON 30 RFHS, and we have answered the call. Registration is now open at the DC30 WWWD landing page

On the right side, there is a heatmap map showing network density. The map has a search bar at the top with the text 'Find address or place' and a search icon. The map itself is a grid of red lines representing streets, with various colored dots (green, yellow, orange, red) indicating network locations. The word 'WIGLE.NET' is visible on the map.



3

<https://grep.app/>



//grep.app

Search across a half million git repos

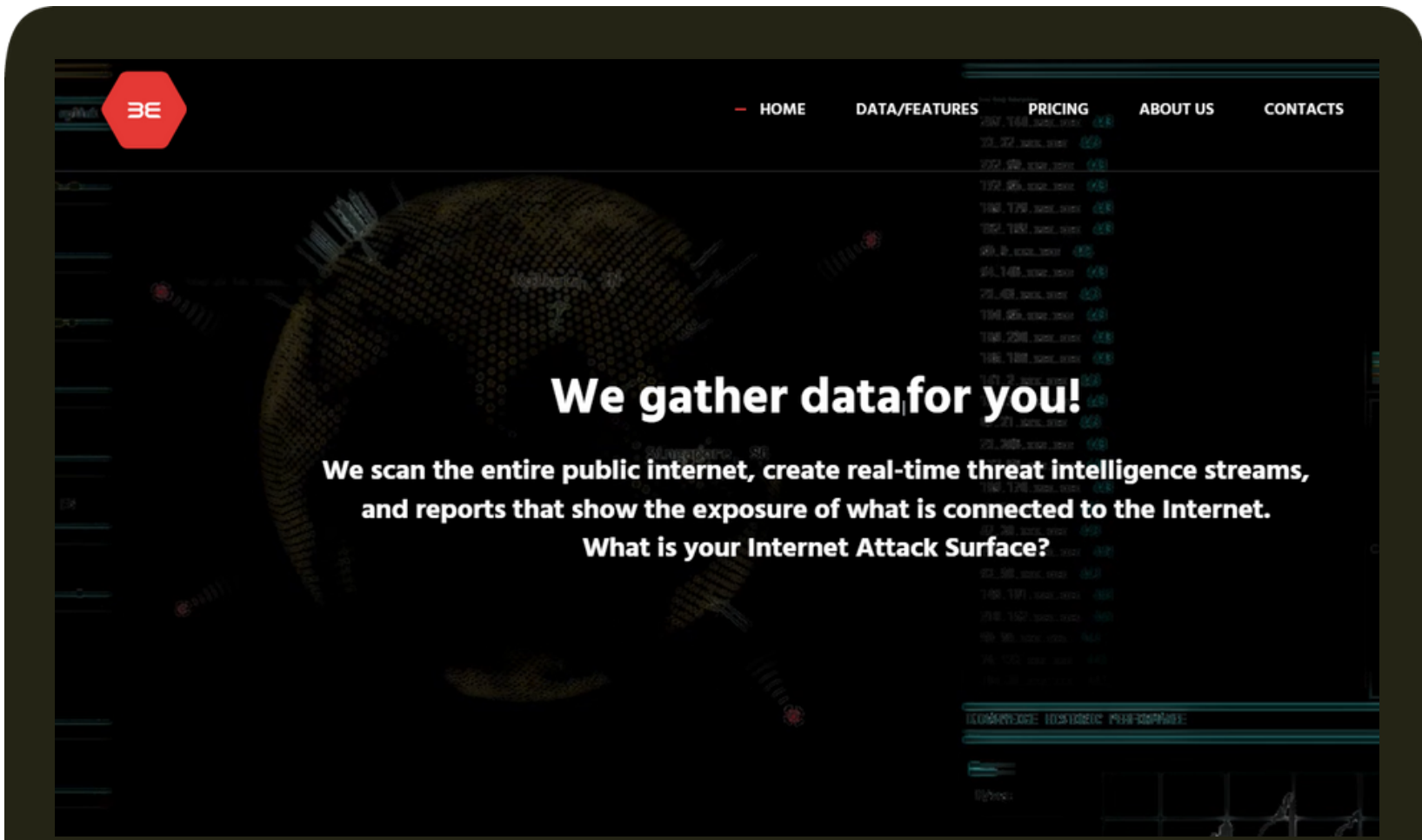
Q Search

Case sensitive Regular expression Whole words

[About](#) [Contact](#)

4

<https://www.binaryedge.io/>



The screenshot shows the homepage of Binary Edge. At the top left is a red hexagonal logo with the letters 'BE'. To the right is a navigation menu with links for HOME, DATA/FEATURES, PRICING, ABOUT US, and CONTACTS. The main content area features a dark background with a globe and a list of IP addresses on the right side. The central text reads: "We gather data for you! We scan the entire public internet, create real-time threat intelligence streams, and reports that show the exposure of what is connected to the Internet. What is your Internet Attack Surface?".

BE

HOME DATA/FEATURES PRICING ABOUT US CONTACTS

We gather data for you!
We scan the entire public internet, create real-time threat intelligence streams, and reports that show the exposure of what is connected to the Internet.
What is your Internet Attack Surface?

207.168.100.100 (US)
70.37.200.100 (US)
222.29.100.100 (US)
172.25.100.100 (US)
190.170.100.100 (US)
102.100.100.100 (US)
90.0.100.100 (US)
64.145.100.100 (US)
75.40.100.100 (US)
194.95.100.100 (US)
198.250.100.100 (US)
198.100.100.100 (US)
107.0.100.100 (US)
0.0.0.0 (US)
70.300.100.100 (US)
194.170.100.100 (US)
97.30.100.100 (US)
80.80.100.100 (US)
198.191.100.100 (US)
198.190.100.100 (US)
98.98.100.100 (US)
98.170.100.100 (US)

LANGUAGE: | HISTORIC | PHISHING



5

<https://www.onyphe.io/>



 **ONYPHE**

[Home](#) [Blog](#) [Documentation](#) [Pricing](#) [Sign-In](#)

Cyber Defense Search Engine

One if is enough

Search




In numbers

- ✓ 200+ ports scanned monthly
- ✓ 7-month of history
- ✓ 0.1 second average API response time
- ✓ 300 million banners collected monthly
- ✓ 300 million URLs scanned monthly
- ✓ 1.2 billion DNS entries monthly



6

<https://www.greynoise.io/>



Explore Our Data

Plans 

KNOW MORE NOISE

GreyNoise is THE source for understanding internet noise.

Create Free Account



<https://censys.io/>



The screenshot shows the Censys website homepage. At the top, there is a navigation bar with links for Blog, News, Resources, Careers, Culture, Contact, Censys Search, and Sales. The main header features the Censys logo and a navigation menu with categories like Attack Surface Management, Data & Search, Integrations, Federal, and Partners. A prominent orange banner contains the headline "A secure internet starts with Censys." and a sub-headline describing the company's role in Attack Surface Management. A video player for "Attack Surface Management" is featured on the right, with a "WATCH THE DEMO VIDEO" button. A "Request a demo" button is located at the bottom left of the banner.

Blog News Resources Careers Culture Contact | Censys Search @ Sales 1-888-985-5547 ☎

censys

Attack Surface Management ▾ Data & Search Integrations Federal Partners [Contact Us](#)

A secure internet starts with Censys.

Your cloud is bigger, wider, and more vast than you know; your internet assets innumerable. Censys is the proven leader in Attack Surface Management by relentlessly searching and proactively monitoring your digital footprint far more broadly and deeply than ever thought possible.

[Request a demo](#)

censys
Attack Surface Management
WATCH THE DEMO VIDEO



8

<https://hunter.io/>



 **hunter**

Product ▾

Pricing

Resources ▾

Company ▾



Sign in

Sign up



Connect with anyone.

Hunter lets you find professional email addresses in seconds and connect with the people that matter for your business.

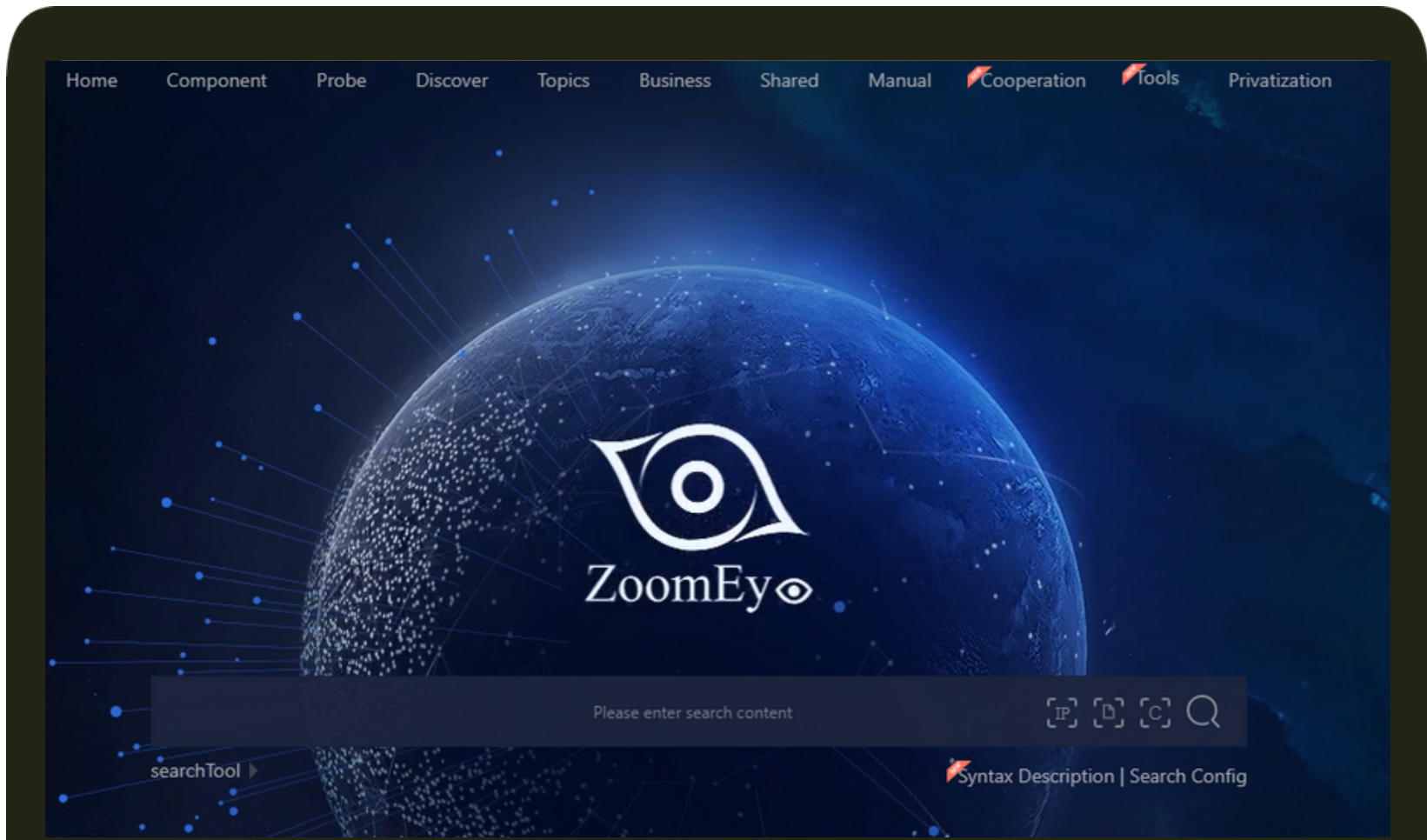
Find email addresses

Enter a domain name to launch the search. For example, hunter.io.



9

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



10

<https://leakix.net/>

The screenshot displays the LeakIX website interface. At the top, there is a navigation bar with the LeakIX logo and various menu items: Search, Graph, preview, Top researchers, beta, Reports, beta, Researchers, Documentation, new, Tools, Community, and Statistics. Below the navigation bar is a search bar with a search icon and a search button. A disclaimer states: "By searching for results, you agree with our Terms of service".

The main content area is divided into several sections:

- Latest news:** A list of recent news items with dates and titles. Each item includes a brief description and a "Read more" link.
 - Jul 07, 2022: **What we know about the China Leak**. Quick analysis of the facts we gathered. [Read more](#)
 - Jun 06, 2022: **D-LINK DIR-842 Rev-B privilege escalation**. A quick blog post on how to enable telnet your REV-B device. [Read more](#)
 - Mar 06, 2022: **Bypassing NTLM auth over HTTP**. Exploring the so called NT ANONYMOUS_LOGON user through HTTP endpoints. [Read more](#)
- Latest reports:** A list of recent reports with dates and authors. Each item includes a title and a "Read more" link.
 - Aug 31, 2022 by BloodyShell: **Contratanet / Simplicity / ElasticSearch is publicly avail...**. Elasticsearch and/or Kibana is currently open without authentication. This results in all... [Read more](#)
 - Apr 29, 2022 by BloodyShell: **Integri Services / Veeam Backup & Replication Remote...**. Your server have been found vulnerable to Veeam RCE. This means any attacker can c... [Read more](#)
 - Apr 29, 2022 by BloodyShell: **Probyteconsulting.be / Veeam Backup & Replication R...**. Your server have been found vulnerable to Veeam RCE. This means any attacker can c... [Read more](#)
- LeakIX monitor:** A section displaying a list of found IP addresses and ports with their associated protocols.
 - Found 47.105.45.171 port 443 https
 - Found 194.182.163.154 port 22 ssh
 - Found 128.199.176.45 port 80 http
 - Found 85.11.152.50 port 80 http
 - Found 156.234.209.102 port 80 http
 - Found 201.172.253.31 port 80 http
 - Found 136.144.186.80 port 80 http
 - Found 195.226.135.19 port 443 https
 - Found 139.59.120.51 port 22 ssh
- About LeakIX:** A section with a play button icon, containing the text: "Who are we?" and "Our goals".



<https://intelx.io/>



IntelligenceX

[About](#) [Product](#) [Blog](#) [Tools](#) [Integrations](#)

[Login](#)

[Sign up](#)

Search Tor, I2P, data leaks, public web..|

Enter a domain, URL, Email, IP, CIDR, Bitcoin address, and more...

Search


[Advanced](#)




12

<https://netlas.io/>



 [Netlas.io](#) [Use Cases](#) [API](#) [Pricing](#) [Bulk Data](#)

[Go to Application](#)



Discover, Research and Monitor any Assets Available Online

Internet intelligence apps that provide accurate technical information on IP addresses, domain names, websites, web applications, IoT devices, and other online assets.

[Sign up for free](#)

[Learn more](#)



13

<https://urlscan.io/>



urlscan.io Search Live API Blog Docs Pricing Login Sponsored by SecurityTrails

urlscan.io

A sandbox for the web

URL to scan Public Scan Options

Recent scans Updates every 10s - Last update: 08:25:21

URL	Age	Size	↻	IPs	🚩	🏠
refraconcepts.be/	6 seconds	12 MB	31	6	3	🇳🇱
www.standaard.be/cnt/dmf20221011_93565190?utm_source=standaard&utm_medium=newsl...	14 seconds	3 MB	116	18	6	🇺🇸
login.accor.com/as/authorization.oauth2?client_id=all.accor&response_type=code&...	18 seconds	3 MB	95	10	4	🇺🇸
bharatpestcontrol.in/	20 seconds	7 MB	85	6	2	🇺🇸
www.mediahuis.be/nl/privacy-beleid/?utm_campaign=goeienavond&utm_content=footer...	23 seconds	588 KB	28	5	3	🇺🇸
www.tumblr.com/airpurifierlive/697792655922528256/what-is-the-working-basis-of-...	28 seconds	2 MB	75	18	1	🇺🇸
bakhtarnews.af/	30 seconds	4 MB	68	10	3	🇦🇫
sage.pnbcommercial.my/eportal/public/signin.aspx?ReturnUrl=%2feportal%2f	34 seconds	1 MB	31	1	1	🇲🇾
www.icann.org/resources/pages/epp-status-codes-2014-06-16-en	36 seconds	2 MB	11	2	1	🇺🇸

14

<https://publicwww.com/>

The screenshot shows the PublicWWW Source Code Search Engine interface. At the top, there is a navigation bar with links for "PublicWWW", "Examples", "Clusters", and "Pricing", along with "Sign Up" and "Log In" buttons. The main heading is "Source Code Search Engine" with a subtitle "Find any alphanumeric snippet, signature or keyword in the web pages HTML, JS and CSS code." Below this is a search input field with the placeholder text "Search for code snippet, signature or keyword..." and a "Search" button. To the right of the search field, it displays "508 748 793 web pages" and "October 11, 2022". Below the search field, there is a note about query syntax: "query syntax: RegEx, ccTLDs, etc." The main content area is divided into two columns. The left column contains a paragraph about the service being an "Ultimate solution for digital marketing and affiliate marketing research" and a list of search examples. The right column is titled "Usage Examples" and shows four examples: AngularJS, Bootstrap, Add This, and reCAPTCHA, each with its logo and a sample search query.

PublicWWW | Examples | Clusters | Pricing | Sign Up | Log In

Source Code Search Engine

Find any alphanumeric snippet, signature or keyword in the web pages HTML, JS and CSS code.

Search for code snippet, signature or keyword... Search





508 748 793 web pages
October 11, 2022

query syntax: RegEx, ccTLDs, etc.

Ultimate solution for digital marketing and affiliate marketing research, PublicWWW allow you to perform searches this way, something that is not possible with other regular search engines:

- Any HTML, JavaScript, CSS and plain text in web page source code
- References to StackOverflow questions in HTML, .CSS and .JS files
- Web designers and developers who hate IE
- Sites with the same analytics id: "UA-19778070-"
- Sites using the following version of nginx: "Server: nginx/1.4.7"
- Advertising networks users: "adserver.adtech.de"
- Sites using same adsense account: "pub-"

Usage Examples

 ANGULARJS <small>by Google</small> "angular.min.js"	 Bootstrap "bootstrap.min.js"
 Add This "addthis_widget.js"	 reCAPTCHA "recaptcha/api.js"

Algalia



15

<https://fullhunt.io/>



The screenshot shows the FullHunt website homepage. At the top, there is a navigation bar with the FullHunt logo and links for Home, Search, Pricing, Products, Platforms, Contact us, Blog, LOGIN, and SIGN UP. The main content area features a dark purple background with the headline "SECURE YOUR ATTACK SURFACE" and "The Next-Generation Attack Surface Security". Below this, a sub-headline reads "If you don't know all your internet-facing assets, which ones are vulnerable, FullHunt is here for you." A prominent button offers "GET A FREE FULLHUNT ENTERPRISE PLATFORM TRIAL". To the right, there is an illustration of server racks. At the bottom, a search bar is visible with the text "Expose your attack surface" and a search icon.



16

<https://crt.sh/>



crt.sh Certificate Search

Enter an **Identity** (Domain Name, Organization Name, etc),
a **Certificate Fingerprint** (SHA-1 or SHA-256) or a **crt.sh ID**:

Search

[Advanced...](#)

© Sectigo Limited 2015-2022. All rights reserved.





17

<https://vulners.com/>



DATABASE

RESOURCES

USE CASES

PRICING

CONTACTS

SIGN IN

Your Search Engine for Security Intelligence

Vulnerabilities or exploits

Search

🔥 Daily Hot!

🔒 Security news

📄 Exploit updates

📖 Blogs review

🐛 Bugbounty

🐧 Linux vulnerabilities

🔍 Scanners plugins updates

📄 CVE Feed

🛠 Security Tools

🦊 Firefox vulnerabilities


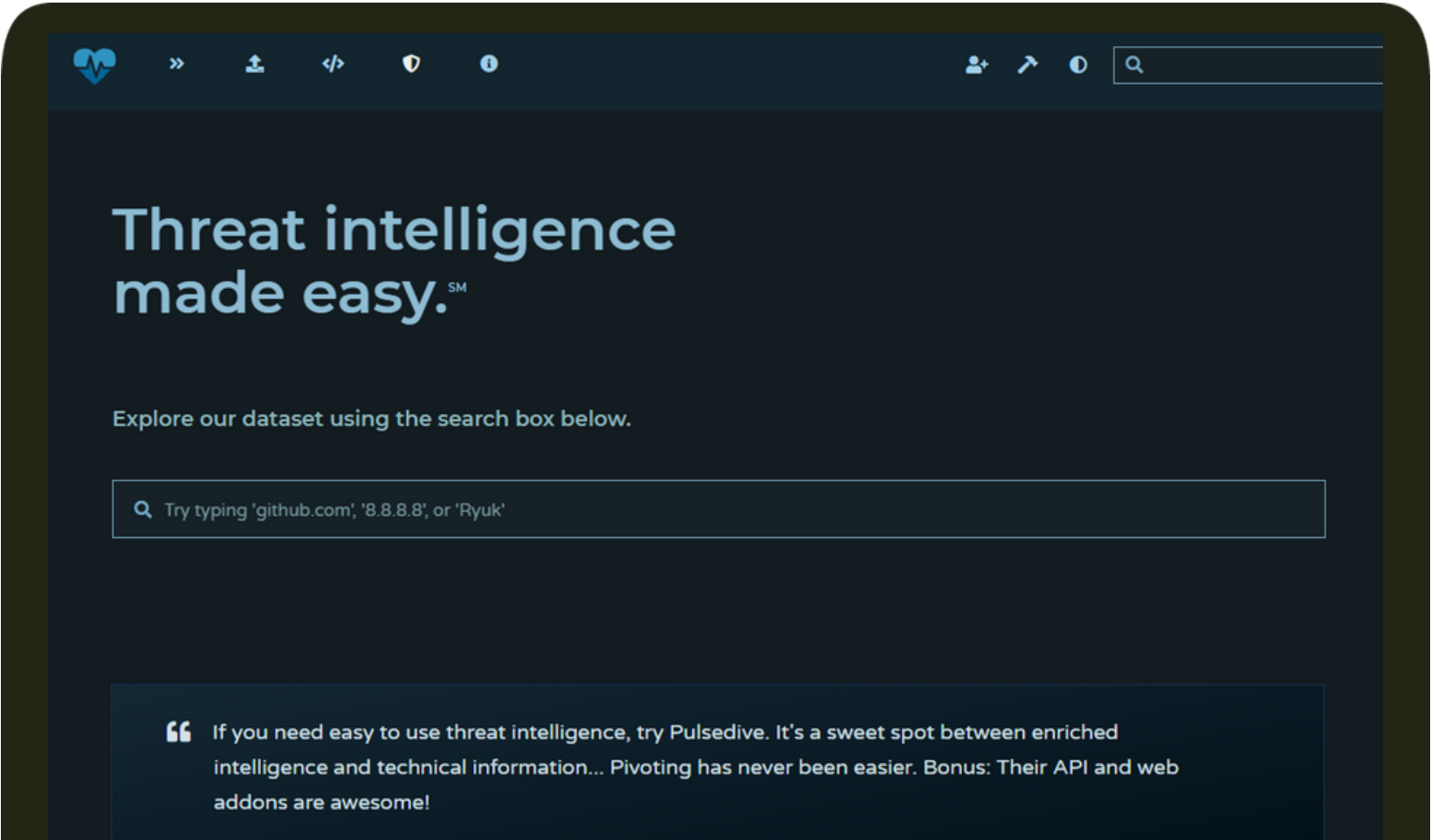

🏆 CVSS High Score

show all



18

<https://pulsedive.com/>



Threat intelligence made easy.SM

Explore our dataset using the search box below.

🔍 Try typing 'github.com', '8.8.8.8', or 'Ryuk'

“ If you need easy to use threat intelligence, try Pulsedive. It's a sweet spot between enriched intelligence and technical information... Pivoting has never been easier. Bonus: Their API and web addons are awesome!



19

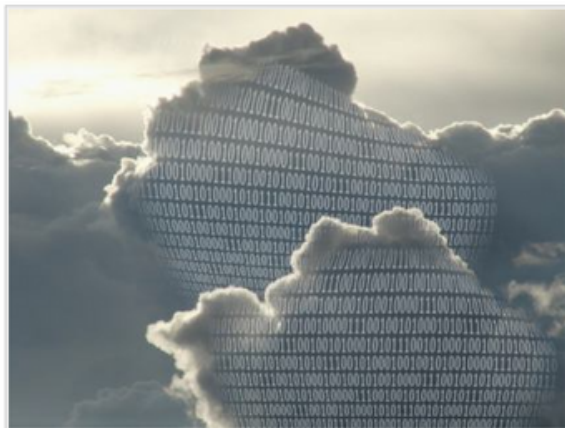
<https://packetstormsecurity.com/>



packet storm Register | Login
 exploit the possibilities

Search ...

Home | Files | News | About | Contact | SERVICES TAG | Add New



Google Makes Major Play For Cloud Security Market



Meta Uncovers 400 Malicious Apps On Android And iOS



iPhones Calling 911 From Owners' Pockets On Rollercoasters



Fortinet Warns Of Critical Flaw In Its Security Appliance OSes, Admin Panels

Follow us on Twitter

Subscribe to an RSS Feed

Recent News

- Singtel Confirms Digital Burglary At Dialog Subsidiary
- Unpatched Zimbra Flaw Lets Hackers Backdoor Servers
- New macOS Vuln Lets Malicious Apps Bypass Security Checks
- Protests In Iran: State-Run Live TV Hacked By Protestors
- Biden Signs Order For EU - U.S. Data Privacy Framework
- 2K Warns Users Their Info Was Stolen Due To A Help Desk Breach
- Binance Says \$100 Million Of Crypto Produced Out Of Thin Air By Hackers
- Feds Ink \$26 Million Contract For Deception Platform For Defense
- NetWalker Ransomware Scumbag Jailed For 20 Years
- Tells Fraud To Go The Dice And More

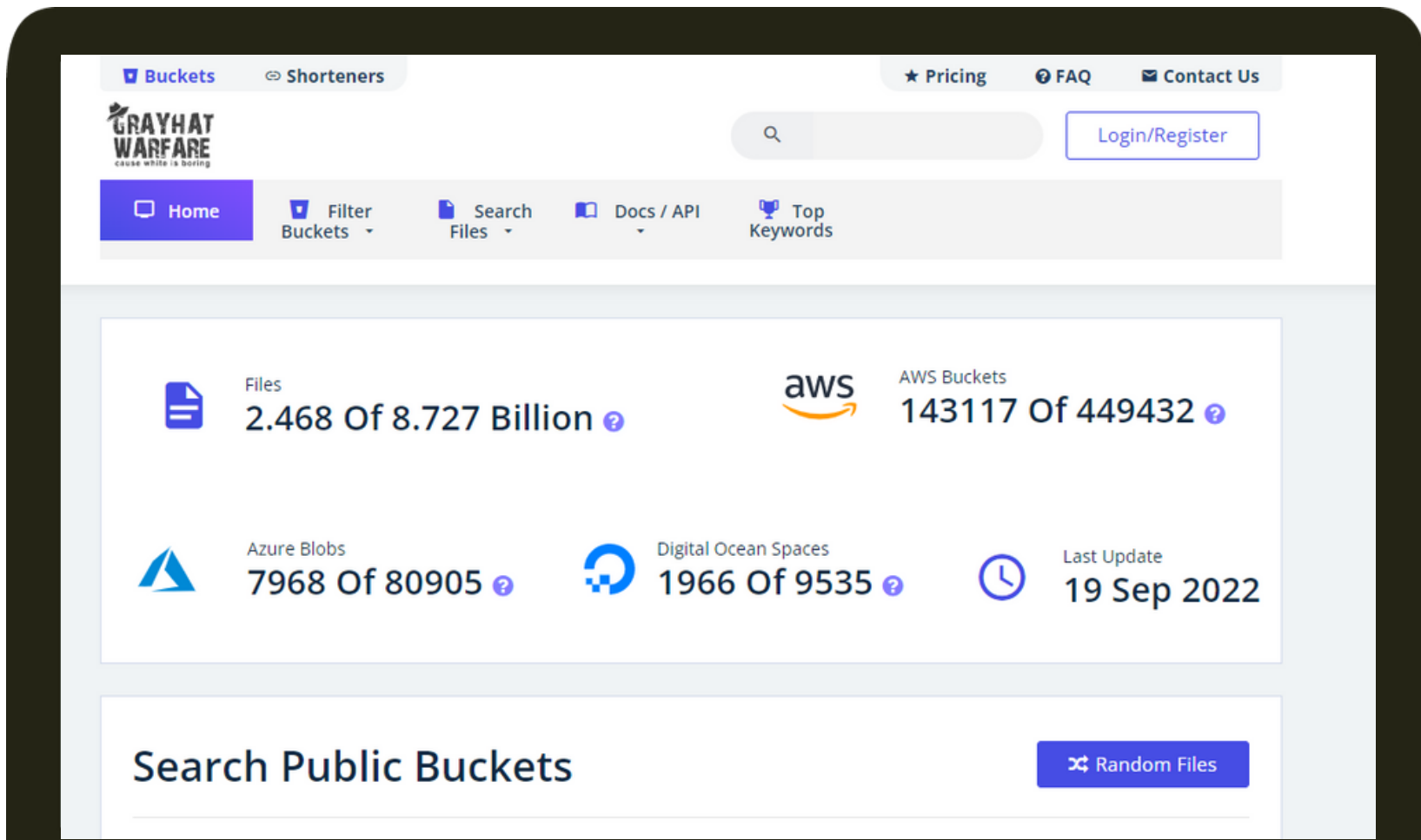
Recent Files

All | Exploits | Advisories | Tools | Whitepapers | Other

Red Hat Security Advisory 2022-6875-01

20

<https://buckets.grayhatwarfare.com/>



The screenshot shows the website interface for Gray Hat Warfare Buckets. The header includes navigation links for Buckets, Shorteners, Pricing, FAQ, and Contact Us. The main navigation bar features Home, Filter Buckets, Search Files, Docs / API, and Top Keywords. The main content area displays statistics for various cloud storage services:

Service	Files	Total
Files	2.468	8.727 Billion
AWS Buckets	143117	449432
Azure Blobs	7968	80905
Digital Ocean Spaces	1966	9535

The last update date is 19 Sep 2022. At the bottom, there is a search bar for public buckets and a button for Random Files.



: الملخص

<https://www.shodan.io>
<https://www.wigle.net>
<https://grep.app/>
<https://www.binaryedge.io/>
<https://www.onyphe.io/>
<https://www.greynoise.io>
<https://censys.io/>
<https://hunter.io/>
<https://www.zoomeye.org/>
<https://leakix.net/>
<https://intelx.io/>
<https://netlas.io/>
<https://urlscan.io/>
<https://publicwww.com/>
<https://fullhunt.io/>
<https://crt.sh/>
<https://vulners.com/>
<https://pulsedive.com/>
<https://packetstormsecurity.com/>
<https://buckets.grayhatwarfare.com/>

شكراً لكم،

RajihSalim

