Università degli Studi di Salerno

Dipartimento di Informatica

Penetration Testing & Ethical Hacking

Enumerating Target e Port Scanning

Parte 3

Arcangelo Castiglione
arcastiglione@unisa.it

Outline

- Concetti Introduttivi
- Suite Protocollare TCP/IP
- Formato dei Messaggi TCP e UDP
- Active Enumeration
  - Network Scanner Nmap
  - Zenmap
  - Unicornscan
  - Masscan
- **Passive Enumeration**
  - Shodan
  - ZoomEye
  - FOFA
  - Censys

Outline

- Concetti Introduttivi
- Suite Protocollare TCP/IP
- Formato dei Messaggi TCP e UDP
- Active Enumeration
  - Network Scanner Nmap
  - Zenmap
  - Unicornscan
  - Masscan
- Passive Enumeration
  - **Shodan**
  - ZoomEye
  - FOFA
  - Censys

Shodan

Caratteristiche

- https://www.shodan.io/
  - **Motore di ricerca** che consente di trovare (tramite opportuni filtri) vari tipi di **dispositivi connessi ad Internet**
  - **Noto per essere il più importante motore di ricerca per dispositivi connessi ad Internet**
    - Computer
    - Webcam
    - Server
    - Router
    - Dispositivi IoT
    - Etc
  - Introdotto nel 2009 da John Matherly

SHODAN
Computer Search Engine

Shodan
Caratteristiche

- https://www.shodan.io/
  - Anche definito come **motore di ricerca di *service banner***
    - Metadati che il Server invia al Client
  - I *service banner* potrebbero contenere informazioni interessanti sui software di rete in esecuzione sul Server
    - Messaggio di benvenuto
    - Eventuali opzioni supportate dal software
    - Qualsiasi altra cosa che potrebbe essere utile al Client prima di interagire con il Server

SHODAN
Computer Search Engine

Shodan
Caratteristiche

- Shodan raccoglie dati su vari servizi di rete
  - *Web Server* (HTTP/HTTPS - porte 80, 8080, 443, 8443)
  - *FTP* (porta 21)
  - *SSH* (porta 22)
  - *Telnet* (porta 23)
  - *IMAP* (porte 143 o 993)
  - *SMTP* (porta 25)
  - *Real Time Streaming Protocol* (*RTSP*, porta 554)
    - Utilizzato per accedere alle webcam ed ai loro flussi video
  - Etc

SHODAN
Computer Search Engine

Shodan
Caratteristiche

- Shodan fornisce inoltre
  - Una propria interfaccia a linea di comando (*Shodan Command-Line Interface*) utilizzabile online
    - **https://cli.shodan.io/**
  - API per scrivere programmi basati su Shodan

- Interessante strumento basato sulle API di Shodan
  - *SearchDiggity*
    - **https://www.bishopfox.com/resources/tools/google-hacking-diggity/attack-tools/**

SHODAN
Computer Search Engine

Shodan
Caratteristiche

- Consente di scoprire
  - Quali sistemi sono presenti in un asset
  - I servizi attivi in tali sistemi (ed i relativi *banner*)
  - Le versioni di tali servizi
  - Etc

- **N.B.** Le **informazioni** fornite da tale strumento **potrebbero non essere allineate** con lo stato corrente dell'asset
  - Prima di proseguire con le fasi successive del processo di penetration testing sarebbe opportuno condurre anche una fase di *Active Target Enumeration*
    - Un host potrebbe non essere più attivo o lo stato/versione delle sue porte/servizi potrebbe essere cambiato

SHODAN
Computer Search Engine

Shodan
Caratteristiche

- Shodan è uno strumento utile per ottenere in maniera «discreta» ed affidabile numerose informazioni

- Il suo *timestamp* permette di avere un'idea su quanto siano recenti i risultati mostrati

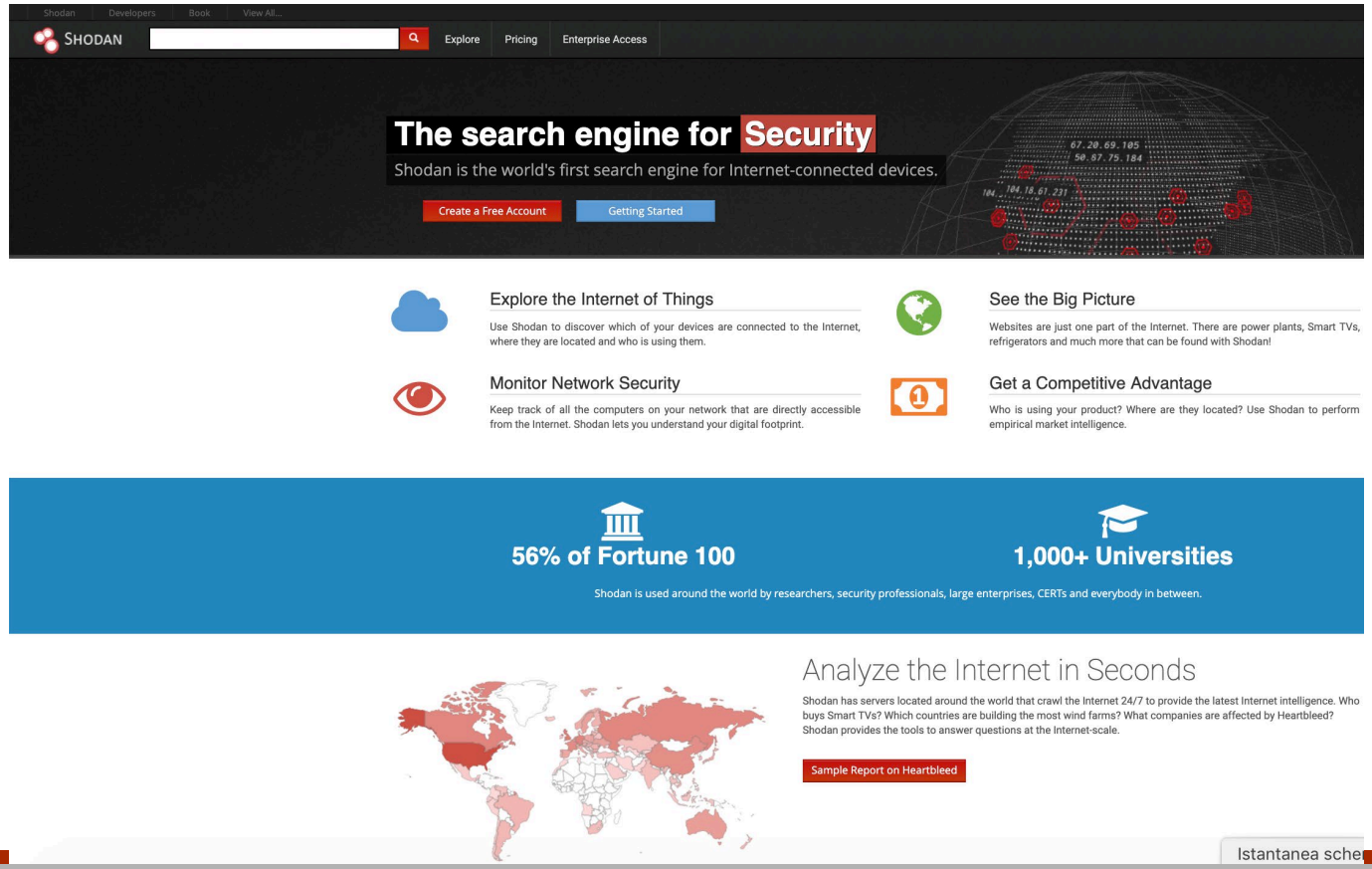
- La versione «free» fornisce funzionalità molto limitate
  - Numero limitato di pagine come risultato per ciascuna query
  - Numero limitato di filtri da applicare
  - Etc

SHODAN
Computer Search Engine

Shodan

Interfaccia

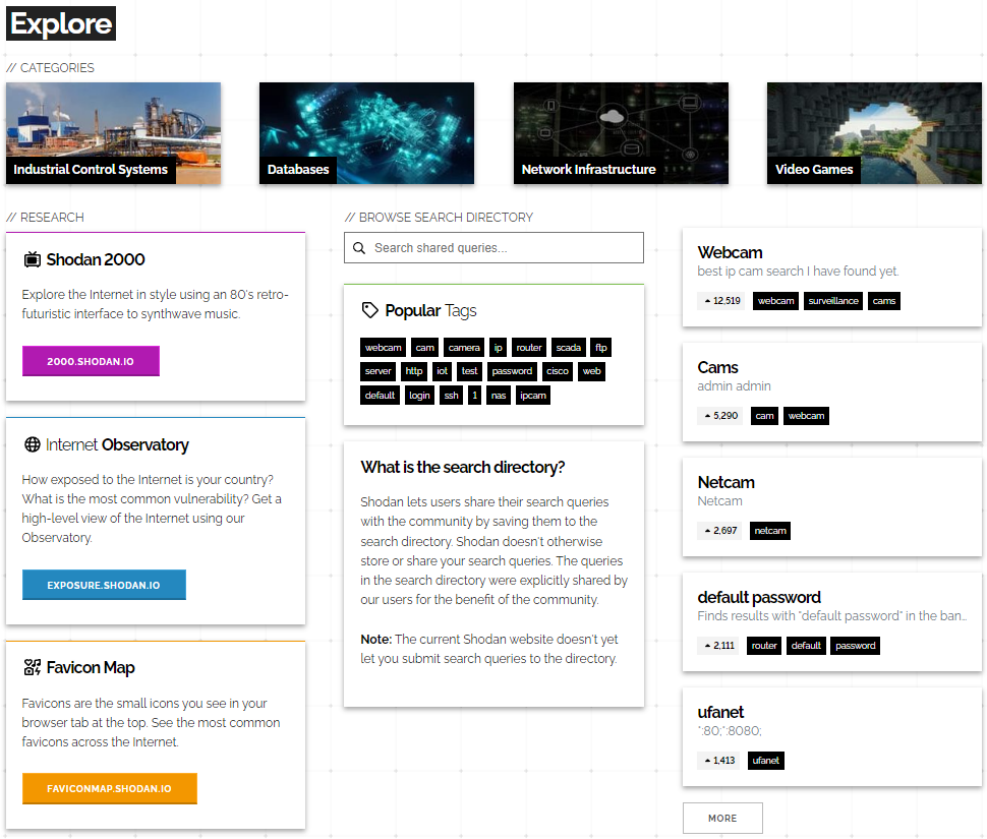
- **https://www.shodan.io/**



Shodan

Dorks – Query Shodan Predefinite

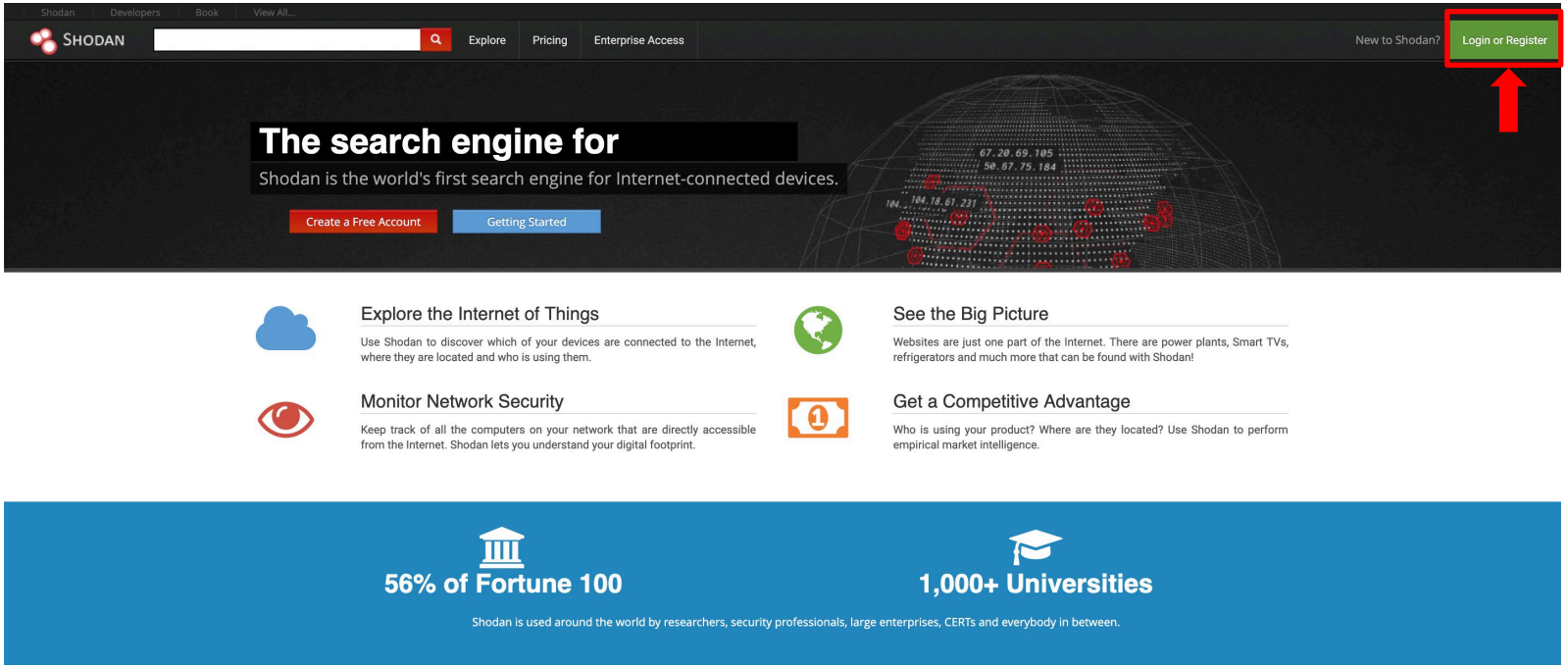
- **https://www.shodan.io/explore**



Shodan

Registrazione

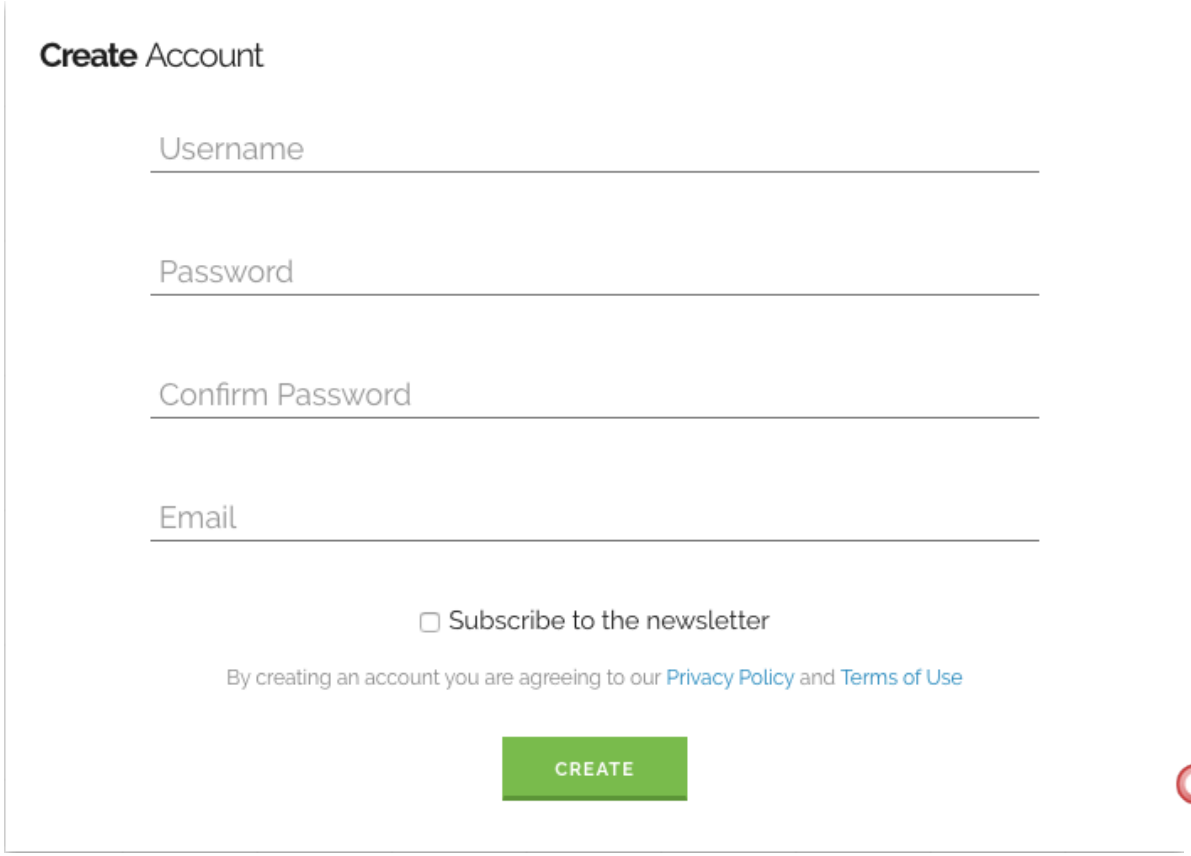
- **N.B.** Prima di utilizzare Shodan è **fortemente consigliata** la **registrazione e** l'**accesso** ad esso
  - **Altrimenti non possono essere usati i suoi filtri di ricerca**



Shodan

Registrazione

- **https://account.shodan.io/register**

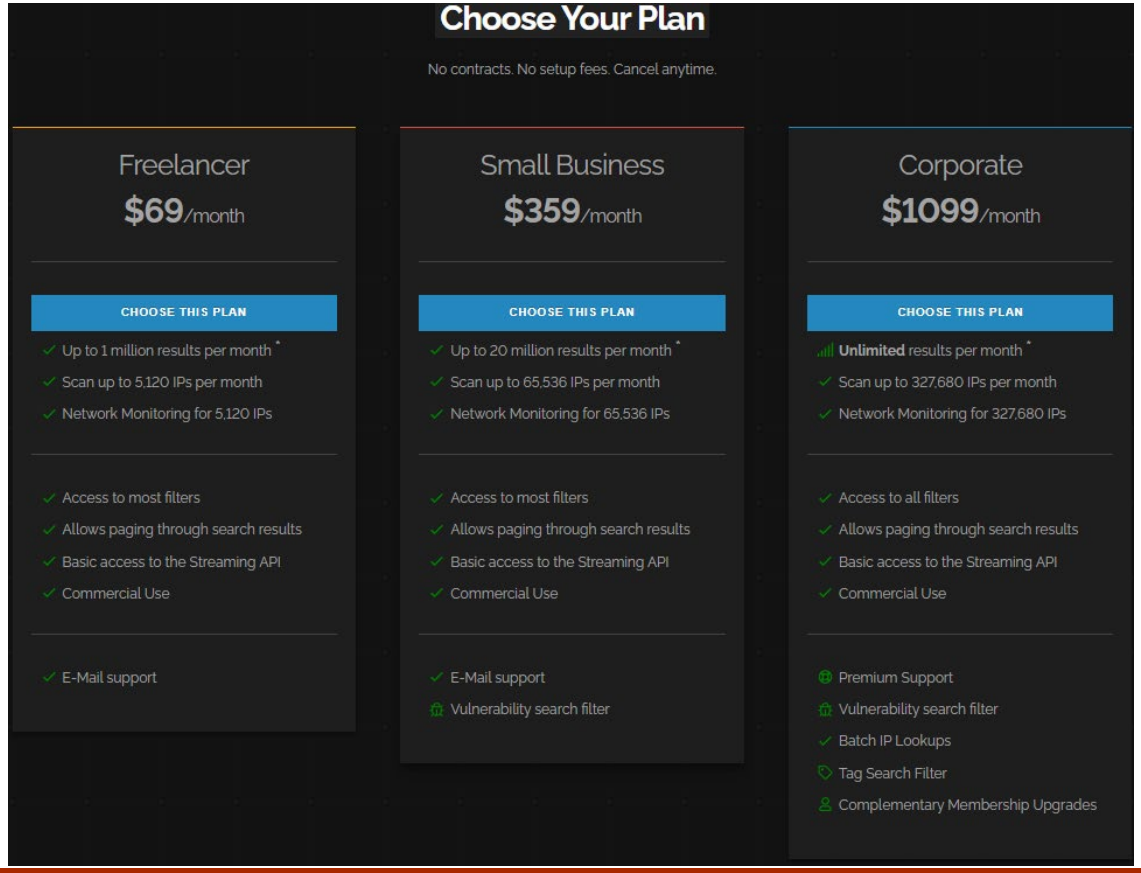


SHODAN
Computer Search Engine

Shodan

Billing

- **`https://account.shodan.io/billing`**



SHODAN
Computer Search Engine

Shodan

Filtri di Ricerca

- Shodan fornisce numerosi filtri di ricerca, raggruppati nelle seguenti categorie
  - **General**
  - **HTTP**
  - **SSL**
  - **Bitcoin**
  - **Restricted**
  - **NTP**
  - **Screenshots**
  - **SNMP**
  - **Telnet**
  - **Cloud**
  - **SSH**

SHODAN
Computer Search Engine

Shodan

Filtri di Ricerca

- Alcuni tra i filtri di Shodan più utilizzati sono
  - **`city:`** cerca i dispositivi in una determinata città
  - **`country:`** cerca i dispositivi in un determinato paese
  - **`geo:`** cerca i dispositivi in base alle coordinate geografiche
  - **`hostname:`** cerca i dispositivi che corrispondono al nome di host
  - **`net:`** ricerca basata su un IP o CIDR
  - **`os:`** ricerca basata sul Sistema Operativo
  - **`port:`** cerca dispositivi che hanno determinate porte aperte
  - **`before/after:`** cerca risultati appartenenti ad un determinato intervallo temporale

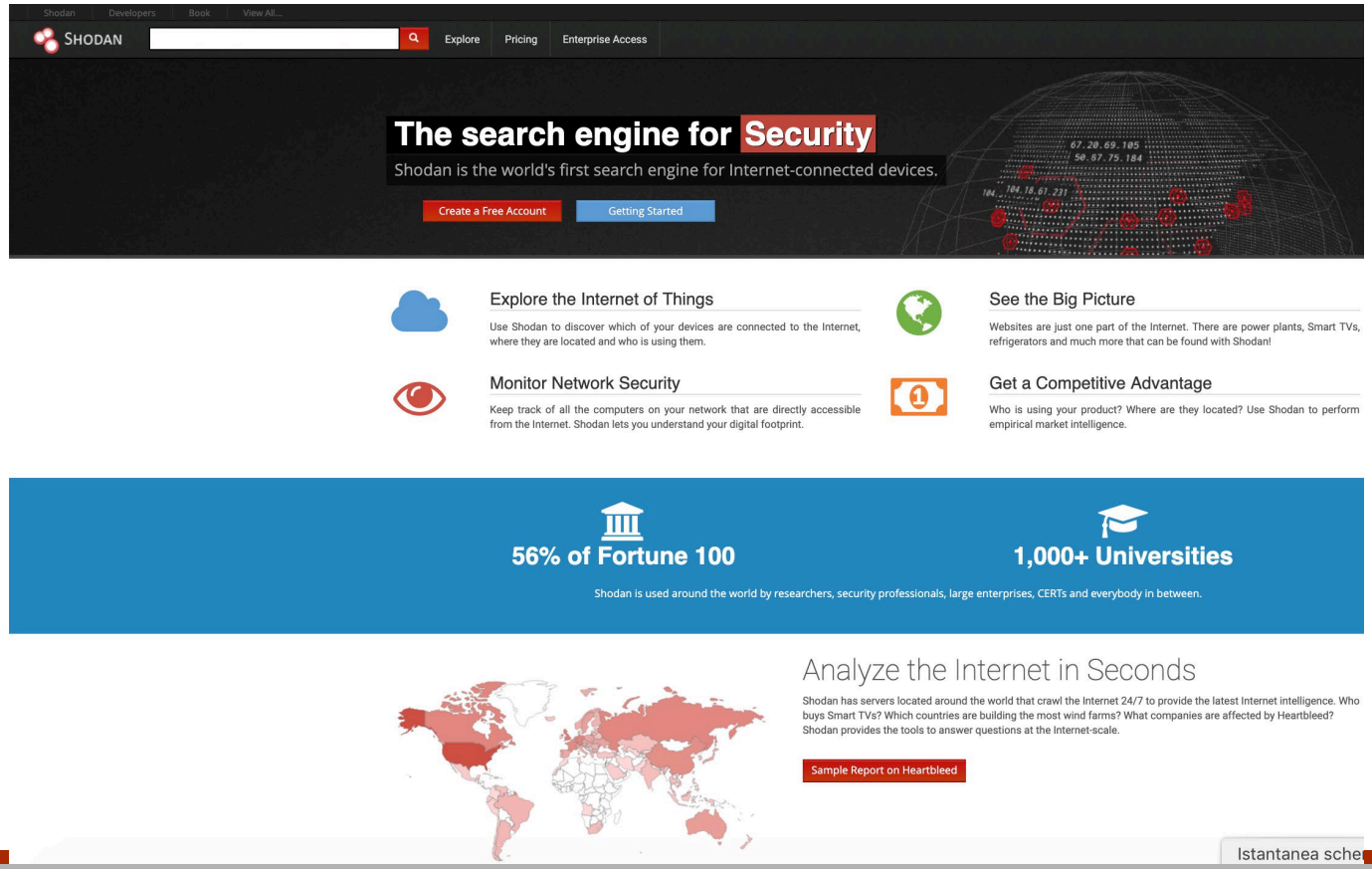
https://www.shodan.io/search/filters

SHODAN
Computer Search Engine

Shodan

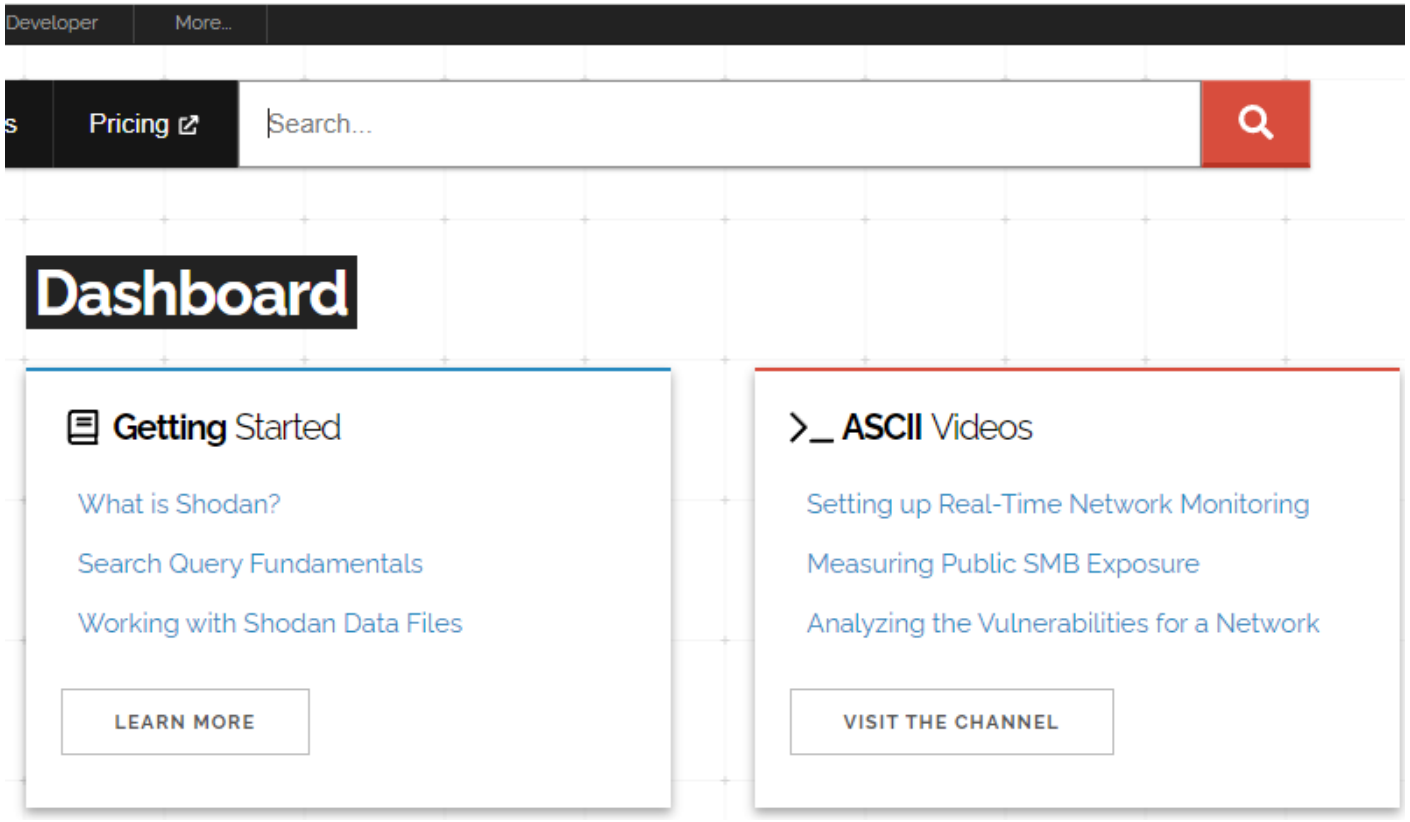
Esempio 1

- **https://www.shodan.io/**



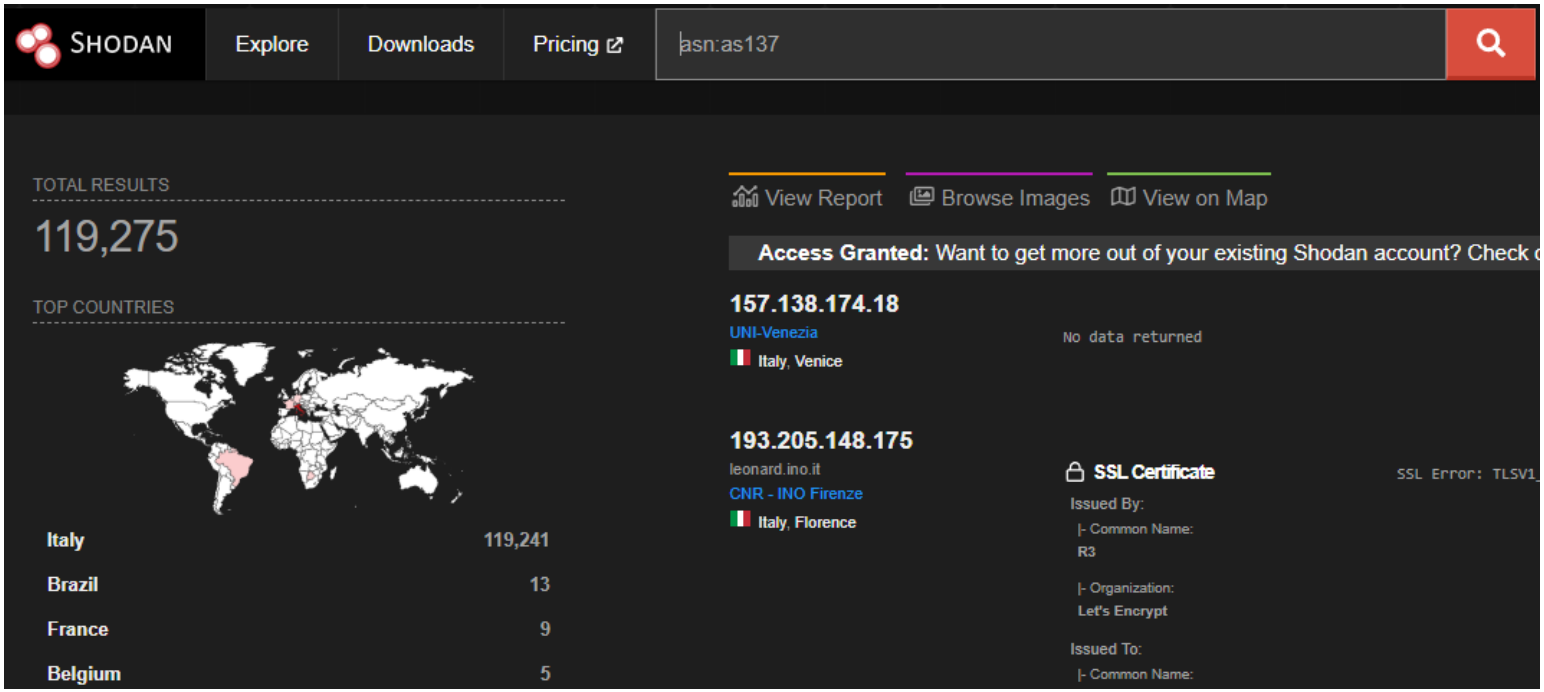
Shodan
Esempio 1

- Effettuiamo una ricerca per Autonomous System Network (**`asn:as137`**)



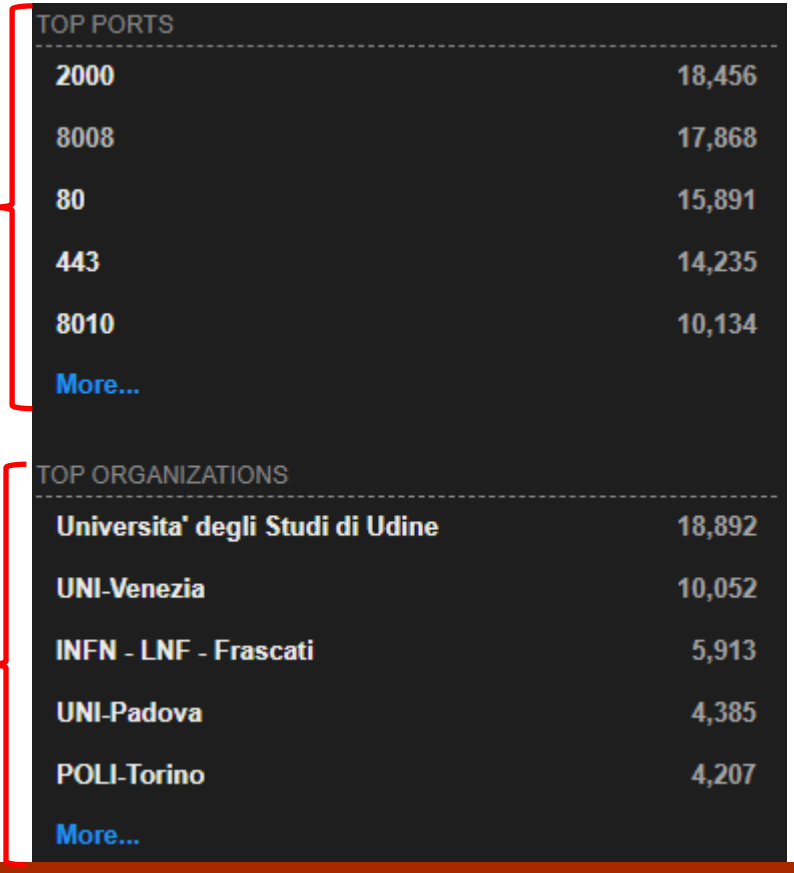
Shodan
Esempio 1

- Effettuiamo una ricerca per Autonomous System Network (**`asn:as137`**)



Shodan
Esempio 1

- Effettuiamo una ricerca per Autonomous System Network (`asn:as137`)



Porte più utilizzate

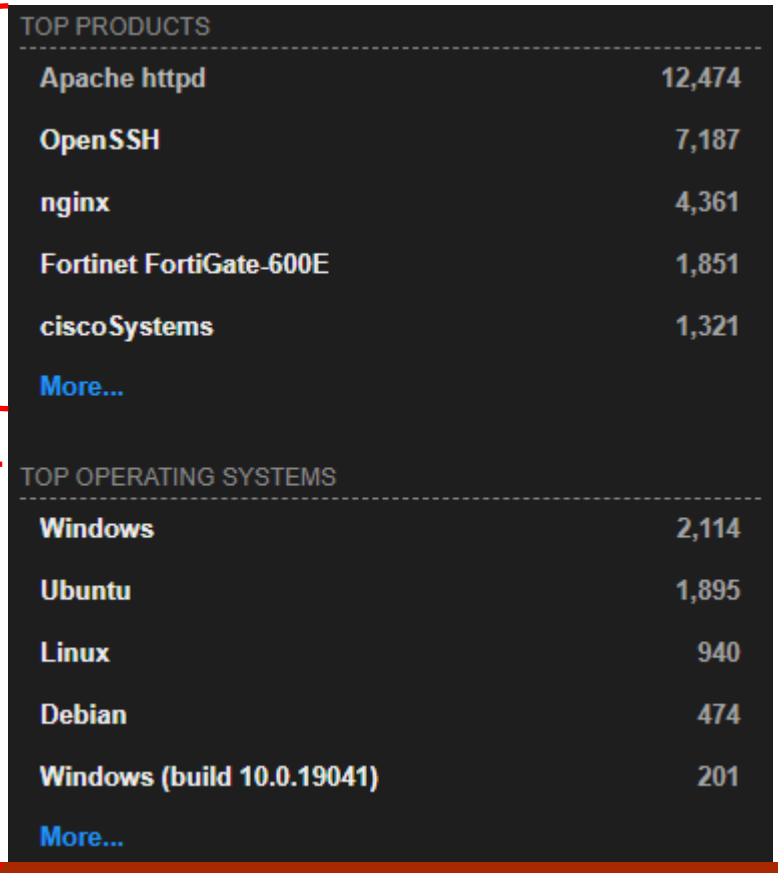
Organizzazioni con il maggior numero di dispositivi censiti

Shodan
Esempio 1

- Effettuiamo una ricerca per Autonomous System Network (`asn:as137`)

Software più utilizzati

Sistemi Operativi più utilizzati

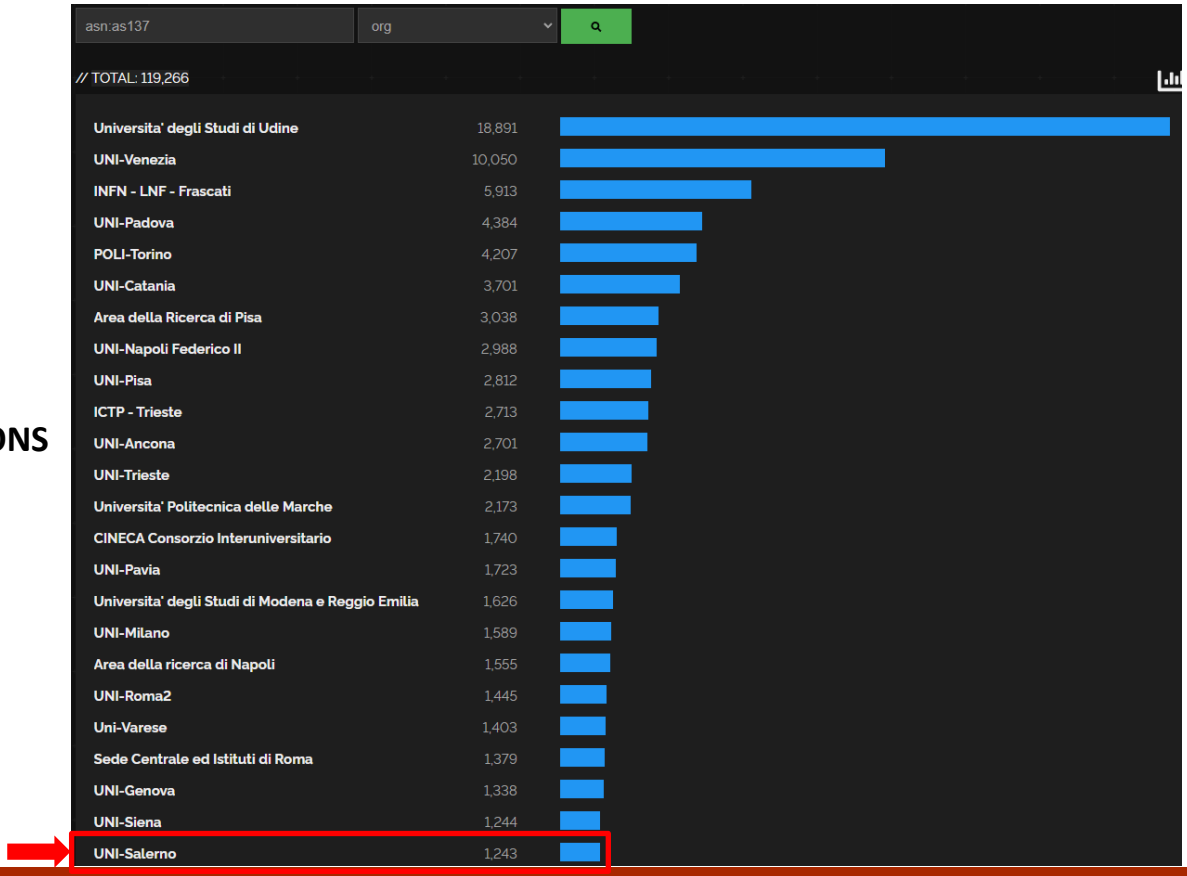


Shodan

Esempio 1

- Selezioniamo l'organizzazione **`UNI-Salerno`**

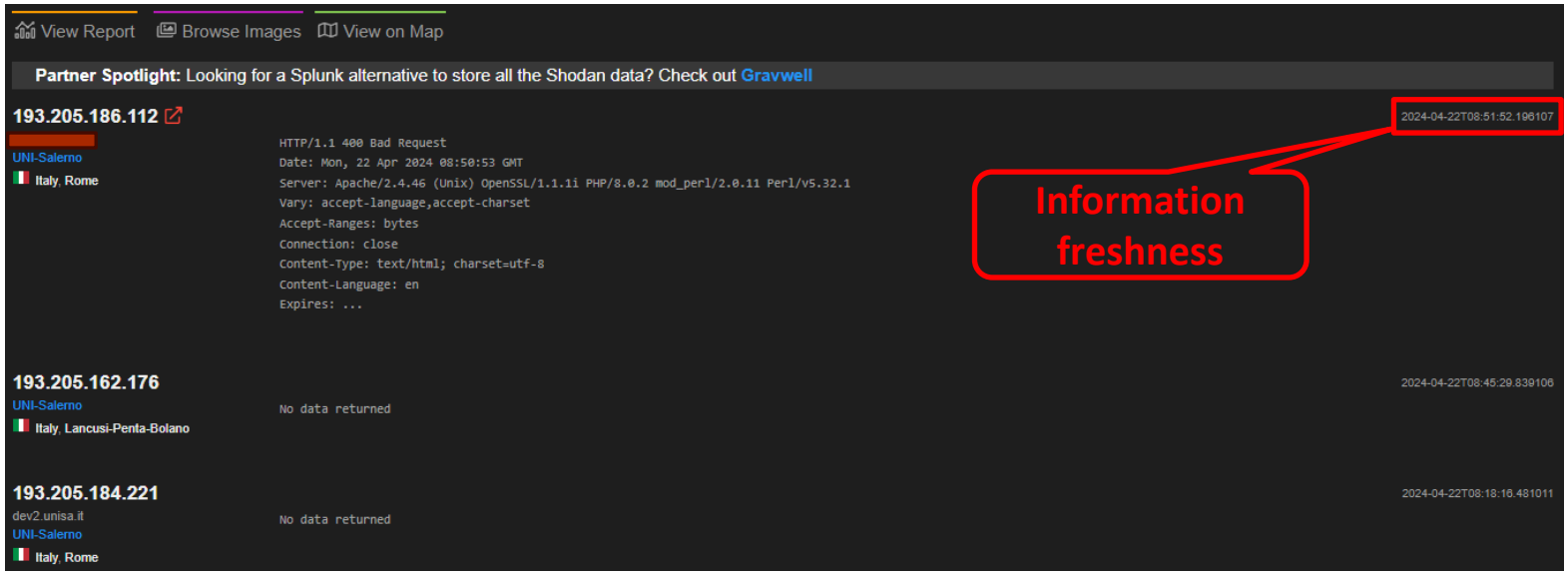
TOP ORGANIZATIONS



Shodan

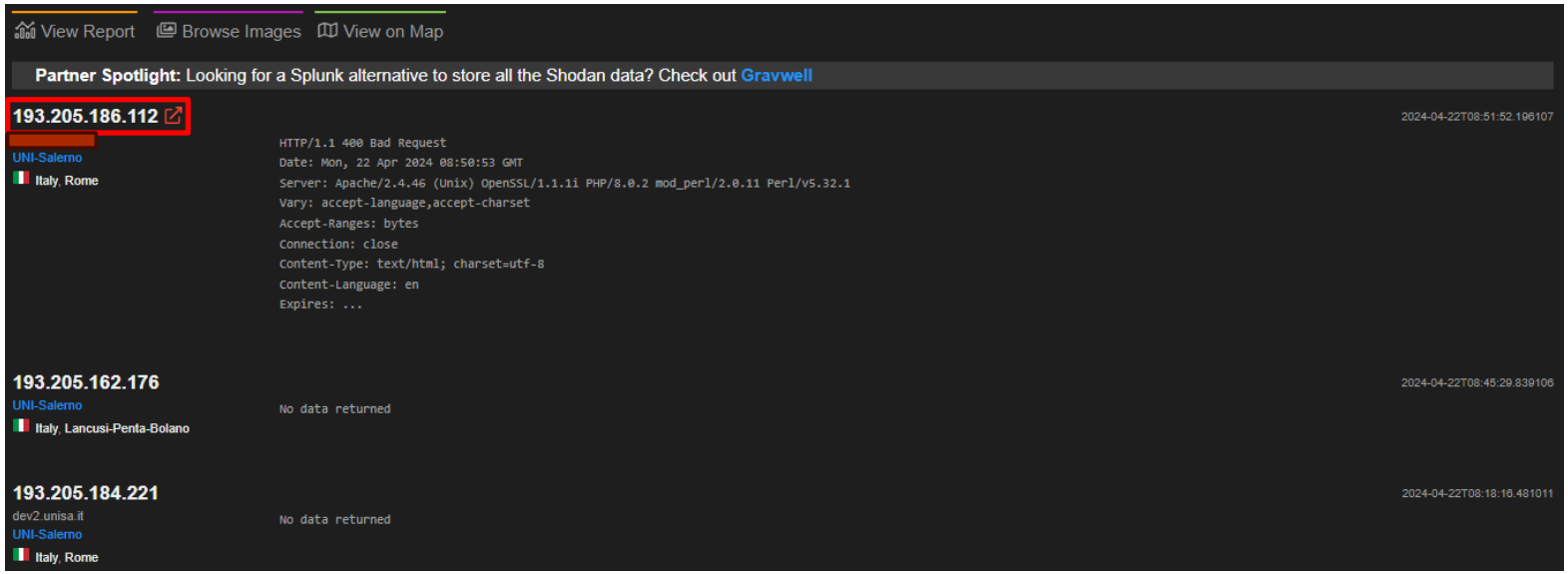
Esempio 1

- Information freshness



Shodan
Esempio 1

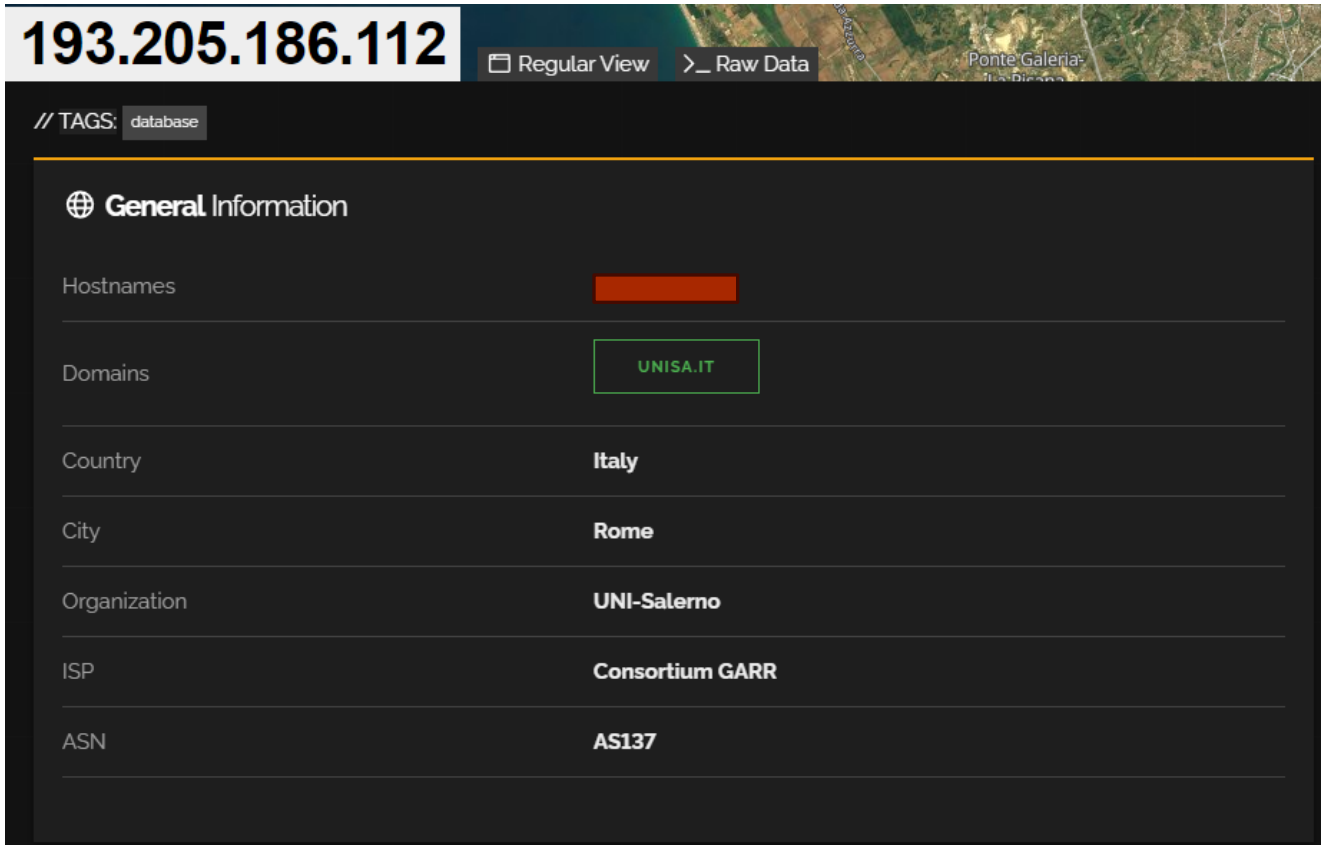
- Selezioniamo l'indirizzo IP 193.205.186.112



Shodan

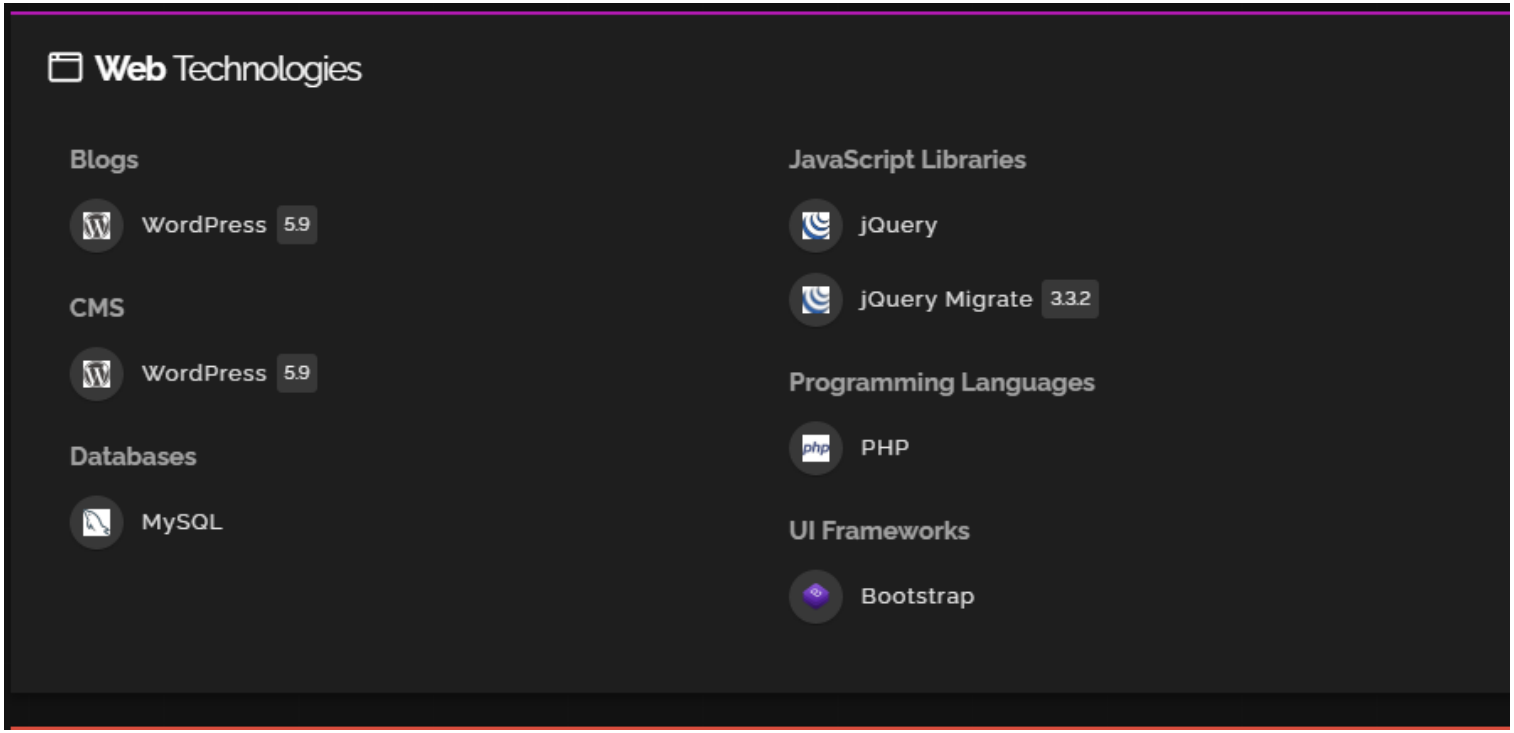
Esempio 1

- Informazioni relative all'indirizzo IP 193.205.186.112 (Informazioni Generali)



Shodan
Esempio 1

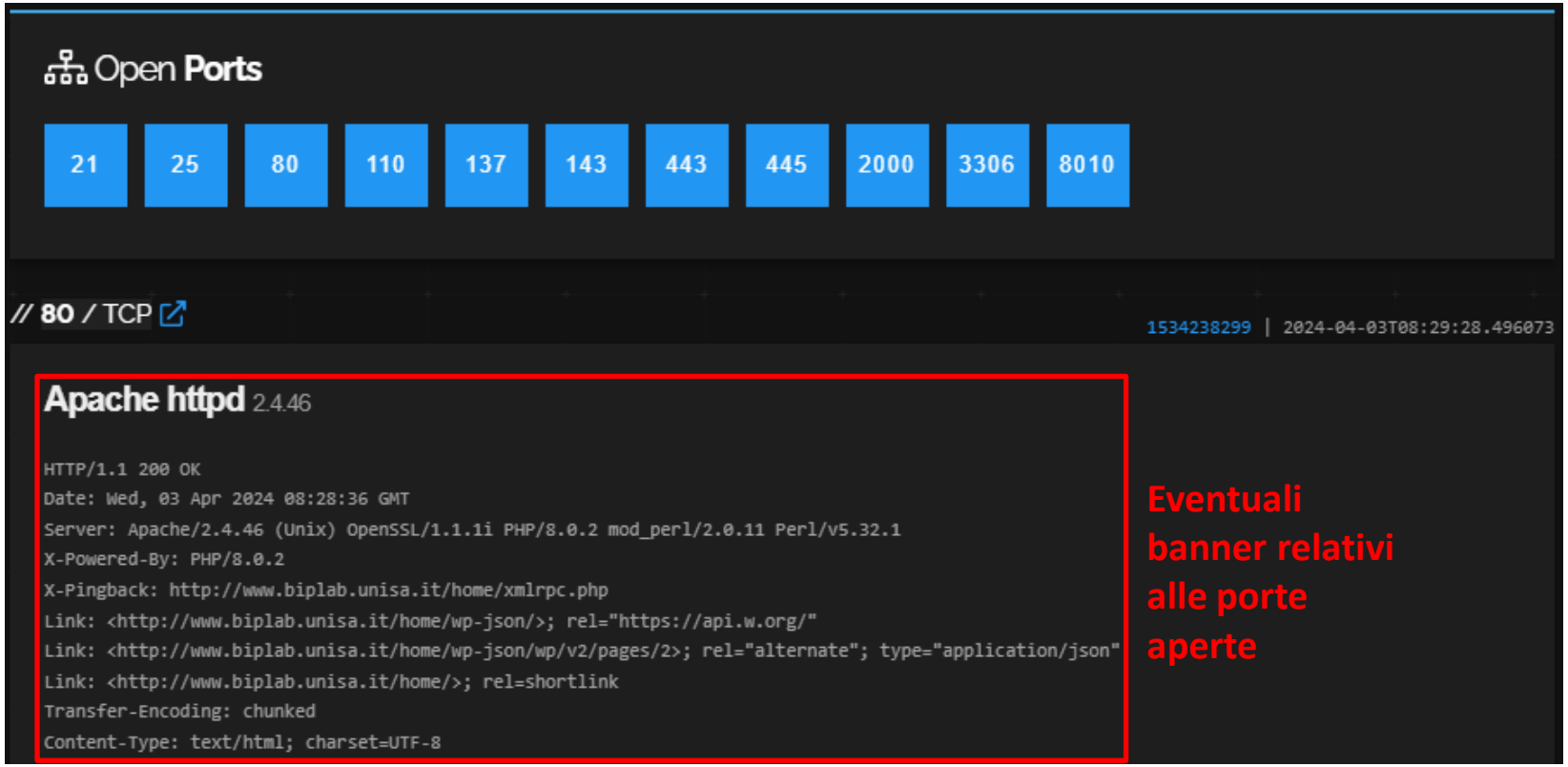
- Informazioni relative all'indirizzo IP 193.205.186.112 (Tecnologie Web)



Shodan

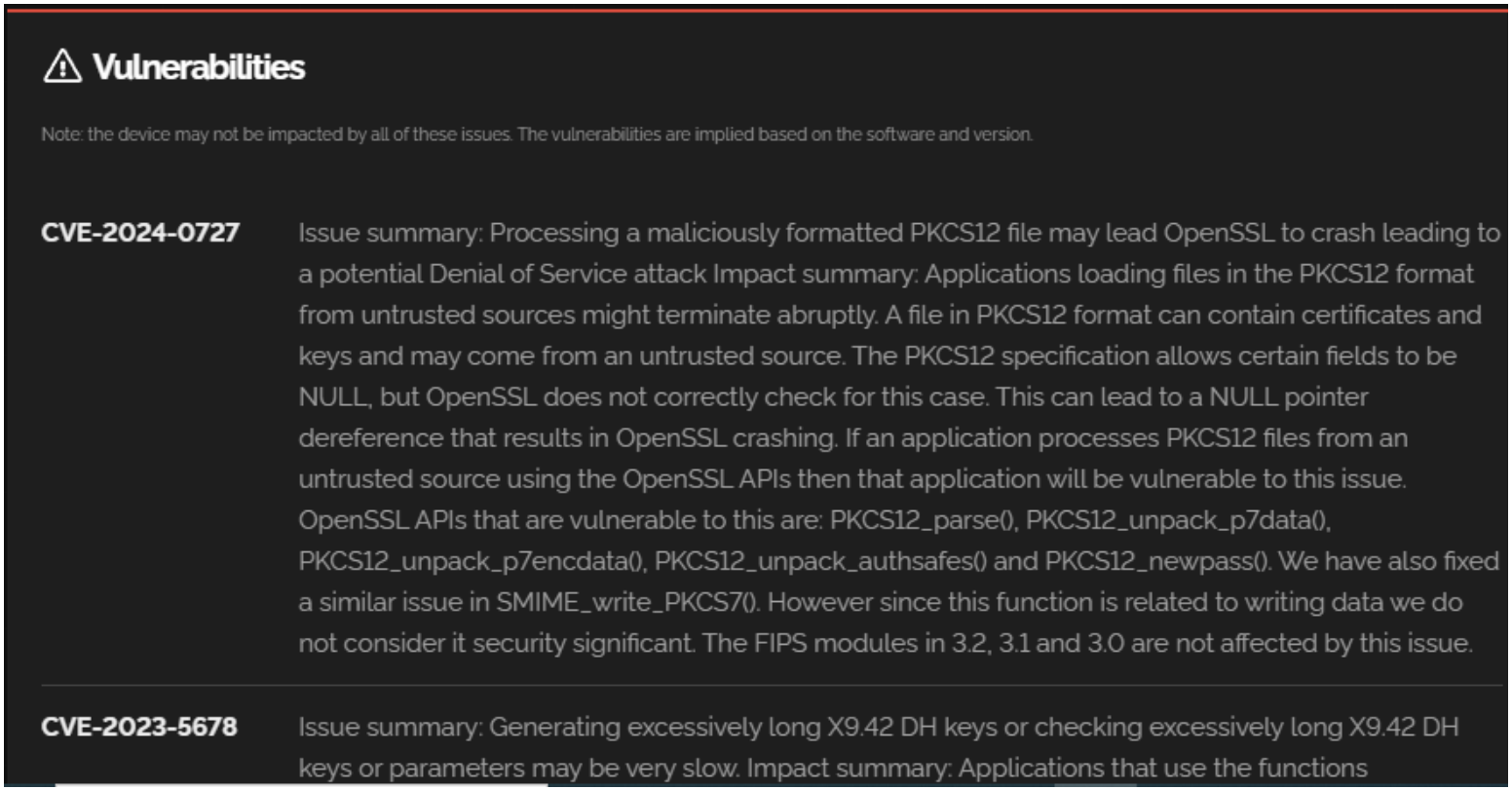
Esempio 1

- Informazioni relative all'indirizzo IP 193.205.186.112 (Porte Aperte)



Shodan
Esempio 1

- Informazioni relative all'indirizzo IP 193.205.186.112 (Vulnerabilità)



⚠ Vulnerabilities

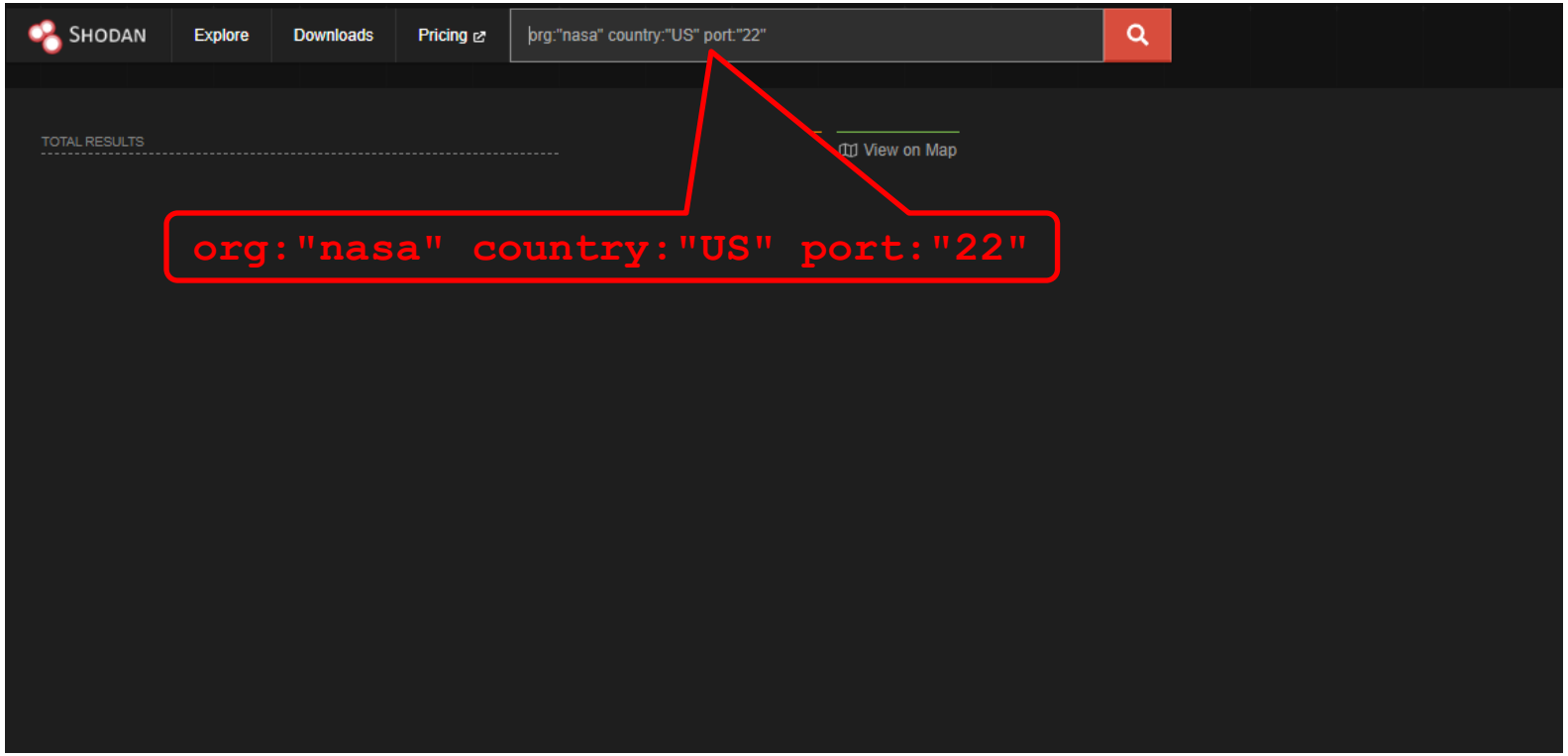
Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2024-0727 Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSL to crash leading to a potential Denial of Service attack Impact summary: Applications loading files in the PKCS12 format from untrusted sources might terminate abruptly. A file in PKCS12 format can contain certificates and keys and may come from an untrusted source. The PKCS12 specification allows certain fields to be NULL, but OpenSSL does not correctly check for this case. This can lead to a NULL pointer dereference that results in OpenSSL crashing. If an application processes PKCS12 files from an untrusted source using the OpenSSL APIs then that application will be vulnerable to this issue. OpenSSL APIs that are vulnerable to this are: PKCS12_parse(), PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes() and PKCS12_newpass(). We have also fixed a similar issue in SMIME_write_PKCS7(). However since this function is related to writing data we do not consider it security significant. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue.

CVE-2023-5678 Issue summary: Generating excessively long X9.42 DH keys or checking excessively long X9.42 DH keys or parameters may be very slow. Impact summary: Applications that use the functions

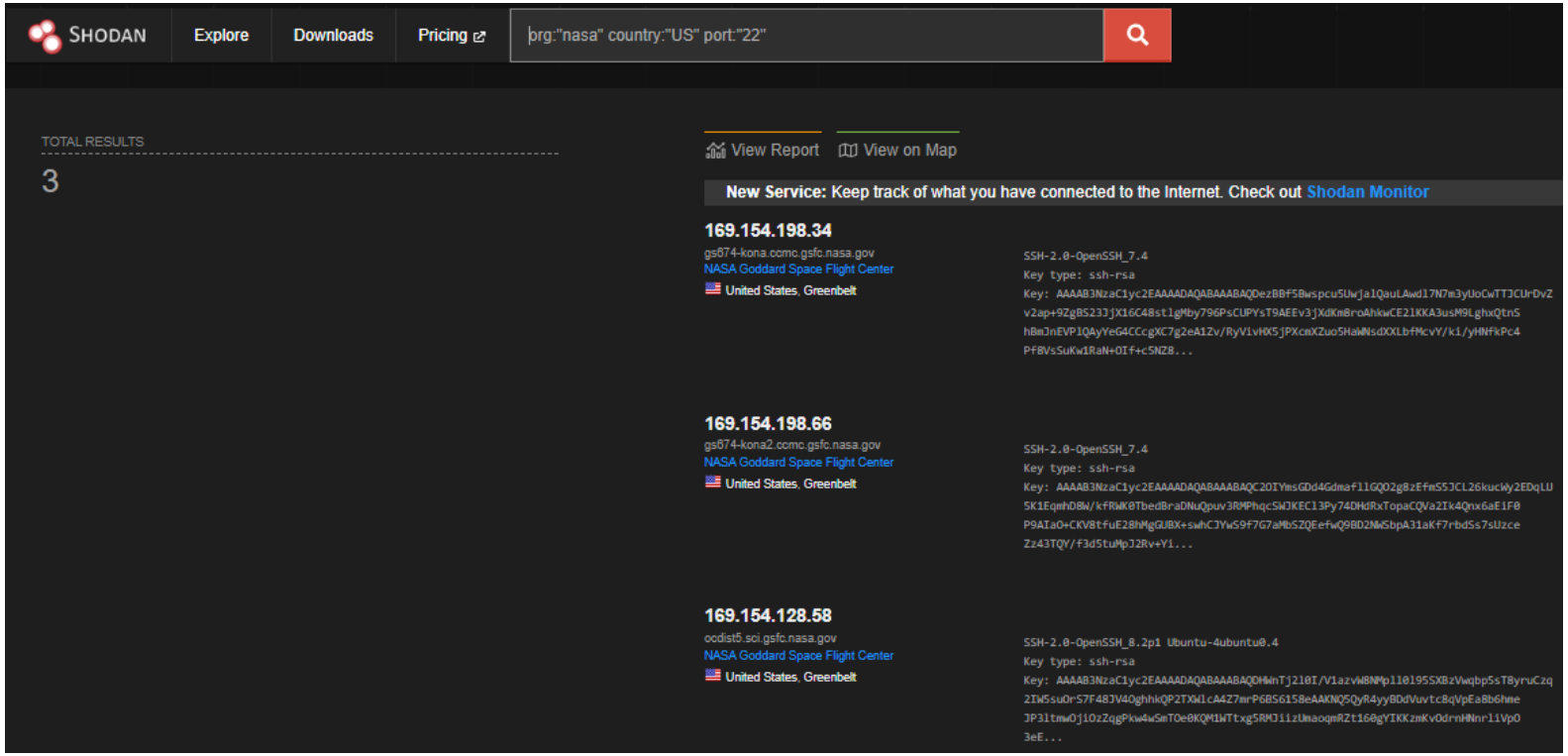
Shodan

Esempio 2



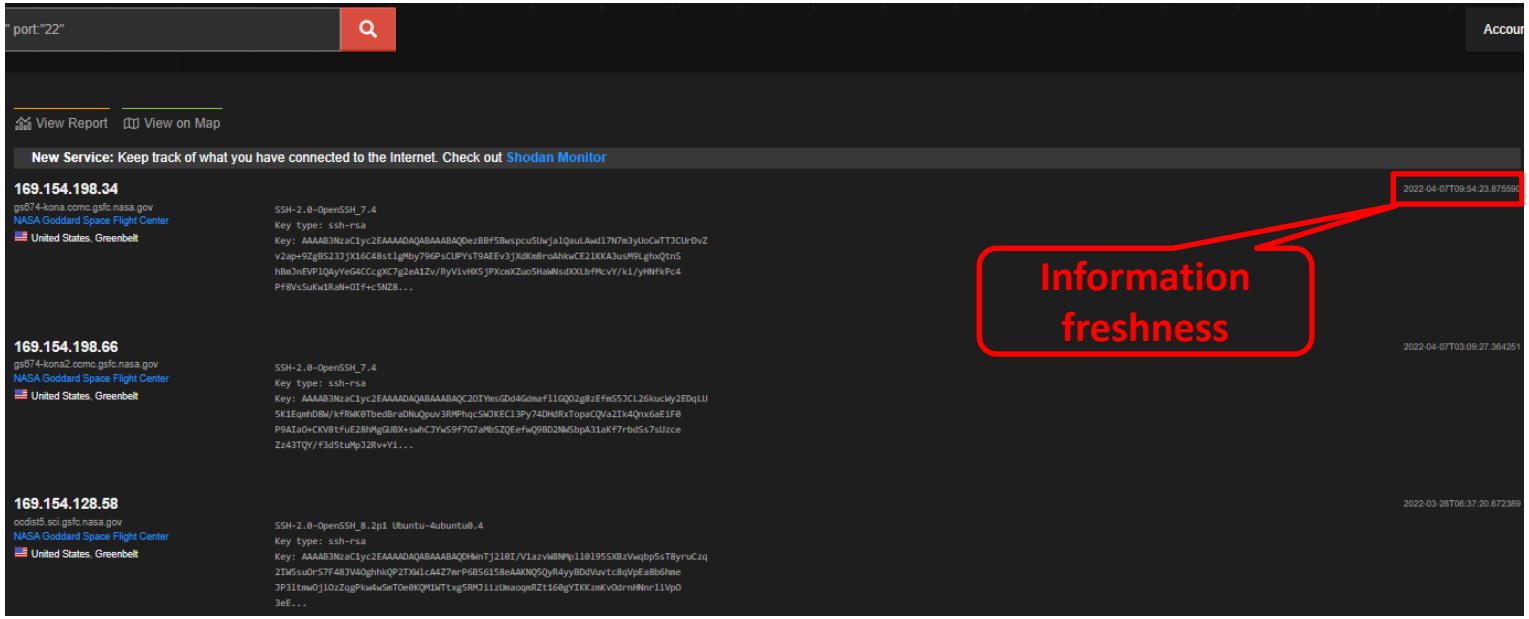
Shodan

Esempio 2



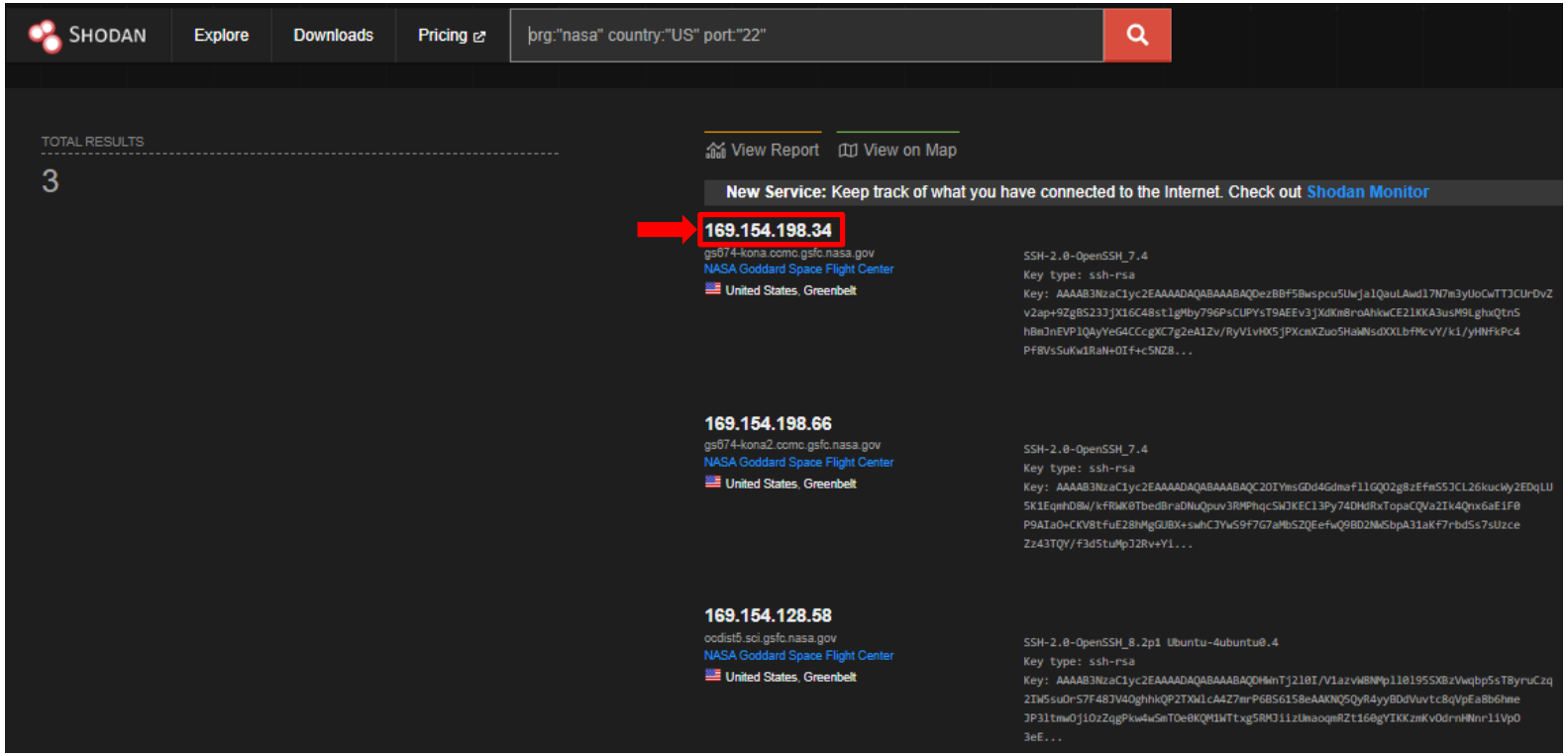
Shodan

Esempio 2



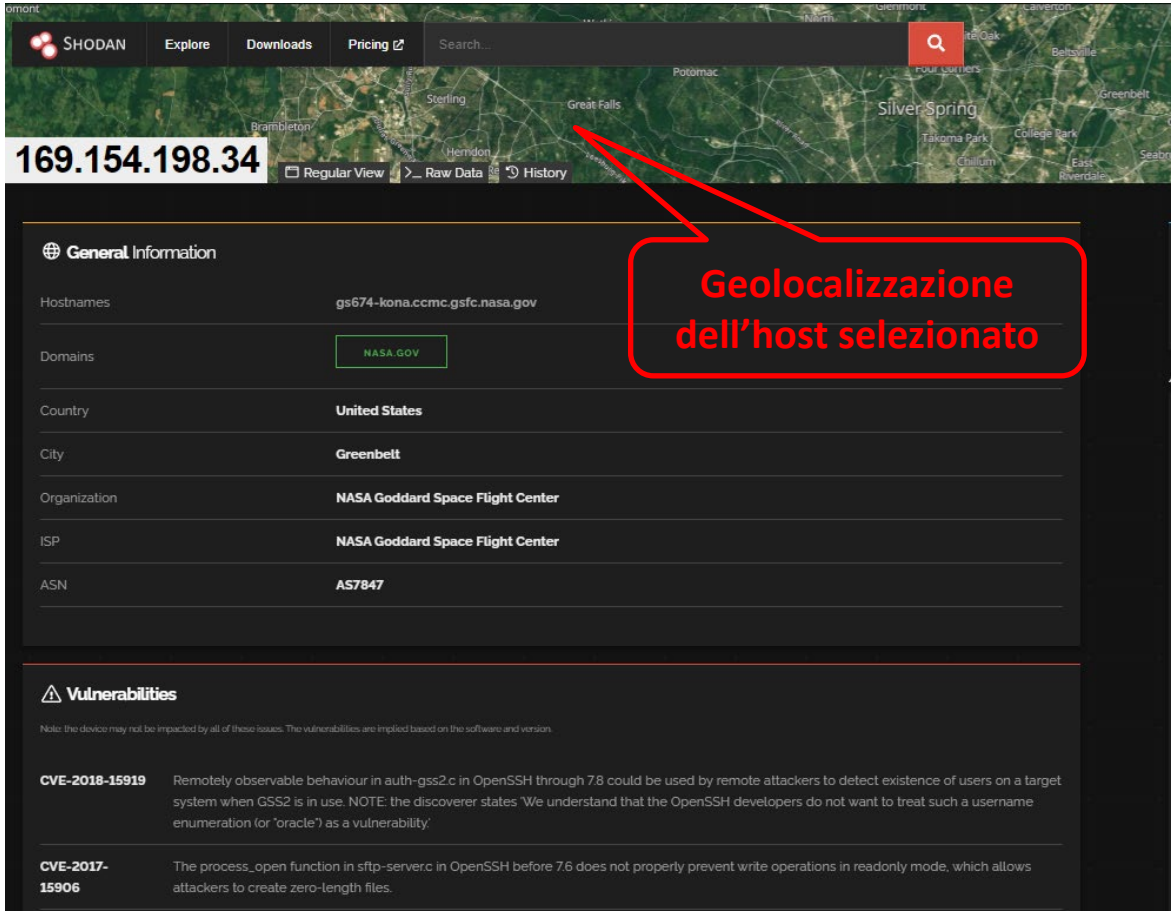
Shodan

Esempio 2



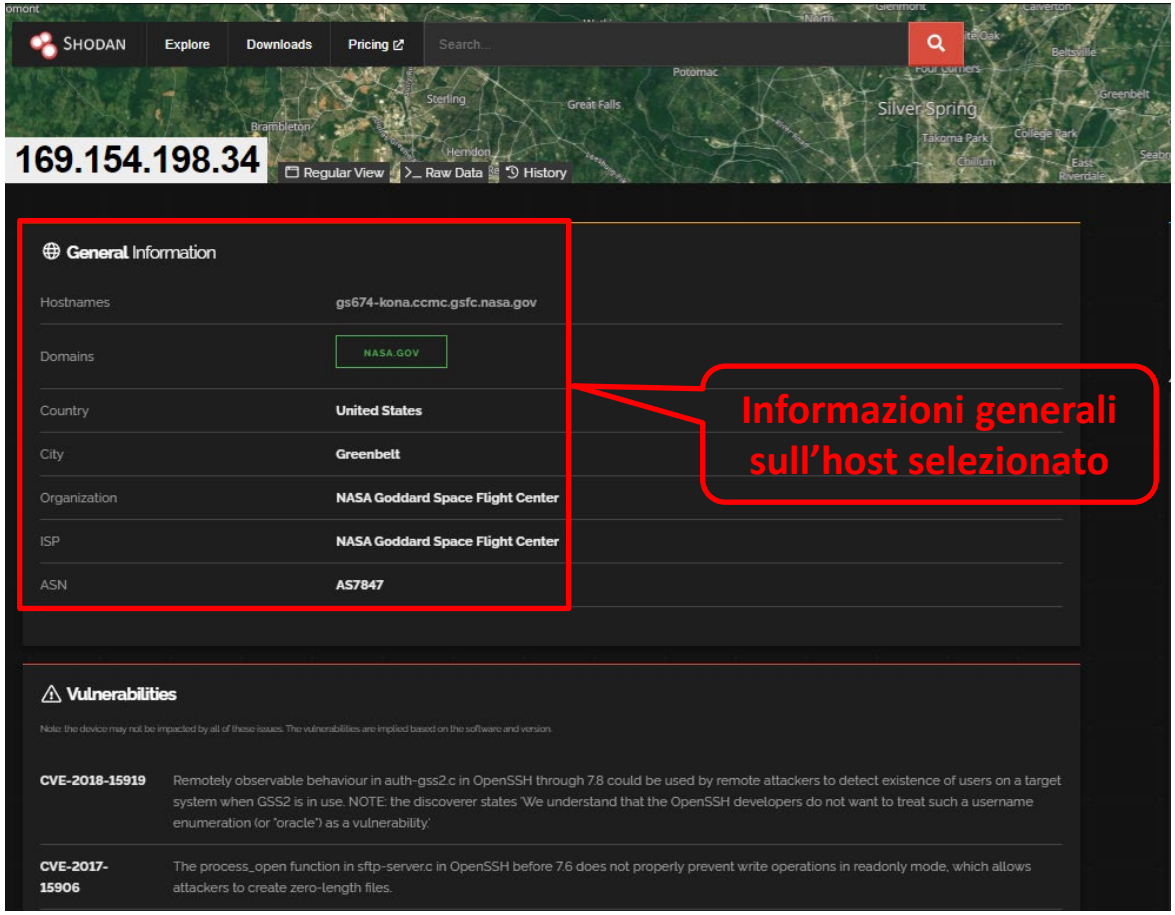
Shodan

Esempio 2



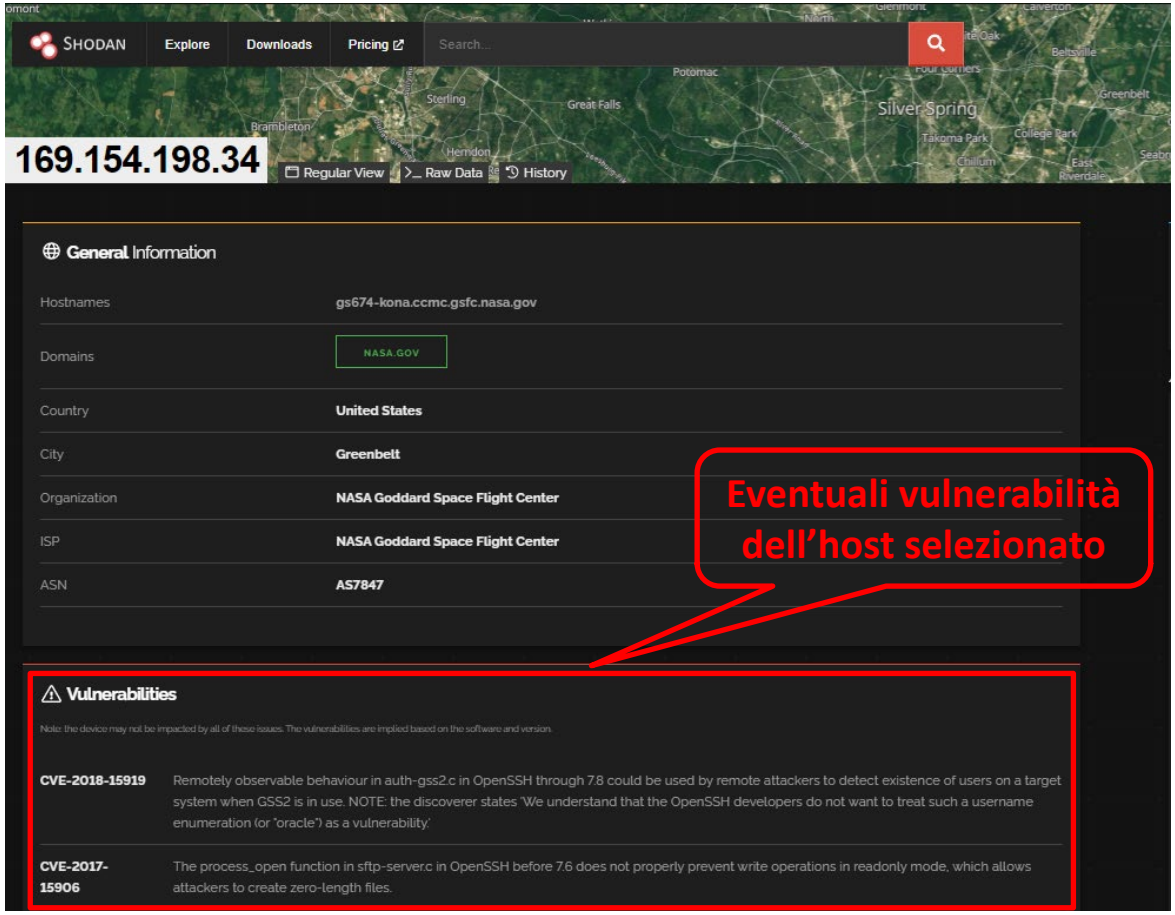
Shodan

Esempio 2



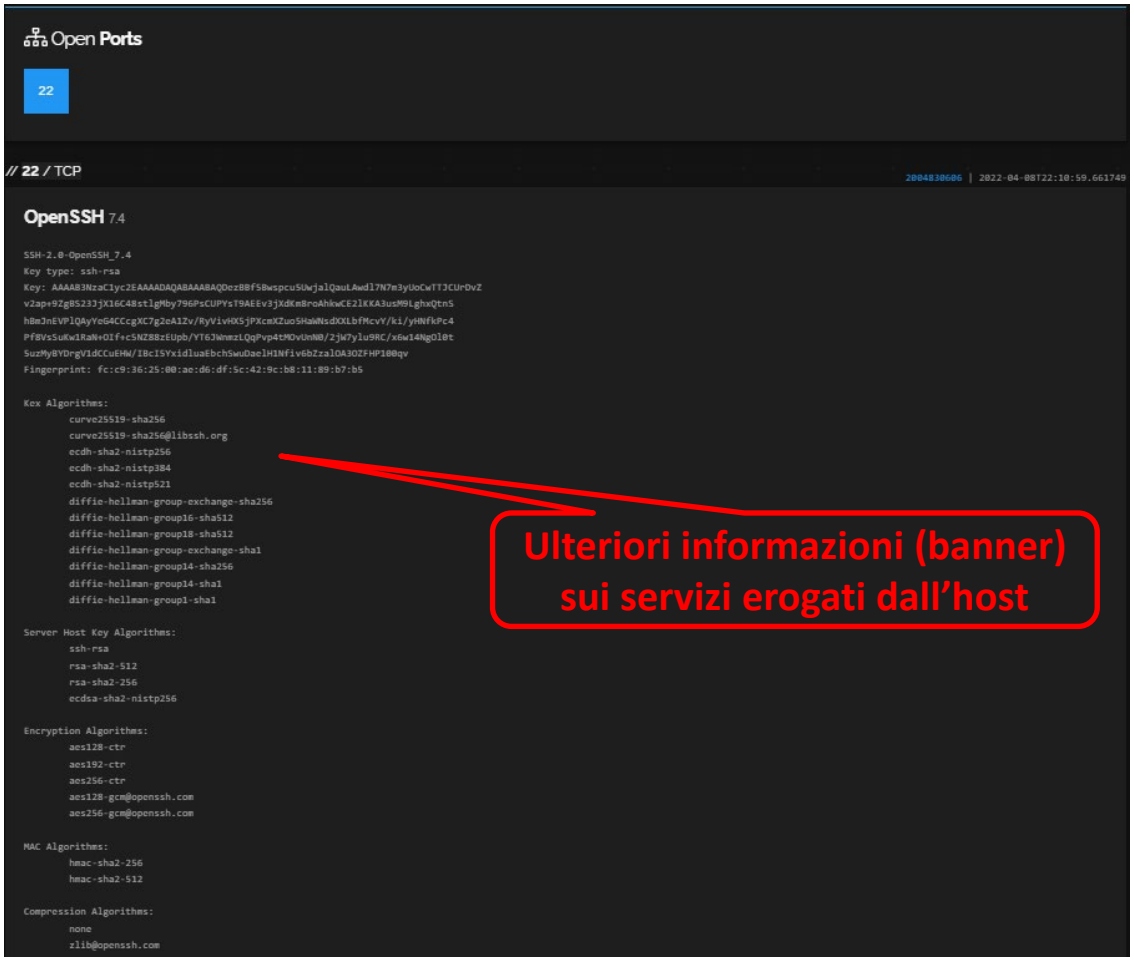
Shodan

Esempio 2



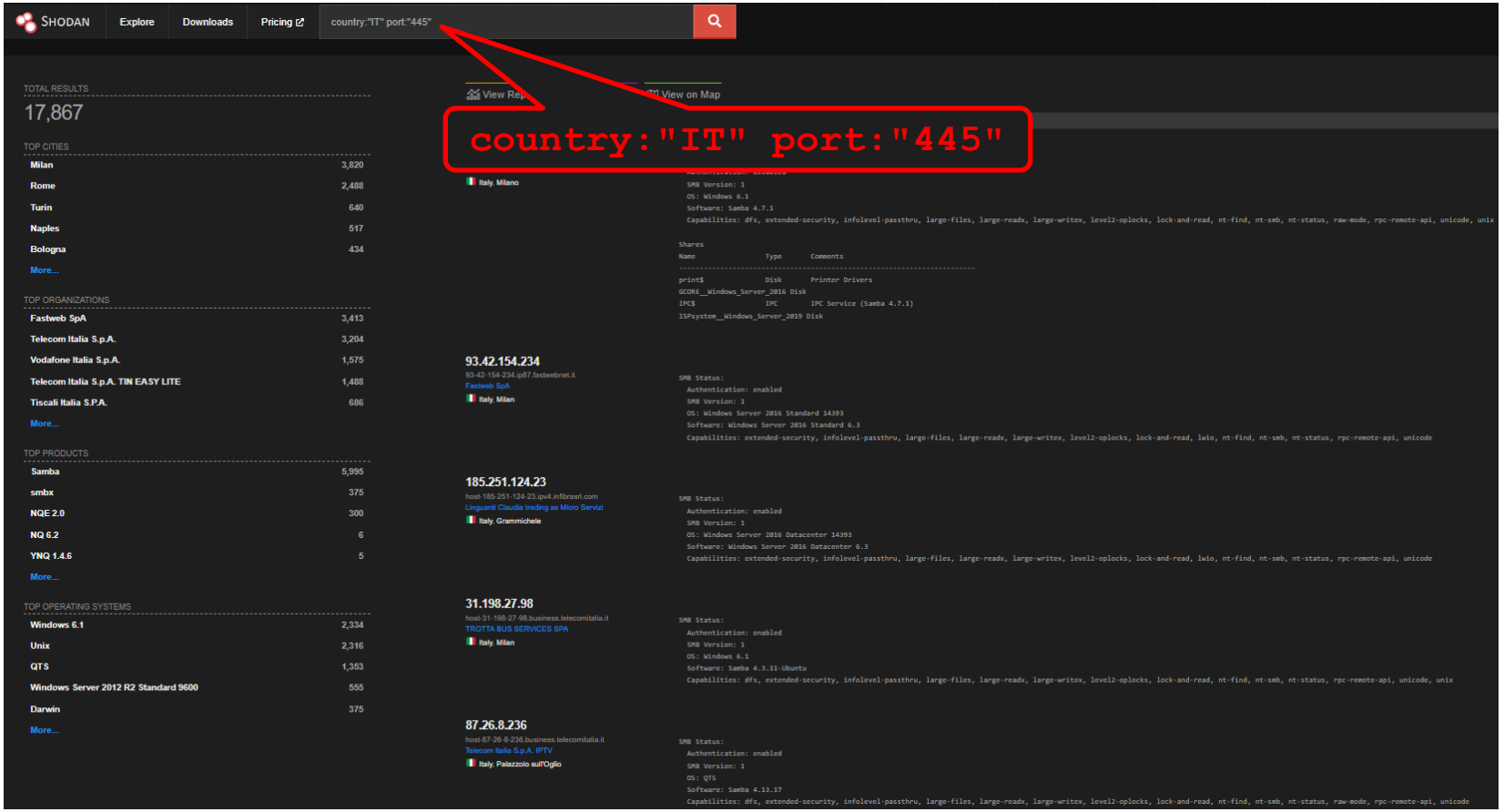
Shodan

Esempio 2



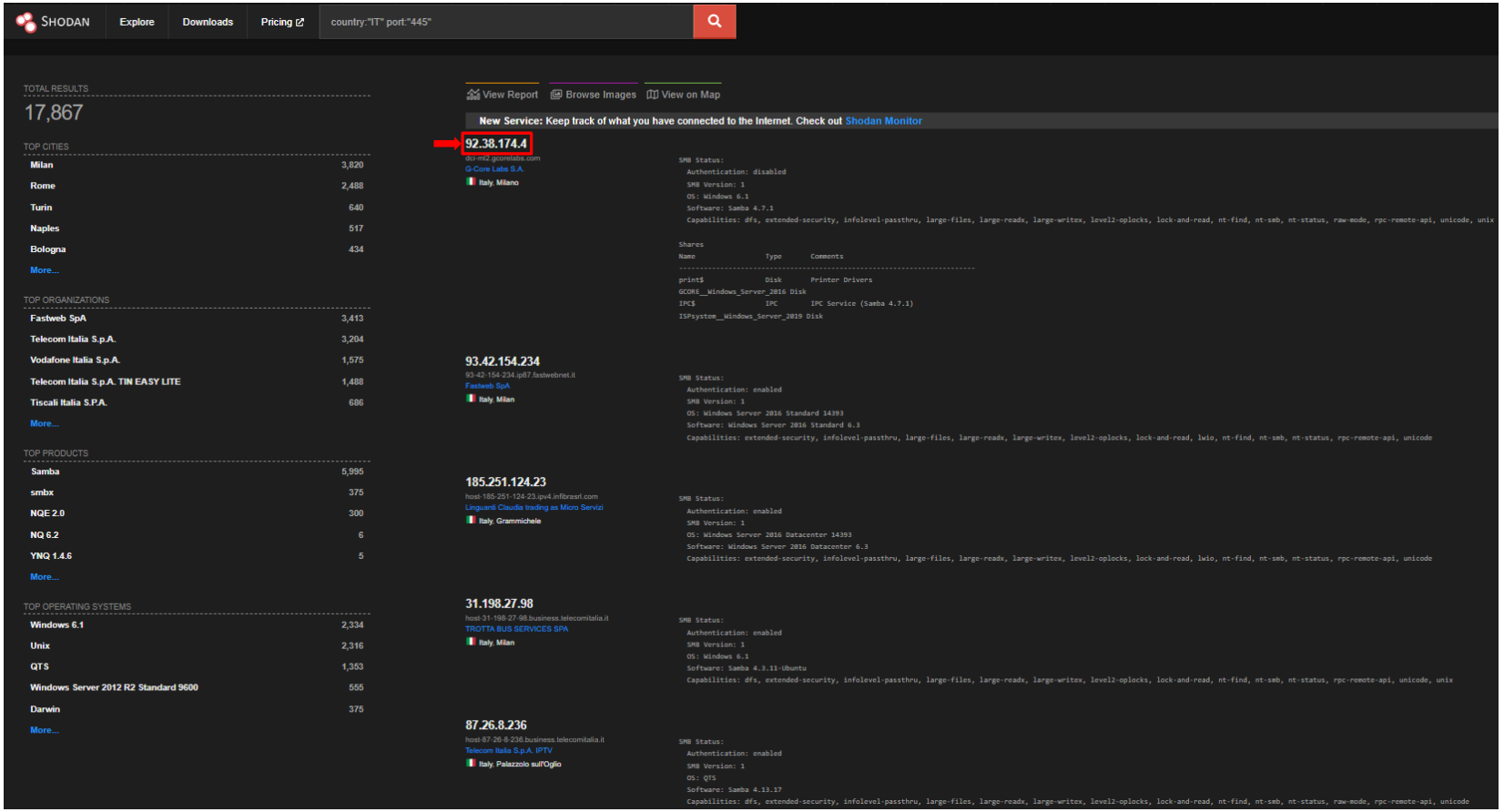
Shodan

Esempio 3



Shodan

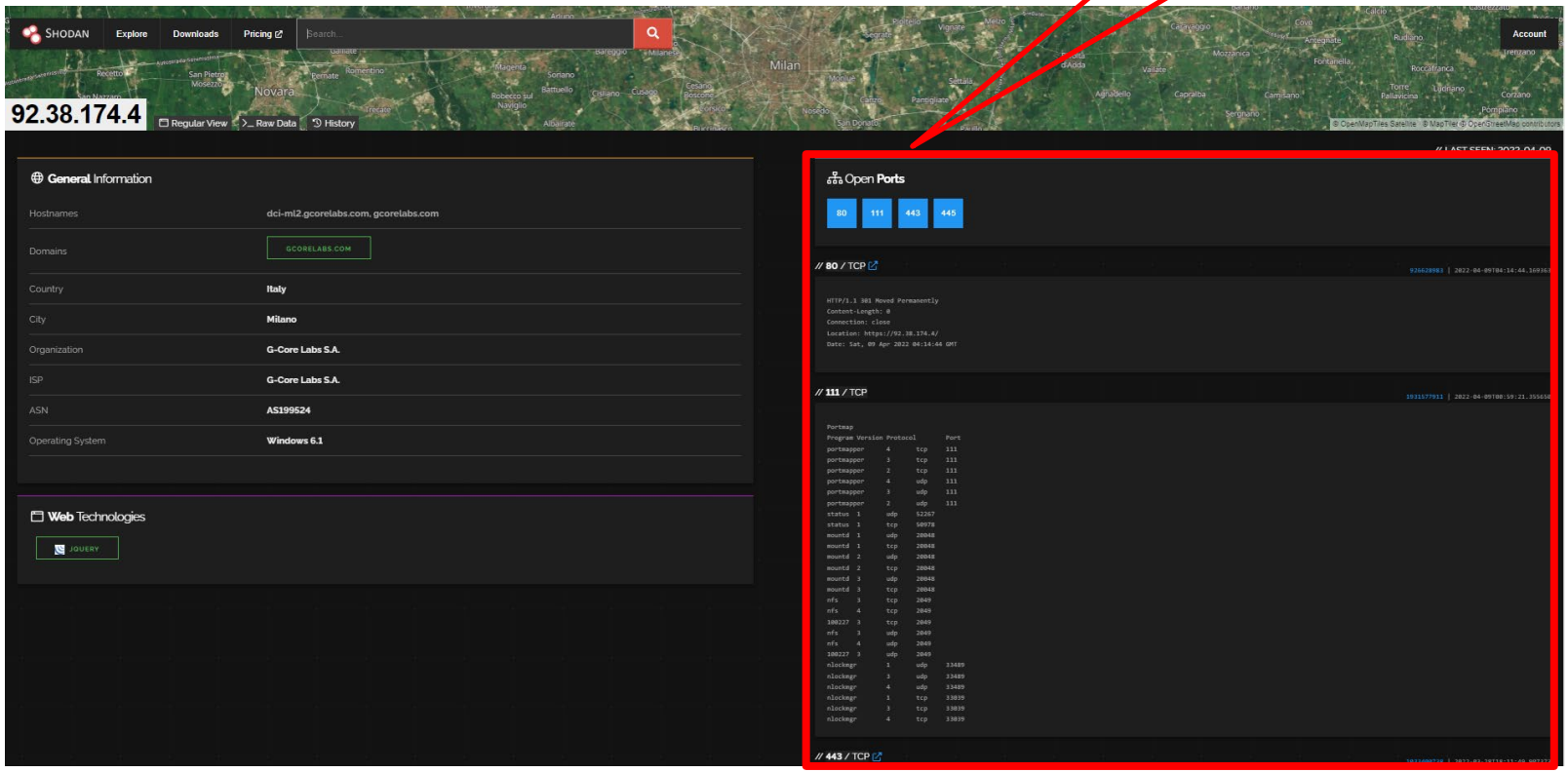
Esempio 3



Shodan

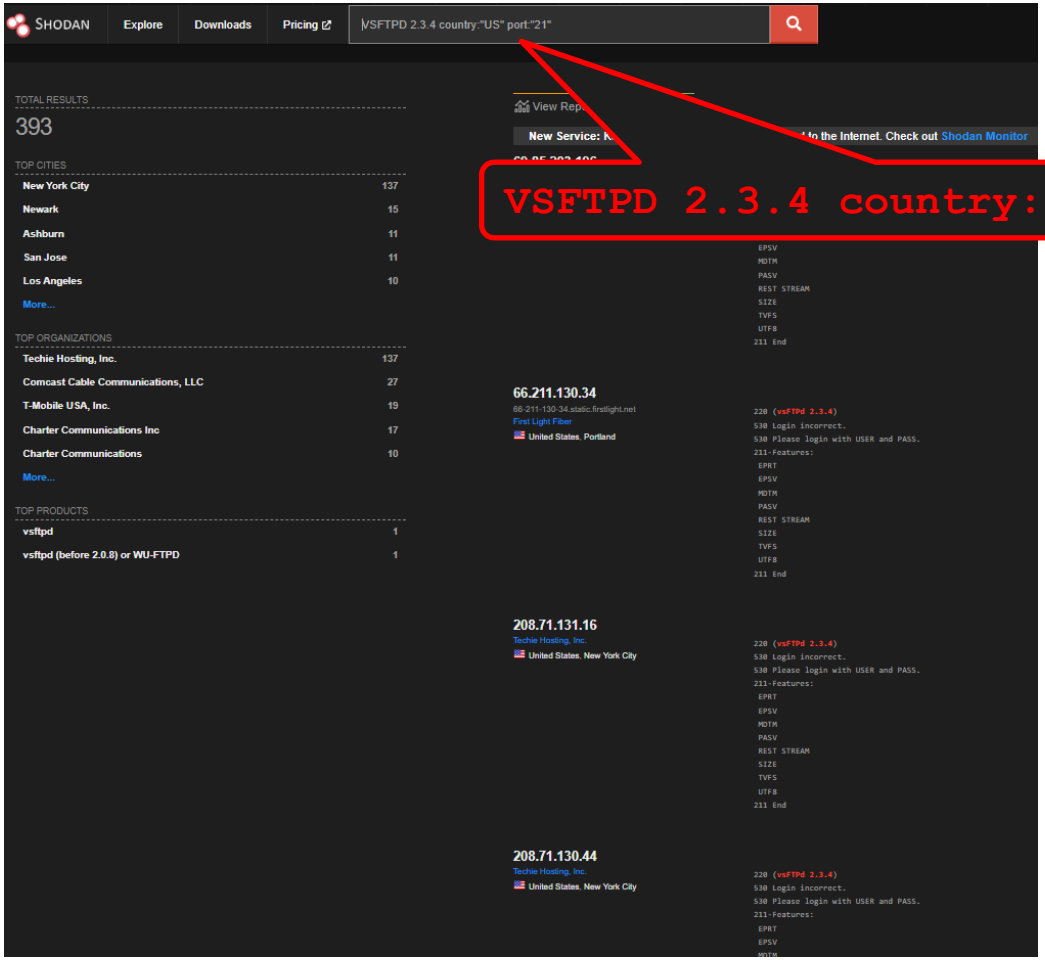
Esempio 3

Informazioni sulle altre porte aperte presenti sull'host selezionato



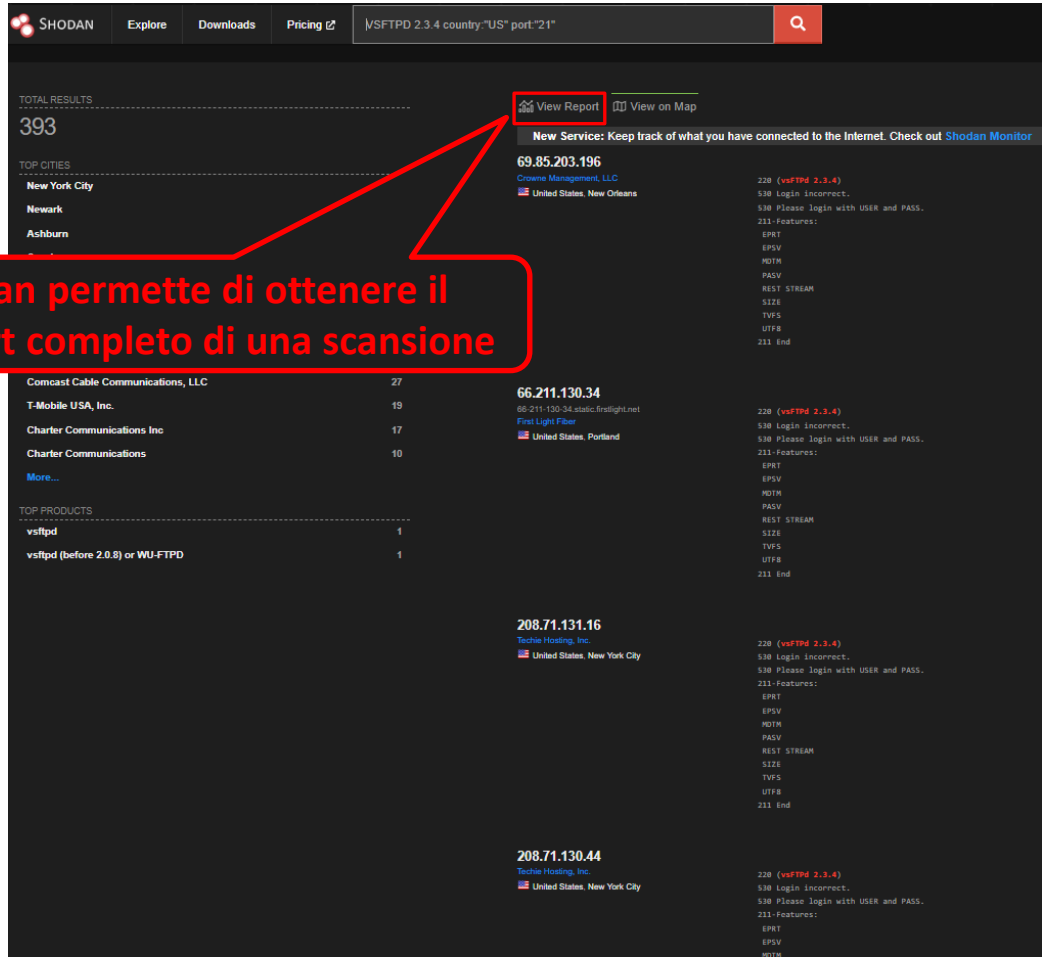
Shodan

Esempio 4



Shodan

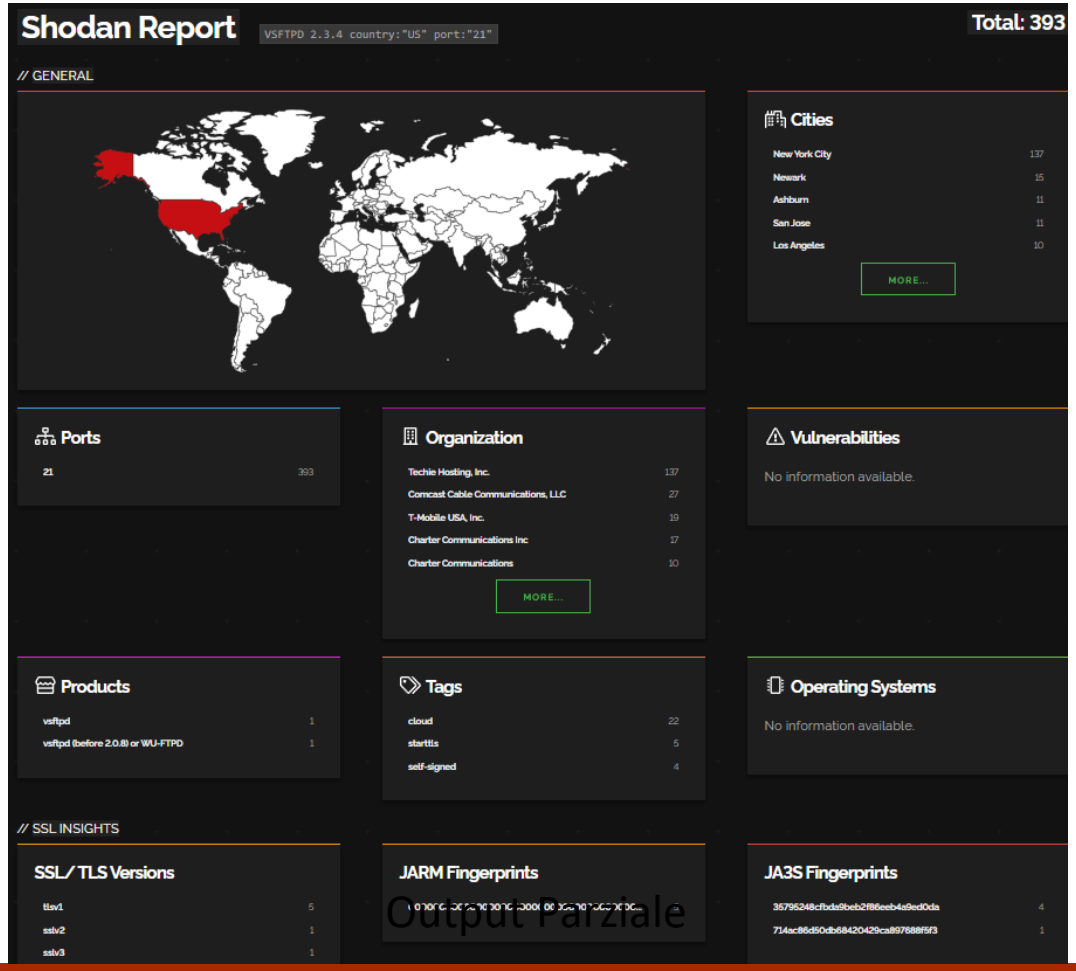
Esempio 4



➢ **Shodan permette di ottenere il report completo di una scansione**

Shodan

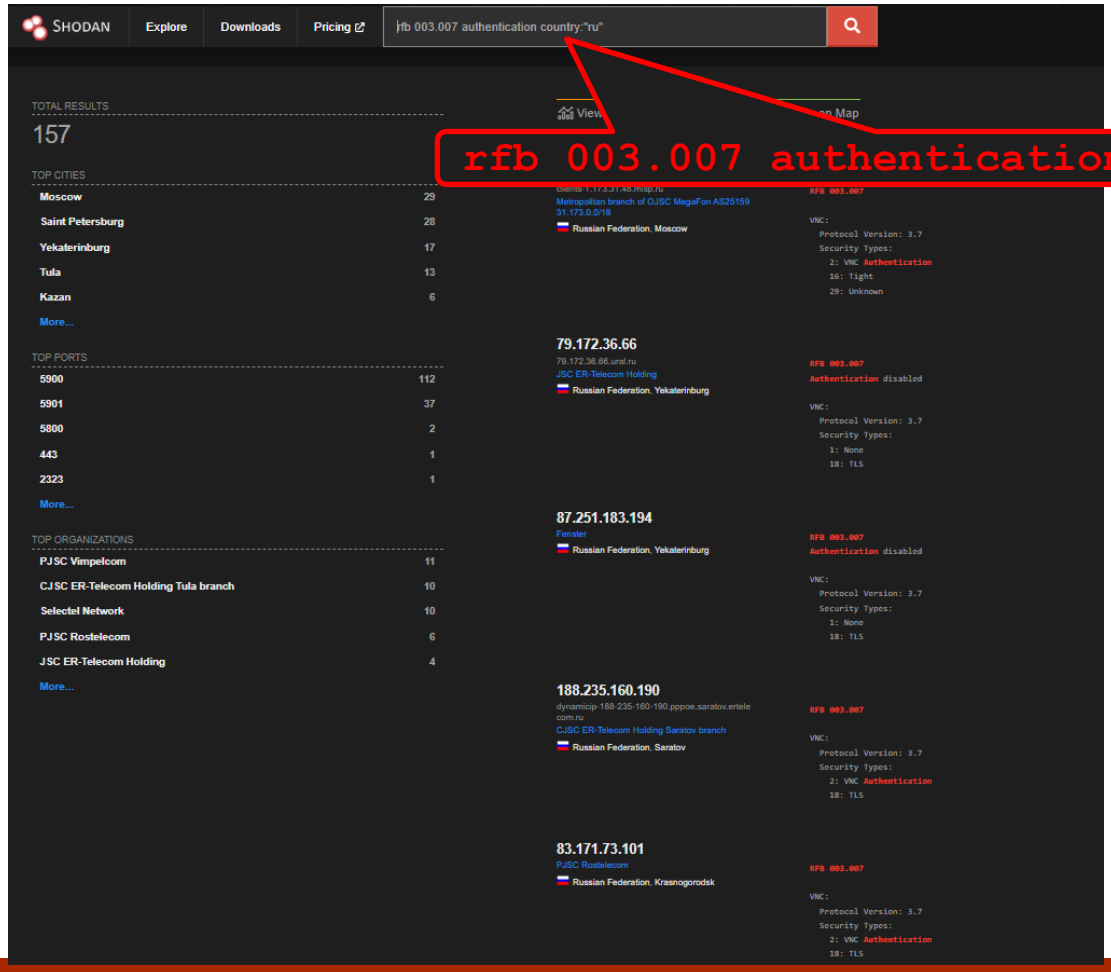
Esempio 4



Output Parziale

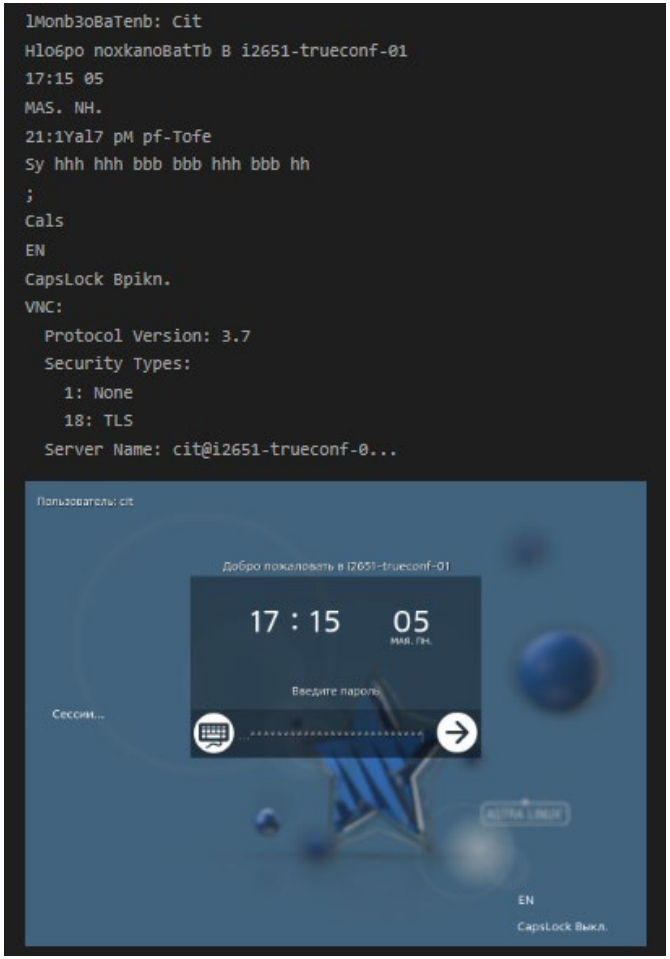
Shodan

Esempio 5



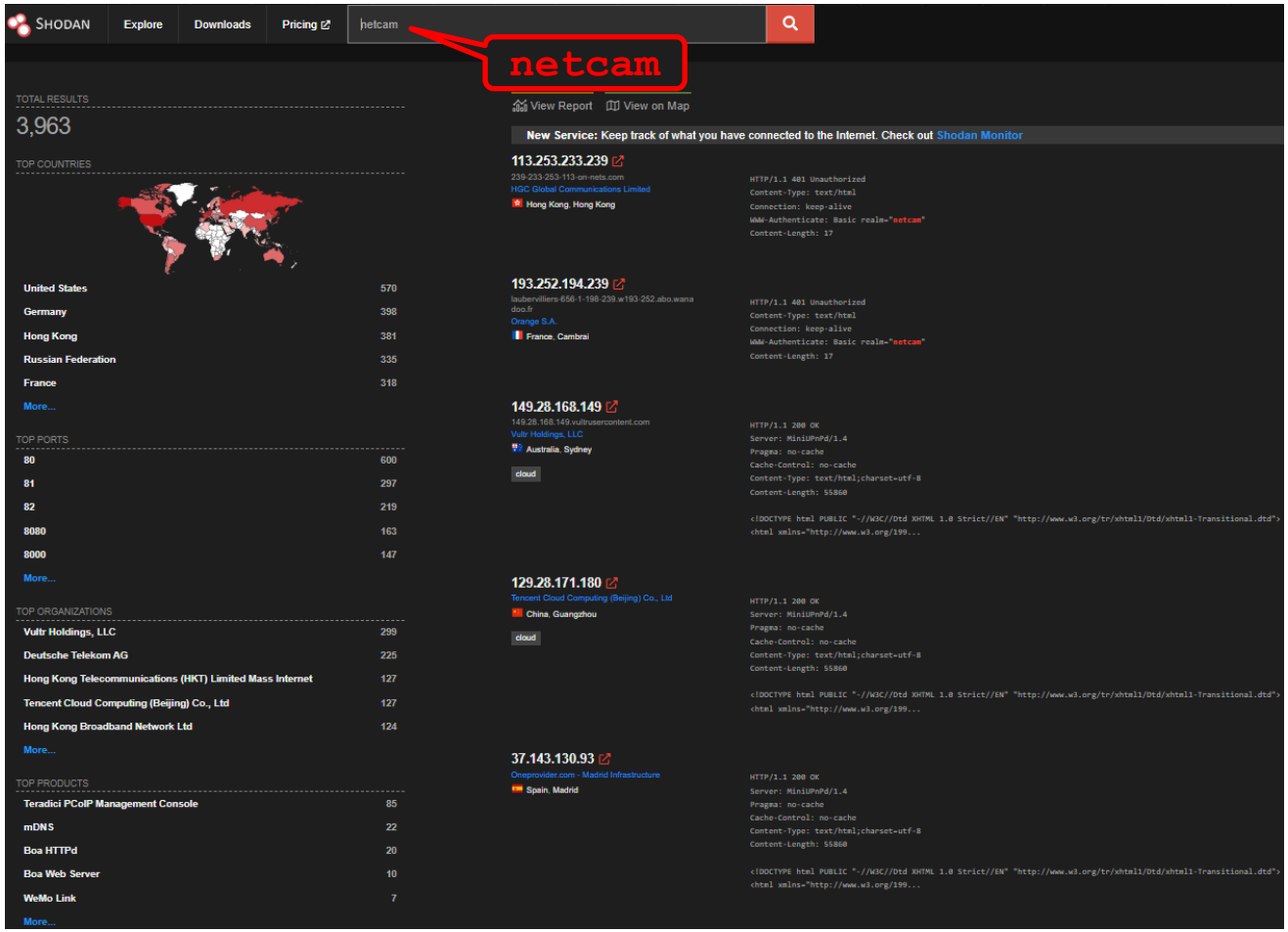
Shodan

Esempio 5



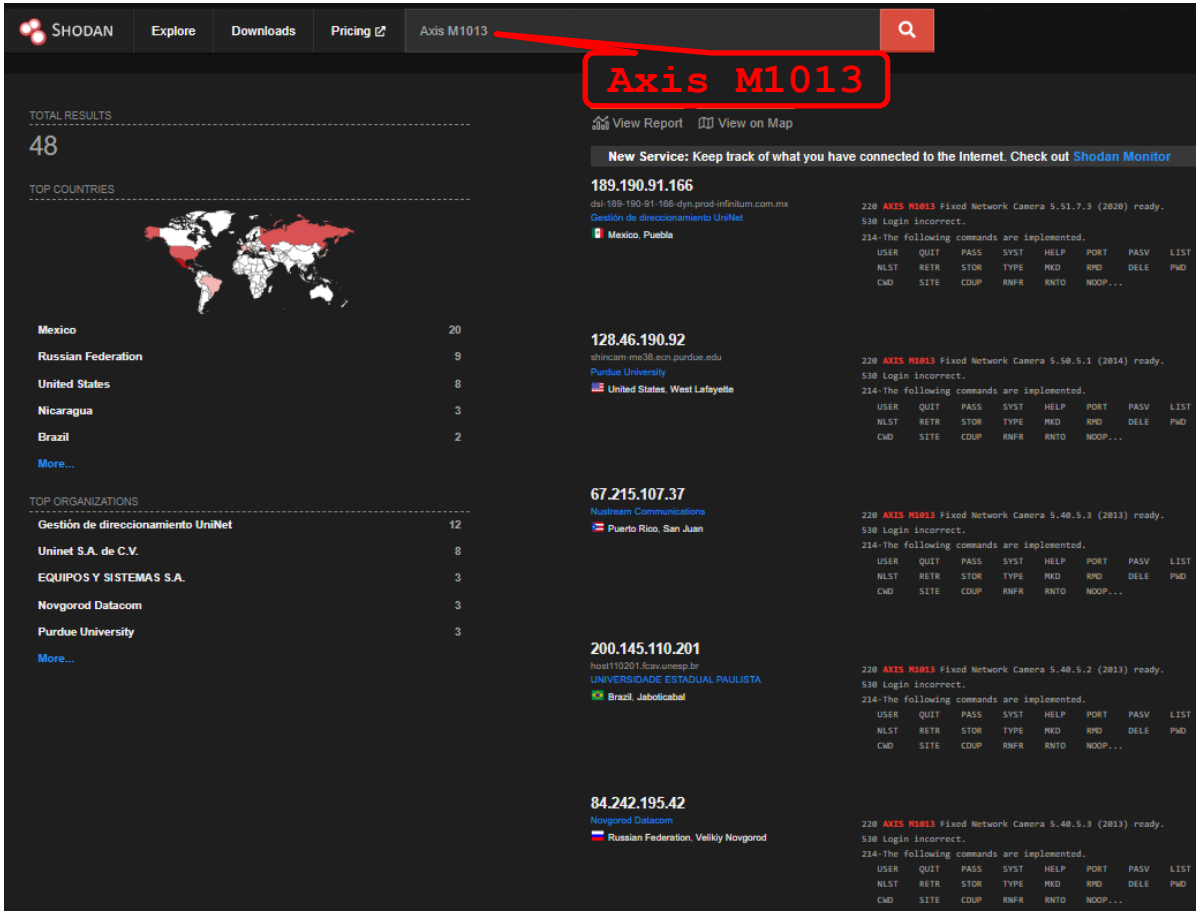
Shodan

Esempio 6



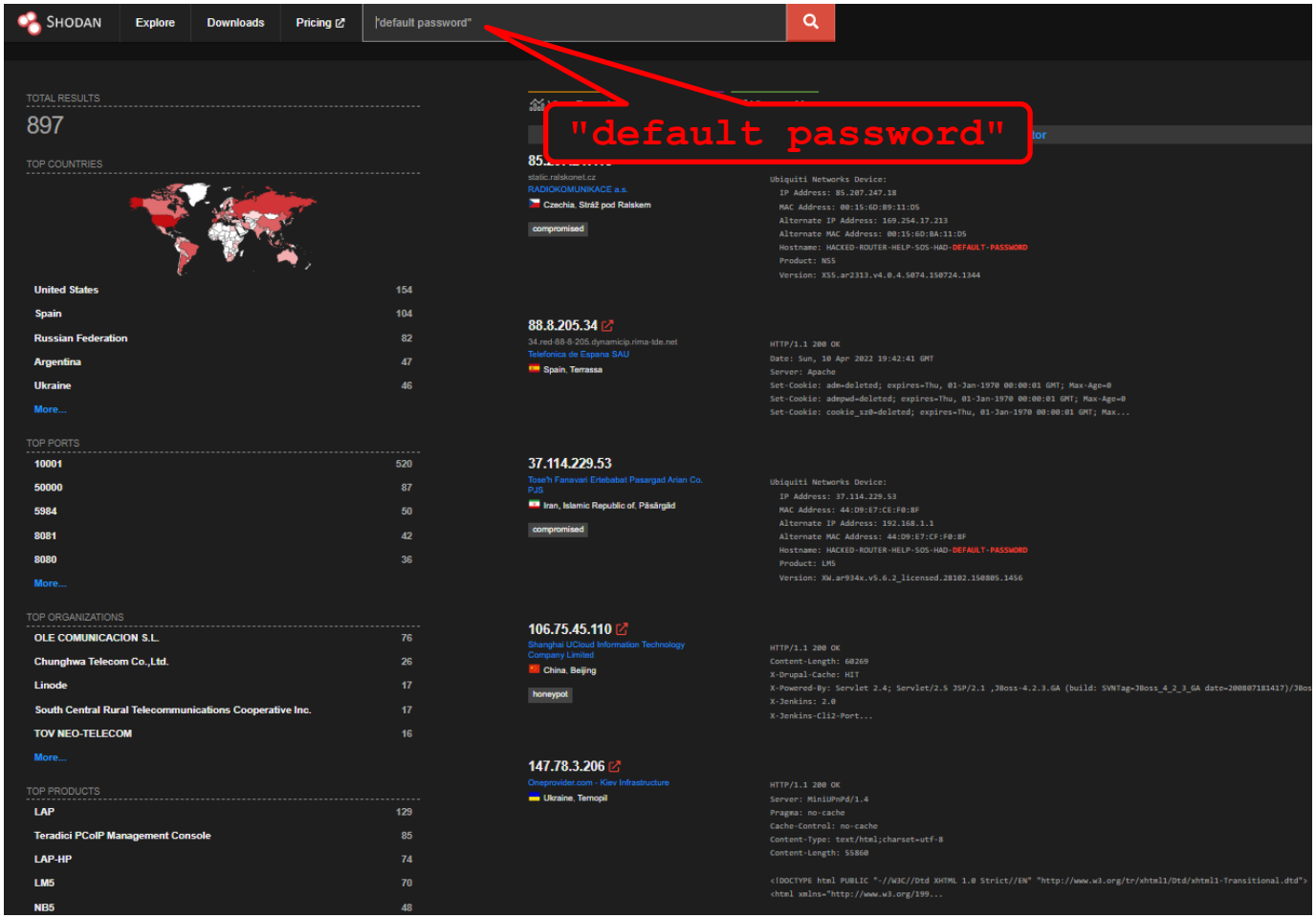
Shodan

Esempio 7



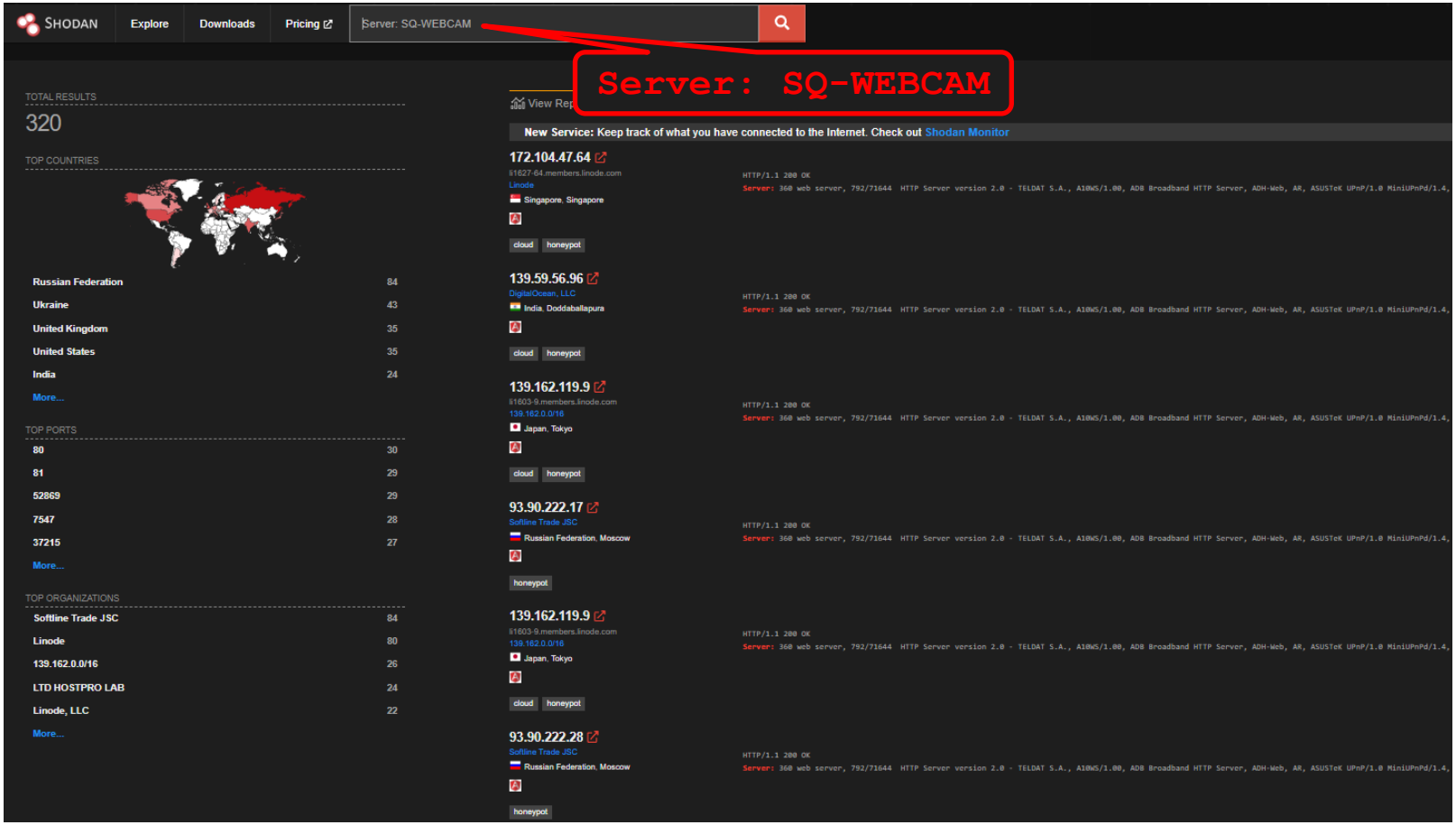
Shodan

Esempio 8



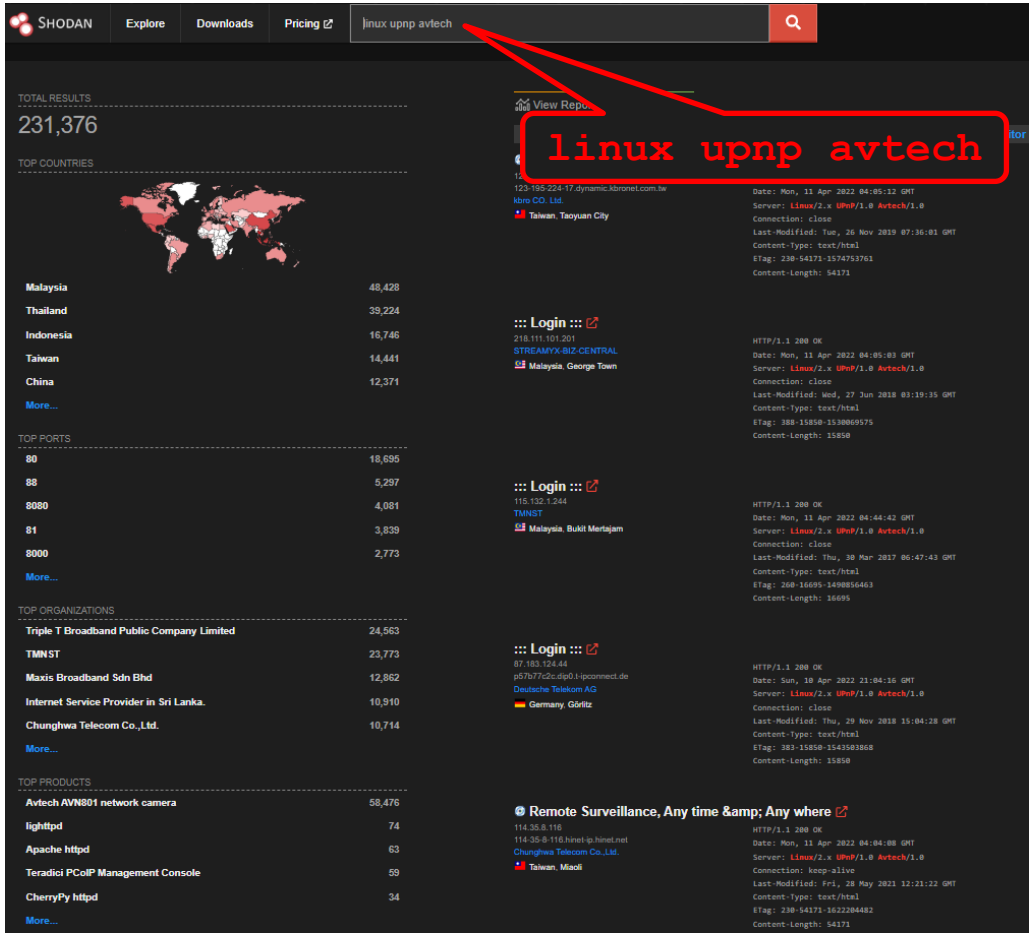
Shodan

Esempio 9



Shodan

Esempio 10



Outline

- Concetti Introduttivi
- Suite Protocollare TCP/IP
- Formato dei Messaggi TCP e UDP
- Active Enumeration
  - Network Scanner Nmap
  - Zenmap
  - Unicornscan
  - Masscan
- Passive Enumeration
  - Shodan
  - **ZoomEye**
  - FOFA
  - Censys

ZoomEye
Caratteristiche

- Motore di ricerca che permette di ottenere informazioni su
  - Dispositivi
  - Siti Web
  - Servizi di rete
  - Componenti di rete
  - Etc
- Prima di utilizzare ZoomEye è fortemente consigliata la registrazione
- Talvolta per l'accesso a ZoomEye potrebbe essere necessario l'utilizzo di VPN
  - A causa di filtri su indirizzi IP provenienti dall'Unione Europea

ZoomEye

Pricing

https://www.zoomeye.ai/pricing

Features & Price		Registered User	Personal (73% OFF) (Security enthusiasts) ~~$708~~ $190/Year Buy Now	Professional (43% OFF) (Security teams and analysts) ~~$1,900~~ $1,090/Year Buy Now	Business (43% OFF) (Medium to large enterprises) ~~$19,188~~ $10,990/Year Buy Now	Corporate (Tailored enterprise solutions) Contact Now
New Explore+	ZoomEye Hub NEW	✗	✓	✓	✓	✓
	ZoomEyeGPT(AI Search) NEW	5 results/Day	30 results/Day	100 results/Day	1000 results/Day	Custom
Primary	Monthly Maximum Results	3,000	100,000	800,000	10,000,000	Custom
	Maximum Result Pages	5	50	50	100	Custom
	API Access Available	Use ZoomEye-Point	✓	✓	✓	✓
	API Request Rate Limit (requests/second)	0.5	1	1	2	Custom
	Number of Result Fields Available	46	71	74	78	78
Ability	Web-based Results Download	Use ZoomEye-Point	✓	✓	✓	✓
	Honeypot Filtering	50 Points	10 Points	10 Points	✓	✓
	Aggregated Results Data	20	50	50	100	100
	Historical Data Access	✗	✗	✗	✓	✓

ZoomEye

Interfaccia

- https://www.zoomeye.ai/

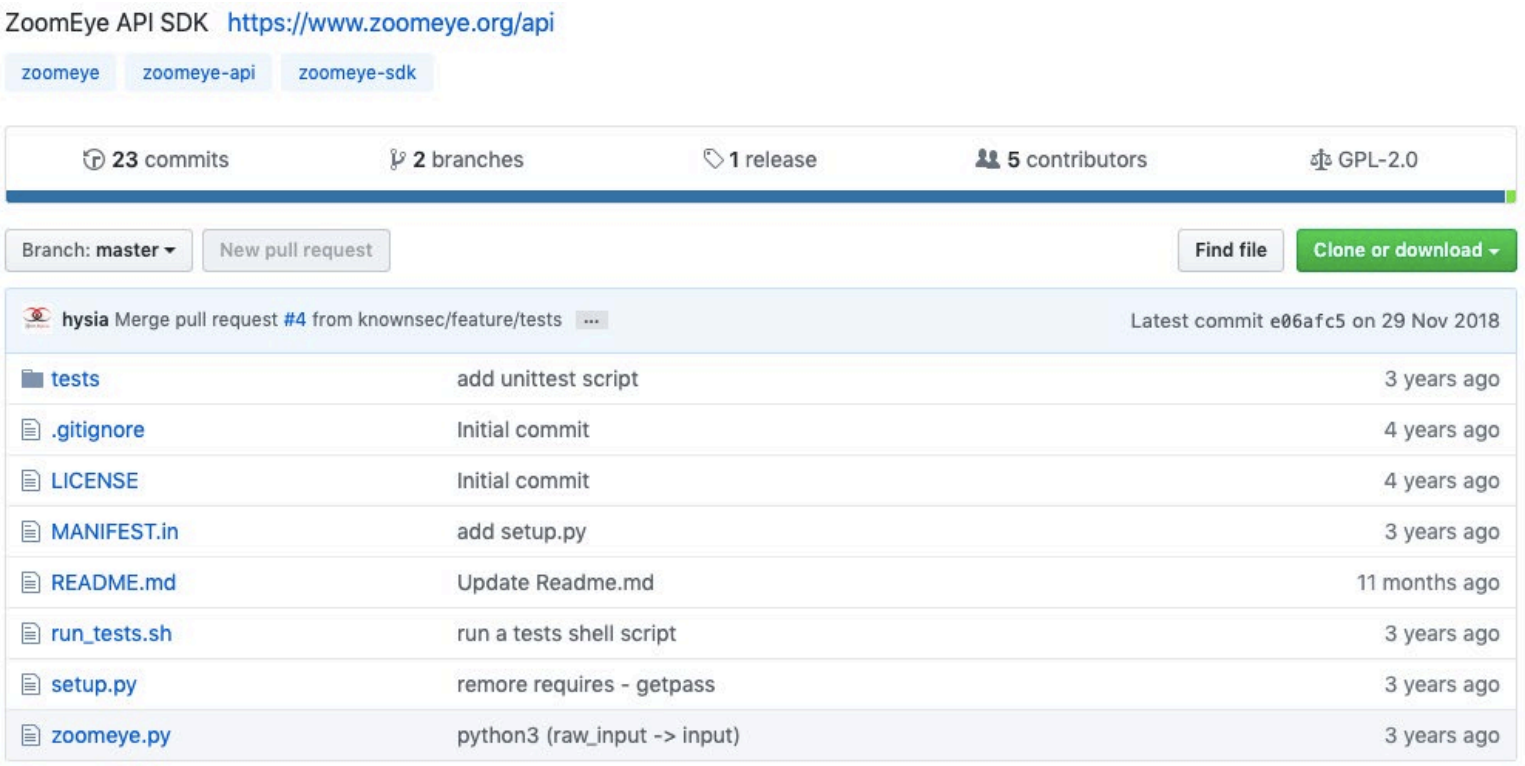
ZoomEye

Interfaccia

- https://www.zoomeye.ai/

ZoomEye
API

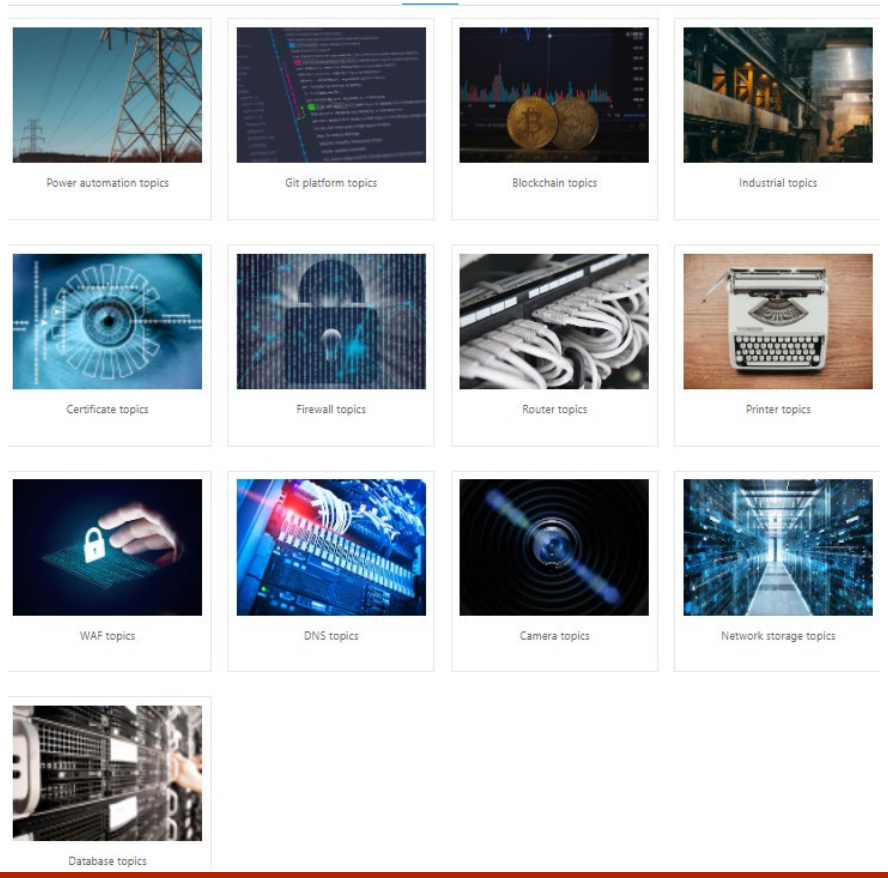
- ZoomEye offre agli utenti la possibilità di utilizzare API
  - **https://github.com/knownsec/ZoomEye**



ZoomEye

Topics

- **https://www.zoomeye.ai/topics**



ZoomEye

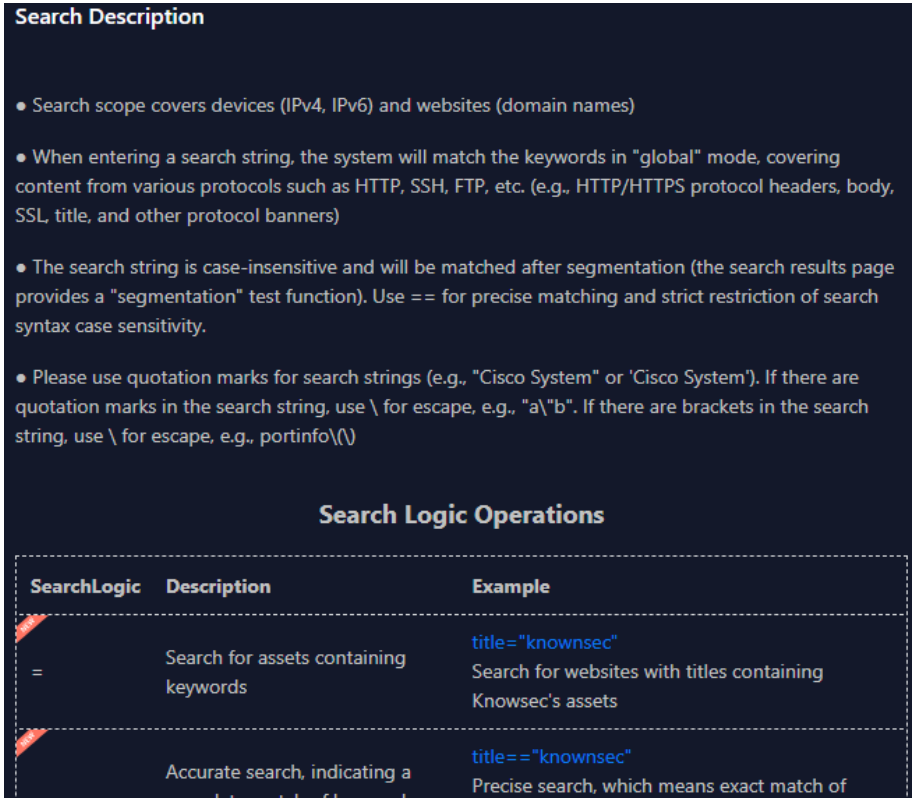
Filtri di Ricerca

- https://www.zoomeye.ai/

ZoomEye

Filtri di Ricerca

- https://www.zoomeye.ai/



Search Description

• Search scope covers devices (IPv4, IPv6) and websites (domain names)

• When entering a search string, the system will match the keywords in "global" mode, covering content from various protocols such as HTTP, SSH, FTP, etc. (e.g., HTTP/HTTPS protocol headers, body, SSL, title, and other protocol banners)

• The search string is case-insensitive and will be matched after segmentation (the search results page provides a "segmentation" test function). Use == for precise matching and strict restriction of search syntax case sensitivity.

• Please use quotation marks for search strings (e.g., "Cisco System" or 'Cisco System'). If there are quotation marks in the search string, use \ for escape, e.g., "a\"b". If there are brackets in the search string, use \ for escape, e.g., portinfo\(\)

Search Logic Operations

SearchLogic	Description	Example
=	Search for assets containing keywords	title="knownsec" Search for websites with titles containing Knowsec's assets
	Accurate search, indicating a	title=="knownsec" Precise search, which means exact match of

ZoomEye
Filtri di Ricerca

- **Alcuni tra i principali filtri di ricerca**
  - **`app:`** nome dell'applicazione
  - **`country:`** country code (ad es., **`UK`**, **`IT`**, **`ES`**, **`FR`**, **`CN`**, **`JP`**)
  - **`city:`** nome della città
  - **`port:`** numero di porta
  - **`os:`** nome del Sistema Operativo (ad es., **`os:linux`**)
  - **`service:`** nome del servizio
  - **`hostname:`** hostname (ad es., **`hostname:google.com`**)
  - **`ip:`** indirizzo IP (ad ed., **`ip:8.8.8.8`**)
  - **`cidr:`** segmento CIDR (ad es., **`cidr:8.8.8.0/24`**)

ZoomEye

Operatori Logici

Simbolo	Descrizione
=	Ricerca asset che abbiano una corrispondenza rispetto alle keywork
==	Ricerca accurata, che richiede una corrispondenza esatta rispetto alle keyword (case sensitive)
||	OR Logico
&&	AND Logico
!=	NOT Logico
()	Forniscono prioritizzazione delle operazioni
*	Fuzzy search, use * for search

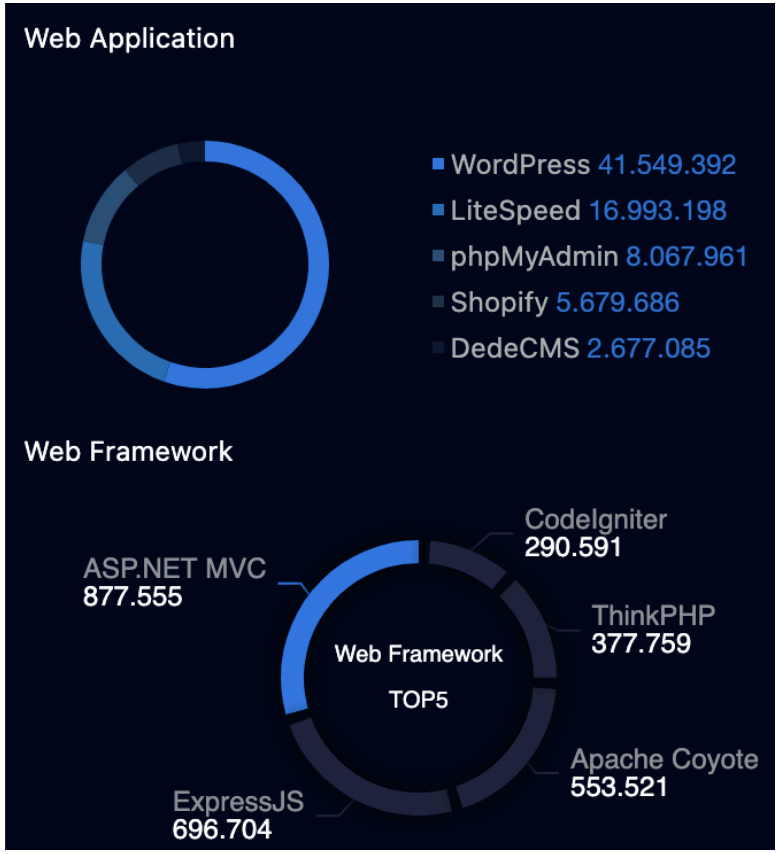
ZoomEye
Dorks

- **`https://www.zoomeye.ai/`**

ZoomEye

Statistiche

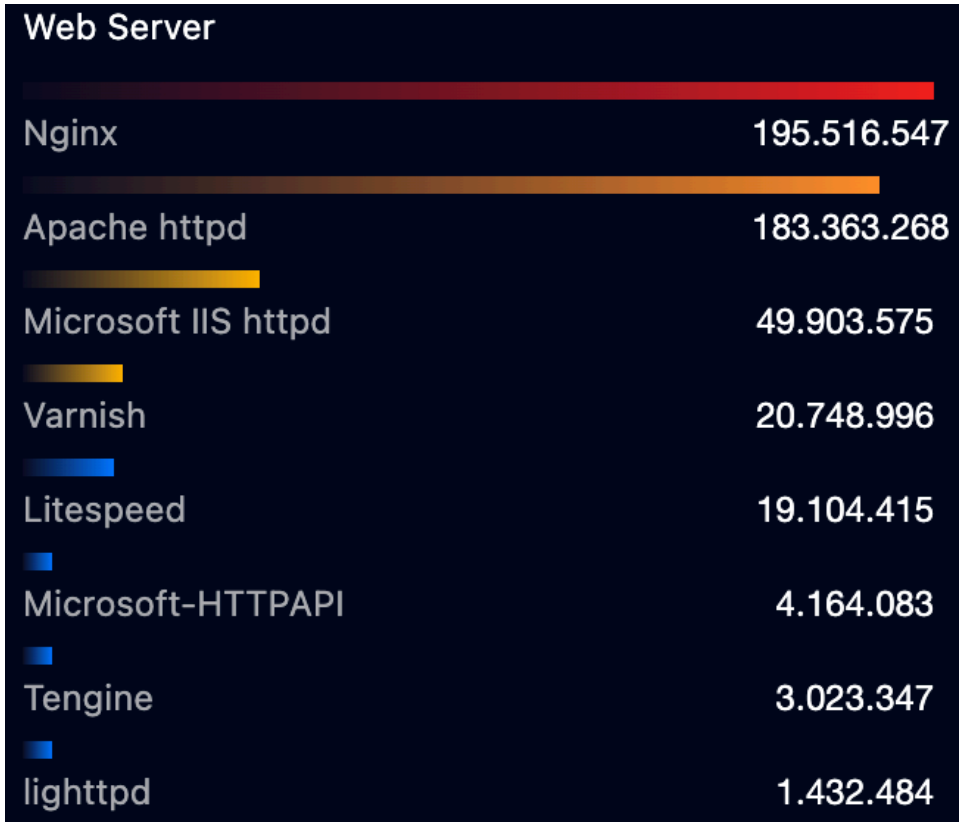
- https://www.zoomeye.ai/statistics



ZoomEye

Statistiche

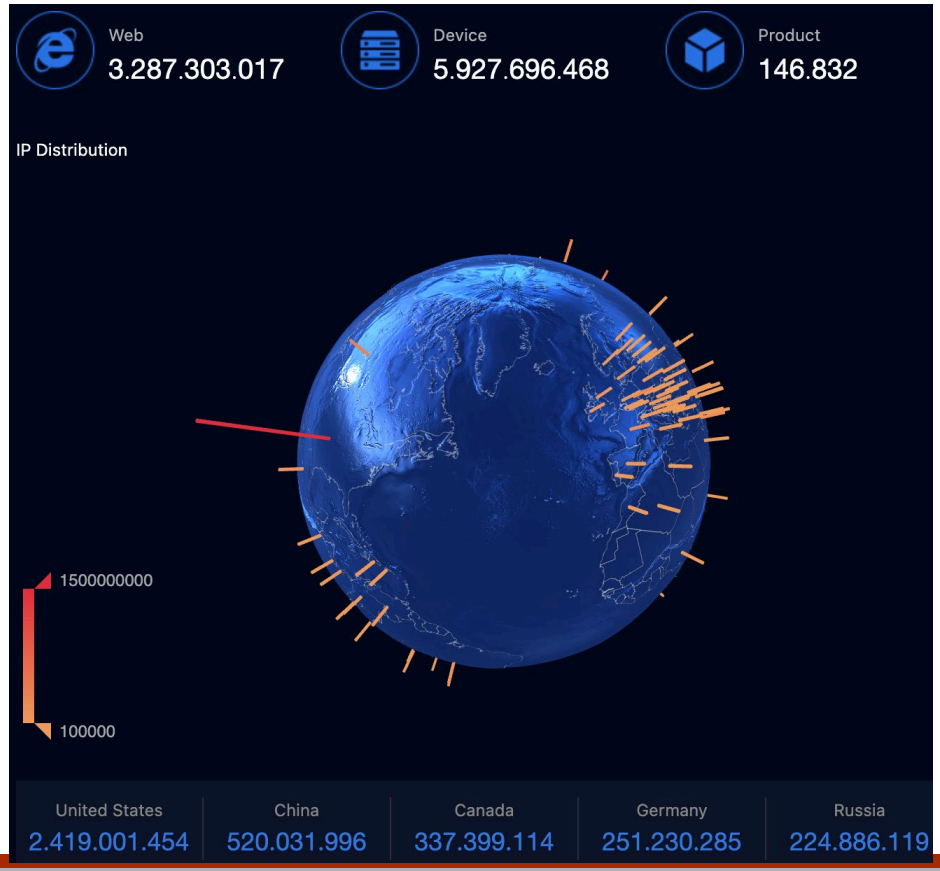
- https://www.zoomeye.ai/statistics



ZoomEye

Statistiche

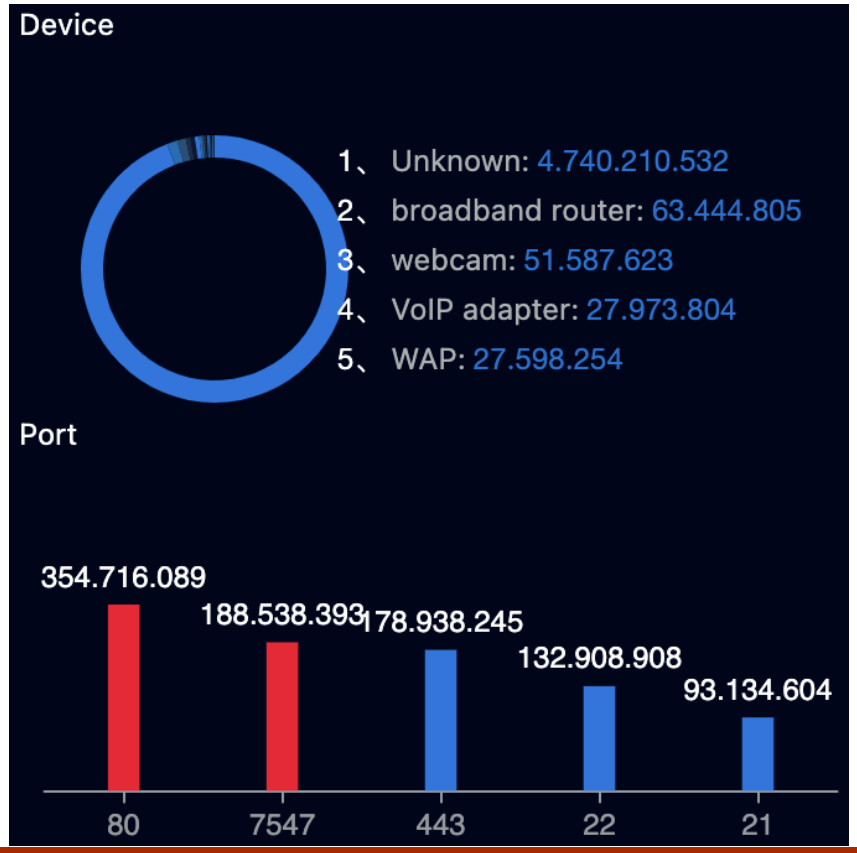
- https://www.zoomeye.ai/statistics



ZoomEye

Statistiche

- https://www.zoomeye.ai/statistics



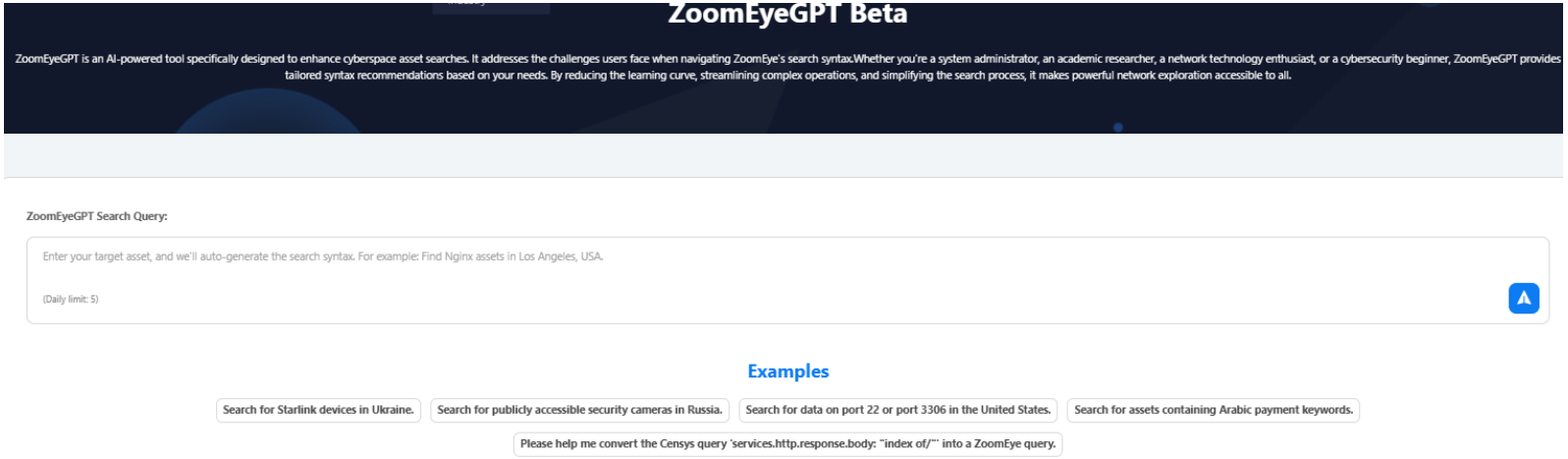
ZoomEye
Statistiche

- https://www.zoomeye.ai/statistics

ZoomEye

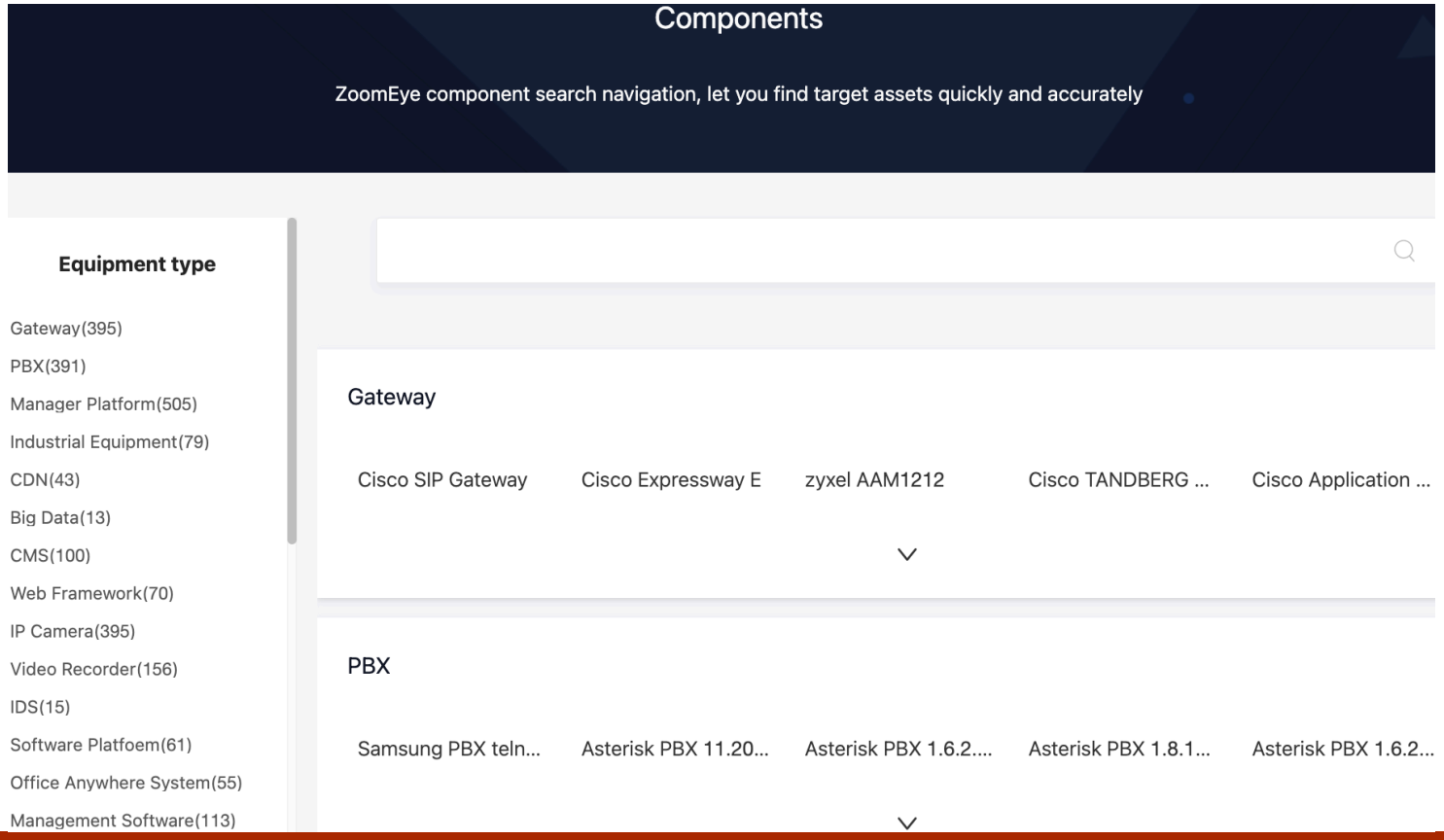
ZoomEyeGPT Beta

- **`https://www.zoomeye.ai/gpt`**



ZoomEye
Componenti

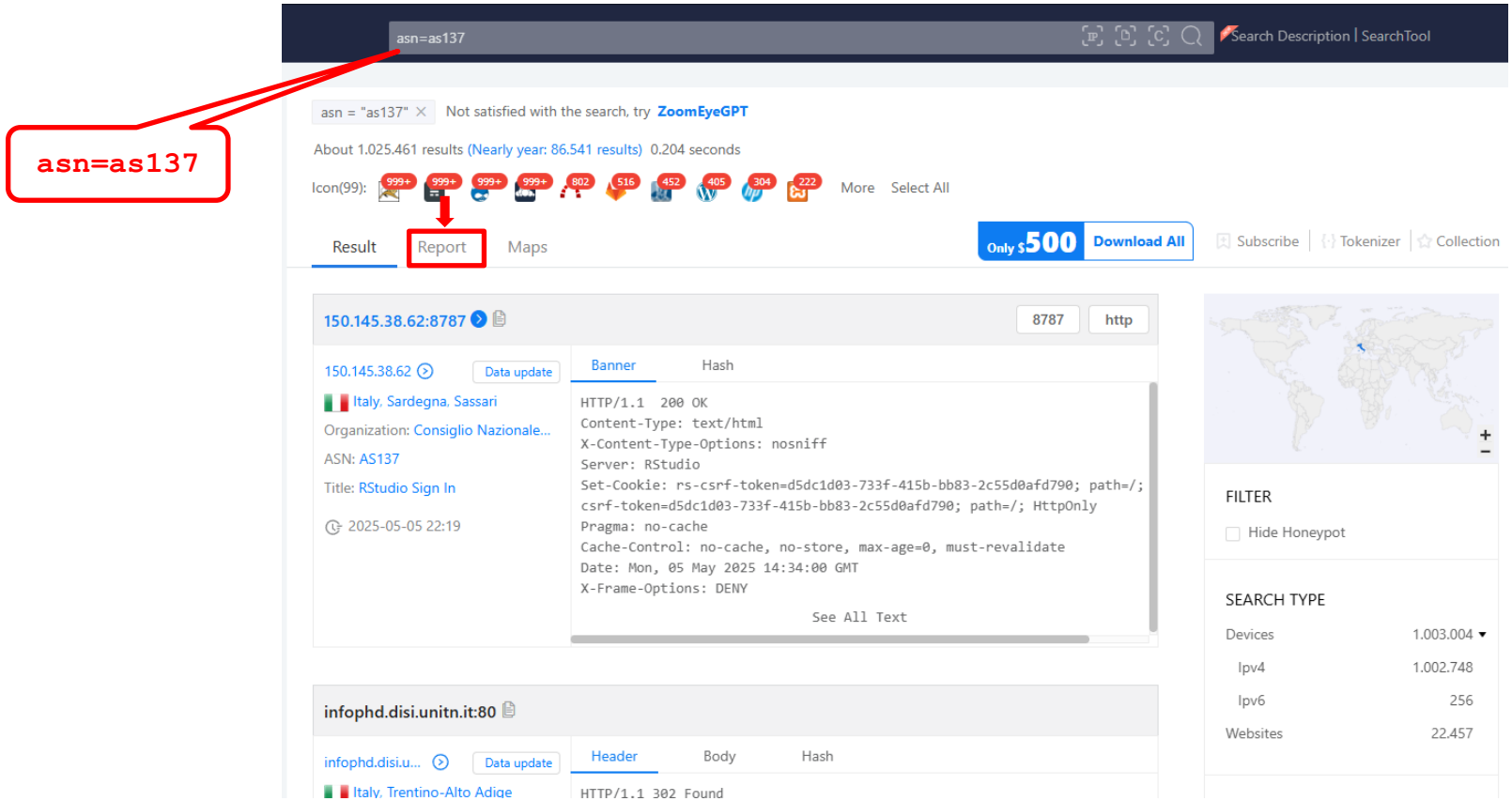
- **https://www.zoomeye.ai/component**



ZoomEye

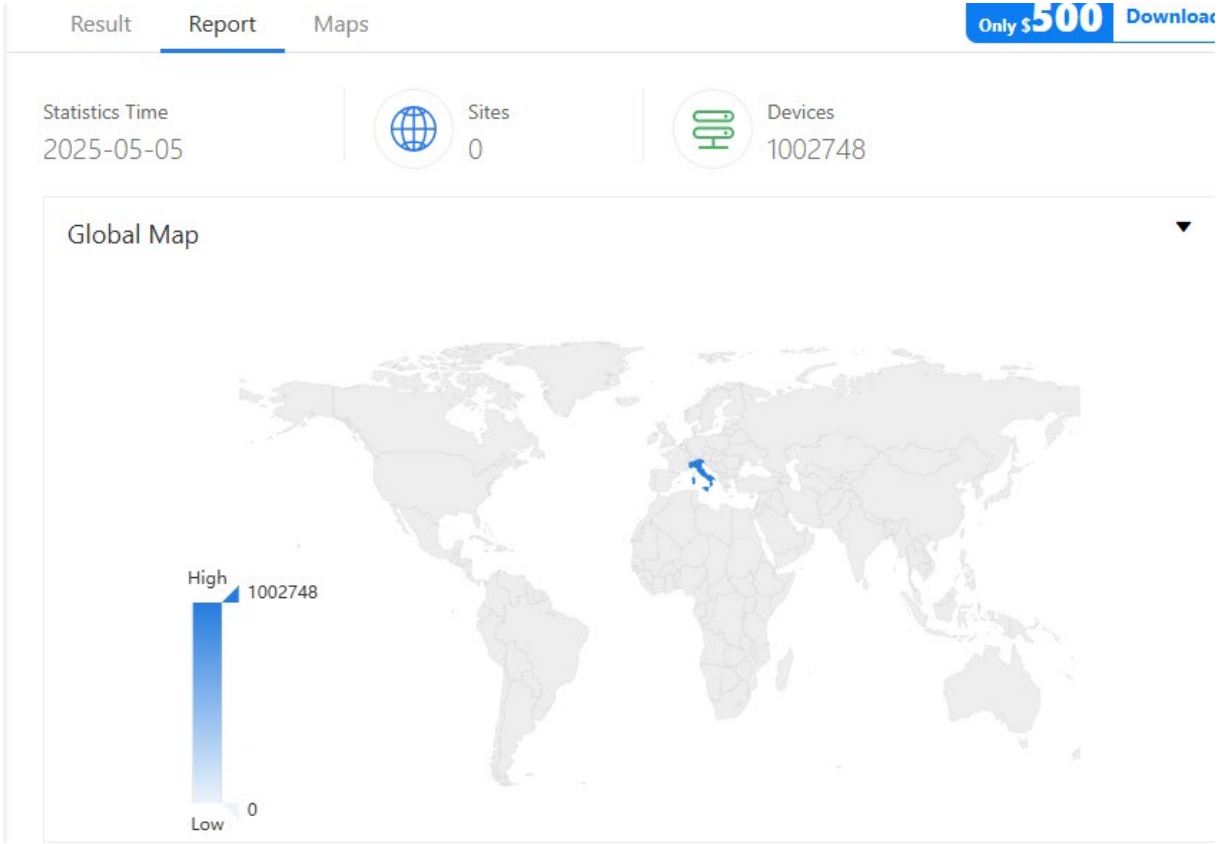
Esempio 1

- Effettuiamo una ricerca per Autonomous System Network (**`asn=as137`**)



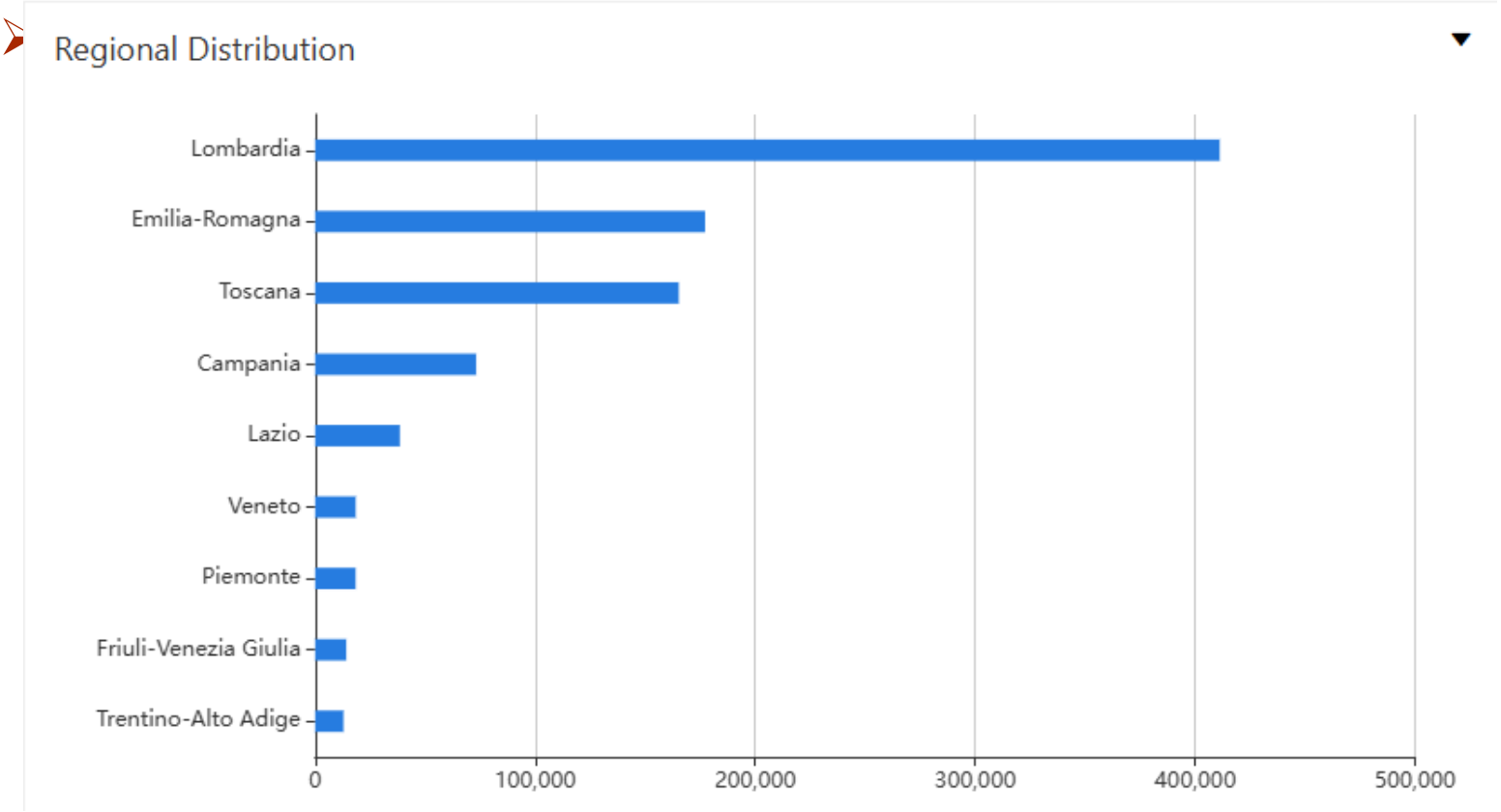
ZoomEye
Esempio 1

- Possiamo visualizzare numerose statistiche relative all'AS AS137



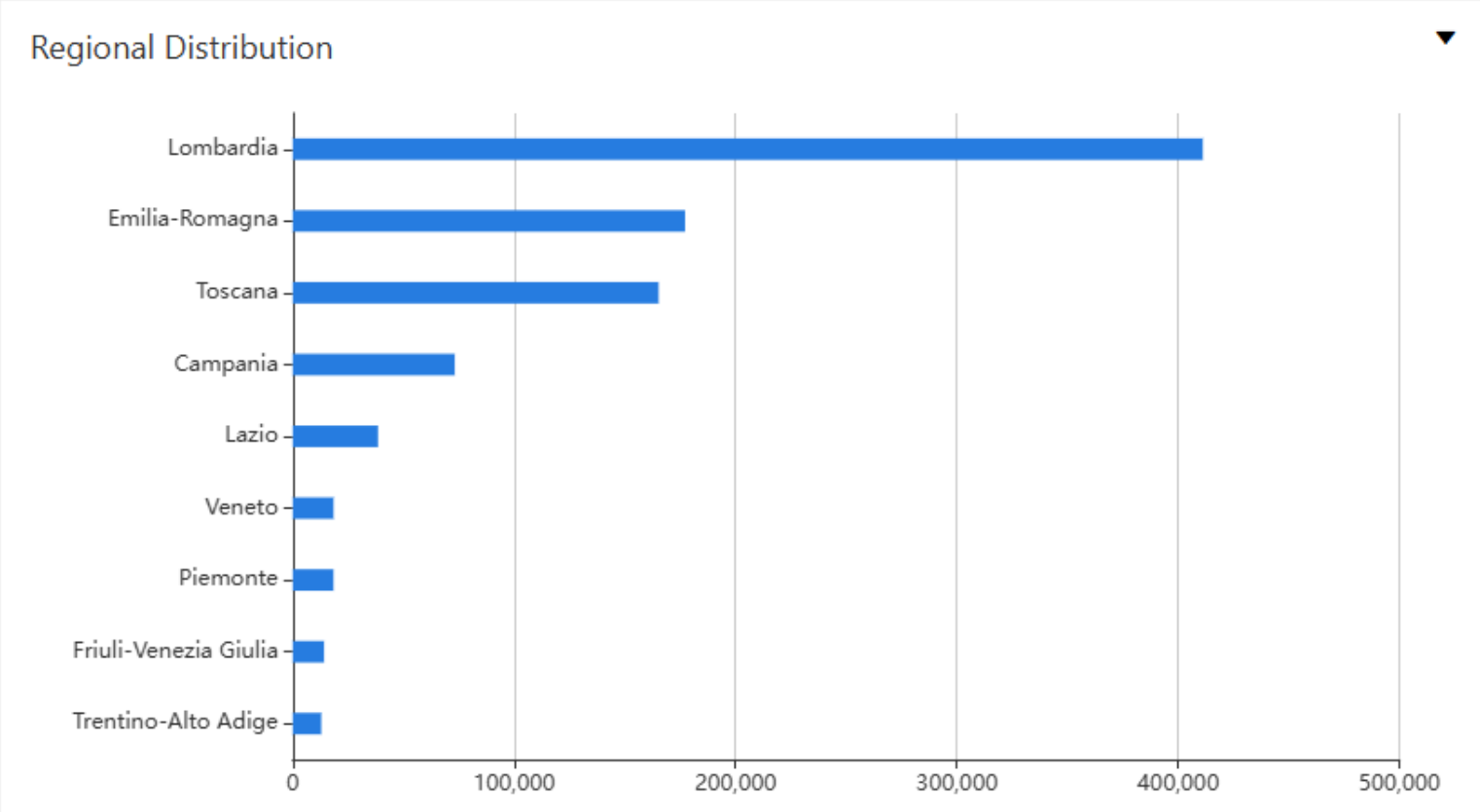
ZoomEye

Esempio 1



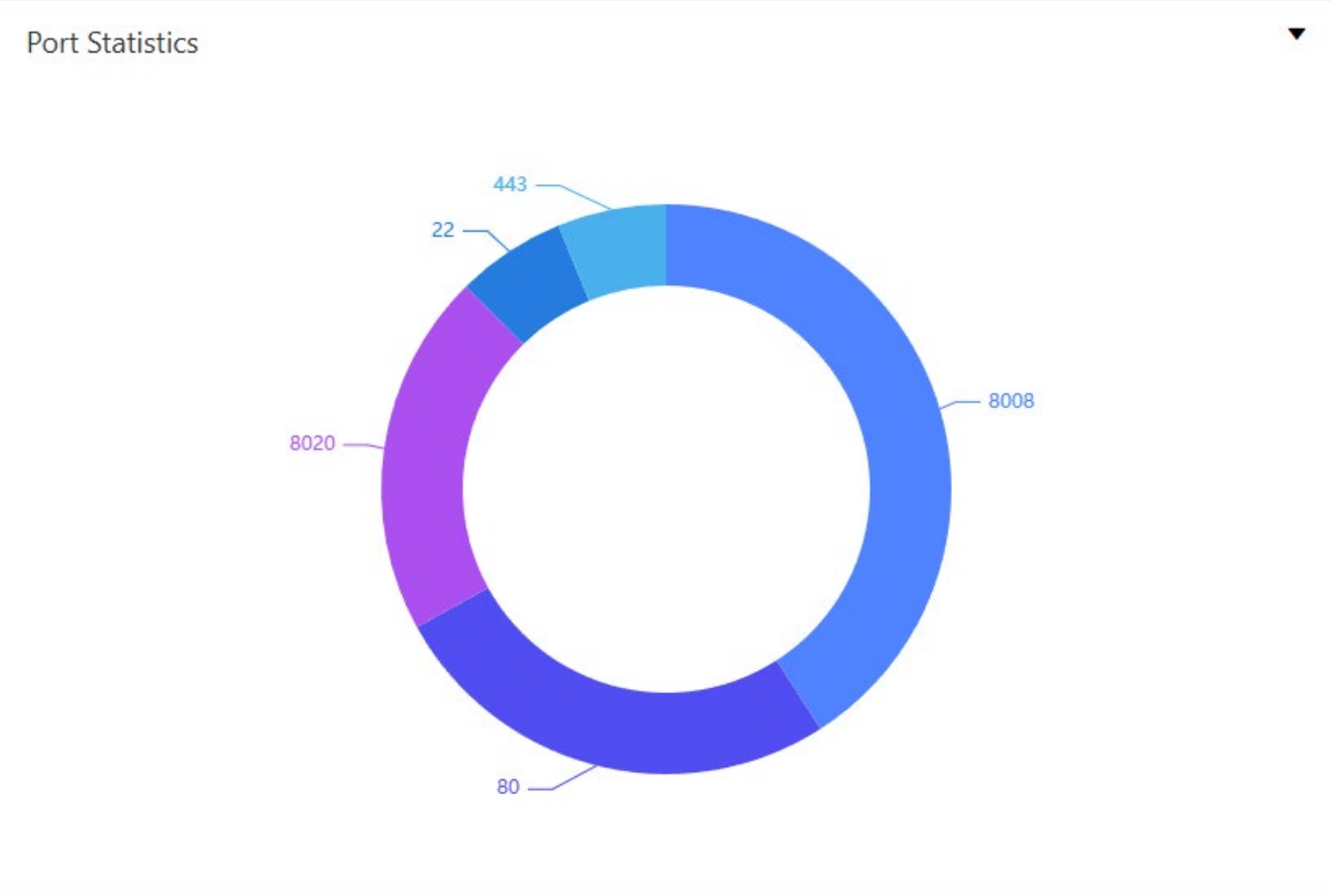
ZoomEye

Esempio 1



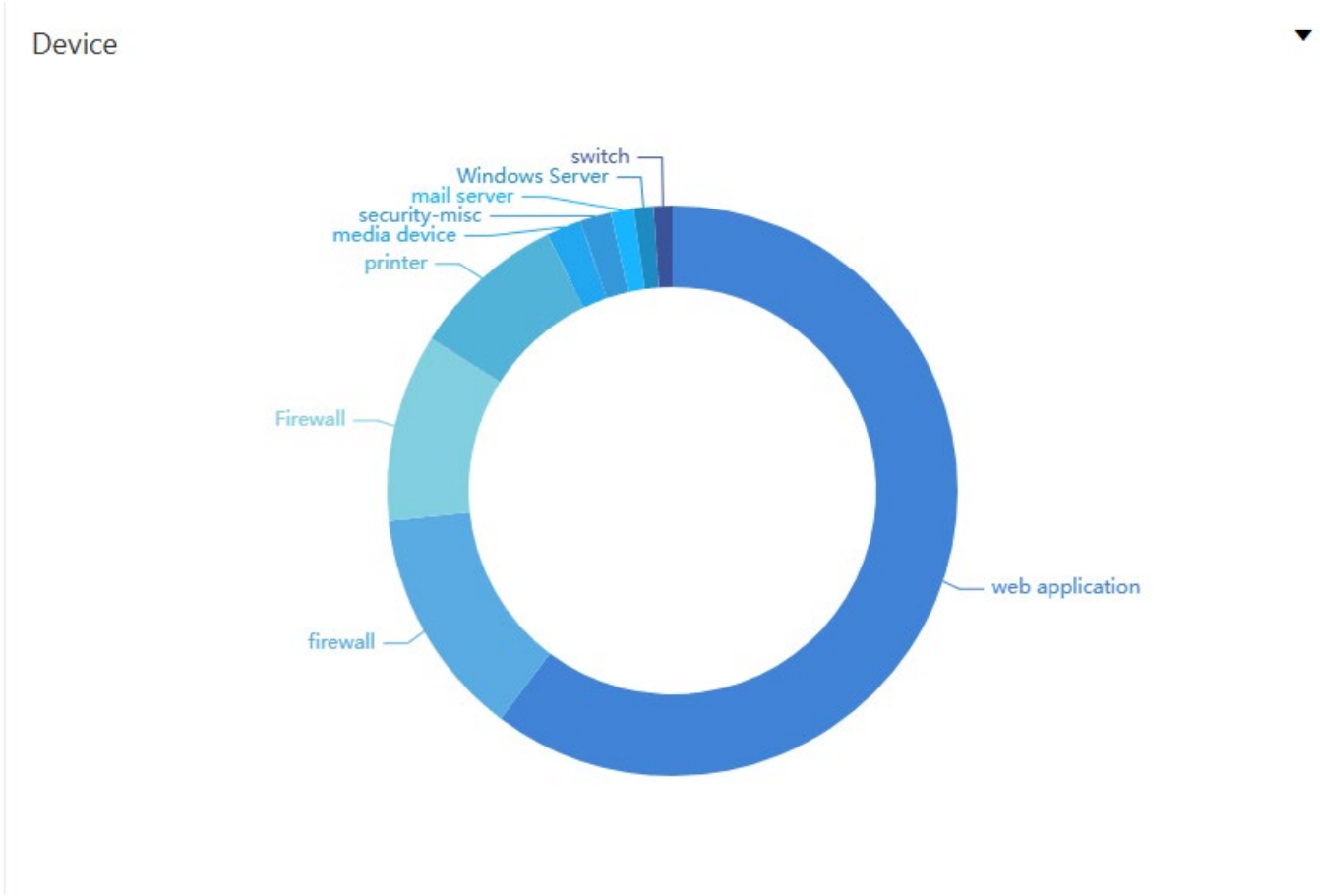
ZoomEye

Esempio 1



ZoomEye

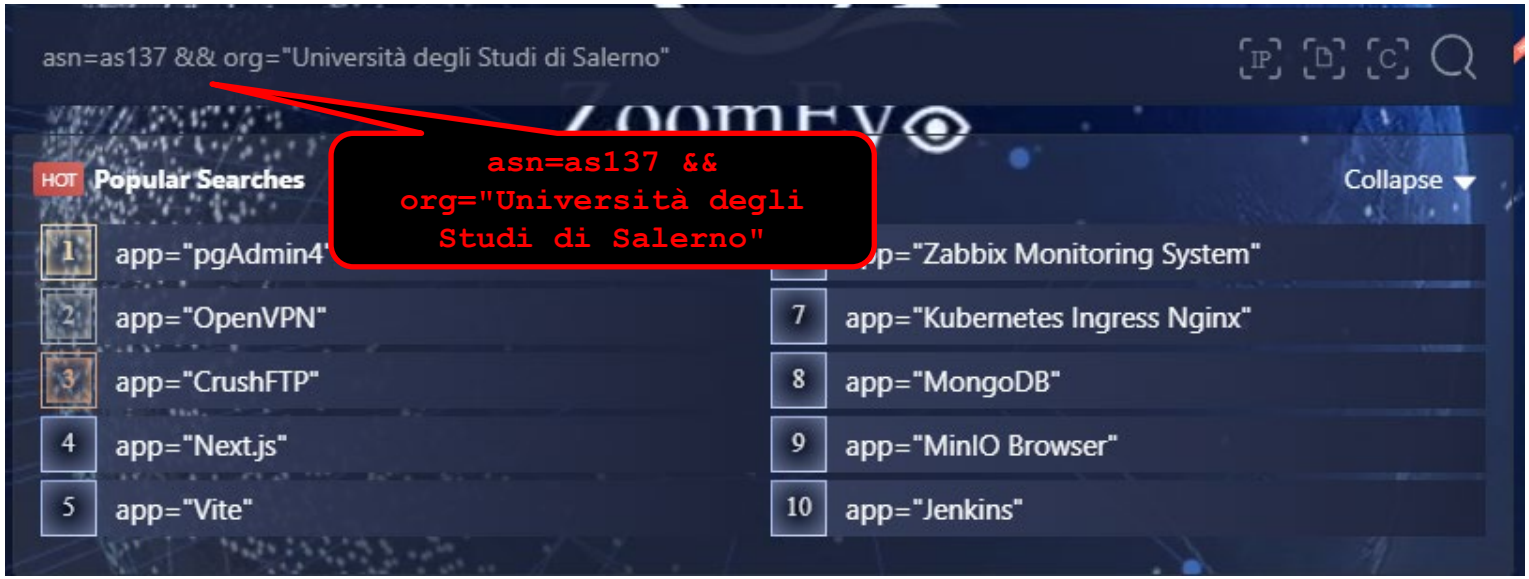
Esempio 1



ZoomEye

Esempio 2

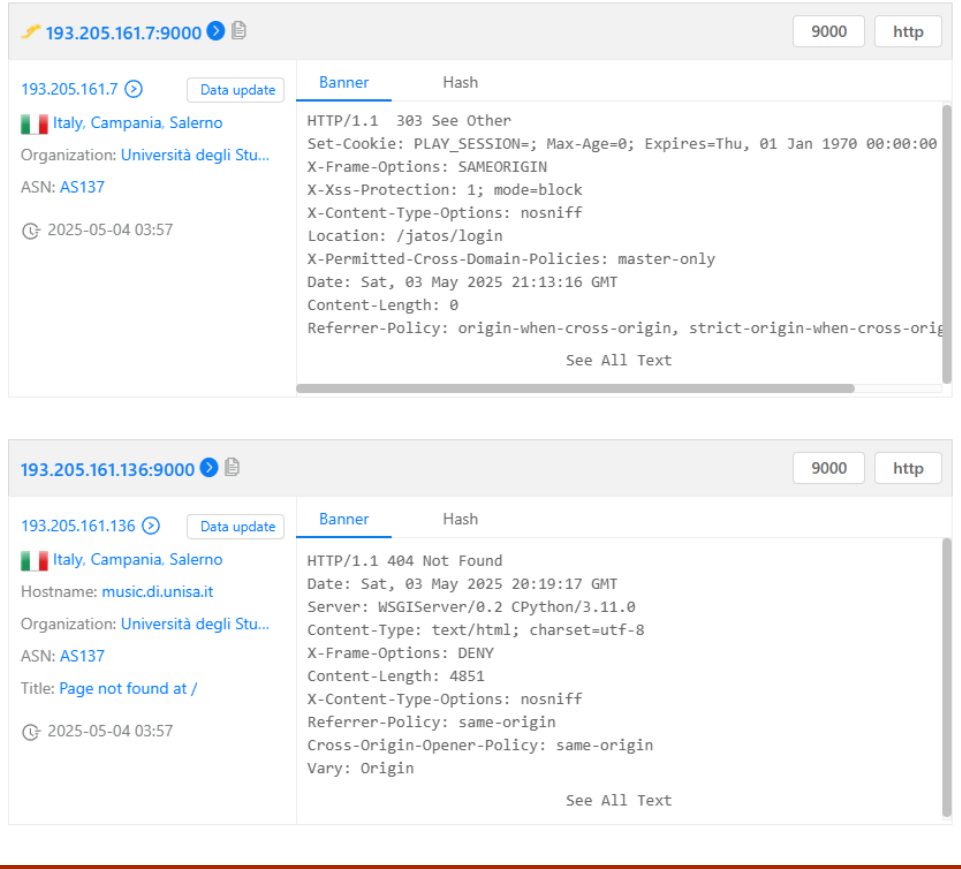
- Specifichiamo l'organizzazione «Università degli Studi di Salerno»



ZoomEye

Esempio 2

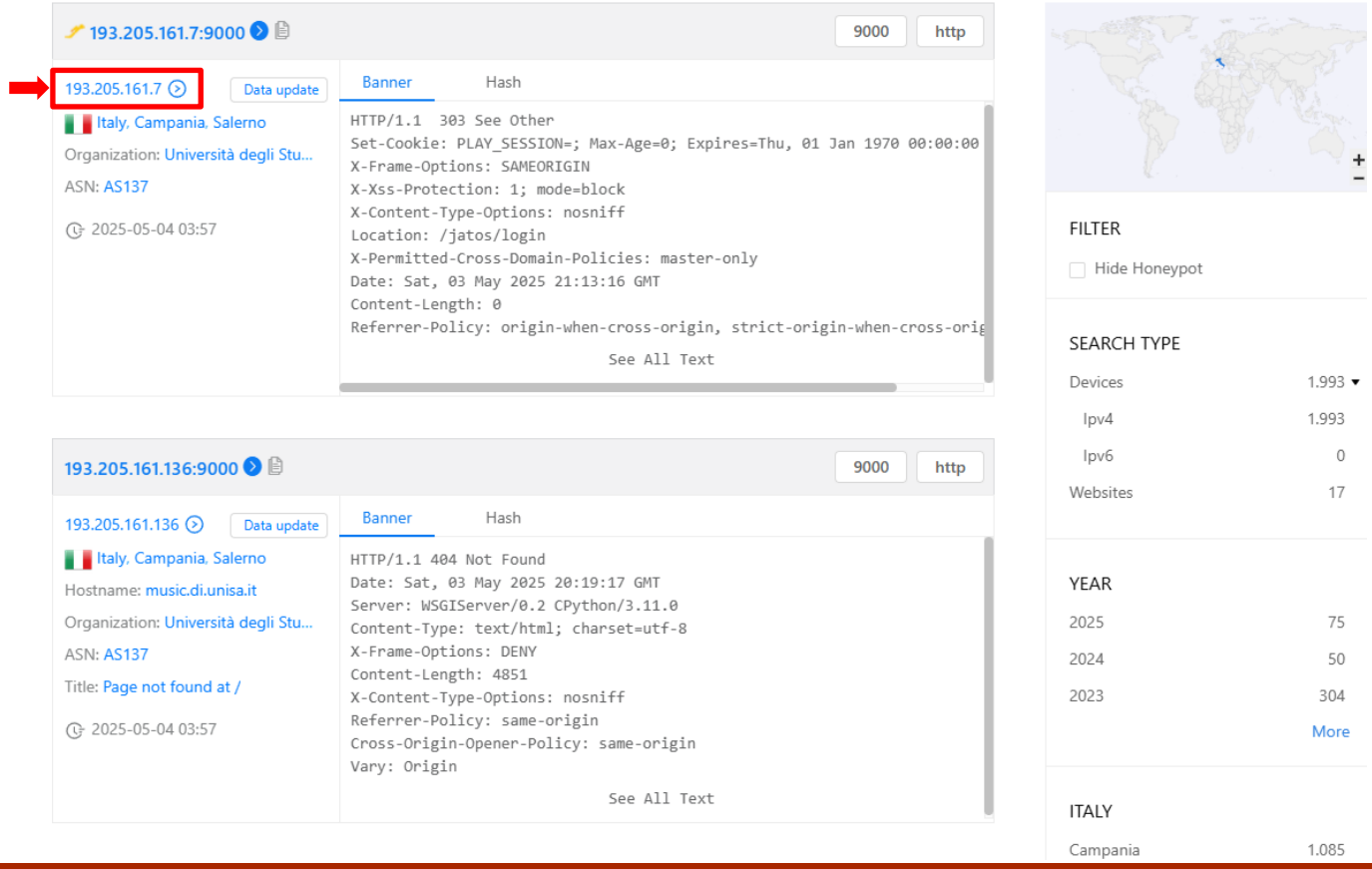
- Vengono mostrati tutti i dispositivi appartenenti all'organizzazione



ZoomEye

Esempio 2

- Possiamo controllare i dettagli relativi a ciascun dispositivo

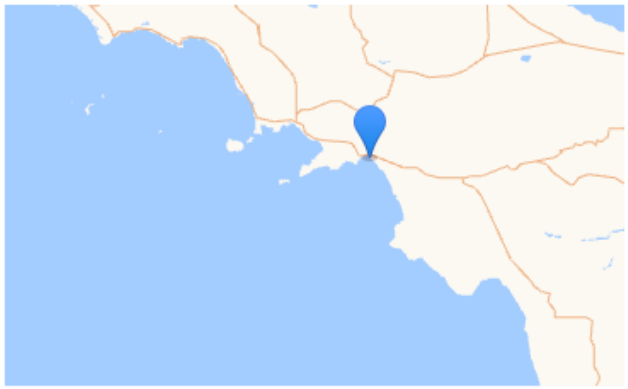


ZoomEye
Esempio 2

- Informazioni di Base

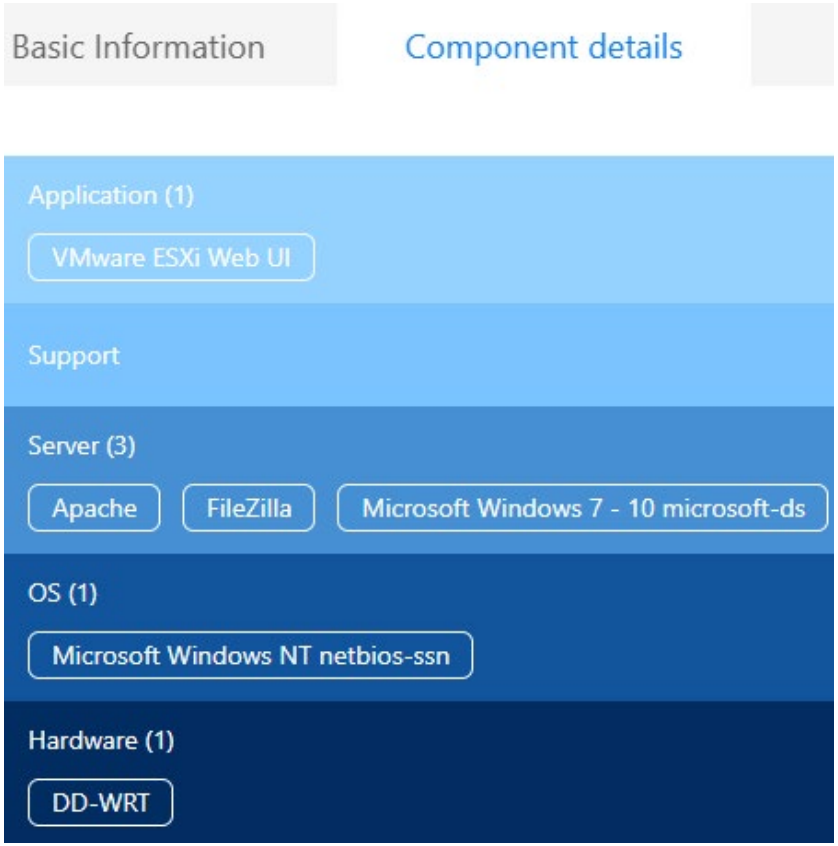
Basic Information | Component details

IP Address	193.205.161.7
City	Salerno
Province / State	Campania
Country	Italy
Location	40.673361, 14.769705
Organization	Universitxe0 degli Studi di Salerno
ISP	
Hostnames	ISIS-PC
ASN	AS137



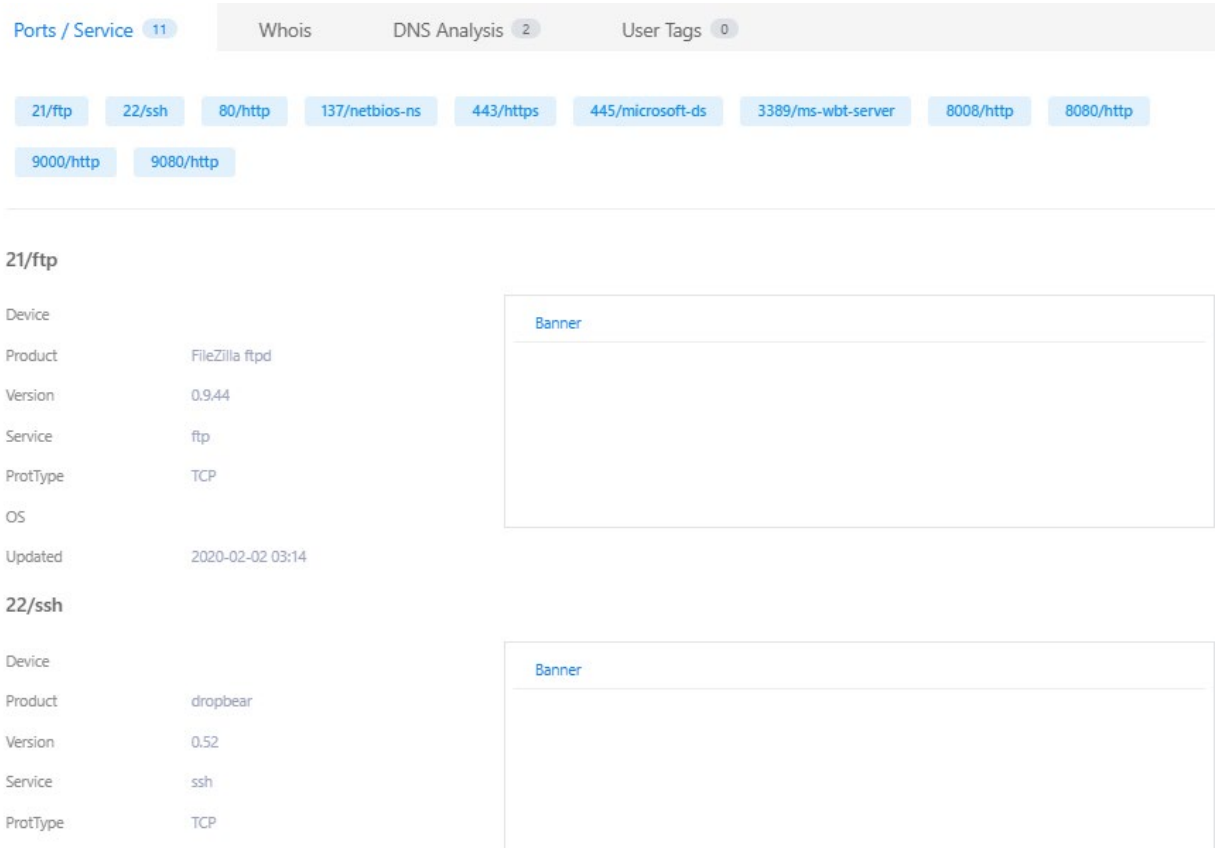
ZoomEye
Esempio 2

- Dettagli relativi al dispositivo



ZoomEye
Esempio 2

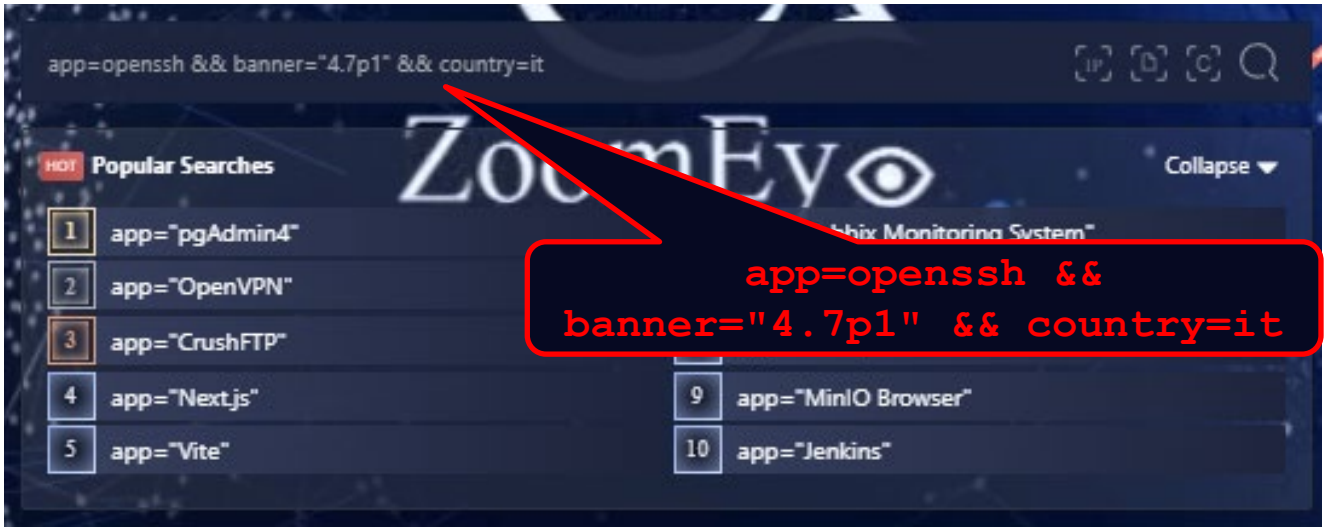
- Informazioni sulle porte aperte ed i relativi servizi e banner



ZoomEye

Esempio 3

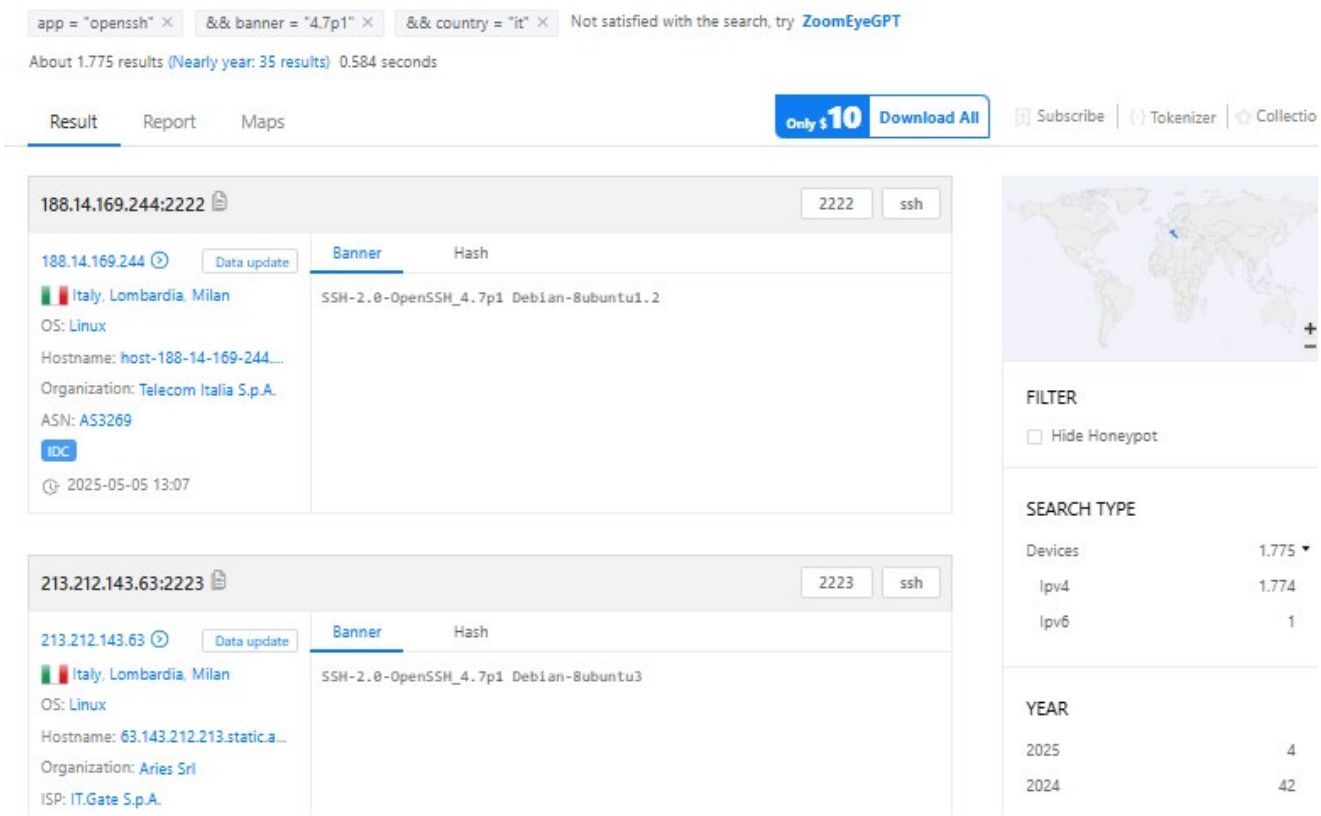
- **https://www.zoomeye.ai/**



ZoomEye

Esempio 3

- **https://www.zoomeye.ai/**



ZoomEye

Esempio 4

- **https://www.zoomeye.ai/**

ZoomEye

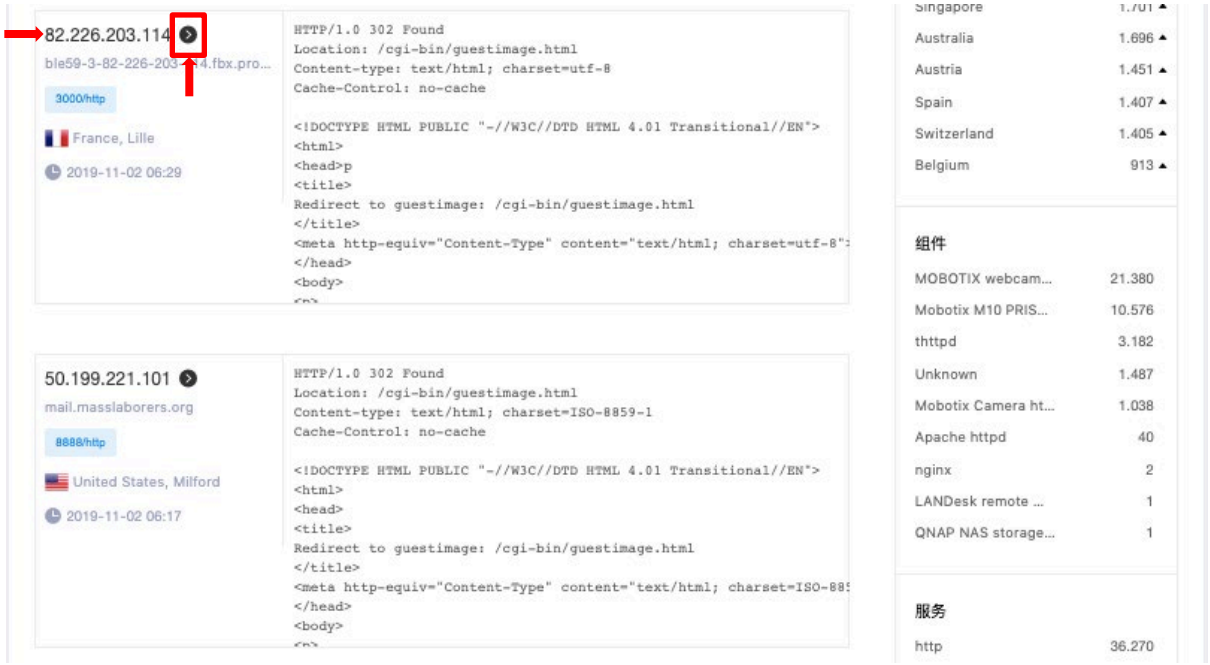
Esempio 4

- **https://www.zoomeye.ai/**

ZoomEye

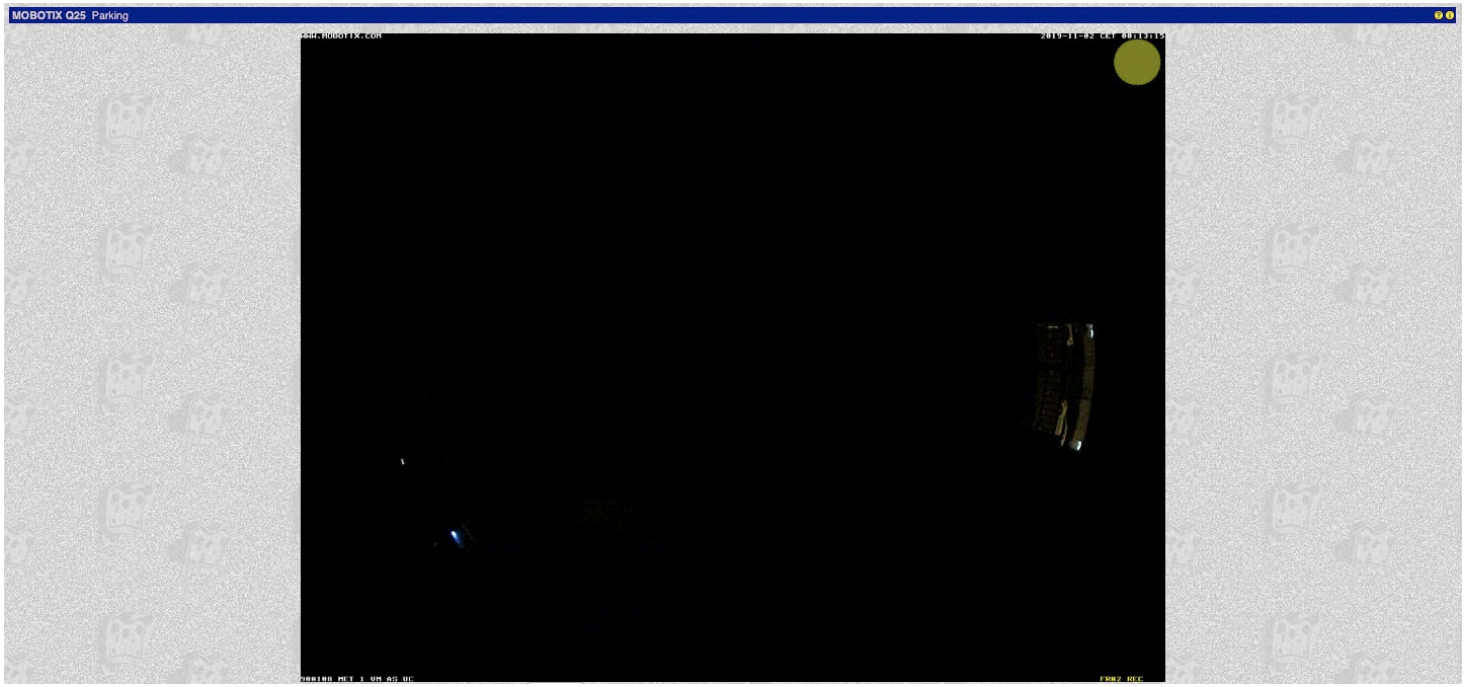
Esempio 4 (Caso 1)

- **https://www.zoomeye.ai/**



ZoomEye
Esempio 4 (Caso 1)

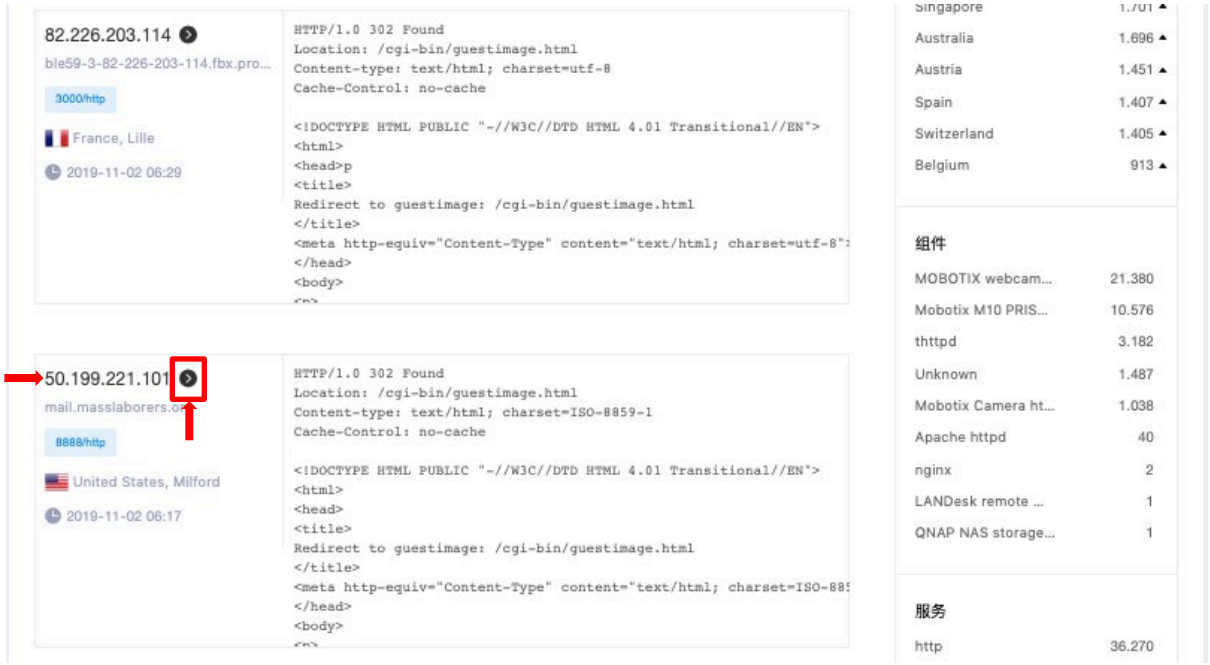
- **https://www.zoomeye.ai/**



ZoomEye

Esempio 4 (Caso 2)

- **https://www.zoomeye.ai/**



ZoomEye

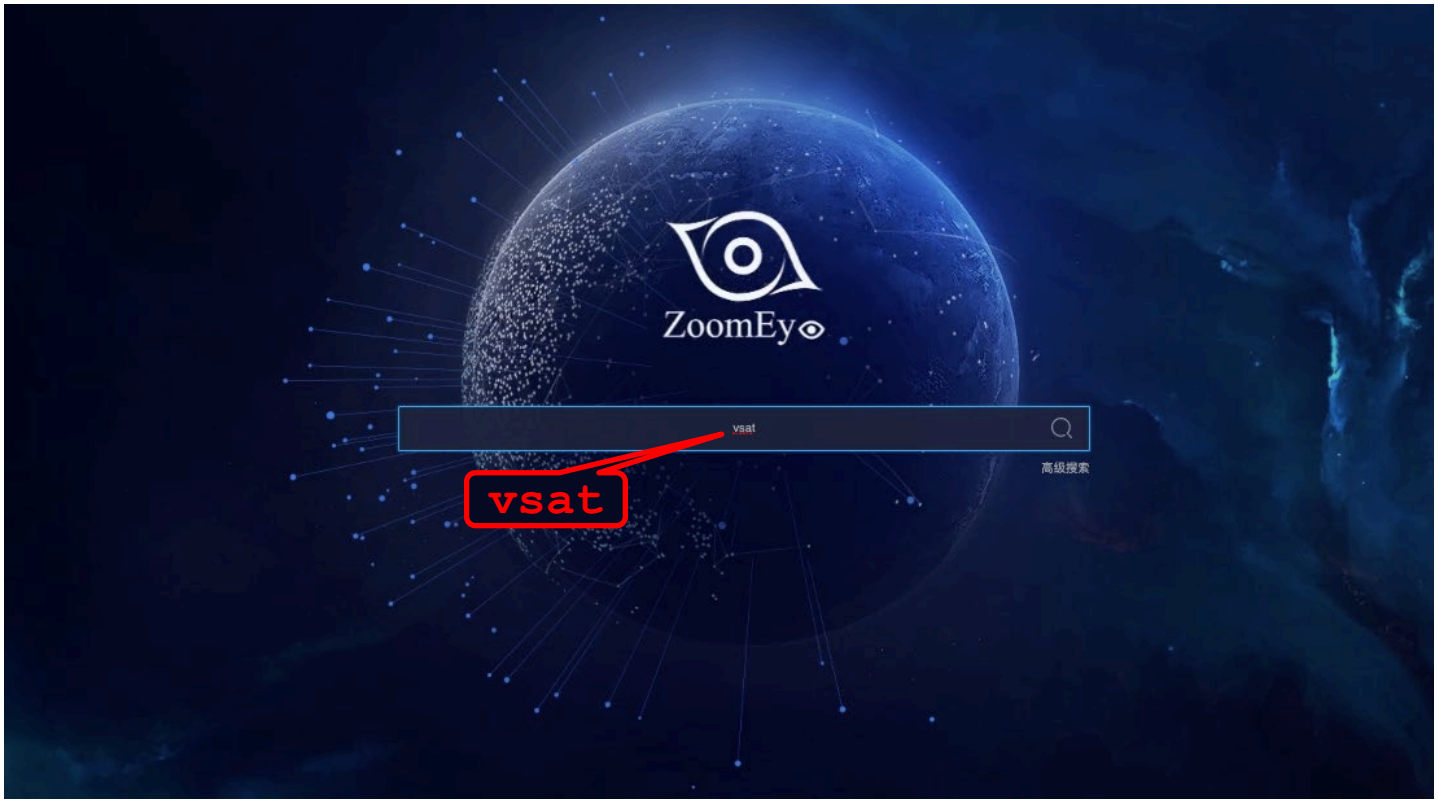
Esempio 4 (Caso 2)

- **https://www.zoomeye.ai/**

ZoomEye

Esempio 5

- **https://www.zoomeye.ai/**



ZoomEye

Esempio 5

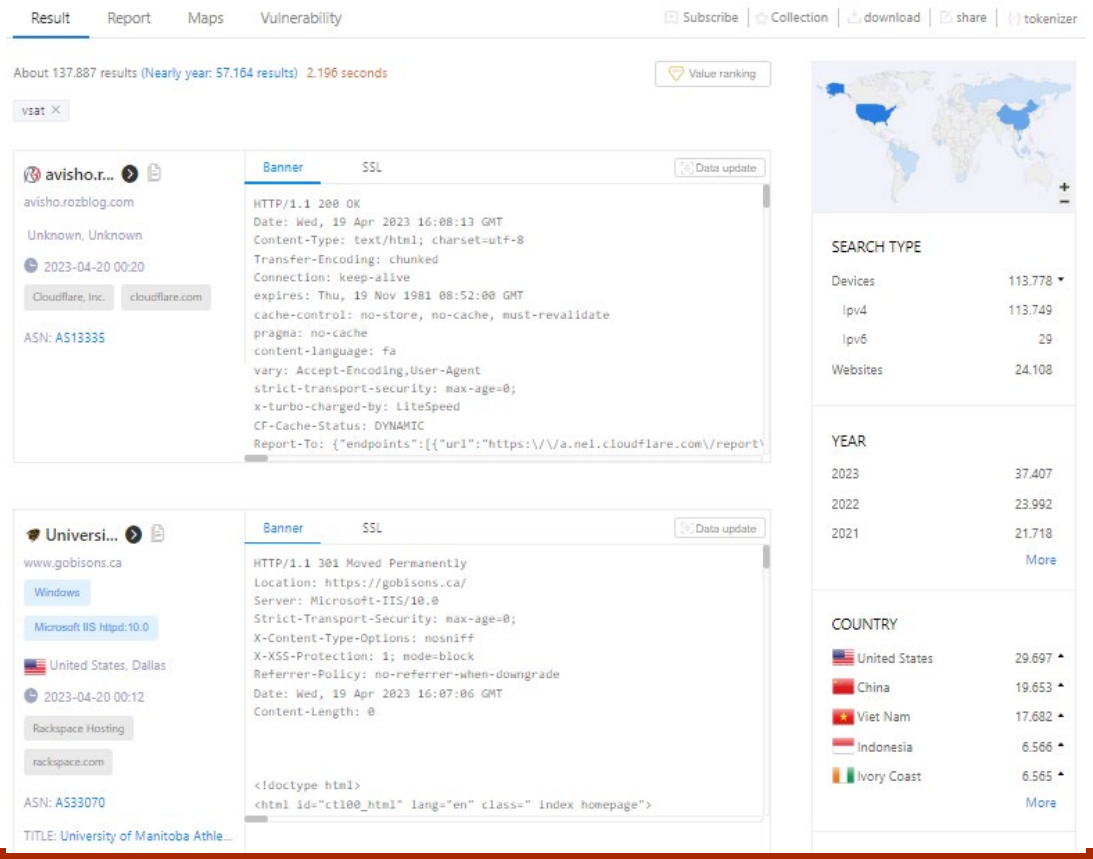
- **https://www.zoomeye.ai/**

- **VSAT *(Very-Small-Aperture Terminal)***
  - **Sistema usato per comunicazioni satellitari**
  - **VSAT utilizza *IPv4* per la comunicazione**

ZoomEye

Esempio 5

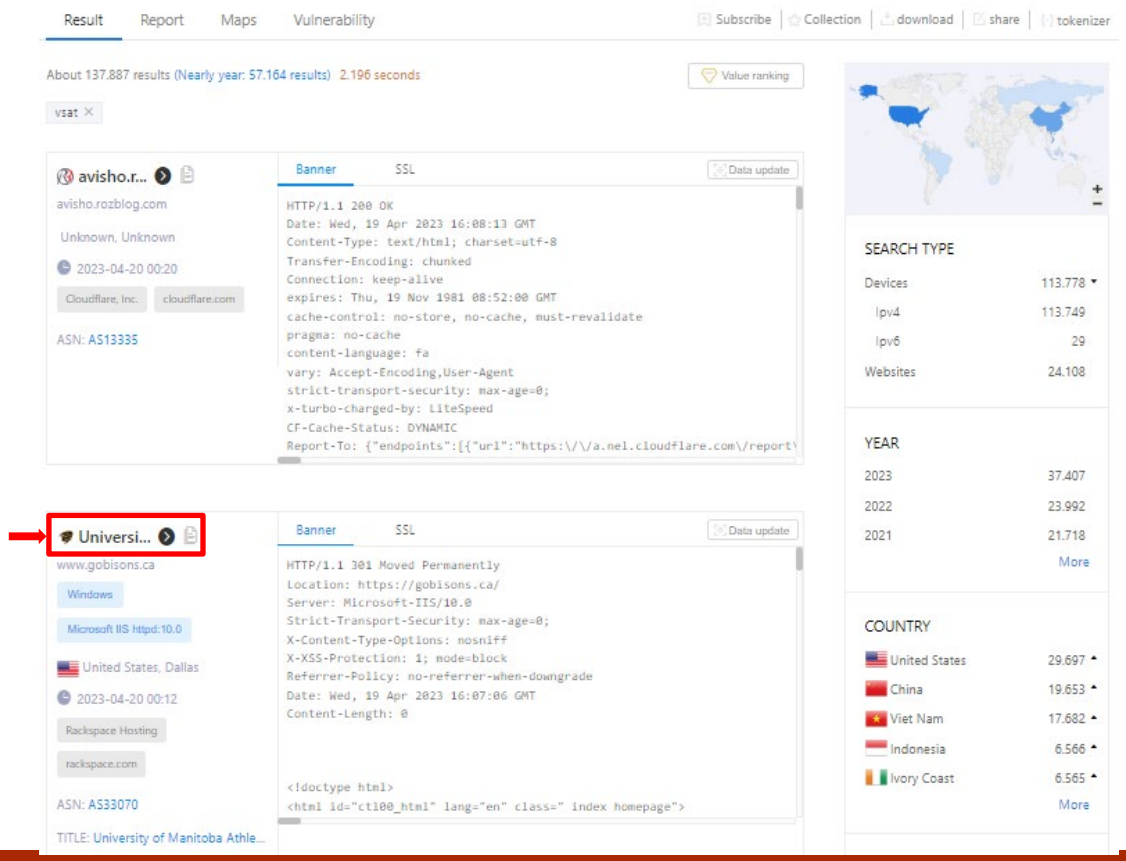
- **https://www.zoomeye.ai/**



ZoomEye

Esempio 5

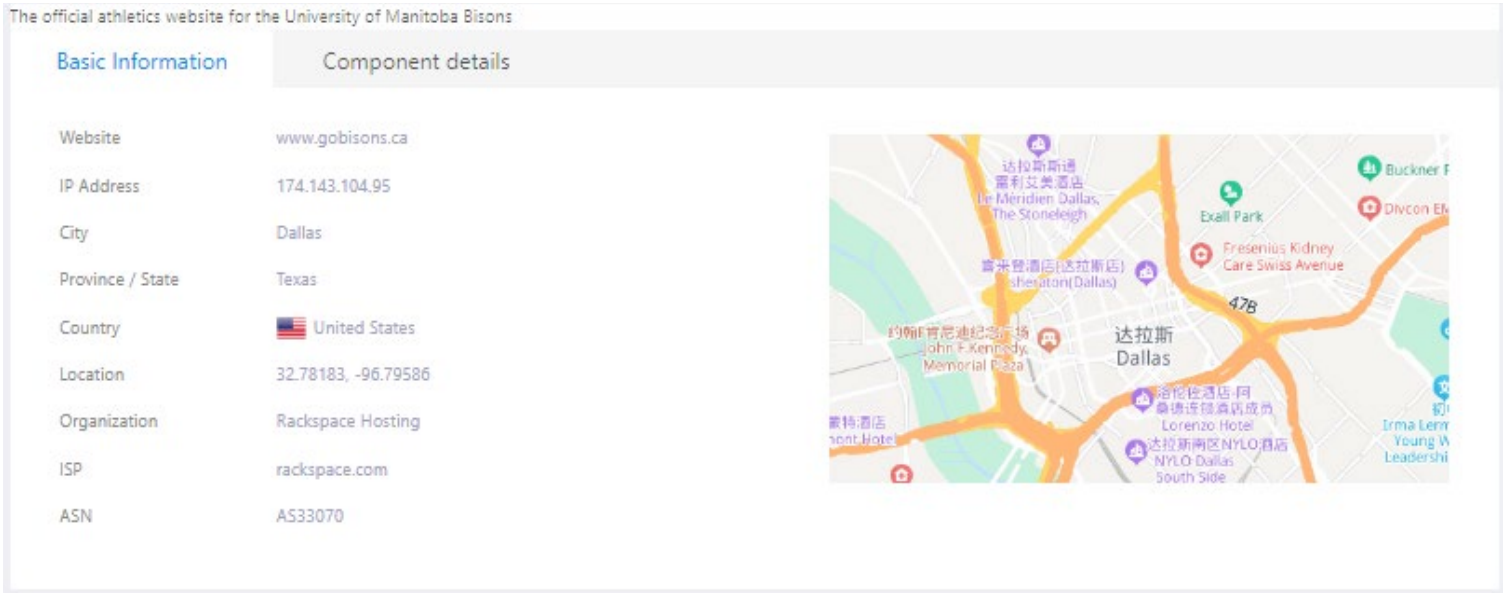
- **https://www.zoomeye.ai/**



ZoomEye

Esempio 5

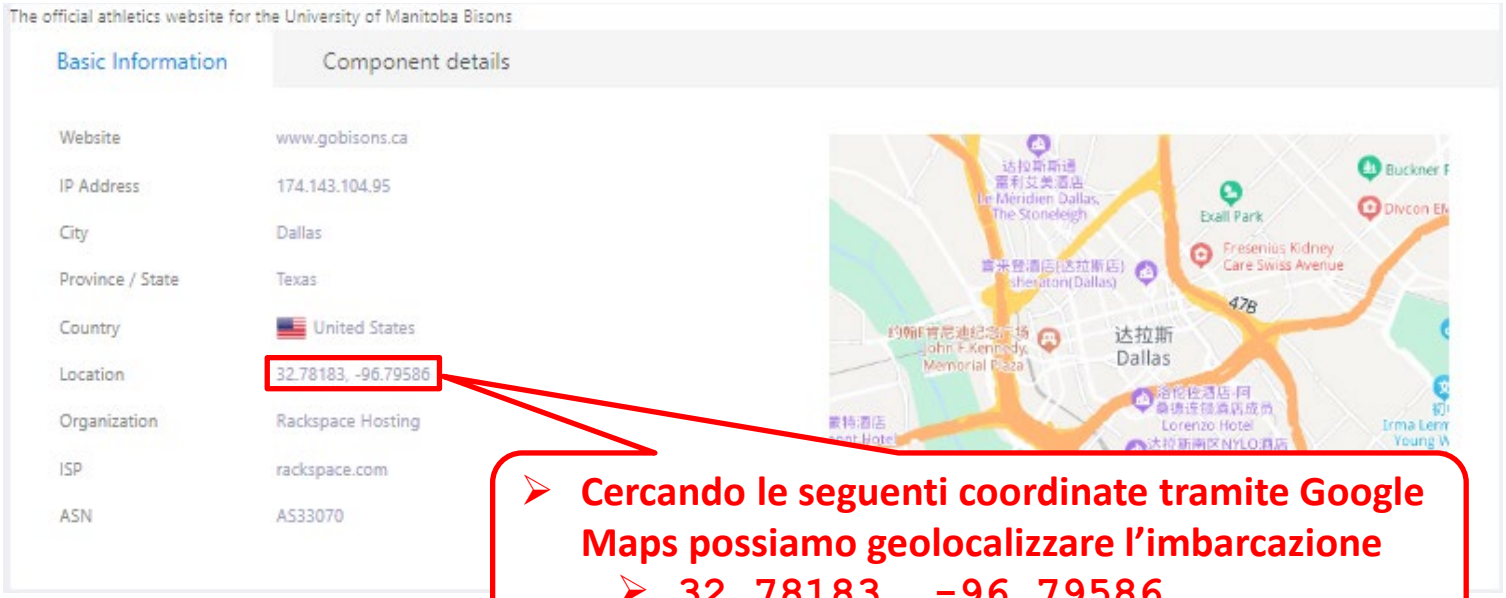
- **https://www.zoomeye.ai/**



ZoomEye

Esempio 5

- **https://www.zoomeye.ai/**



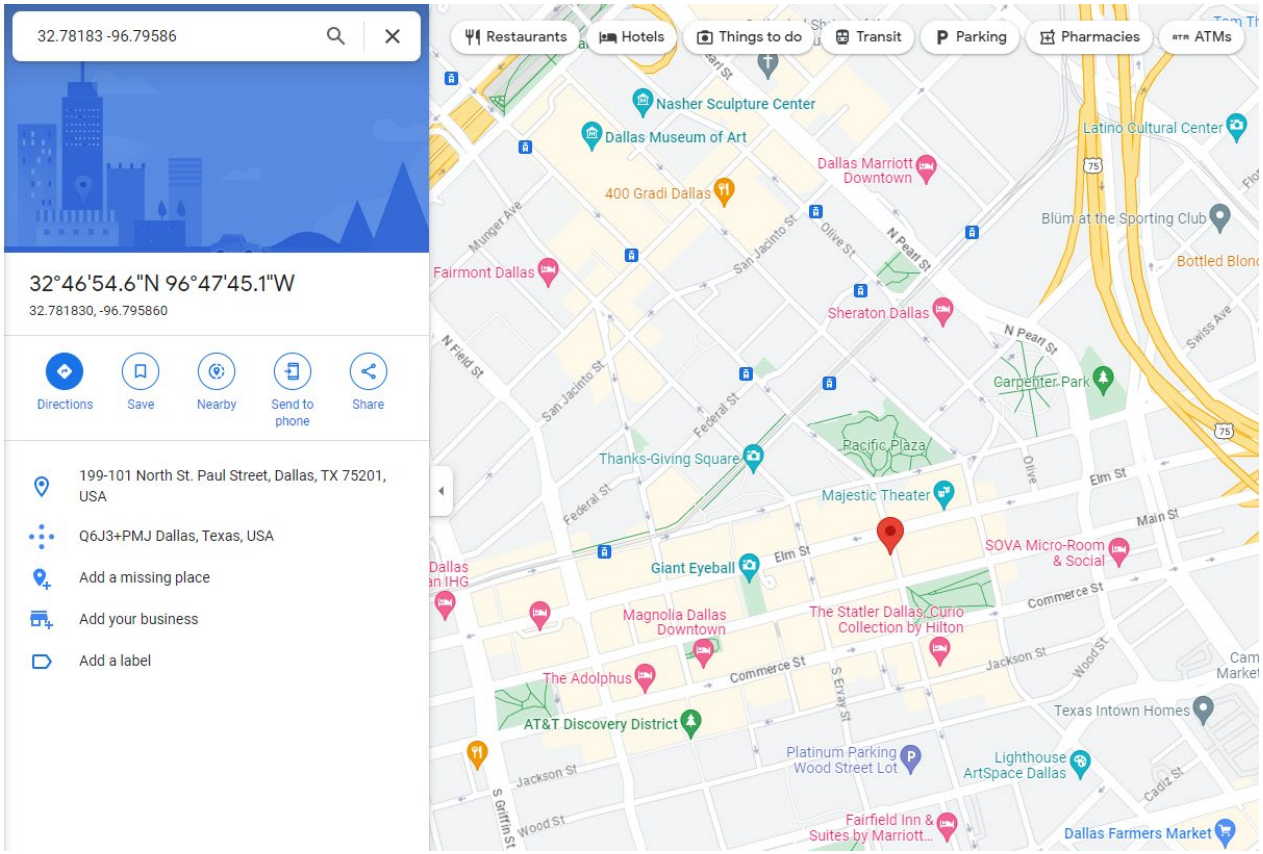
- **Cercando le seguenti coordinate tramite Google Maps possiamo geolocalizzare l'imbarcazione**
  - **32.78183, -96.79586**

ZoomEye

Esempio 5

- **https://www.zoomeye.ai/**

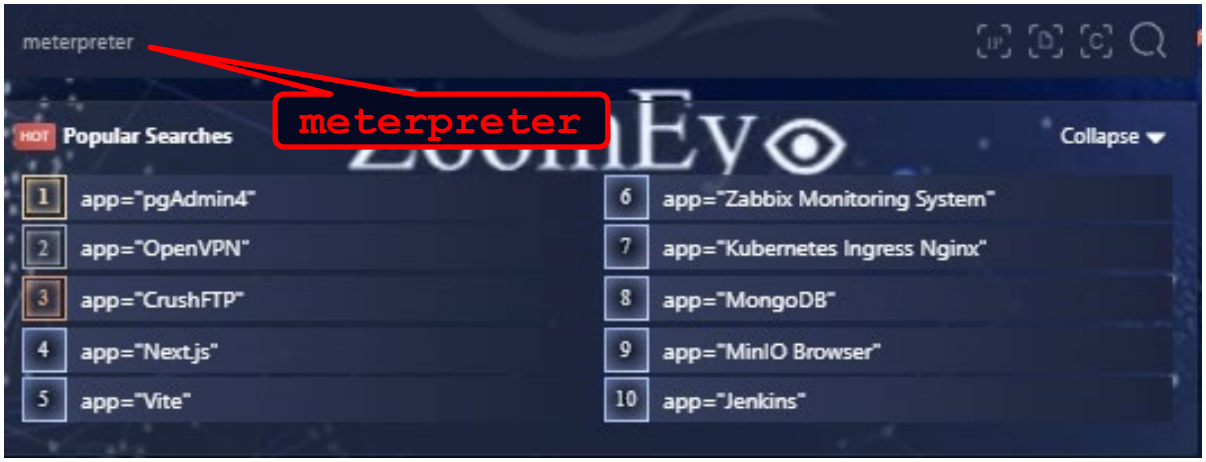
Possiamo inserire le coordinate geografiche su Google Maps



ZoomEye

Esempio 6

- **https://www.zoomeye.ai/**

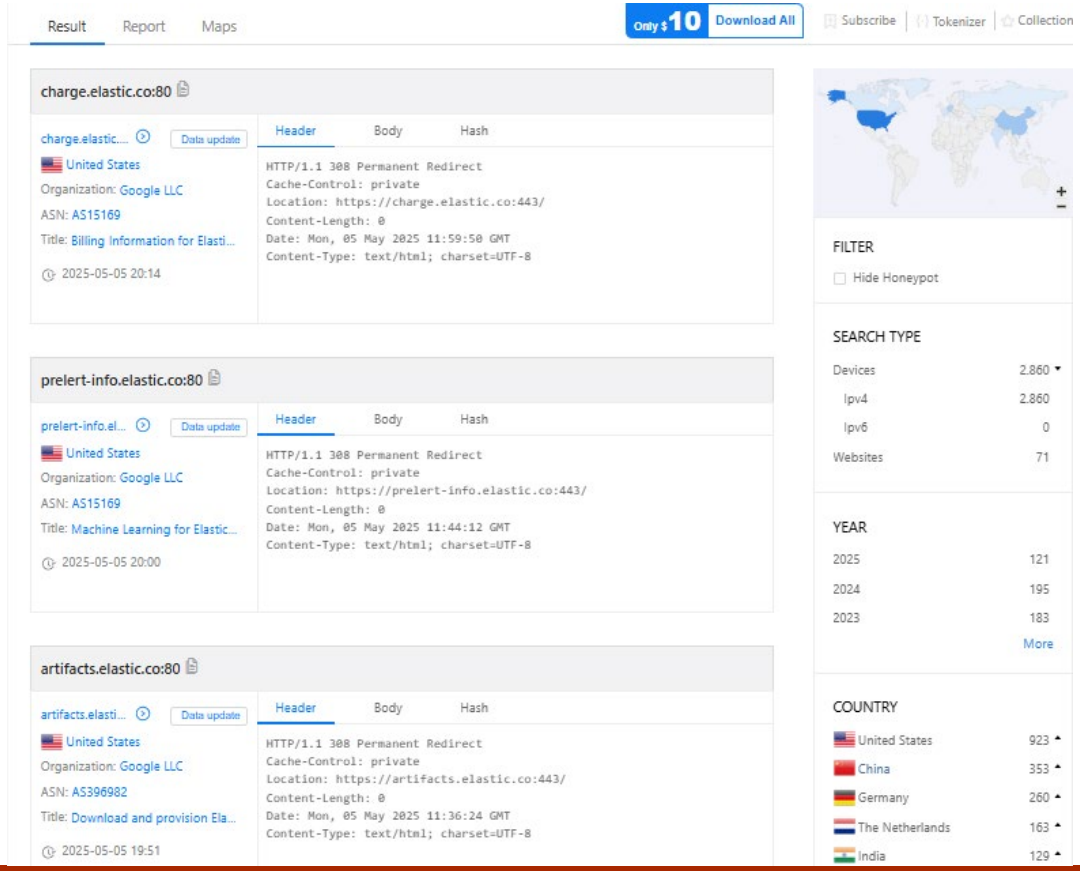


- **Meterpreter**
  - **Payload avanzato, appartenente alla suite Metasploit**
  - **Consente l'accesso remoto ad una macchina target**

ZoomEye

Esempio 6

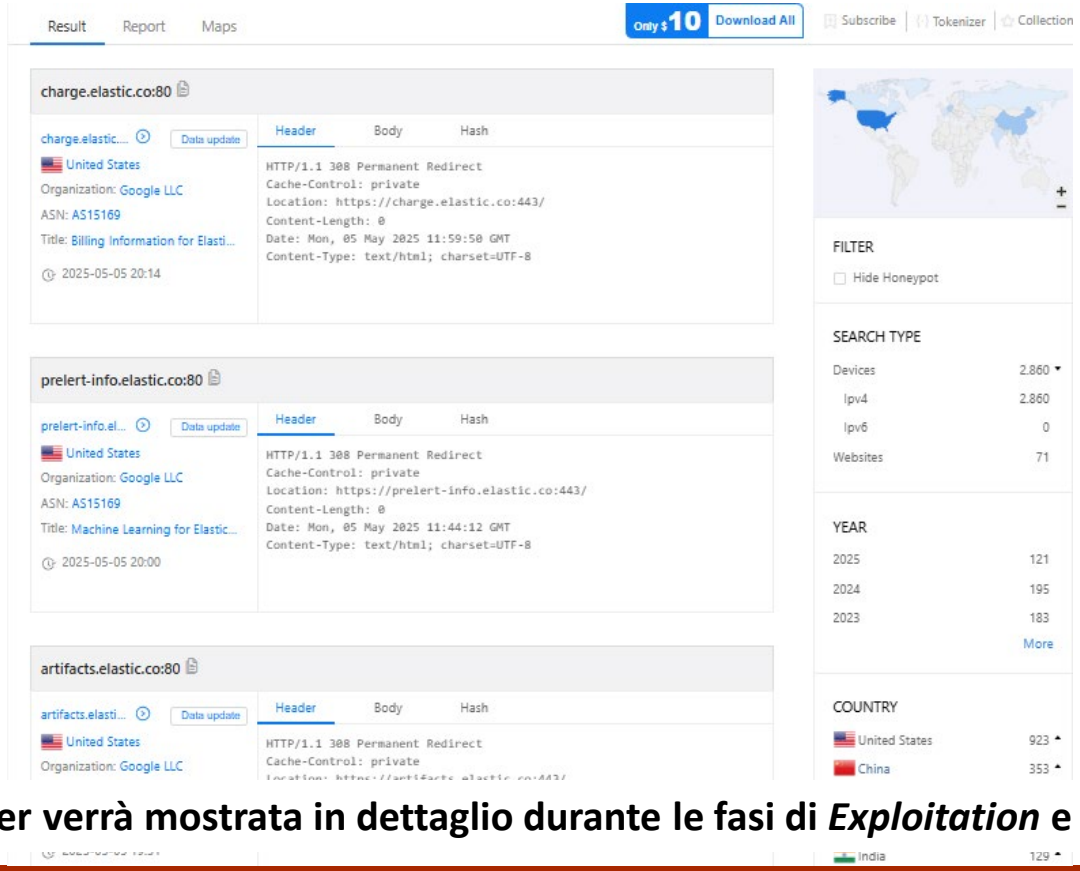
- **https://www.zoomeye.ai/**



ZoomEye

Esempio 6

- **https://www.zoomeye.ai/**



La suite Meterpreter verrà mostrata in dettaglio durante le fasi di *Exploitation* e *Post Exploitation*

Outline

- Concetti Introduttivi
- Suite Protocollare TCP/IP
- Formato dei Messaggi TCP e UDP
- Active Enumeration
  - Network Scanner Nmap
  - Zenmap
  - Unicornscan
  - Masscan
- Passive Enumeration
  - Shodan
  - ZoomEye
  - **FOFA**
  - Censys

FOFA

- Motore di ricerca cinese per dispositivi e servizi esposti su Internet, simile a Shodan o ZoomEye

- Effettua ricerche passive su IP, domini, certificati SSL, header HTTP ed altri metadati di rete

- Usato in ambito:
  - OSINT
  - Security assessment
  - Threat hunting
  - Bug bounty e pentest

FOFA

Pricing

- **https://en.fofa.info/vip**

FOFA

Interfaccia

- **https://en.fofa.info/**

FOFA

Query Syntax

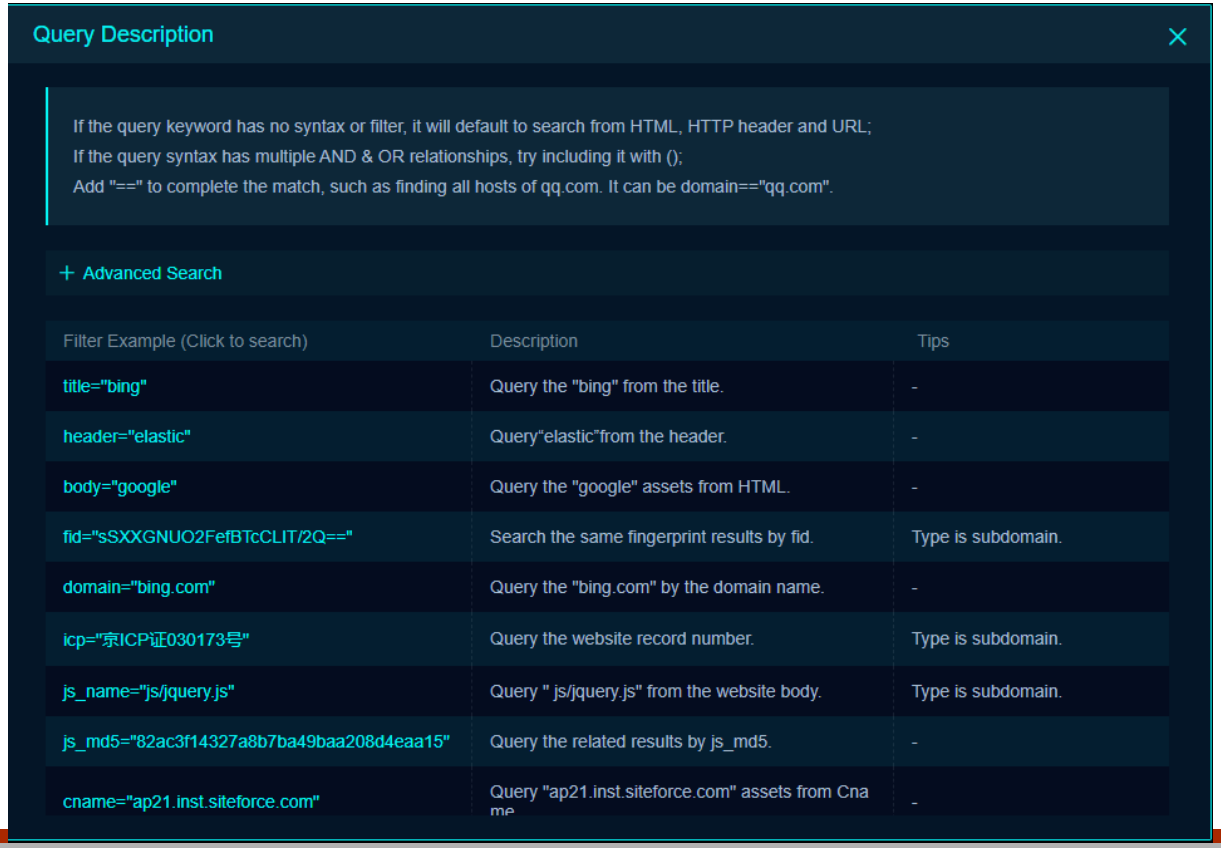
- Offre funzionalità molto simili a quelle fornite da Shodan e ZoomEye, accessibili mediante opportuni «filtri»

FOFA

Query Description

- **https://en.fofa.info/**

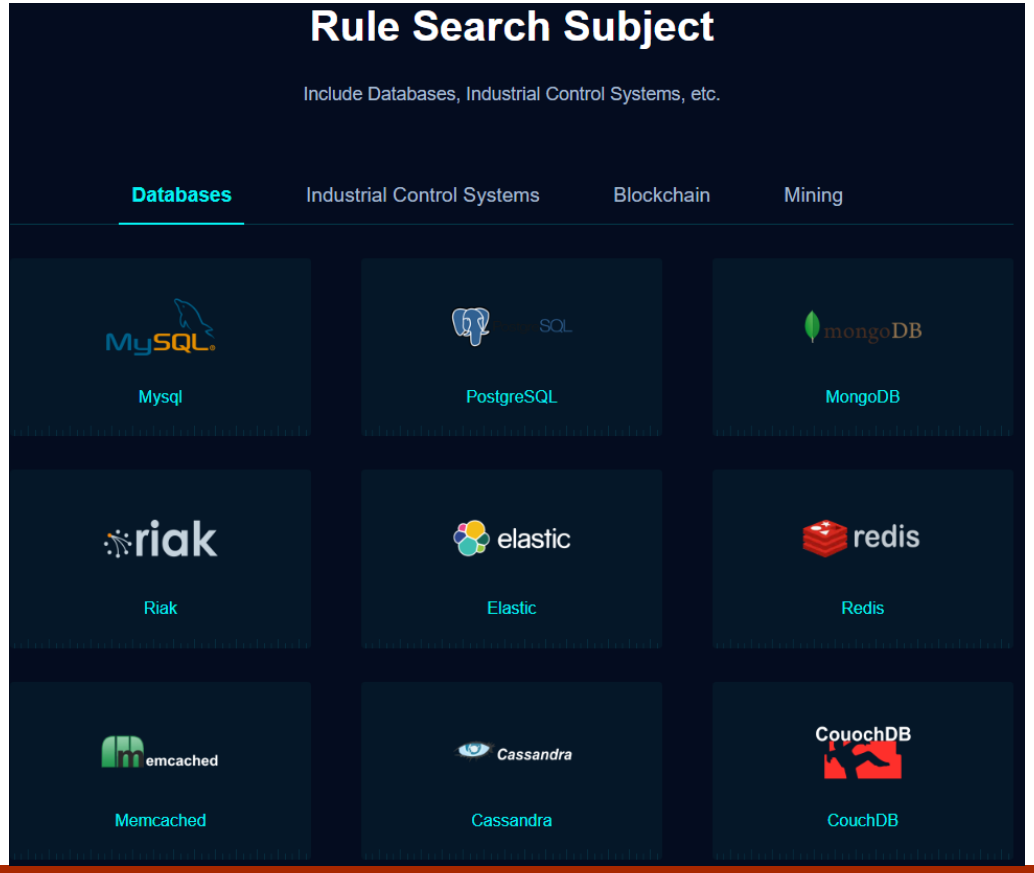
Output Parziale



FOFA

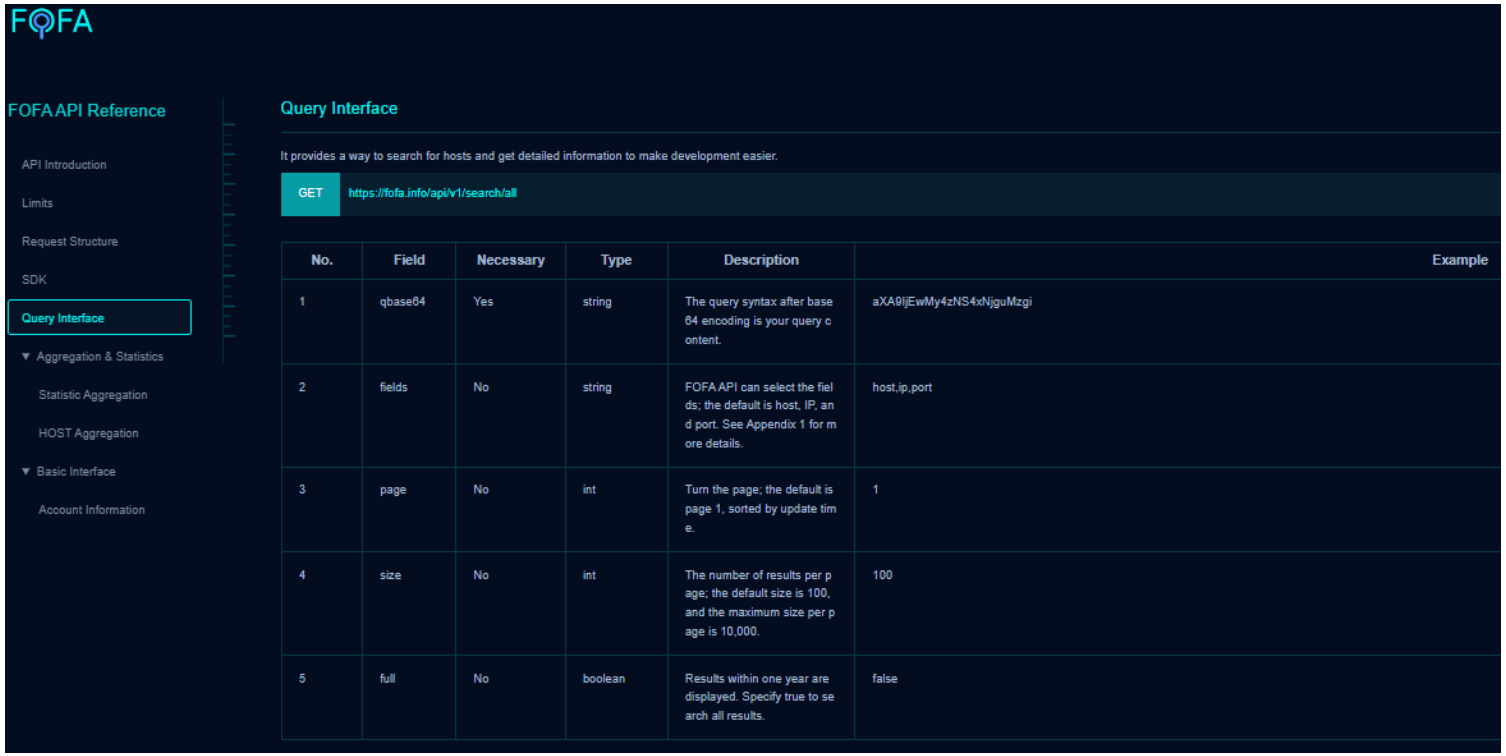
Featured Categories

- https://en.fofa.info/subject



FOFA
API

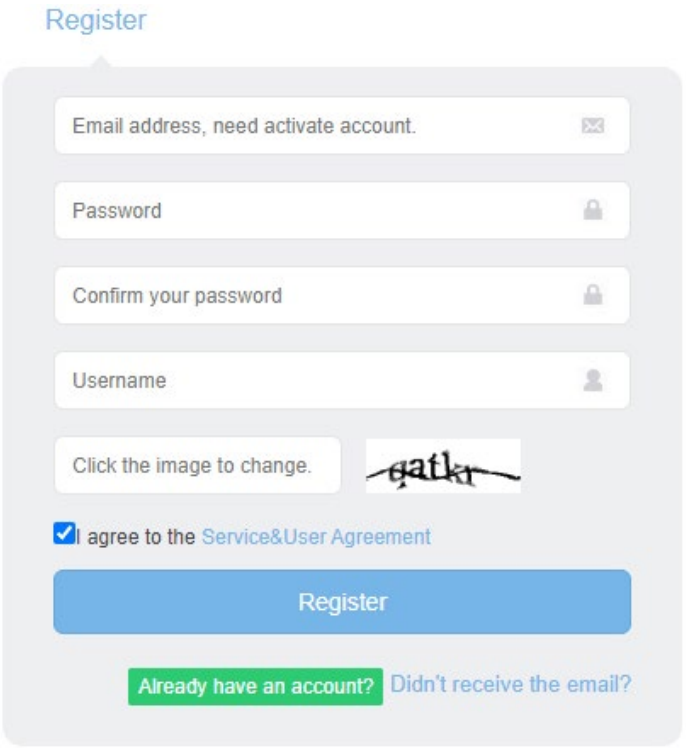
- FOFA offre delle proprie API
  - **https://en.fofa.info/api**



FOFA

Registrazione

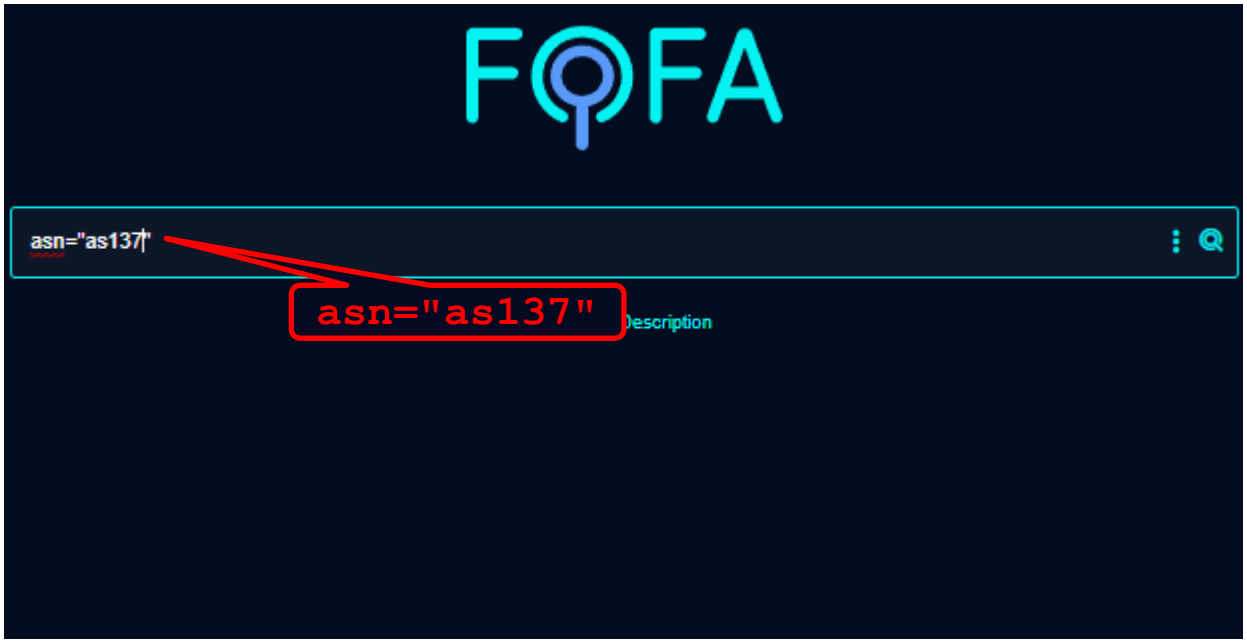
- Prima di utilizzare FOFA è opportuno registrarsi su
  - https://i.nosec.org/register?locale=en&service=https://en.fofa.info/f_login



FOFA

Esempio 1

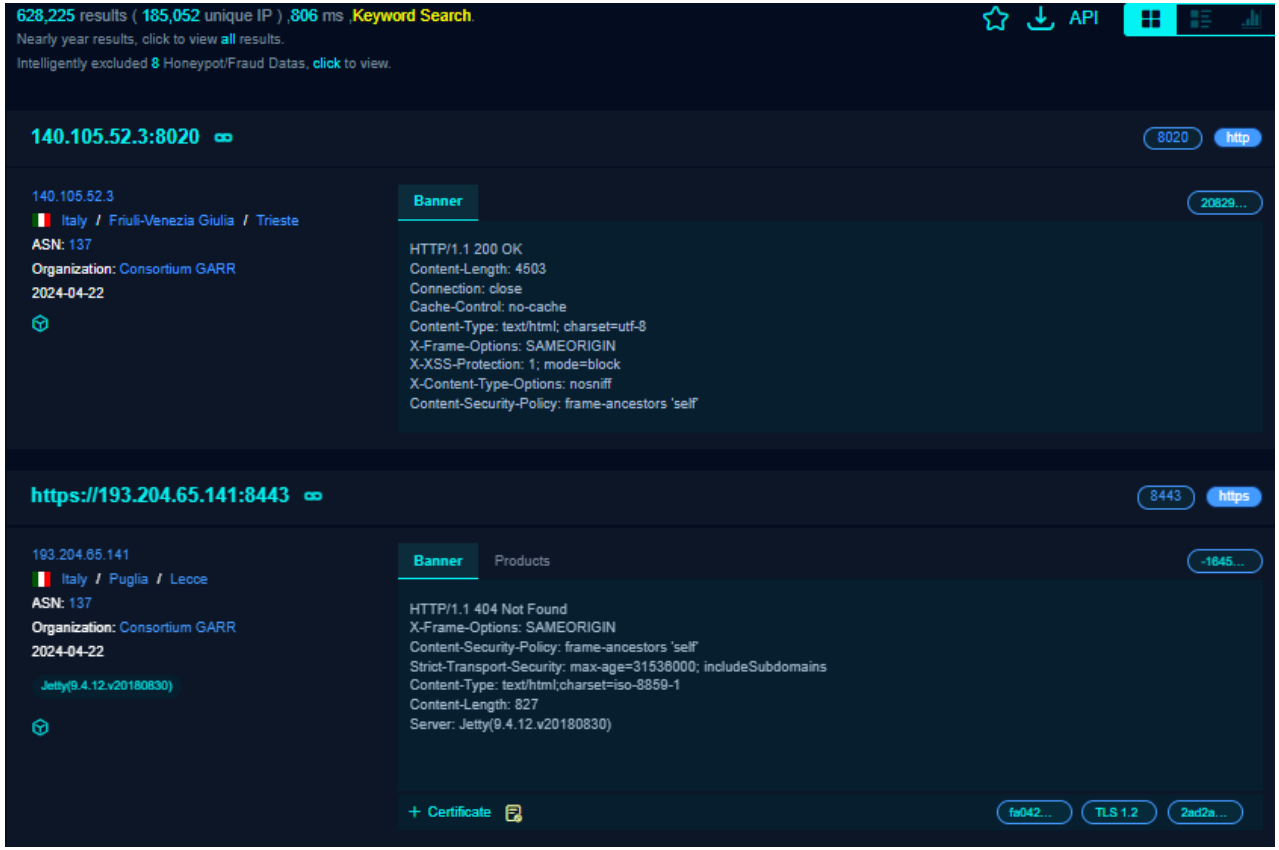
- Effettuiamo una ricerca per Autonomous System Network (**`asn=as137`**)



FOFA

Esempio 1

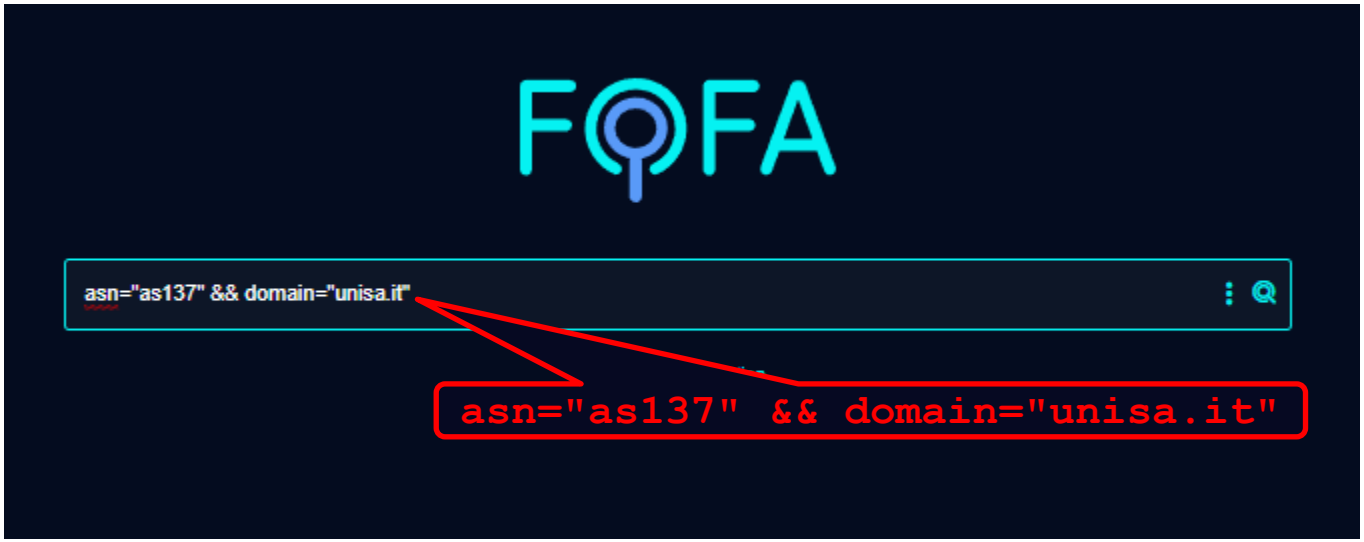
- Effettuiamo una ricerca per Autonomous System Network (**`asn=as137`**)



FOFA

Esempio 2

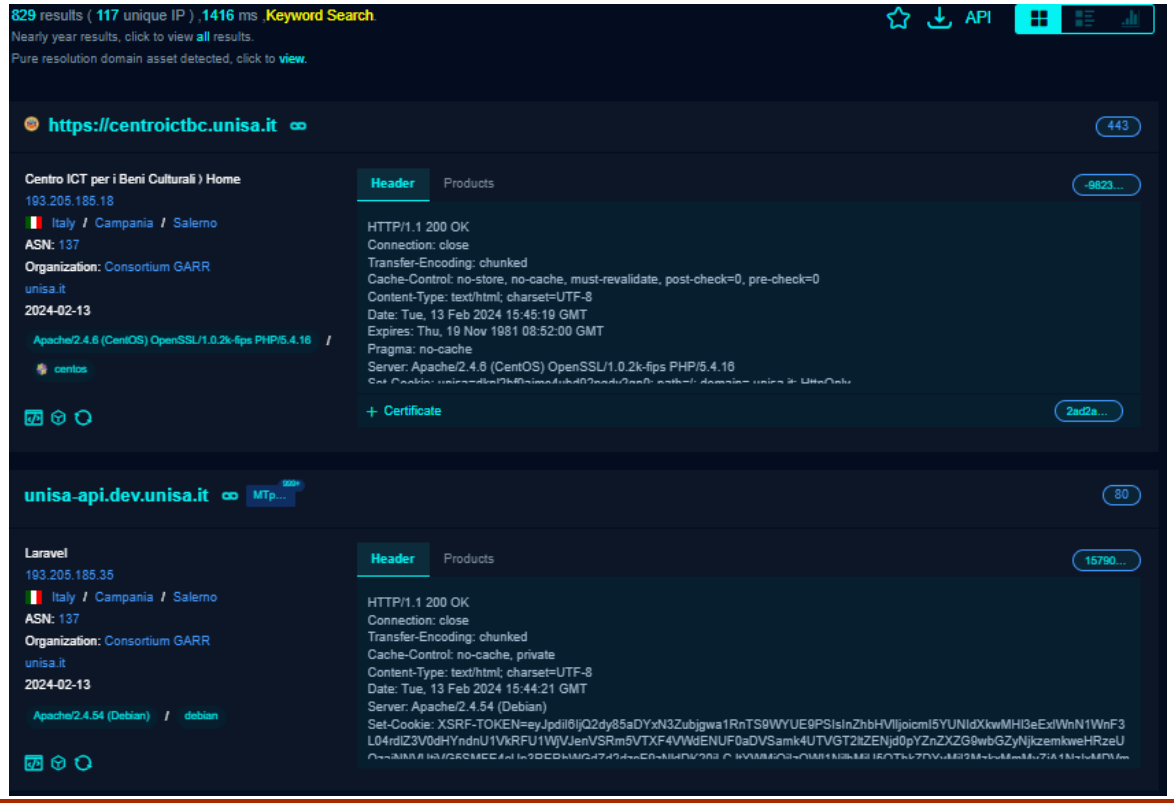
- Effettuiamo una ricerca per Autonomous System Network (**`asn=as137`**) e dominio **`unisa.it`**



FOFA

Esempio 2

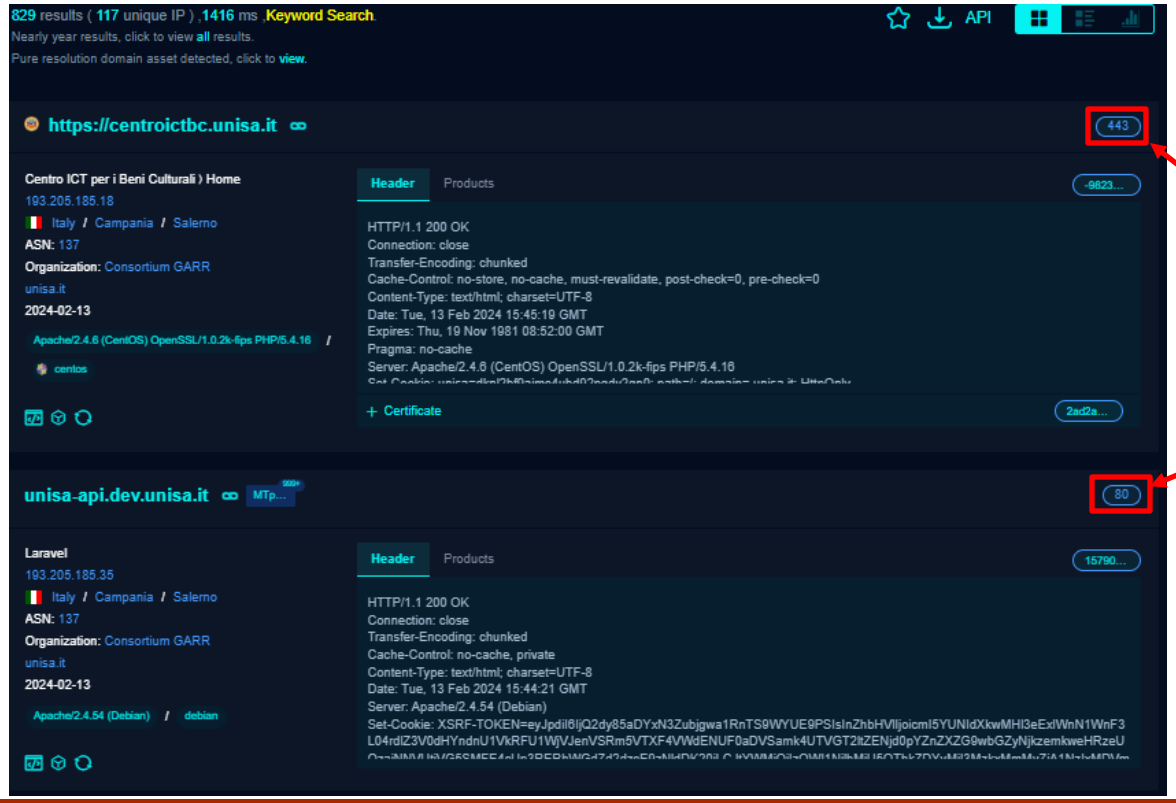
- Effettuiamo una ricerca per Autonomous System Network (**`asn=as137`**) e dominio **`unisa.it`**



FOFA

Esempio 2

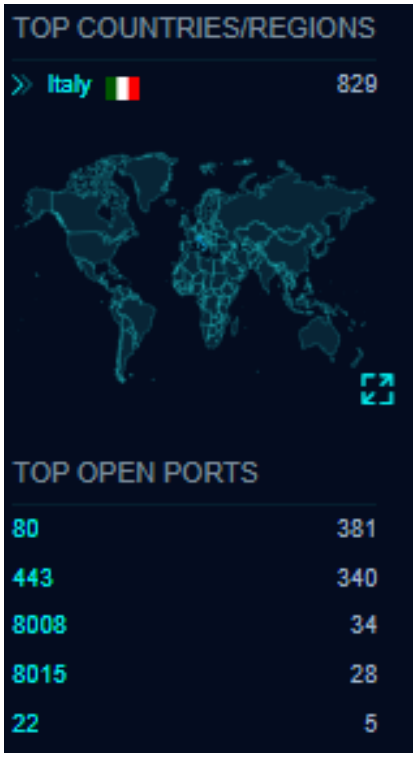
- Effettuiamo una ricerca per Autonomous System Network (**`asn=as137`**) e dominio **`unisa.it`**

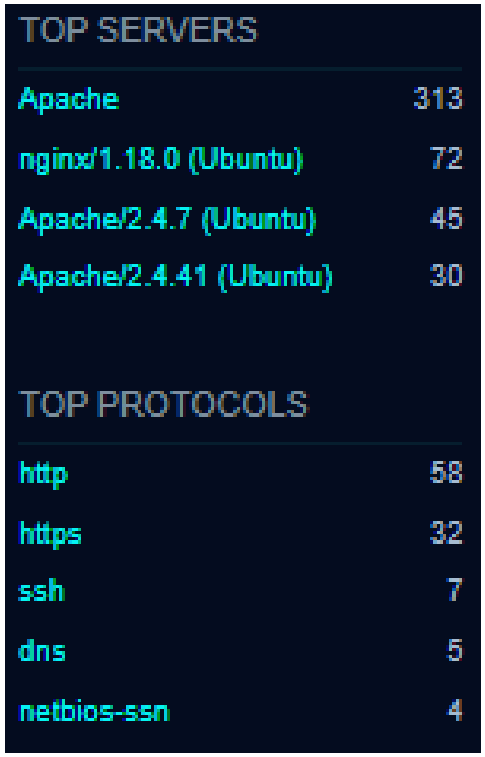


FOFA

Esempio 2

- Effettuiamo una ricerca per Autonomous System Network (**`asn=as137`**) e dominio **`unisa.it`**





Outline

- Concetti Introduttivi
- Suite Protocollare TCP/IP
- Formato dei Messaggi TCP e UDP
- Active Enumeration
  - Network Scanner Nmap
  - Zenmap
  - Unicornscan
  - Masscan
- Passive Enumeration
  - Shodan
  - ZoomEye
  - FOFA
  - **Censys**

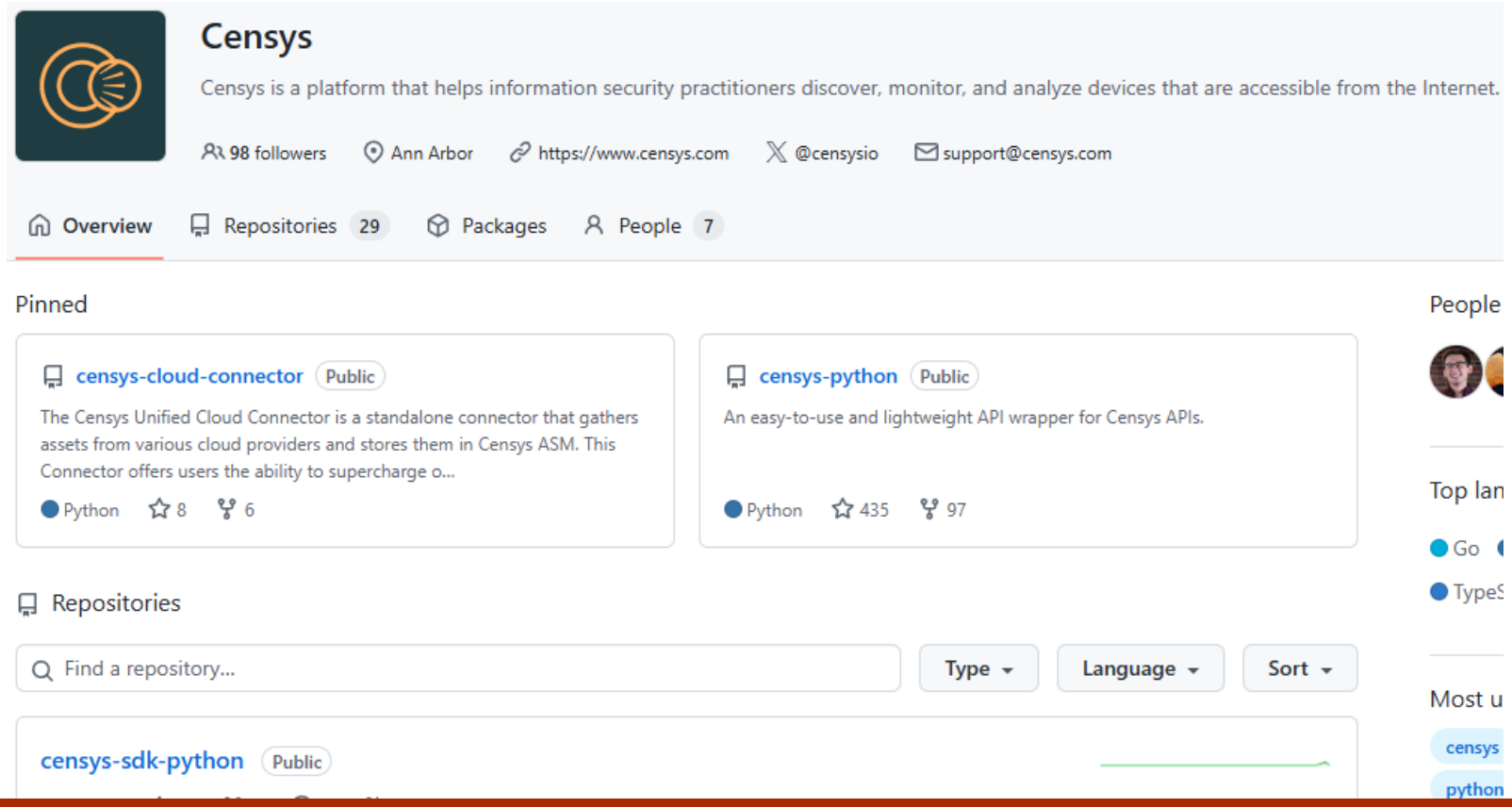
Censys
Caratteristiche

- Piattaforma open-source e commerciale per l'analisi della superficie d'attacco online
- Ricerca dispositivi, domini e certificati digitali esposti
- Individua anche vulnerabilità note, configurazioni errate, ed asset non registrati
- Scannerizza continuamente IPv4, IPv6, HTTP, HTTPS, SMTP, SSH, etc.
- Integra feed CVE, Shodan-like query, API, dashboard di analisi
- Supporta filtri avanzati, JSON search e tagging automatico

Censys

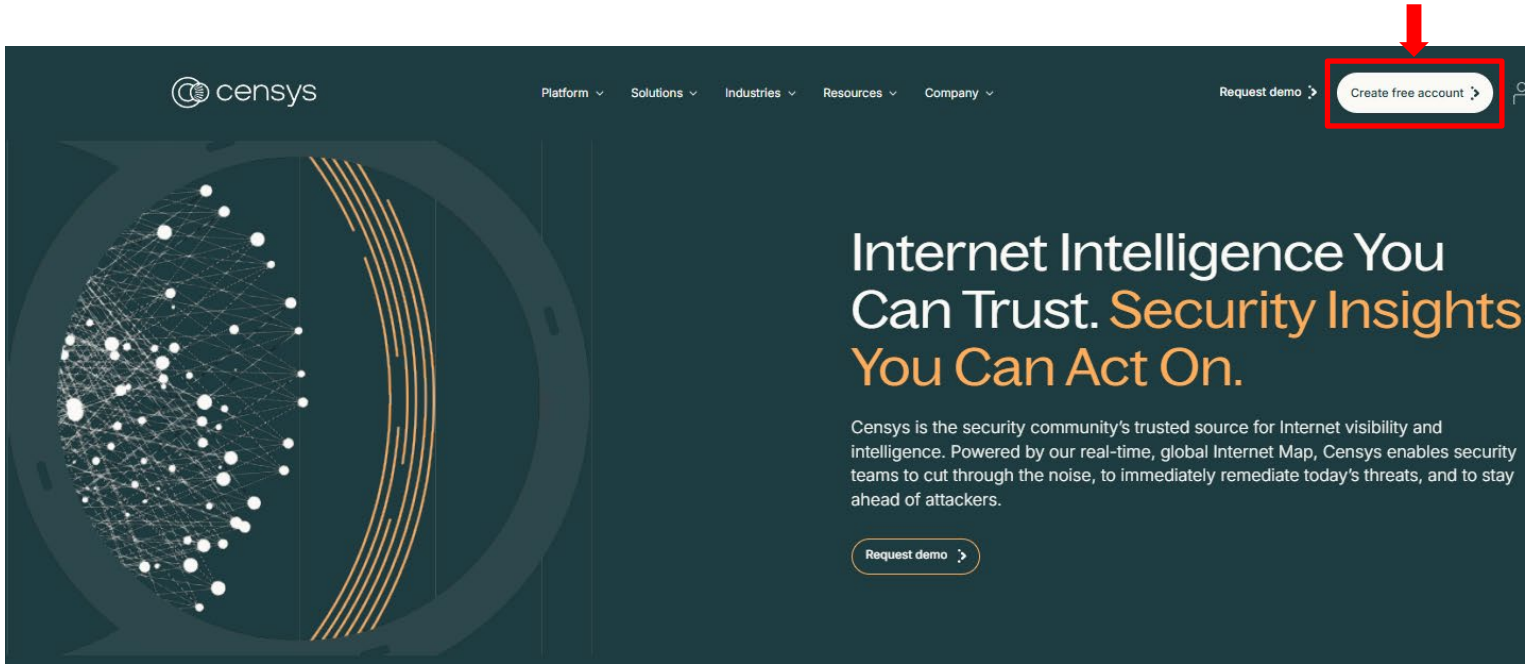
Progetto GitHub

- **`https://github.com/censys`**



Censys
Interfaccia Web

- **`https://censys.com/`**

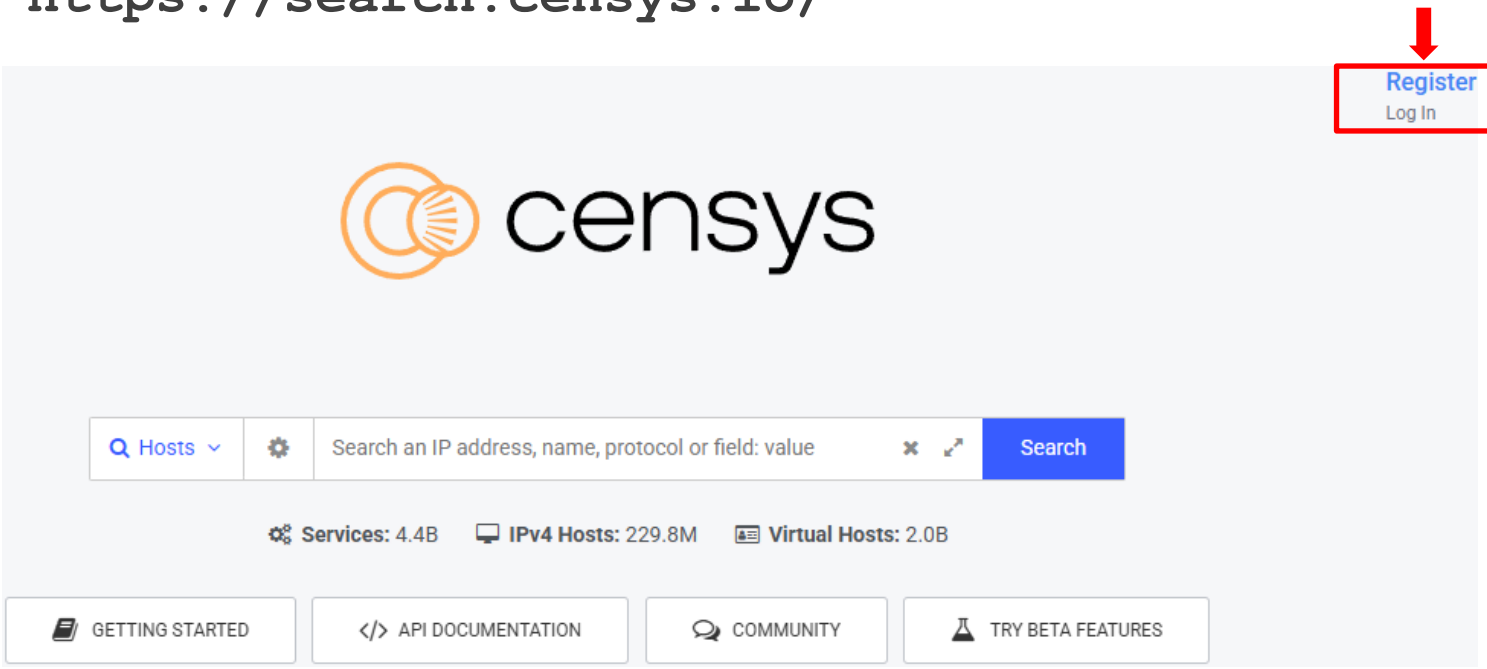


Per poter utilizzare Censys è necessaria la registrazione

Censys

Vecchia Interfaccia Web (ancora funzionante)

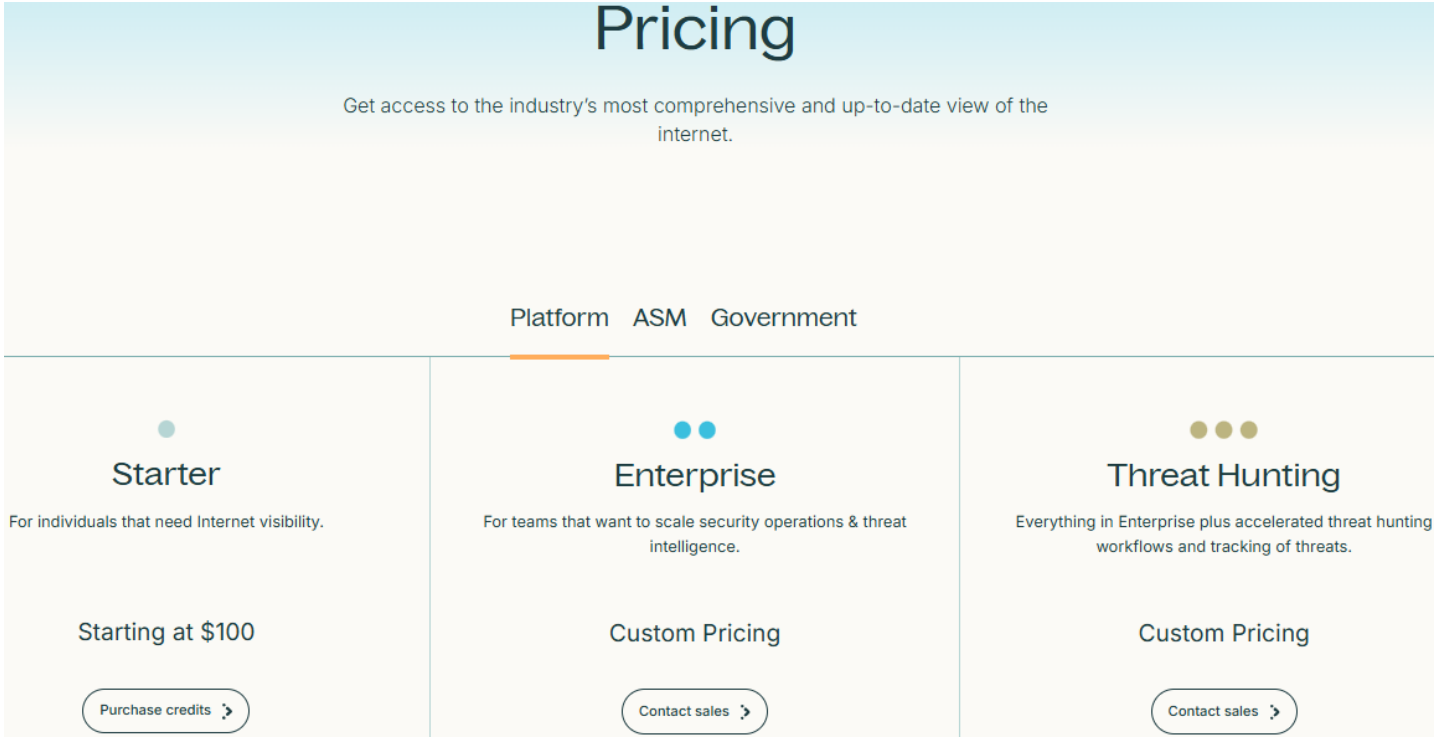
- **`https://search.censys.io/`**



Per poter utilizzare Censys è necessaria la registrazione

Censys
Pricing

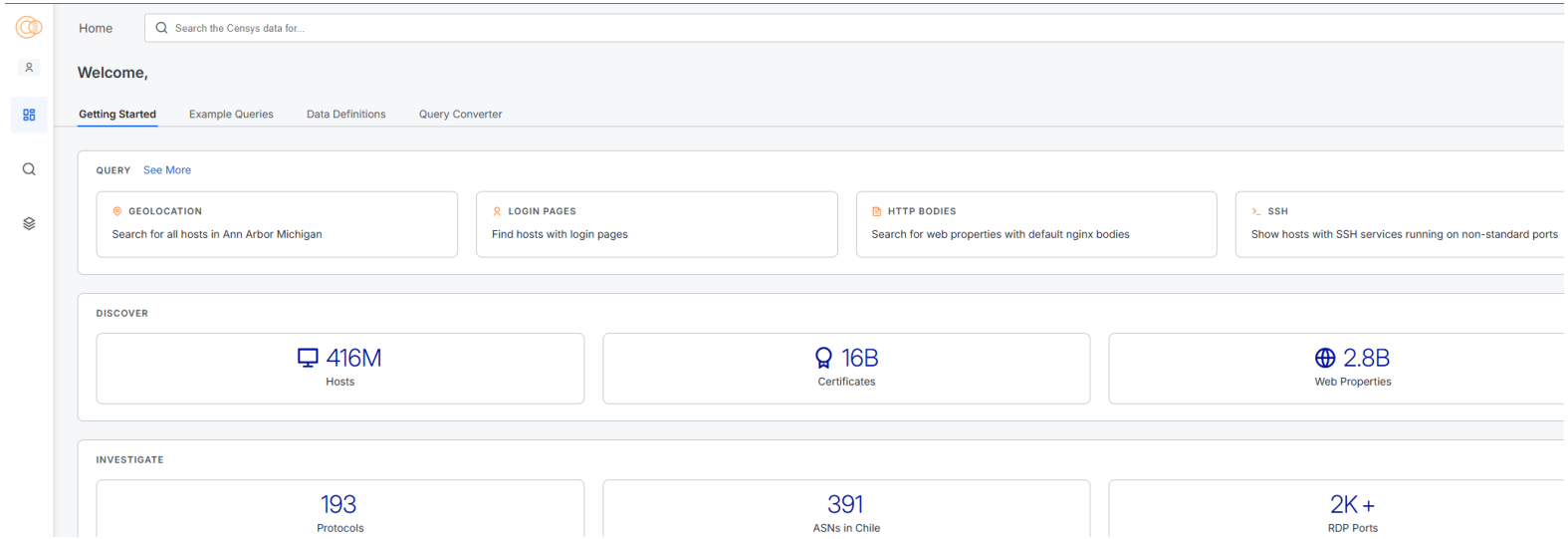
- **`https://censys.com/resources/pricing`**



Censys

Interfaccia di Ricerca

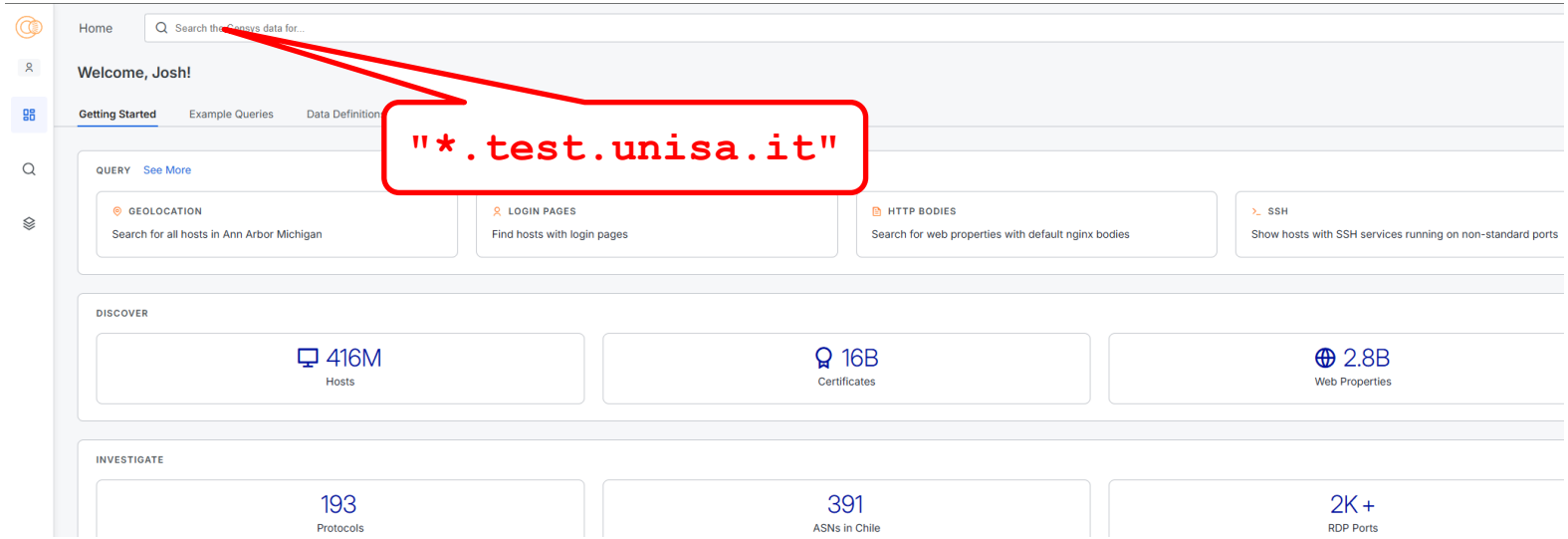
- **https://censys.io/**



Censys

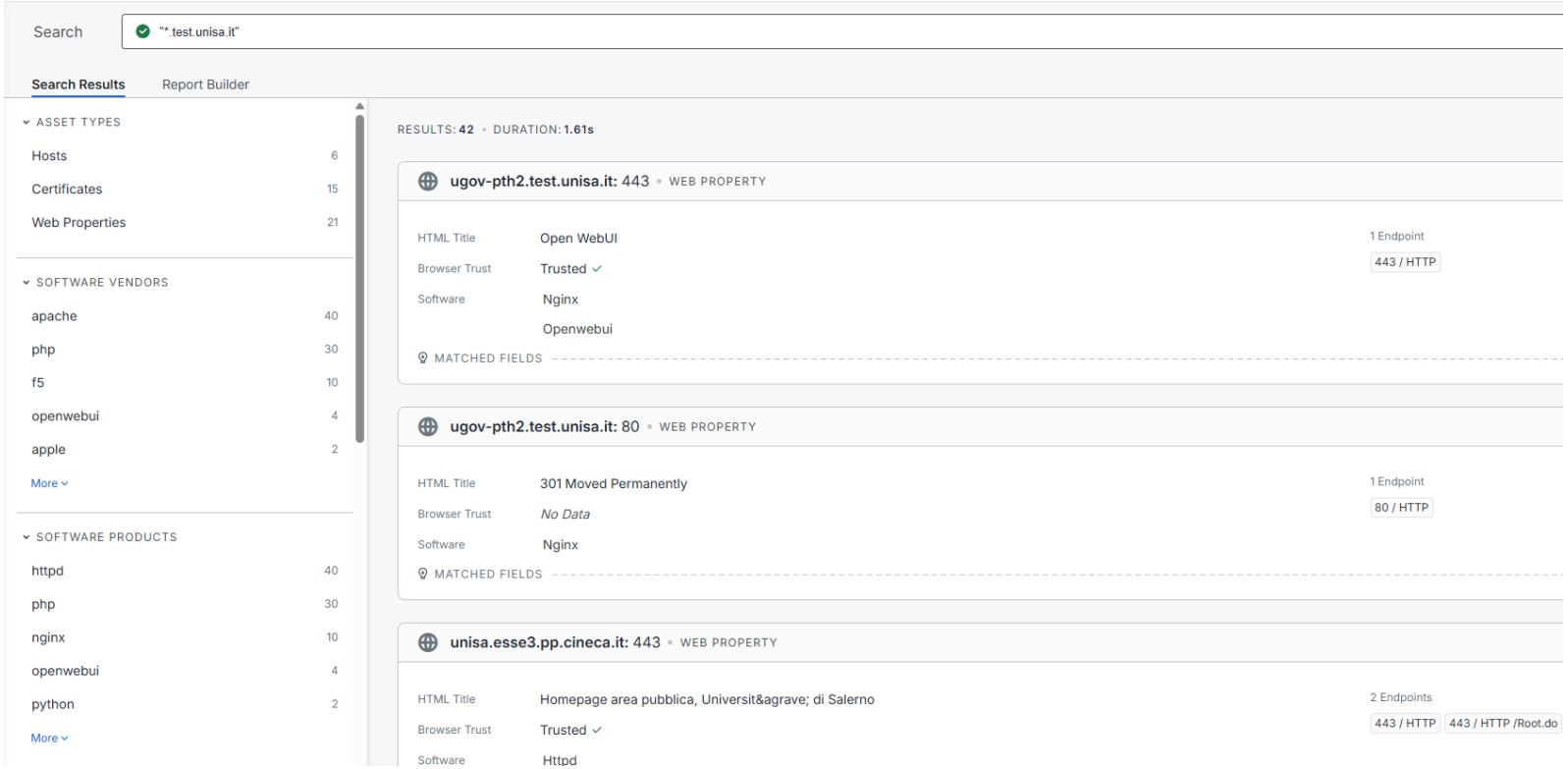
Interfaccia di Ricerca – Esempio

- **https://censys.io/**



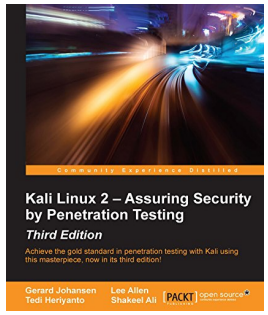
Censys

Interfaccia di Ricerca – Esempio

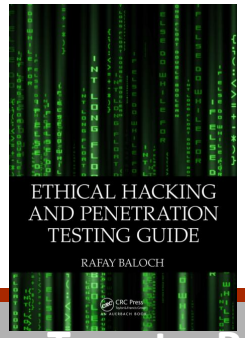


Bibliografia

- **Kali Linux 2 - Assuring Security by Penetration Testing. Third Edition**. Gerard Johansen, Lee Allen, Tedi Heriyanto, Shakeel Ali. Packt Publishing. 2016
  - Capitolo 6



- **Ethical Hacking and Penetration Testing Guide**. Rafay Baloch. CRC Press. 2014
  - Capitolo 4



Bibliografia

- **Guida di riferimento di Nmap (pagina del manuale)**
  - https://nmap.org/man/it/

- **Guida Rapida per Nmap**
  - https://www.stationx.net/nmap-cheat-sheet

Bibliografia

- **ZoomEye**
  - https://www.zoomeye.org/doc

- **Shodan**
  - https://danielmiessler.com/study/shodan/
  - https://help.shodan.io/the-basics/search-query-fundamentals
  - https://github.com/JavierOlmedo/shodan-filters