Open Source Intelligence (OSINT) Investigation Report

I. Introduction

A. Purpose of the Investigation	Perform OSINT information on the domain "atomic-nuclear.site" & document sensitive information that is publicly available
B. Scope	atomic-nuclear.site and its subdomains

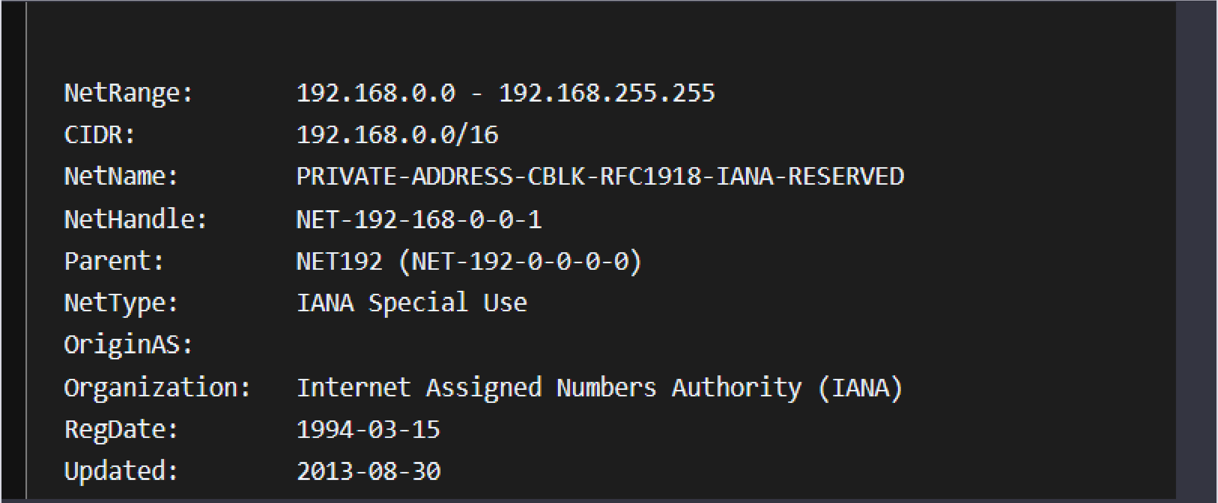
II. Methodology

A. Tools Used	theHarvester, dnsenum, dnsrecon ,dnsmap, Sublistr3,spiderfoot
B. Techniques Employed	• Step1 - We will do WHOIS lookup for Domain name availability. • Step2 - Find the subdomains, Ip address, mail serves, email Ids. • Step3 – Proceed with Web analysis, server related information (censys), Relevant Information using Wayback machine and Shadon search engine, using google dorks • Step4 - Location gathering for the List of Ip address • Step5 – Find Social Media Presence • Step6 – Final step Analysis. • Step7 – Using OSINT TOOL like spiderfoot, verify the information.

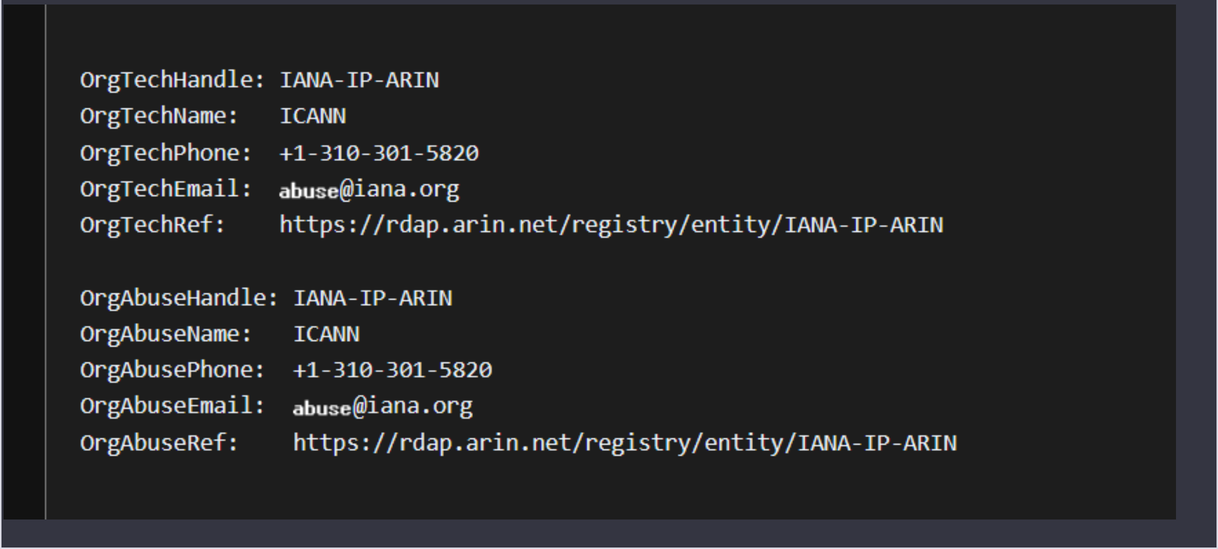
III. Findings

A. **WHOIS Information**

Domain Registration Date	Owner Information	Registration History
1994-03-15	ICANN	-



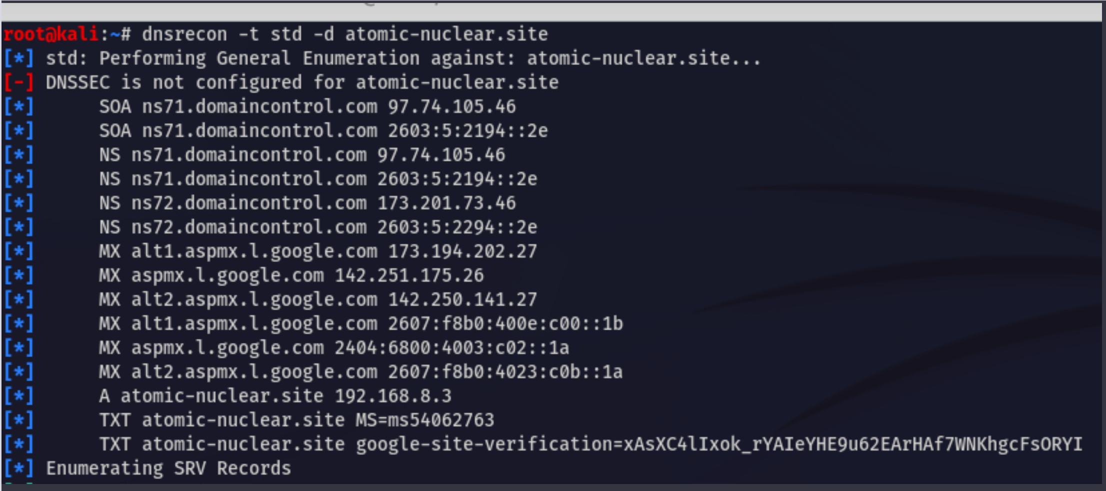
```
NetRange:       192.168.0.0 - 192.168.255.255
CIDR:           192.168.0.0/16
NetName:        PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
NetHandle:      NET-192-168-0-0-1
Parent:         NET192 (NET-192-0-0-0-0)
NetType:        IANA Special Use
OriginAS:
Organization:   Internet Assigned Numbers Authority (IANA)
RegDate:        1994-03-15
Updated:        2013-08-30
```



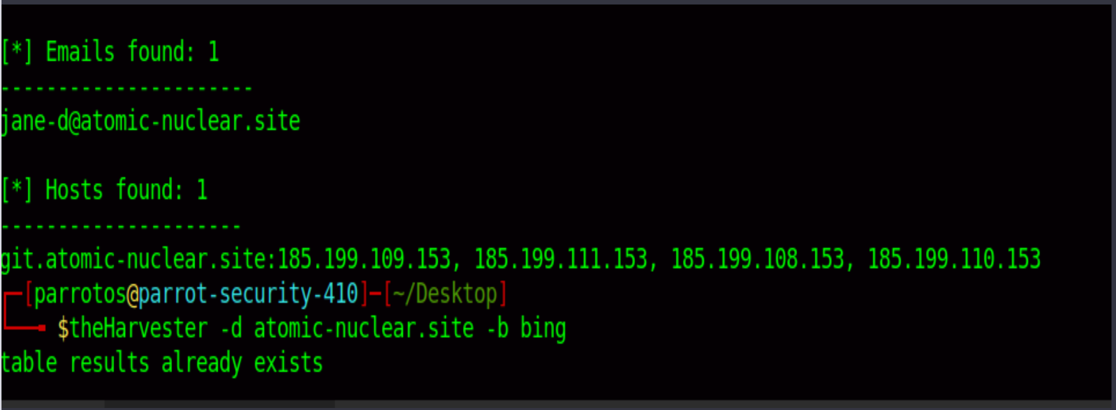
```
OrgTechHandle: IANA-IP-ARIN
OrgTechName:   ICANN
OrgTechPhone:  +1-310-301-5820
OrgTechEmail:  abuse@iana.org
OrgTechRef:    https://rdap.arin.net/registry/entity/IANA-IP-ARIN

OrgAbuseHandle: IANA-IP-ARIN
OrgAbuseName:   ICANN
OrgAbusePhone:  +1-310-301-5820
OrgAbuseEmail:  abuse@iana.org
OrgAbuseRef:    https://rdap.arin.net/registry/entity/IANA-IP-ARIN
```

B. **DNS Information**

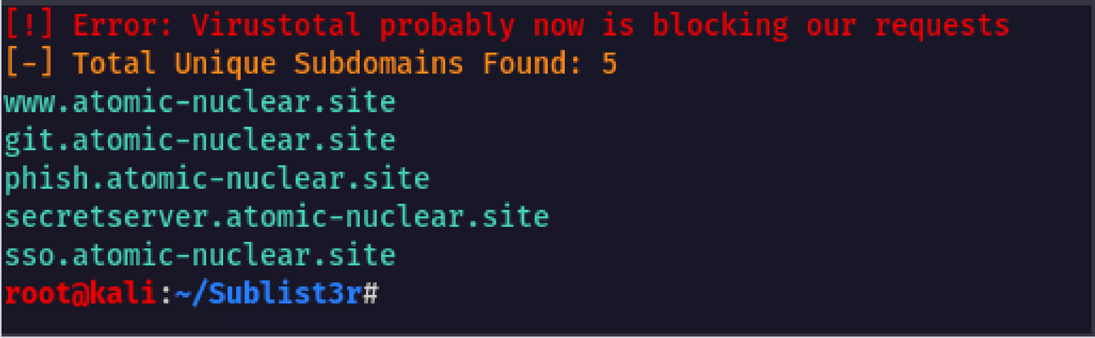
Domain Records	Subdomains	IP Addresses
Hostname,nameservermailservers	git.atomic-nuclear.site, sso.atomic-nuclear.site, phish.atomic-nuclear.site, secretserver.atomic-nuclear.site, sso.atomic-nuclear.site	[List of IP Addresses given below]



```
root@kali:~# dnsrecon -t std -d atomic-nuclear.site
[*] std: Performing General Enumeration against: atomic-nuclear.site...
[-] DNSSEC is not configured for atomic-nuclear.site
[*]      SOA ns71.domaincontrol.com 97.74.105.46
[*]      SOA ns71.domaincontrol.com 2603:5:2194::2e
[*]      NS ns71.domaincontrol.com 97.74.105.46
[*]      NS ns71.domaincontrol.com 2603:5:2194::2e
[*]      NS ns72.domaincontrol.com 173.201.73.46
[*]      NS ns72.domaincontrol.com 2603:5:2294::2e
[*]      MX alt1.aspmx.l.google.com 173.194.202.27
[*]      MX aspmx.l.google.com 142.251.175.26
[*]      MX alt2.aspmx.l.google.com 142.250.141.27
[*]      MX alt1.aspmx.l.google.com 2607:f8b0:400e:c00::1b
[*]      MX aspmx.l.google.com 2404:6800:4003:c02::1a
[*]      MX alt2.aspmx.l.google.com 2607:f8b0:4023:c0b::1a
[*]      A atomic-nuclear.site 192.168.8.3
[*]      TXT atomic-nuclear.site MS=ms54062763
[*]      TXT atomic-nuclear.site google-site-verification=xAsXC4lIxok_rYAIeYHE9u62EArHAf7WNKhgcFsORYI
[*] Enumerating SRV Records
```



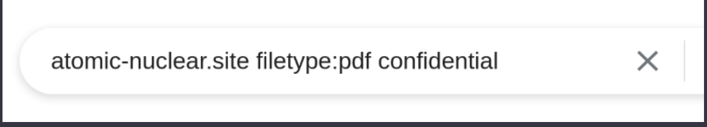
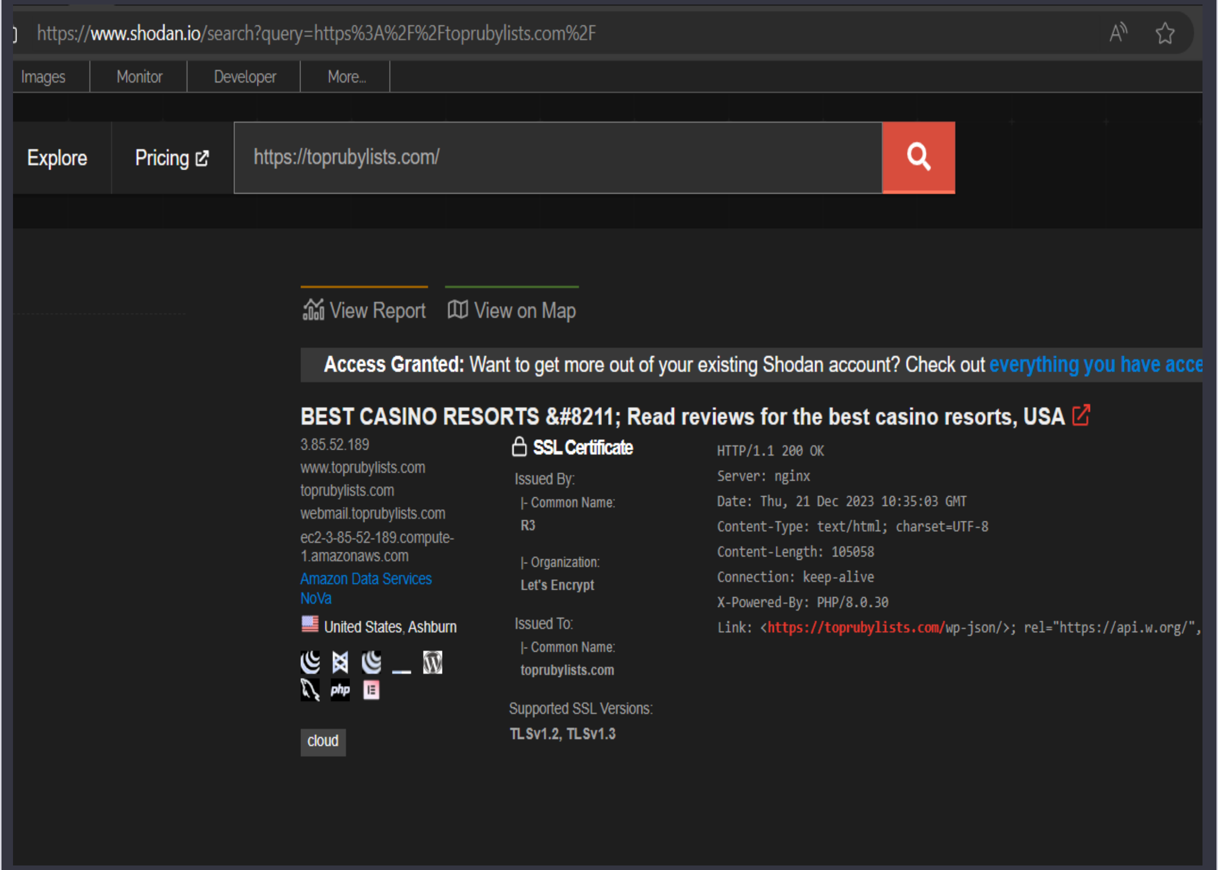
```
[*] Emails found: 1
----------------------
jane-d@atomic-nuclear.site

[*] Hosts found: 1
---------------------
git.atomic-nuclear.site:185.199.109.153, 185.199.111.153, 185.199.108.153, 185.199.110.153
┌─[parrotos@parrot-security-410]─[~/Desktop]
└──╼ $theHarvester -d atomic-nuclear.site -b bing
table results already exists
```



```
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 5
www.atomic-nuclear.site
git.atomic-nuclear.site
phish.atomic-nuclear.site
secretserver.atomic-nuclear.site
sso.atomic-nuclear.site
root@kali:~/Sublist3r#
```

C. **Website Analysis**

We used to **google dorks for finding any confidential pdf and found one(link - ,** https://fissilematerials.org/library/nrc14.pdf)wayback machine and **Shadon search engine** (censys also) for finding information. From **Wayback machine** we do not get any relevant information.

Content Description	Notable Information	Structure Overview
Information gathering through website	Screenshot attached below	Hit all the domain on browser for getting any contact details, use robots.txt or sitemap for other URL (can used Dir buster for url enumeration)
 atomic-nuclear.site filetype:pdf confidential 		

https://www.shodan.io/search?query=https%3A%2F%2Ftoprubylists.com%2F
Images
Monitor
Developer
More...
Explore
Pricing
https://toprubylists.com/
View Report
View on Map

Access Granted: Want to get more out of your existing Shodan account? Check out everything you have acce

BEST CASINO RESORTS &#8211; Read reviews for the best casino resorts, USA

3.85.52.189
www.toprubylists.com
toprubylists.com
webmail.toprubylists.com
ec2-3-85-52-189.compute-1.amazonaws.com
Amazon Data Services NoVa
United States, Ashburn

cloud

SSL Certificate

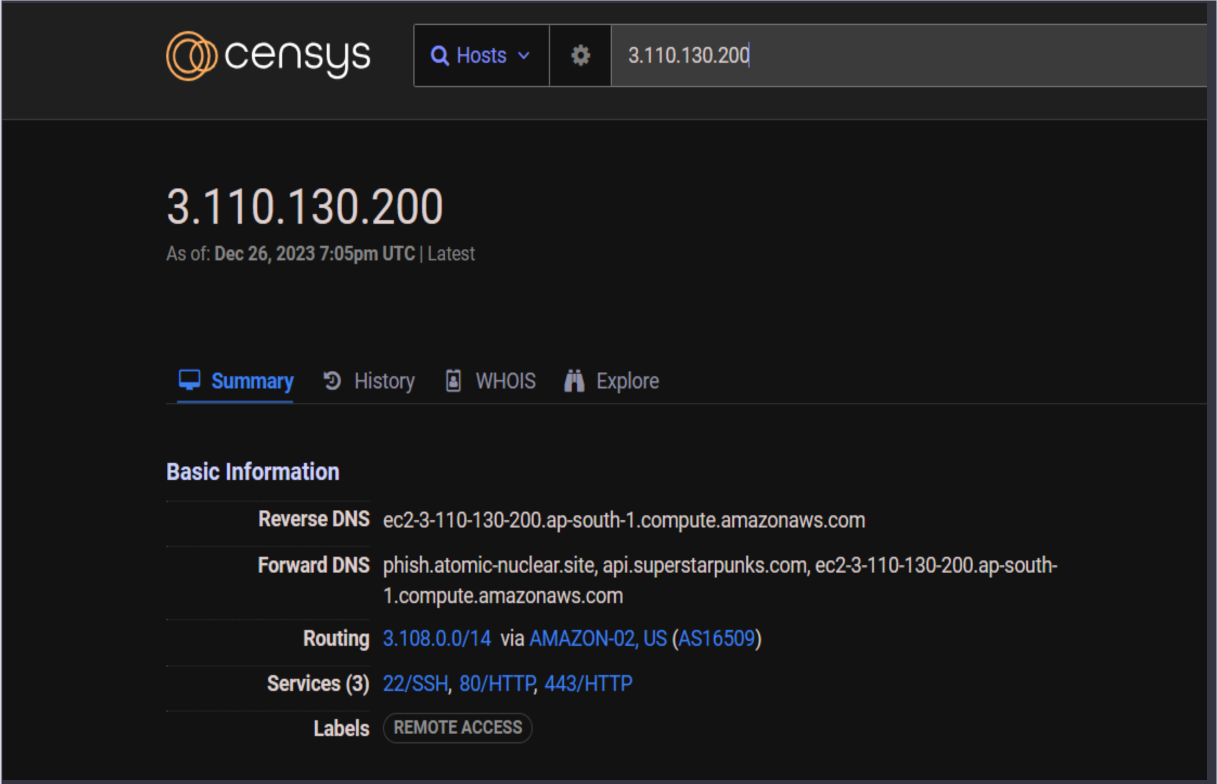
Issued By:
|- Common Name:
R3
|- Organization:
Let's Encrypt

Issued To:
|- Common Name:
toprubylists.com

Supported SSL Versions:
TLSv1.2, TLSv1.3

```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 21 Dec 2023 10:35:03 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 105058
Connection: keep-alive
X-Powered-By: PHP/8.0.30
Link: <https://toprubylists.com/wp-json/>; rel="https://api.w.org/",
```

Content Description	Notable Information	Structure Overview

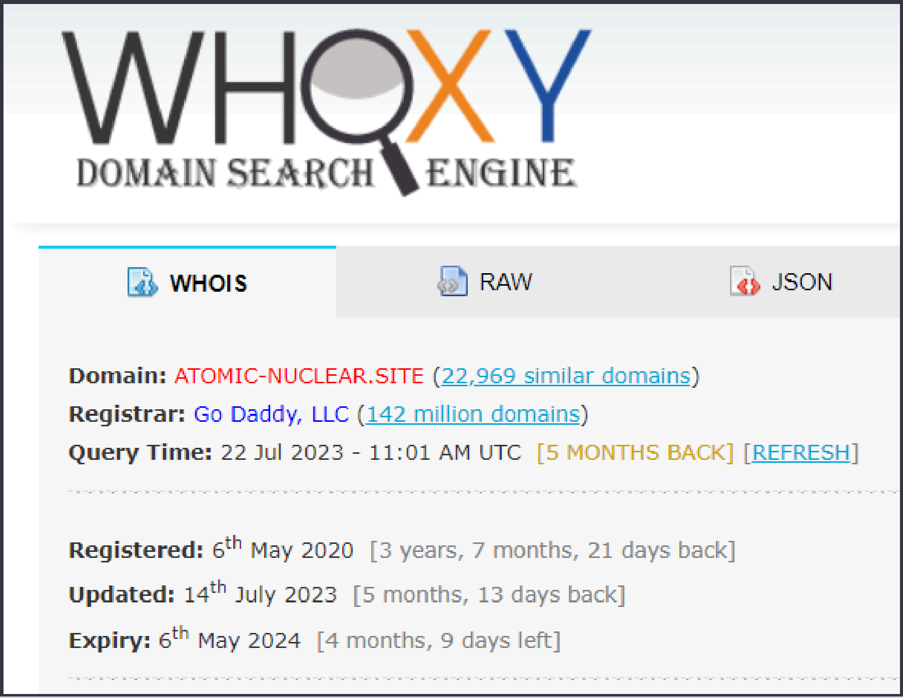


3.110.130.200

As of: Dec 26, 2023 7:05pm UTC | Latest

Basic Information

Reverse DNS	ec2-3-110-130-200.ap-south-1.compute.amazonaws.com
Forward DNS	phish.atomic-nuclear.site, api.superstarpunks.com, ec2-3-110-130-200.ap-south-1.compute.amazonaws.com
Routing	3.108.0.0/14 via AMAZON-02, US (AS16509)
Services (3)	22/SSH, 80/HTTP, 443/HTTP
Labels	REMOTE ACCESS



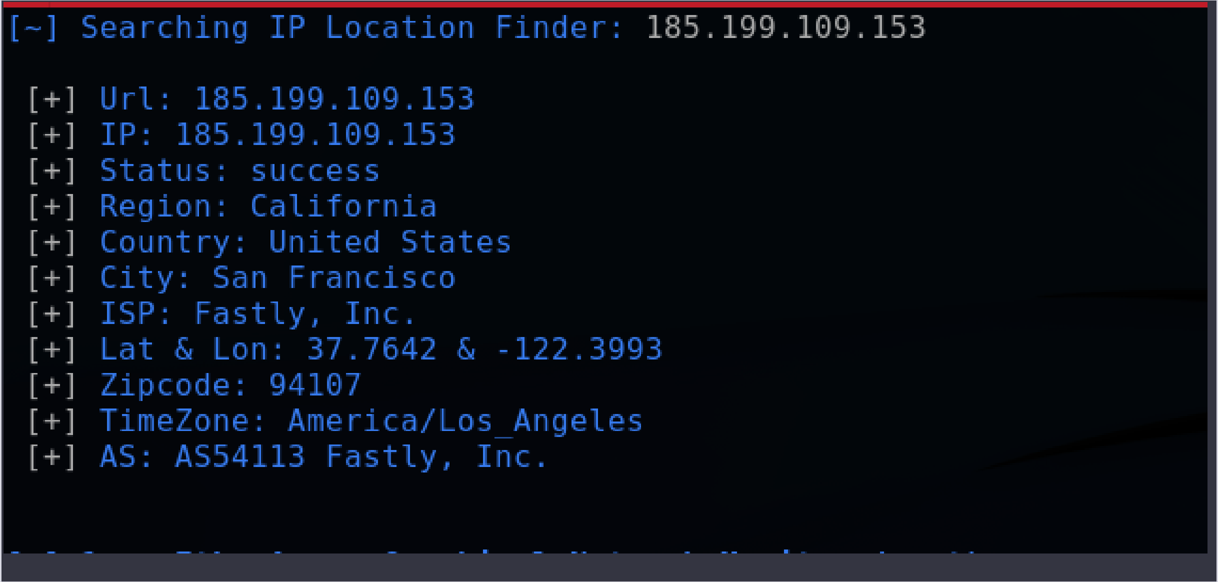
Domain: ATOMIC-NUCLEAR.SITE (22,969 similar domains)
Registrar: Go Daddy, LLC (142 million domains)
Query Time: 22 Jul 2023 - 11:01 AM UTC [5 MONTHS BACK] [REFRESH]

Registered: 6th May 2020 [3 years, 7 months, 21 days back]
Updated: 14th July 2023 [5 months, 13 days back]
Expiry: 6th May 2024 [4 months, 9 days left]

D. **IP Address Investigation**

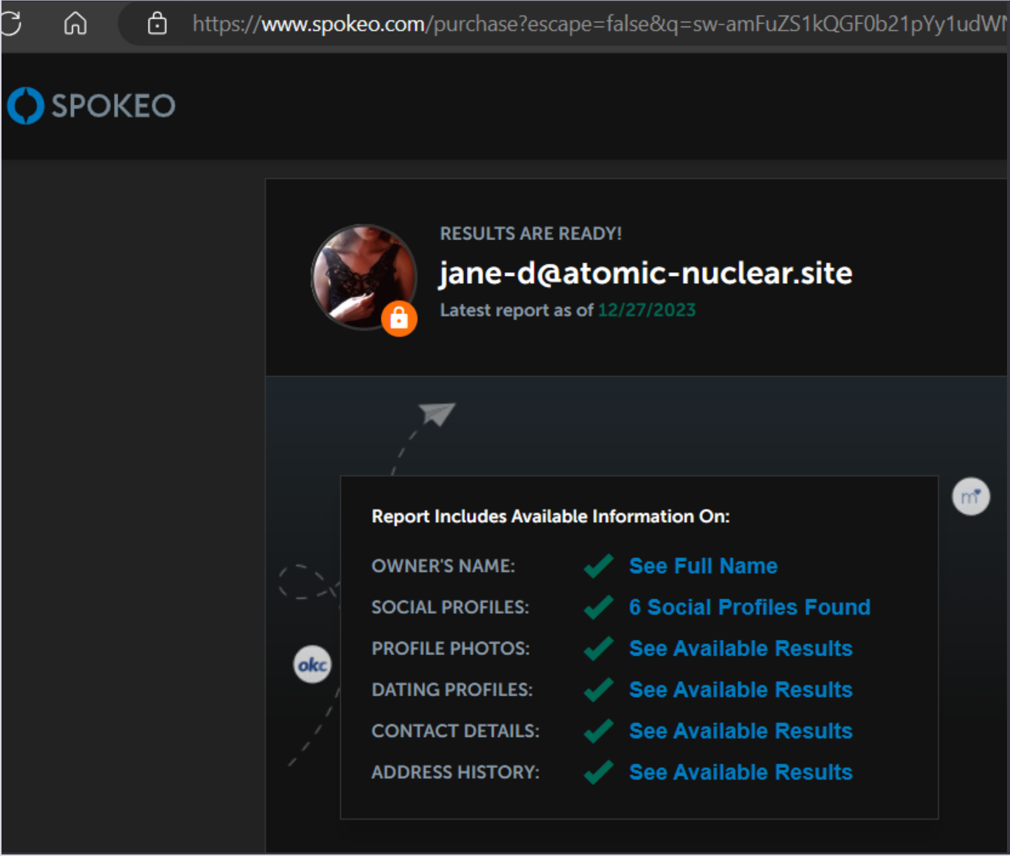
Here we have used **ghost_eye tool** for getting location from the IP address.

IP Address	Location	Associated Domains
185.199.109.153	[Location]	Atomic-nuclear.site

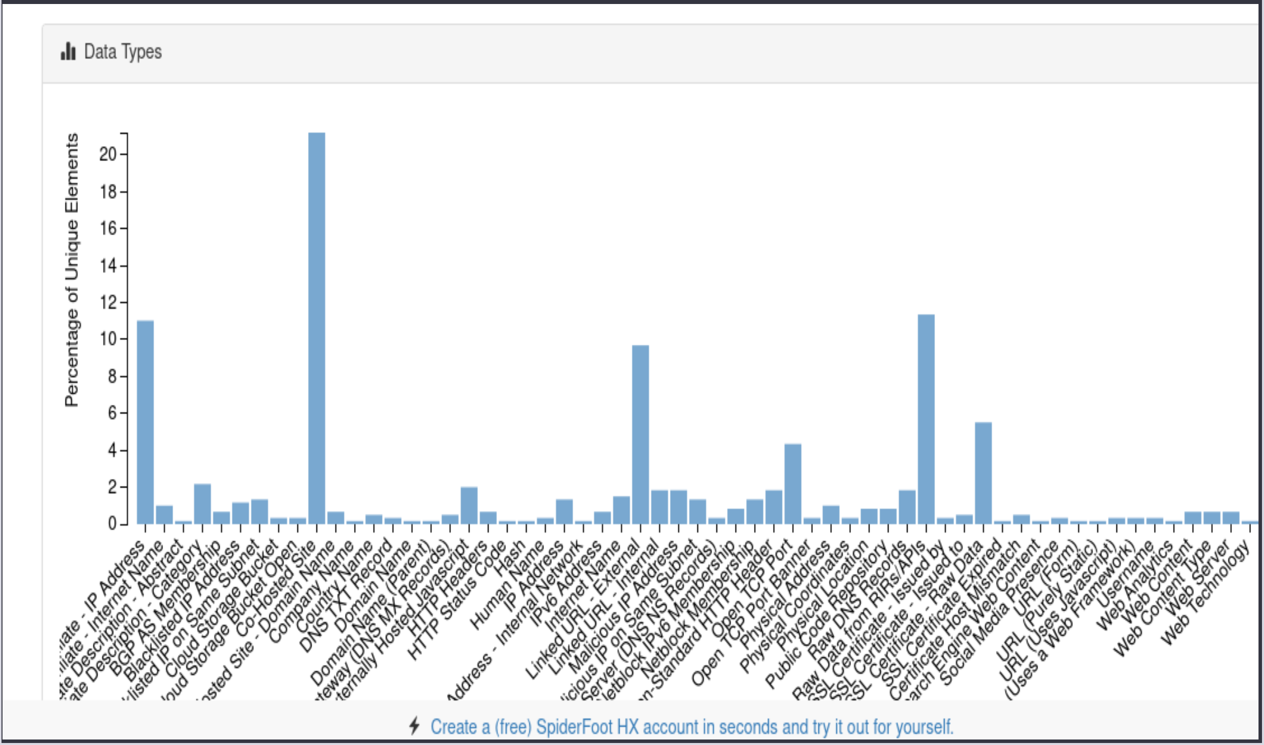


```
[~] Searching IP Location Finder: 185.199.109.153

 [+] Url: 185.199.109.153
 [+] IP: 185.199.109.153
 [+] Status: success
 [+] Region: California
 [+] Country: United States
 [+] City: San Francisco
 [+] ISP: Fastly, Inc.
 [+] Lat & Lon: 37.7642 & -122.3993
 [+] Zipcode: 94107
 [+] TimeZone: America/Los_Angeles
 [+] AS: AS54113 Fastly, Inc.
```

E. **Social Media Presence**

Social Media Platform	Profile Information	Tools used
Facebook	6 matches found	**Spokeo.com**
 https://www.spokeo.com/purchase?escape=false&q=sw-amFuZS1kQGF0b21pYy1udWI SPOKEO RESULTS ARE READY! jane-d@atomic-nuclear.site Latest report as of 12/27/2023 Report Includes Available Information On: OWNER'S NAME: ✓ See Full Name SOCIAL PROFILES: ✓ 6 Social Profiles Found PROFILE PHOTOS: ✓ See Available Results DATING PROFILES: ✓ See Available Results CONTACT DETAILS: ✓ See Available Results ADDRESS HISTORY: ✓ See Available Results		

F. Other Relevant Information using **OSINT tool spiderfoot**

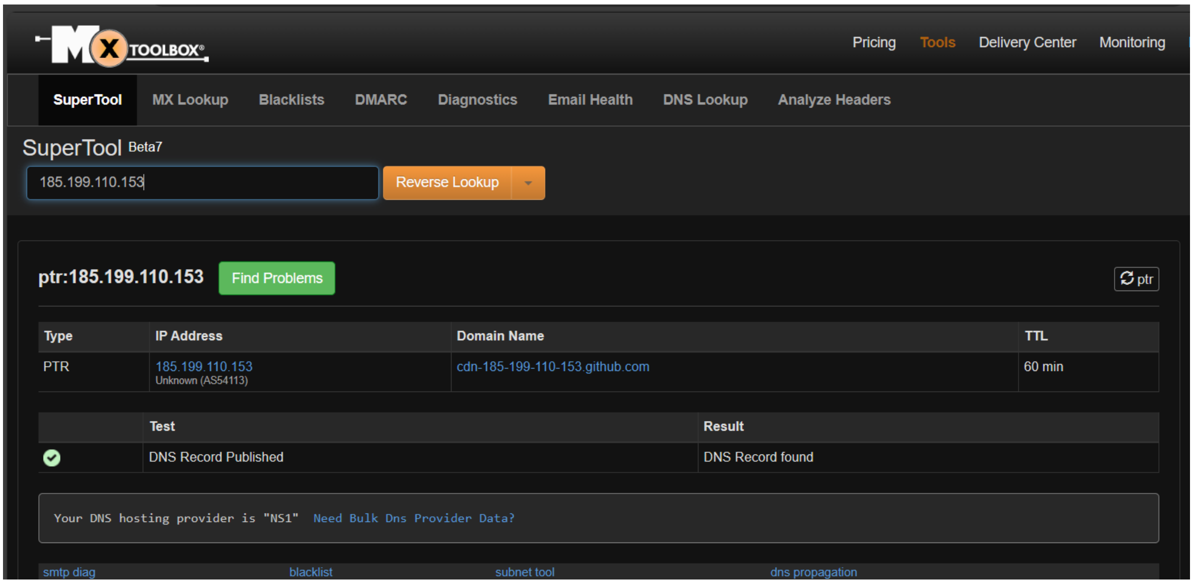
Source	Information Details
SPIDERFOOT	External, Internal account, Malicious IP, parent Domain etc.
 Data Types Percentage of Unique Elements 20 18 16 14 12 10 8 6 4 2 0 liate - IP Address iliate - Internet Name ate Description - Abstract ate Description - Category BGP AS Membership Blacklisted IP Address klisted IP on Same Subnet Cloud Storage Bucket oud Storage Bucket Open Co-Hosted Site osted Site - Domain Name Company Name Country Name DNS TXT Record Domain Name Domain Name (Parent) teway (DNS MX Records) ternally Hosted Javascript HTTP Headers HTTP Status Code Hash Human Name IP Address Address - Internal Network IPv6 Address Internet Name Linked URL - External Linked URL - Internal Malicious IP Address licious IP on Same Subnet Server (DNS NS Records) Netblock IPv6 Membership Netblock Membership n-Standard HTTP Header Open TCP Port Open TCP Port Banner Physical Address Physical Coordinates Physical Location Public Code Repository Raw DNS Records Raw Data from RIRs/APIs SSL Certificate - Issued by SSL Certificate - Issued to SSL Certificate - Raw Data SSL Certificate Expired Certificate Host Mismatch arch Engine Web Content Social Media Presence URL (Form) URL (Purely Static) URL (Uses Javascript) (Uses a Web Framework) Username Web Analytics Web Content Web Content Type Web Server Web Technology Create a (free) SpiderFoot HX account in seconds and try it out for yourself.	

G. **Analysis**

A. Patterns and Trends	Identify patterns or trends in the collected information that may be relevant to the investigation.
B. Correlations	Highlight any correlations between different pieces of information gathered.

OTHER INFORMATION FROM DIFFERENT RESOURCES

-REVERSE LOOK UP -INFO



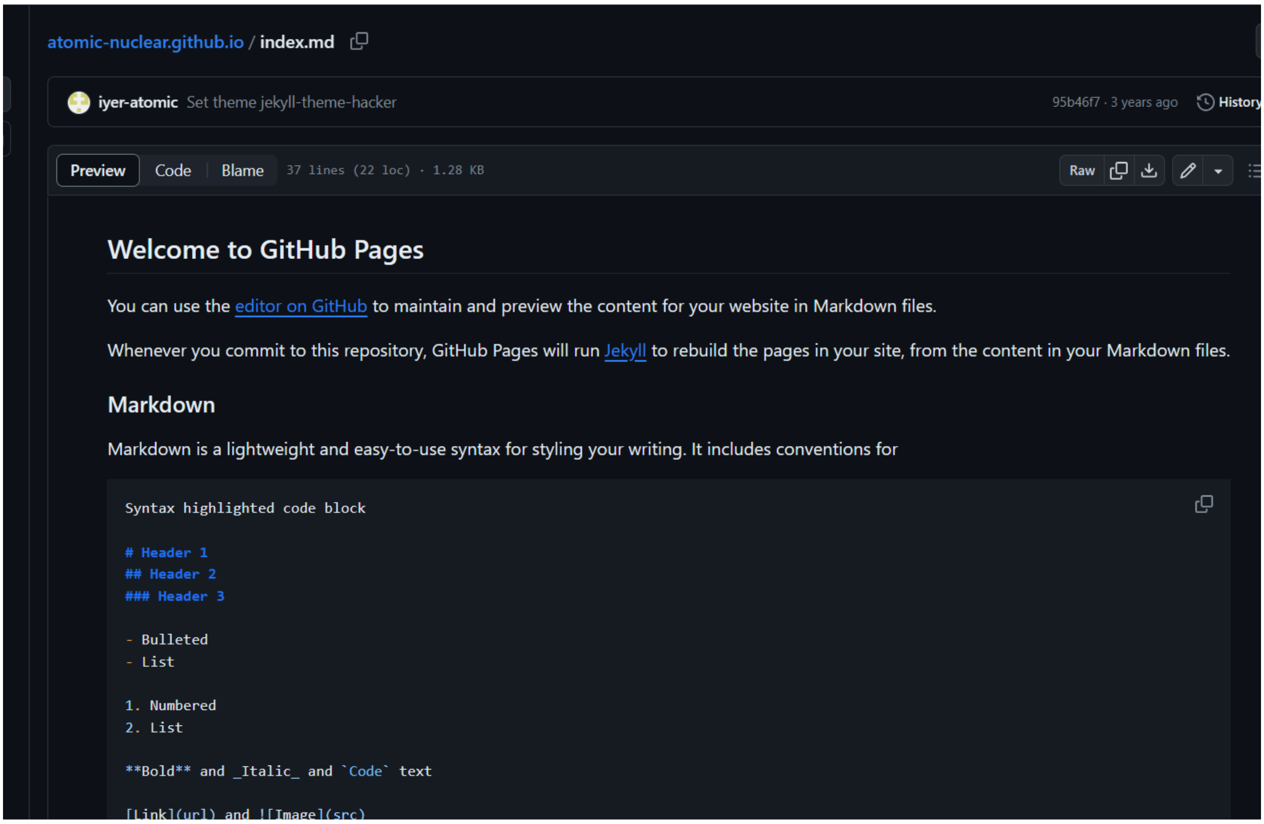
ptr:185.199.110.153

Type	IP Address	Domain Name	TTL
PTR	185.199.110.153 Unknown (AS54113)	cdn-185-199-110-153.github.com	60 min

	Test	Result
✓	DNS Record Published	DNS Record found

```
Your DNS hosting provider is "NS1"  Need Bulk Dns Provider Data?
```

-JEYLL tool used for Deployment.


atomic-nuclear.github.io / index.md
iyer-atomic Set theme jekyll-theme-hacker
95b46f7 · 3 years ago
History
Preview
Code
Blame
37 lines (22 loc) · 1.28 KB
Raw

Welcome to GitHub Pages

You can use the editor on GitHub to maintain and preview the content for your website in Markdown files.

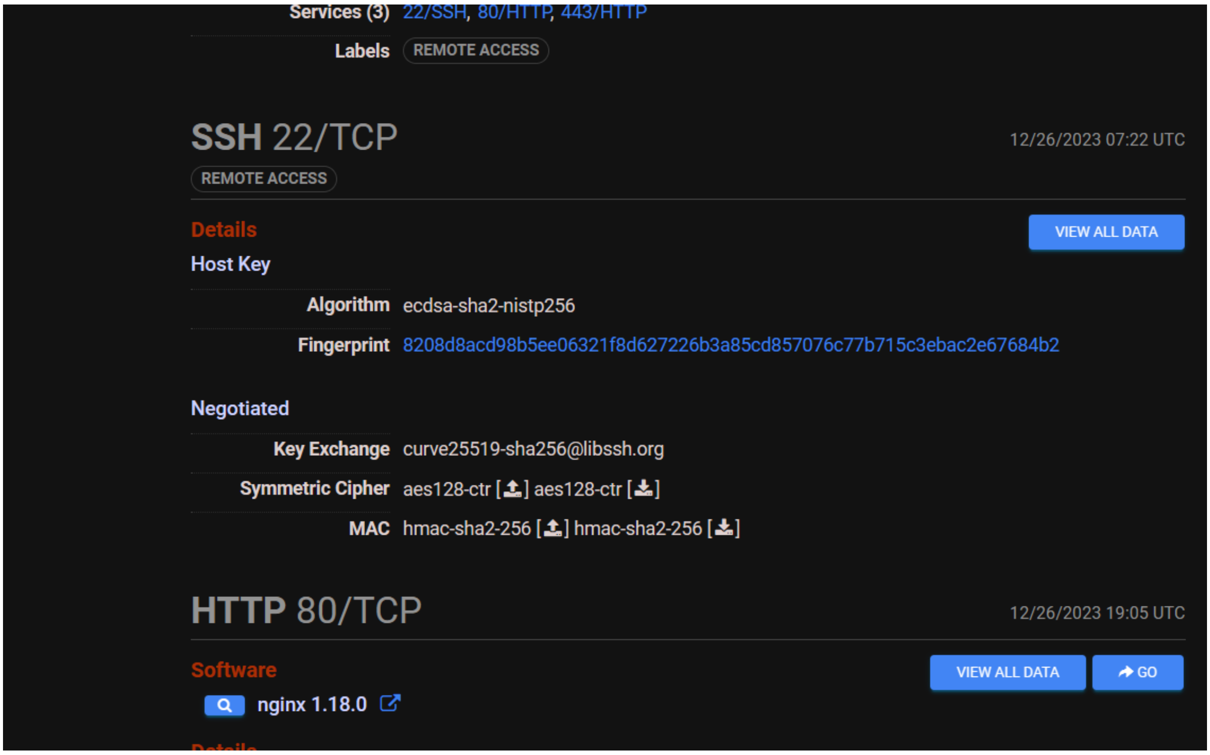
Whenever you commit to this repository, GitHub Pages will run Jekyll to rebuild the pages in your site, from the content in your Markdown files.

Markdown

Markdown is a lightweight and easy-to-use syntax for styling your writing. It includes conventions for

```
Syntax highlighted code block

# Header 1
## Header 2
### Header 3

- Bulleted
- List

1. Numbered
2. List

**Bold** and _Italic_ and `Code` text

[Link](url) and ![Image](src)
```

-**Ports Used in Communication**



Services (3) 22/SSH, 80/HTTP, 443/HTTP

Labels REMOTE ACCESS

SSH 22/TCP 12/26/2023 07:22 UTC

REMOTE ACCESS

Details

Host Key

Algorithm ecdsa-sha2-nistp256

Fingerprint 8208d8acd98b5ee06321f8d627226b3a85cd857076c77b715c3ebac2e67684b2

Negotiated

Key Exchange curve25519-sha256@libssh.org

Symmetric Cipher aes128-ctr [⬆] aes128-ctr [⬇]

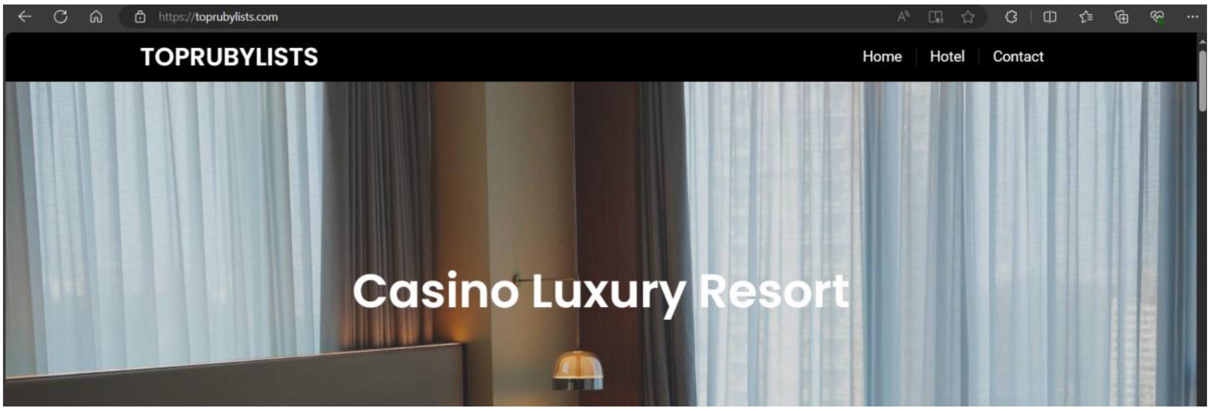
MAC hmac-sha2-256 [⬆] hmac-sha2-256 [⬇]

HTTP 80/TCP 12/26/2023 19:05 UTC

Software

nginx 1.18.0

-secretserver.atomic-nuclear.site redirects to below website(WordPress used)-



https://toprubylists.com
TOPRUBYLISTS
Home
Hotel
Contact
Casino Luxury Resort