CYBER SECURITY JULY MINOR PROECT

PROBLEM STATEMENT:

1.

Perform Foot printing on Amazon Website and gather information about website by

using online Websites (Whois / netcraft / Shodan / dnsdumpster., etc.) as much as

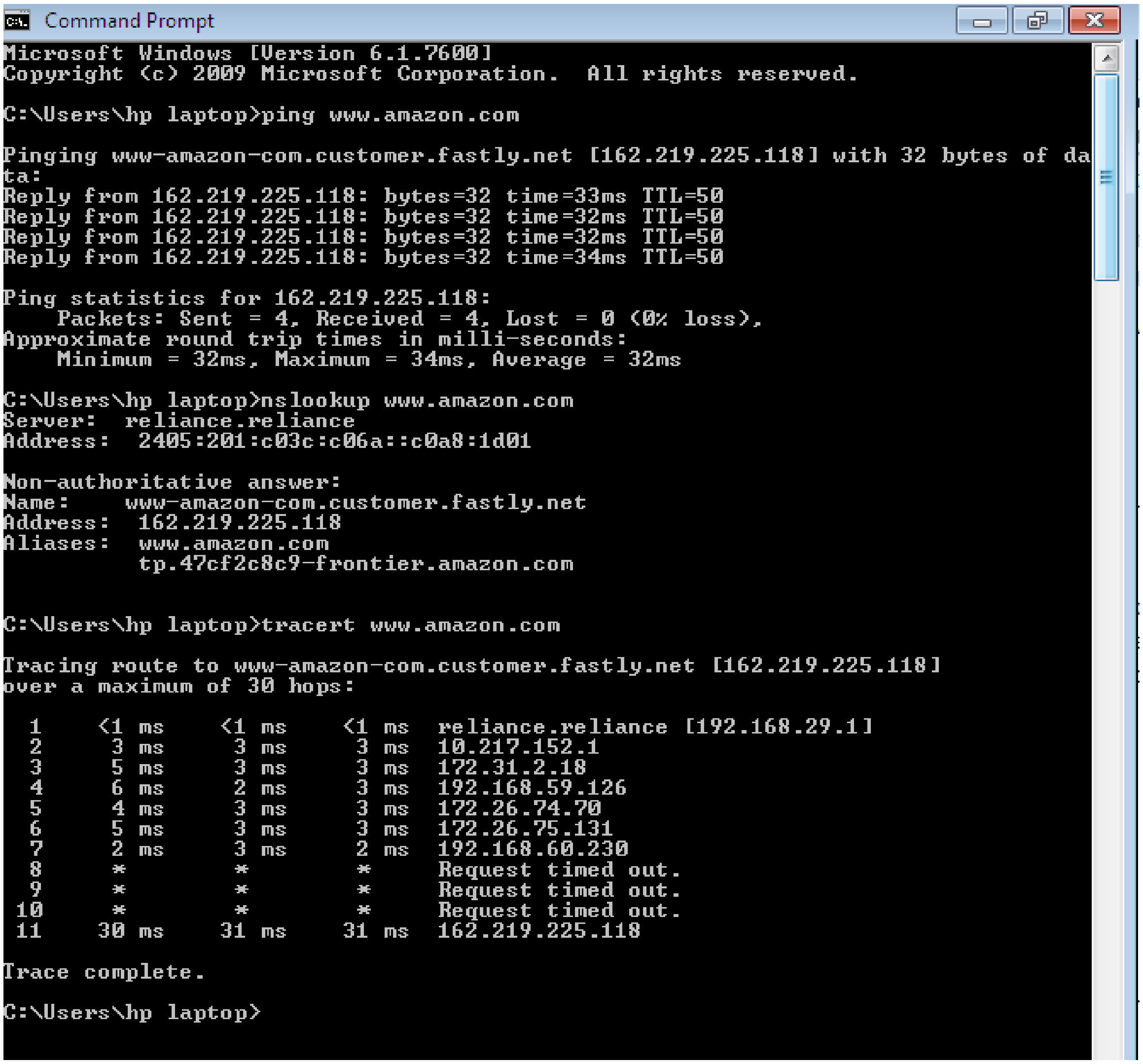
possible and write report on gathered info along with screenshots .

INTRODUCTION:

American multinational technology company which focuses on e-commerce, cloud computing, digital streaming, and artificial intelligence. It has been referred to as "one of the most influential economic and cultural forces in the world," and is one of the world's most valuable brands.

Founded	July 5, 1994; 28 years ago
Founder	Jeff Bezos
Headquarters	Seattle, Washington and Arlington, Virginia, U.S.
Area served	Worldwide

COMMAND PROMPT



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\hp laptop>ping www.amazon.com

Pinging www-amazon-com.customer.fastly.net [162.219.225.118] with 32 bytes of da
ta:
Reply from 162.219.225.118: bytes=32 time=33ms TTL=50
Reply from 162.219.225.118: bytes=32 time=32ms TTL=50
Reply from 162.219.225.118: bytes=32 time=32ms TTL=50
Reply from 162.219.225.118: bytes=32 time=34ms TTL=50

Ping statistics for 162.219.225.118:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 32ms, Maximum = 34ms, Average = 32ms

C:\Users\hp laptop>nslookup www.amazon.com
Server:  reliance.reliance
Address:  2405:201:c03c:c06a::c0a8:1d01

Non-authoritative answer:
Name:    www-amazon-com.customer.fastly.net
Address:  162.219.225.118
Aliases:  www.amazon.com
          tp.47cf2c8c9-frontier.amazon.com


C:\Users\hp laptop>tracert www.amazon.com

Tracing route to www-amazon-com.customer.fastly.net [162.219.225.118]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  reliance.reliance [192.168.29.1]
  2     3 ms     3 ms     3 ms  10.217.152.1
  3     5 ms     3 ms     3 ms  172.31.2.18
  4     6 ms     2 ms     3 ms  192.168.59.126
  5     4 ms     3 ms     3 ms  172.26.74.70
  6     5 ms     3 ms     3 ms  172.26.75.131
  7     2 ms     3 ms     2 ms  192.168.60.230
  8     *        *        *     Request timed out.
  9     *        *        *     Request timed out.
 10     *        *        *     Request timed out.
 11    30 ms    31 ms    31 ms  162.219.225.118

Trace complete.

C:\Users\hp laptop>
```

WHOIS FOOT PRINTING

Direct search using website name is giving no result so IP address is used:

IP address - 162.219.225.118

NetRange: *162.219.224.0 - 162.219.227.255*

CIDR: *162.219.224.0/22*

NetName: *AMAZO-4*

NetHandle: *NET-162-219-224-0-1*

```
Parent:           NET162 (NET-162-0-0-0-0)

NetType:          Direct Allocation

OriginAS:

Organization:     Amazon.com, Inc. (AMAZO-4)

RegDate:          2018-10-11

Updated:          2018-10-11

Ref:              https://rdap.arin.net/registry/ip/162.219.224.0


OrgName:          Amazon.com, Inc.

OrgId:            AMAZO-4

Address:          Amazon Web Services, Inc.

Address:          P.O. Box 81226

City:             Seattle

StateProv:        WA

PostalCode:       98108-1226

Country:          US

RegDate:          2005-09-29

Updated:          2021-09-30

Comment:          For details of this service please see

Comment:          http://ec2.amazonaws.com

Ref:              https://rdap.arin.net/registry/entity/AMAZO-4


OrgNOCHandle: AANO1-ARIN

OrgNOCName:       Amazon AWS Network Operations
```

OrgNOCPhone: +1-206-266-4064

OrgNOCEmail: email@amazon.com

OrgNOCRef: https://rdap.arin.net/registry/entity/AANO1-ARIN

OrgTechHandle: ANO24-ARIN

OrgTechName: Amazon EC2 Network Operations

OrgTechPhone: +1-206-266-4064

OrgTechEmail: email@amazon.com

OrgTechRef: https://rdap.arin.net/registry/entity/ANO24-ARIN

OrgAbuseHandle: AEA8-ARIN

OrgAbuseName: Amazon EC2 Abuse

OrgAbusePhone: +1-206-266-4064

OrgAbuseEmail: email@amazonaws.com

OrgAbuseRef: https://rdap.arin.net/registry/entity/AEA8-ARIN

OrgRoutingHandle: ARMP-ARIN

OrgRoutingName: AWS RPKI Management POC

OrgRoutingPhone: +1-206-266-4064

OrgRoutingEmail: email@amazon.com

OrgRoutingRef: https://rdap.arin.net/registry/entity/ARMP-ARIN

OrgRoutingHandle: IPROU3-ARIN

OrgRoutingName: IP Routing

OrgRoutingPhone: +1-206-266-4064

OrgRoutingEmail: email@amazon.com

OrgRoutingRef: https://rdap.arin.net/registry/entity/IPROU3-ARIN

IP address: 162.219.225.110

NetRange: 162.219.224.0 - 162.219.227.255

CIDR: 162.219.224.0/22

NetName: AMAZO-4

NetHandle: NET-162-219-224-0-1

Parent: NET162 (NET-162-0-0-0-0)

NetType: Direct Allocation

OriginAS:

Organization: Amazon.com, Inc. (AMAZO-4)

RegDate: 2018-10-11

Updated: 2018-10-11

Ref: https://rdap.arin.net/registry/ip/162.219.224.0

OrgName: Amazon.com, Inc.

OrgId: AMAZO-4

Address: Amazon Web Services, Inc.

Address: P.O. Box 81226

City: Seattle

StateProv: WA

PostalCode: 98108-1226

```
Country:            US
RegDate:            2005-09-29
Updated:            2021-09-30
Comment:            For details of this service please see
Comment:            http://ec2.amazonaws.com
Ref:                https://rdap.arin.net/registry/entity/AMAZO-4

OrgTechHandle: ANO24-ARIN
OrgTechName:    Amazon EC2 Network Operations
OrgTechPhone:   +1-206-266-4064
OrgTechEmail:   email@amazon.com
OrgTechRef:     https://rdap.arin.net/registry/entity/ANO24-ARIN

OrgRoutingHandle: ARMP-ARIN
OrgRoutingName:    AWS RPKI Management POC
OrgRoutingPhone:   +1-206-266-4064
OrgRoutingEmail:   email@amazon.com
OrgRoutingRef:     https://rdap.arin.net/registry/entity/ARMP-ARIN

OrgRoutingHandle: IPROU3-ARIN
OrgRoutingName:    IP Routing
OrgRoutingPhone:   +1-206-266-4064
OrgRoutingEmail:   email@amazon.com
OrgRoutingRef:     https://rdap.arin.net/registry/entity/IPROU3-ARIN
```

OrgAbuseHandle: AEA8-ARIN

OrgAbuseName: Amazon EC2 Abuse

OrgAbusePhone: +1-206-266-4064

OrgAbuseEmail: email@amazonaws.com

OrgAbuseRef: https://rdap.arin.net/registry/entity/AEA8-ARIN

OrgNOCHandle: AANO1-ARIN

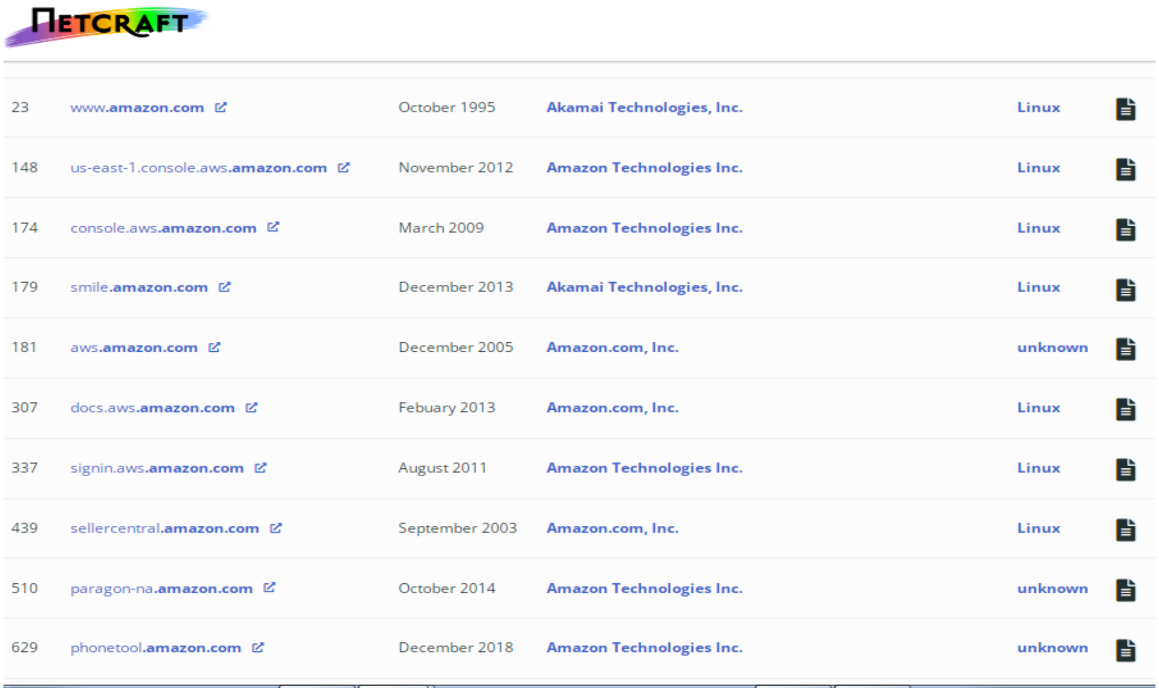
OrgNOCName: Amazon AWS Network Operations

OrgNOCPhone: +1-206-266-4064

OrgNOCEmail: email@amazon.com

OrgNOCRef: https://rdap.arin.net/registry/entity/AANO1-ARIN

NETCRAFT FOOT PRINTING



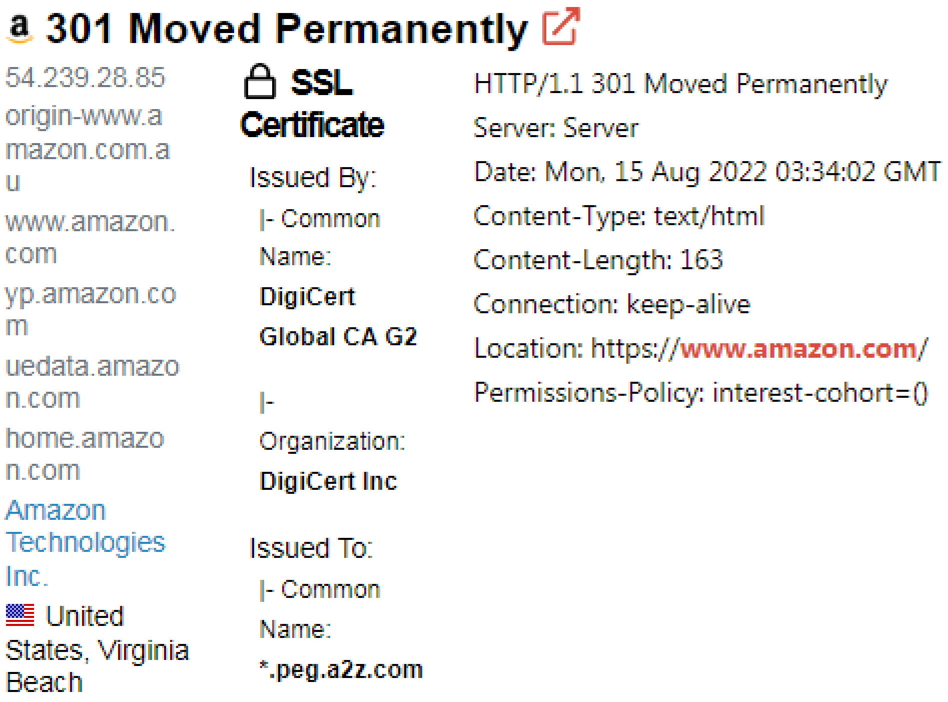
23	www.amazon.com	October 1995	Akamai Technologies, Inc.	Linux
148	us-east-1.console.aws.amazon.com	November 2012	Amazon Technologies Inc.	Linux
174	console.aws.amazon.com	March 2009	Amazon Technologies Inc.	Linux
179	smile.amazon.com	December 2013	Akamai Technologies, Inc.	Linux
181	aws.amazon.com	December 2005	Amazon.com, Inc.	unknown
307	docs.aws.amazon.com	Febuary 2013	Amazon.com, Inc.	Linux
337	signin.aws.amazon.com	August 2011	Amazon Technologies Inc.	Linux
439	sellercentral.amazon.com	September 2003	Amazon.com, Inc.	Linux
510	paragon-na.amazon.com	October 2014	Amazon Technologies Inc.	unknown
629	phonetool.amazon.com	December 2018	Amazon Technologies Inc.	unknown

Site report containing all the background, HTML, IP information:

----

https://sitereport.netcraft.com/?url=http://www.amazon.com

SHODAN FOOT PRINTING



301 Moved Permanently

54.239.28.85

origin-www.amazon.com.au

www.amazon.com

yp.amazon.com

uedata.amazon.com

home.amazon.com

Amazon Technologies Inc.

🇺🇸 United States, Virginia Beach

SSL Certificate

Issued By:

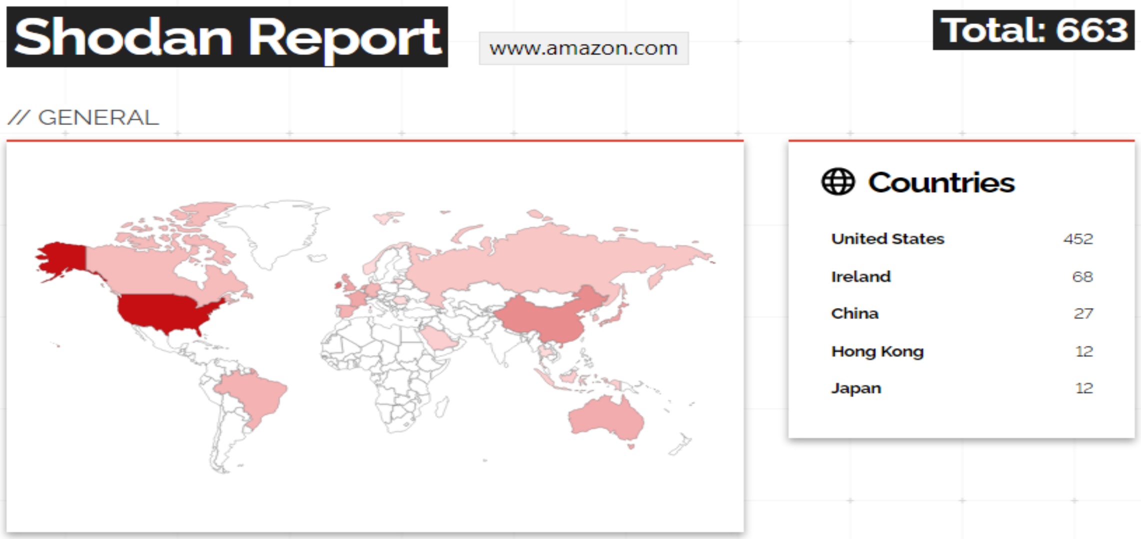
|- Common Name: **DigiCert Global CA G2**

|- Organization: **DigiCert Inc**

Issued To:

|- Common Name: ***.peg.a2z.com**

```
HTTP/1.1 301 Moved Permanently
Server: Server
Date: Mon, 15 Aug 2022 03:34:02 GMT
Content-Type: text/html
Content-Length: 163
Connection: keep-alive
Location: https://www.amazon.com/
Permissions-Policy: interest-cohort=()
```

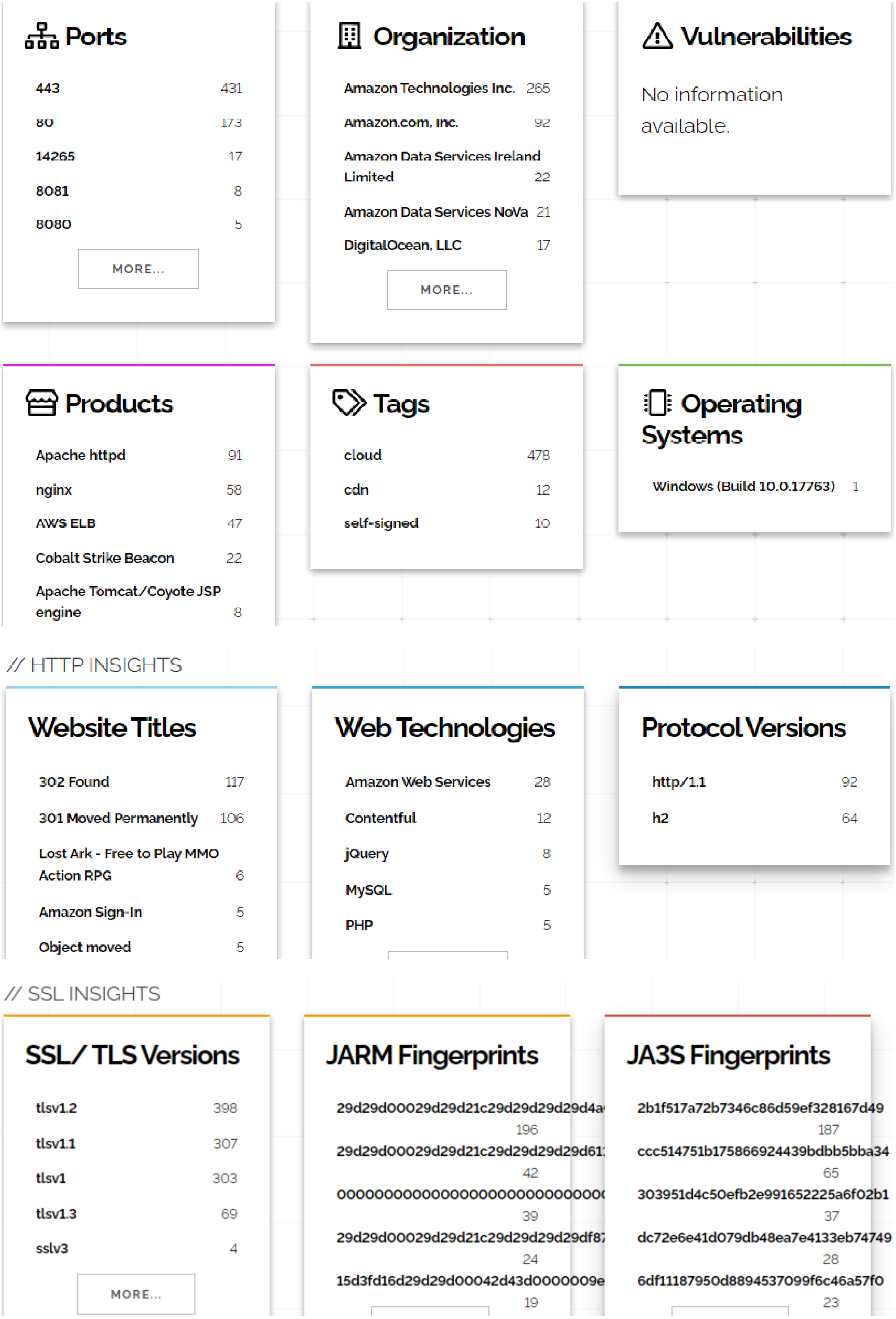


Shodan Report www.amazon.com **Total: 663**

// GENERAL

Countries

United States	452
Ireland	68
China	27
Hong Kong	12
Japan	12



Ports

443	431
80	173
14265	17
8081	8
8080	5

Organization

Amazon Technologies Inc.	265
Amazon.com, Inc.	92
Amazon Data Services Ireland Limited	22
Amazon Data Services NoVa	21
DigitalOcean, LLC	17

Vulnerabilities

No information available.

Products

Apache httpd	91
nginx	58
AWS ELB	47
Cobalt Strike Beacon	22
Apache Tomcat/Coyote JSP engine	8

Tags

cloud	478
cdn	12
self-signed	10

Operating Systems

Windows (Build 10.0.17763)	1

// HTTP INSIGHTS

Website Titles

302 Found	117
301 Moved Permanently	106
Lost Ark - Free to Play MMO Action RPG	6
Amazon Sign-In	5
Object moved	5

Web Technologies

Amazon Web Services	28
Contentful	12
jQuery	8
MySQL	5
PHP	5

Protocol Versions

http/1.1	92
h2	64

// SSL INSIGHTS

SSL/TLS Versions

tlsv1.2	398
tlsv1.1	307
tlsv1	303
tlsv1.3	69
sslv3	4

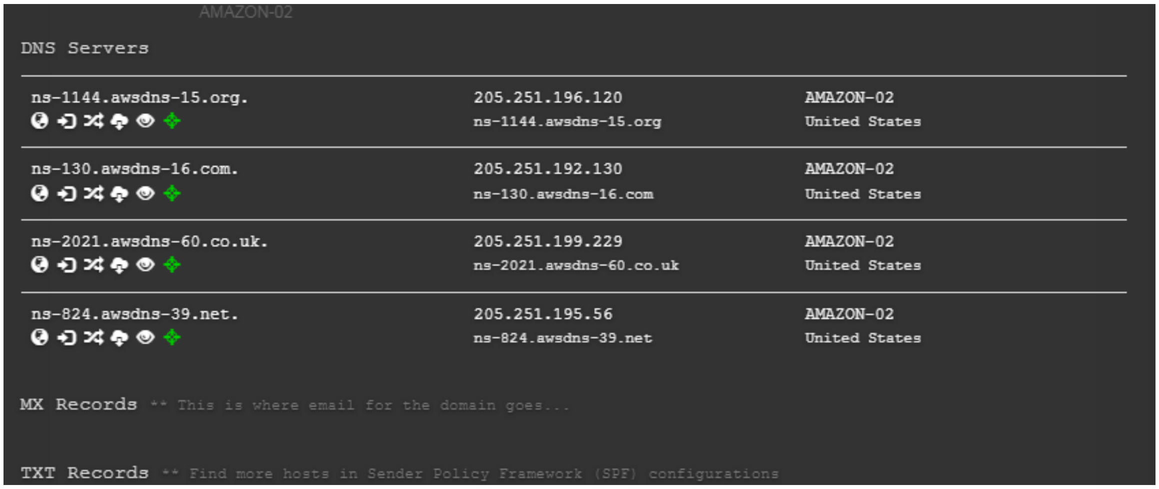
JARM Fingerprints

29d29d00029d29d21c29d29d29d4a	196
29d29d00029d29d21c29d29d29d61	42
00000000000000000000000000000	39
29d29d00029d29d21c29d29d29df87	24
15d3fd16d29d29d00042d43d0000009e	19

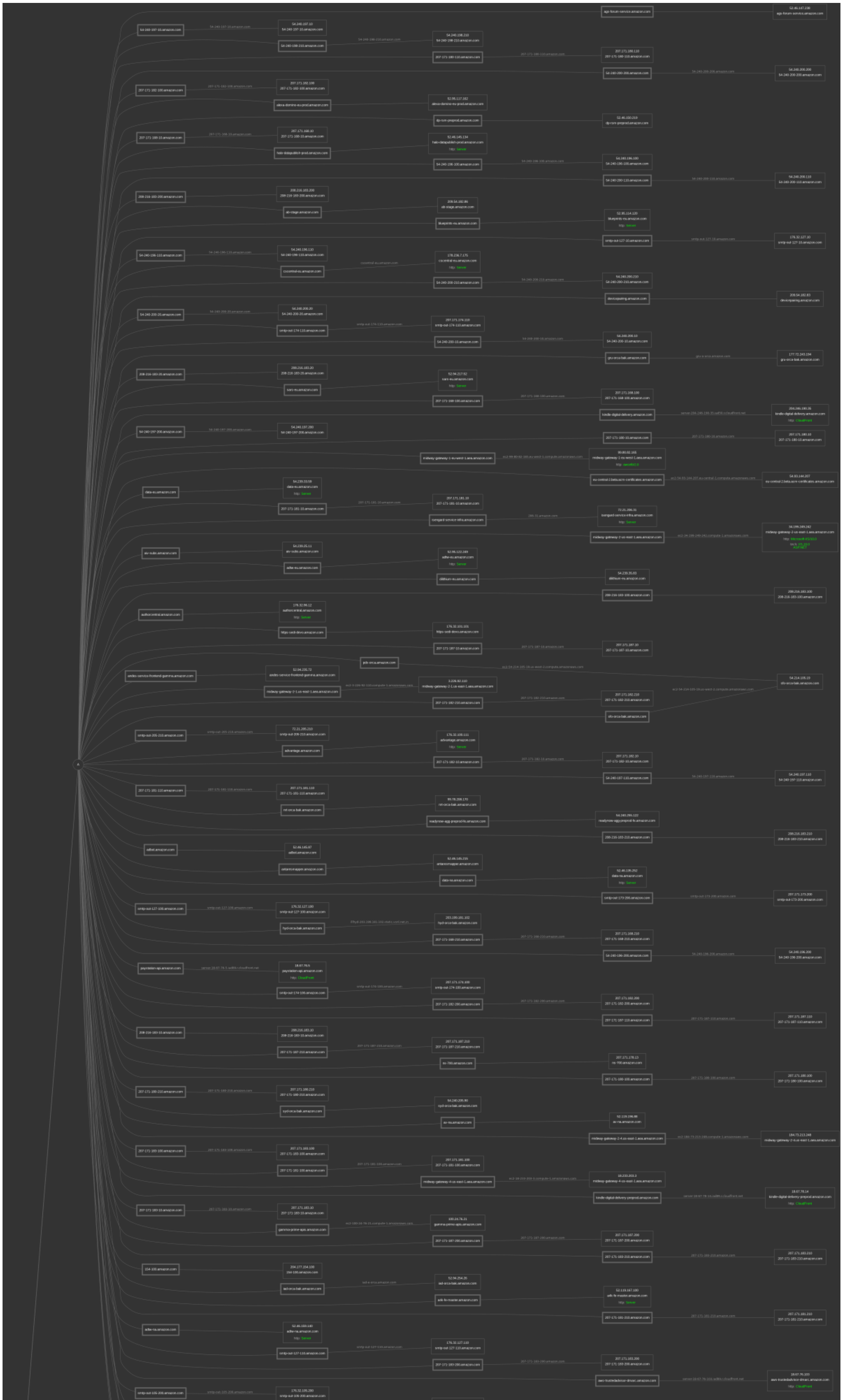
JA3S Fingerprints

2b1f517a72b7346c86d59ef328167d49	187
ccc514751b175866924439bdbb5bba34	65
303951d4c50efb2e991652225a6f02b1	37
dc72e6e41d079db48ea7e4133eb74749	28
6df11187950d8894537099f6c46a57f0	23

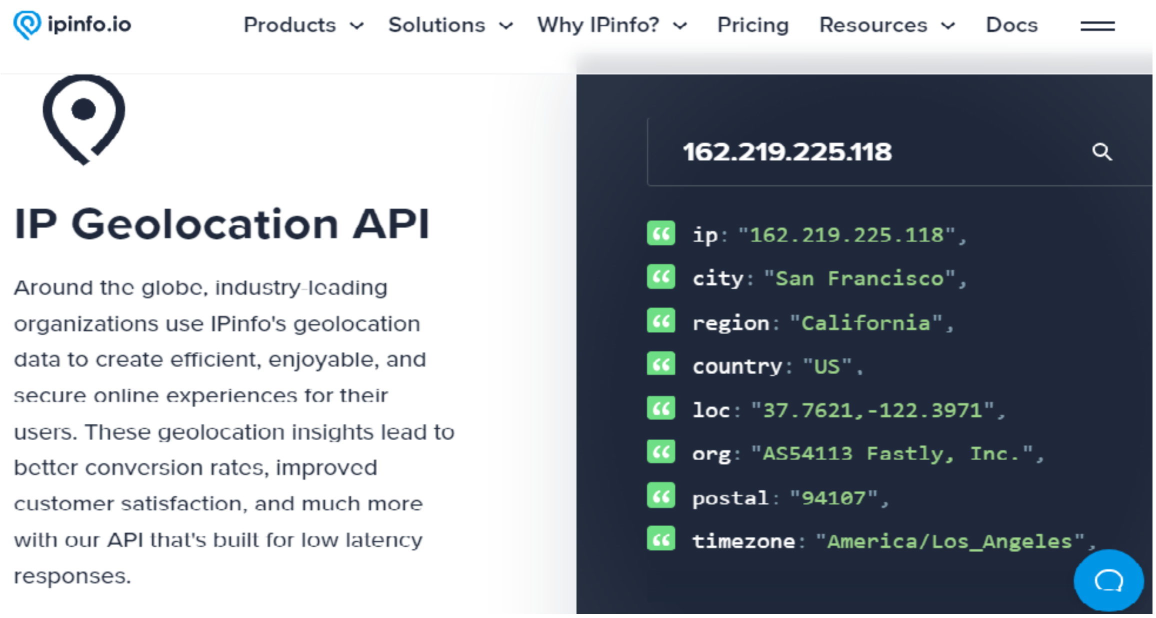
DNSDUMPSTER FOOT PRINTING



```
                AMAZON-02

DNS Servers
--------------------------------------------------------------------------------
 ns-1144.awsdns-15.org.           205.251.196.120          AMAZON-02
                                  ns-1144.awsdns-15.org    United States
--------------------------------------------------------------------------------
 ns-130.awsdns-16.com.            205.251.192.130          AMAZON-02
                                  ns-130.awsdns-16.com     United States
--------------------------------------------------------------------------------
 ns-2021.awsdns-60.co.uk.         205.251.199.229          AMAZON-02
                                  ns-2021.awsdns-60.co.uk  United States
--------------------------------------------------------------------------------
 ns-824.awsdns-39.net.            205.251.195.56           AMAZON-02
                                  ns-824.awsdns-39.net     United States

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

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


54-240-197-10.amazon.com
54-240-197-10.amazon.com
54.240.197.10
54-240-197-10.amazon.com
54-240-198-210.amazon.com
54-240-198-210.amazon.com
54.240.198.210
54-240-198-210.amazon.com
207-171-180-110.amazon.com
207-171-182-100.amazon.com
207-171-182-100.amazon.com
207.171.182.100
207-171-182-100.amazon.com
alexa-domino-eu-prod.amazon.com
52.95.117.162
alexa-domino-eu-prod.amazon.com
dp-rsm-preprod.amazon.com
207-171-168-10.amazon.com
207-171-168-10.amazon.com
207.171.168.10
207-171-168-10.amazon.com
halo-datapublish-prod.amazon.com
52.46.145.134
halo-datapublish-prod.amazon.com
http: Server
54-240-196-100.amazon.com
208-216-183-200.amazon.com
208.216.183.200
208-216-183-200.amazon.com
ab-stage.amazon.com
209.54.182.86
ab-stage.amazon.com
blueprints-eu.amazon.com
54-240-196-110.amazon.com
54-240-196-110.amazon.com
54.240.196.110
54-240-196-110.amazon.com
cscentral-eu.amazon.com
cscentral-eu.amazon.com
178.236.7.175
cscentral-eu.amazon.com
http: Server
54-240-200-210.amazon.com

IPINFO FOOT PRINTING



IP Geolocation API

Around the globe, industry-leading organizations use IPinfo's geolocation data to create efficient, enjoyable, and secure online experiences for their users. These geolocation insights lead to better conversion rates, improved customer satisfaction, and much more with our API that's built for low latency responses.

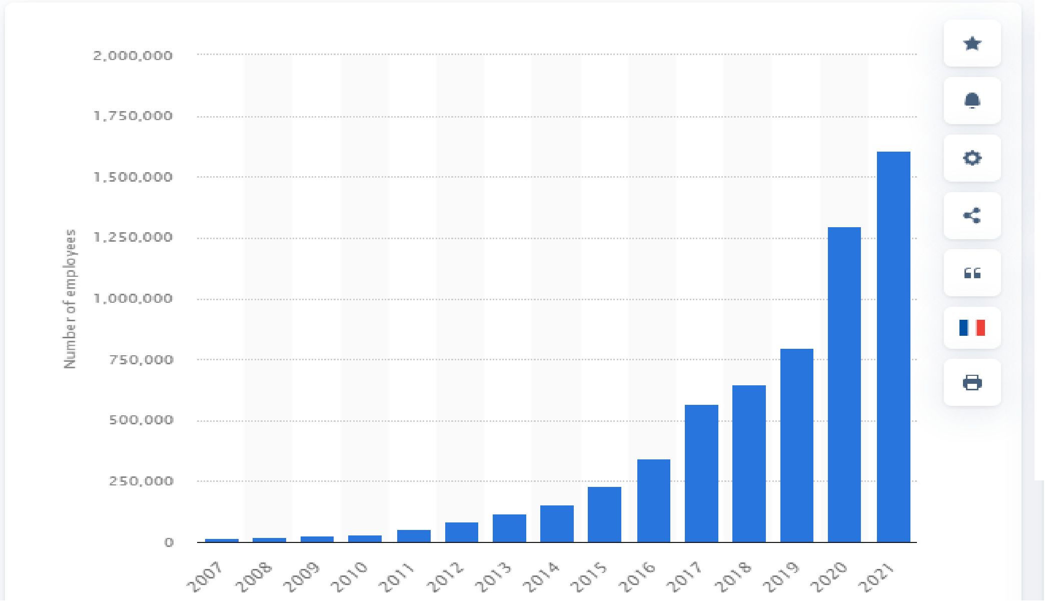
162.219.225.118

```
ip: "162.219.225.118",
city: "San Francisco",
region: "California",
country: "US",
loc: "37.7621,-122.3971",
org: "AS54113 Fastly, Inc.",
postal: "94107",
timezone: "America/Los_Angeles",
```

So far using different sites information regarding network,system has been collected.

->Amazon employee report

Number of Amazon.com employees from 2007 to 2021

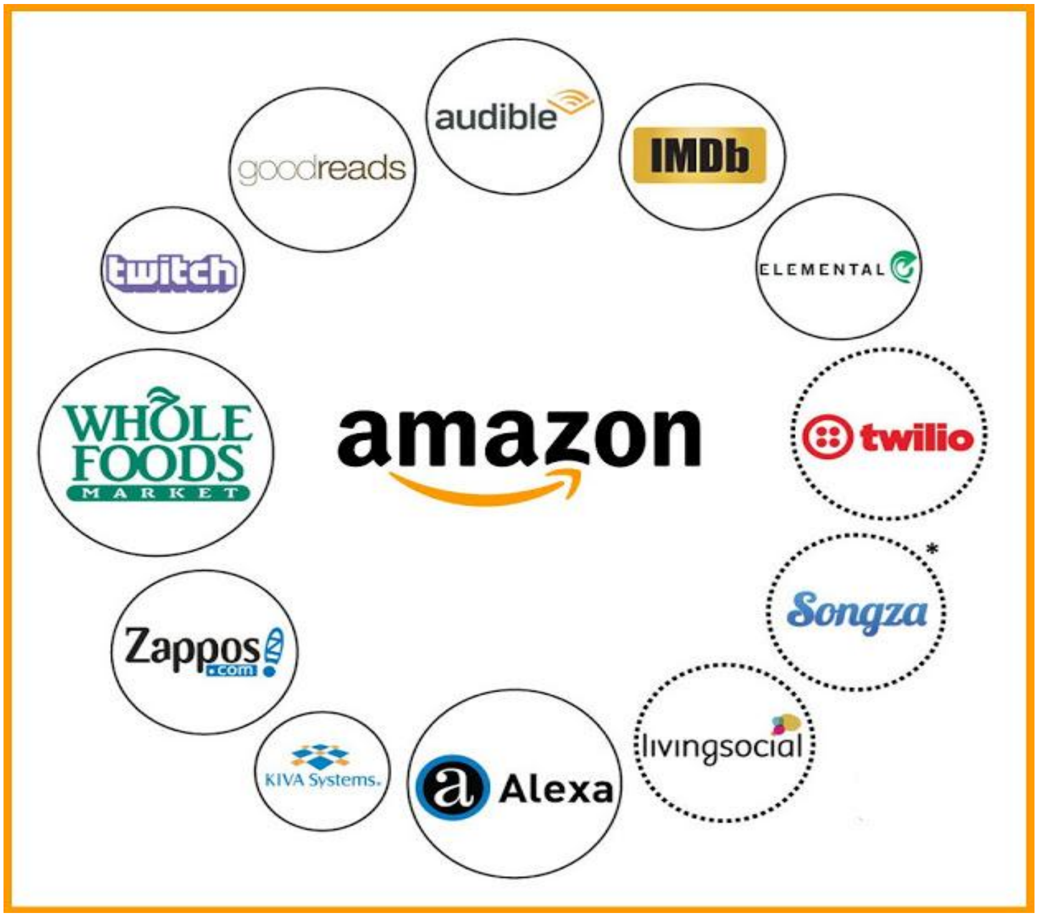


The combined number of full- and part-time employees of Amazon.com has increased significantly between 2007 and 2021. In 2021, the American multinational e-commerce company, headquartered in Seattle, Washington, employed 1,608,000 full- and part-time employees. Every year, Amazon hires additional staff during the holiday season, because of the higher amounts of incoming orders. In the 2021 holiday season, roughly 125,000 workers were employed in the United States.

Link containing the info about key directors and officers of the company:

https://ir.aboutamazon.com/officers-and-directors/default.aspx

Business subsidaries



ATTACKS POSSIBLE ON A WEBSITE

-Bots

-DDoS Attacks

-SQL Injections and Cross-site Scripting

-Malware Attacks

How to fight these common attacks?

The last thing one want to deal with while trying to run and build a small business is a data breach or a cyber attack. Not only do they harm a business operations, but they can also leave that reputation permanently damaged, turning away customers in droves.

Fortunately, one can ward off these common attacks with the right layer of protection. With Sectigo's SiteLock Basic Website Security Plan, the site and its configuration will be scanned automatically every day for critical security issues and vulnerabilities that leave one open for attack. There are also advanced plans offering web application firewall, database protection, CMS patching, and more.

Having this layer of protection in place - regularly updated with the latest anti-hacking software - allows one to have the peace of mind knowing that you and your customers can operate business safely and privately online.

Other safety precautions:

FOR INDIVIDUAL

1. Delete or De-activate old accounts

Once your account is assigned online, it can be shared anywhere with your full name, email address, pictures, location, and other information. Official email accounts provided to the employees are also available online. Once the employee has left the organization, the email account must be deleted to avoid fraudulent transactions using the same.

2. Unsubscribe from unwanted mails

All of us keep subscribing to newsletters, events registrations, offers and to many other mail lists. While some of these lists may be useful, most of them result in unnecessary clutter in our mailbox. Unsubscribe to all unnecessary emails so that you can reduce your digital footprinting on the internet.

3. Use stealth mode

There are many browsers which help you to surf with privacy. This is how you can search online with ease and avoid websites from tracking your interests, location, etc. Using browsers like TOR, Duck Duck Go with some advance settings in your regular browser can restrict the sharing of your information online.

4. Use a VPN

There are many VPNs, or Virtual Private Networks, available that you can use for privacy. A VPN provides you with an extra layer of security to protect your privacy over the internet. This will prevent others from tracking your web activity and being able to collect data by watching your surfing patterns.

5. SEO

Prevent search engines from crawling through your cached webpages and user anonymous registration details, and minimize unwanted footprints.

6. Configure Web servers

Configure your web servers to avoid information leakage and block all unwanted protocols to prevent any unethical external scans. Use TCP/IP and IPSec Protocols. Always maintain a separation between the internal and external DNS.

7. Do it yourself

Perform footprinting techniques as we have discussed above and do a check to see whether any sensitive or unwanted information of yours is available on the internet. Use the OSINT framework to delve deeper, and remove posted/ shared data that reveals any kind of sensitive information which can be a potential threat. Share tips and tricks to avoid fraud calls and social engineering.

FOR WEBSITES OR A COMPANY

1. Restrict the employees to access social networking sites from organization's network.

2. Configure web servers to avoid information leakage.

3. Educate employees to use pseudonyms on blogs, groups, and forums.

4. Do not reveal critical information in press releases, annual reports, product catalogues, etc.

5. Limit the amount of information that you are publishing on the website/Internet.

6. Use footprinting techniques to discover and remove any sensitive information publicly available.

7. Prevent search engines from caching a web page and use anonymous registration services.

8. Enforce security policies to regulate the information that employees can reveal to third parties.

9. Set apart internal and external DNS or use split DNS, and restrict zone transfer to authorized servers.

10. Disable directory listings in the web servers.

11. Educate employees about various social engineering tricks and risks.

12. Opt for privacy services on Whois Lookup database.

13. Avoid domain-level cross-linking for the critical assets.

14. Encrypt and password protect sensitive information.

____