Smartknower Minor Project

Project Name: Cyber Security March Minor Project

Problem Statement: Perform Foot printing on Microsoft 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

Information gathered from different websites on www.microsoft.com:

Foot printing MICROSOFT :

----------x---------x----------

From Whois.domaintools.com :

Domain Name: microsoft.com

Registrant Org Microsoft Corporation

Registrant Country us

Registrar MarkMonitor, Inc. MarkMonitor Inc.

IANA ID: 292

URL: http://www.markmonitor.com

Dates 11,313 days old

Created on 1991-05-01

Expires on 2023-05-02

Updated on 2022-04-18

Name Servers NS1-39.AZURE-DNS.COM (has 399,861 domains)

NS2-39.AZURE-DNS.NET (has 276 domains)

NS3-39.AZURE-DNS.ORG (has 230 domains)

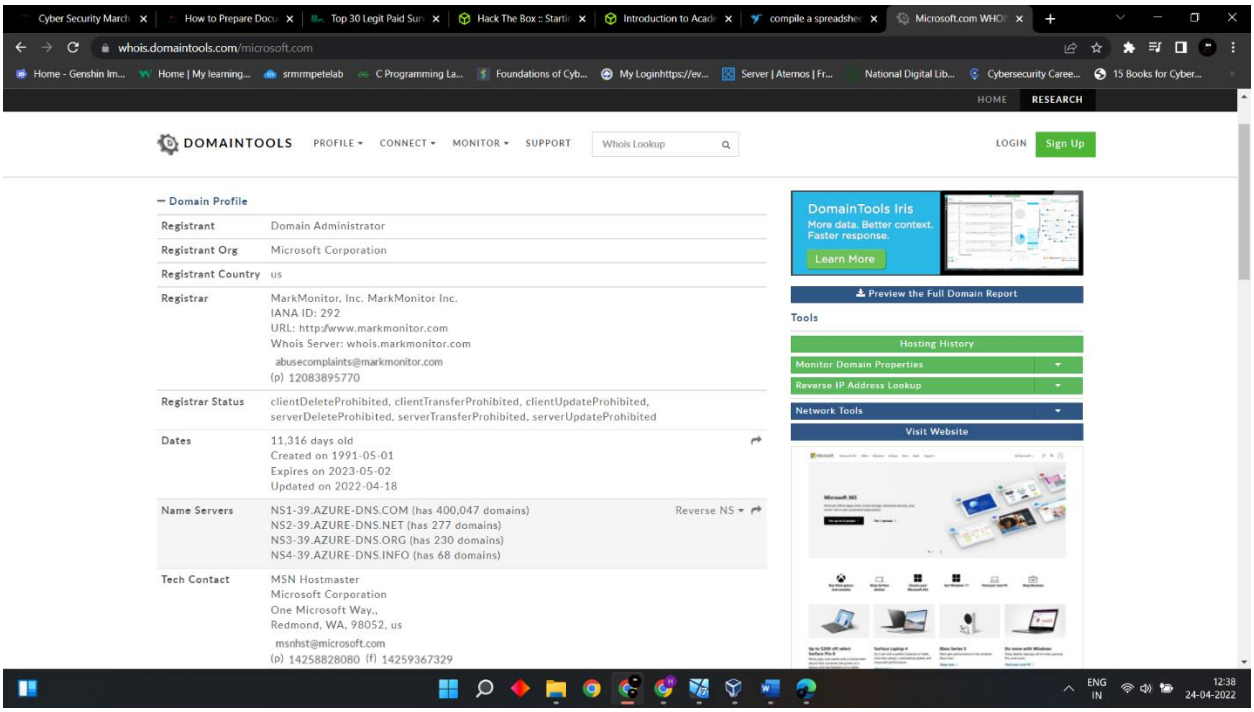
NS4-39.AZURE-DNS.INFO (has 67 domains)

IP Address 104.97.41.163 - 16 other sites hosted on this server

Reverse IP

IP Location United States - Washington - Seattle - Akamai Technologies Inc

IP History 259 changes on 259 unique IP addresses over 18 years



whois.domaintools.com/microsoft.com

DOMAINTOOLS PROFILE CONNECT MONITOR SUPPORT Whois Lookup LOGIN Sign Up

```
Registry Domain ID: 2724960_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2022-04-18T19:25:49+0000
Creation Date: 1991-05-02T04:00:00+0000
Registrar Registration Expiration Date: 2023-05-03T00:00:00+0000
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895770
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: Microsoft Corporation
Registrant Street: One Microsoft Way,
Registrant City: Redmond
Registrant State/Province: WA
Registrant Postal Code: 98052
Registrant Country: US
Registrant Phone: +1.4258828080
Registrant Phone Ext:
Registrant Fax: +1.4259367329
Registrant Fax Ext:
Registrant Email: admin@domains.microsoft
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: Microsoft Corporation
Admin Street: One Microsoft Way,
Admin City: Redmond
Admin State/Province: WA
Admin Postal Code: 98052
Admin Country: US
Admin Phone: +1.4258828080
Admin Phone Ext:
Admin Fax: +1.4259367329
```

ENG IN 12:38 24-04-2022

whois.domaintools.com/microsoft.com

DOMAINTOOLS PROFILE CONNECT MONITOR SUPPORT Whois Lookup LOGIN Sign Up

```
Admin Fax: +1.4259367329
Admin Fax Ext:
Admin Email: admin@domains.microsoft
Registry Tech ID:
Tech Name: MSN Hostmaster
Tech Organization: Microsoft Corporation
Tech Street: One Microsoft Way,
Tech City: Redmond
Tech State/Province: WA
Tech Postal Code: 98052
Tech Country: US
Tech Phone: +1.4258828080
Tech Phone Ext:
Tech Fax: +1.4259367329
Tech Fax Ext:
Tech Email: msnhst@microsoft.com
Name Server: ns1-39.azure-dns.com
Name Server: ns4-39.azure-dns.info
Name Server: ns2-39.azure-dns.net
Name Server: ns3-39.azure-dns.org
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/

For more information on WHOIS status codes, please visit:
  https://www.icann.org/resources/pages/epp-status-codes

MarkMonitor Domain Management(TM)
Protecting companies and consumers in a digital world.

Visit MarkMonitor at https://www.markmonitor.com
Contact us at +1.8007459229
In Europe, at +44.02032062220
----
```

Sitemap Blog Terms Privacy Contact California Privacy Notice Do Not Sell My Personal Information © 2022 DomainTools

ENG IN 12:38 24-04-2022

----------X---------X----------

From netcraft.com :

Site rank 69

DNS admin azuredns-hostmaster@microsoft.com

IPv4 address 104.95.181.163

IPv4 autonomous systems AS16625

IPv6 address 2a02:26f0:5700:1ae:0:0:0:356e

IPv6 autonomous systems AS20940

Reverse DNS a104-95-181-163.deploy.static.akamaitechnologies.com

Nameserver

ns1-39.azure-dns.com

Validity period From Jul 28 2021 to Jul 28 2022 (12 months)

Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142 104.120.141.176 Linux unknown 21-Apr-2022

Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB 184.24.201.171 Linux unknown 21-Apr-2022

Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB 23.36.169.159 Linux unknown 17-Apr-2022

Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142 23.211.185.163 Linux unknown 10-Apr-2022

Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142 184.31.225.172 Linux unknown 3-Apr-2022

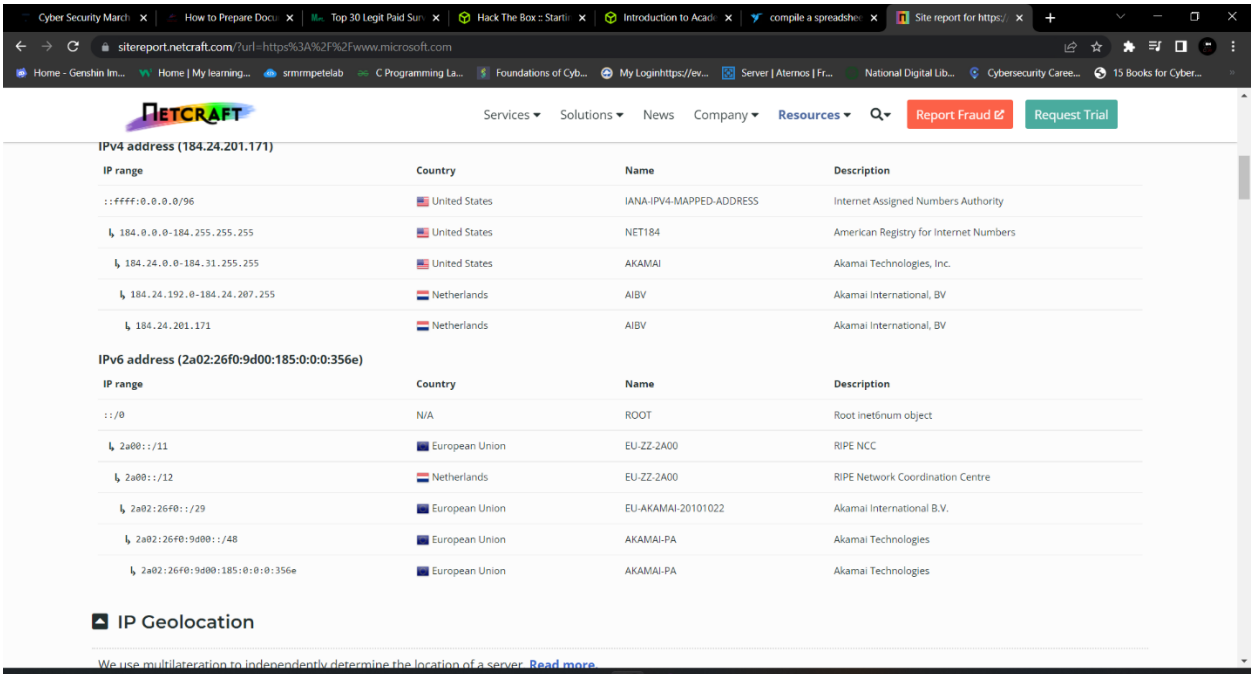
Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142 104.120.141.176 Linux unknown 20-Mar-2022

Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142 184.31.225.172 Linux unknown 13-Mar-2022

Akamai 88.221.16.244 Linux unknown 26-Feb-2022

Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142 184.31.225.172 Linux unknown 19-Feb-2022

Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142 104.110.245.246 Linux unknown 5-Feb-2022



IPv4 address (184.24.201.171)

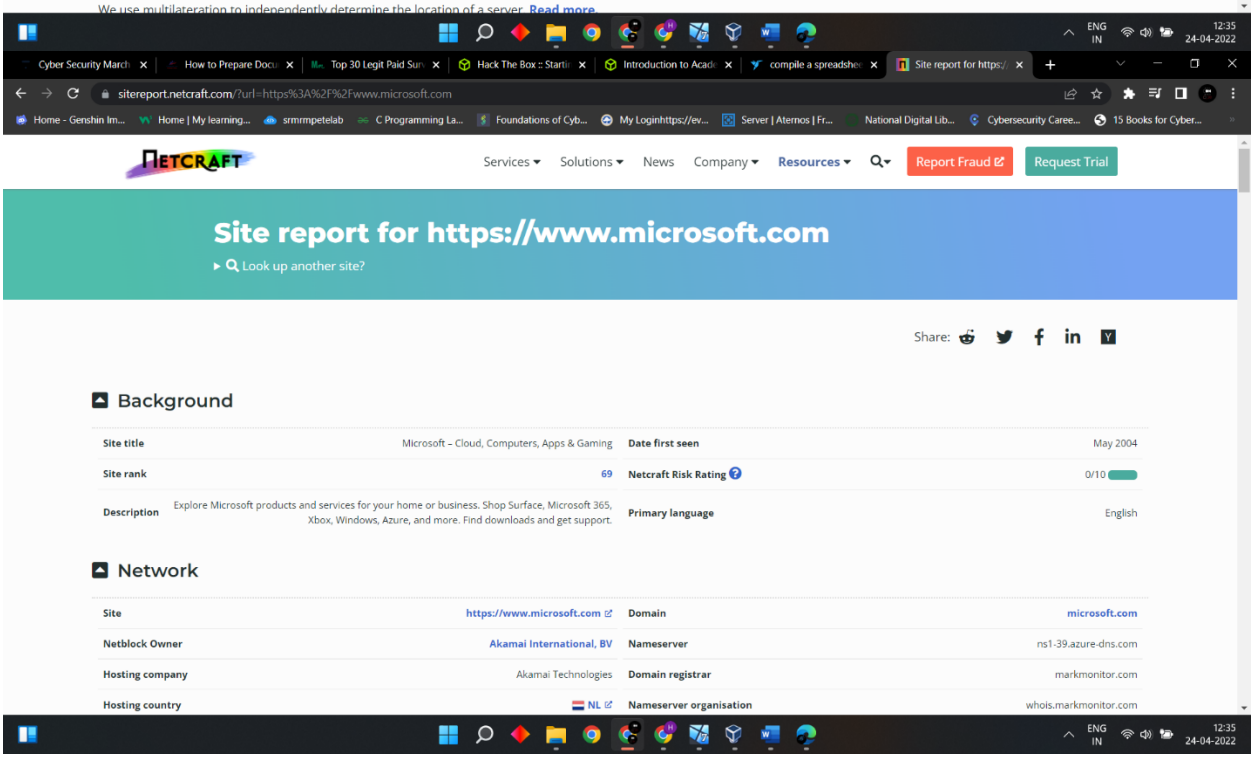
IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
184.0.0.0-184.255.255.255	United States	NET184	American Registry for Internet Numbers
184.24.0.0-184.31.255.255	United States	AKAMAI	Akamai Technologies, Inc.
184.24.192.0-184.24.207.255	Netherlands	AIBV	Akamai International, BV
184.24.201.171	Netherlands	AIBV	Akamai International, BV

IPv6 address (2a02:26f0:9d00:185:0:0:0:356e)

IP range	Country	Name	Description
::/0	N/A	ROOT	Root inet6num object
2a00::/11	European Union	EU-ZZ-2A00	RIPE NCC
2a00::/12	Netherlands	EU-ZZ-2A00	RIPE Network Coordination Centre
2a02:26f0::/29	European Union	EU-AKAMAI-20101022	Akamai International B.V.
2a02:26f0:9d00::/48	European Union	AKAMAI-PA	Akamai Technologies
2a02:26f0:9d00:185:0:0:0:356e	European Union	AKAMAI-PA	Akamai Technologies

IP Geolocation

We use multilateration to independently determine the location of a server. Read more



Site report for https://www.microsoft.com

Look up another site?

Share:

Background

Site title	Microsoft - Cloud, Computers, Apps & Gaming	Date first seen	May 2004
Site rank	69	Netcraft Risk Rating	0/10
Description	Explore Microsoft products and services for your home or business. Shop Surface, Microsoft 365, Xbox, Windows, Azure, and more. Find downloads and get support.	Primary language	English

Network

Site	https://www.microsoft.com	Domain	microsoft.com
Netblock Owner	Akamai International, BV	Nameserver	ns1-39.azure-dns.com
Hosting company	Akamai Technologies	Domain registrar	markmonitor.com
Hosting country	NL	Nameserver organisation	whois.markmonitor.com

Cyber Security March | How to Prepare Docu | Top 30 Legit Paid Sur | Hack The Box :: Startir | Introduction to Acad | compile a spreadshe | Site report for https:/

sitereport.netcraft.com/?url=https%3A%2F%2Fwww.microsoft.com

Home - Genshin Im... | Home | My learning... | srmrmpetelab | C Programming La... | Foundations of Cyb... | My Loginhttps://ev... | Server | Aternos | Fr... | National Digital Lib... | Cybersecurity Caree... | 15 Books for Cyber...

NETCRAFT

Services ▾ Solutions ▾ News Company ▾ Resources ▾ Report Fraud Request Trial

SSL/TLS

Assurance	Organisation validation	Perfect Forward Secrecy	Yes
Common name	www.microsoft.com	Supported TLS Extensions	RFC8446 supported versions, RFC8446 key share, RFC4366 server name, RFC4492 elliptic curves, RFC7301 application-layer protocol negotiation, RFC4366 status request
Organisation	Microsoft Corporation	Application-Layer Protocol Negotiation	h2
State	WA	Next Protocol Negotiation	Not Present
Country	US	Issuing organisation	Microsoft Corporation
Organisational unit	Microsoft Corporation	Issuer common name	Microsoft RSA TLS CA 01
Subject Alternative Name	privacy.microsoft.com, c.s-microsoft.com, microsoft.com, i.s-microsoft.com, staticview.microsoft.com, www.microsoft.com, wwwqa.microsoft.com	Issuer unit	Not Present
Validity period	From Jul 28 2021 to Jul 28 2022 (12 months)	Issuer location	Not Present
Matches hostname	Yes	Issuer country	US
Server	Not Present	Issuer state	Not Present
Public key algorithm	rsaEncryption	Certificate Revocation	http://mscrl.microsoft.com/pki/mscorp/crl/Microsoft%20RSA%20TLS%20CA%2001.crl

12:36 24-04-2022 ENG IN

Cyber Security March | How to Prepare Docu | Top 30 Legit Paid Sur | Hack The Box :: Startir | Introduction to Acad | compile a spreadshe | Site report for https:/

sitereport.netcraft.com/?url=https%3A%2F%2Fwww.microsoft.com

Home - Genshin Im... | Home | My learning... | srmrmpetelab | C Programming La... | Foundations of Cyb... | My Loginhttps://ev... | Server | Aternos | Fr... | National Digital Lib... | Cybersecurity Caree... | 15 Books for Cyber...

NETCRAFT

Services ▾ Solutions ▾ News Company ▾ Resources ▾ Report Fraud Request Trial

Certificate check	ok	OCSP servers	http://ocsp.msocsp.com - 100% uptime in the past 24 hours Performance Graph
Signature algorithm	sha256WithRSAEncryption	OCSP stapling response	Certificate valid
Serial number	0x120014f1ec2395d56fdcc4dcb700000014f1ec	OCSP data generated	Apr 20 21:00:47 2022 GMT
Cipher	TLS_AES_256_GCM_SHA384	OCSP data expires	Apr 24 21:00:47 2022 GMT
Version number	0x02		

Certificate Transparency

Signed Certificate Timestamps (SCTs)

Source	Log	Timestamp	Signature Verification
Certificate	Google Argon 2022 KXm+8J45OSHwVnOfY6V35b5XfZxgCvj5TV0mXCVdx4Q=	2021-07-28 21:32:10	Success
Certificate	Cloudflare Nimbus 2022 QcJKsd8iRkoQxqE6CUKHXk4x1xsD6+tLx2JukGKWBvY=	2021-07-28 21:32:10	Success
Certificate	Google Xenon 2022 RqVV63X6kSAwtaKJafTzfREsQXS+/Um4havy/HD+bUc=	2021-07-28 21:32:10	Success

SSLv3/POODLE

This site does not support the SSL version 3 protocol.

More information about SSL version 3 and the POODLE vulnerability.

12:36 24-04-2022 ENG IN

Cyber Security March | How to Prepare Docu | Top 30 Legit Paid Sur | Hack The Box :: Startir | Introduction to Acad | compile a spreadshe | Site report for https:/

sitereport.netcraft.com/?url=https%3A%2F%2Fwww.microsoft.com

Home - Genshin Im... | Home | My learning... | srmrmpetelab | C Programming La... | Foundations of Cyb... | My Loginhttps://ev... | Server | Aternos | Fr... | National Digital Lib... | Cybersecurity Caree... | 15 Books for Cyber...

NETCRAFT

Services ▾ Solutions ▾ News Company ▾ Resources ▾ Report Fraud Request Trial

SSL Certificate Chain

Hosting History

Netblock owner	IP address	OS	Web server	Last seen
Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142	104.120.141.176	Linux	unknown	21-Apr-2022
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	184.24.201.171	Linux	unknown	21-Apr-2022
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.36.169.159	Linux	unknown	17-Apr-2022
Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142	23.211.185.163	Linux	unknown	10-Apr-2022
Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142	184.31.225.172	Linux	unknown	3-Apr-2022
Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142	104.120.141.176	Linux	unknown	20-Mar-2022
Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142	184.31.225.172	Linux	unknown	13-Mar-2022
Akamai	88.221.16.244	Linux	unknown	26-Feb-2022
Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142	184.31.225.172	Linux	unknown	19-Feb-2022
Akamai Technologies, Inc. 145 Broadway Cambridge MA US 02142	104.110.245.246	Linux	unknown	5-Feb-2022

Sender Policy Framework

A host's Sender Policy Framework (SPF) describes who can send mail on its behalf. This is done by publishing an SPF record containing a series of rules. Each rule consists of a qualifier followed by a specification of which domains to apply this qualifier to. For more information please see open-spf.org

ENG IN 12:36 24-04-2022

Cyber Security March | How to Prepare Docu | Top 30 Legit Paid Sur | Hack The Box :: Startir | Introduction to Acad | compile a spreadshe | Site report for https:/

sitereport.netcraft.com/?url=https%3A%2F%2Fwww.microsoft.com

Home - Genshin Im... | Home | My learning... | srmrmpetelab | C Programming La... | Foundations of Cyb... | My Loginhttps://ev... | Server | Aternos | Fr... | National Digital Lib... | Cybersecurity Caree... | 15 Books for Cyber...

NETCRAFT

Services ▾ Solutions ▾ News Company ▾ Resources ▾ Report Fraud Request Trial

Site Technology (fetched today)

Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

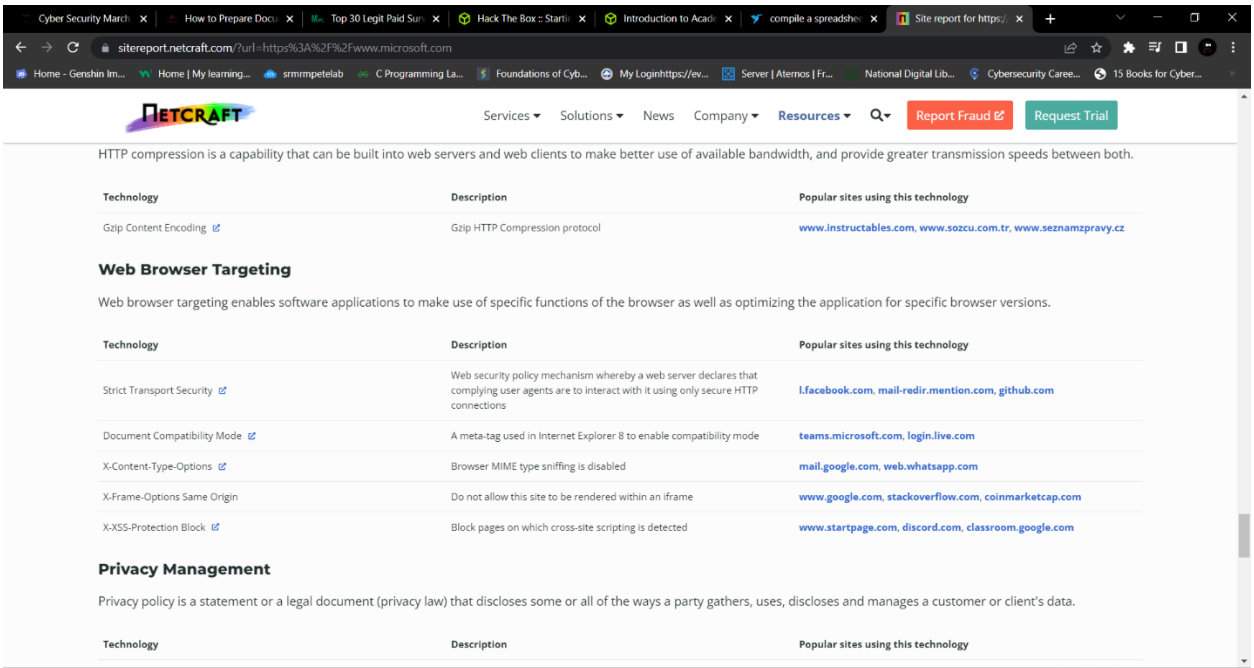
Technology	Description	Popular sites using this technology
SSL	A cryptographic protocol providing communication security over the Internet	
Using ASP.NET	ASP.NET is running on the server	www1.sedecatastro.gob.es, www.cnblogs.com, www.webmd.com

Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

Technology	Description	Popular sites using this technology
Web Worker	*No description*	www.paloaltonetworks.com, www.finanz.ru, www.haberturk.com
Asynchronous Javascript	*No description*	www.foxnews.com, www.hulu.com, www.roblox.com
Local Storage	*No description*	www.ebay.co.uk, www.w3schools.com, www.amazon.in
Session Storage	*No description*	www.ilovepdf.com, www.bankofamerica.com, www.cisco.com
JavaScript	Widely-supported programming language commonly used to power client-side dynamic content on websites	

ENG IN 12:36 24-04-2022



HTTP compression is a capability that can be built into web servers and web clients to make better use of available bandwidth, and provide greater transmission speeds between both.

Technology	Description	Popular sites using this technology
Gzip Content Encoding	Gzip HTTP Compression protocol	www.instructables.com, www.sozcu.com.tr, www.seznamzpravy.cz

Web Browser Targeting

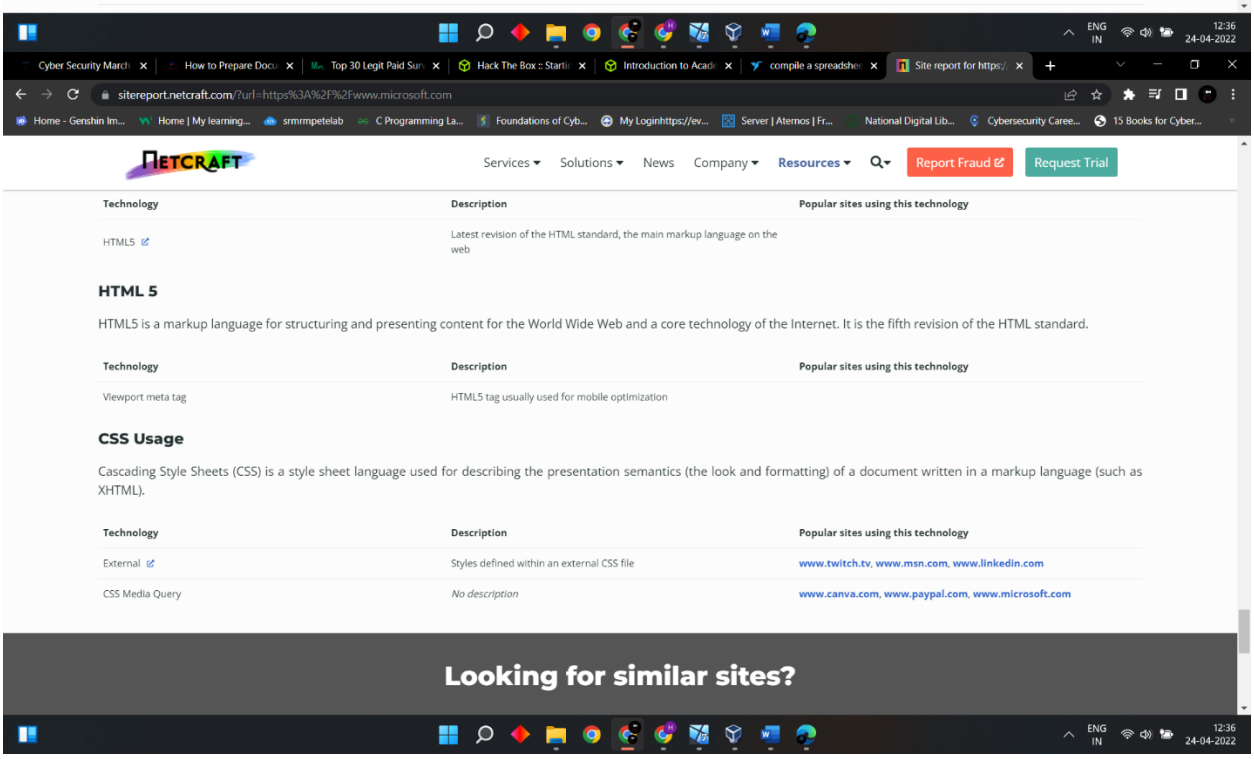
Web browser targeting enables software applications to make use of specific functions of the browser as well as optimizing the application for specific browser versions.

Technology	Description	Popular sites using this technology
Strict Transport Security	Web security policy mechanism whereby a web server declares that complying user agents are to interact with it using only secure HTTP connections	l.facebook.com, mail-redir.mention.com, github.com
Document Compatibility Mode	A meta-tag used in Internet Explorer 8 to enable compatibility mode	teams.microsoft.com, login.live.com
X-Content-Type-Options	Browser MIME type sniffing is disabled	mail.google.com, web.whatsapp.com
X-Frame-Options Same Origin	Do not allow this site to be rendered within an iframe	www.google.com, stackoverflow.com, coinmarketcap.com
X-XSS-Protection Block	Block pages on which cross-site scripting is detected	www.startpage.com, discord.com, classroom.google.com

Privacy Management

Privacy policy is a statement or a legal document (privacy law) that discloses some or all of the ways a party gathers, uses, discloses and manages a customer or client's data.

Technology	Description	Popular sites using this technology



Technology	Description	Popular sites using this technology
HTML5	Latest revision of the HTML standard, the main markup language on the web	

HTML 5

HTML5 is a markup language for structuring and presenting content for the World Wide Web and a core technology of the Internet. It is the fifth revision of the HTML standard.

Technology	Description	Popular sites using this technology
Viewport meta tag	HTML5 tag usually used for mobile optimization	

CSS Usage

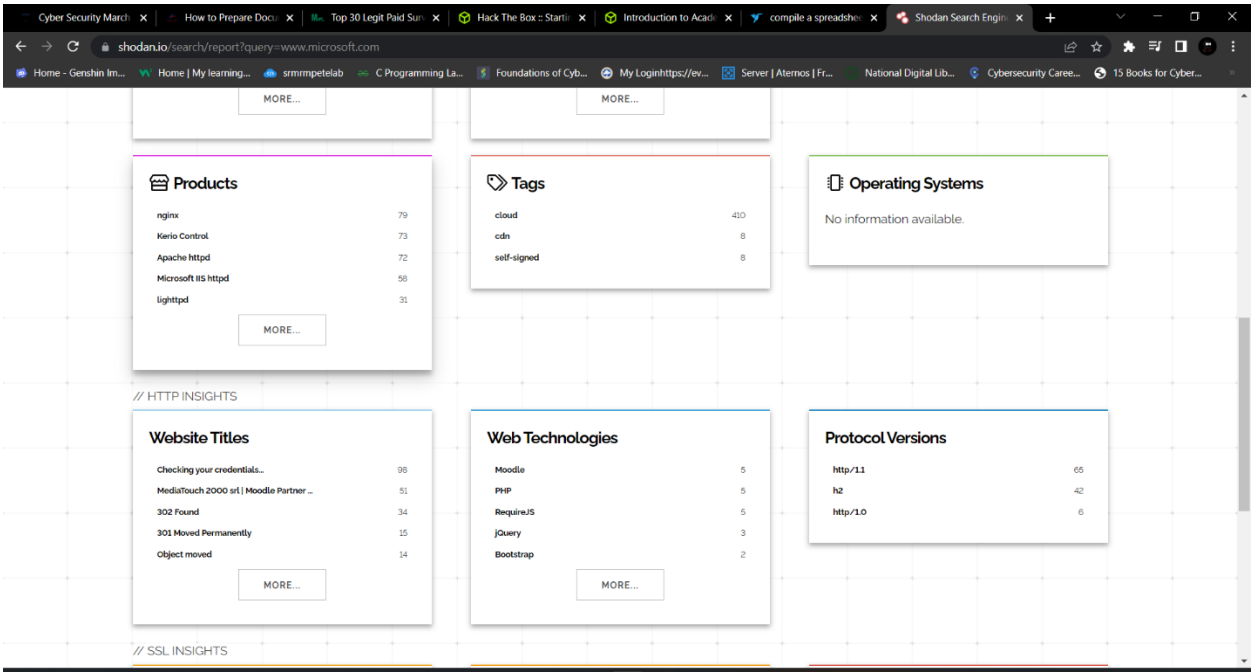
Cascading Style Sheets (CSS) is a style sheet language used for describing the presentation semantics (the look and formatting) of a document written in a markup language (such as XHTML).

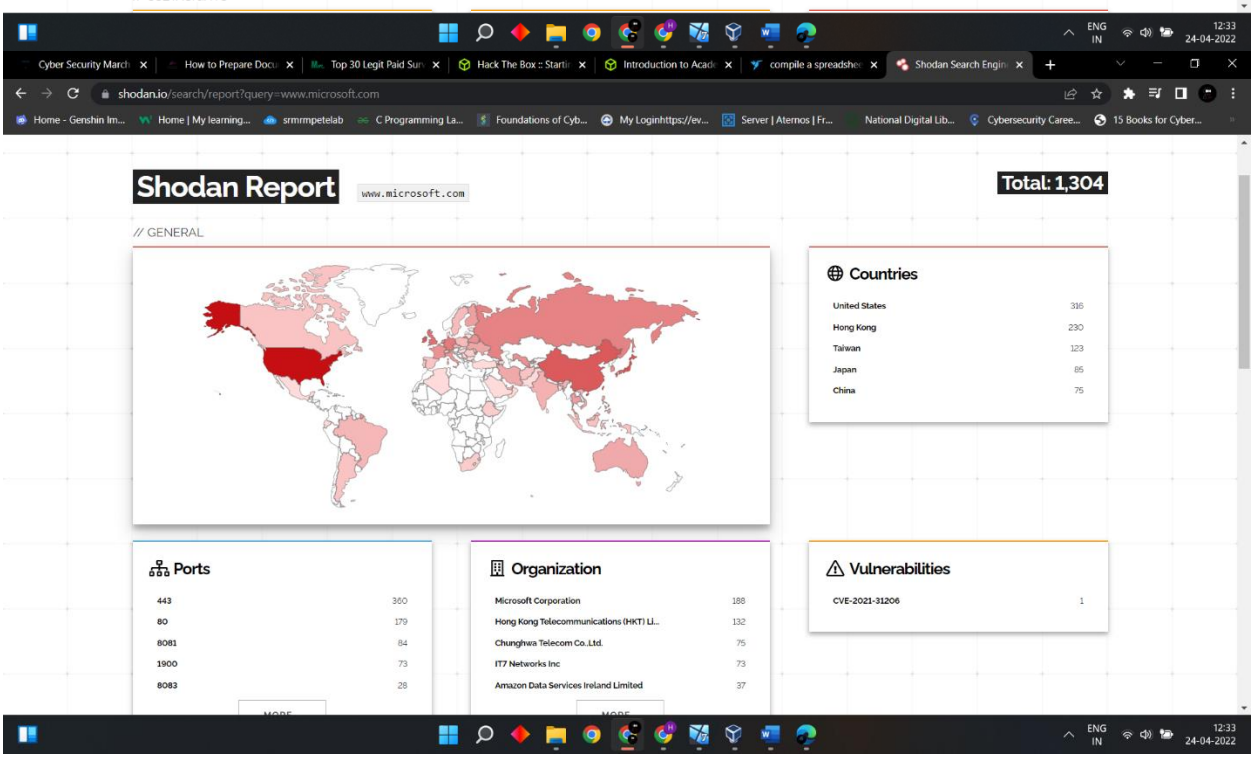
Technology	Description	Popular sites using this technology
External	Styles defined within an external CSS file	www.twitch.tv, www.msn.com, www.linkedin.com
CSS Media Query	*No description*	www.canva.com, www.paypal.com, www.microsoft.com

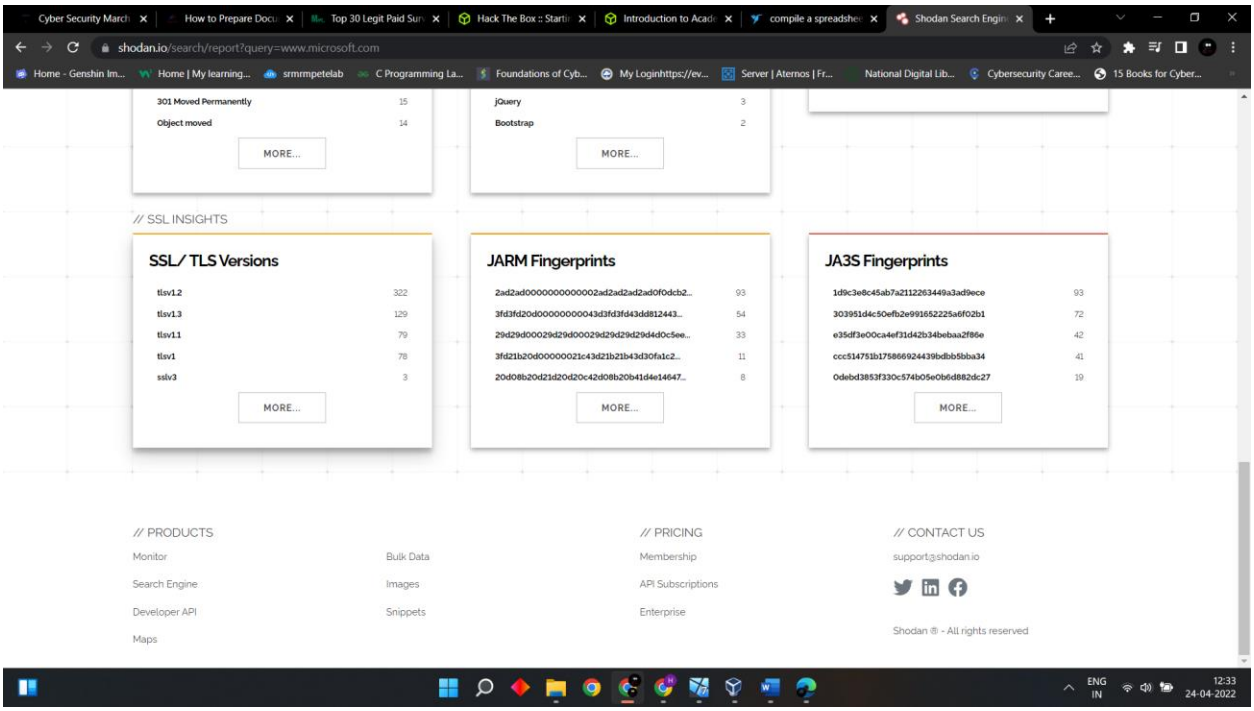
Looking for similar sites?

----------x---------x----------

From shodan.io :







----------x---------x----------

From dnsdumpster.co

www.microsoft.com

HTTP: AkamaiGHost

HTTPS: AkamaiGHost 23.35.78.52

a23-35-78-52.deploy.static.akamaitechnologies.com AKAMAI-AS

United States

controls-ppe.platform.account.www.microsoft.com

52.229.38.152

MICROSOFT-CORP-MSN-AS-BLOCK

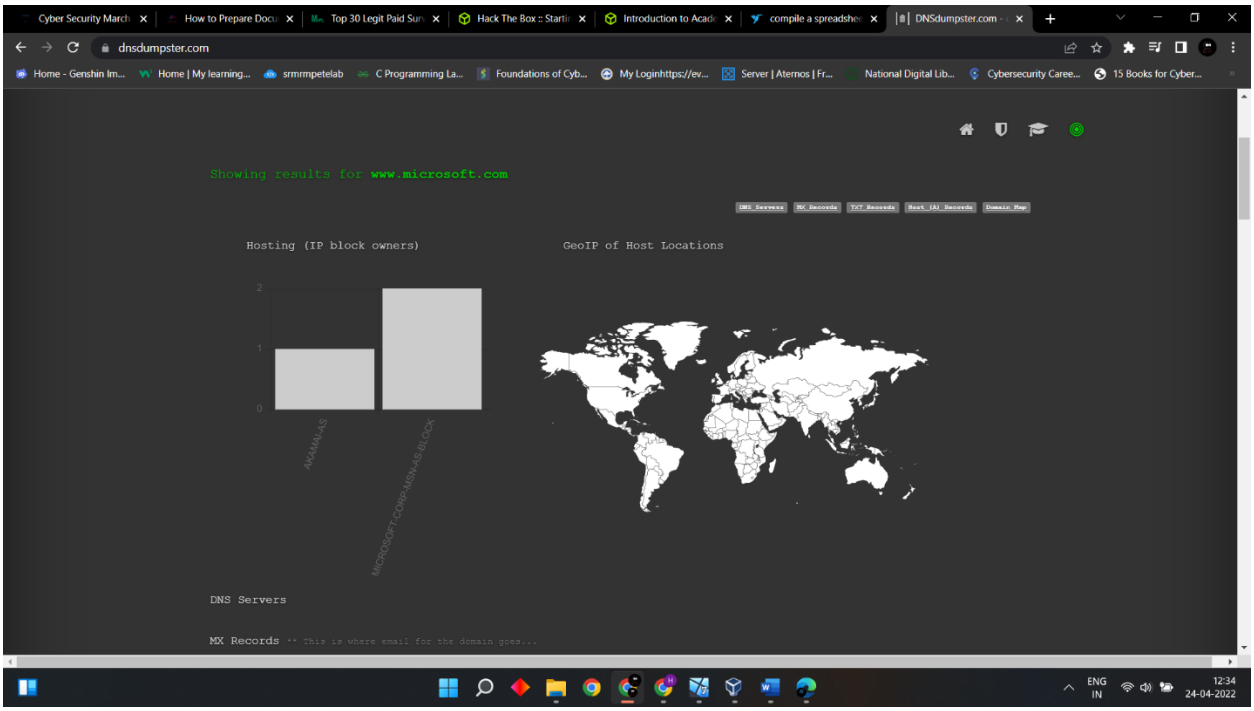
United States

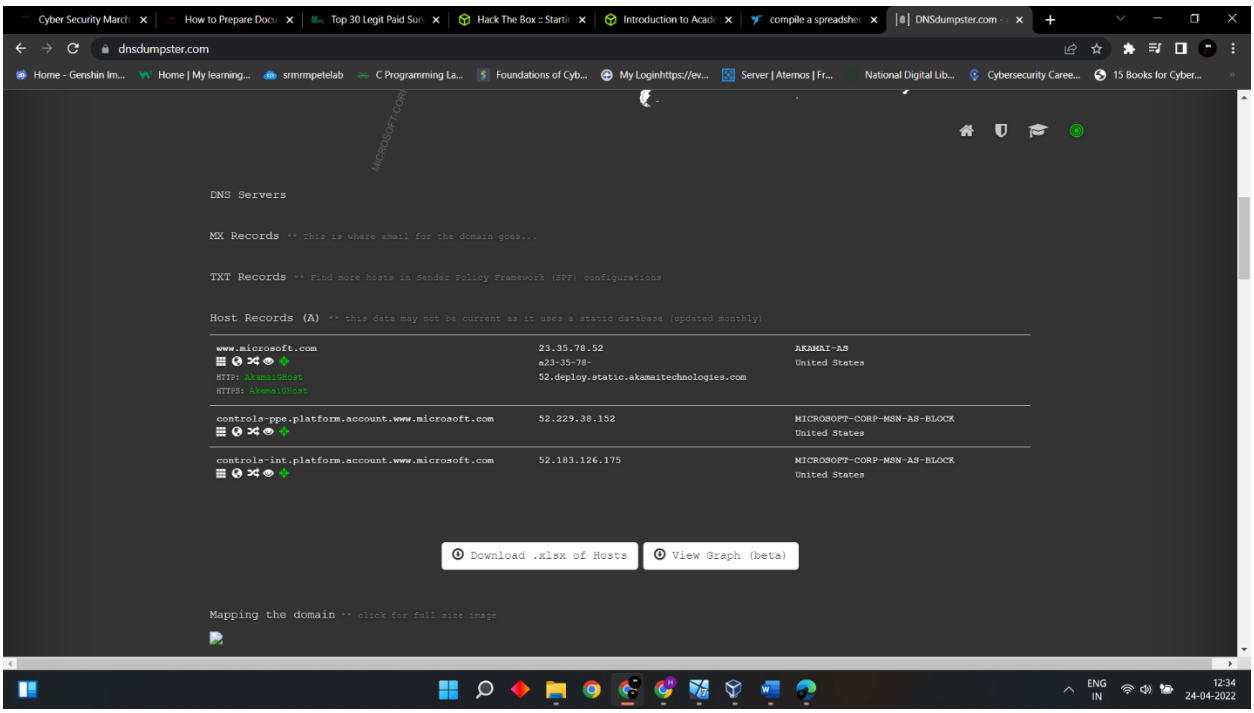
controls-int.platform.account.www.microsoft.com

52.183.126.175

MICROSOFT-CORP-MSN-AS-BLOCK

United States





BY: HARSH JAIN SRM IST