



Laboratorio 1 - Ciberseguridad

Fabián Valero Duque

Integrantes: Alejandra Campo Archbold, María Fernanda Rodríguez, Jham Pool Murillo

5 de agosto de 2022

Información sobre Shodan

Análisis Comparativos

1. Modbus

Colombia

Colombia vs otros países de Latinoamérica

2. Información sobre el producto Hikvision IP Camera y conexión web

Colombia

Colombia vs otros países de Latinoamérica

3. Servicios de impresoras

Colombia

Colombia vs otros países de Latinoamérica

4. Remote Desktop Protocol (RDP)

Colombia

Colombia vs otros países de Latinoamérica

5. MongoDB Puerto 27017

Colombia vs otros países de Latinoamérica

Colombia

Cambiando el comando de búsqueda de MongoDB

6. Virtual Private Network (VPN)

Colombia vs otros países de Latinoamérica

Colombia

7. Minerías de Ethereum (ETH)

Colombia vs otros países de Latinoamérica

Colombia

8. Dispositivos con Windows 7

Colombia

Colombia vs otros países de Latinoamérica

[9. Outlook web app](#)

[Colombia](#)

[Colombia vs otros países de Latinoamérica](#)

[10. Ark survival evolved](#)

[Colombia](#)

[Colombia vs otros países de Latinoamérica](#)

[Conclusiones](#)

[Referencias](#)

Información sobre Shodan

Shodan es un motor de búsqueda de dispositivos conectados a Internet. Shodan recopila información sobre todos los dispositivos conectados directamente a Internet. Si un dispositivo está conectado directamente a Internet, Shodan lo consulta para obtener información disponible públicamente. Los tipos de dispositivos que se indexan pueden variar enormemente: desde pequeños escritorios hasta plantas de energía nuclear y todo lo demás. Info: **What is Shodan?**

- **Complete guide to shodan:** Es un libro oficial escrito por el fundador que explica los *ins y outs* del motor de búsqueda. Los lectores conocerán la variedad de sitios web que están disponibles para acceder a los datos, cómo automatizar tareas comunes usando la línea de comandos y cómo crear soluciones personalizadas usando la API del desarrollador.
- **Project SHINE (SHodan INtelligence Extraction):** Es un proyecto desarrollado para extraer información sobre la existencia de dispositivos SCADA e ICS accesibles desde Internet. Se utiliza el motor de búsqueda en línea existente llamado SHODAN que escanea Internet en busca de dispositivos conectados. Esos dispositivos pueden ser computadoras, impresoras, conmutadores, PLC, SCADA RTU, etc, cualquier cosa con una dirección IP.
- **Awesome Shodan Search Queries:** Usuario que recolectó variedad de consultas de búsqueda interesantes, divertidas y deprimentes para conectarlas a SHODAN, el motor de búsqueda de Internet. Algunos devuelven resultados *facepalm-inducing*, mientras que otros devuelven vulnerabilidades graves y/o antiguas en la naturaleza.
- **An exploration of the cybercrime ecosystem around Shodan:** Es un paper que analiza discusiones relacionadas con IoT que son potencialmente ciberdelincuentes por naturaleza. En particular, analizan los hilos del foro que tratan sobre el motor de búsqueda Shodan. La fuente de estas publicaciones es el conjunto de datos CrimeBB proporcionado por

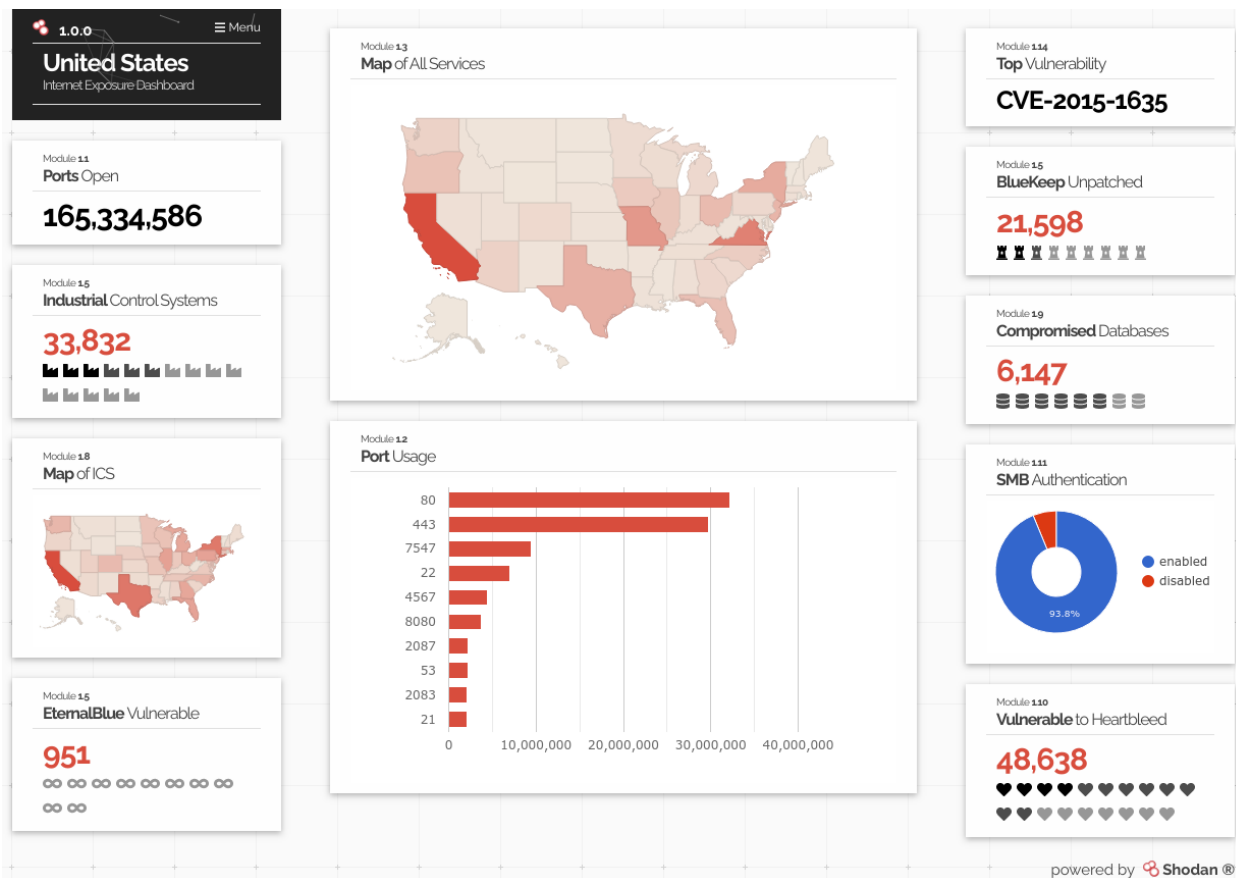
Cambridge Cybercrime Centro (CCC). Exploran 1051 discusiones de hilos de 19 foros entre 2009 y 2020. El objetivo general del trabajo es explorar los principales casos de uso de Shodan y resaltar los objetivos y motivaciones de los piratas informáticos.

General Filters

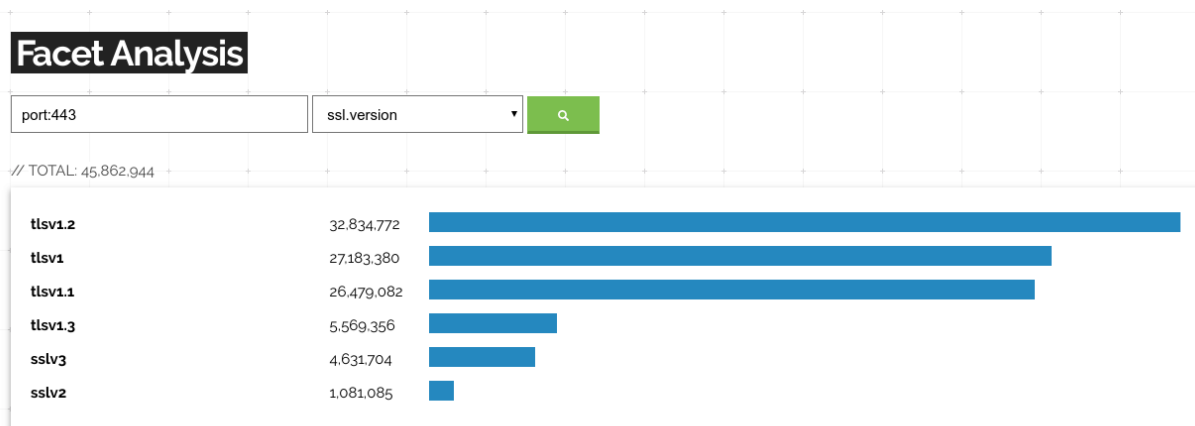
Name	Description	Type
after	Only show results after the given date (dd/mm/yyyy)	string
asn	Autonomous system number	string
before	Only show results before the given date (dd/mm/yyyy)	string
category	Available categories: ics, malware	string
city	Name of the city	string
country	2-letter country code	string
geo	Accepts between 2 and 4 parameters. If 2 parameters: latitude,longitude. If 3 parameters: latitude,longitude,range. If 4 parameters: top left latitude, top left longitude, bottom right latitude, bottom right longitude.	string
hash	Hash of the data property	integer
has_ipv6	True/ False	boolean
has_screenshot	True/ False	boolean
hostname	Full hostname for the device	string
ip	Alias for net filter	string
isp	ISP managing the netblock	string
net	Network range in CIDR notation (ex. 199.4.1.0/24)	string
org	Organization assigned the netblock	string
os	Operating system	string
port	Port number for the service	integer
postal	Postal code (US-only)	string
product	Name of the software/ product providing the banner	string
region	Name of the region/ state	string
state	Alias for region	string
version	Version for the product	string
vuln	CVE ID for a vulnerability	string

Filtros generales para utilizar en el monitor de búsqueda de Shodan. Fuente: [Complete guide to shodan](#)

Otra funcionalidad destacable de Shodan es la generación de estadísticas a través de Facet Analysis. La API de Shodan permite obtener una distribución de valores para una propiedad utilizando un concepto llamado facetas; éste permite encontrar facetas para el ver el panorama general de los resultados.



Ejemplo de uso del reporte. Fuente: **Generating Statistics**



Ejemplo de uso de Facet Analysis con comandos. Fuente: **Generating Statistics**

Análisis Comparativos



1. Modbus



port:502

Los clientes y servidores Modbus TCP/IP escuchan y reciben datos Modbus a través del puerto 502.

La aplicación principal de Modbus es en aplicaciones *multi master-slave* para comunicarse entre dispositivos inteligentes y sensores e instrumentos para monitorear dispositivos de campo usando PC de escritorio e interfaces hombre-máquina. Modbus es un protocolo para aplicaciones relacionadas con RTU en las que se requiere comunicación inalámbrica. Es por eso que se utiliza en un sinnúmero de servicios públicos de subestaciones de gas y petróleo. Modbus es un protocolo industrial; Además, las aplicaciones de construcción, infraestructura, transporte y energía también pueden utilizar los beneficios de Modbus. El factor común es la estructura de mensajería que admiten todos los dispositivos.

Colombia

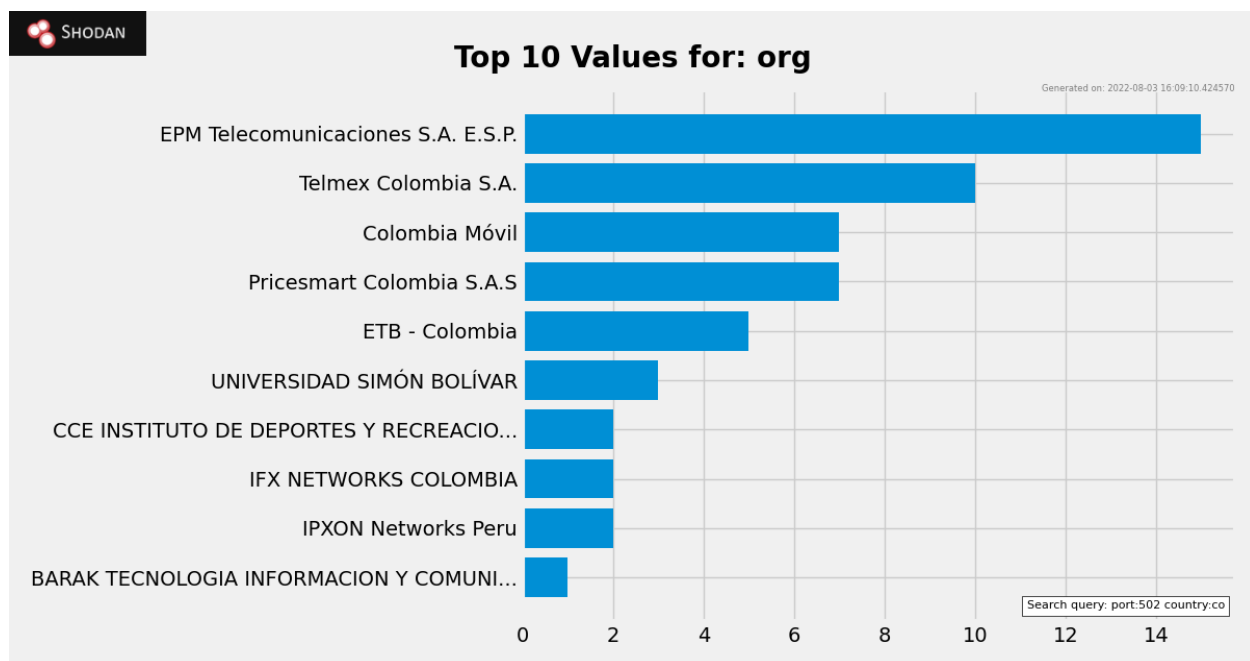
- port:502 country:co

En Colombia, podemos encontrar que las principales empresas que exponen el puerto 502 (Modbus) son EPM, Telmex y Colombia Móvil. Estas empresas brindan servicios de telecomunicaciones asociados a teléfonos, televisión, entre otros. Durante la búsqueda se puede denotar que los sistemas operativos que más son afectados son los de MikroTik RouterOS y

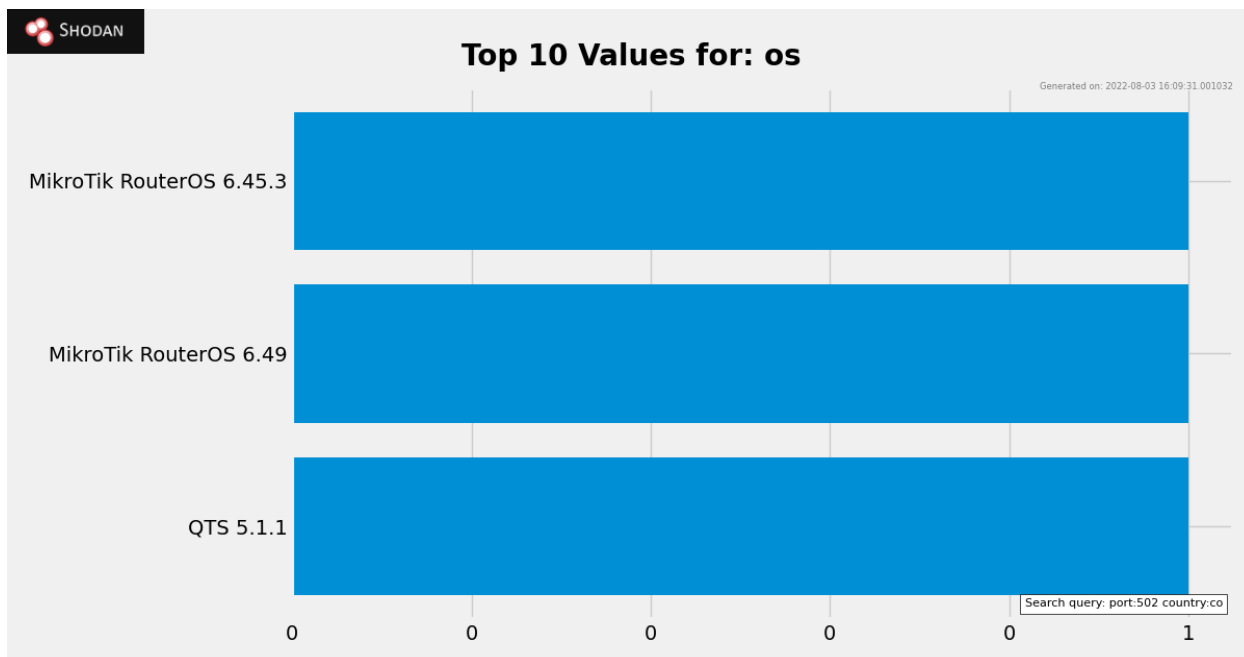
QTS; El primero se puede utilizar para modificar el sistema informático como router de red confiable, el segundo os, ofrece un almacenamiento con funciones y aplicaciones versátiles de valor añadido, como instantáneas, servidores multimedia Plex y un acceso sencillo a su nube personal.

Por otro lado, las vulnerabilidades más presentes en las direcciones IPs encontradas son cve-2022-1292, cve-2020-1971, cve-2021-23840, cve-2021-23841, cve-2021-3712, cve-2021-4160, cve-2021-4160 y cve-2022-2068. Sin embargo, para Colombia, no presenta vulnerabilidades verificadas.

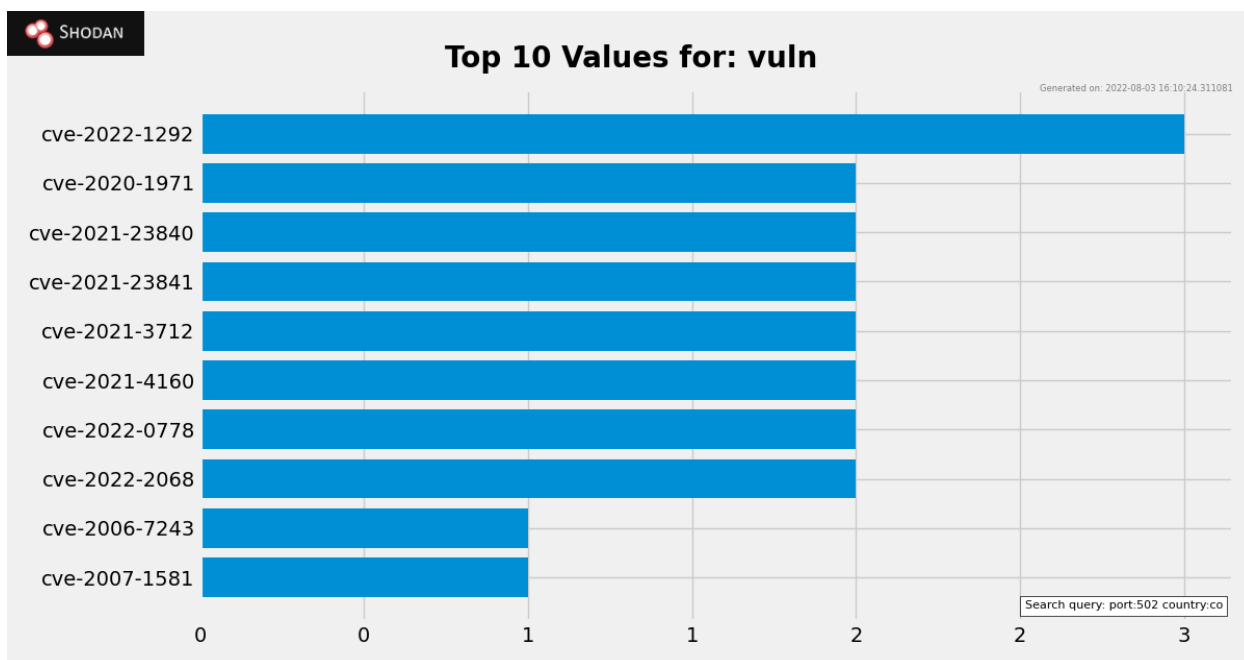
Por ejemplo cve-2022-1292 hace referencia a que el **script c_rehash** no desinfecta correctamente los metacaracteres del shell para evitar la inyección de comandos. Este script es distribuido por algunos sistemas operativos de manera que se ejecuta automáticamente. En dichos sistemas operativos, un atacante podría ejecutar comandos arbitrarios con los privilegios del script. El uso del script c_rehash se considera obsoleto y debe reemplazarse por la herramienta de línea de comandos de rehash de OpenSSL. Corregido en OpenSSL 3.0.3 (Afectado 3.0.0,3.0.1,3.0.2). Corregido en OpenSSL 1.1.1o (Afectado 1.1.1-1.1.1n). Corregido en OpenSSL 1.0.2ze (Afectado 1.0.2-1.0.2zd). Esta vulnerabilidad tiene **nivel crítico**.



Top 10 empresas con vulnerabilidades presentes en el puerto 502. Report: Facet Analysis



Top sistemas operativos afectados. Report: Facet Analysis



Top 10 de las vulnerabilidades presentes en el puerto 502. Report: Facet Analysis

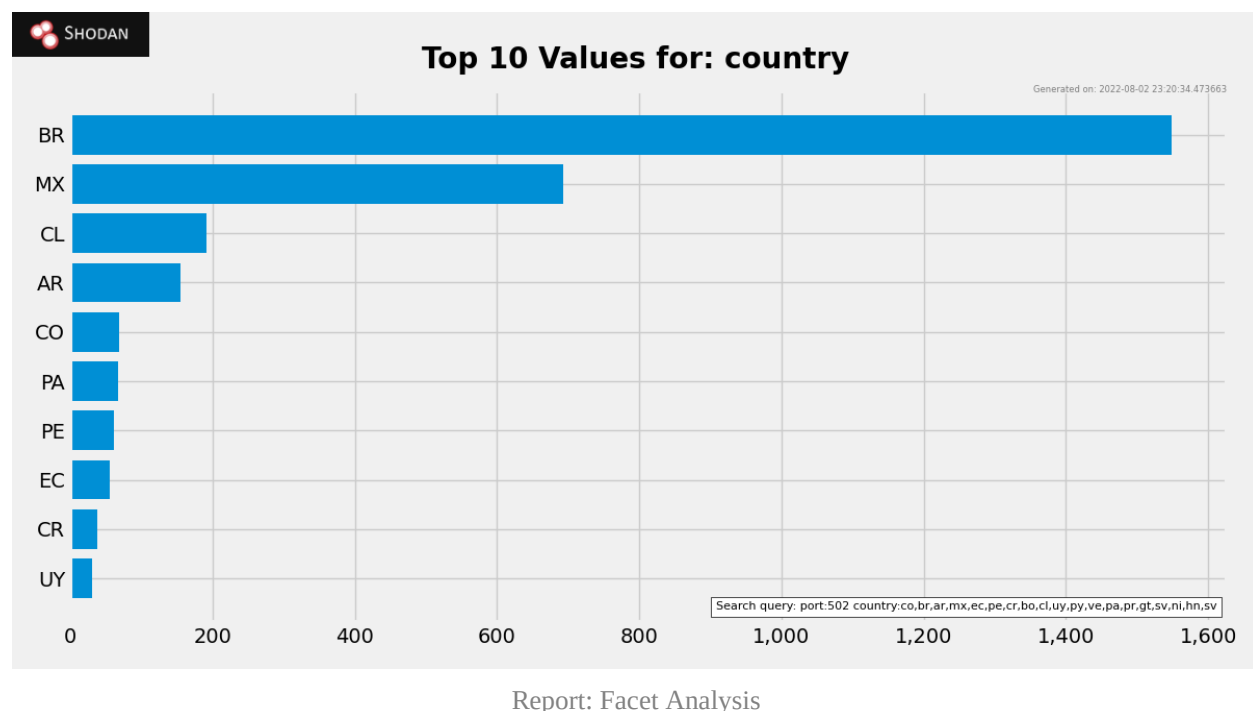
Colombia vs otros países de Latinoamérica

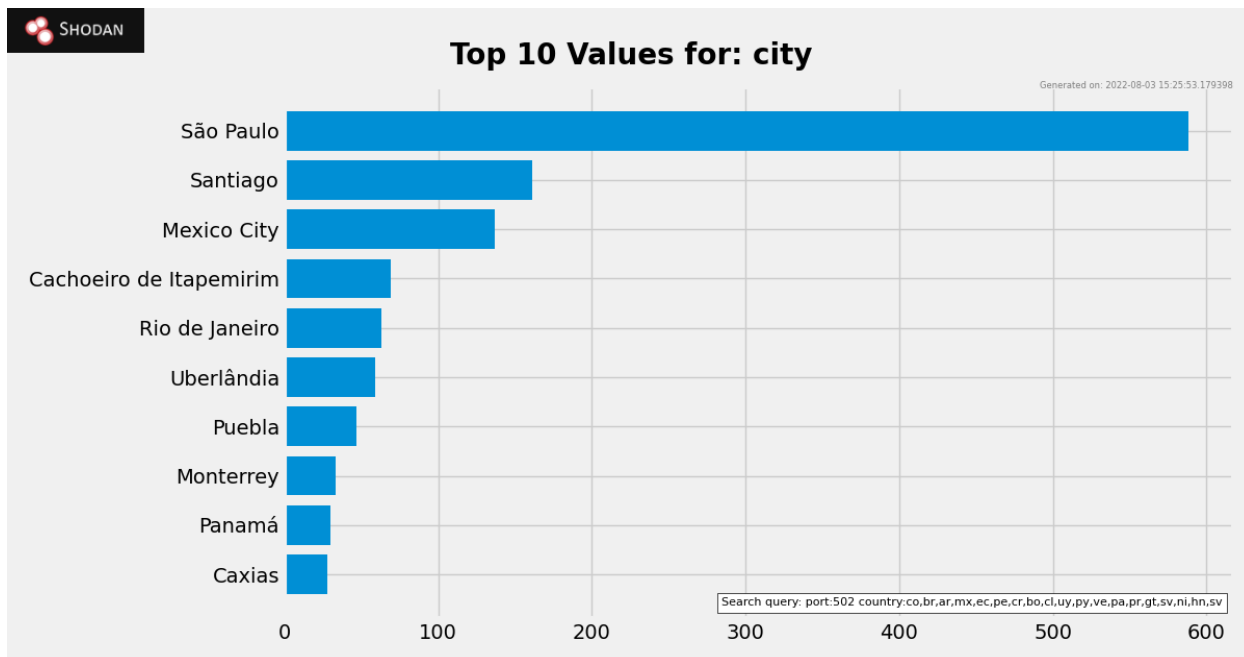
- port:502 country:co,br,ar,mx,ec,pe,cr,bo,cl,uy,py,ve,pa,pr,gt,sv,ni,hn,sv

En Latinoamérica las principales ciudades con información pública sobre sistemas industriales Modbus son: São Paulo, Santiago, Mexico City, Cachoeiro de Itamemirim, Rio de Janeiro, Uberlândia, Puebla, Monterrey, Panamá, Caxias. La mayoría de estas ciudades son el país de Brasil y seguida de México. Algunas de las empresas encontradas son de telecomunicaciones como: Amazon Data Services Brazil, Uninet S.A. de C.V, Gestión de direccionamiento UniNet, ALGAR TELECOM S/A, entre otros.

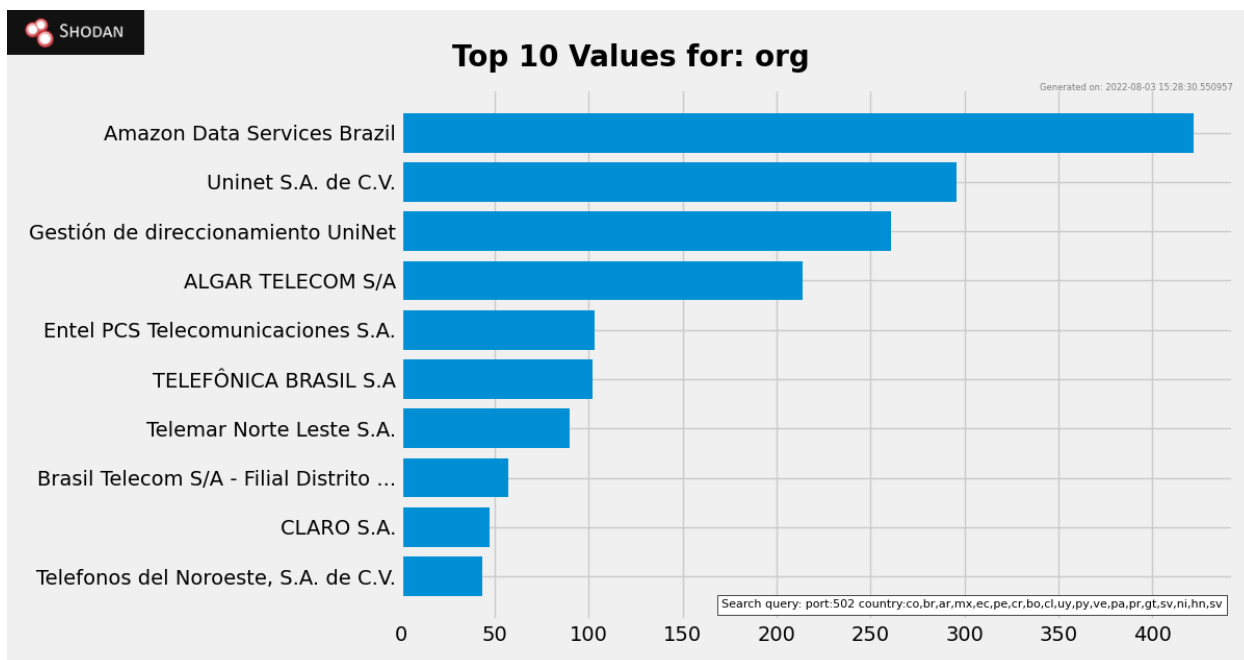
Los productos destacados son Hikvision IP Camera, OpenSSH, SAS TSXETY4103, Plex, BMX P34 2020, entre otros. Estos sistemas son cámaras de seguridad, servicios de conectividad segura, módulos de Ethernet.

En términos de vulnerabilidades, existen dos verificadas: cve-2015-1635 y ms15-034. El cve-2015-1635 describe que el HTTP.sys en Microsoft Windows 7 SP1, Windows Server 2008 R2 SP1, Windows 8, Windows 8.1 y Windows Server 2012 Gold y R2 permite a atacantes remotos ejecutar código arbitrario a través de solicitudes HTTP manipuladas, también conocida como "vulnerabilidad de ejecución remota de código HTTP.sys. Por otro lado, ms15-034 es podría permitir la ejecución remota de código si un atacante envía una solicitud HTTP especialmente diseñada a un sistema Windows afectado.

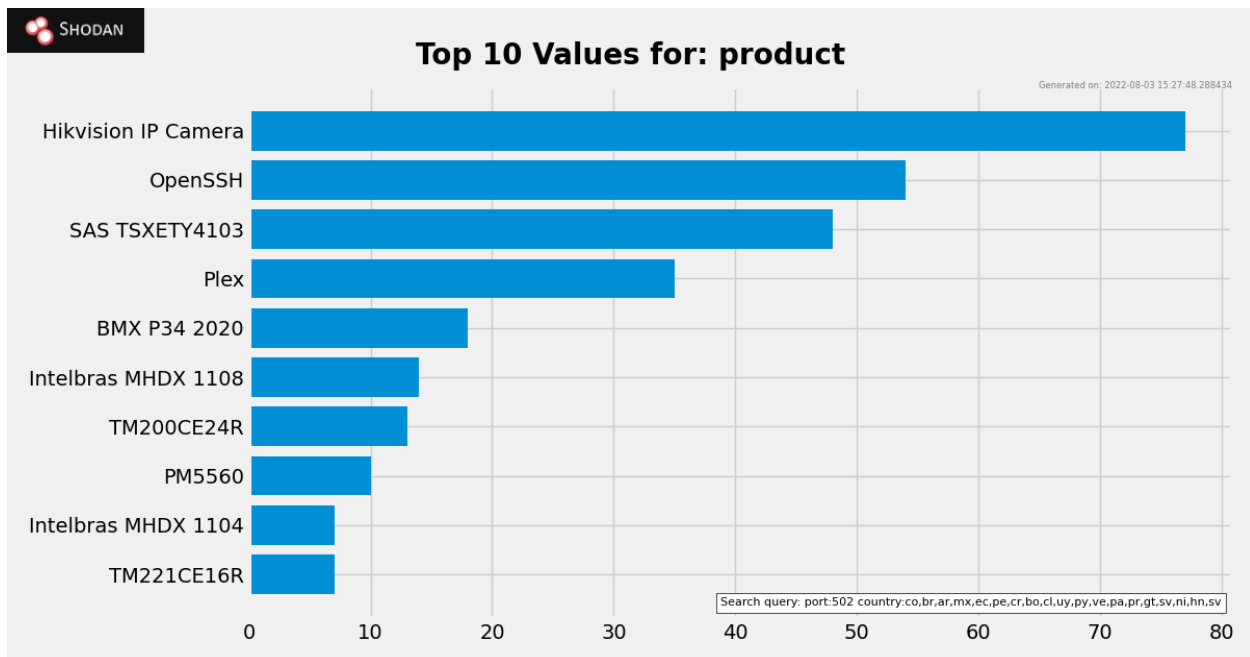




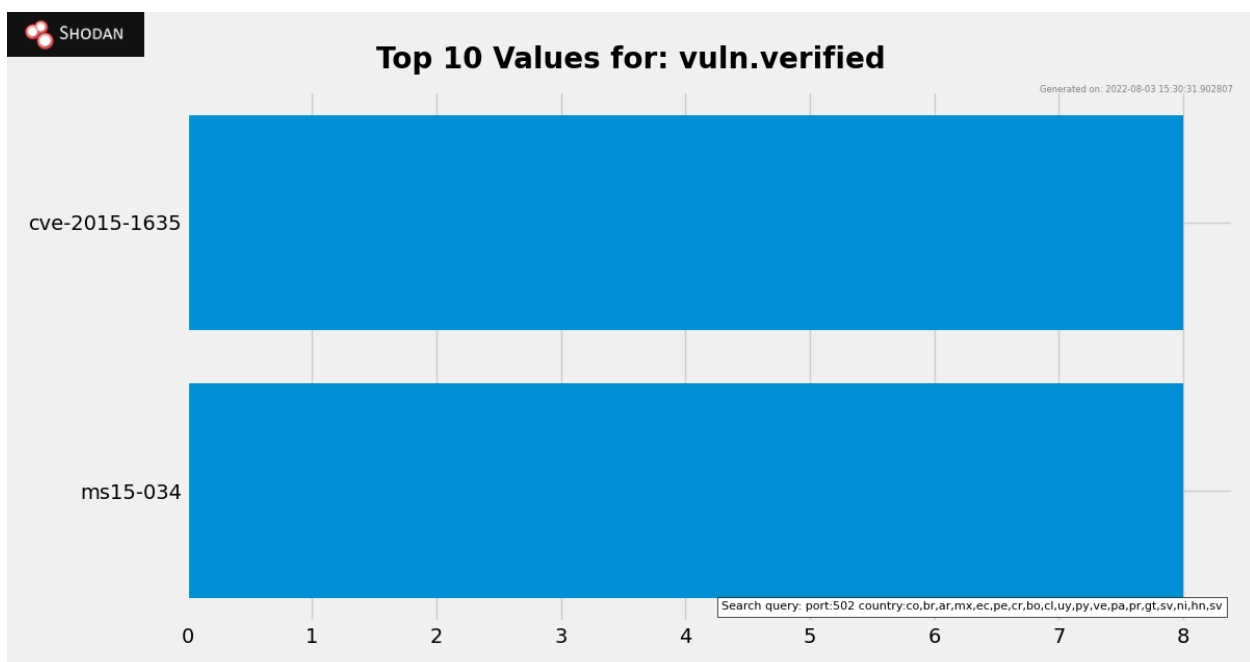
Report: Facet Analysis



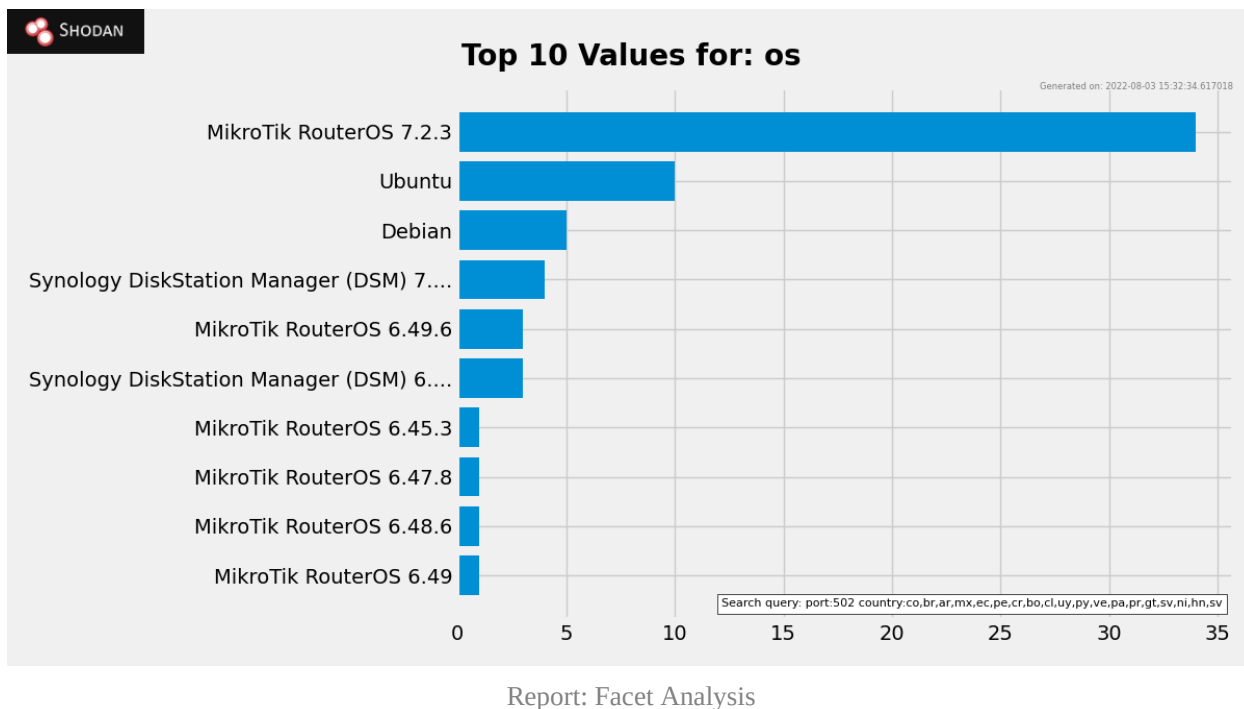
Report: Facet Analysis



Report: Facet Analysis



Report: Facet Analysis



2. Información sobre el producto Hikvision IP Camera y conexión web

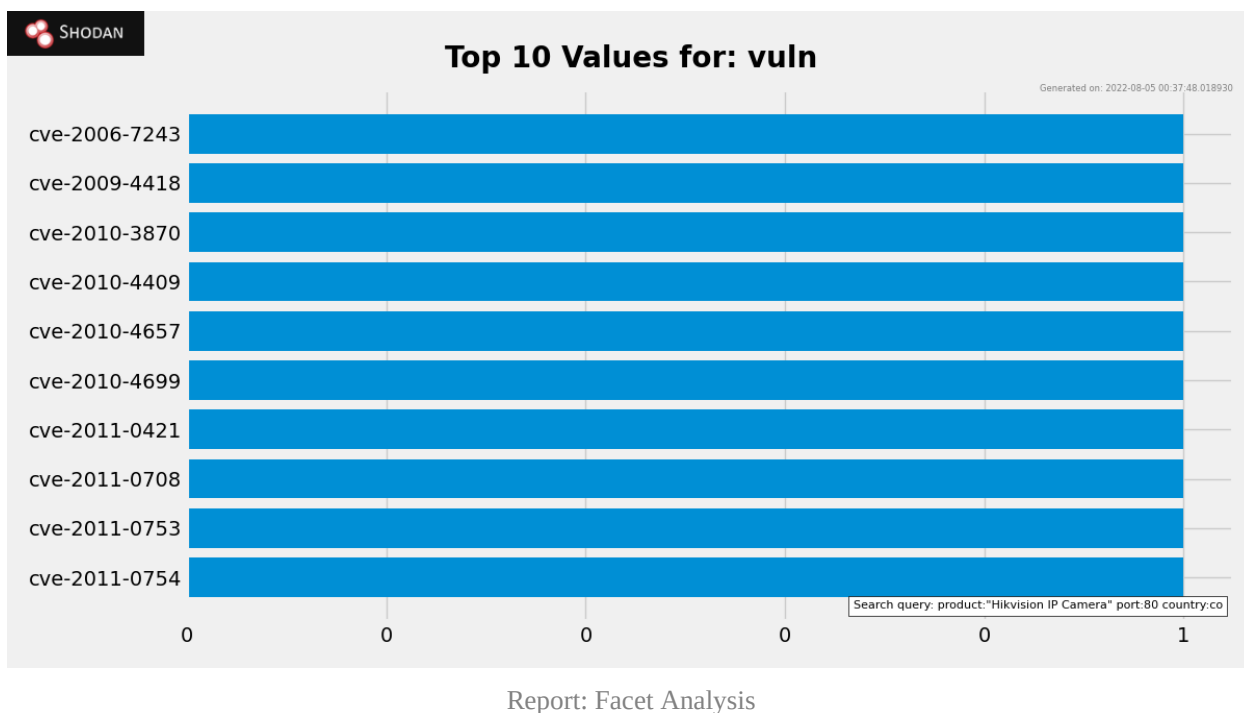
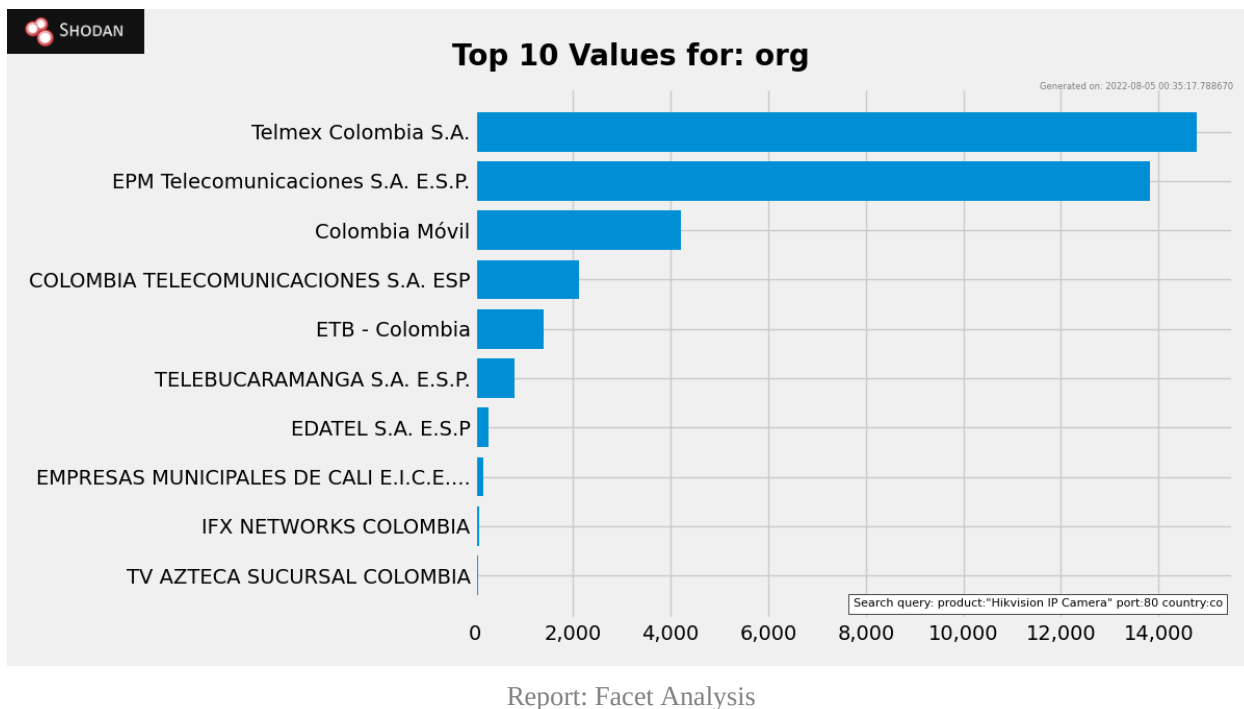


`product:"Hikvision IP Camera" port:80`

El producto Hikvision diseña y adapta cámaras de red para satisfacer diversas necesidades, desde monitoreo de video general hasta análisis de contenido de video con algoritmos de aprendizaje profundo y más. Por otro lado, el puerto 80 se usa para la navegación web de forma no segura HTTP.

Colombia

- `product:"Hikvision IP Camera" port:80 country:co`

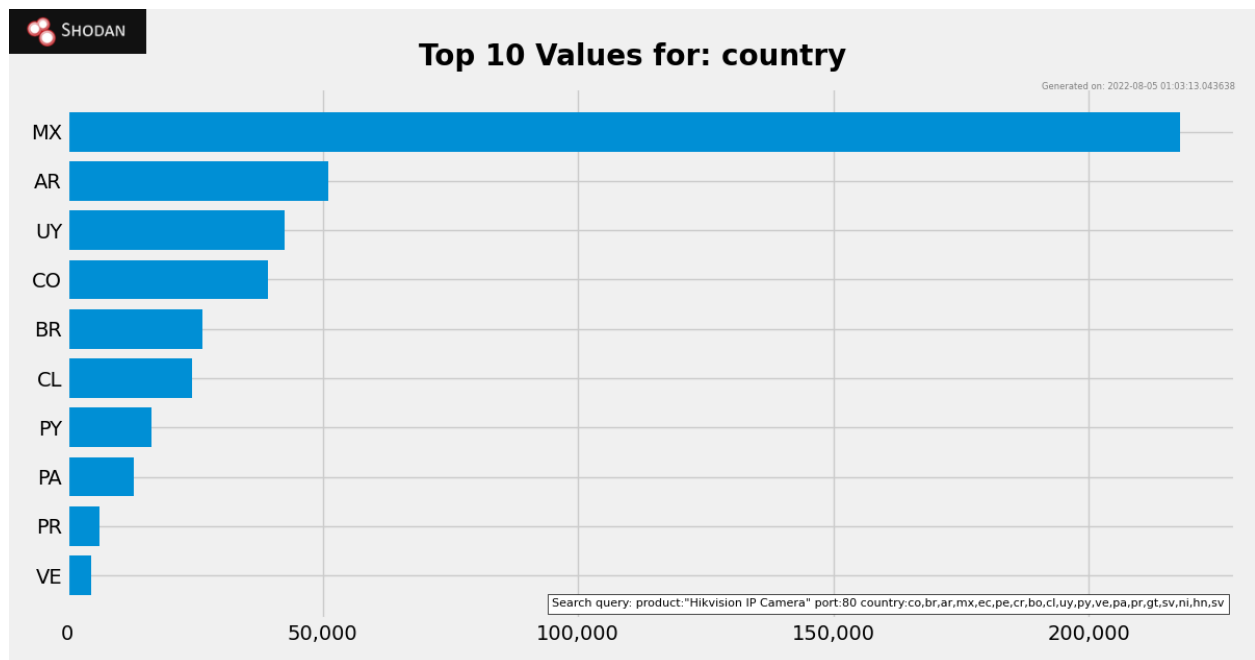


En Colombia, las empresas Telmex Colombia S.A y EPM son las destacadas en utilizar el producto Hikvision para cámaras de seguridad. Estos presentan algunas vulnerabilidades como el cve-2006-7243 significa que el PHP anterior a 5.3.4 acepta el carácter \0 en un nombre de ruta, lo que podría permitir a los atacantes dependientes del contexto eludir las restricciones de acceso

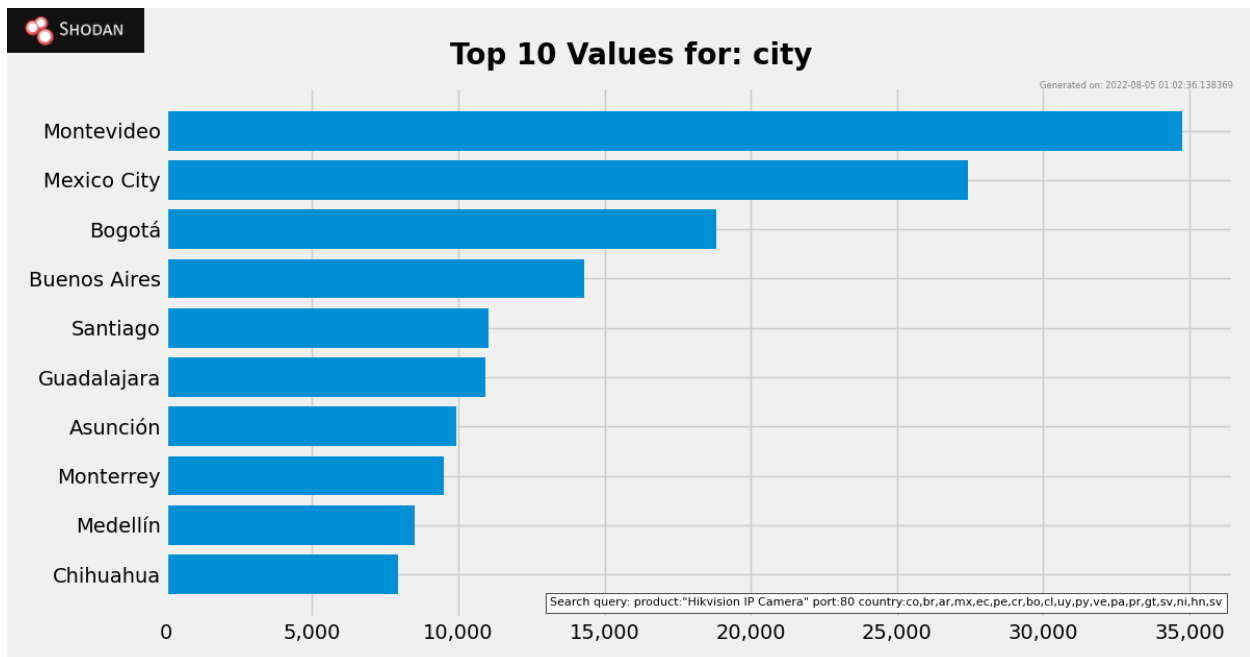
previstas colocando una extensión de archivo segura después de este carácter, como lo demuestra .php\0.jpg al final del argumento a la función file_exists.

Colombia vs otros países de Latinoamérica

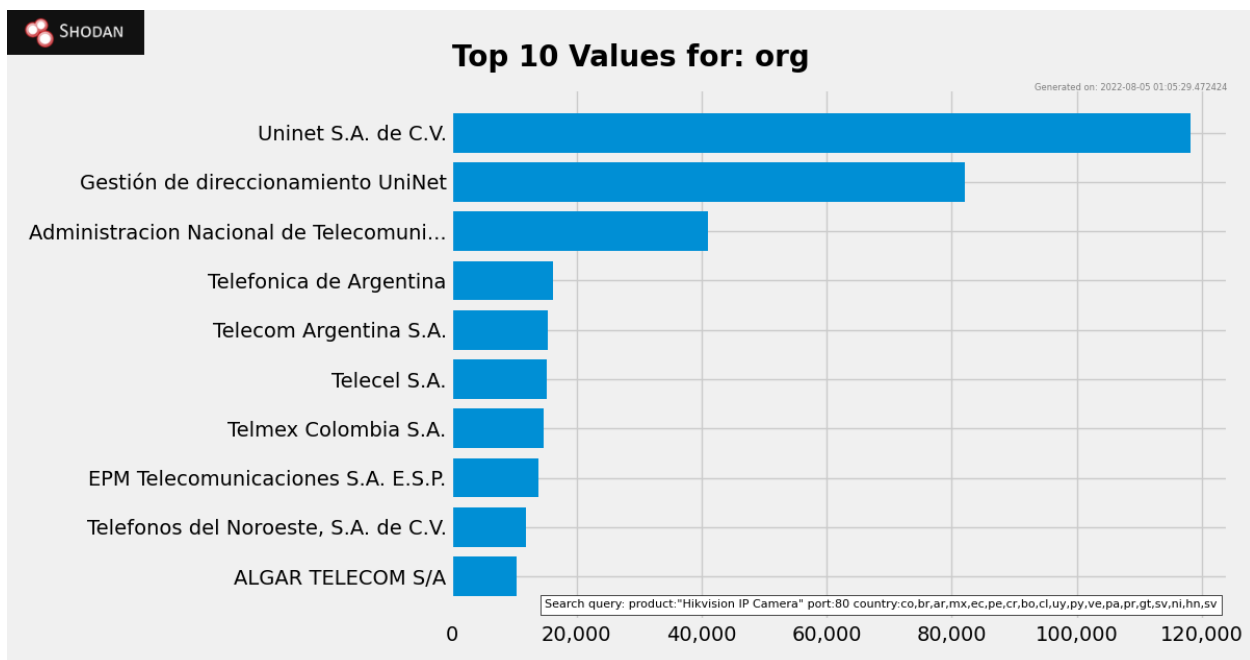
- `product:"Hikvision IP Camera" port:80`
`country:co,br,ar,mx,ec,pe,cr,bo,cl,uy,py,ve,pa,pr,gt,sv,ni,hn,sv`



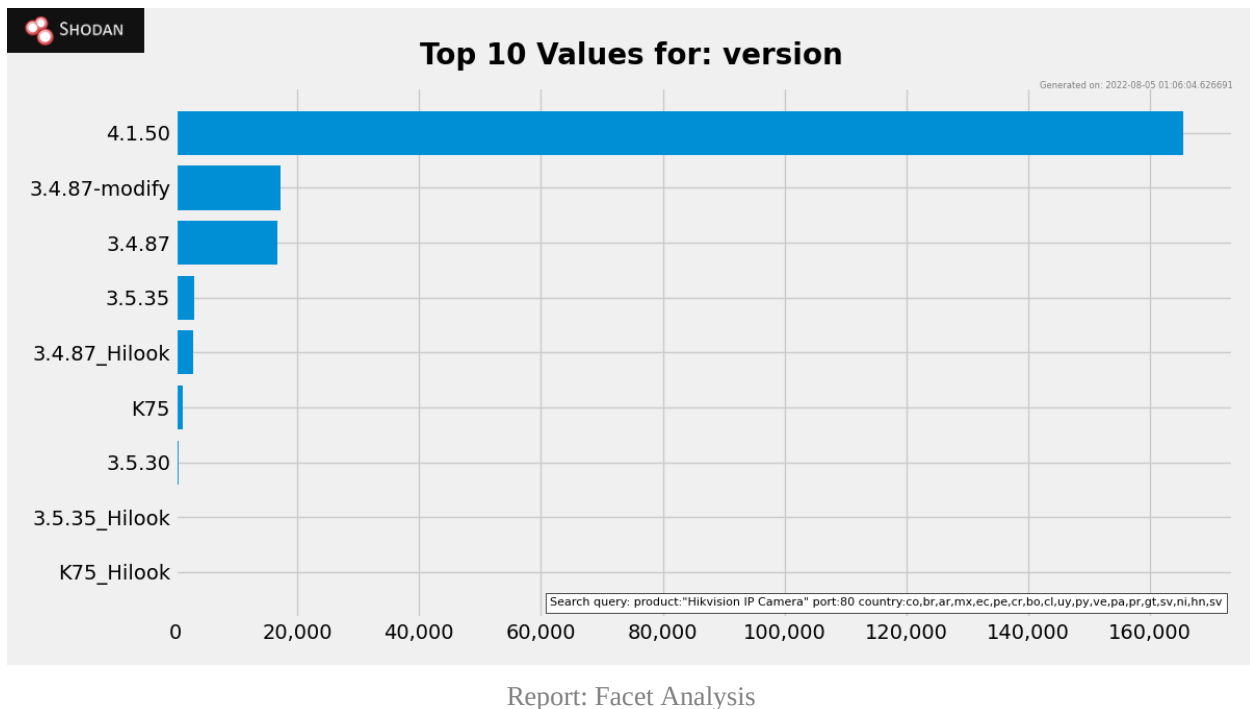
Report: Facet Analysis



Report: Facet Analysis

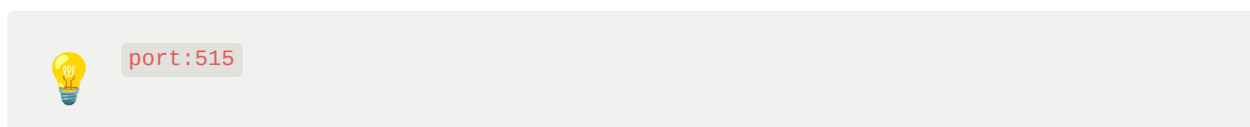


Report: Facet Analysis



Los países y ciudades destacadas son de Brasil, México y Colombia. Para esta cámara la versión con más vulnerabilidades es la 4.1.50 porque presenta problemas de *firmware*, que es un programa de software que permite controlar y comunicarse con el hardware de un equipo de forma directa.

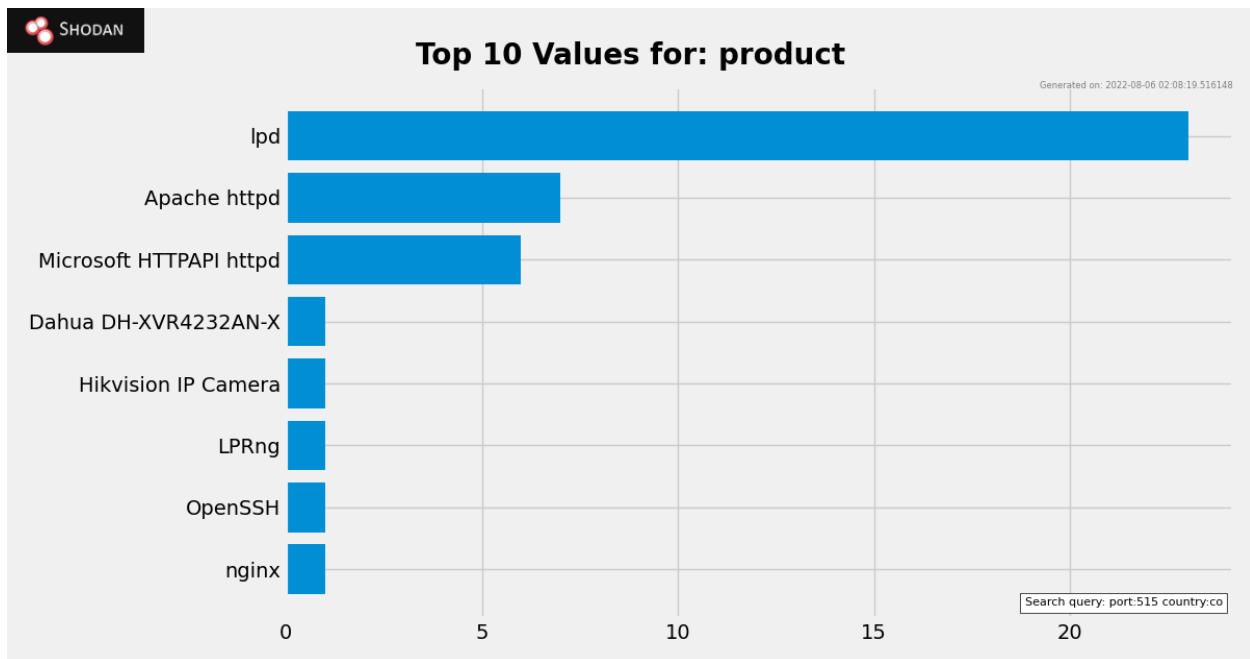
3. Servicios de impresoras



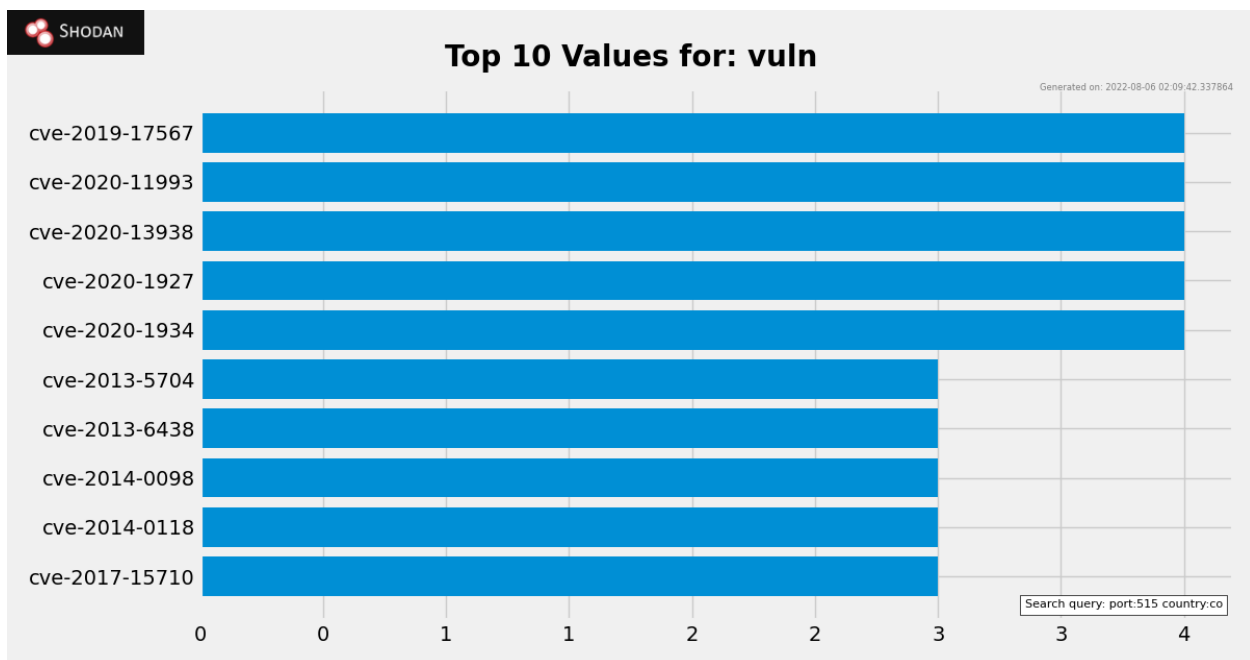
El puerto 515 es un protocolo TCP que conecta a servicios de impresoras. TCP garantiza la entrega de datos y también garantiza que los paquetes se entregarán en el puerto 515 en el mismo orden en que se enviaron.

Colombia

- port:515 country:co



Report: Facet Analysis



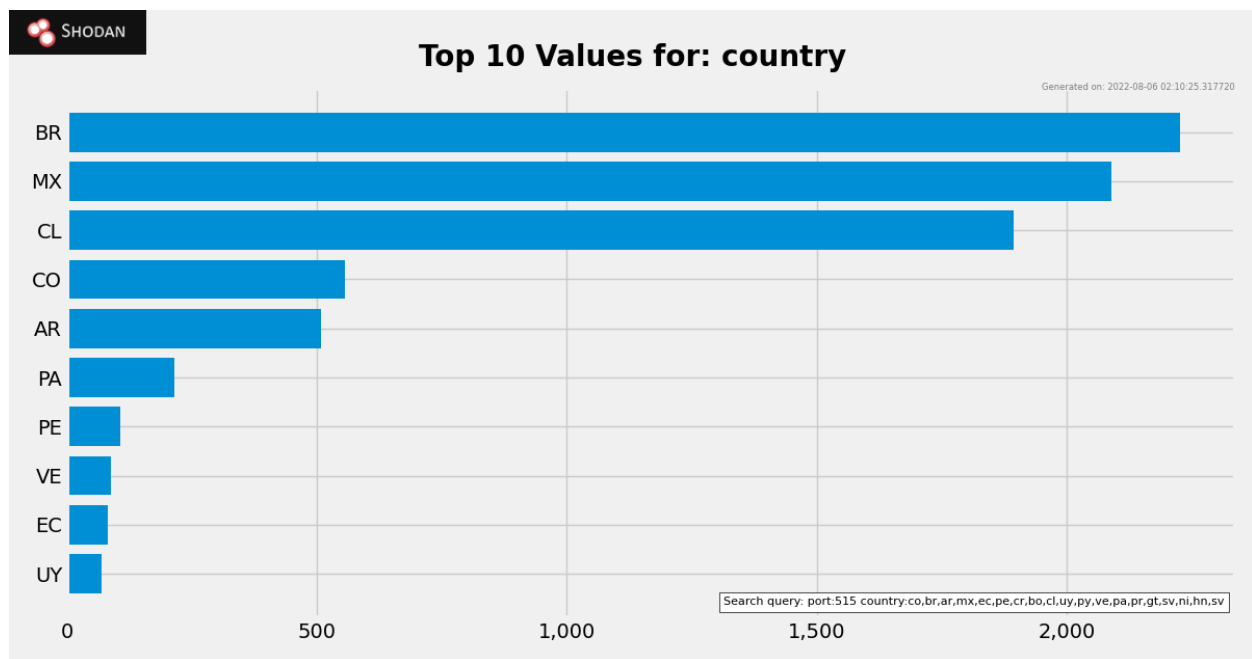
Report: Facet Analysis

Los productos destacados que se conectan al puerto 515 son lpd, Apache httpd, Microsoft HTTPAPI httpd. Donde la vulnerabilidad más destacada es cve-2019-17567 donde el Apache HTTP Server versiones 2.4.6 a 2.4.46 mod_proxy_wstunnel configurado en una URL que no está necesariamente actualizada por el servidor de origen estaba tunelizando toda la conexión

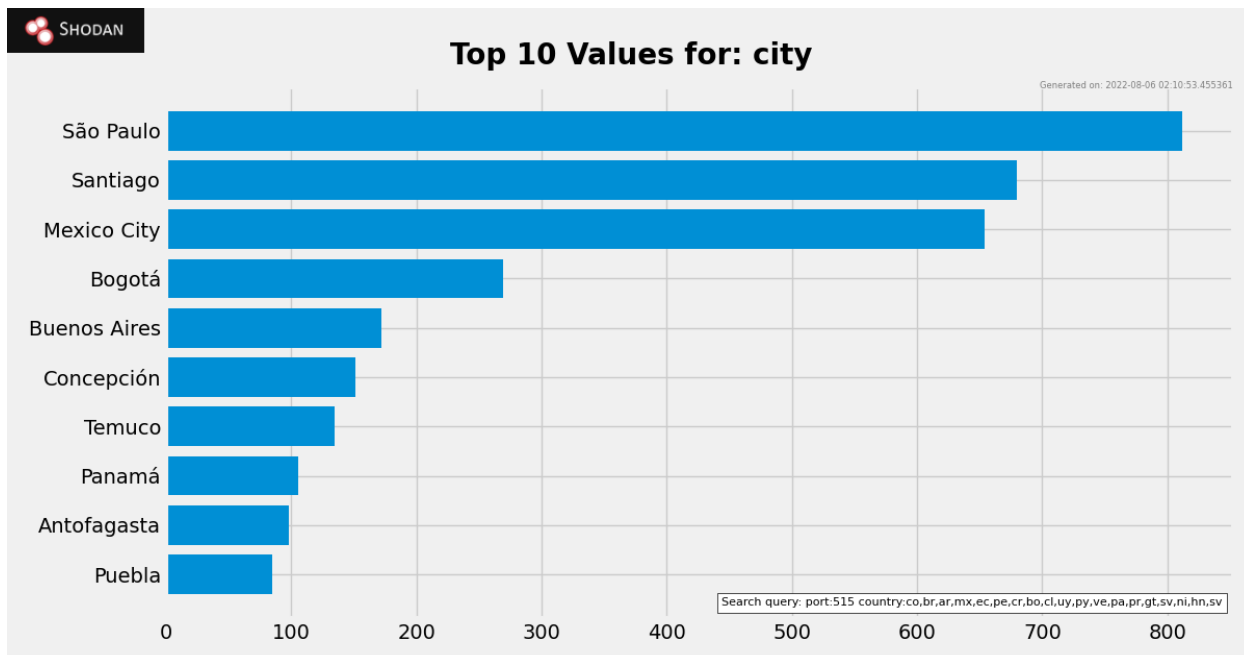
independientemente, lo que permitió que las solicitudes posteriores en la misma conexión pasaran sin validación HTTP, autenticación o autorización posiblemente configurada.

Colombia vs otros países de Latinoamérica

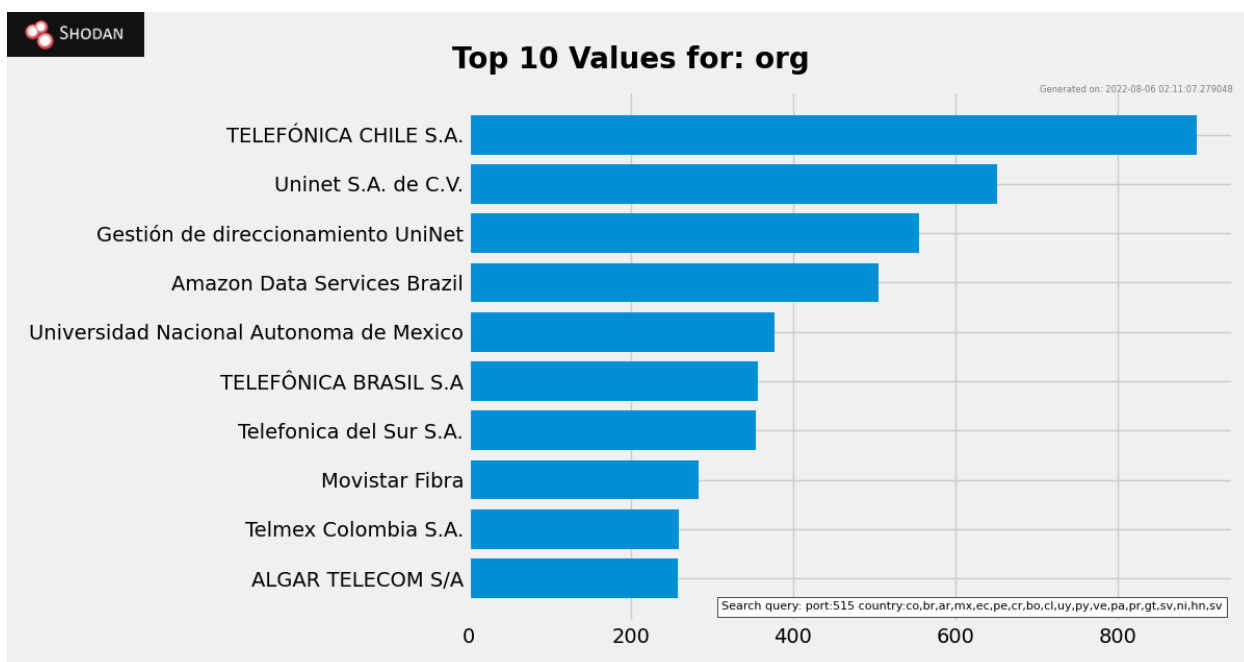
- `port:515 country:co,br,ar,mx,ec,pe,cr,bo,cl,uy,py,ve,pa,pr,gt,sv,ni,hn,sv`



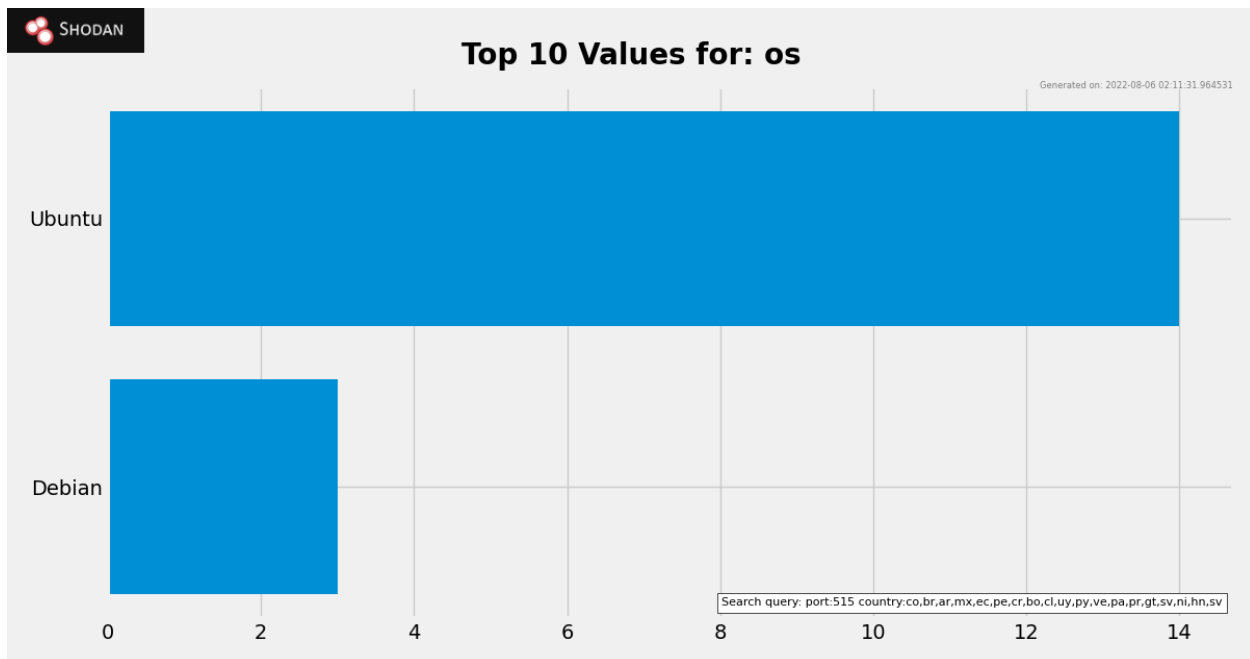
Report: Facet Analysis



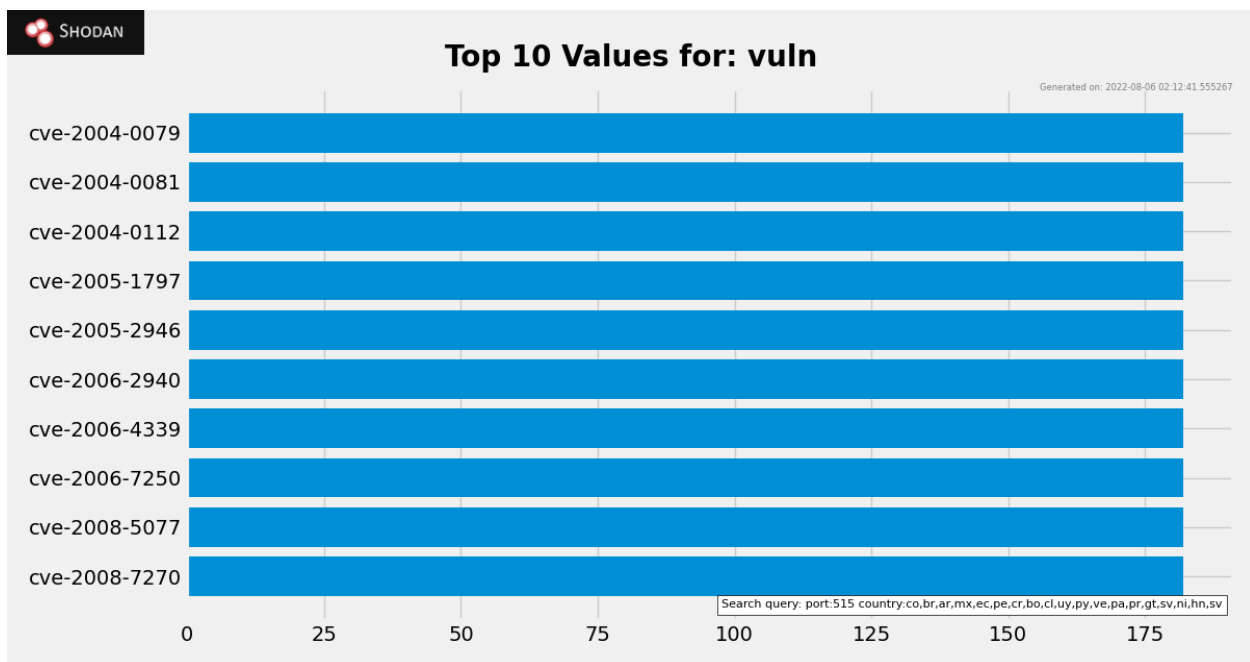
Report: Facet Analysis



Report: Facet Analysis



Report: Facet Analysis



Report: Facet Analysis

Para este caso, las empresas más destacadas con TELEFÓNICA CHILE S.A, Uninet S.A. de C.V y Gestión de direccionamiento UniNet. Empresas de conexiones y telecomunicaciones.

Los OS más expuestos son Ubuntu y Debian.

La vulnerabilidad cve-2004-0079 implica que la función `do_change_cipher_spec` en OpenSSL 0.9.6c a 0.9.6k, y 0.9.7a a 0.9.7c, permite a atacantes remotos provocar una denegación de servicio (bloqueo) a través de un protocolo de enlace SSL/TLS diseñado que desencadena una desreferencia nula.

4. Remote Desktop Protocol (RDP)

RDP es un protocolo desarrollado por Microsoft Windows. Proporciona al usuario una interfaz gráfica para conectarse a otra computadora a través de una conexión de red. Nuestro objetivo ahora es investigar en Shodan cuántas computadoras en Latinoamérica ejecutan el software de servidor RDP, observando organizaciones y productos que lo utilizan, entre otros datos importantes.

Colombia

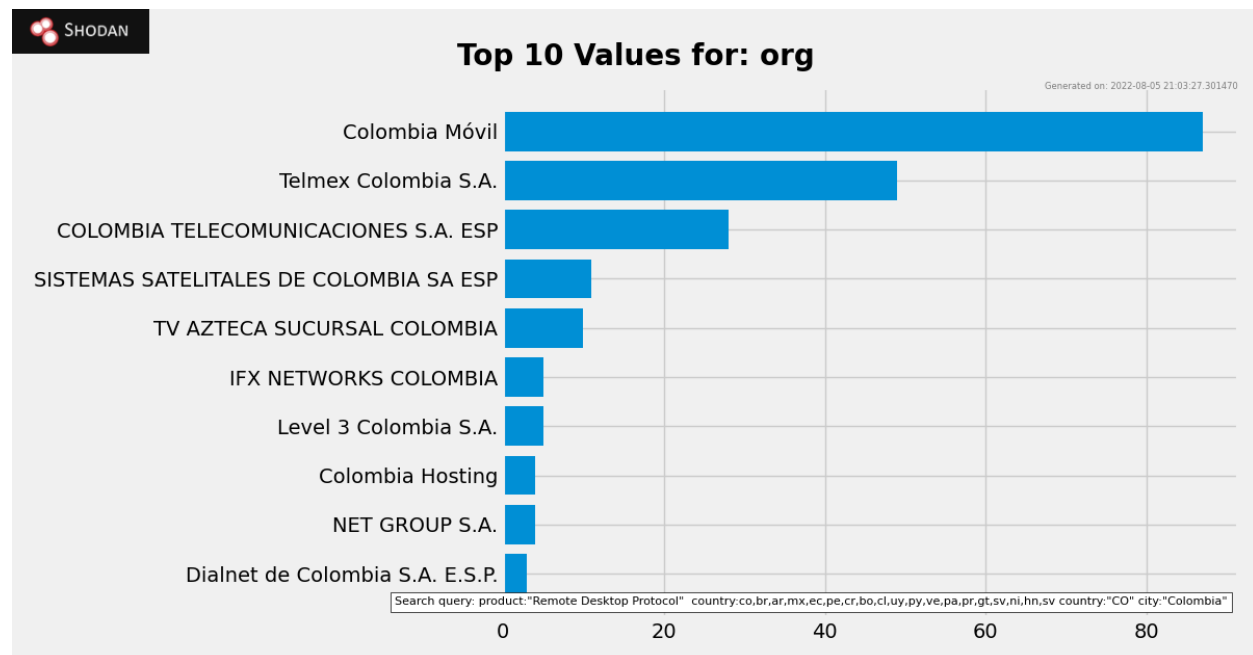


```
product:"Remote Desktop Protocol" country:co
```

Total de resultados: 242.

Ciudad principal: Bogotá.

Top 10 de organizaciones en Colombia:



Nuevamente observamos que todos los sistemas operativos utilizados son versiones de Windows. Encontramos por ejemplo en Colombia Móvil una máquina activa, junto con información sobre su *Target Name*. También se ve que no han realizado las actualizaciones de Windows. Sabemos en que parche están y por tanto sabemos las vulnerabilidades de las cuales no están protegidos. En caso de tener el usuario y contraseña, también sería posible ingresar a la computadora. Se observan otros datos importantes, como el hecho de que están usando Diffie-Hellman Fingerprint, RFC2409/Oakley Grupo 2 para generar las claves secretas.

181.204.46.106

Static-BA-181-204-46-1
06.figoune.com.co

Colombia Móvil



Colombia, Colombia

self-signed

SSL Certificate

Issued By:

- Common Name:

WIN-QSN7THU1T47

Issued To:

- Common Name:

WIN-QSN7THU1T47

Supported SSL

Versions:

TLSv1, TLSv1.1,

TLSv1.2

Diffie-Hellman

Fingerprint:

RFC2409/Oakley

Group 2

Remote Desktop Protocol NTLM Info:

OS: Windows 8.1/Windows Server 2012 R2

OS Build: 6.3.9600

Target Name: WIN-QSN7THU1T47

NetBIOS Domain Name: WIN-QSN7THU1T47

NetBIOS Computer Name: WIN-QSN7THU1T47

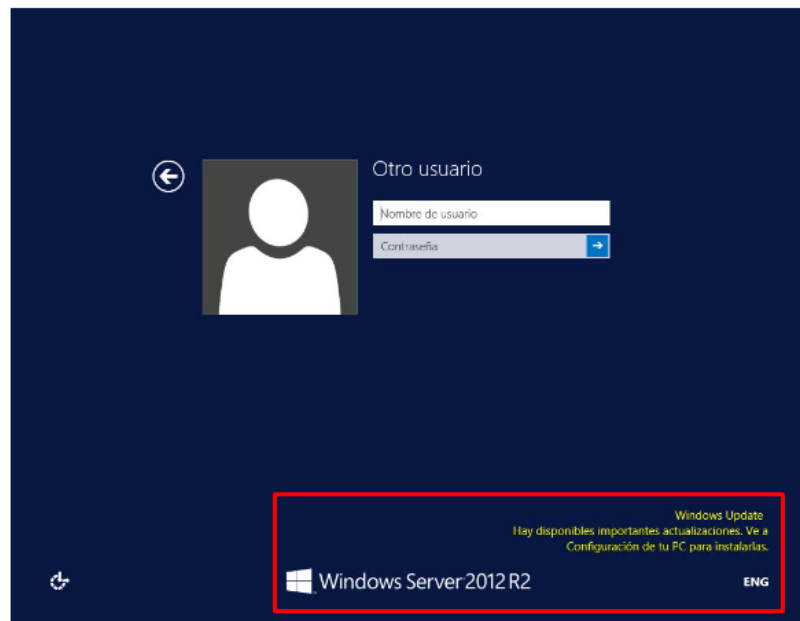
DNS Domain Name: WIN-QSN7THU1T47

FQDN: WIN-QSN7THU1T47

Otro usuario

Contraseña

Windo...



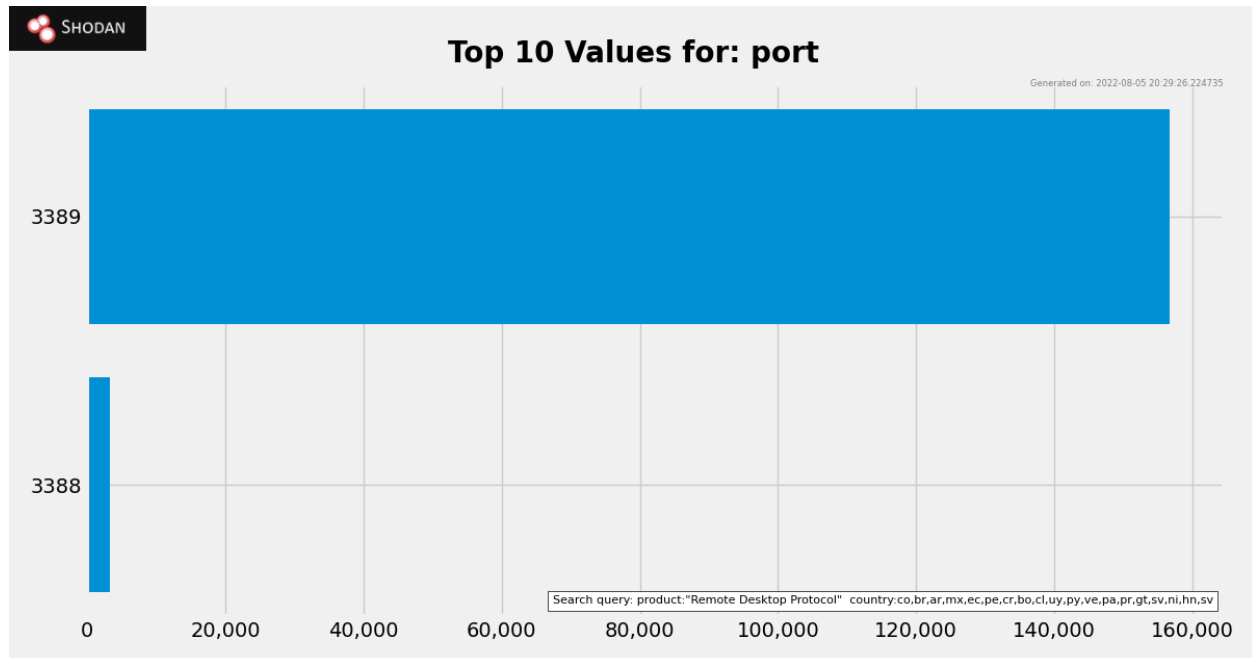
Colombia vs otros países de Latinoamérica



product:"Remote Desktop Protocol"

country:co,br,ar,mx,ec,pe,cr,bo,cl,uy,py,ve,pa,pr,gt,sv,ni,hn,sv

El total resultados en Latinoamérica es de **159,957**.



Puertos más utilizados en el Remote Desktop Protocol

Como observamos, el puerto abierto mas común es el 3389. Este puerto es el que permite una comunicación bidireccional con la cual se puede realizar el control remoto hacia la otra computadora. En el primer resultado podemos encontrar de forma más ampliada lo importante que es el puerto TCP 3389 en RDP:

Remote Desktop Protocol

Remote Desktop Protocol NTLM Info:

OS: Windows 10/Windows Server 2019

OS Build: 10.0.17763

Target Name: BRUCE

NetBIOS Domain Name: BRUCE

NetBIOS Computer Name: RDP

DNS Domain Name: bruce.local

DNS Tree Name: bruce.local

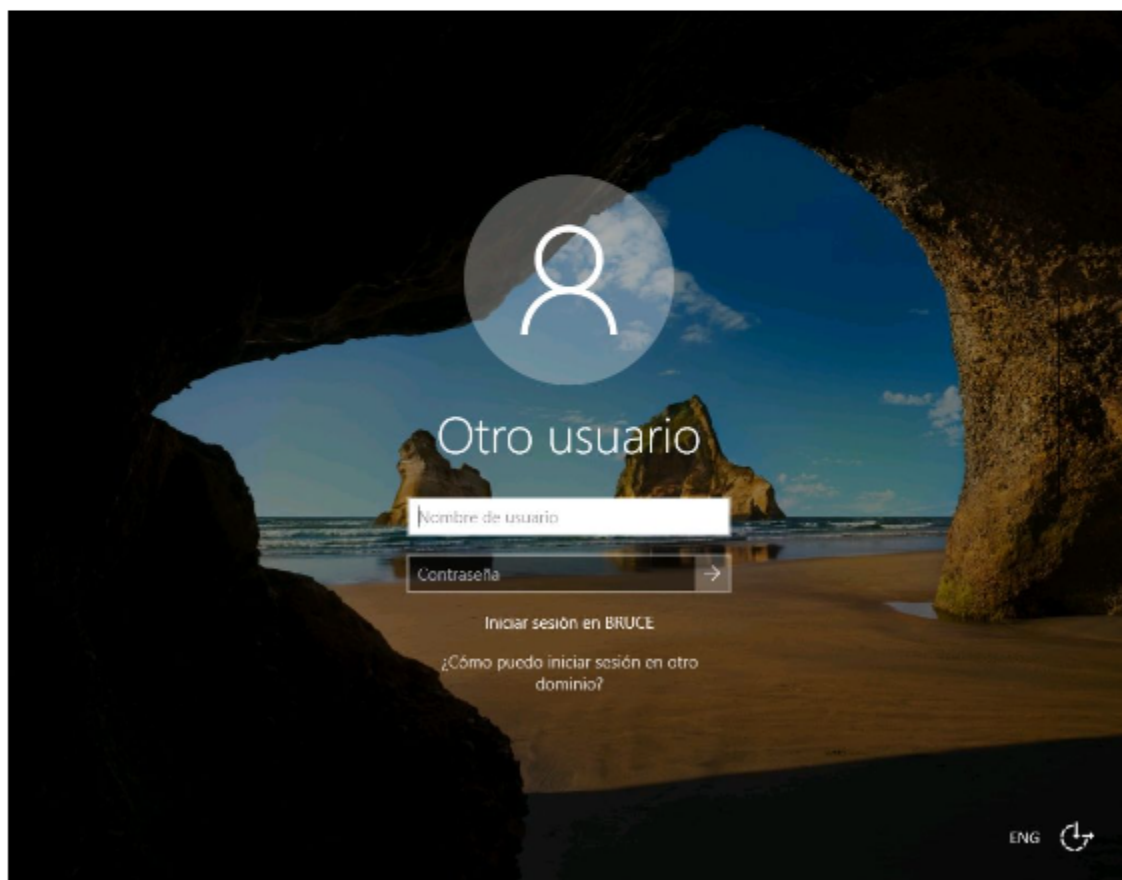
FQDN: RDP.bruce.local

- Otro usuario

Contraseña

Iniciar sesión en BRUCE

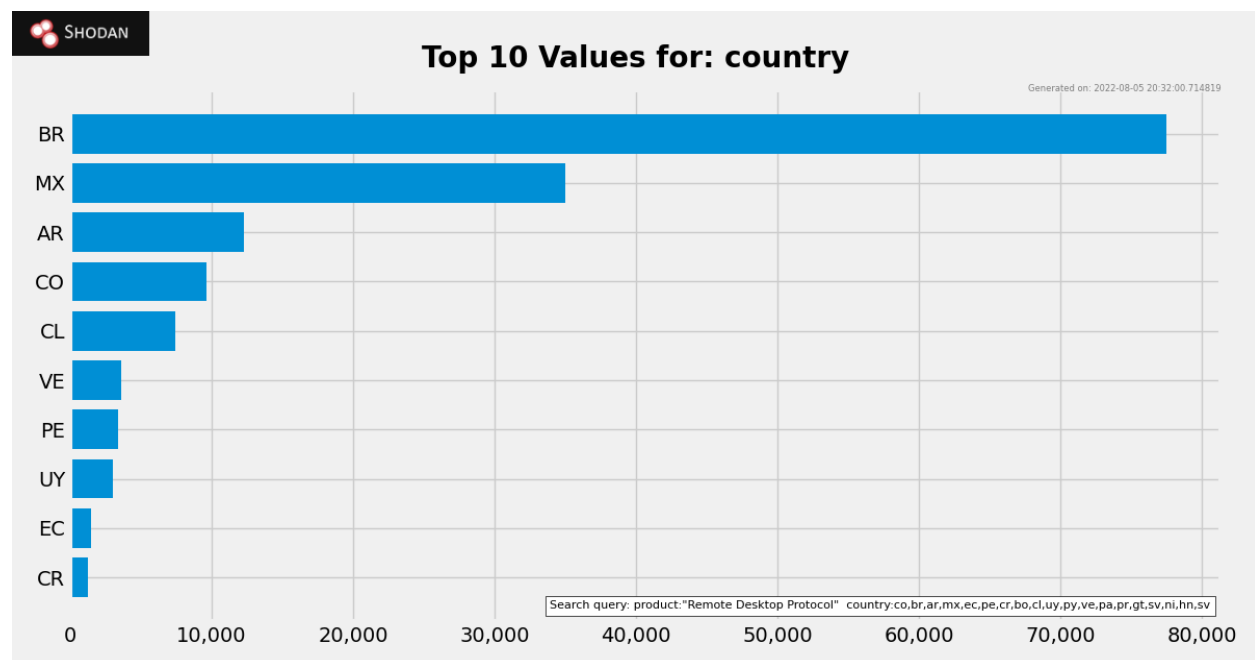
¿Cómo puedo iniciar sesión en otro dominio?



También observamos que en los resultados se encuentra visible el *target name*, con el cual podemos realizar un escaneo de red completo.

El top de sistemas operativos siempre está entre diversas versiones de *Windows* ya que sólo en este sistema funciona el RDP.

Observamos el top 10 de países que usan el RDP, en donde se ve que Colombia ocupa el cuarto lugar. Con respecto a los demás países se encuentran resultados balanceados a excepción de Brasil y México, los cuales cuentan con mayor población.



Top 10 países de américa latina con remote desktop protocol

5. MongoDB Puerto 27017

MongoDB es una herramienta que almacena datos en documentos flexibles, de manera que los campos pueden variar entre documentos y la estructura de datos cambiar con el tiempo.

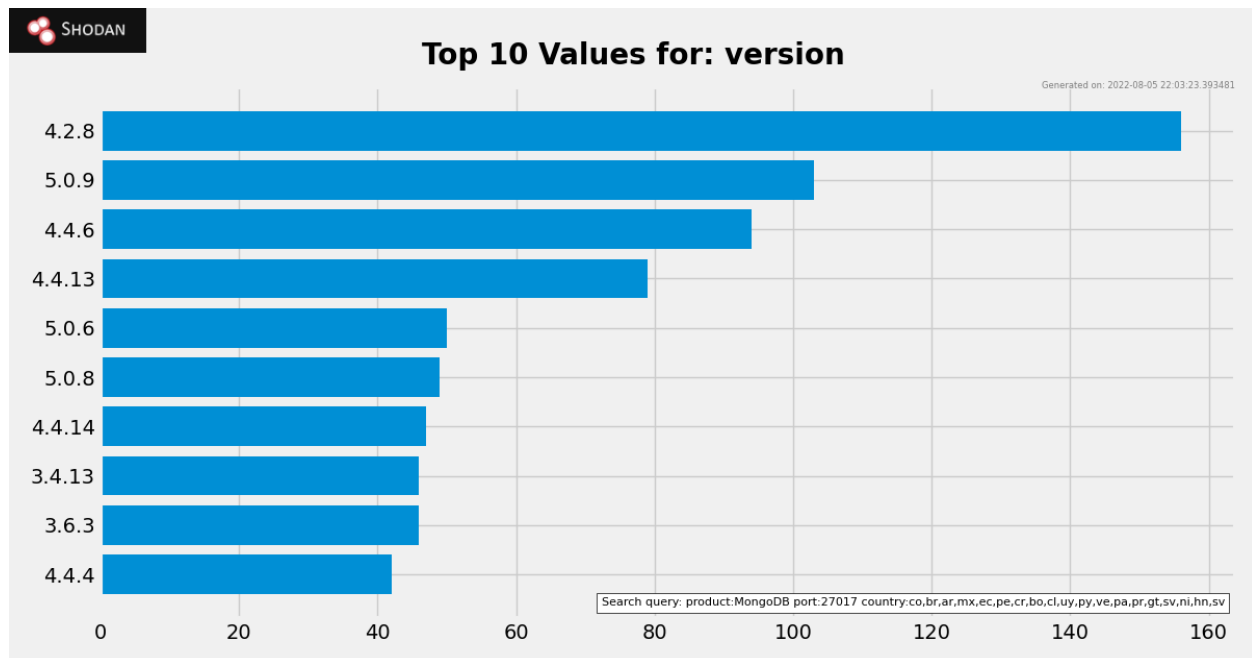
Investigaremos en Shodan los países de Latinoamérica que utilizan el producto: MongoDB y el puerto 27017, el cual es el puerto que MongoDB utiliza por defecto.



```
product:MongoDB port:27017  
country:co,br,ar,mx,ec,pe,cr,bo,cl,uy,py,ve,pa,pr,gt,sv,ni,hn,sv
```

Total de resultados: 2,766.

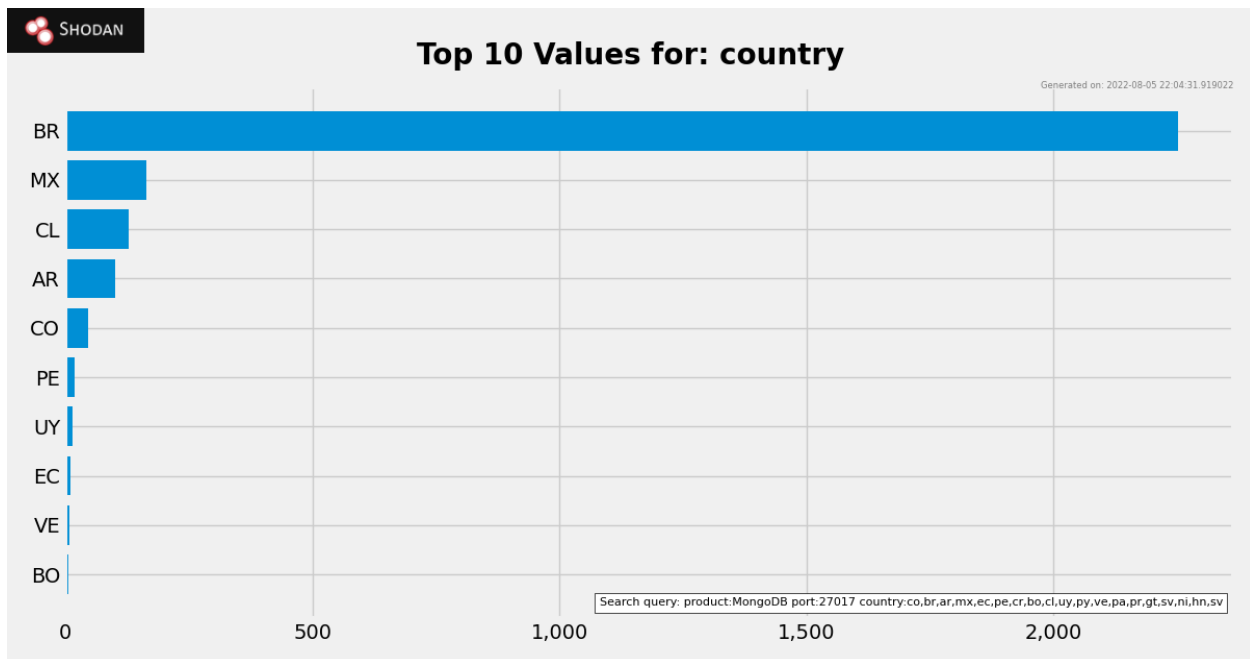
Observamos que la versión de MongoDB más utilizada es la 4.2.8.



Top 10, versiones de MongoDB mas frecuentes.

Colombia vs otros países de Latinoamérica

Sólo encontramos 47 máquinas que utilizan MongoDB en Colombia. Esto es relativamente parejo comparado con los demás países de Latinoamérica y exceptuando Brasil. Este país tiene mucha población por lo cual es normal que presente siempre más datos que los demás.



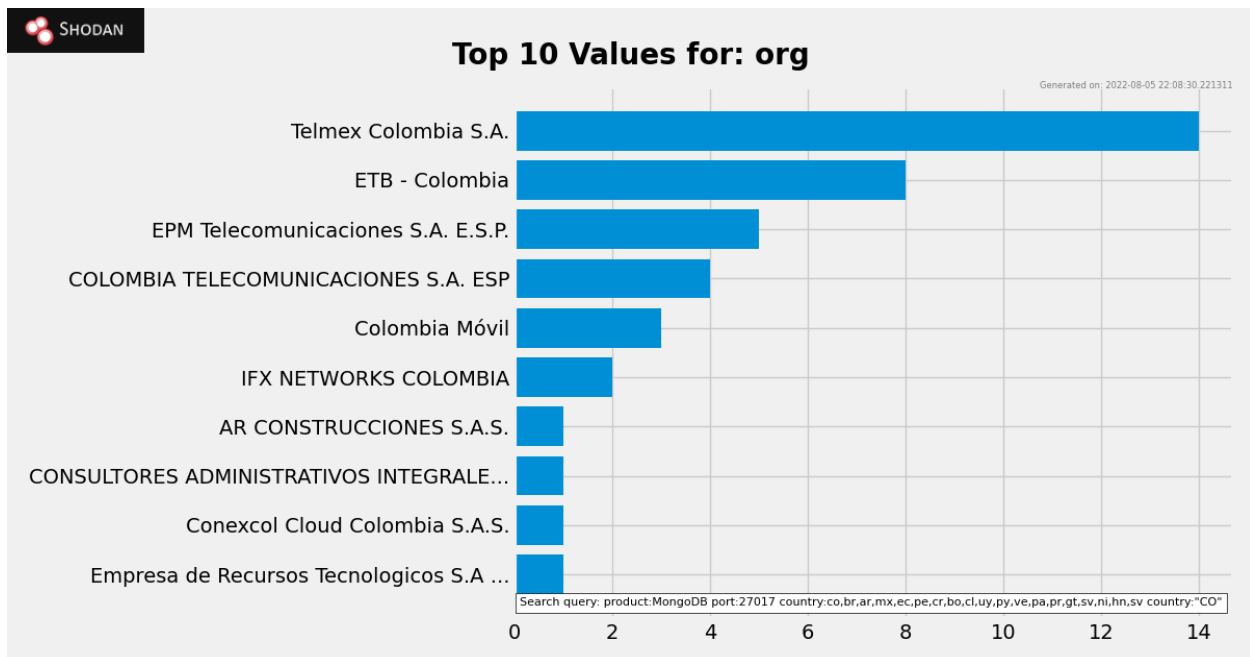
Top 10, países que utilizan MongoDB

Colombia

Total resultados: 47.

Ciudad principal: Bogotá.

Observamos que Telmex y ETB son las organizaciones que más destacan en MongoDB Colombia.



Top 10 organizaciones en Colombia que utilizan MongoDB.

Observando el puerto 27017 podemos observar la estructura de la base de datos de la empresa. Puede ser que encontremos información sensible. Esta es una muestra del puerto en la empresa ETB - Colombia.

```
// 27017 / TCP -685216318 | 2022-07-30T12:14:26.893599

MongoDB 4.2.6

MongoDB Server Information
{
  "process": "C:\\Program Files\\MongoDB\\Server\\4.2\\bin\\mongod.exe",
  "pid": 4384,
  "connections": {
    "current": 1,
    "available": 999999,
    "active": 1,
    "totalCreated": 505
  },
}
```

Shodan nos muestra además las vulnerabilidades que puede presentar debido a la falta de actualizaciones.

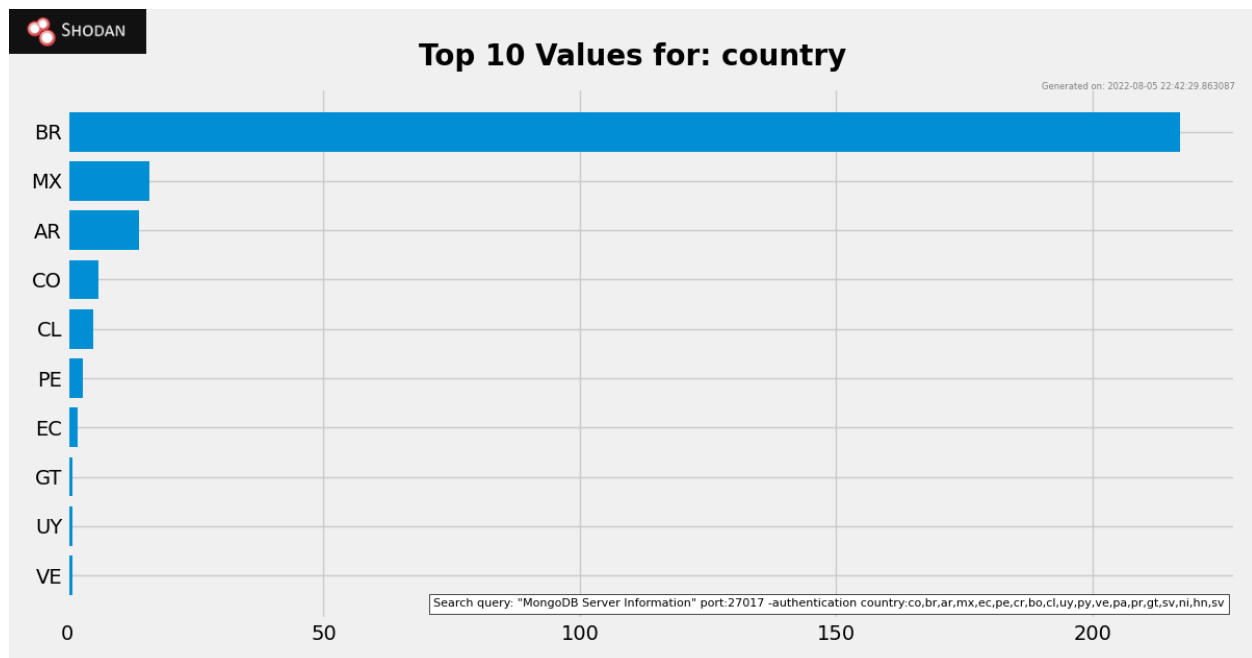
Cambiando el comando de búsqueda de MongoDB

Ahora cambiaremos ligeramente el comando de búsqueda de MongoDB, de manera que nos muestre una base de datos comprometida.



"MongoDB Server Information" port:27017 -authentication
country:co,br,ar,mx,ec,pe,cr,bo,cl,uy,py,ve,pa,pr,gt,sv,ni,hn,sv

Total de resultados: 266.



Observamos sólo 6 resultados en Colombia. Las organizaciones con una base de datos de Mongo comprometida fueron: EPM Telecomunicaciones, Telmex, Colombia Movil, ETB.

Todos los resultados tienen el tag de “database compromised” con lo cual confirmamos que la integridad de la base de datos se encuentra en riesgo.

186.30.161.69

static-186-30-161-69.st
atic.etb.net.co

ETB - Colombia

Colombia, Bogotá



MongoDB Server Information

```
{
  "process": "C:\\Program Files\\MongoDB\\Server\\4.2\\bin\\mongod.exe",
  "pid": 4384,
  "connections": {
    "current": 1,
    "available": 999999,
    "active": 1,
    "totalCreated": 505
  },
  "locks": {
    "Database": {
      ...
    }
  }
}
```

6. Virtual Private Network (VPN)

Una VPN es una tecnología de red que genera conexión segura entre dos dispositivos a través de una red insegura como internet.

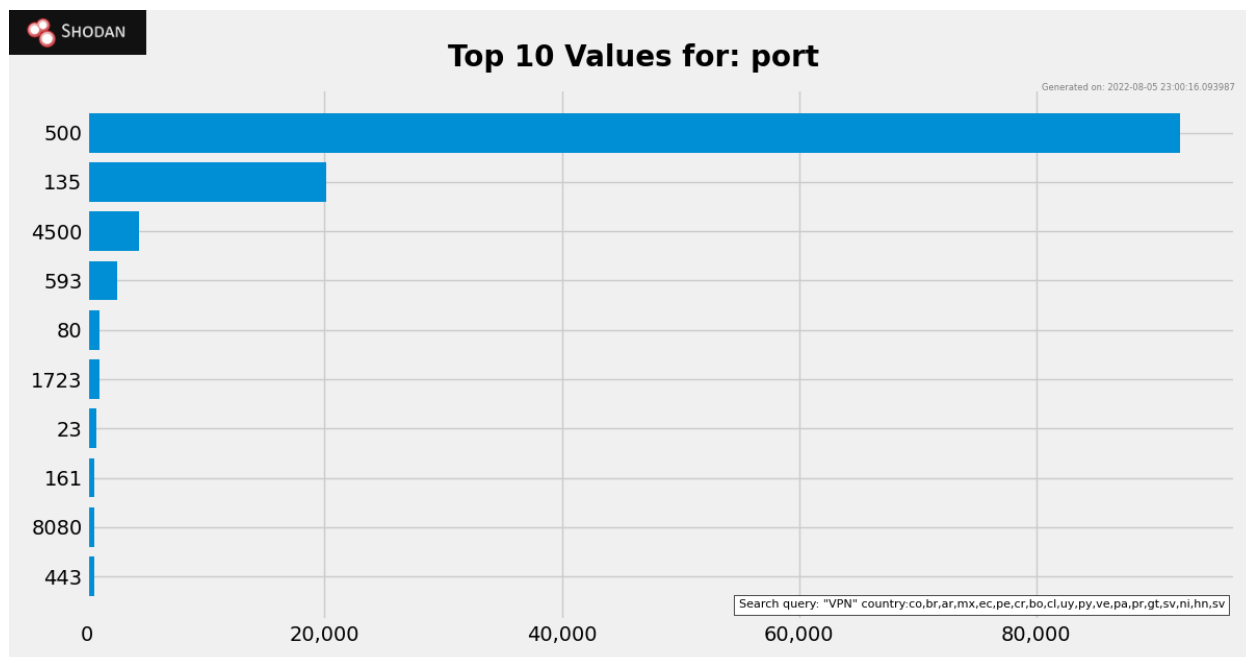
Observaremos los dispositivos con Virtual Private Network en toda latinoamérica. Para eso utilizamos el siguiente comando:



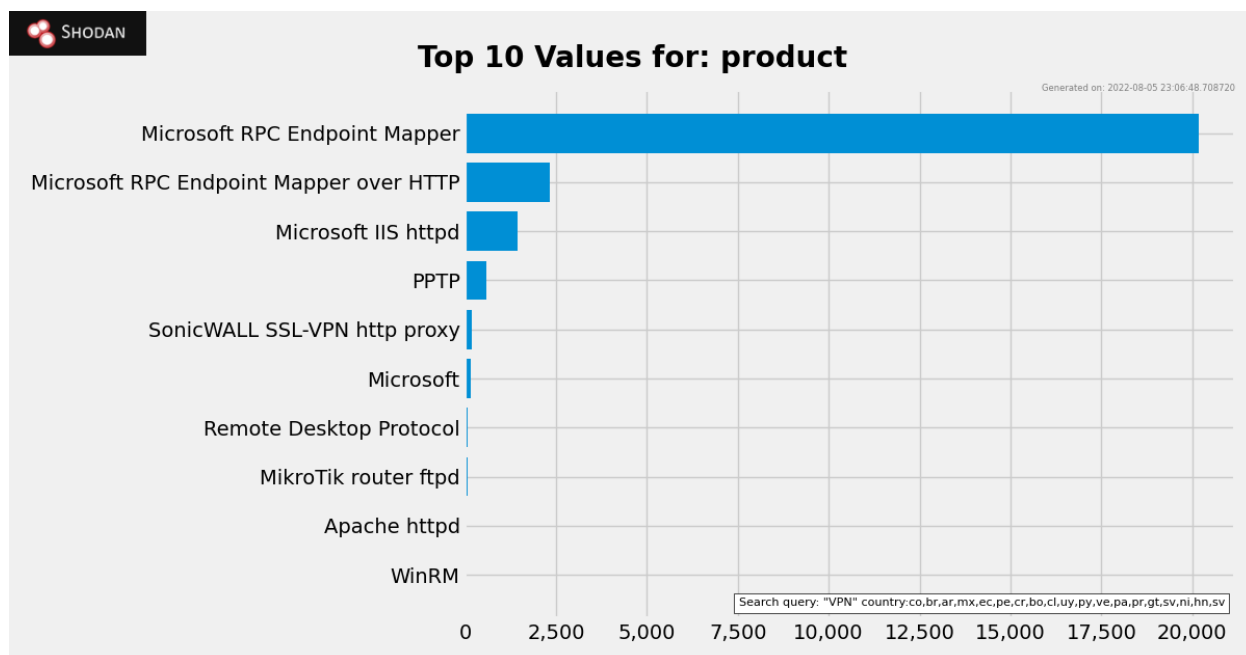
```
"VPN" country:co,br,ar,mx,ec,pe,cr,bo,cl,uy,py,ve,pa,pr,gt,sv,ni,hn,sv
```

Total de resultados: 205,615.

Observando el top de puertos, tenemos como resultado que los mas relevantes son el puerto 500 y puerto 135. El puerto 500 es utilizado por el protocolo de VPN IPsec para establecer la conexión. El segundo puerto mencionado cumple la misma función de comunicación cliente servidor RPC.



El producto que se encuentra más relacionado con el VPN es **Microsoft RPC Endpoint Mapper**, el cual permite determinar el número de puerto asignado a escuchar las llamadas a procedimientos remotos del cliente.



El sistema operativo a utilizar siempre varía en las versiones de MikroTik RouterOS, el cual es un software que logra convertir un PC en un router dedicado. Este dispositivo puede funcionar

como servidor de VPN, ya que todo el tráfico, incluyendo la navegación por internet sale por la red remota.

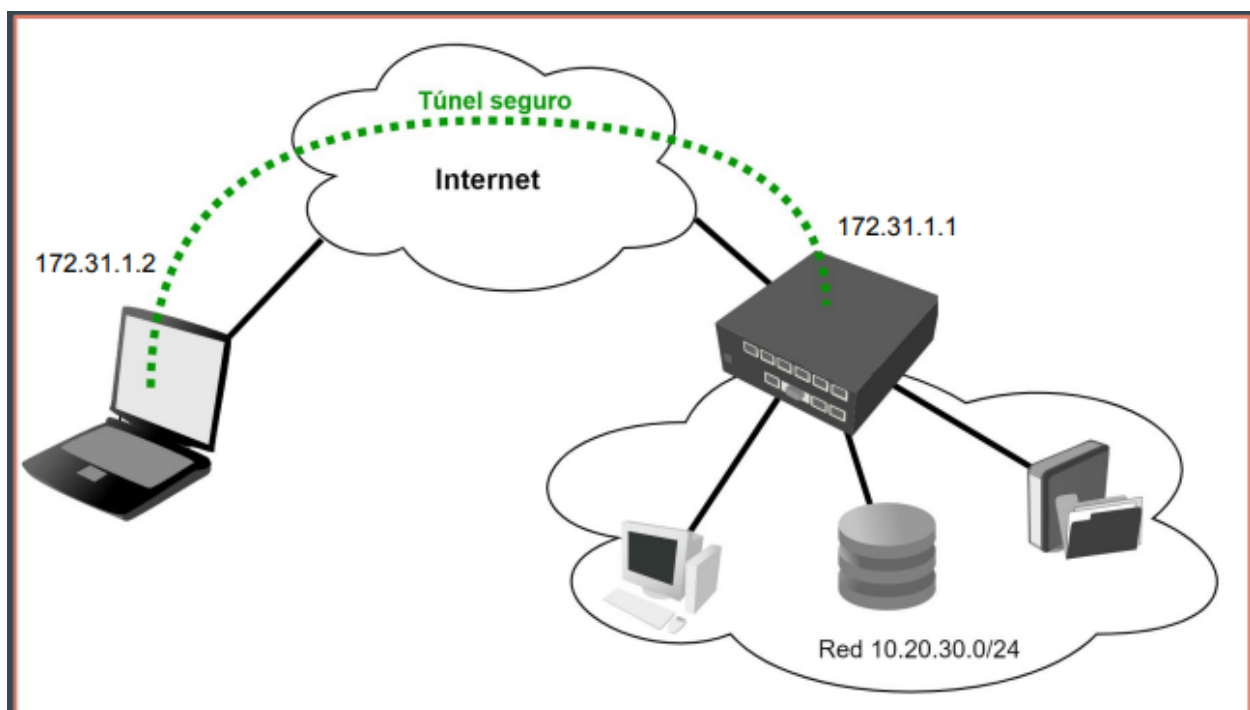
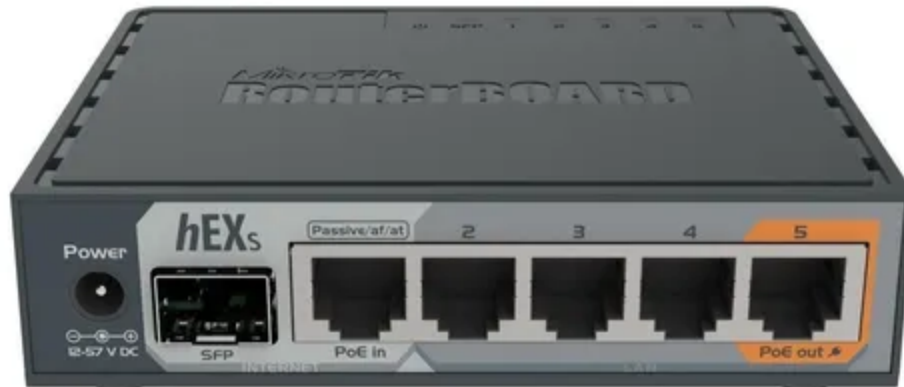
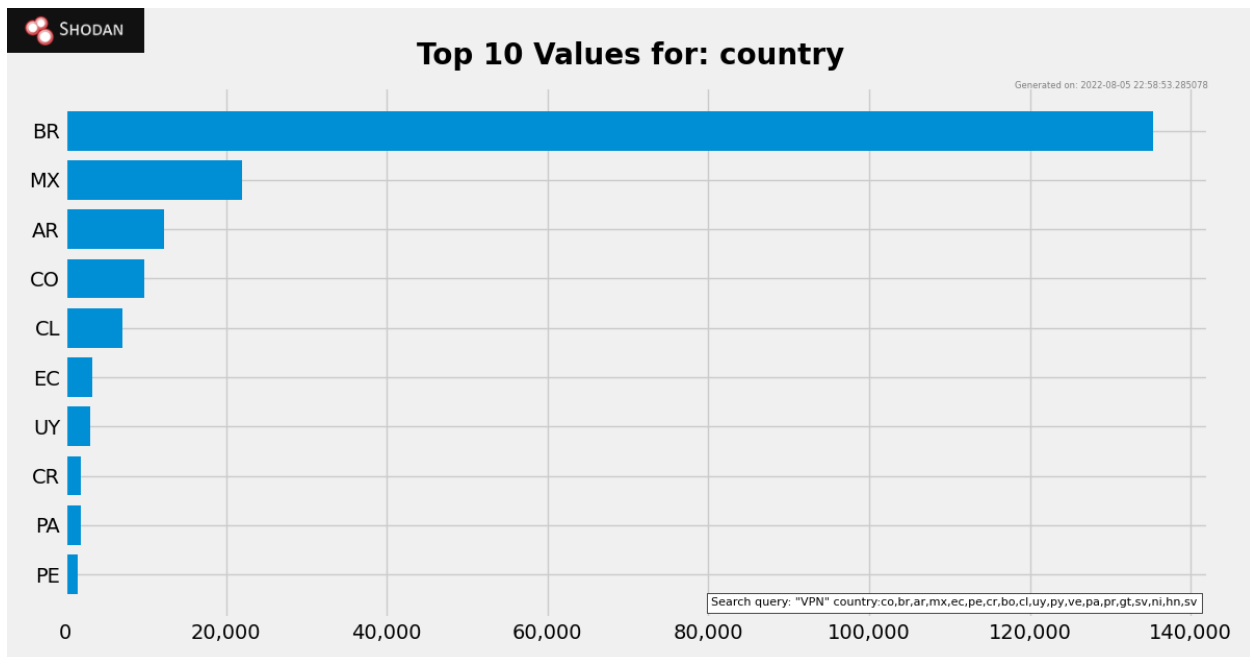


Imagen de: <https://www.prozcenter.com/wp-content/uploads/200327-VPNs-seguras-con-MikroTik-RouterOS.pdf>

Colombia vs otros países de Latinoamérica

Observando el top de países de Latinoamérica, Colombia se encuentra en el cuarto lugar y es relativamente parejo con los demás, a excepción de Brasil el cual tiene mucha población.



Colombia

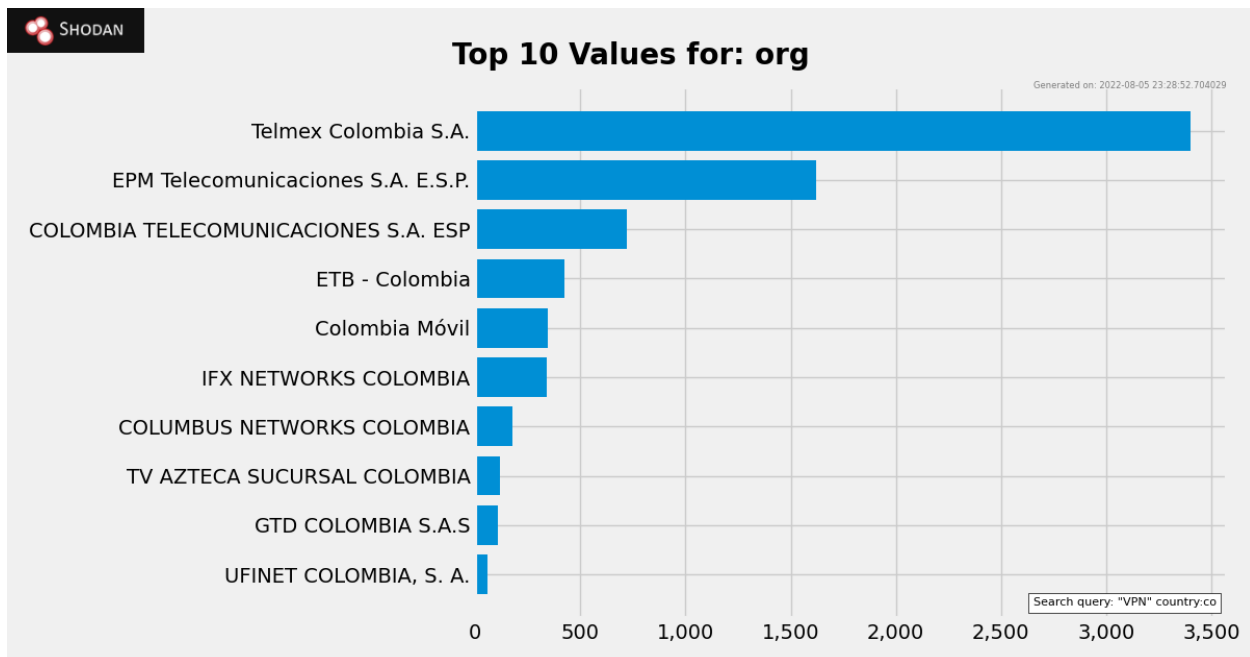


"VPN" country:co

En Colombia obtenemos que las principales ciudades que utilizan VPN son Bogotá y Medellín, con datos de 5,537 y 1,239 respectivamente.

Los puertos más relevantes siguen siendo los mismos, el puerto 500 con popularidad de 7,278 y el puerto 135 con 1,855.

Este es el ranking de organizaciones que utilizan VPN, en donde encontramos nuevamente en el top a empresas como Telmex, EPM Telecomunicaciones, ETB y Colombia Móvil.



En el top de productos, el único relevante es **Microsoft RPC Endpoint Mapper**, cuya función fue explicada anteriormente.

Al observar detenidamente el puerto 500 UDP, encontramos información importante, tales como la clave del Initiator SPI y Responder SPI, la versión utilizada, y sabemos que no tiene una encriptación y autenticación.

```
// 500 / UDP

VPN (IKE)

Initiator SPI: 6a6d6b6674636177
Responder SPI: 6e776f6332763967
Next Payload: RESERVED
Version: 2.0
Exchange Type: DOI Specific Use
Flags:
  Encryption:      False
  Commit:          False
  Authentication:  False
Message ID: 00000000
Length: 36
```

7. Minerías de Ethereum (ETH)

Ethereum es la plataforma digital con tecnología de Blockchain. Ether es su criptomoneda nativa y es la segunda más grande del mercado.

El siguiente dock cumple la función de buscar todas las minerías de Ethereum en Latinoamérica.

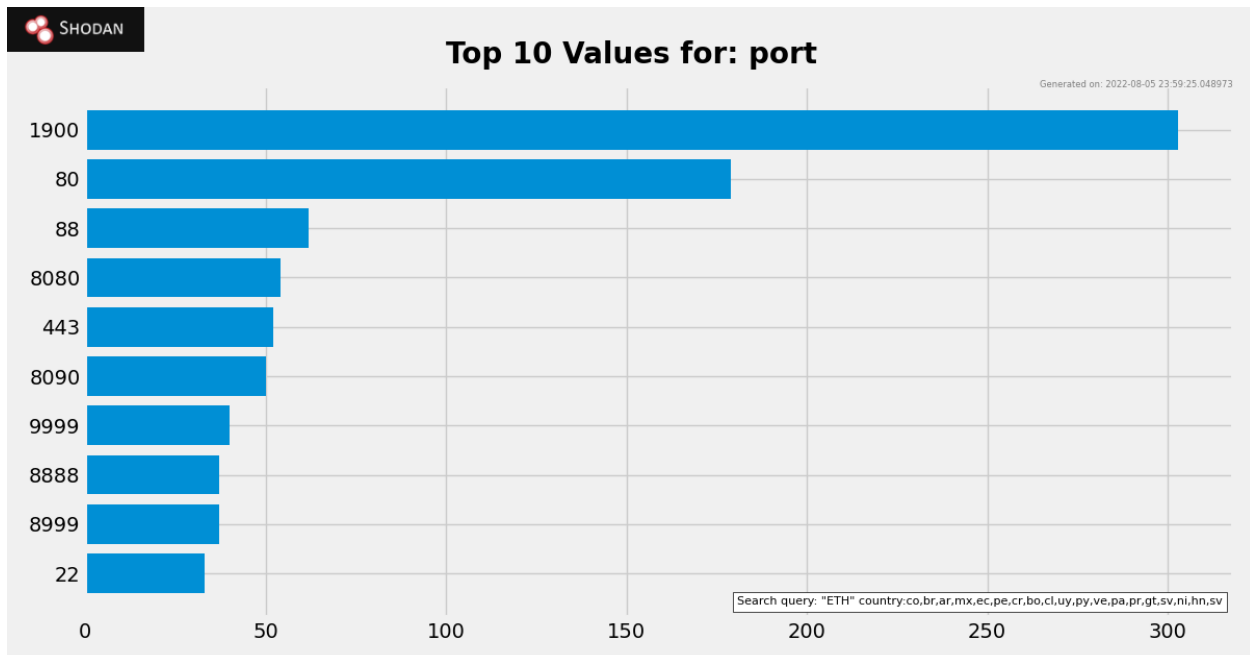


```
"ETH" country:co,br,ar,mx,ec,pe,cr,bo,cl,uy,py,ve,pa,pr,gt,sv,ni,hn,sv
```

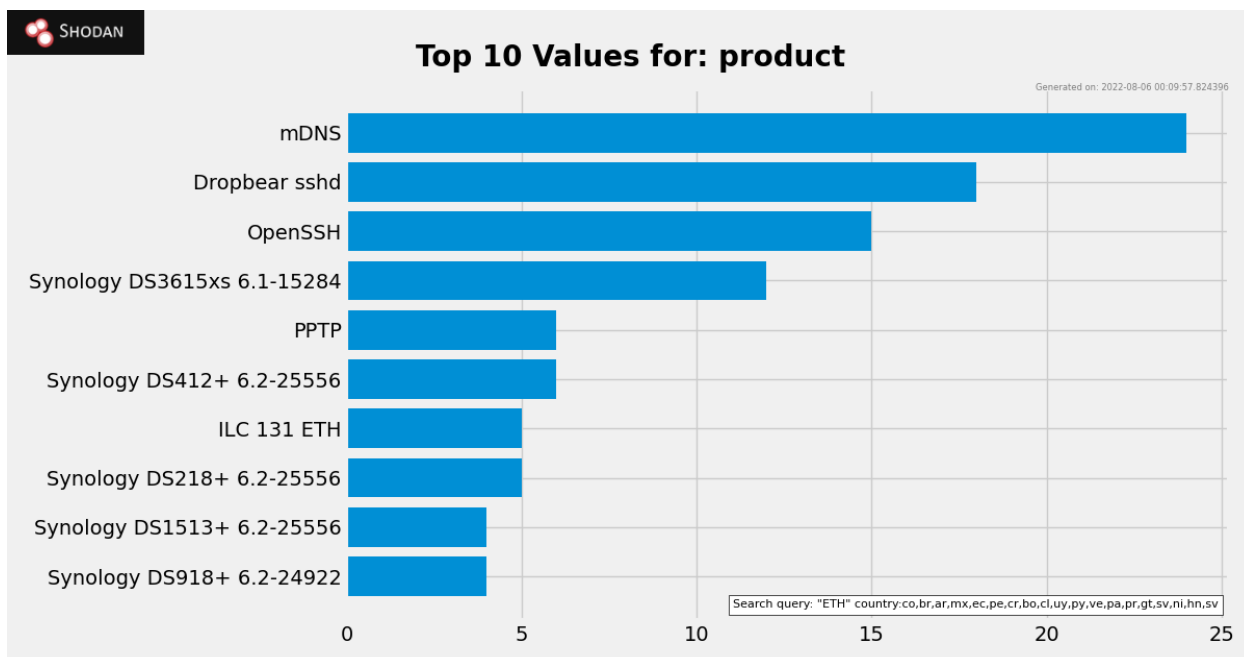
Total resultados: 1,225.

Top de los puertos más utilizados:

- **Puerto 1900:** Garantiza la entrega de paquetes de datos en la misma orden en que fueron mandados.
- **Puertos: 80, 8080, 8888, 443:** Son puertos orientados a web. Al estar abiertos pueden permitir ataques web como de inyección SQL, XSS, entre otros. Todos estos puertos son conocidos por ser utilizados para la minería de criptomonedas.



Top de productos utilizados para la minería de ETH:

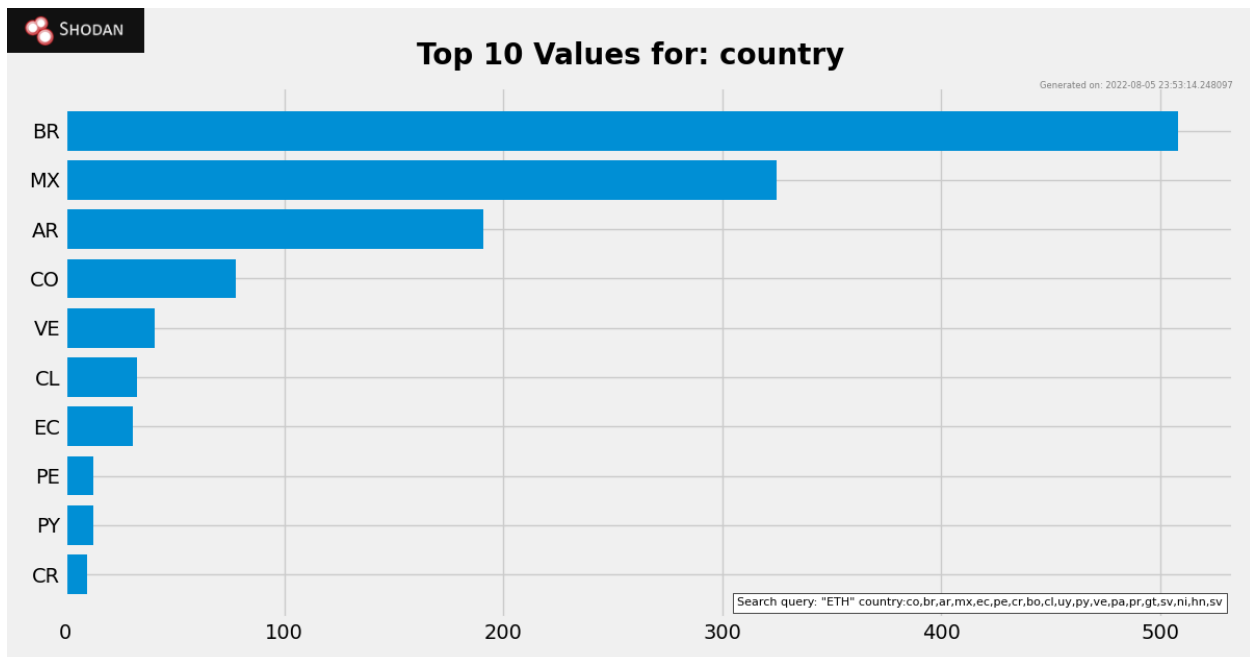


- **mDNS:** El protocolo DNS de multidifusión se encarga de que todos los dispositivos de red del mismo enlace local realicen funciones DNS estándar.
- **OpenSSH:** Nos proporciona un canal seguro sobre una red insegura en una arquitectura cliente-servidor. Dropbear sshd funciona de la misma manera.
- **Synology DiskStation DS3615xs:** Diseñado para servir a las empresas a gran escala que desean configurar un servidor integral y al mismo tiempo conservar la opción de expandir sus capacidades de almacenamiento en el futuro. Es el disco duro ideal para guardar datos confidenciales, función necesaria al realizar una minería de criptomonedas.



Colombia vs otros países de Latinoamérica

Colombia es el cuarto país en Latinoamérica que tiene minerías de ETH, además no se encuentra una diferencia relevante en comparación a los demás países.



El top de sistemas operativos tanto en Colombia como en los demás países se basa en versiones de Mikrotik RouterOS, el cual como vimos anteriormente también es utilizado para funcionar como VPN. Esta es una función importante dentro de las minerías de criptomonedas.

Colombia

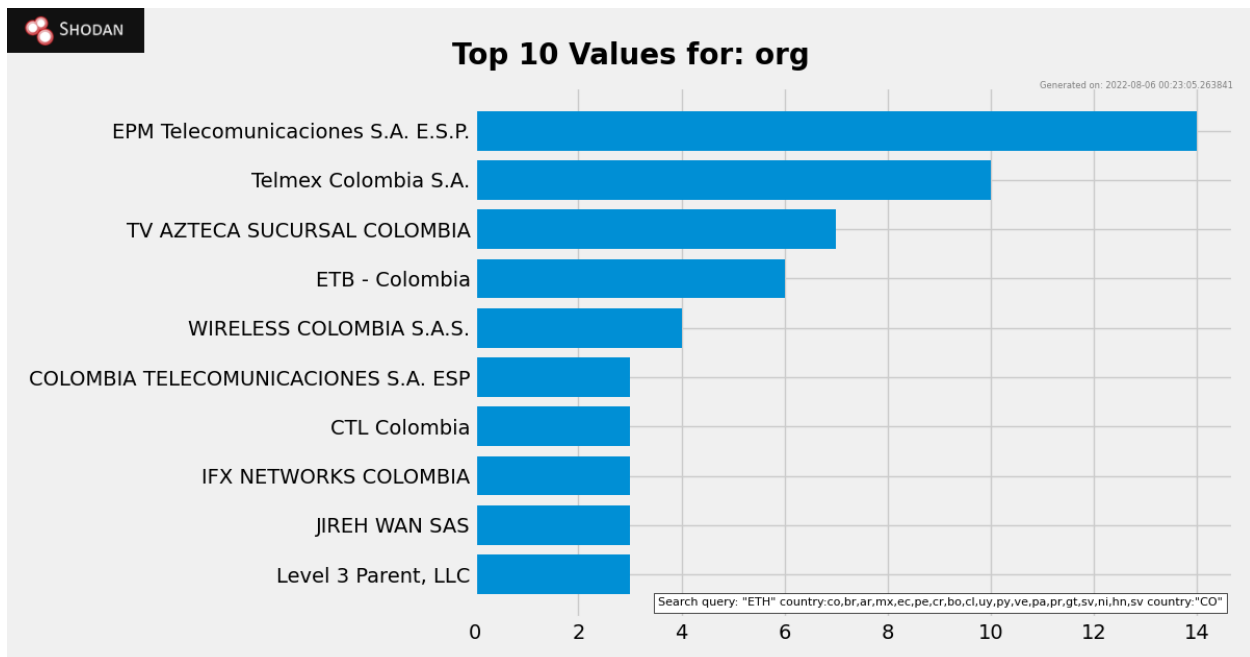
Total de resultados: 77.

Ciudad principal: Bogotá.

Top puertos: 1900, 80, 8082.

Top de productos: OpenSSH y dispositivos Synology.

Top de organizaciones:



8. Dispositivos con Windows 7

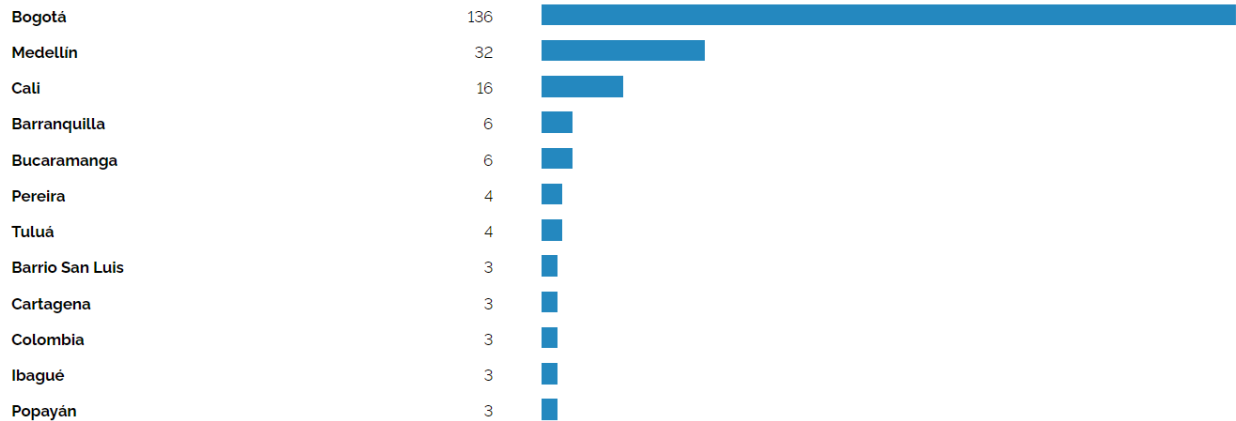


OS:"windows 7"

- Windows 7 es una versión de Microsoft Windows, línea de sistemas operativos producida por Microsoft Corporation. Se lanzó en octubre de 2009. Esta versión estaba diseñada para uso en PC, incluyendo equipos de escritorio en hogares y oficinas, equipos portátiles, tabletas, netbooks y equipos multimedia.

Colombia

- OS:"windows 7" country:co

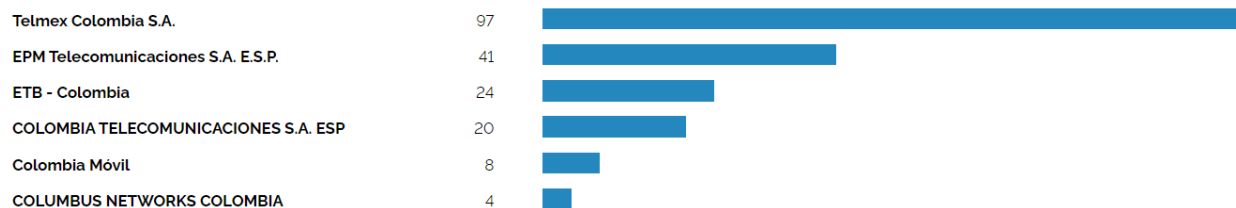


Analizando el top de ciudades de Colombia podemos observar que las ciudades con mayor dispositivos con win7 son aquellas más pobladas y principales del país, aquí podemos observar un poco la desigualdad y en parte la poca cobertura del país al resto de ciudades.

TOP PORTS

3389	156
445	101
3388	3

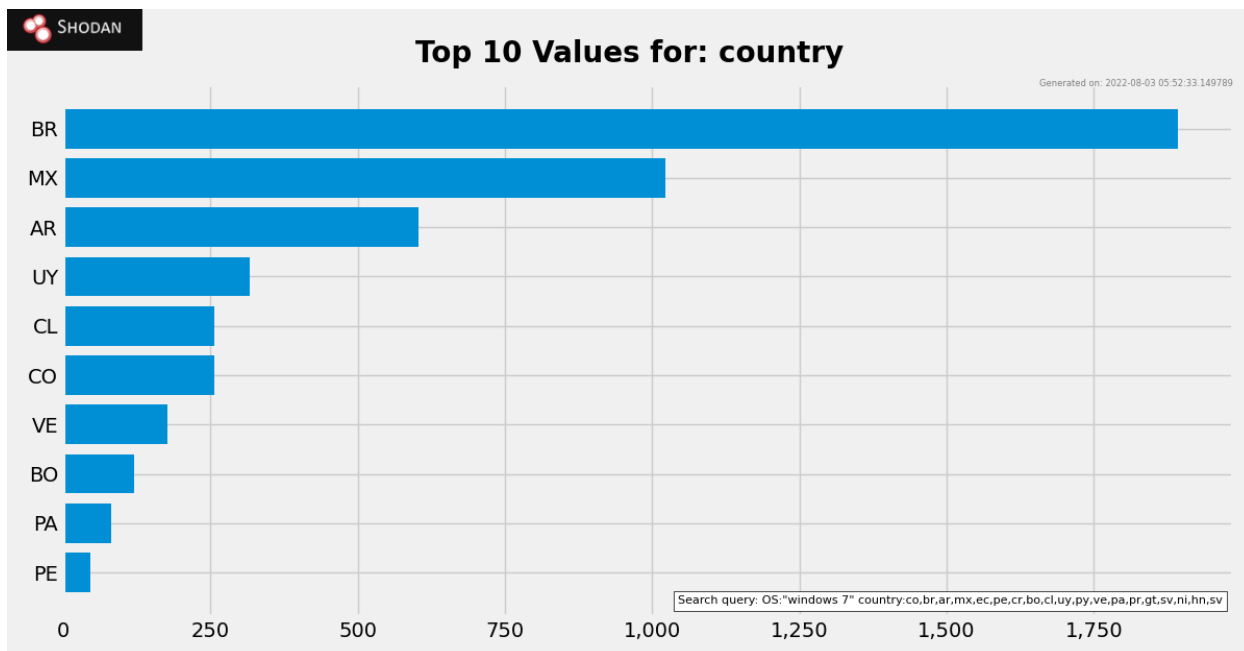
El puerto más expuesto es el 3389 es el puerto que usa el escritorio remoto de Windows, muy recomendable cambiarlo como podemos ver. teniendo esto en cuenta podemos decir que aquellos dispositivos de escritorio son los más expuestos.



Por ultimo como dato adicional y curioso es que otra vez la compañía Telmex aparece como top 1, nos da a entender que es de las organizaciones menos seguras y que expone más a sus usuarios

Colombia vs otros países de Latinoamérica

- OS: "windows 7" country:co,br,ar,mx,ec,pe,cr,bo,cl,uy,py,ve,pa,pr,gt,sv,ni,hn,sv



Dejando atrás a países con como MX y BR que son demasiado poblados, podríamos decir que Argentina es el país que esta un poco más desactualizado referente a Sistemas Operativos, y también que es de el más expuesto, mientras que Colombia se mantiene en un buen promedio estando más seguro y no tan atrasado con referencia a sus vecinos.



top de las organizaciones que más exponen a sus usuarios.



Por ultimo, algo curioso es que Montevideo es la ciudad con más dispositivos vulnerables, ganando a la ciudades con más de el triple de habitantes. respecto a Colombia, su capital es la 6

ciudad más expuesta.

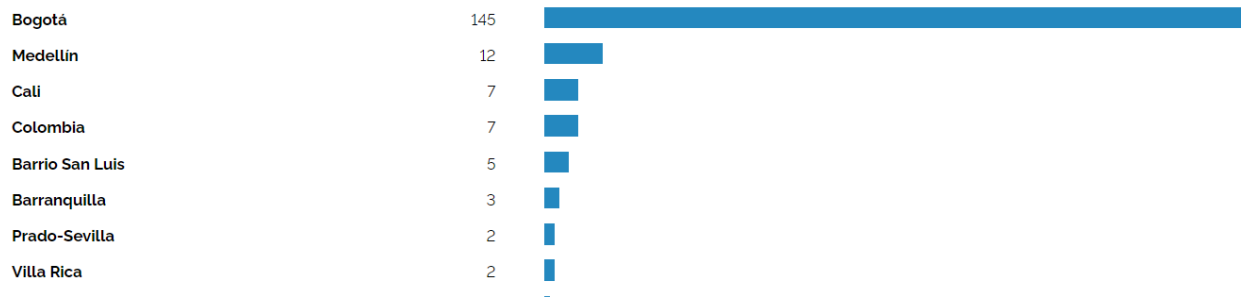
9. Outlook web app



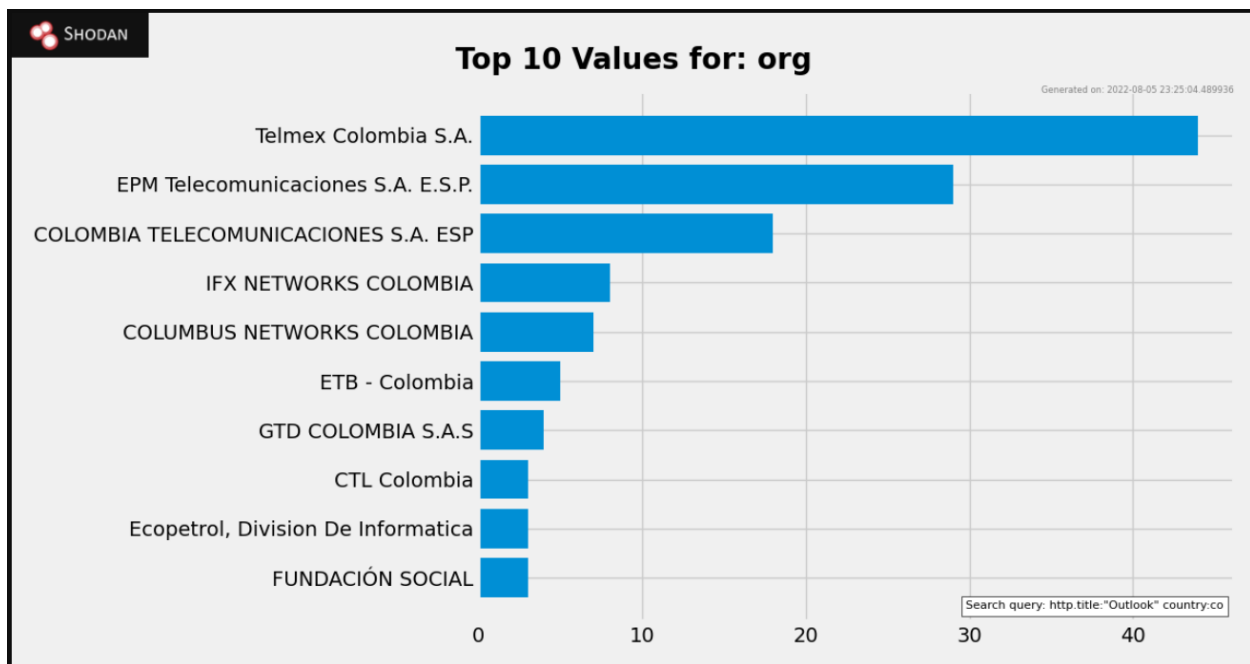
`http.title:"Outlook" country:co`

- Outlook en la web es una aplicación web de administración de información personal de Microsoft. Incluye un cliente de correo electrónico basado en la web, una herramienta de calendario, un administrador de contactos y un administrador de tareas.

Colombia

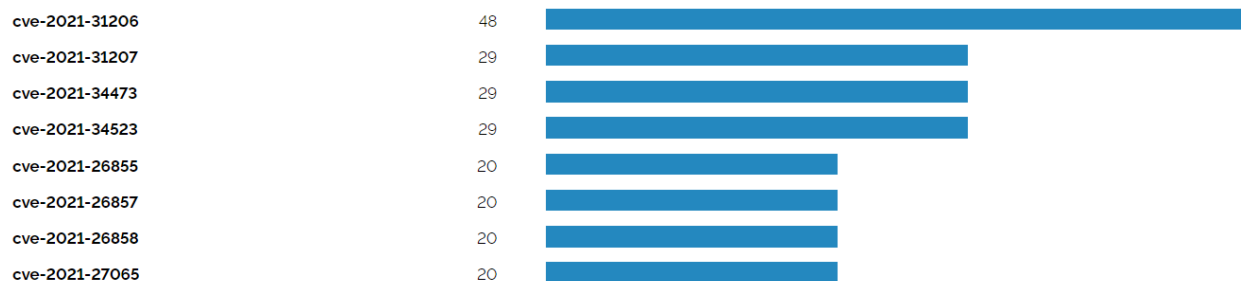


El top de ciudades, de nuevo, las del top son las principales ciudades del país y Bogotá con una gran mayoría siendo la 1 y con mucha diferencia



El top de compañías, Telmex siendo la primera y con ventaja, vuelve a ser la más insegura para los usuarios.

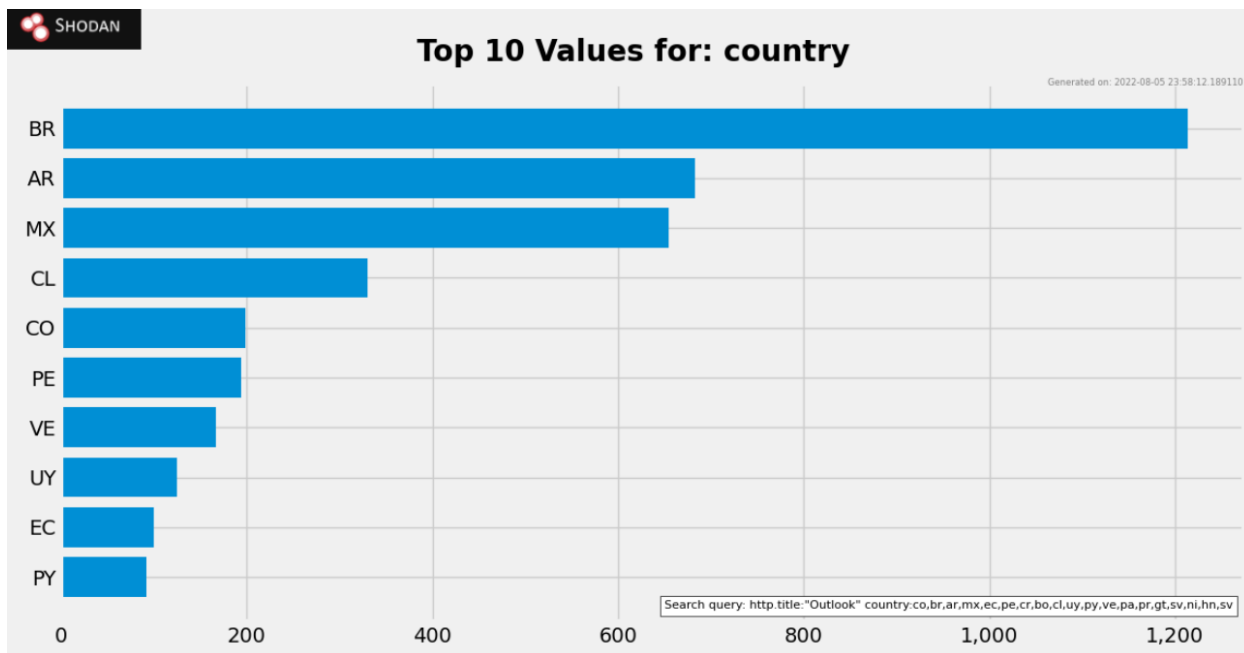
- puerto 443: el puerto estándar para el tráfico HTTPS. Sin embargo, el puerto HTTPS 443 también permite que los sitios estén disponibles a través de conexiones HTTP. Si el sitio usa HTTPS pero no está disponible en el puerto 443 por algún motivo, el puerto 80 intervendrá para cargar el sitio web habilitado para HTTPS. este es el puerto principal en la búsqueda.



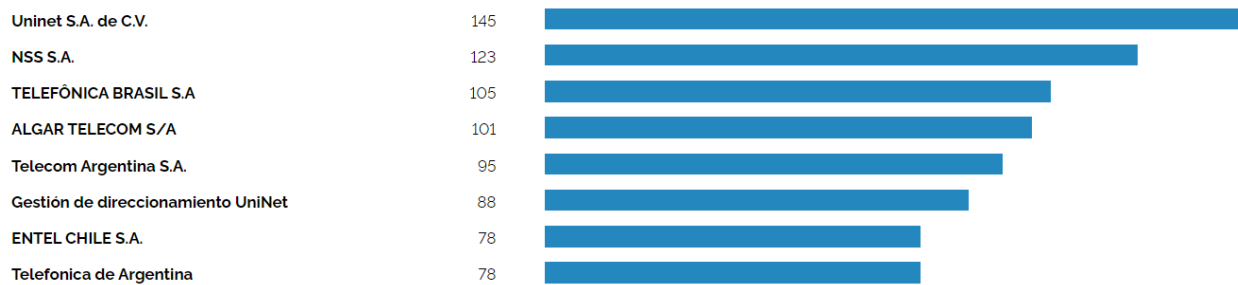
top de vulnerabilidades del puerto 443

Colombia vs otros países de Latinoamérica

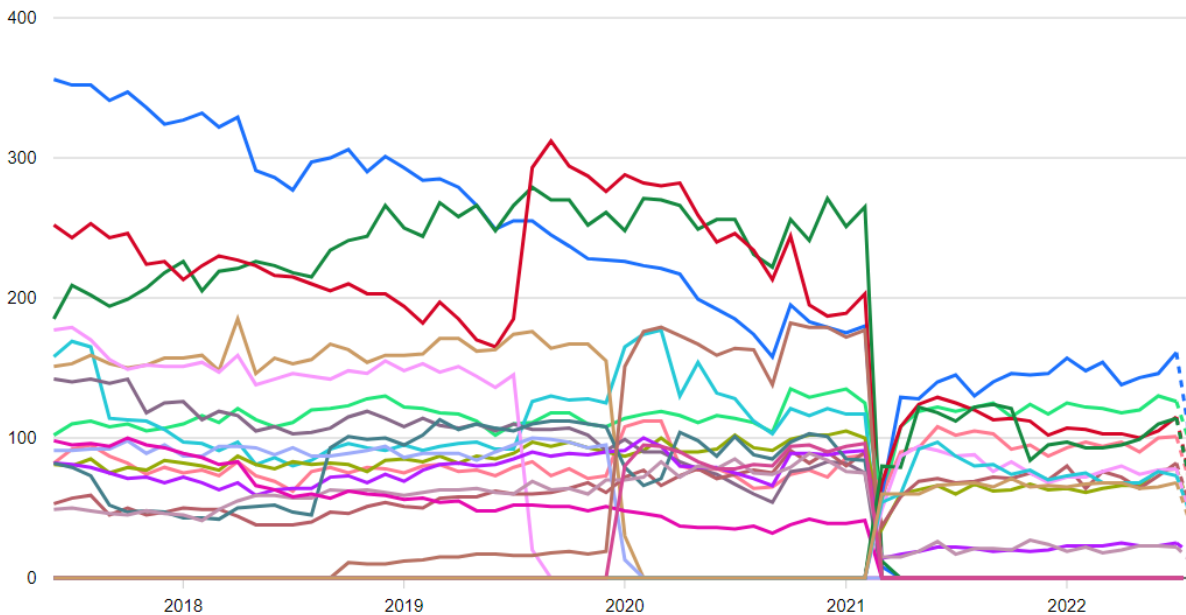
- `http.title:"Outlook" country:co,br,ar,mx,ec,pe,cr,bo,cl,uy,py,ve,pa,pr,gt,sv,ni,hn,sv`



Top de países. Observamos como Argentina rompe lo establecido y saca a México del top 2.



Top de compañías en países latinoamericanos, siendo de nuevo Unitet S.A de C.V el top1. es el Telmex de Colombia.



top compañías, aquí podemos ver que al paso de los años, las empresas van tomando más precauciones o que la gente va mudándose de servicios, en este caso pasan de usar Outlook por otros más innovadores como lo son Gmail.

10. Ark survival evolved

Ark: Survival Evolved' es un videojuego de supervivencia y sandbox desarrollado por el equipo de Studio Wildcard. Los jugadores aparecen en un mundo salvaje y lleno de dinosaurios. A partir de ese momento, tendrán que buscar los métodos para sobrevivir y no morir de hambre, sed o frío.

Desarrollador: **Wildcard Studios**-Editor: **Wildcard Studios**

Fecha de lanzamiento: **2016**-Género: **MMORPG**

Tema: **Dinosaurios.**



`product:"ark survival evolved" country:co,`

Colombia

Con este dork podemos ver todos los servers expuestos que hay en Colombia sobre Ark, en este caso no son muchos son 5, pero hasta jugando en un server privado con amigos, podemos

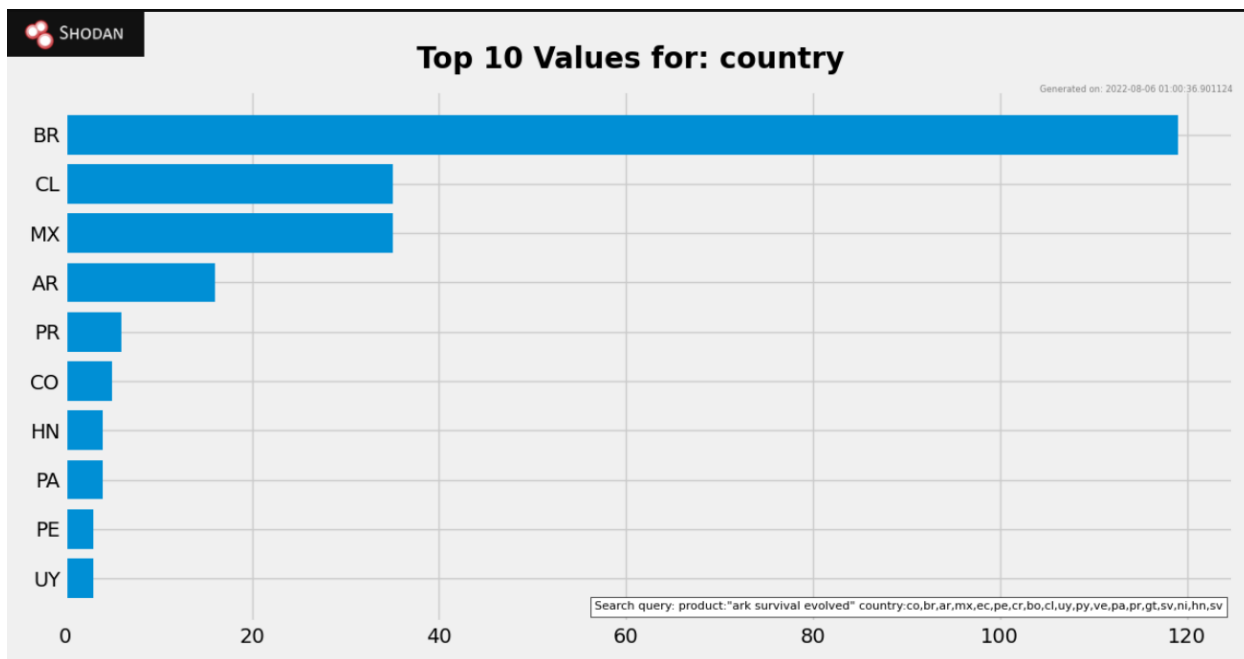
exponer nuestra informacion

TOP CITIES	
Bogotá	4
Pereira	1
TOP PORTS	
27015	4
27016	1
TOP ORGANIZATIONS	
Telmex Colombia S.A.	3
ETB - Colombia	1
SERVICIOS EN SALUD ANDINA LTDA	1

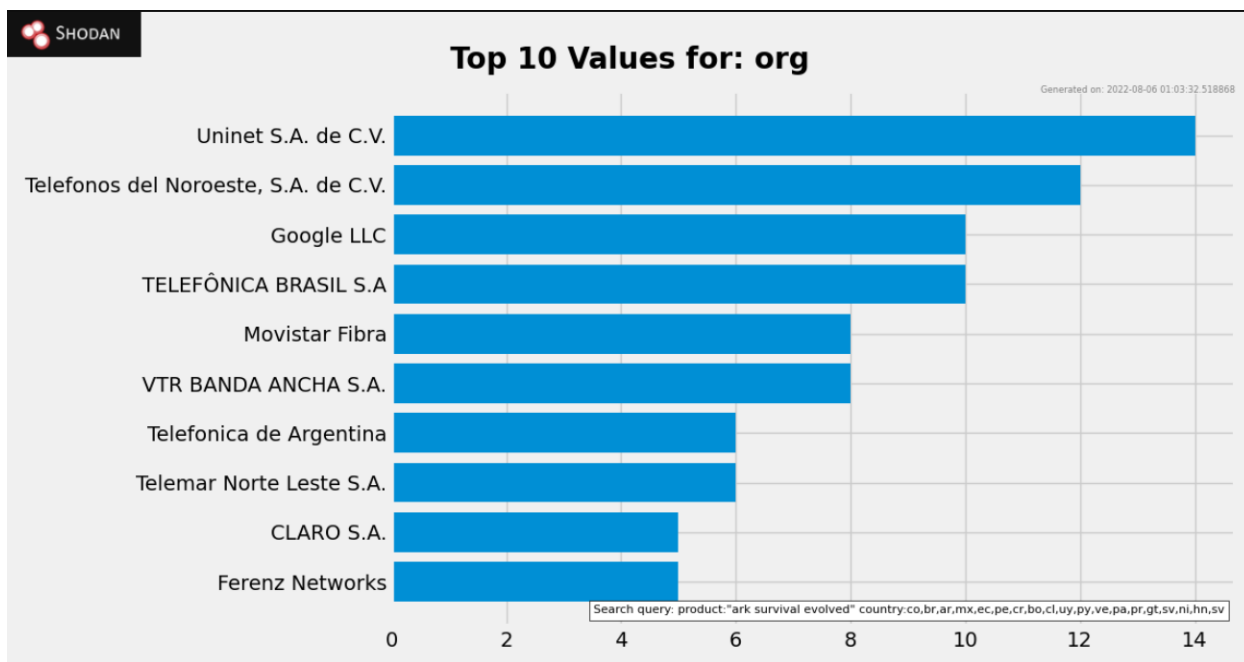
Podemos ver unas regularidades y patrones, como siempre Bogotá siendo la ciudad con más exposición, el puerto TCP **27015**: usa el Protocolo de Control de Transmisión. TCP es uno de los protocolos principales en redes TCP/IP. TCP es un protocolo orientado en la conexión, necesita el apretón de manos para determinar comunicaciones de principio a fin. este puerto es uno de los más usados en videojuegos y usados por Steam.

El top 1 Telmex exponiendo la información, ETB tampoco se queda atrás, pero muy raro que aparezca la compañía de salud andina.

Colombia vs otros países de Latinoamérica



El top de países, como casi siempre Brasil liderando, y la sorpresa de Chile en top 2 con México, podemos observar que a pesar del tiempo, ark aun tiene muchos servidores en línea, y muchos de ellos expuestos son casi 300 servidores expuestos.




El top de compañías de Latinoamérica.

Ahora miremos un poco de la información que se expone con este dork

189.229.209.75

dsl-189-229-209-75-dyn.prod-in
finitum.com.mx

Uninet S.A. de C.V.

 Mexico, San Miguel Ajusco

videogame

ARK: **Survival Evolved** Server

Name: Ark The Island Charly - (v348.6)

Players: 0/10

Operating System: Linux

Map: TheIsland

Version: 1.0.0.0

podemos ver el país y la ciudad, la compañía, el juego con su versión, el numero de jugadores en linea en este servidor, el sistema operativo y el mapa.

Conclusiones

- ▼ Shodan es una plataforma muy útil para realizar footprinting, es decir recopilar información sobre nuestro objetivo. Mediante esta herramienta, logramos hacer la búsqueda de routers, servidores, datos importantes que pueden ser sensibles para una empresa, entre otras cosas.
- ▼ Al observar los resultados de Latinoamérica notamos que Brasil y México siempre lideraban los resultados. Consideramos que esto se debe a que superan con creces la población de los demás países de américa latina.
- ▼ Dentro de las organizaciones de Colombia siempre encontramos como más relevantes las siguientes: EPM Telecomunicaciones, Telmex, Colombia Móvil, ETB. Como podemos observar estas son empresas destacadas por prestar servicios de comunicación.
- ▼ En el top de ciudades de Colombia contábamos siempre con las principales, como Bogotá y Medellín, por lo cual estas pueden ser más vulnerables a ataques si no se configuran sus dispositivos de manera adecuada y segura.
- ▼ Al realizar la actividad de búsqueda profunda en Shodan nos damos cuenta de lo relacionados que están ciertos puertos y productos a una actividad en específico. Por ejemplo, que estén abiertos los puertos 80, 8080, 8888 y 443 podría estar relacionado a una actividad de criptomonedas. Otro ejemplo es el MikroTik RouterOS, el cual fue utilizado para obtener una

conexión segura proporcionando el servicio de VPN y que también estuvo relacionado con su uso para las minerías de criptomonedas.

Referencias

- ▼ SHODAN. Obtenido de: www.shodan.io
- ▼ Binance Pool cambiará la URL del estrato de minería de Smart Pool. (Marzo, 2021). Obtenido de: <https://www.binance.com/es/support/announcement/4d17014d93254714b329539a3793bd09>
- ▼ VPNs seguras con MikroTik RouterOS. Prozcenter. Obtenido de: <https://www.prozcenter.com/wp-content/uploads/200327-VPNs-seguras-con-MikroTik-RouterOS.pdf>
- ▼ Los 14 puertos que no debes abrir en tu router para máxima seguridad. Soriano, David. (Marzo, 2022). Obtenido de: <https://www.adslzone.net/noticias/redes/puertos-no-debes-abrir-router-tcp-udp/>
- ▼ Synology DiskStation DS3615xs Review. StorageReview Consumer Desk. Abril, 2016. Obtenido de: [Synology DiskStation DS3615xs Review - StorageReview.com](http://Synology%20DiskStation%20DS3615xs%20Review%20-%20StorageReview.com)
- ▼ NATIONAL VULNERABILITY DATABASE. Obtenido de <https://nvd.nist.gov/vuln>.