

Selamlar herkese sizlere Shodan nedir? Nasıl kullanılır? Bunları anlatacağım.

SHODAN NEDİR?

Shodan IoT cihazları için bir arama motorudur. Shodan'ın Google , Yandex veya Bing gibi arama motorlarından farkı interneti taramasıdır. Temel amacı güvenlik sorunlarını belirlemektir. Shodan'ın ücretli ve ücretsiz seçenekleri vardır. Shodan güvenlik kameraları trafik ışıkları bebek monitörleri ve birçok cihazla bağlantı kurabilir.

Peki Shodan bizim cihazlarımızın verilerini de ifşa edebilir mi?

Bu sorunun cevabı evet ancak Shodan sadece açık bağlantı noktalarına sahip cihazları görebilir yani internet bağlantısını kesmek yeterli olur. İnternete bağlı olan cihazlar için ise şifre ile korumak ve ağ güvenlik duvarı kullanmak korunmamızı sağlar. Shodan monitörü kullanarak da güvenliğinizi sağlayabiliriz. Shodan monitör ile kendi ağınıza izleyebilir ve herhangi bir güvenlik açığı oluştuğunda bildirim almayı sağlayabiliriz. Shodan monitörü ve diğer bazı özellikleri kullanmak için ücretsiz üyelik yetmez ancak bir edu mailiniz varsa bu özellikleri ücretsiz bir şekilde kullanabilirsiniz. Shodana <https://www.shodan.io/> adresinden ulaşabilirsiniz.

SHODAN NASIL KULLANILIR?

Bir siteye ping atarak ip adresini öğrenebiliriz. Daha sonra ip adresini Shodan'da arayarak kullandığı portları, servisleri ve site hakkındaki genel bilgileri öğrenebiliriz.

157.240.234.35 Regular View Raw Data History

// LAST SEEN: 2022-02-27

General Information

Hostnames	edge-star-mini-shv-02-sof1.facebook.com
Domains	FACEBOOK.COM
Country	United States
City	Shreveport
Organization	Facebook, Inc.
ISP	Facebook, Inc.
ASN	AS32934

Open Ports

80	443
----	-----

// 80 / TCP -1431726786 | 2022-02-27T17:11:35.286581

```
HTTP/1.1 301 Moved Permanently
Vary: Accept-Encoding
Location: http://www.facebook.com/
Content-Type: text/html; charset="utf-8"
X-FB-Debug: vvDv0gM8QtPL/B/F+AK50CEi4CQOZ4/LK0G
hcVJf8Sh1a5x12ByQ5REJO56rMigCc+F1VHdbkXHK5B6HR1
KwAw==
Date: Sun, 27 Feb 2022 17:11:34 GMT
Priority: u=3,1
Alt-Svc: h3=":443"; ma=3600, h3-29=":443"; ma=3600
Connection: keep-alive
Content-Length: 0
```

Shodan BT uzmanlarına yardımcı olacak şekilde tasarlanmıştır. Arama filtresi ile istediğiniz sorguyu yapabiliriz. Bazı arama filtreleri şunlardır:

data : Hizmetin kendisinden gelen ana yanıt

ip_str : Cihazın IP adresi

port : Hizmetin port numarası

org : Bu IP alanına sahip olan kuruluş

country : Cihazın bulunduğu ülke

product : Ürüne göre filtreleme

asn : AS numarası

Os : İşletim sistemi

before/after : sınırlı zaman dilimi(before:2010->2010dan önceki sonuçlar)

hostname : hostname ismi

vuln : güvenlik açığı

 SHODAN

port:3389



TOPLAM SONUÇLAR

4,256,847

EN İYİ ÜLKELER



Amerika

Birleşik

Devletleri

Çin 1,496,166

1,007,544

Almanya

194,158

Hollanda

 Raporu görüntüle

 Sonuçları İndir

 Tarihsel Eğilim

 Resimlere Göz Atın

 Haritada görüntüle

Yeni Hizmet: İnternete ne bağladığınızı takip edin. **Shodan Monitor'e** göz atın

54.83

ec2-54-83-1
45-119.com
pute-1.amaz
onaws.com

Amazon
Teknolojileri
A.Ş.

Amerika
Birleşik
Devletleri ,
Ashburn

Bulut

kendinden imzalı

 **SSL
Sertifikası**

Veren

kuruluş:

|- OrtakAd:

EC2AMAZ-

KH7SEUT

Adına

yayınlanan:

|- OrtakAd:

EC2AMAZ-

KH7SEUT

Desteklenen

2022-03-04T10:17:07.746344

Uzak Masaüstü Protokolü NTLM Bilgisi:

İşletim Sistemi: Windows 10/Windows Server 2019

İşletim Sistemi Yapısı: 10.0.17763

Hedef Adı: EC2AMAZ-KH7SEUT

NetBIOS Etki Alanı Adı: EC2AMAZ-KH7SEUT

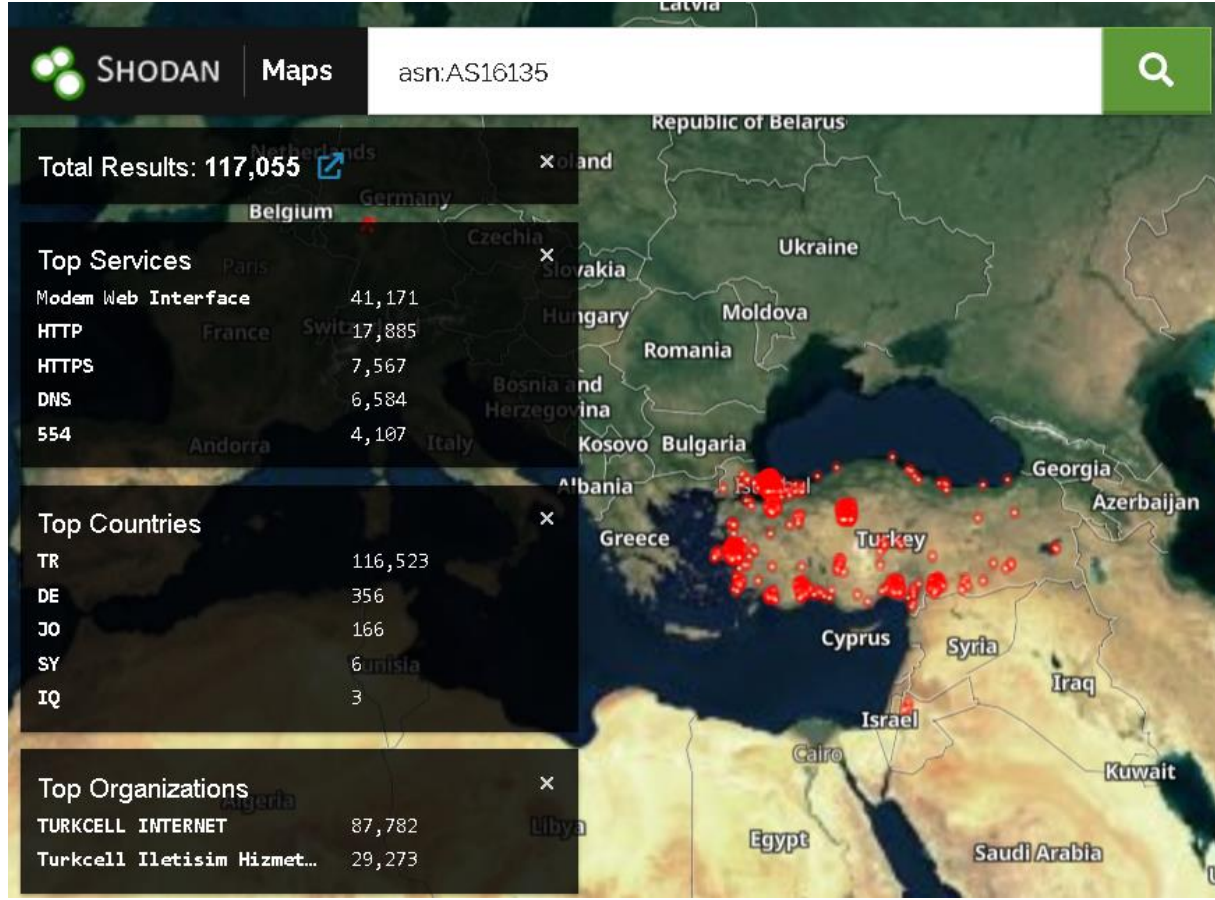
NetBIOS Bilgisayar Adı: EC2AMAZ-KH7SEUT

DNS Etki Alanı Adı: EC2AMAZ-KH7SEUT FQDN: EC2AMA

FQDN: EC2AMAZ -KH7SEUT

Sistem Saati: 2022-03-04 10:17:...

Bu sorgumuz sonucunda toplam kaç tane sonuç olduğunu ülke , organizasyon , ürün ve işletim sistemi bazlı kaç tane sonuç olduğunu görebiliyoruz.



ASN numarası yani Otonom Sistem Numarası bir şirketin sahip olduğu bütün IP adreslerinin genel tanımlayıcısıdır. Örneğin Turcell İletişim Hizmetleri A. Ş.'nin asn numarası AS16135 .

Asn numarasına göre arama yaptığımızda sadece o şirketin ürünlerini listeler. Shodan maps ile cihaz yoğunluğuna göre haritayı görebiliriz.



TOPLAM SONUÇLAR

1,240

Raporu görüntüle

Sonuçları İndir

Tarihsel Eğilim

Haritada görüntüle

Arada bir satı boşluk bırakarak 2 sorguyu birlikte kullanabiliriz. Sonuçları indir bölümünden sorgunun sonuçlarını indirebiliriz.

KAYNAKLAR:

<https://help.shodan.io/the-basics/what-is-shodan>

<https://www.safetynetives.com/blog/what-is-shodan-and-how-to-use-it-most-effectively/>

