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

SHODAN NEDİR?

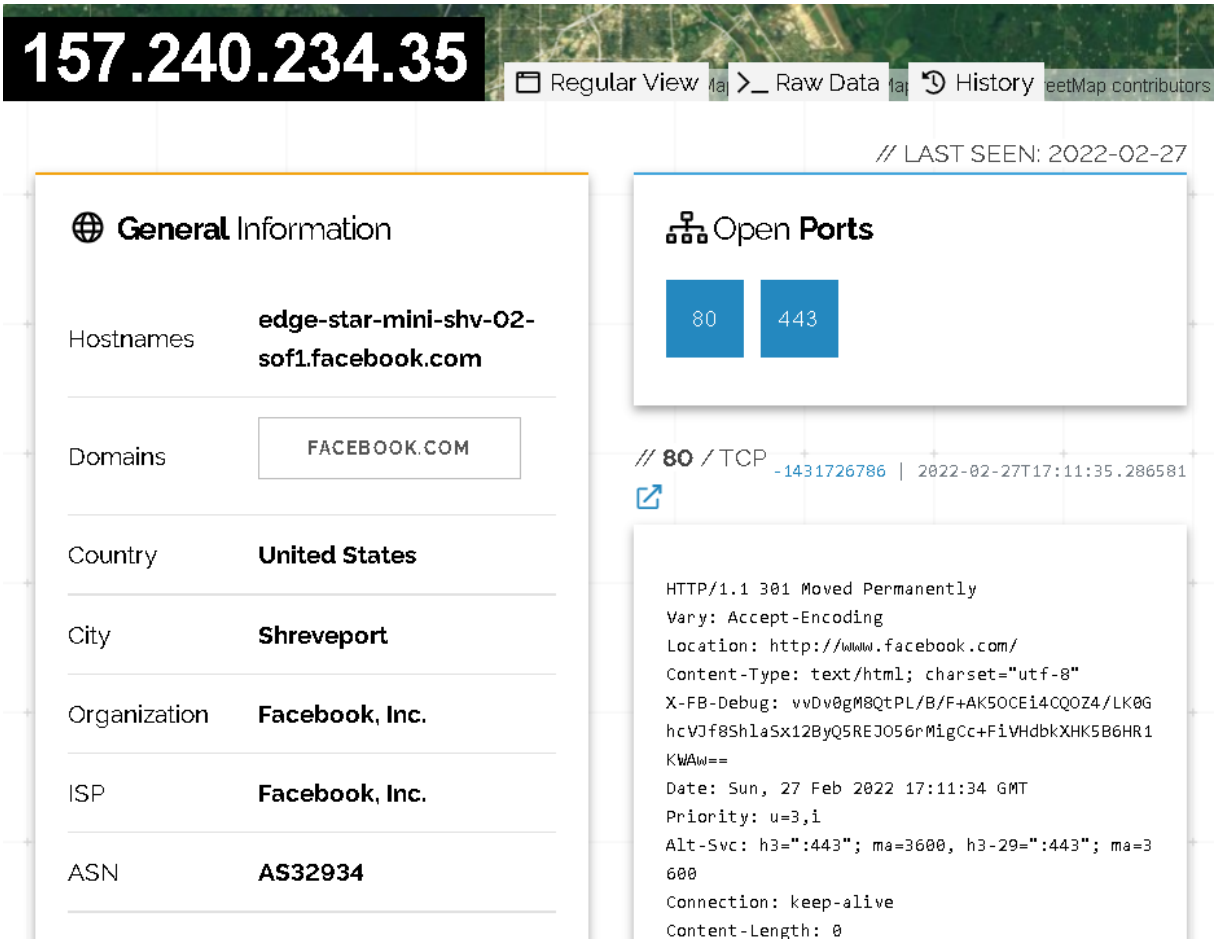
Shodan IoT cihazları için bir arama motorudur. Shodan'ın Google , Yandex veya Bing gibi arama motorlarından farkı interneti taramasıdır. Temel amacı güvenlik sorunlarını belirlemektir. Shodan'ın ücretli ve ücretsiz seçenekleri vardır. Shodan güvenlik kameraları trafik ışıkları bebek monitörleri ve birçok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



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 gör filtreleme

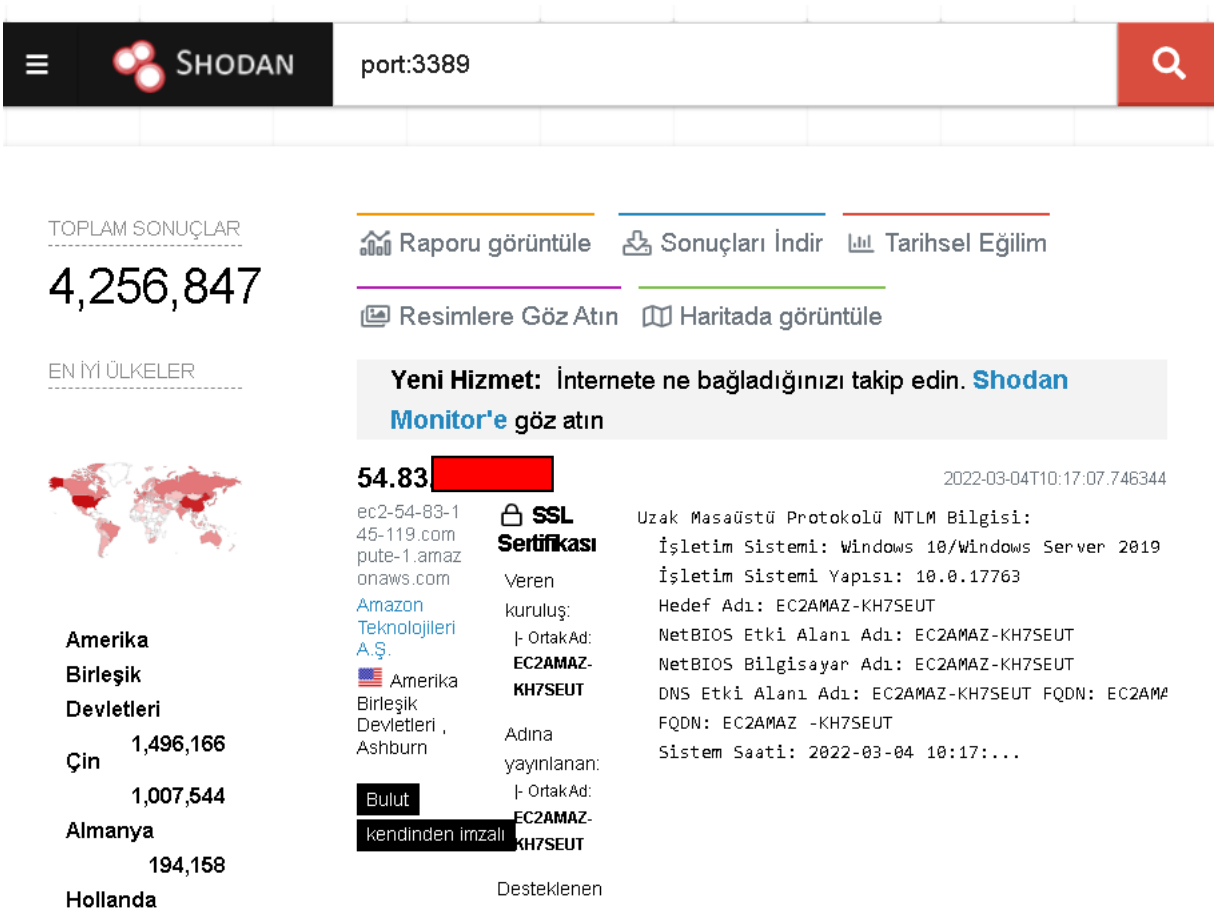
asn : AS numarası

Os : İşletim sistemi

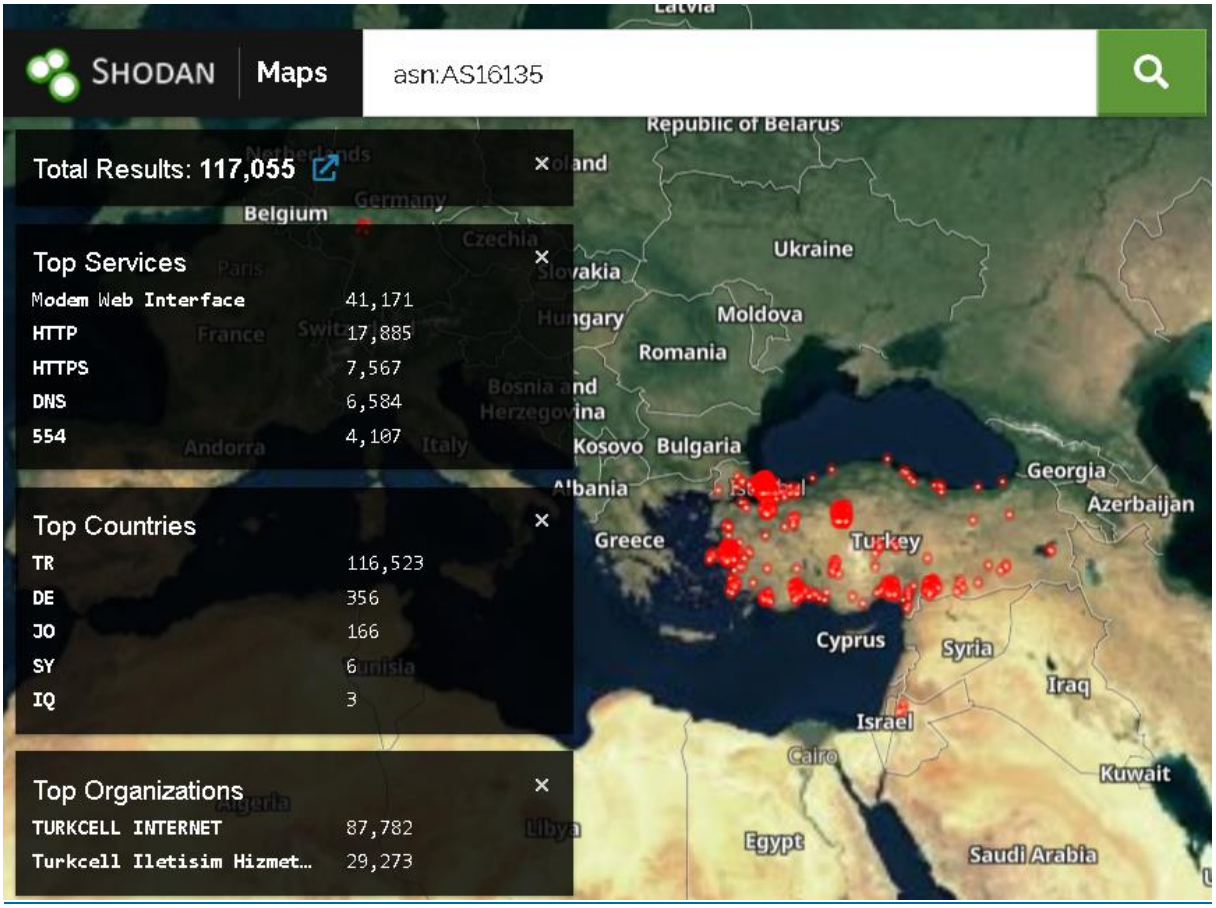
before/after : sınırlı zaman dilimi(before:2010->2010dan önceki sonuçlar)

hostname : hostname ismi

vuln : güvenlik açığı

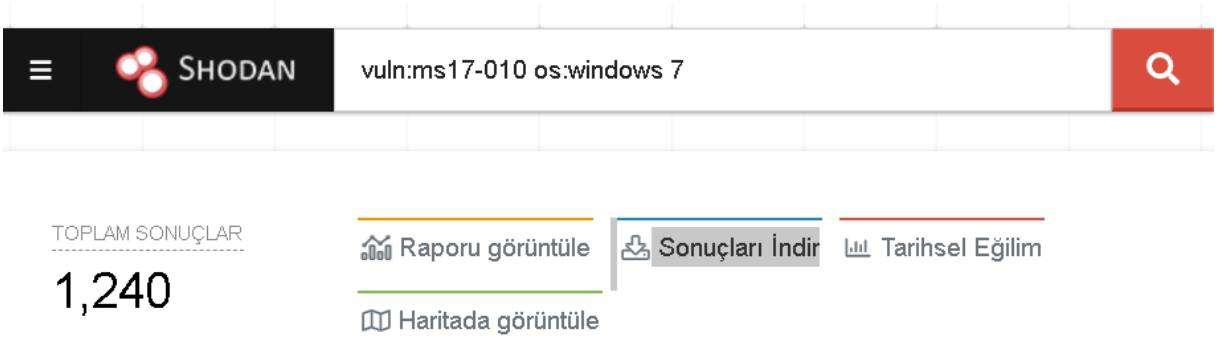


Bu sorgumuz sonucunda toplam kaç tane sonuç olduğunu ülke , organizasyon , ürün ve işletim sistemi bazlı kaç tane sonuç olduğunu görebiliyoruz.



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.



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.safetydetectives.com/blog/what-is-shodan-and-how-to-use-it-most-effectively/