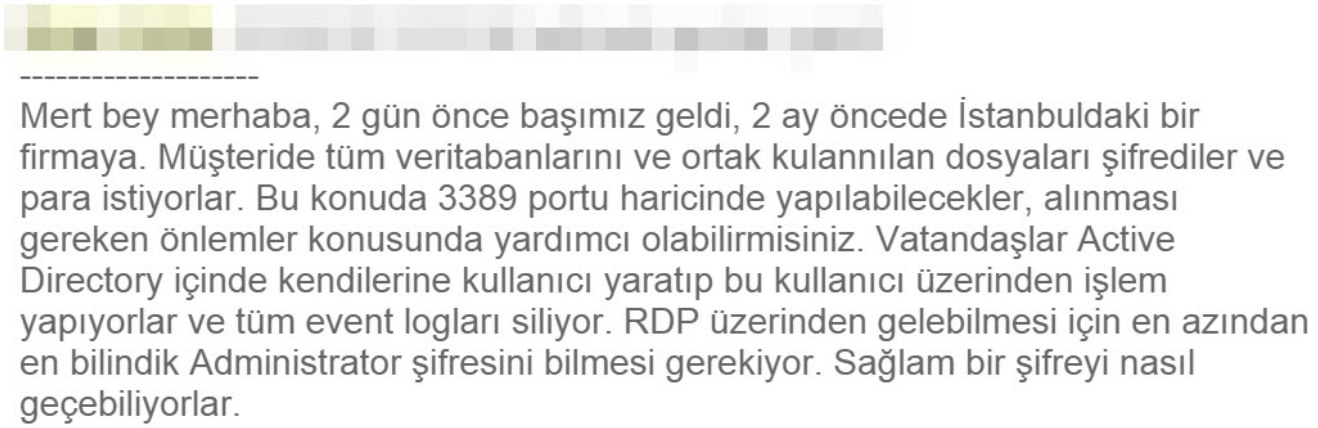
Shodan ile Durum Değerlendirmesi

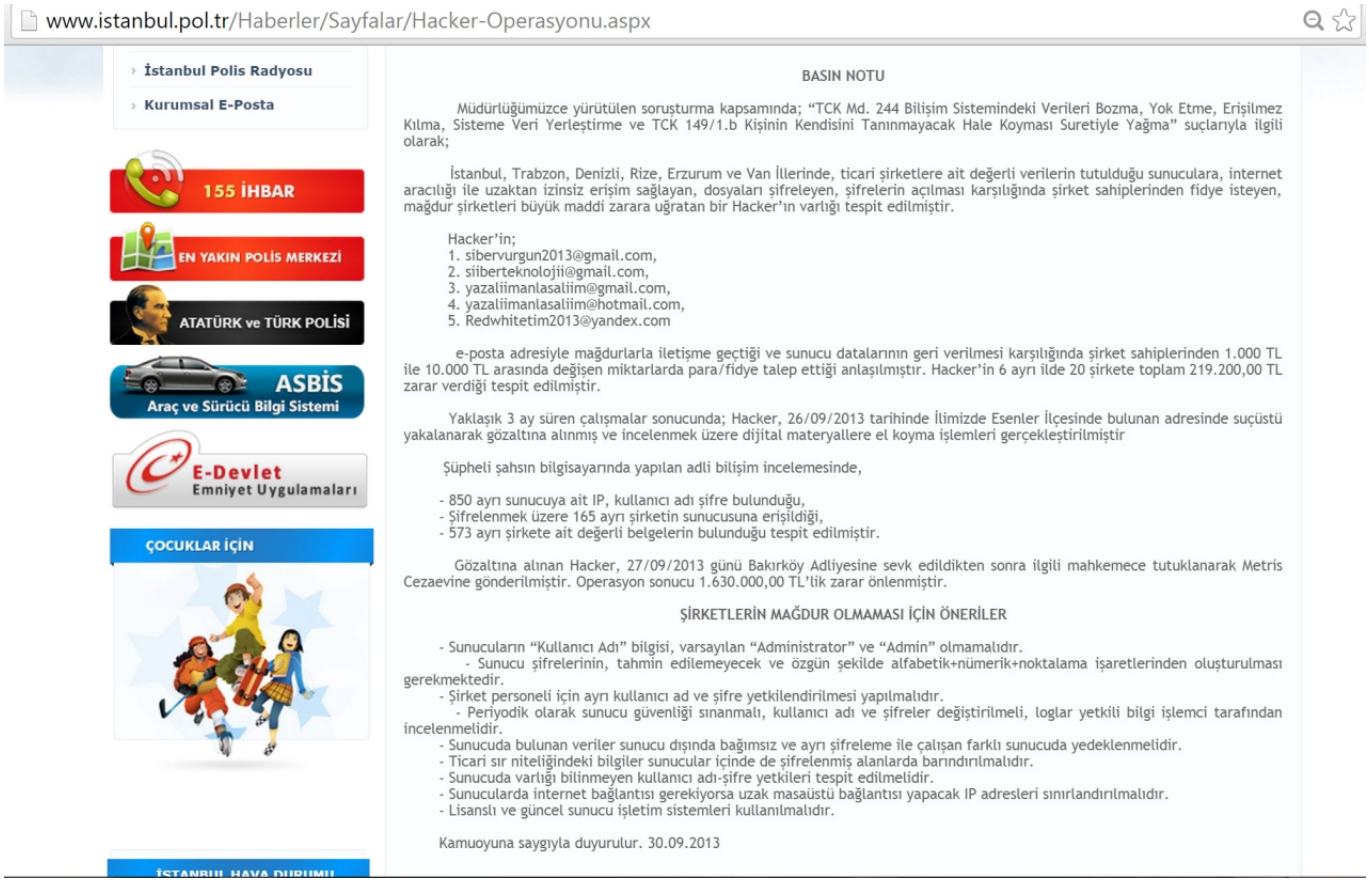
written by Mert SARICA | 1 January 2016

Bu zamana dek küçük ve orta ölçekli işletmelerde (KOBİ) çalışan veya bir yakını olan arkadaşlarımdan özellikle bir konu hakkında çok fazla yardım istediğini farkettim. Benzer yardım taleplerine Netsec bilgi güvenliği e-posta grubunda da denk geliyorum. Evet, sizlerin de az çok tahmin edeceği üzere, kullanıcıların/kurumların verilerini şifreleyen ve bunun karşılığında fidye isteyen siber fidyecilerden bahsediyorum.



Mert bey merhaba, 2 gün önce başımız geldi, 2 ay öncede İstanbuldaki bir firmaya. Müşteride tüm veritabanlarını ve ortak kulannılan dosyaları şifrediler ve para istiyorlar. Bu konuda 3389 portu haricinde yapılabilecekler, alınması gereken önlemler konusunda yardımcı olabilirmisiniz. Vatandaşlar Active Directory içinde kendilerine kullanıcı yaratıp bu kullanıcı üzerinden işlem yapıyorlar ve tüm event logları siliyor. RDP üzerinden gelebilmesi için en azından en bilindik Administrator şifresini bilmesi gerekiyor. Sağlam bir şifreyi nasıl geçebiliyorlar.

Bu siber fidyecilerle ilgili olarak yerli basında belki farkındalık adına çok sayıda habere rastlamıyoruz ancak resmi kaynaklardan elde edilen bilgiler ışığında, hem gerçekleştirilen siber saldırıların sayısına hem de bu saldırganların yol açtığı zararlara baktığımızda, rakamların azımsanamayacak kadar yüksek olduğunu görebiliyoruz. Bu tür saldırılarla karşılaşanların çoğu, kulaktan dolma haberler ve/veya önyargıları nedeniyle emniyet müdürlüğünün bu konuda çözüm üretemeyeceğini düşünerek yetkili mercilere başvurmaktan kaçınıyorlar. Ancak emniyet müdürlüğünün web sayfasına bakacak olursanız, zaman zaman bu ve benzeri siber çetelere / dolandırıcılara karşı başarılı operasyonlara imza attıklarını görebilirsiniz.


www.istanbul.pol.tr/Haberler/Sayfalar/Hacker-Operasyonu.aspx

İstanbul Polis Radyosu
Kurumsal E-Posta
155 İHBAR
EN YAKIN POLİS MERKEZİ
ATATÜRK ve TÜRK POLİSİ
ASBİS
Araç ve Sürücü Bilgi Sistemi
E-Devlet
Emniyet Uygulamaları
ÇOCUKLAR İÇİN

BASIN NOTU

Müdürlüğümüzce yürütülen soruşturma kapsamında; "TCK Md. 244 Bilişim Sistemindeki Verileri Bozma, Yok Etme, Erişilmez Kılma, Sisteme Veri Yerleştirme ve TCK 149/1.b Kişinin Kendisini Tanınmayacak Hale Koyması Suretiyle Yağma" suçlarıyla ilgili olarak;

İstanbul, Trabzon, Denizli, Rize, Erzurum ve Van İllerinde, ticari şirketlere ait değerli verilerin tutulduğu sunuculara, internet aracılığı ile uzaktan izinsiz erişim sağlayan, dosyaları şifreleyen, şifrelerin açılması karşılığında şirket sahiplerinden fidye isteyen, mağdur şirketleri büyük maddi zarara uğratan bir Hacker'ın varlığı tespit edilmiştir.

Hacker'in;
1. sibervurgun2013@gmail.com,
2. siiberteknolojii@gmail.com,
3. yazaliimanlasaliim@gmail.com,
4. yazaliimanlasaliim@hotmail.com,
5. Redwhitetim2013@yandex.com

e-posta adresiyle mağdurlarla iletişme geçtiği ve sunucu datalarının geri verilmesi karşılığında şirket sahiplerinden 1.000 TL ile 10.000 TL arasında değişen miktarlarda para/fidye talep ettiği anlaşılmıştır. Hacker'in 6 ayrı ilde 20 şirkete toplam 219.200,00 TL zarar verdiği tespit edilmiştir.

Yaklaşık 3 ay süren çalışmalar sonucunda; Hacker, 26/09/2013 tarihinde İlimizde Esenler İlçesinde bulunan adresinde suçüstü yakalanarak gözaltına alınmış ve incelenmek üzere dijital materyallere el koyma işlemleri gerçekleştirilmiştir

Şüpheli şahsın bilgisayarında yapılan adli bilişim incelemesinde,

- 850 ayrı sunucuya ait IP, kullanıcı adı şifre bulunduğu,
- Şifrelenmek üzere 165 ayrı şirketin sunucusuna erişildiği,
- 573 ayrı şirkete ait değerli belgelerin bulunduğu tespit edilmiştir.

Gözaltına alınan Hacker, 27/09/2013 günü Bakırköy Adliyesine sevk edildikten sonra ilgili mahkemece tutuklanarak Metris Cezaevine gönderilmiştir. Operasyon sonucu 1.630.000,00 TL'lik zarar önlenmiştir.

ŞİRKETLERİN MAĞDUR OLMAMASI İÇİN ÖNERİLER

- Sunucuların "Kullanıcı Adı" bilgisi, varsayılan "Administrator" ve "Admin" olmamalıdır.
- Sunucu şifrelerinin, tahmin edilemeyecek ve özgün şekilde alfabetik+nümerik+noktalama işaretlerinden oluşturulması gerekmektedir.
- Şirket personeli için ayrı kullanıcı ad ve şifre yetkilendirilmesi yapılmalıdır.
- Periyodik olarak sunucu güvenliği sınanmalı, kullanıcı adı ve şifreler değiştirilmeli, loglar yetkili bilgi işlemci tarafından incelenmelidir.
- Sunucuda bulunan veriler sunucu dışında bağımsız ve ayrı şifreleme ile çalışan farklı sunucuda yedeklenmelidir.
- Ticari sır niteliğindeki bilgiler sunucular içinde de şifrelenmiş alanlarda barındırılmalıdır.
- Sunucuda varlığı bilinmeyen kullanıcı adı-şifre yetkileri tespit edilmelidir.
- Sunucularda internet bağlantısı gerekiyorsa uzak masaüstü bağlantısı yapacak IP adresleri sınırlandırılmalıdır.
- Lisanslı ve güncel sunucu işletim sistemleri kullanılmalıdır.

Kamuoyuna saygıyla duyurulur. 30.09.2013

Yazılı ve görsel medyadsa çıkan onlarca habere ve uyarıya rağmen sahte polis, savcı ve jandarma kılığında dolandırıcılara para kaptıran vatandaşımızın, siber dünyada var olan tehditlerden haberdar olması ve bunlara karşı önlem alması devlet eli olmadan yakın gelecekte pek mümkün olacak gibi görünmüyor. Gönül ister ki İngiltere'de olduğu gibi belediyelerimizin bünyelerinde birimler kurulsun ve bu birimler, vatandaşımızı, küçük ve orta ölçekli işletmeler, siber saldırılara karşı korusun, danışmanlık versin.

Bu fidyecilerin izledikleri yöntemlerin başında Türkiye ip bloğunu taramak (port scan) ve genele açık servisleri/sunucuları (RDP, MSSQL vb.) tespit etmek geliyor. Bu servisleri tespit ettikten sonra ise sözlük saldırısı (dictionary attack) ile zayıf parolalar tespit edip sistemlere yönetici yetkisi ile bağlanıyorlar. Ardından herkesin bildiği gibi diskte bulunan tüm verileri şifreledikten (encryption) sonra bir not bırakıp sistemden ayrılıyorlar. Verilerini yedeklemeyen kullanıcılar ve KOBİler ise yana yakıla bu notta yer alan kişilerle iletişime geçerek kimi zaman talep edilen bedeli ödemek zorunda kalıyorlar.

Neden bu yöntemi kullanmaya devam ediyorlar ? Gerçekten internette genele açık olan sistemler, sunucular bu kadar çok mu ? gibi aklımı kurcalayan

sorulara yanıt bulmak için ufak bir araştırma yapmaya karar verdim. Tabii bunun için massscan gibi bir araç ile tüm Türkiye ip bloğunu tarayıp, tespit ettiğim sistemlere sözlük saldırısı gerçekleştirmedim :) Aksine tarama işlemini benim için yapan ve doğrulama kontrolü (authentication) yapılmayan sistemleri tespit eden ve rapor çekmeye imkan tanıyan Shodan arama motorunu kullanmaya karar verdim.

Shodan arama motoru temelde Google'dan çok farklı olmayan, interneti tarayıp internete açık olan sistemleri, cihazları, aygıtları tespit edip bunları bağlantı noktasına (port:"3389″), türüne (os:"Windows XP", coğrafi lokasyonuna (country:"TR" gibi) ve servis bilgisine (Anonymous user logged in) göre sınıflandırmaktadır. Bu bilgiler sayesinde de ülke bazında özel aramalar gerçekleştirilebilmektedir. Hatta ve hatta Shodan tarafından taranan sistemlerin ekran görüntülerine bile ulaşmak mümkündür.

Shodan sadece internete açık olan sistemleri cihazları, aygıtları tespit etmek ile kalmayıp Scanhub servisi sayesinde de nmap, massscan gibi tarama araçlarının çıktılarını alarak görsel olarak analiz etmenize de imkan tanımaktadır. Örneğin bu örnekte olduğu gibi bir zararlı yazılımın haberleştiği komuta kontrol merkezini izleyebilirsiniz.

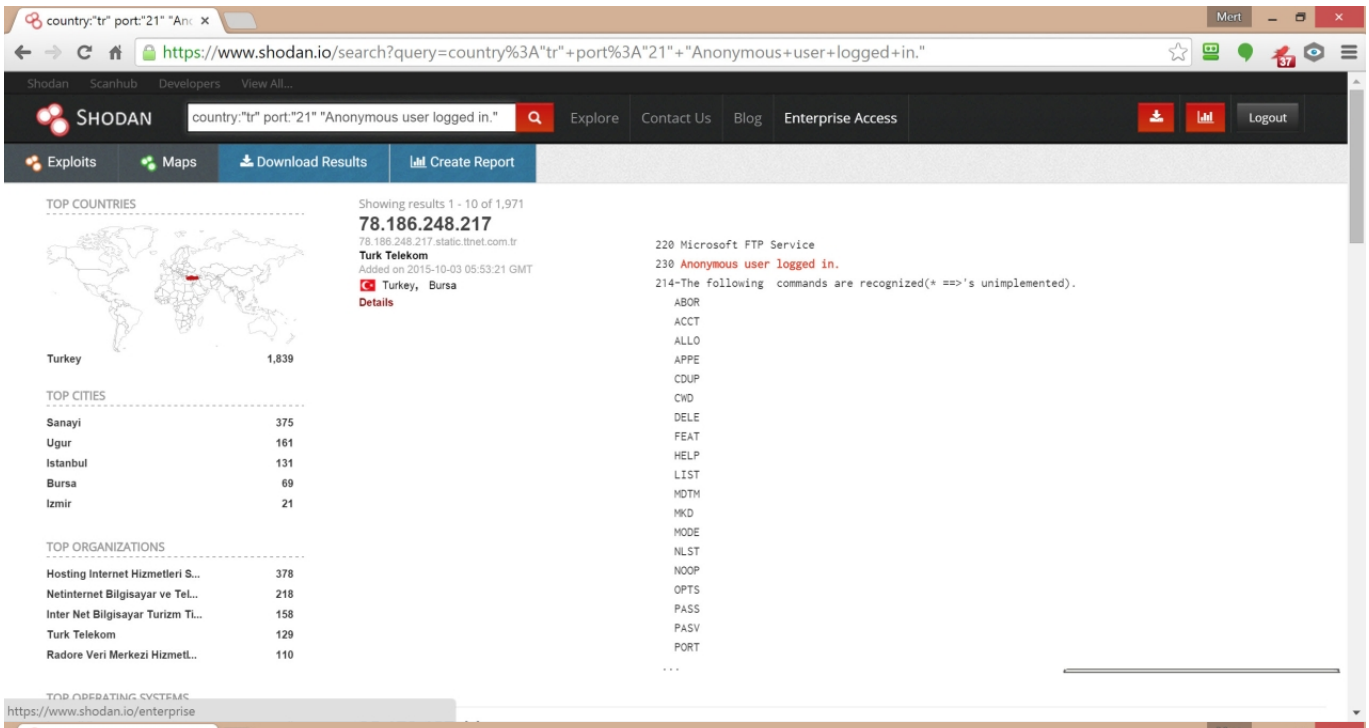
Shodan üzerinde Scanhub servisine ilave olarak özellikle sızma testi uzmanlarının faydalanabileceği Exploit servisi de bulunmaktadır. Bu servis ile Exploit-DB gibi istismar kodlarının yayınlandığı siteler üzerinden istismar kodunun çeşidine ve hedef uygulamaya göre çeşitli aramalar yapabilir ve istismar koduna ulaşabilirsiniz. (Örnek)

Python, Ruby gibi programlama dillerine hakimseniz, Shodan API sayesinde geliştirmiş olduğunuz programınız/betiğiniz ile Shodan üzerinden aramalar da yapabiliyorsunuz.

Unutmadan Shodan'ın temelde ücretsiz bir servis olduğunu ancak kullanacağınız her bir servis özelinde detaylı arama sonuçlarına ulaşmak istediğinizde sizden ilave ücretler talep edeceğini de hatırlatmakta fayda var. (Örnek: Developer Servisi, Scanhub Servisi)

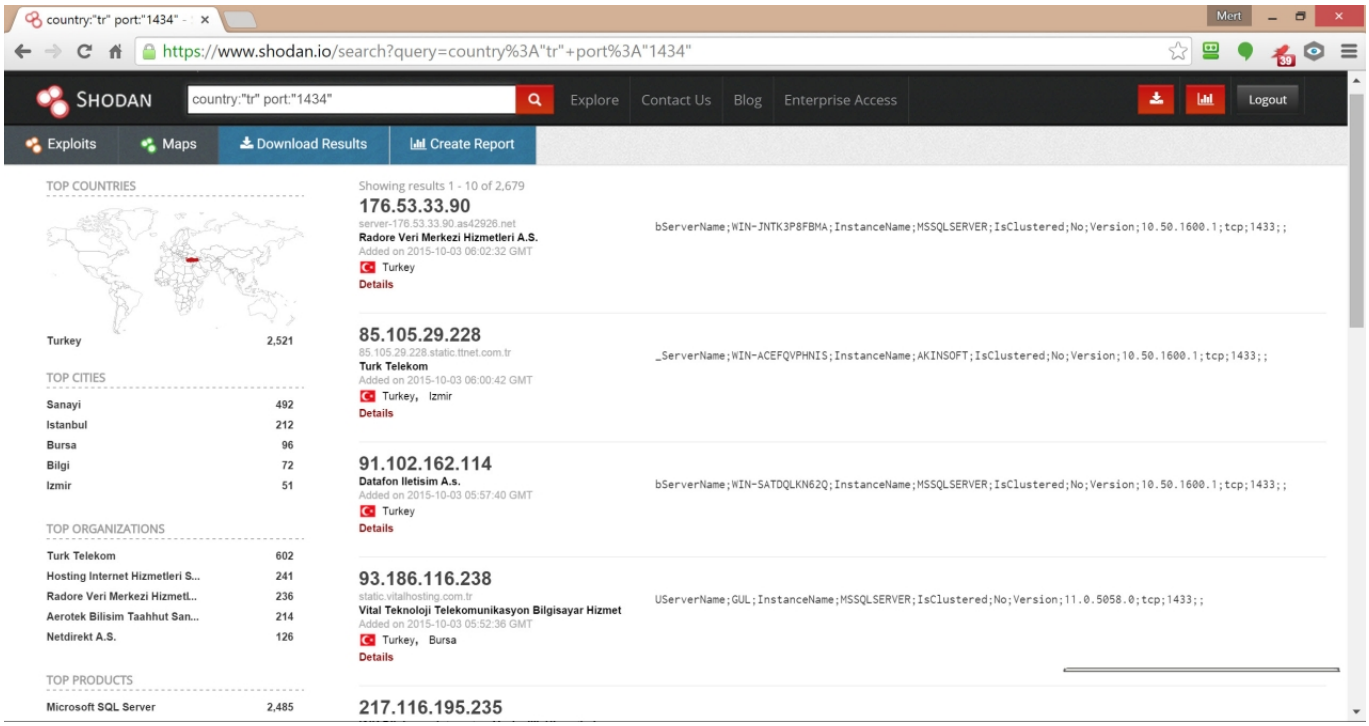
İlk olarak anonim kullanıcı (anonymous) yetkisi ile ftp bağlantısına izin veren sunucuların/sistemlerin sayısına bakmak istedim. Hatalı konfigürasyon neticesinde çok sayıda bilgiye anonim olarak erişilmesine yol açan bu hesabın

veri hırsızlarının gözdesi olduğunu söyleyebiliriz. Türkiye ip bloğunda anonim kullanıcı yetkisine izin veren sunuculara/sistemlere baktığımda, sayının azımsanamayacak kadar fazla olduğunu gördüm. (1956 sistem/sunucu)

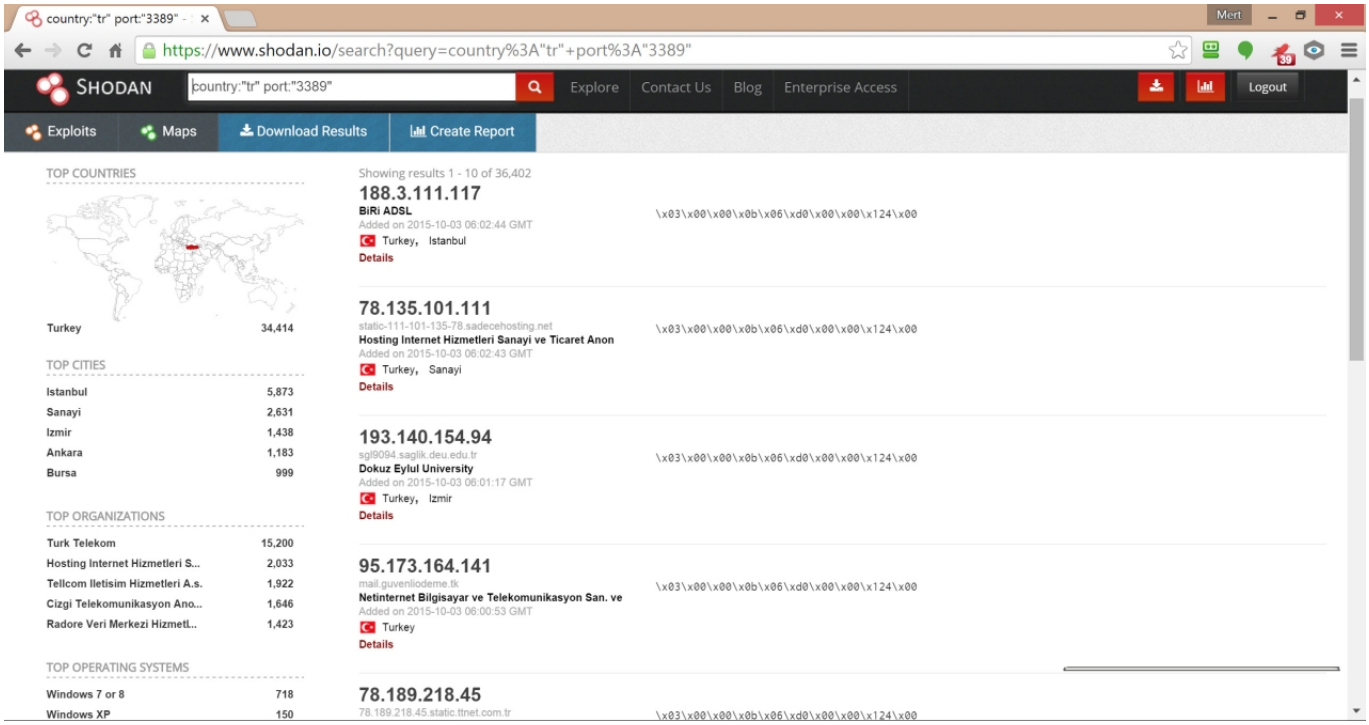


İkinci olarak ise veritabanlarına internetten erişime izin veren ağlara bakmaya karar verdim. Bildiğiniz gibi kurumsal verilerin saklandığı veritabanlarının, bilgi güvenliği adına kısıtlı bir erişime sahip olması gerekmektedir aksi halde zayıf parolalar ile korunan veritabanlarında yer

alan verilerin, art niyetli kişiler tarafından sözlük saldırısı ile çalınması mümkündür. (kullanıcı:sa şifre:sa gibi) Bunun için Türkiye ip bloğunda, Microsoft SQL veritabanı sunucusu tarafından kullanılan 1434. bağlantı noktasına erişim veren ip bloklarını kontrol ettiğimde, sayının anonim ftp erişimine izin veren ağlar kadar fazla olduğunu (2521 sistem/sunucu) olduğunu gördüm.



Son olarak fidyeciler tarafından hedef sistemlere uzaktan bağlanmak için sıklıkla kötüye kulanılan RDP (remote desktop) servisini internete açan sistemleri kontrol ettiğimde ise 34.314 tane sistem ile karşılaşmam, siber fidyecilerin neden bu yöntemi hala kullanmaya devam ettiklerini ve başarılı olduklarını açıkça ortaya koyuyordu.



Siber fidiyecilere karşı hem KOBİler'in hem de son kullanıcıların daha dikkatli olması gerekmektedir. Bunun için öncelikle modem ayarlarınızdan hangi sistemlerinizin ve bağlantı noktalarının, servislerin internete/dış dünyaya açık olduğunu tespit etmeniz faydalı olacaktır. İkinci olarak ise RDP ve MSSQL kullanıcı hesaplarına ait şifrelerin, güçlü, karmaşık ve tahmin edilmesi güç olması, fidyeciler tarafından hedef alınmanızı zorlaştıracaktır. Son olarak ise kullanılan sistemlerin sıkılaştırılması (hardening, güncel yamaların yüklenmesi vb.), gereksiz bağlantı noktalarının ve servislerin dış dünyaya kapatılması, üzerine yoğunlaşmanız gereken bir diğer önemli noktadır.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.