ParSecure Brute Force (Kaba Kuvvet) Siber Saldırı Raporu

22/04/2020

Hakkımızda

Bilişim 112, Müşterilerinin bilişim sistemlerinin her zaman sorunsuz, kesintisiz ve verilerinin maksimum güvenliğini sağlamayı hedeflemektedir. Bilişim 112 hedefleri doğrultusunda çok önemli siber güvenlik ürünlerini kendi bünyesinde tamamen Türk yazılımcı ekibi ile geliştirmiştir. Ayrıca dünyadaki güvenlik ürünlerini çok iyi analiz ederek distribütörlük kapsamında bünyesine katmıştır. Bilişim 112 sürekli kendini geliştiren siber saldırganlara karşı geliştirdiği ParSecure siber istihbarat ürünü sayesinde çok özel stratejiler uygulayarak güvenlik hizmeti ve ürünlerini geliştirmektedir.

ParSecure Hakkında

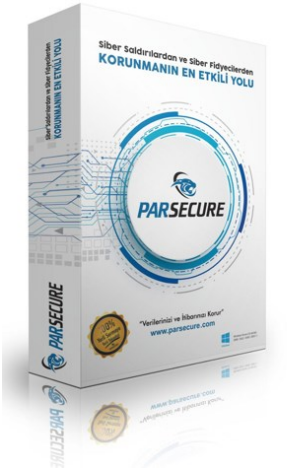
ParSecure, konusunda uzman ekipler ile Bilişim 112 firması tarafından Türkiye'nin en büyük tematik teknoloji geliştirme bölgesi olan Bilişim Vadisinde geliştirilmiş siber istihbarat ve siber güvenlik ürünüdür.

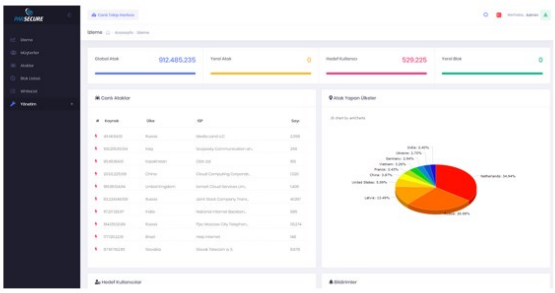
Bilişim 112 tarafından geliştirilen ParSecure honeypotları Türkiye dahil 52 ülkede konumlandırılmış durumdadır. Honeypotlardan elde edilen bilgiler, derinlemesine yapılan analizler, büyük veri sorguları ve dark web – deep web den elde edilen istihbarat bilgileri anlık olarak değerlendirme sunucusunda işlendikten sonra milisaniye kadar kısa süre içerisinde ParSecure güncelleme sunucusuna iletilir.

ParSecure Siber Güvenlik Yazılımı 60 saniyede bir güncel saldırgan bilgileri güncelleme sunucusundan alır ve blok rollerini oluşturarak tespit ettiğimiz saldırganlar ParSecure Siber Güvenlik Yazılımını kullanan kurumları hedeflemeden engellenirler. ParSecure X-API ürünü ise anlık güncellenir ve kurumların mevcut güvenlik ürünlerini besler. (Firewall vb. güvenlik ürünlerine bir kural ile entegre olabilir.)

ParSecure İstihbarat ürünü 3. parti istihbarat servislerinden beslenmez.

ParSecure Siber İstihbarat ürünü tarafından tespit edilen bilgiler doğrultusunda kritik kurumları bilgilendirmektedir.





Giriş

Raporumuzda siber saldırganların veri sızıntısı ve ransomware (fidye) saldırılarını gerçekleştirmek için kullandığı kaba kuvvet (Brute-Force) saldırılarını ele alacağız. Raporumuzda yer alan tabloların tamamı, Türkiye / Bilişim Vadisi'nde yerli olarak geliştirdiğimiz ParSecure siber istihbarat ve siber güvenlik yazılımı veri tabanında bulunan bilgiler yardımı ile oluşturulmuştur. Raporumuzda olabildiğince Türkçe anlamlara yer verilmiştir. Raporumuzda yer alan bilgilerin tamamı ParSecure veri tabanından alınmıştır.

Brute-Force'nin Türkçe karşılığı kaba kuvvettir. Kaba kuvvet saldırıları, bir parola oluşturabilecek olası tüm kombinasyonları hesaplayıp, doğru parola olup olmadığını test ederek çalışır. Parolanın uzunluğu arttıkça doğru parolayı bulmak için ortalama süre katlanarak artar. Ancak saldırganlar süreyi kısaltmak adına birçok çalışma ve araç geliştirmişlerdir.

Örnek vermek gerekirse, saldırganlar günümüzde RDP (Uzak Masaüstü) için kaba kuvvet saldırıları yapmadan önce port taraması ve ardından kullanıcı adı tespiti yapmaktadır. Bu nedenle RDP portunu değiştirmiş olmanız saldırganın işini pek de zorlaştırmaz ve sizi bulunmaz hâle getirmez. Saldırgan, bazı tarama araçlarını kullanarak RDP hizmeti açık olan sunucunuzdaki tüm kullanıcı adlarını hızlı bir şekilde tespit edebilir ve sadece o kullanıcı adları için kaba kuvvet saldırısı yapabilir. Bu durum saldırganların işini ve hesaplarınızın birkaçının ele geçirilmesi işlemini kolaylaştırmaktadır. Sunucunuza bağlanmasına izin verdiğiniz kullanıcıların yönetici yetkisine sahip olmaması yine saldırganların işini zorlaştırmaz. Saldırgan, yönetici yetkisi olmayan bir kullanıcının bazı güvenlik zâfiyetlerini kullanarak kullanıcıya yönetici hakları atayabilir.

Peki, sunucunuzdaki bir hesabın ele geçirilmesinin sonuçları neler olabilir?

1) Saldırgan tarafından sunucunuzdaki tüm veriler kriptolanarak kullanılmaz hâle gelebilir ve verilerinizin tekrar kullanılabilir hâle gelmesi için fidye ödeyebilirsiniz.
2) Sunucunuzdaki ya da ağınızdaki veriler saldırgan tarafından sızdırılabilir.
3) Sunucunuz siber saldırı amacı ile saldırgan tarafından kullanılabilir.
4) Sunucunuz, Deep Web'de ve Dark Web'de bulunan pazar yerlerinde silah ve uyuşturucu gibi yasa dışı ürünlerin satılmasına alet edilebilir.
5) Sunucunuz, dünyayı etkileyen zararlı bir yazılımın komuta merkezi olarak ya da barındırılması amacıyla kullanılabilir.

Bunlar sadece beş basit örnektir.

Ülke Bazlı Kaba Kuvvet Saldırıları

Peki, dünya genelinde kaba kuvvet saldırıları ne durumda?

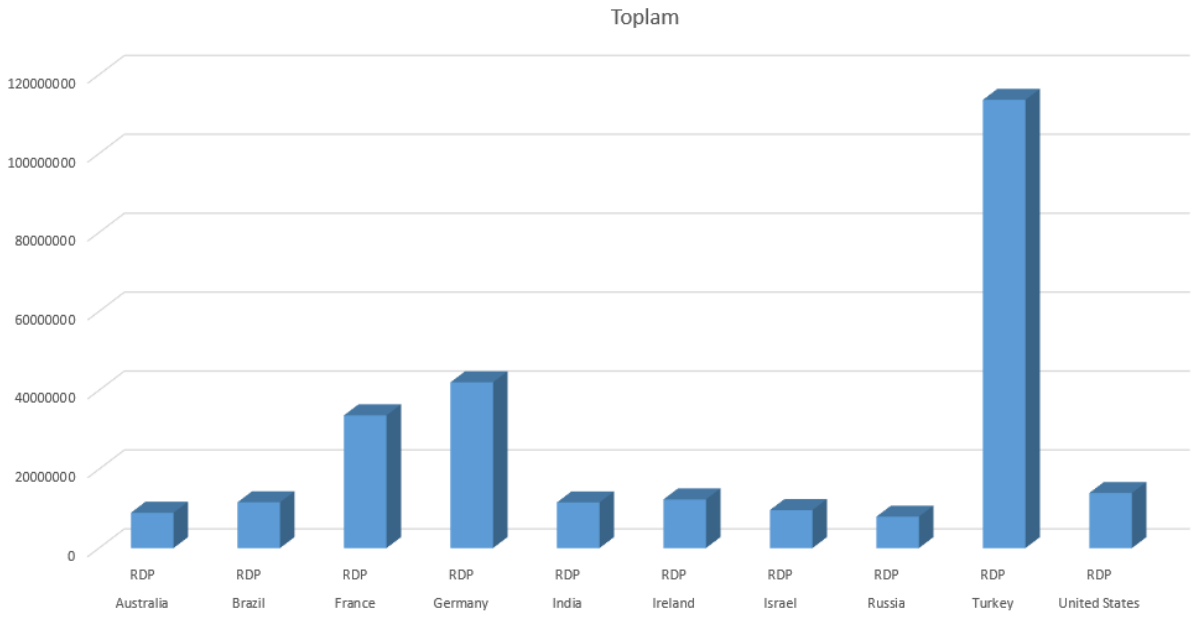
Saldırganlar, genelde, kaba kuvveti ransomware (fidye) saldırıları için kullanırlar. Fidye saldırıları, ciddi gelir elde etmenin ve bir ülkeyi parasal yönden sömürebilmenin en kolay yöntemlerinden biridir.

ParSecure olarak tespit ettiğimiz milyar dolar seviyesinde gelir elde etmiş ve arkasında ciddi destekler olan saldırgan gruplar bulunmaktadır. Ayrıca kullandıkları IP adresleri, veri merkezleri ve private sunucuları tespit edilmiş ve firmamız tarafından dünya genelinde ransomware (fidye) vakalarına maruz kalmış birçok kuruma çözüm hizmeti sunulmuştur.

Saldırganlar, 2017 yılında 5 milyar USD gelir elde ettiler. Dünya ekonomisine ise 609 milyar USD zarar verdiler. Saldırganların 2021 yılında dünya ekonomisine 6 trilyon USD zarar verecekleri öngörülmektedir.

Peki, Türkiye bu saldırıların neresinde yer alıyor?

Türkiye, kaba kuvvet ve doğal olarak fidye saldırılarına uğrayan dünya ülkeleri sıralamasında beşinci; Avrupa ülkeleri arasında ise çoğu zaman birinci sırada yer almaktadır. Bu bilgileri ParSecure veri tabanından alınan bir rapor ile doğrulamak mümkün.



Son 1 yıla ait RDP kuvvet saldırısı alan ülkeler sıralamasına ait tablo.

Türkiye'nin kaba kuvvet ve fidye saldırıları sıralamasına, saldırganların fidye gelirlerine ve dünya ekonomisine verdikleri zararı karşılaştıracak olursak ülkemiz için durumun iç açıcı olmadığı kanaatine varmak hiç de zor olmaz.

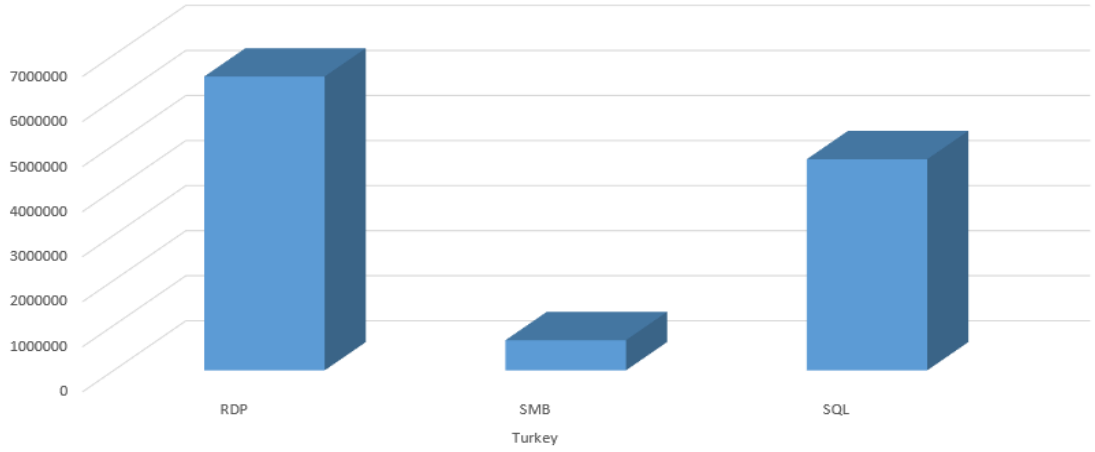
ParSecure honeypotları tarafından tespit edilen, Türkiye'ye yapılan en eski RDP kaba kuvveti, 06.01.2018 00:54:40 tarihinden bu raporun yazıldığı saate kadar devam etmektedir. (13.04.2020)

Türkiye'den Çıkan Kaba Kuvvet Saldırıları

Firewall cihazlarına tanımlanan ülke bazlı IP adresi filtrelemelerini atlamanın yöntemlerinden biri de aynı ülkeye ait bir ya da birden fazla IP adreslerinden yapılan kaba kuvvet saldırılarıdır.

Firewall cihazınızda Türkiye dışında farklı ülkelerdeki IP adreslerinden gelen trafikleri engellemek gibi. Ancak saldırganlar, Türkiye'den savunmasız bir sistemi ele geçirip, ülke bazlı filtreleme yapan bir sisteme saldırı düzenleyebilir. Saldırgan, yukarıda belirttiğimiz yöntemle ülke bazlı yapılan filtreleme kuralını atlayarak saldırıyı başarılı bir şekilde sonuçlandırabilir. Hatta bu durum Türkiye'yi saldırı yapan ilk 8 ülke arasına girmesine sebebiyet verebilmekte.

Türkiye'den çıkan kaba kuvvet saldırılarını inceleyelim.



Türkiye'den Türkiye IP bloklarına RDP, SMB ve SQL kaba kuvvet saldırılarına ait son bir yılın tablosu.

Türkiye'den Türkiye'ye 6 milyonun üzerinde RDP kaba kuvvet yapıldığını bu tabloda görüyoruz. Bu da ülkemizde çok fazla savunmasız sistemlerin olduğunu ortaya koymaktadır.

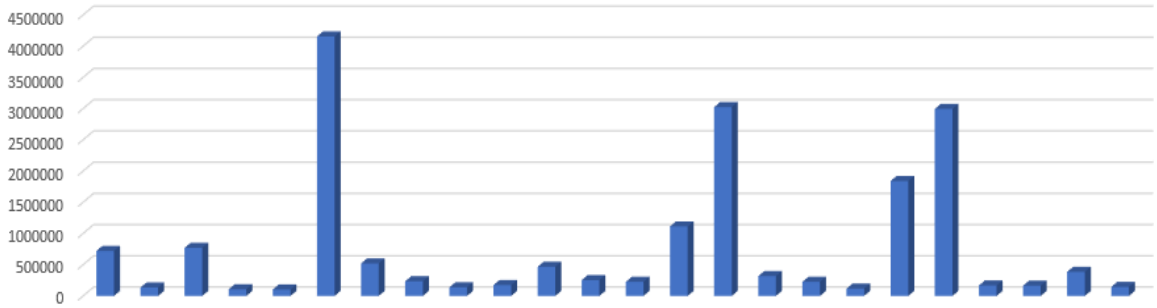
Vaka incelemelerimizde saldırganların ele geçirdikleri sistemleri keşfederken aynı zamanda da kaba kuvvet amacıyla ya da diğer alternatif saldırı amacı için kullandıklarını gözlemlemekteyiz. Saldırganlar, keşif süresi sonunda genelde maddi değeri olan verileri kriptolayarak kullanılamaz hâle getirir ve ardından fidye talep eder.

Bir saldırganın 8 ay boyunca ele geçirdiği sistemde varlığını hissettirmeden keşif yaptığı bilinmektedir.

Firewall cihazlarına tanımlanan farklı bir kuralı atlamanın yöntemi ise, benzersiz binlerce IP adresinin her birinden sadece bir parola denemesidir. Örneğin, saldırgan 10.000 benzersiz IP adresinden 10.000 adet başarılı parola denemesi yapabilmektedir.

Hatta saldırganların aynı internet servis sağlayıcısı üzerinden yaptığı kaba kuvvet saldırılarına da şahit olmaktayız. Örneğin saldırganlar, XX internet sağlayıcısı abonelerine yapacakları kaba kuvvet saldırılarını, yine ele geçirdikleri XX internet sağlayıcı abonelerine ait sistemler üzerinden yapmaktadır. Bu durumu en çok Türkiye deki 5 ISP'den birinde MSSQL kaba kuvvet saldırılarında görmekteyiz.

Türkiye'den en çok çıkan 25 kaba kuvvete internet servis sağlayıcı ve veri merkezi bazlı göz atalım:
Sıralamada firma bilgilerini affınıza sığınarak yanlış anlaşılmaya sebebiyet vermemek için yayınlamıyoruz. Ancak sıralamadan bahsetmek gerekirse 1 ve 2. sırada 2 veri merkezleri sonrasındaki 4 sıra herkesin bildiği ISP ler.



Türkiye'den çıkan kaba kuvvet saldırılarının en çok yapıldığı 25 ISP tablomuzda yer almaktadır.

Daha hızlı, kesintisiz ve güvenilir olması için veri merkezlerini seçen kurumlar, maalesef yaptıkları basit hatalar yüzünden güvenlik kısmını ıskalayabiliyorlar. Güvenlik, kurumunuzun giriş kapısının önüne koyacağınız güvenlik personelinden ibaret olmadığını anlamanın zamanı çoktan geldi. Unutmamak gerekir ki dünyanın en iyi 10 güvenlik duvarını sunucunuzun önüne koysanız da yapacağınız basit bir hata felâketle sonuçlanabilir. İşte bu nedenle kalıplaşmış güvenlik ürünlerini canlı siber istihbarat servisleri ile beslemek gerekmektedir. Birkaç saat sonra ya da bir gün sonra gelecek imza tabanlı güvenlik sizin için geç kalınmış olabilir.

Yukarıdaki tabloda dikkatinizi çekmek istediğimiz önemli ancak görmediğiniz kısımlardan biri de National Academic Network. RIPE' de Türkiye devlet üniversiteleri, National Academic Network and Information Center olarak geçer. Tablodan anlaşılacağı gibi üniversitelerimizden de kaba kuvvet saldırıları çıktığı ParSecure sensörleri tarafından tespit edilmiştir. Üniversitelerimizin savunmasız sistemleri, saldırganlar tarafından ele geçirilerek saldırı amacı ile kullanılabiliyor.

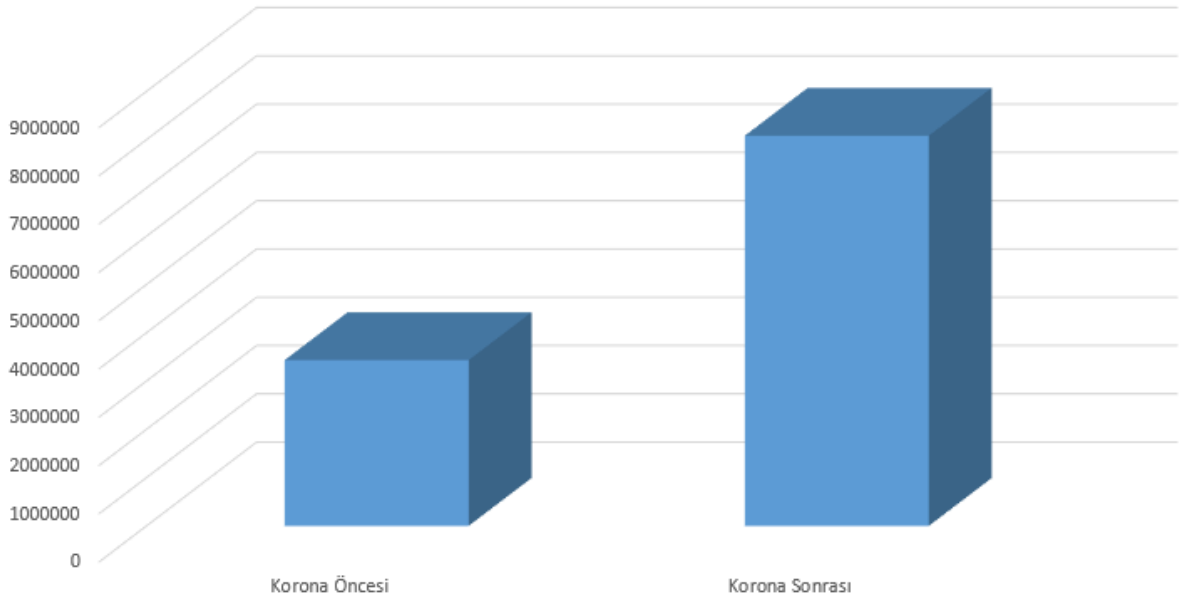
Ya da..

ParSecure siber güvenlik olarak yaptığımız tespitler doğrultusunda ilgili kurumları bilgilendiriyoruz ve saldırganların faaliyetlerini sonlandırarak kurumların bu durumdan zarar görmelerinin önüne geçmeye çalışıyoruz.

Geçmişte benzer bilgilendirmeleri üç büyük operatöre yapsak da sesimizi sadece bir operatöre duyurabildik.

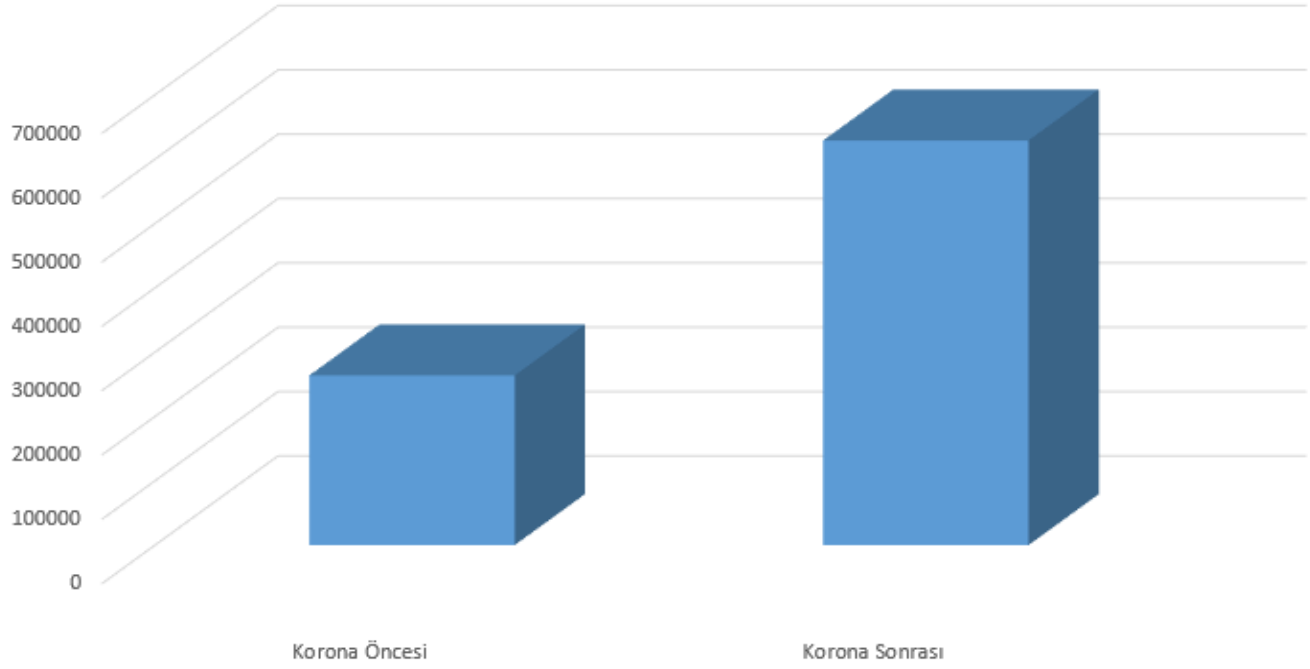
Korona Virüsü, Kaba Kuvvet Saldırılarında Türkiye Nasıl Etkilendi?

Bu sorunun cevabını ülkemizde Korona vakalarının ilk açıklandığı 11 Mart 2020 tarihinden 1 ay öncesine ve 1 ay sonrasına ait Türkiye'ye gelen kaba kuvvet saldırılarını ParSecure veri tabanımızdan alınan raporlara ait tablolarda inceleyelim.
Dikkatinizi çekmek istediğimiz bir diğer konu aşağıdaki tabloda yer alan artışa oranla çok fazla fidye (ransomware) vakalarının Türkiye'de yaşandığını gözlemlemekteyiz.



Ülkemizde Korona vakalarının ilk açıklandığı 11.03.2020 tarihinden itibaren bir önceki aya göre Türkiye'ye gelen kaba kuvvet saldırılarında 4.5 milyon artış gözlemliyoruz.

İnceleyeceğimiz bir diğer tablo da ülkemizde ilk Korona vakalarının açıklandığı tarihten sonra Türkiye'den çıkan kaba kuvvet saldırılarındaki değişikliği gösteren tablodur. Birçok kurum, evden çalışma sistemine geçtikten sonra sunucularını korunmasız olarak internete açtı. Bu durum saldırganların daha fazla sistemin ele geçirmesini ve Türkiye'den çıkan saldırıların artış göstermesine sebebiyet verdi.



Yukarıdaki tabloda ülkemizde Korona vakalarının ilk açıklandığı 11.03.2020 tarihinden itibaren bir ay içerisinde, bir önceki aya göre Türkiye'den çıkan RDP kaba kuvvet saldırılarında 400.000 artış gözlemliyoruz.

Dünya Genelinde Aralıksız RDP Kaba Kuvvet Çıkışı Olan IP Adresleri

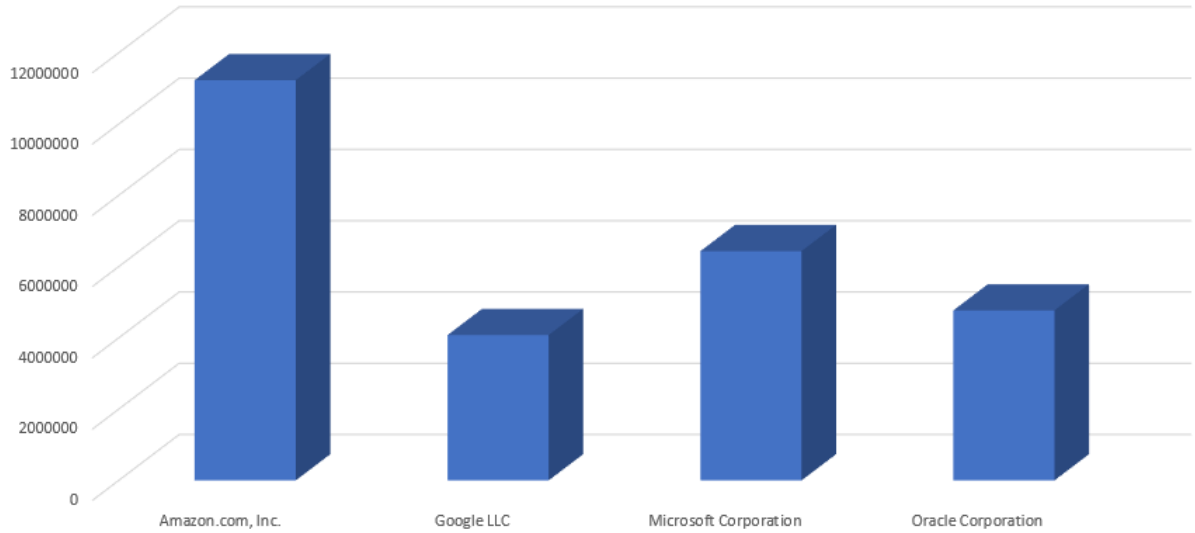
Dünya genelinde 2017 ve 2018 yılından bugüne kadar aralıksız devam eden kaba kuvvet saldırılarını incelediğimizde çıkan sonuca ait ilk 10 IP adresleri aşağıdaki gibidir.

IP Adres	Başlangıç	Son atak
58.218.204.196	14.05.2017 15:53	15.04.2020 02:52
80.211.133.41	13.08.2017 18:12	15.04.2020 04:44
200.153.11.82	24.04.2018 06:06	15.04.2020 01:40
71.41.84.2	1.06.2018 10:39	15.04.2020 17:26
92.62.65.128	9.08.2018 17:34	15.04.2020 18:26
61.164.219.59	14.08.2018 08:06	15.04.2020 08:07
129.158.123.254	10.10.2018 17:17	15.04.2020 23:04
5.188.206.26	11.10.2018 20:40	15.04.2020 04:37
193.169.252.69	7.12.2018 16:16	15.04.2020 02:34
212.116.73.22	24.12.2018 14:29	15.04.2020 16:03

Yukarıdaki liste güvenlik araştırmacılarına ilham verebilir. Ortak çalışmalar yapabileceğimiz Türk güvenlik araştırmacılarıyla yukarıdaki listede yer almayan, tespit ettiğimiz private IP adreslerini paylaşabileceğimizi belirtelim.

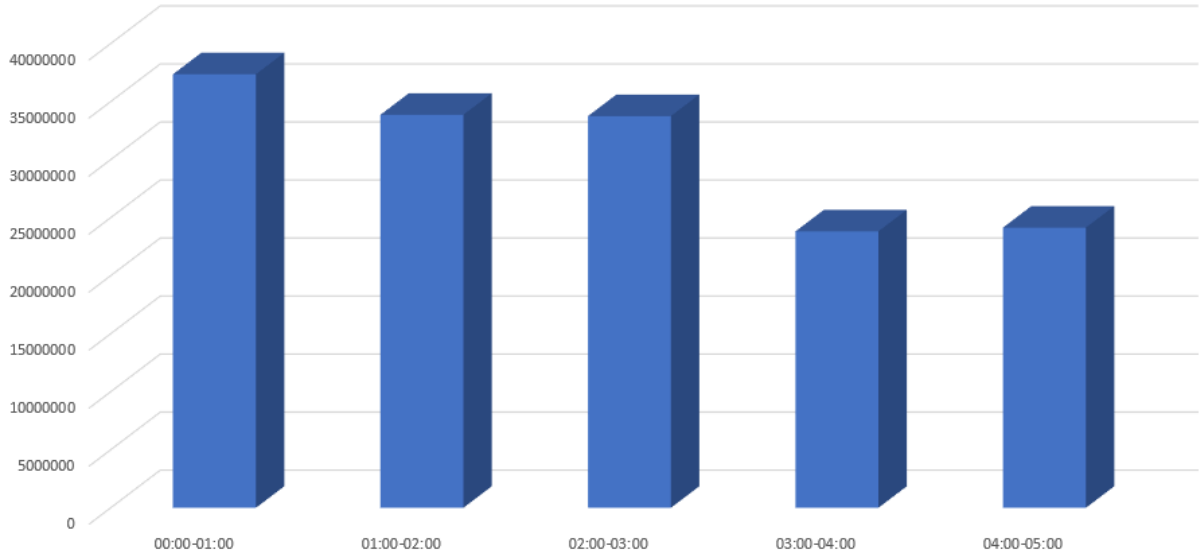
Kısa Süreli Ücretsiz Bulut Hizmetleri ile İstismar Edilen 4 Büyük Firma

Aşağıdaki tabloda insanların bulut hizmetlerini ücretsiz deneyebilmelerine imkân tanıyan 4 büyük firma bulunmaktadır. Ancak saldırganların ücretsiz kullanım kredilerini istismar ederek kaba kuvvet amaçları için kullandığını görmekteyiz. Bu gibi durumlar için tüm ISP ve Veri Merkezlerinin önlem almaları insanlık için faydalı olacaktır.



En Çok Kaba Kuvvet Saldırısı Yapılan 5 Saat Aralığı

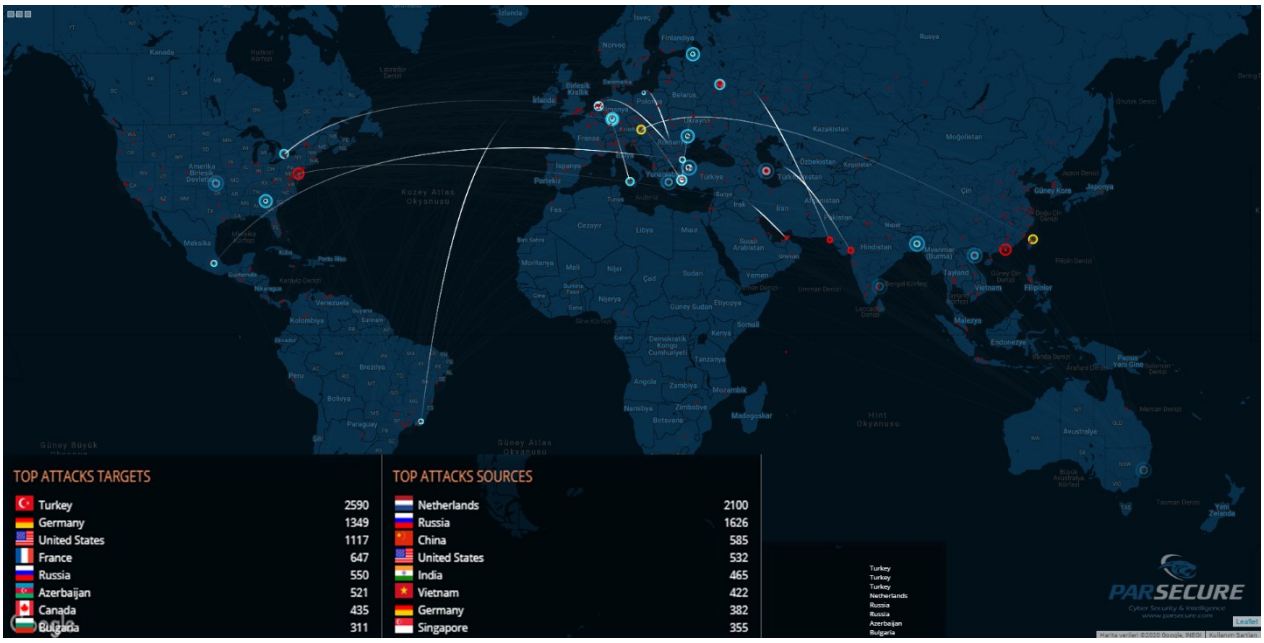
Mesai saatlerinde olası bir siber saldırıya müdahale imkanı çok zordur. Saldırganlar genelde saldırılarını ilgili ülkelerin mesai saatleri dışında yaparlar.
Saldırganların en çok kaba kuvvet saldırısı yaptıkları saat aralıkları aşağıdaki listede yer almaktadır. İlgili saat aralıkları için farklı güvenlik önlemleri almak mümkün olabilir.



Medyanın Siber Saldırılardaki Gücü

ParSecure honeypotlarından gelen bilgiler canlı olarak **www.parsecuremap.com** gerçek zamanlı siber saldırı haritasını besler.

Kaba kuvvet saldırıları alan ilk 10 ülke sıralamasında Amerika genellikle son sıralarda yer almaktaydı. Son günlerde, Amerika'nın Korona virüs salgınından en fazla etkilendiği ve zor günler geçirdiği söylenen haberlerin çokça çıkmasının ardından Amerika, **parsecuremap.com** gerçek zamanlı siber saldırı haritamızda ilk 3'te yer almaya başladı.



Yaptıkları saldırıların ardından umduklarını bulan saldırganlar salgının ardından daha da iştahlı olacaklardır ve Amerika sıralamasını korumaya devam edecektir.

Türkiye'de En Çok Kaba Kuvvet Saldırısı Yapılan Kullanıcı Adları

Türkiye'de en çok kaba kuvvet saldırısı yapılan ilk 25 kullanıcı adını aşağıdaki listede bulabilirsiniz. Yazımızın başında belirttiğimiz gibi saldırganlar kaba kuvvet saldırılarında bazı zafiyetleri sömürerek yada oluşturdukları veri tabanları sayesinde saldırılarının daha kısa sürede olumlu sonuçlanmasını sağlayabiliyorlar.

Aşağıda yer alan kullanıcı adları için farklı güvenlik kuralları uygulayabilirsiniz. ParSecure Siber Güvenlik Yazılımı sizi sistemlerinizde denenen kullanıcı adlarına ve exploitler sayesinde sunucularınızda oluşturulan kullanıcılara karşı sizi uyarır.

Kullanıcı adı
administrator
ADMINISTRATOR
ADMIN
Admin
root
SA
Server
UZAK
Depo
UZAK1
PLANLAMA
muhasebe
USER1
UZAK2
YÖNETICI
UZAK3
ARGE
LOGO
MUHASEBE2
YONETICI
Test
dkullanıcı
VEGA
ETA
TERMINAL

ParSecure ailesi olarak bilişim sistemlerinizin güvende olduğu sağlıklı günler dileriz.