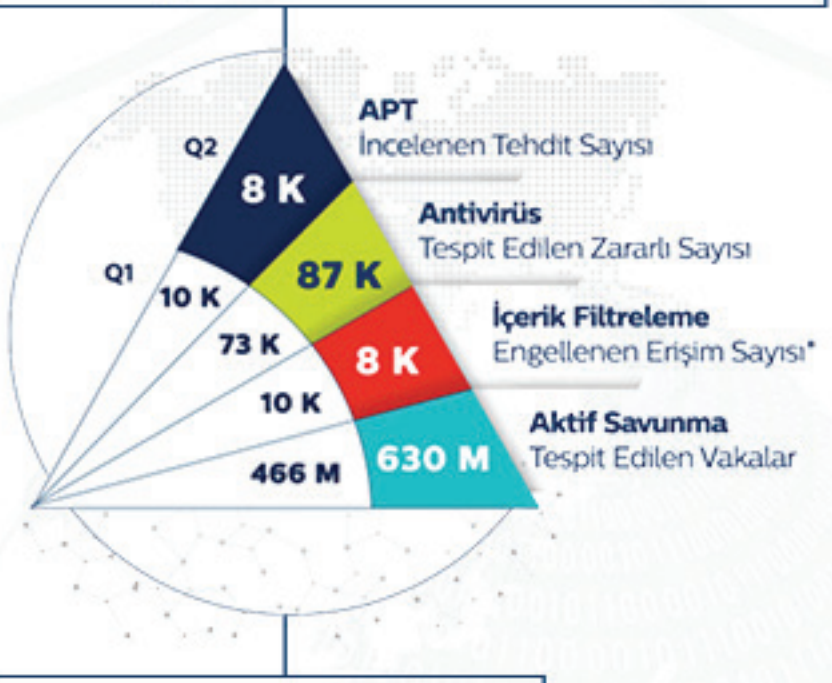
Türk Telekom Siber Bülten

Türk Telekom
Değerli Hissettirir

2. Sayı

Vaka trendleri: Türk Telekom siber güvenlik servisleri tarafından tespit edilen tehditler

2020 Çeyrek Bazlı Vaka Trendleri



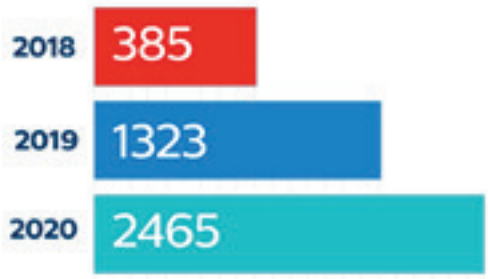
*İçerik filtreleme, USOM kategorisinde engellenen erişim sayısını göstermektedir.

DDOS Atak Trendleri

DDOS 1Gbps üzeri atak sayısı	Q1 1.2 K	Q2 1.3 K
DDOS En yüksek atak boyutu	Q1 372 Gbps	Q2 242 Gbps

Geçmiş yıllara göre DDOS atak sayılarında önemli artış gözlenmektedir.

1 Gbps üzeri DDOS Atak Sayıları*



*İlgili yıllar için Mayıs YTD karşılaştırmasıdır.

Globalde Yaşanan Siber Saldırılar

World Health Organization

Dünya Sağlık Örgütü siber saldırılarda 5 kat artış olduğunu bildirdi.

amazon web services

Amazon, bugüne kadar yapılmış en büyük DDOS saldırısına maruz kaldı (2,3 Tbps).

Yerel Etkileri Bulunan Tehditler

“Toplu Taşıma Belgeleri.xls” Zararlı Dosya İncelemesi

COVID-19 salgını nedeni ile şehirlerarası seyahat kısıtlaması ve seyahat izin belgesi gündemi konuşulurken, “Toplu Taşıma Belgeleri.xsl” adında bir zararlı yazılımın saldırganlar tarafından oltalama amacı ile kullanıldığı tespit edilmiştir. Son dönemde, oltalama saldırılarında “xls, docx, pdf” uzantılı dosyaların kullanımının yaygınlaştığı gözlemlenmektedir.

“xsl” uzantılı belge Türk Telekom APT servisi tarafından analiz edilmiş ve dosyanın içerisinde yer alan URL adresine kullanıcıların istekte bulunması halinde, saldırgan tarafından oluşturulan komutun ilgili sistemlere yerleşmesi için tasarlandığı anlaşılmıştır. Zararlı davranışın tespit edilmesi üzerinde **Türk Telekom Antivirüs** ve **İçerik Filtreleme** servisleri tarafından engellenmiştir.

Dosya HASH Bilgisi:

“ Toplu Taşıma Belgeleri.xls “

MD5 edb7b61f93ab49ef35d1924d2495e06b

SHA-256fc93592b044f73f95690e28f79990e53016335e4d10dfe2368a09ded2e58d85a

Global Etkileri Bulunan Tehditler

IoT Cihazlarını Hedefleyen Yeni Kötü Amaçlı Yazılım - Kaiji

"Kaiji" olarak bilinen yeni bir Linux kötü amaçlı yazılım türü, SSH kaba kuvvet saldırıları yoluyla nesnelerin interneti (IoT) cihazlarını hedefliyor. Intezer güvenlik firmasının araştırmacıları, IoT cihazlarını ve sunucularını SSH kaba kuvvet teknikleri ile hedefleyen botnet'i gözlemlediklerini ve Nisan ayında bu Linux kötü amaçlı yazılıma rastladıklarını açıkladı.

"Kaiji" olarak adlandırılan tehdidin, saldırı işlevlerinin çoğunu açık kaynaklı ve bilinen kötü amaçlı yazılım kodları ile türetmediği için diğer IoT botnet'lerinden farklı olduğunu belirttiler. Bu zararlı yazılımı yayan saldırganların, Kaiji'yi nadir bir programlama dili olan Golang'ı kullanarak sıfırdan yazdıklarını açıkladılar.

Kaiji'yi diğer dijital tehditlerden ayıran tek şey programlama dili değildi. Intezer, ayrıca Kaiji'nin kök kullanıcıyı özel olarak hedeflemek için SSH kaba kuvvet tekniğinin kullanımına tanık oldu. Bu tür saldırılar yalnızca yetkili kullanıcılara verilen ağ erişim yetkilerinin kullanımı ile mümkündür. Bu nedenle kötü amaçlı yazılımın, bulaştığı kaynakları bot'a dönüştürerek saldırganlar tarafından DDoS saldırıları için de kullanılmasına olanak vermektedir.

3- Şüpheli IP Adresleri

104[.]152[.]52[.]18
109[.]70[.]100[.]32
128[.]14[.]209[.]154
128[.]14[.]209[.]226
128[.]14[.]209[.]234
128[.]14[.]209[.]242
138[.]99[.]216[.]112
156[.]96[.]119[.]148
156[.]96[.]156[.]39
156[.]96[.]58[.]108
162[.]243[.]135[.]174
162[.]243[.]136[.]153
162[.]243[.]136[.]201
162[.]243[.]138[.]145
162[.]243[.]138[.]174
162[.]243[.]138[.]179
162[.]243[.]138[.]186
162[.]243[.]138[.]190
162[.]243[.]139[.]116
162[.]243[.]139[.]142
162[.]243[.]139[.]48
162[.]243[.]140[.]109
162[.]243[.]142[.]247
162[.]243[.]143[.]109
162[.]243[.]143[.]11
162[.]243[.]144[.]244
162[.]243[.]144[.]4
162[.]243[.]144[.]44
162[.]243[.]144[.]57
162[.]243[.]145[.]55
167[.]172[.]179[.]39
173[.]212[.]225[.]214
185[.]142[.]236[.]34
185[.]142[.]41[.]223
185[.]156[.]73[.]64
185[.]172[.]111[.]206
185[.]172[.]111[.]210
185[.]234[.]216[.]198
185[.]234[.]218[.]174
185[.]234[.]218[.]239
192[.]241[.]209[.]175
195[.]3[.]146[.]114
195[.]54[.]160[.]130
209[.]126[.]1[.]2
213[.]217[.]0[.]184

223[.]71[.]167[.]166
27[.]115[.]124[.]10
27[.]115[.]124[.]9
34[.]235[.]123[.]193
34[.]243[.]174[.]205
45[.]95[.]168[.]97
52[.]167[.]219[.]241
71[.]6[.]147[.]254
80[.]82[.]77[.]214
82[.]221[.]105[.]7
91[.]199[.]118[.]138
94[.]102[.]49[.]190
118[.]70[.]113[.]1
162[.]243[.]138[.]182
162[.]243[.]143[.]210
185[.]234[.]218[.]239
37[.]49[.]226[.]245
51[.]15[.]80[.]14
62[.]210[.]37[.]82
78[.]188[.]119[.]233
80[.]82[.]77[.]240
37[.]49[.]226[.]250
37[.]49[.]230[.]180
38[.]39[.]232[.]172
45[.]125[.]65[.]74
45[.]141[.]87[.]4
45[.]143[.]220[.]122
45[.]14[.]44[.]242
45[.]14[.]45[.]2
45[.]148[.]10[.]62
45[.]148[.]10[.]93
45[.]227[.]254[.]30
45[.]56[.]78[.]64
45[.]95[.]168[.]97
47[.]57[.]86[.]202
51[.]89[.]234[.]101
52[.]167[.]219[.]241
61[.]147[.]103[.]136
62[.]171[.]160[.]189
66[.]240[.]236[.]119
71[.]6[.]147[.]254 11
71[.]6[.]199[.]23
77[.]247[.]110[.]30
78[.]128[.]113[.]6
78[.]138[.]96[.]3

80[.]82[.]77[.]214
80[.]82[.]77[.]33
82[.]221[.]105[.]7
88[.]218[.]17[.]114
89[.]248[.]167[.]131
89[.]248[.]168[.]223
89[.]248[.]168[.]62
89[.]248[.]171[.]97
89[.]248[.]174[.]151
89[.]248[.]174[.]215
89[.]248[.]174[.]219
91[.]199[.]118[.]138
92[.]118[.]37[.]64
94[.]102[.]49[.]190
95[.]111[.]231[.]14
96[.]127[.]169[.]2
195[.]62[.]32[.]200
198[.]20[.]103[.]178
199[.]34[.]228[.]59
207[.]180[.]220[.]254
208[.]91[.]109[.]50
208[.]93[.]152[.]20
208[.]93[.]152[.]30
209[.]126[.]1[.]2
213[.]217[.]0[.]184
223[.]71[.]167[.]166
23[.]254[.]128[.]8
2[.]56[.]176[.]34
27[.]115[.]124[.]10
27[.]115[.]124[.]9
27[.]34[.]30[.]58
31[.]155[.]76[.]231
34[.]235[.]123[.]193
34[.]243[.]174[.]205
35[.]208[.]6[.]125
37[.]187[.]152[.]112
37[.]230[.]116[.]62
37[.]49[.]226[.]161
37[.]49[.]226[.]227
37[.]49[.]226[.]236

Not: Cihaza ekleme yaparken Word içerisinde ctrl+h kombinasyonu ile [.] > . işlemini yaparsanız eklemede kolaylık sağlayacaktır.

Gelişen siber saldırılara karşı etkin koruma: Türk Telekom Siber Güvenlik Servisleri

Türk Telekom olarak her geçen gün gelişen ve çeşitlenen siber saldırılara karşı ihtiyacınız olan korumayı, uzman kadromuz ve güçlü altyapımız ile her ölçekteki kurumsal müşterimizin hizmetine sunmaktayız. Her sayıda farklı ürün & servis içeriklerine yer vereceğimiz siber bültenin bu sayısında servis kataloğumuzdan, L7 DDOS atak önleme ve DDOS atak simülasyonu servis detaylarını bulabilirsiniz.

L7 Inline DDOS Atak Önleme Servisi

TÜRK TELEKOM ÖNERİYOR UZMANLARI

Türk Telekom L7 Inline Koruma

- Tüm ME hızlarına karşılık bir koruma kapasitesi tahsis edilir.
- Capex maliyeti oluşmaz. Aylık ödeme modeli ile hizmet alınabilir.
- Yönetimi alanında uzman Türk Telekom teknik ekibi yapar ve uygulamalarınızı 7/24 izler.

Onprem Çözümler

- Onprem kutu kapasitesi Arbor'da en küçük 500 MB, A10'da is 5 GB'dir.
- Kurulum, bakım ve destek için ek opex, lisans için capex maliyeti oluşur.
- Personel maliyeti oluşur.

DDOS Atak Simülasyonu

DDOS atakları web siteleri, e-posta sistemleri, online ödeme sistemleri gibi internete açık platformların karşılayabileceğinin daha üzerinde sahte yoğunluk yaratılması ya da hedef sistemin kaynaklarının yüksek oranlarda tüketilmesi ile servislerin yayınını engellemek ve işlevsiz kılmak için gerçekleştirilen siber saldırılardır.

Kurumlar hem kendi hem de servis sağlayıcı network'lerine yatırım yaparak L3, L4 ve/veya L7 tiplerindeki ataklara karşı önlem almaktadırlar. Bu noktada yapılan yatırımların saldırılara karşı ne oranda koruma sağladığı noktasında test ihtiyacı doğmaktadır.

Türk Telekom bu ihtiyacı hedef alarak Siber Güvenlik alanındaki tecrübesiyle kendi DDOS atak simülasyon platformunu oluşturmuştur. Bu platform ile kurumlara DDOS ataklarının tespiti ve cevap yeteneklerini belirleyerek olgunluk seviyesini ölçümleme imkânı sunmaktadır.

33 Farklı L3,L4 ve L7 atak tipleri

70 Gbps (max)

200+ BotNet

DDOS Olgunluk Raporu

Siber Sözlük

HASH Değeri:
Dosyaların kendilerine özel parmak izleridir. Hash değerine göre dosyada değişiklik yapılıp yapılmadığını, dosyanın düzgün bir şekilde bilgisayarınıza inip inmediğini kontrol edebilirsiniz.

Oltalama Saldırısı:
İnternet tarihinin en eski ve en etkili saldırı türlerinden biridir. Bu saldırı türünde genel olarak kurbanların e-posta hesaplarına hediye, indirim veya benzeri cezbedici sahte iletiler gönderilerek parola, kimlik bilgisi ya da hassas verilerin çalınması amaçlanır.

İletilen e-posta mesajlarındaki zararlı bağlantılar tıklandığı zaman kurbanın av olması sağlanabildiği gibi e-postalar ile birlikte ek olarak gönderilen virüslü dosyaların çalıştırılması ile kurbanların bilgisayarları saldırganlar tarafından ele geçirilebilir.

SSH Kaba Kuvvet Saldırısı:
Brute force saldırısı olarak da geçen bu yöntem hackerların herhangi bir kullanıcı hesabına erişmek için deneme-yanılma yöntemi kullanmasına denir.

Bot:
Bilgisayar veya yazılımlar üzerinde herhangi bir aktiviteyi yerine getirmekten sorumlu olan otomatik çalışan yazılımlardır. Botların temel amacı insanları taklit ederek, insan aktvitelerini kendi başlarına daha hızlı şekilde gerçekleştirmeleridir.

Ele geçirilmiş olan bilgisayarlar saldırganlar tarafından verilen komutları uygulamak üzere kullanılabilir. Bu cihazlara bot (zombi bilgisayar) denilmektedir.

Botnet:
Saldırganlar tarafından ele geçirilmiş zombi cihazlar ağına botnet denir. Botnet'ler saldırganların komutlarını uygulayarak yüksek hacimli DDOS saldırılarına neden olabilir.

Kurumumuza özel teknolojik çözümlerimiz ile ilgili detaylı bilgi almak için Türk Telekom satış yöneticiniz ile iletişime geçebilirsiniz.

BU İŞTE BERABERİZ

Türk Telekom
Değerli Hissettirir