Türk Telekom Siber Bülten

Türk Telekom
Değerli Hissettirir

1. Sayı

Giriş:

COVID-19 salgını ile birlikte çalışma, iletişim kurma ve iş yapış şekillerimiz hızla değişiyor. Bazı özel şirketler, kamu kurumları ve bankalar, çalışanların evden çalışmasını zorunlu kılmaya başladı. Birçok çalışan için bu ilk kez yaşanan bir deneyim, şirketler uzaktan çalışmaya tüm çalışanları ve sistemleri ile adapte olmaya çalışırken hacker'lar da bu durumu fırsat bilerek siber saldırı çeşitlerini geliştiriyor.

Dünya, Koronavirüs salgını ile mücadele ederken, siber saldırganlar, insanların endişesini ve merakını kötü amaçlı yazılım yaymak ve zarar vermek için kullanıyor. Bu çoğunlukla, Koronavirüs ile ilgili bilgi ve istatistiklerin bulunduğu söylenen uygulamalara yönlendirilerek yapılıyor.

E-posta ile gönderilen ya da web sitesinde bulunan dosya ve bağlantılar çalıştırıldığında, saldırganlar zararlı içeriği kullanıcı sistemlerine bulaştırmış oluyor.

Güncel Global Tehditler

Siber saldırganlar kötü amaçlı yazılım yaymak için son kullanıcı router'ları ele geçiriyor.

Router'lara yapılan DNS saldırıları, bilgi çalan kötü amaçlı yazılım içeriğiyle binden fazla kurbanı hedef aldı. Siber suçlular, kurbanları sahte Koronavirüs uygulamaları tanıtan saldırganların kontrolündeki sitelere yönlendirmek için router cihazlarının açıklarından yararlanarak DNS ayarlarını değiştiriyor.

Saldırganların savunmasız router'ları internetten araştırıp, brute force (kaba kuvvet saldırıları, hacker'ların bir hesaba erişmek için deneme yanılma yöntemi kullanması) saldırı yöntemi ile şifre güvenliğini aşmayı ve DNS IP ayarlarını değiştirmeyi hedefledikleri ortaya çıkmıştır.

Saldırganlar, router'ları ele geçirdikten sonra, DNS'te bulunan IP adreslerini değiştirerek kullanıcıların girdikleri web sitesi adını, kendi denetimlerinde bulunan sahte sitelere yönlendirebilirler. Bu sitelere ulaşmaya çalışan kurbanlara, daha fazla Koronavirüs bilgisi ("indir" butonu aracılığıyla) sunan bir uygulama yüklemelerini söyleyen ve Dünya Sağlık Örgütü gibi davranan bir mesaj gösterilir. Bu butona tıklayan kullanıcılar zararlı yazılımı bulaştırmış olurlar.

Koronavirus (COVID-19) kimlik avı ve kötü amaçlı yazılımlara karşı dikkatli olun!

Son dönemde siber suçluların bilgisayarları enfekte ederek, uygulamalara giriş ve kişisel bilgilerin çalınmasına neden olabilecek sahte e-posta ve SMS kimlik avı saldırıları göndermek için Koronavirüsten yararlandıkları görülmektedir.

Kullanıcılara gönderilen SMS tabanlı kimlik avı saldırısı, mesaj içerisinde "COVID-19 güvenlik hattı semptomları ile ilgili yeni bir mesaj" olduğunu ve test yaptırabileceğiniz tesislerin yerini gösteren bir mesaj içeriği ile kişilerin verilerini ele geçirme konusunda ortaya çıkmış bir saldırı şeklidir.

Tokyo 2020 Olimpiyatları'na bilet satan şüpheli alan adları

Koronavirüs pandemisi nedeniyle Tokyo 2020 Olimpiyatları'nın açılışında belirsizlik yaşandığı dönemde, siber suçlular etkinlikten kötü amaçlı faydalanmanın yollarını bulmak için çalıştılar.

Büyük spor etkinlikleri ve turnuvalar gibi küresel ilginin merkezinde yer alan etkinlikler, saldırganlar tarafından kullanıcıları kimlik avı dolandırıcılığı, kötü amaçlı yazılım kampanyaları ve kişisel ve ödeme ayrıntılarının çalınması için kandırmak için sıklıkla kullanılır.

Alan adlarını kontrol ettiğimizde aşağıdaki gibi tehlikeli gördüğümüz domain'leri sizler için sıraladık.

1. **tickets-tokyo2020[.]com**
2. **euro-2020-tickets[.]com.**
3. **olympic2020tickets[.]com**
4. **eurosportstickets[.]com**
5. **ticketsmarketplace[.]co.uk**

TOKYO 2020

Zoom'da yeni zero day

Pandemi döneminde, Zoom'un bilinirliği ve kullanımı oldukça arttı, ancak aynı zamanda şirketin güvenlik uygulamalarına ve gizlilik vaatlerine daha fazla odaklanmaya yol açtı. Windows güvenlik şifrelerini çalmak için kötüye kullanılabilecek bir Zoom hatası bulan iki güvenlik araştırmacısının yanı sıra, web kamerasına ve mikrofona dokunmak da dâhil olmak üzere Zoom kullanıcısının Mac'ini ele geçirmek için kullanılabilecek iki yeni hata daha bulundu.

Bu hatalardan yararlanan saldırganlar, kullanıcı bilgisayarının iç kısımlarına kalıcı erişim elde edebilir ve bu bilgileri gizleyebilir, böylece kötü amaçlı yazılım veya casus yazılım yükleyebilirler.

Zoom, Mac uygulamasını kullanıcı etkileşimi olmadan yüklemek için "malware (kötücül yazılım)" tekniği kullanır. Düşük yetkili kullanıcı ayrıcalıklarına sahip yerel bir saldırganın, "root" olarak bilinen en üst düzey kullanıcı ayrıcalıklarını elde etmek için Zoom yükleyicisine kötü amaçlı kod enjekte edebileceğini buldu.

Bu temel seviyedeki kullanıcı ayrıcalıkları, saldırganın çoğu kullanıcı için genellikle kapalı olan temeldeki macOS işletim sistemine erişebileceği anlamına gelir ve bu da kullanıcının fark etmeden kötü amaçlı yazılım veya casus yazılım çalıştırmasını kolaylaştırır.

İkinci hata ise, Zoom'un Mac'lerde web kamerasını ve mikrofonu nasıl ele aldığı konusunda bir açıktan yararlanıyor. Siber saldırganların, Zoom'a kötü amaçlı kod enjekte ederek Zoom'un sahip olduğu web kamerası ve mikrofona erişim verebileceği gözlemlendi. Saldırgan, Zoom'u kötü niyetli kodunu yüklemek için kandırdığında, kod Zoom'un erişim haklarından herhangi birini veya tümünü otomatik olarak devralır ve Zoom'un web kamerasına ve mikrofona erişimini sağlar.

Son dönemde yaşanan saldırılardan dolayı Zoom çeşitli güncellemeler yayınlayarak bu açıkları kapatmaya çalışıyor. Zoom güncel değil ise Zoom'un web sitesi ya da mobil uygulaması üzerinden güncelleme yapılabilir.

Türk Telekom Kurumsal Güvenlik Servisleri Tarafından Tespit Edilen Vakalar

Aktif Savunma (IPS) servisinde tespit edilen vaka

IPS ağ trafiğini olası bir saldırı için izler. Potansiyel olarak tehlikeli aktivite tespit ettiğinde, saldırıyı durdurmak için harekete geçer. Bu saldırılar genellikle kötü amaçlı paketlerin engellenmesi, ağ trafiğinin engellenmesi veya bağlantıların sıfırlanması şeklinde olur. IPS olası zararlı etkinliklerle ilgili alarm da oluşturabilir.

Bugünün IPS çözümleri genellikle bir saldırıyı belirlemek için farklı yöntemler kullanır. İmzaya dayalı algılama, bilinen istismarların işaretlerini arar. Önceden tanımlanmış bir saldırı ile ilişkili etkinlik bulduğunda, saldırıyı engellemek için harekete geçer. Bu tür algılama, yalnızca önceden tanımlanmış saldırıları durdurabilmesi nedeniyle geleneksel antivirüs teknolojisine benzer.

Atakları tanımlamak için diğer bir yöntem ise istatistiksel anomali temelli tespittir. Bu tekniği kullanan bir IPS, mevcut ağ etkinliğini normal olanla karşılaştırır. Bir sapma bulduğunda, bir uyarı gönderebilir veya başka önleyici tedbirler alabilir. Bu yaklaşım ile sıfırıncı gün saldırılarının tespitine yardımcı olurken false positive'leri (yanılma payı) beraberinde getirmektedir.

Sıfırıncı gün ataklarına karşı IPS tek başına yeterli değildir, bu nedenle APT servisi ile birlikte kullanılması daha etkin koruma sağlar.

• IPS servisinde profili etkin olan müşterileri baz aldığımızda, 2020 yılının ilk çeyreğinde yaklaşık 2,7 milyar IPS imzası ile eşleşen erişim olduğu gözlenmiştir.
• Tespit edilen imzalar kategorize edilip incelenmiş ve bu inceleme sonucunda kritik kategoride en fazla rastlanan tehdidin router cihazlarındaki açıktan faydalanarak uzaktan kod enjekte eden bir zafiyet olduğu belirlenmiştir.

Tespit edilen güvenlik açığı: Kimliği doğrulanmamış komut enjeksiyonu

Saldırı vektörü: Uzaktan kod çalıştırma

Tehdit: LAN'daki kimliği doğrulanmamış bir saldırgan tarafından kullanılması

Bu zararlının aktiviteleri:

• Ağ trafiğini gizlice dinlemek ve arka kapı açmak için kurumsal switch'leri, load balancer, router ve VPN gateway cihazlarını etkileyen iki kritik uzaktan komut enjeksiyon yöntemi ile zafiyet oluşturmaktadır.
• Bu zafiyet saldırganlar tarafından, yetkisiz uzak bağlantı kurmak ve sistemlere komut enjekte etmek için kullanılabilir.
• IPS servisi ile bu açıktan faydalanmak isteyen tehditler tespit edilmiş ve gerekli aksiyonlar alınmıştır.

Gelişmiş Tehdit Önleme (APT) servisinde tespit edilen vakalar

APT servisi alan bir banka müşterimize gönderilen dosya incelendiğinde aşağıdaki şekilde zararlı aktivite olduğu tespit edilmiştir.

• Şüpheli dosya incelendiğinde saldırganlar tarafından sızma işlemlerinde kullanılan duckdns* diğer adıyla Dinamik DNS ile ilişkili bir domain'e sahip olduğu gözlemlenmiştir.
• Şüpheli dosya çalıştırıldığında içerisinde bulunan komutun tetiklenmesi durumunda saldırgan tarafından daha önce oluşturulmuş olan "vbc.exe" zararlı yazılımının ilişkili URL üzerinden indirilmesi sağlanıp, kritik kullanıcı verilerinin ele geçirilmesine yönelik işlemlerin gerçekleştiği gözlenmiştir.

***Duckdns (Dinamik DNS)**: Kullanıcıların statik bir IP adresine sahip olamadığı durumlarda bu hizmeti dolaylı yoldan almasını sağlayan bir teknolojidir IP adresinizin üzerine bir hosting açar ve bu hosting'de sizin IP adresinizi sabitler.

Sandbox cihazında yapılan incelemelerde diğer bir zararlı yazılımın ise, CORONOVIRUS COVID-19 DOCUMENT_zip.arj isimli dosya ile mail olarak gönderildiği tespit edilmiştir.

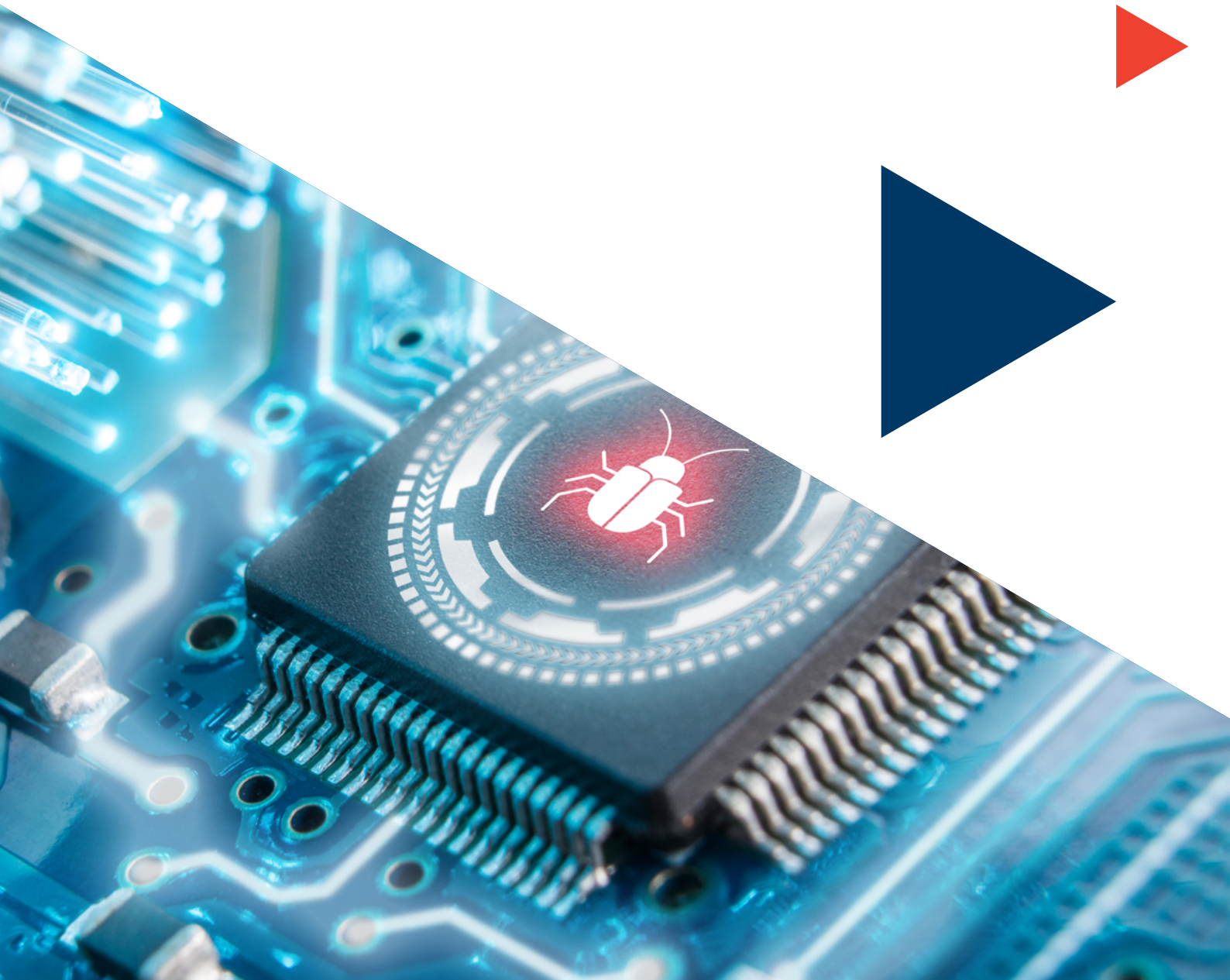
Gönderen: "HASTALIK KONTROL VE YÖNETİM MERKEZİ"

Konu: "COVID-19 GUNCELLEME // İŞ SÜREKLİLİĞİ PLANI DUYURUSU 2020 MART'TAN BAŞLAYAN"

EK: CORONOVIRUS COVID-19 DOCUMENT_zip.arj ÜZERİNDEKİ FARKINDALIĞA UYARI

Loki-bot olarak adlandırılan bu zararlı yazılım şekli, çeşitli uygulamalardan bilgi çalmak için geliştirilmiştir. Loki-bot en çok kullanılan web tarayıcılarından, FTP'den, e-posta istemcilerinden ve virüslü makineye yüklenen 100'ün üzerinde yazılım aracından bilgi toplayan bir kötü amaçlı yazılımdır.

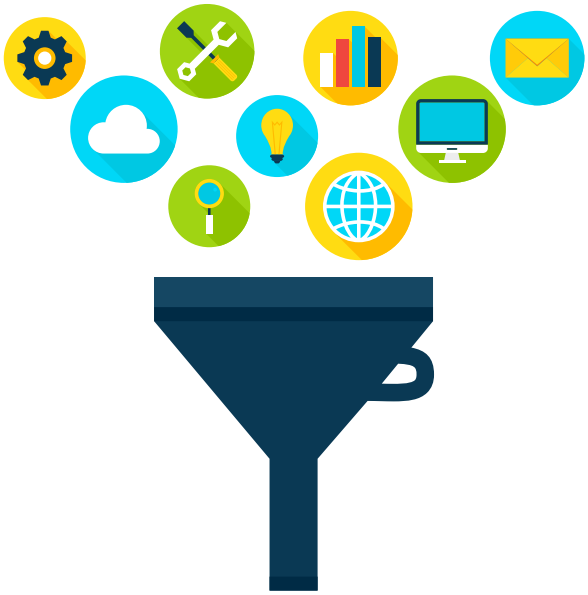
Bu yazılımı etkin hale getirmek için Microsoft Office dosyası veya arşiv dosyası gibi e-posta eklerinin açılması gerekir. Daha sonrasında zararlı içerisinde bulunan sunucu ile iletişime geçerek arka kısımda zararlı dosyalar sunucudan indirilerek çekilir ve artık sistem Loki-bot'un amacı doğrultusunda işlem yapmaya hazır hale gelir.



İçerik (URL) filtreleme servisinde tespit edilen vaka

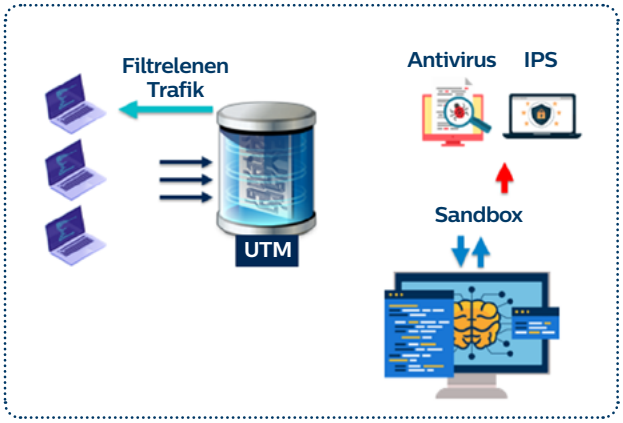
İçerik filtreleme tarafında kurum ağından dışarıya doğru olan web trafiği, yaklaşık 60-80 kategoride sınıflandırılan milyonlarca web sitesinin bir listesini içeren URL filtreleme veri tabanıyla karşılaştırır ve aksiyonlar alınır.

USOM belirli aralıklarla zararlı bağlantıları içeren listeler paylaşmaktadır. Gelen ihbarlarla, tarama sistemleriyle zararlı URL'leri tespit edip belirli formatlarla bildirimler gerçekleştiriyor. IT çalışanları ya manual yöntemlerle ya da dinamik listelerle bu IP'leri güvenlik duvarlarında, güvenlik profillerinde engelliyorlar. Next Generation Firewall cihazlarımızın web filtreleme profilleri USOM listeleriyle entegre çalışmaktadır.



USOM'un paylaşmış olduğu zararlı URL'ler listesindeki linklerden en çok tıklama alan adres dw.cbsi.com domain'idir. Bu domain ile ilişkili IP adresine (64.30.230.22) ait önceden 10 farklı passive DNS adresi olduğu gözlemlenmiştir. Totalde dw.cbsi.com domain adresinin sahip olduğu IP ile ilişkili birçok zararlı yazılımın barındırıldığı tespit edilmiştir.

Uzaktan Çalışma Dönemine Uygun bir Türk Telekom Siber Güvenlik Çözümü Olarak "Gelişmiş Tehdit Önleme (APT)"



- Coğrafi ve marka yedekli altyapı
- 7/24 Yönetim ve profesyonel raporlama
- Zero day ataklara karşı proaktif koruma
- Diğer güvenlik çözümleriyle bütünleşik çalışma

Oltalama saldırılarında önemli bir artışın yaşandığı bu dönemde şirketler çalışanlarını korumak için sandbox çözümlerine ihtiyaç duymaktadır fakat COVID-19'un yaratmış olduğu etki nedeniyle tedarik sürecinde yaşanan aksamalar ve kurulum için lokasyonda bulunma gerekliliği bu ihtiyacın ötelenmesine neden olabilir.

Türk Telekom'un omurgadan sunmakta olduğu APT servisi ile hızlı devreye alım ve kurulum kolaylığından yararlanarak sistemlerinizi oltalama saldırıları ve sıfırıncı gün ataklarına karşı koruma altına alabilirsiniz. APT, aynı zamanda antivirüs ve IPS servisleri ile entegre çalışarak ihtiyacınız olan hızlı ve esnek çözümü sunmaktadır.

APT servisi erişim bağımsız sunulmaktadır, farklı operatörden hizmet alan internet müşterileri de Türk Telekom APT servisinden aylık ödeme modeli ile yararlanabilir.

Gelişmiş Siber Tehdit Önleme Hizmeti

- Kurumlara yapılan bilinmeyen atakları tespit eder ve bilinir hale getirir.
- Günümüzün gelişmiş siber saldırılarını ya da zero day ataklarını tespit eder.
- Threat Intelligence bulutu sayesinde dünyanın herhangi bir yerinde tespit edilen atakları anlık olarak paylaşır ve imza veri tabanına ekler.
- Gelişmiş Tehdit Önleme Hizmeti, diğer hizmetlerden en az biriyle birlikte verilmesi gereken premium bir hizmettir.

Gelişmiş Tehdit Önleme Nasıl Çalışır?

1. İnternet üzerinden indirilen dosyaları inceler ve analiz eder.
2. Zararlı olduğunu tespit ettiği dosyaların indirilmesini önler.
3. Sandboxing (Denetleme Ortamı), Siber İstihbarat, Raporlama
4. Tüm atak vektörleri için koruma: Email, web trafiği, anlık mesajlaşma
5. Desteklenen dosya tipleri: PDF, EXE, APK, Microsoft Office, ZIP/RAR, JAWA, FLASH
6. Desteklenen işletim sistemleri: Microsoft Windows XP, Microsoft Windows 7, Mac OSX, Android, Linux

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

BU İŞTE BERABERİZ

Türk Telekom
Değerli Hissettirir