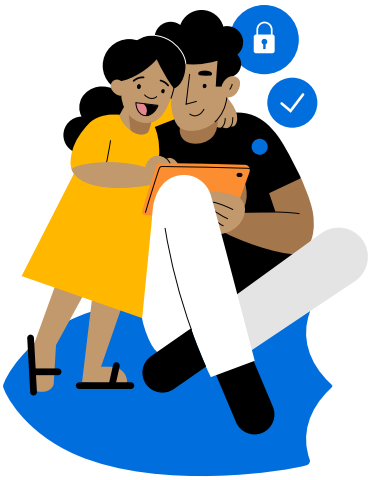


Milyonlarca Uygulama İçin Güvenilir Bir Ekosistem Oluşturmak

App Store'daki güvenlik önlemlerinin önemi

Haziran 2021

2007

“Birbirine tamamen zıt iki şeyi aynı anda yapmaya çalışıyoruz: Geliştiricilere ileri düzey ve açık bir platform sunarken bir yandan da iPhone kullanıcılarını virüslere, kötü amaçlı yazılımlara, gizliliğe yönelik saldırılara ve bunun gibi birçok şeye karşı korumak için uğraşıyoruz. Bu kolay bir iş değil.”

Steve Jobs, 2007[1]

2016

“Yalnızca resmi uygulama pazarını kullanın. Kullanıcılar... kötü amaçlı uygulama indirme riskini minimuma indirmek için üçüncü taraf kaynaklardan uygulama indirmemelidir. Kullanıcılar yasal ve özgün kaynaklardan gelmeyen uygulamaları dışarıdan yüklememelidir.”

Avrupa Birliği Siber Güvenlik Ajansı (ENISA), 2016[2]

2017

“Saldırılara açık uygulamaların oluşturduğu tehdidi azaltmaya yönelik en iyi çözümler, kötü amaçlı ve gizliliği ihlal eden uygulamalarla ilgilidir. Ayrıca, kullanıcılar dışarıdan uygulama yüklemekten ve resmi olmayan uygulama mağazalarını kullanmaktan kaçınmalıdır. Kurumlar da aygıtlarına bu konuda kısıtlama getirmelidir.”

ABD İç Güvenlik Bakanlığı Raporu, 2017[3]

Günümüzde telefonlarımız yalnızca birer telefon değil. Bu aygıtlarda kişisel ve profesyonel hayatımızla ilgili en hassas bilgileri saklıyoruz. Telefonlarımızı gittiğimiz her yere götürüyoruz. Sevdiklerimizle görüşmek ve mesajlaşmak, çocuklarımızın fotoğraflarını çekip saklamak, kaybolduğumuzda yolumuzu bulmak, adımlarımızı saymak ve para göndermek için onları kullanıyoruz. Mutlu anlarımızda da acil durumlarda da telefonlarımız hep yanımızda.

iPhone'u, bunları göz önünde bulundurarak tasarladık. App Store'u ise dünyanın her yerindeki geliştiricilere yenilikçi uygulamalar geliştirip bunları büyüyen ve gelişen küresel bir toplulukta bir milyardan fazla kullanıcıya ulaştırabilecekleri bir yer sunmak amacıyla kurduk. App Store'da kullanıcıların indirebileceği yaklaşık iki milyon uygulama bulunuyor ve bunlara her hafta binlercesi ekleniyor. App Store platformunun genişliği dikkate alındığında, iPhone'un güvenliği bizim için en başından beri çok önemliydi. Güvenlik araştırmacıları iPhone'un en güvenli mobil aygıt olduğu konusunda hemfikir. Bu da kullanıcılarımızın en hassas verilerini aygıtlarında güvenle saklamalarını sağlıyor. iPhone'u sektör lideri güvenlik önlemleriyle donattık. Aynı zamanda kullanıcıların uygulamaları gönül rahatlığıyla keşfedip indirebilecekleri güvenilir bir yer olan App Store'u kurduk. App Store'da yönergelerimize uymayı kabul etmiş, tanınan geliştiricilerin uygulamaları bulunuyor. Bu uygulamalar üçüncü tarafların müdahalesi olmadan kullanıcılara güvenli bir şekilde ulaştırılıyor. Her bir uygulamayı ve güncellemeyi, yüksek standartlarımıza uyup uymadıklarını belirlemek için inceliyoruz. Sürekli geliştirmeye çalıştığımız bu süreç zararlı yazılımları, siber suçluları ve dolandırıcıları App Store'dan uzaklaştırarak kullanıcılarımızı korumak için tasarlandı. Çocuklar için tasarlanan uygulamaların veri toplama konusunda katı yönergelere uyması ve çocukları koruyacak biçimde tasarlanmış olması gerekiyor. Ayrıca bu uygulamaların iOS ebeveyn denetimi özellikleriyle sıkı bir şekilde entegre olması da şart.

Gizliliğin yalnızca önemli değil, aynı zamanda temel bir insan hakkı olduğuna inanıyoruz. Bu prensiple ürünlerimizde yüksek gizlilik standartları uyguluyoruz. Bir ürünü veya hizmeti sunmak için sadece gerekli olan kişisel verileri topluyoruz. Uygulamaların hassas verilere erişmesini izne bağlı tutarak kontrolü kullanıcıya veriyoruz. Mikrofon, kamera ve kullanıcının konumu gibi özelliklere erişmek isteyen uygulamaları net bir biçimde belirtiyoruz. Kullanıcı gizliliği konusundaki kararlılığımızın bir parçası olarak, App Store'daki gizlilik etiketleri ve Uygulama Takibinde Şeffaflık adında iki yeni gizlilik özelliğimizle kullanıcılara benzersiz bir denetim imkanı veriyoruz. Daha şeffaf bilgiler sunarak kullanıcıların bilinçli tercihler yapmalarına yardımcı oluyoruz. Tüm bu güvenlik önlemleri sayesinde kullanıcılar App Store'daki her uygulamayı

Bunları biliyor muydunuz?

Apple, kullanıcılara zarar verme ihtimali olanları tespit etmek için App Store'daki tüm uygulamaları ve güncellemeleri inceliyor. Uygunsuz içeriklere sahip olan, kullanıcı gizliliğini ihlal eden veya kötü ya da tehlikeli amaçlarla kullanıldığı bilinen yazılımlar içeren uygulamalar tespit ediliyor.

Yapılan bir araştırmada, Android kullanan aygıtlarda iPhone'a kıyasla 15 kat daha fazla kötü amaçlı yazılım bulunduğu tespit edildi. Bunun temel sebebinin ise Android uygulamaları "neredeyse her yerden indirilebiliyorken" iPhone kullanıcılarının uygulamaları yalnızca App Store'dan indirebilmesi olduğu anlaşıldı.[4]

gönül rahatlığıyla indirebiliyor. Bu durum aynı zamanda geliştiricilerin de işine yarıyor. Uygulamaları güvenle indirebilen geniş bir kitleye ulaşabiliyorlar.

Bu güvenlik ve gizlilik yaklaşımının son derece etkili olduğunu gördük. Bugün bir kullanıcının iPhone'da kötü amaçlı yazılımla karşılaşma ihtimali inanılmaz derecede düşük.[5] Geliştiricilerin uygulamalarını App Store dışında, web sitelerinden veya üçüncü taraf uygulama mağazalarından da dağıtmaları için bazı çözümler oluşturmamızı önerenler oldu. Buna "dışarıdan yükleme" adı veriliyor. Fakat dışarıdan yüklemeye izin vermek iOS platformunun güvenliğini azaltacağı gibi kullanıcıları yalnızca üçüncü taraf uygulama mağazalarında değil, App Store'da da ciddi güvenlik riskleriyle karşı karşıya bırakabilir. iPhone kullanıcı tabanının genişliği ve telefonlarda saklanan fotoğraflar, konum bilgileri, sağlık ve finans bilgileri gibi hassas veriler nedeniyle, dışarıdan yüklemeye izin verilmesi platforma yönelik saldırılara yeni ve büyük yatırımlar yapılmasına yol açabilir. Kötü niyetli gruplar bu fırsattan yararlanmak için iOS kullanıcılarını hedef alan karmaşık saldırılar geliştirmeye daha fazla kaynak aktarabilir. Bu da "tehdit modeli" olarak adlandırılan ve tüm kullanıcıların korunması gereken tehlikeli istismarların ve saldırıların artmasına neden olabilir. Kötü amaçlı yazılım saldırısı riskindeki bu artış, tüm kullanıcıları daha büyük bir riskle karşı karşıya bırakabilir. Yalnızca App Store'dan uygulama indirenleri bile. Ayrıca, yalnızca App Store'dan uygulama indirmeyi tercih eden kullanıcılar bile iş veya okul için gereken bir uygulamayı, App Store'da yer verilmediği takdirde üçüncü taraf mağazalarından indirmek zorunda kalabilirler. Veya App Store gibi görünen üçüncü taraf uygulama mağazalarından uygulama indirmek durumunda kalıp kandırılabilirler.

Yapılan araştırmalar, uygulamaların incelemeye tabi tutulmadığı üçüncü taraf Android uygulama mağazalarının resmi uygulama mağazalarına kıyasla riskli ve kötü amaçlı yazılım içerme ihtimalinin daha fazla olduğunu ortaya koyuyor.[6] Bunun sonucunda, güvenlik uzmanları tüketicilere üçüncü taraf uygulama mağazalarını güvenli olmadıkları için kullanmamalarını öneriyor.[3,7] Dışarıdan yüklemeye izin verildiği zaman kullanıcıların riskleri kabul etmekten başka bir şansı kalmayabiliyor. Çünkü bazı uygulamalar App Store'da bulunmadığında kullanıcılar dolandırılabilir ve App Store'dan güvenle uygulama indirdiklerini sanarken aslında farklı bir yerden indirme yapıyor olabilirler. Dışarıdan yüklemeyle kullanıcılar; yanlış yönlendirmek, iPhone'un güvenlik özelliklerine saldırmak ve kullanıcı gizliliğini ihlal etmek için uygulamalardan yararlanmak isteyen dolandırıcıların saldırılarına açık hale gelebilir. Bu durum ayrıca kullanıcıların Satın Alma İzni ve Ekran Süresi özelliklerine güvenmesini de zorlaştırabilir. Bir ebeveyn denetimi özelliği olan Satın Alma İzni, ebeveynlere çocuklarının indirdiği uygulamalar ve uygulama içi satın almalar üzerinde kontrol imkanı veriyor. Ekran Süresi ise çocukların aygıtta geçirdiği süreyi yönetmeyi sağlıyor. Dolandırıcılar uygulamaların yapısını değiştirerek bu iki özelliğin etkisini azaltıp çocukları ve ebeveynleri kandırma ve yanlış yönlendirme fırsatı yakalayabilir.

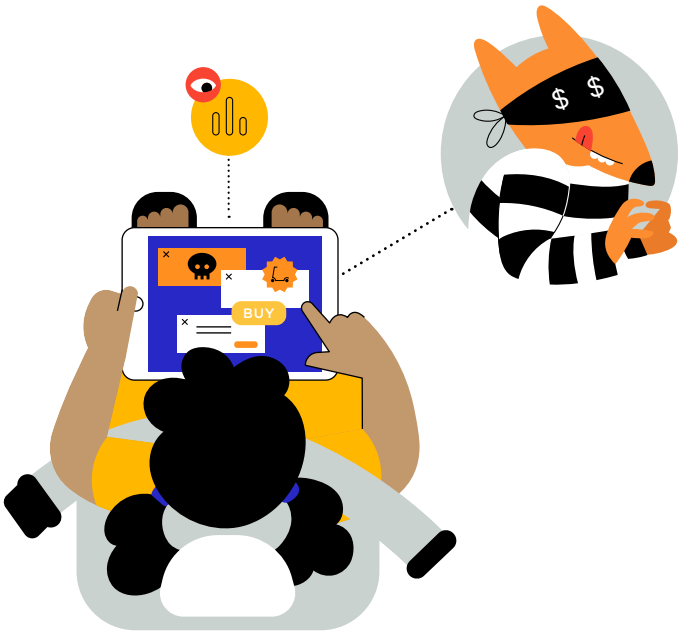
Sonuç olarak böyle bir durumda kullanıcıların dolandırıcılık girişimlerine karşı sürekli tetikte olması gerekir. Kullanıcılar neye ve kime güveneceklerini asla bilemeyeceklerinden daha az geliştiriciden daha az sayıda uygulama indirebilirler. Geliştiriciler ise kötü niyetli gruplara ait, kötü amaçlı yazılım içeren ve yayan geliştirici araçlarının oluşturduğu tehditlere karşı daha savunmasız hale gelir. Ayrıca geliştiriciler, emeklerinin karşılığını almalarını engelleyen korsanlığa da daha fazla maruz kalmış olur.

Dışarıdan yüklemeye izin veren platformlarda yaşanmış gerçek saldırı örnekleri

Çocuklara yönelik Android uygulamalarının, çocukların gizliliğini ihlal eden veri toplama yöntemleri kullandığı ortaya çıktı. Bu uygulamalar Google Play Store'dan kaldırılmış olmalarına rağmen üçüncü taraf uygulama mağazalarında Android kullanıcılarını hedef alarak büyümeyi sürdürüyor.[8]

Kötü niyetli gruplar çocuklara yönelik uygulamalara uygunsuz veya müstehcen reklamlar yerleştirdi.[9]

Dışarıdan yüklemeyle bir ailenin günlük iPhone kullanma deneyiminin ne kadar farklı olacağına göz atalım. John ve 7 yaşındaki kızı Emma'nın belirsizliklerle dolu bu dünyada geçirdiği bir günü izleyeceğiz.



Dışarıdan yüklenen bir oyun ebeveyn denetimlerini atlatıyor

Emma okulda arkadaşlarından duyduğu bir oyunu oynamak için John'dan izin istiyor. John oyunu App Store'da arıyor fakat geliştirici uygulamayı yalnızca üçüncü taraf uygulama mağazalarından sunmuş. John bundan rahatsız oluyor fakat Emma gerçekten denemek istediği için oyunu indiriyor. Üçüncü taraf uygulama mağazası uygulamanın çocuklar için uygun olduğunu iddia ediyor. Daha sonra parka gitmek için yola çıkıyorlar ve Emma arabanın arka koltuğunda oyunu oynarken uygulama ona başka web sitelerine ve hedefli reklamlara yönlendiren çok sayıda bağlantı gönderiyor. Oyunu indirdiğinde Emma'nın başlangıç paketini alması için kredi kartı bilgilerini ekleyen John, Satın Alma İzni ebeveyn denetiminin dışarıdan yüklenen bu uygulamayla çalışmayacağını fark etmiyor. Emma oyunu oynarken çok sayıda ekstra hak ve özel obje satın alıyor. Emma aslında bunlara babasının izin vermediğinin farkında değil. Ayrıca uygulamada yerleşik olarak üçüncü taraf veri izleyicileri bulunuyor. Bunlar Emma'nın verilerini toplayıp analiz ederek veri aracılarına satıyor. Yani uygulamanın çocuklara yönelik olması hiçbir şeyi değiştirmiyor.

Dışarıdan yüklemeye izin veren platformlarda yaşanmış gerçek saldırı örnekleri

Android'de dışarıdan yüklenen uygulamaların "kilitleyen" fidye yazılımı saldırıları için kullanıldığı biliniyor. Bu kötü amaçlı uygulamalar, kullanıcı fidye ödemeyi kabul etmezse telefonu kilitliyor veya fotoğrafları hedef alıyor.[10,11]

Android kullanıcıları Netflix ve Candy Crush gibi uygulamaların sahte sürümlerini indirmek için kandırılarak güvensiz yöntemlere yönlendirildi. Bu sahte uygulamalar, verilen erişim izninden veya platformdaki açıklardan yararlanarak mikrofonla Android kullanıcılarını takip edebiliyor; aygıtların ekran görüntüsünü alabiliyor; konumu, kısa mesajları ve rehberdeki kişileri izleyebiliyor; kullanıcının oturum açma bilgilerini çalabiliyor ve kullanıcıların telefonlarında değişiklik yapabiliyor.[12,13,14] Bazı uygulamalar bankacılıkla ilgili kimlik bilgilerini çalıp kullanıcıların banka hesaplarını ele geçirmek için kullanılabiliyor.[15,16,17,18]

En son yaşanan fidye yazılımı saldırılarından birinde, COVID-19 temaslı takip uygulaması gibi görünen bir Android uygulaması kullanıldı. Bu uygulama, kurulduğunda tüm kişisel bilgileri şifreliyor ve kullanıcıya verilerini kurtarmak için iletişime geçebileceği bir mail adresi veriyor.[19]

Üçüncü taraf Android uygulama mağazalarında bulunan bir uygulama ise sistem güncellemesi gibi görünerek kullanıcıları kandırıyor. Bu uygulama yüklendiğinde ekranda "Güncelleme aranıyor" bildirimi çıkıyor. Bu sırada uygulama kullanıcının mesajları, kişileri ve resimleri gibi kişisel verilerine erişip bunları çalıyor.[20,21]

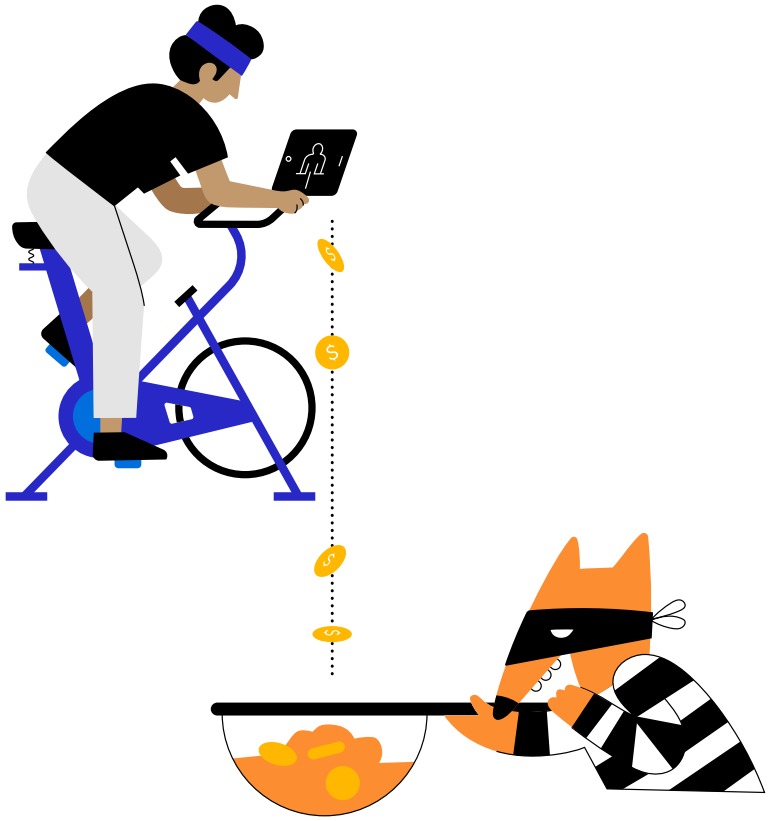
John'un dışarıdan yüklediği sahte filtre uygulaması, fidye ödemediği takdirde onu tüm fotoğraflarını silmekle tehdit ediyor

John ve Emma parktayken, John iyi bilinen bir uygulama geliştiricisinin yaptığı selfie filtresi uygulamasının bir reklamını görüyor. Bu uygulamayı kullanarak Emma ile eğlenceli vakit geçireceklerini düşünüyor. Reklam, uygulamayı indirmesi için John'u uygulama geliştiricisinin App Store'daki sayfasına benzer bir sayfaya yönlendiriyor. John da bu nedenle güvende olduğunu düşünüyor. Aslında bir üçüncü taraf uygulama mağazasından uygulamanın sahte bir versiyonunu indirdiğini fark etmiyor. John filtre uygulamasının iyi bilinen ve güvenilir bir geliştiriciden geldiğini düşünerek fotoğraflarına erişim izni veriyor. Ancak, uygulama çalışmaya başladığında John bir hata yaptığını anlıyor. Uygulama John'u, kredi kartı bilgileri girilip fidye ödenmediği takdirde film rulosundaki tüm fotoğrafları silmekle tehdit ediyor. iPhone'daki aygıt içi güvenlik önlemleri, uygulamaların fotoğraflara erişim izinlerinin denetimini John'a veriyor fakat bu durumda dışarıdan yüklenen uygulama bir selfie filtresi gibi görünüp John'u kandırarak fotoğraflara erişim izni vermesini sağlıyor.

Dışarıdan yüklemeye izin veren platformlarda yaşanmış gerçek saldırı örnekleri

Yapılan bir araştırmaya göre, üçüncü taraf uygulama mağazalarında yayınlanan korsan uygulamalar geliştiricilere her yıl milyarlarca dolara mâl oluyor.[22]

Korsan ve diğer türlerdeki yasal olmayan uygulamalara Android'de sıkça rastlanıyor. Bu tür uygulamalar arasında hile yapmaya yarayan (örn. kişilerin konumunu başka yerde gibi gösterebilen korsan Pokémon Go sürümü); özel içeriklere veya özelliklere korsan erişim sağlayacak biçimde değiştirilen; yasa dışı kumar oynama imkanı ve yetişkinlere yönelik içeriklere erişim sunan uygulamalar yer alıyor.[23,24,25]

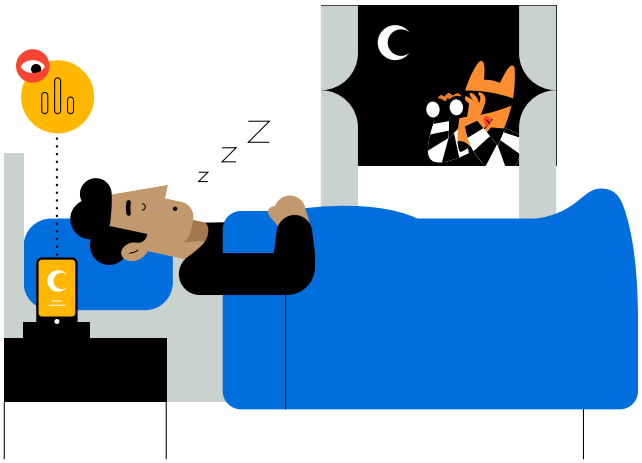


John farkına varmadan üçüncü taraf uygulama mağazasından bir korsan uygulama indiriyor

John'un arkadaşı severek kullandığı bir fitness uygulamasını denemesi için John'a davetiye gönderiyor. Ancak bu davetiye yalnızca John uygulamayı App Store'dan değil de bir üçüncü taraf uygulama mağazasından indirirse çalışıyor. John uygulamayı indiriyor ve aylık abone oluyor. Ancak her ikisi de bu uygulamanın korsan olduğunun farkında değil. Bu da her ay ödediği paranın uygulamayı tasarlayıp oluşturan geliştiriciye değil, uygulamayı çalan dolandırıcılara gittiği anlamına geliyor. John bu fitness uygulamasının geliştiricisine destek olarak doğru bir şey yaptığına inanıyor. Fakat aslında dolandırıcıların ceplerini dolduruyor, geliştiricilerin kazançlarından olmalarına neden olan bir dolandırıcılık yöntemine bilmeden destek oluyor.

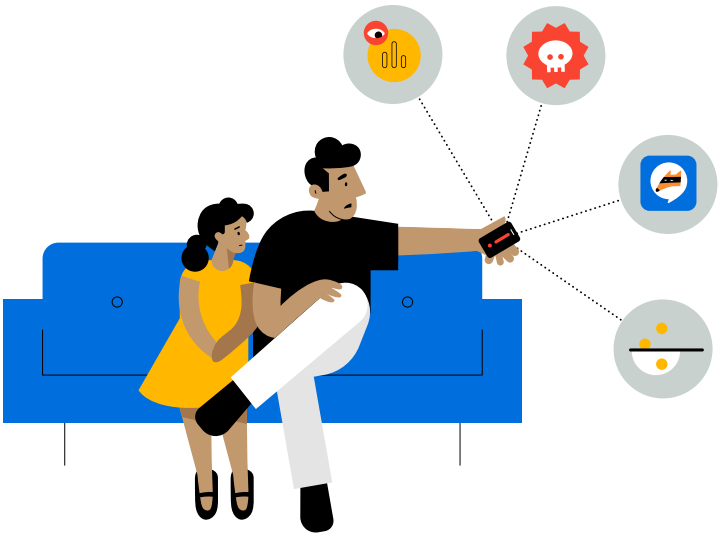
Apple'ın gizlilik önlemleri hakkında daha fazla bilgi edinin

Uygulama Takibinde Şeffaflık özelliği ve App Store'daki gizlilik etiketlerinin size uygulamaların verilerinizi toplama ve kullanma yöntemleriyle ilgili sunduğu şeffaflık ve denetim imkanı hakkında daha fazla bilgi edinmek için Verilerinizin Bir Günü adlı belgeyi okuyabilir ve **apple.com/tr/privacy/control sayfasını ziyaret edebilirsiniz.**



Dışarıdan yüklenen bir uygulama John'un gizliliğini ihlal ediyor

John yeni bir uyku takibi uygulamasını denemek istiyor fakat bu uygulama App Store'da bulunmuyor. Uygulamayı bir üçüncü taraf uygulama mağazasından indiriyor, mail adresini kullanarak kaydoluyor ve uyku kalitesini takip etmek için kullanmaya başlıyor. Uygulama kullanıcıların sağlık ve kullanım verilerini tamamen gizli tuttuğunu ve bunları dış verilere bağlamadığını veya üçüncü taraflarla paylaşmadığını iddia ediyor. Ancak bu iddianın doğru olmadığı ortaya çıkıyor. Uygulama dışarıdan yüklendiği için geliştirici istediğini yapabiliyor. Bu sayede uygulama John'u mail adresi üzerinden izinsiz bir şekilde takip ediyor. Geliştirici John'un verilerini diğer uygulamalardan topladığı verilerle birleştiriyor, sağlık verilerini kullanıcının izni olmadan ve durdurulma endişesi yaşamadan veri aracılarına satıyor.



Her gün bir milyardan fazla kişi iPhone'u bankacılık işlemlerini yapmak, sağlık verilerini kontrol etmek ve sevdiklerinin fotoğraflarını çekmek için kullanıyor. Bu geniş kullanıcı tabanı siber suçlular ve dolandırıcılar için çekici ve kârlı bir hedef. Dışarıdan yüklemeye izin vermek, iPhone'a yönelik saldırılara yeni ve büyük yatırımlar yapılmasına yol açabilir. Bu saldırılar, Mac gibi diğer platformlara yönelik saldırılardan çok daha büyük ölçekli olabilir. Dolandırıcılar uzmanlaşarak iPhone'un aygıt güvenliğine saldırmaya yarayacak araçlar geliştirmek için harekete geçebilir. App Store bugünkü saldırıları tespit edip engelleyecek biçimde tasarlandı. Ama eğer tehdit modelleri değişirse bu önlemler atlatılabilir. Dolandırıcılar yeni geliştirdikleri araçları ve uzmanlıklarını kullanarak üçüncü taraf mağazalarının yanı sıra App Store'u da hedef alabilir. Bu da uygulamaları yalnızca App Store'dan indiren kullanıcıları bile büyük bir risk altına sokabilir. Dışarıdan yüklemenin getirdiği ek dağıtım kanalları sayesinde kötü niyetli gruplar sistem açıklarından daha çok yararlanma fırsatı elde ediyor. Bu da saldırganları daha fazla kötü amaçlı yazılım geliştirmeye ve yaymaya teşvik ediyor.

Tüm bunların sonucunda iPhone ve App Store'un güvenliğine alışan John gibi kullanıcılar her zaman tetikte olmak zorunda kalabilir. Çünkü kime veya neye güvenebileceklerini bilemeden siber suçluların ve dolandırıcıların sürekli değişen yöntemlerine karşı savunmasız hale gelirler. Bazı durumlarda John'un App Store'da bulunmayan bir uygulamayı üçüncü taraf mağazalarından indirerek risk almaktan başka çaresi kalmayabilir. Hatta John bunu yapması için kandırılabilir. Daha ciddi durumlarda ise, dışarıdan yüklenen uygulamalar aslında olmadıkları gibi görünebilir. Örneğin bir Apple yazılım güncellemesi olduğu iddia edilen veya indirme sayfası App Store'a benzeyen uygulamalarla karşılaşılabilir. Bu uygulamalar iPhone'un aygıt içi güvenlik önlemlerini aşmaya çalışarak mesajlar, fotoğraflar ve konum gibi koruma altındaki verilere erişebilir. Tüm bu riskler ve dolandırıcılık yöntemleri karşısında John hangi uygulamaları indireceğine çok daha fazla dikkat etmek zorunda kalır. Bu yüzden daha az uygulama indirir ve güvenilir birkaç geliştiricinin sunduğu uygulamalara mecbur kalır. Ve sonuç olarak yeni ve yetenekli geliştiricilerin inovatif uygulamalarıyla kullanıcılara ulaşmaları zorlaşmış olur. Kısacası John, iPhone'undaki uygulamaların kendisi ve kızı için en güvenli seçenekler olduğunu bilmenin rahatlığını yaşayamaz.

Biliyor muydunuz?

Güvenliklerinden ve gizliliklerinden endişe eden kullanıcılar daha az uygulama indiriyor ve aygıtlarından uygulama silmeye daha yatkın oluyor.[26,27,28] Kullanıcılar, uygulama indirirken kendilerini rahat hissetmedikleri daha güvensiz bir ekosistemde yenilikçi uygulamaları daha az deniyor veya yeni ya da az bilinen geliştiricilerin uygulamalarına şans vermiyor. Uygulama ekonomisinde büyümeyi engelleyen bu durum hem kullanıcılara hem de geliştiricilere zarar veriyor.

Apple'ın güvenlik katmanları ve App Review; John'u, Emma'yı ve onların aygıtlarını koruyor

iOS kullanıcılarını kötü amaçlı uygulamalardan korumak ve dünyanın en iyi platform güvenliğini sunmak için birden fazla koruma katmanına sahip çok yönlü bir yaklaşım sergiliyoruz. iOS'e özgü zorlu güvenlik önlemleri bulunuyor çünkü kullanıcılar aygıtlarına sık sık yeni uygulamalar yüklemeye devam ediyor. Ve iOS aygıtlarının, çocukların gözetim altında olmadan kullanabilecekleri kadar güvenli olması gerekiyor. Kullanıcı sayısı, davranışları ve beklentileri farklı olduğu için iPhone'da Mac'e kıyasla daha da sıkı bir güvenlik yaklaşımı benimsiyoruz.

- **Mac'te olduğu gibi uygulamaları, bilinen kötü amaçlı yazılımlara karşı otomatik bir yazılımla tarıyoruz. Kötü amaçlı yazılım içeren uygulamaların App Store'da yer almalarını engelleyerek kullanıcılara ulaşmalarını veya onlara zarar vermelerini önlüyoruz.**
- **Ayrıca uygulama geliştiricilerinin, uygulamalarını ve bunların özelliklerini açıklamasını zorunlu tutuyoruz.** Bu bilgiler App Review sürecinde uzman bir ekip tarafından inceleniyor ve uygulamayı indirmeyi düşünen kullanıcılara sunuluyor. Bu süreç kötü amaçlı yazılım yaymak için sıkça kullanılan, kötü amaçlı yazılımı popüler bir uygulama olarak gösterme veya gerçekte olmayan dikkat çekici özelliklere sahip olduğunu iddia etme gibi yöntemlere karşı etkili bir bariyer oluşturuyor.
- Uzmanlar, uygulamadaki özelliklerin belirtildiği gibi çalıştığını ve uygulamanın App Store sayfasının doğru olduğunu onaylamaya ek olarak, **uygulamanın gereksiz yere hassas verilere erişim izni isteyip istemediğini manuel olarak kontrol ediyor ve çocuklara yönelik uygulamaların veri toplama ve güvenlik kurallarına tamamen uyup uymadığını inceliyor.**
- **App Store'da yayınlandıktan sonra yönergelerimizi ihlal ettiği tespit edilen uygulamalar olduğunda, geliştiriciyle birlikte hareket ederek sorunu hızla çözüyoruz.** Dolandırıcılık ve kötü amaçlı faaliyetler gibi tehlikeli durumlar tespit edildiğinde uygulama anında App Store'dan kaldırılıyor ve uygulamayı indiren kullanıcılara kötü amaçlı özellikler hakkında bildirim gönderilebiliyor.
- **App Review sürecinin amacı, App Store'daki uygulamaların güvenilirliğinden** ve App Store sayfasında verilen bilgilerde uygulamaların nasıl çalıştığının ve hangi verilere erişeceğinin doğru gösterildiğinden emin olmak. Bu süreci sürekli geliştiriyoruz, araçlarımızı ve yöntemlerimizi yenileyip iyileştiriyoruz.

Kullanıcılar App Store'dan indirdikleri uygulamaların çalışma şeklini ve erişebildiği verileri Uygulama Takibinde Şeffaflık ve izinler gibi özelliklerle denetleyebiliyor. Ebeveynler, Satın Alma İzni özelliğiyle çocuklarının ne satın alacağını kontrol edebiliyor. Ekran Süresi özelliğiyle belirli uygulama kategorilerinde çocukların ne kadar zaman geçirdiğini ve hangi verileri paylaştıklarını denetleyebiliyor. Ayrıca kullanıcılar, Uygulama İçi Ödemeler bölümünde uygulamalarla ilgili tüm ödemeleri tek bir merkezden yönetebiliyor ve ödeme yapılan abonelikleri kolayca görüntüleyip iptal edebiliyor. Dışarıdan yüklenen uygulamalarda ise bu denetimleri tam olarak yapabilmek mümkün değil.

App Review ile sunulan güvenlik önlemlerine ek olarak, aygıtlarımızdaki donanım ve yazılımları, indirilebilecek kötü amaçlı uygulamalara karşı bir savunma hattı görevi görecek biçimde tasarlıyoruz. Örneğin, App Store'dan iPhone'a indirilen uygulamalar "izole ediliyor." Böylece uygulamalar kullanıcının izni olmadan diğer uygulamaların sakladığı dosyalara erişemiyor veya aygıtta değişiklik yapamıyor.

En iyi savunma, tüm katmanların bir araya gelmesiyle sağlanıyor. Sağlam aşamalardan oluşan App Review süreci kötü amaçlı uygulamaların yüklenmesini önlemeye yardımcı olurken güçlü platform önlemleri de bu uygulamaların verebileceği zararları kısıtlıyor. iOS için tasarlanan güçlü güvenlik özellikleri, tüketicilere yönelik herhangi bir aygıttaki en iyi koruma önlemlerini içeriyor. Ancak bu önlemler, kullanıcıların kandırılarak yaptıkları tercihlere karşı da işe yarayacak şekilde geliştirilmiyor. App Review, kullanıcalara zarar vermeye veya hassas verilerine erişmek amacıyla onları kandırmaya çalışan uygulamalara karşı koruma sağlayan App Store politikalarını destekliyor. Ayrıca, kötü amaçlı uygulamaların aygıt içi güvenlik önlemlerini atlatmaya çalışması gibi çok ciddi durumlarda App Review en baştan bu uygulamaların aygıtlara ulaşmasını zorlaştırıyor.

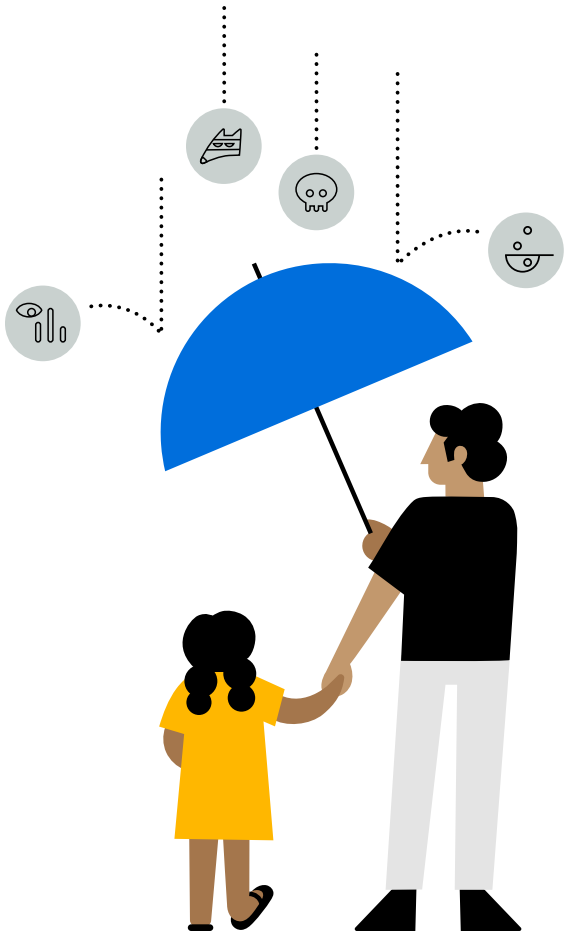
Ve tüm bunların sonucunda, güvenlik uzmanları iPhone'un en güvenli mobil aygıt olduğunu kabul ediyor. Apple, kötü amaçlı yazılımlara karşı çok sayıda güvenlik katmanından oluşan benzersiz bir koruma sağlıyor. Bu şekilde kullanıcılara güven veriyor.

App Review

App Review süreciyle uygulamaların kontrolden geçmiş kaynaklardan geldiğine ve kötü amaçlı bileşenler içermediğine emin oluyoruz. Ayrıca uygulamaların sizi istemediğiniz alışverişlere yönlendirmek veya kişisel verilerinize erişim vermenizi sağlamak için kandırmaya çalışıp çalışmadığını da denetliyoruz. Geliştiricileri ve kullanıcıları kontrol edip uygunsuz davranışta bulunanları uzaklaştırıyoruz. App Review süreçleri düşük kaliteli uygulamaların tamamının dağıtımını engelleyemese de bu alandaki teknolojilerimizi, yöntemlerimizi ve işlemlerimizi sürekli yenileyip geliştirmeye devam ediyoruz.

Apple'ın 2020'de hayata geçirdiği uygulama güvenlik önlemleri

- **Her hafta ortalama 100.000 yeni uygulama ve güncelleme** 500'den fazla özel uzmandan oluşan bir ekip tarafından farklı dillerde inceleniyor.
- **Yaklaşık bir milyon yeni uygulama ve benzer sayıda güncelleme reddedildi veya kaldırıldı:**
  - 150.000'den fazlası spam veya taklit olduğu ya da kullanıcıları yanlış yönlendirdiği için
  - 215.000'den fazlası gizlilik yönergelerini ihlal ettiği için
  - 48.000'den fazlası gizli veya belirtilmeyen özellikler taşıdığı için
  - Yaklaşık 95.000'i yasa dışı veya diğer uygunsuz eylemleri gerçekleştirmek için başta "yemle ve değiştir" işlevleri olmak üzere dolandırıcılık amaçlı çeşitli ihlaller içerdiği için
- **Apple, dolandırıcılık potansiyeli taşıyan 1,5 milyar dolar tutarındaki işlemi durdurdu.**
- **Apple, dolandırıcılıkla ilgili nedenlerden dolayı 470.000 ekibi Apple Geliştirici Programı'ndan çıkardı.** Ayrıca yaklaşık 205.000 geliştiricinin kayıt talebi dolandırıcılıkla ilgili endişeler nedeniyle reddedildi.
- **Apple 244 milyon tüketicinin hesabını dolandırıcılık ve sahte yorumlar gibi kötü davranışlar sebebiyle devre dışı bıraktı.** Ayrıca 424 milyon hesap oluşturma talebi de dolandırıcılık ve kötü davranış belirtileri nedeniyle reddedildi.



John, App Review sayesinde uygulamaları gönül rahatlığıyla indiriyor

App Store'un güvenlik ve gizlilik özellikleri sayesinde John, kendisi ve kızı için uygulamaları gönül rahatlığıyla indiriyor. Apple'ın App Store'daki uygulamaların %100'ünü bilinen kötü amaçlı yazılımlara karşı taradığını bilen John, diğer aygıtlara kıyasla iPhone'da kötü amaçlı yazılımlarla karşılaşma ihtimalinin inanılmaz düşük olduğunun farkında.

Apple'ın güvenlik önlemleri hakkında daha fazla bilgi edinin

Apple'ın App Store'da güvenliğinizi ve gizliliğinizi nasıl koruduğu hakkında daha fazla bilgi edinmek için lütfen apple.com/tr/app-store sayfasını ziyaret edin.

Apple'ın konum verilerinizi nasıl koruduğu hakkında daha fazla bilgi edinmek için lütfen Konum Servisleri Bilgi Sayfası'nı okuyun.

iOS'teki ebeveyn denetimleriyle ilgili daha fazla bilgi edinmek için lütfen apple.com/tr/families sayfasını ziyaret edin.

Sık Sorulan Sorular

Dışarıdan yükleme nedir?

Mobil aygıtlara resmi App Store yerine bir web sitesinden veya üçüncü taraf uygulama mağazasından uygulama indirip yüklemeye "dışarıdan yükleme" adı veriliyor. Kullanıcıların güvenliğini ve gizliliğini korumak için iPhone'u en başından itibaren dışarıdan yüklemeye izin vermeyecek şekilde tasarladık.

Tehdit modeli nedir?

Kullanıcıların korunması gereken saldırılara ve savunmasız noktalardan oluşan açıklara tehdit modeli deniyor. Farklı aygıtların, kullanıcıların ve çevrelerin farklı tehdit modelleri bulunuyor. Güvenliğin de bu modellere göre geliştirilmesi gerekiyor. App Store, iPhone tehdit modeline karşı korunmak için çok önemli bir güvenlik bileşeni. Kullanıcıların Apple tarafından incelenen uygulamaları güvenle indirebildiği bir yer olan App Store'da Apple'ın yönergelerine uymak zorunda olan, bilindik geliştiricilerin uygulamalarına yer veriliyor.

Web siteleri ve üçüncü taraf uygulama mağazaları üzerinden iPhone'a dışarıdan yüklemeye izin verilmesi, uygulamalarını yalnızca App Store'dan indiren kullanıcıları da tehdit eder mi?

Evet. iPhone'a dışarıdan yüklemeye izin verip ekstra dağıtım kanalları açmak, tehdit modelini değiştirmek ve potansiyel saldırıların kapsamını genişletmek tüm kullanıcıları riske atabilir. Uygulamaları yalnızca App Store'dan indirerek kendilerini korumak için çaba gösteren kullanıcılar bile bundan etkilenebilir. Dışarıdan yüklemeye izin vermek, iPhone'a yönelik saldırılara yeni ve büyük yatırımlar yapılmasına yol açabilir. Kötü niyetli gruplar, iPhone güvenliğine çok büyük ölçekte saldırmaya yarayacak araçlar geliştirmeye ve bu alanda uzmanlaşmaya yönelebilir. Daha karmaşık saldırılar yapabilecek seviyeye gelen bu gruplar, üçüncü taraf uygulama mağazalarının yanı sıra App Store'u da hedef alarak tüm kullanıcıları büyük bir riskle karşı karşıya bırakabilir. Ayrıca, yalnızca App Store'dan uygulama indirmeyi tercih eden kullanıcılar bile iş veya okul için gereken bir uygulamayı App Store'da bulamadıkları takdirde üçüncü taraf mağazalarından

indirmek zorunda kalabilirler. Veya App Store gibi görünen üçüncü taraf uygulama mağazalarından uygulama indirmek durumunda kalıp kandırılabilirler.

Apple'ın App Review süreci nasıl işliyor?

Gelişmiş teknolojiyle insan uzmanlığını bir araya getirerek her bir uygulamayı ve güncellemeyi dikkatle inceliyoruz. Uygulamaların, App Store'un sağlam gizlilik ve güvenlik yönergelerine uyup uymadıklarını değerlendiriyoruz. Otomatik incelemenin yeterli olmadığı durumlarda insan uzmanlığına güveniyoruz. Özellikle gizlilik ihlalleri veya katı yönergelerimize uymayan, çocuklara yönelik uygulamalar gibi konularda. Yönergelerimiz yeni tehditlere ve zorluklara uyum sağlamak için zaman içinde sürekli değişiyor. Böylece kullanıcıları korumayı ve onlara App Store'da mümkün olan en iyi deneyimi sunmayı hedefliyoruz. Her hafta ortalama 100.000 yeni uygulama ve güncelleme, dünyanın dört bir yanındaki 500'ün üzerinde özel uzmandan oluşan bir ekip tarafından inceleniyor.

Neler inceleniyor?

App Store'a gönderilen tüm uygulamalar ve güncellemeler App Review sürecinden geçiyor.

Apple aygıtlarında ne gibi ebeveyn denetimleri bulunuyor?

Ebeveynlere çocuklarının aygıtları nasıl kullandıklarını denetleme imkanı veren özellikler tasarlıyoruz. Ekran Süresi özelliği, ebeveynlere çocuklarının uygulamalarda, web sitelerinde ve aygıtlarda geçirdiği süre hakkında daha ayrıntılı bilgi veriyor. Ayrıca, çocukların her gün belirli kategorilerdeki uygulamalarda ve web sitelerinde ne kadar zaman geçirebileceklerini belirleme imkanı da sunuyor. Satın Alma İzni özelliği ise ebeveynlere çocuklarının uygulama alışverişlerini ve indirme taleplerini kendi aygıtlarından onaylama veya reddetme olanağı sağlıyor. Satın Alma İzni özelliği art arda satın almayı engellemek için işlemler arasına on beş dakika süre koyuyor.

App Store'daki Uygulama Takibinde Şeffaflık özelliği ve gizlilik etiketleri ne işe yarıyor?

Bu yeni özellikler sayesinde kullanıcılar verileri ve gizlilikleri üzerinde daha fazla kontrol sahibi oluyor. Uygulama Takibinde Şeffaflık özelliği, uygulamaların kullanıcı verilerini diğer şirketlere ait uygulamalarda ve web sitelerinde takip edebilmek için kullanıcıdan izin almasını zorunlu tutuyor. App Store'daki gizlilik etiketleri sayesinde tüm uygulamalar için kullanıcıların kolayca görebileceği şekilde gizlilik şartlarının özetlenmesi zorunlu tutuluyor. Böylece kullanıcılar verilerinin uygulama tarafından nasıl kullanıldığı hakkında önemli bilgilere ulaşabiliyor.

Kaynaklar

1. Jobs, Steve, "Third Party Applications on the iPhone"(iPhone'da Üçüncü Taraf Uygulamaları), 17 Ekim 2007,

tidbits.com/2007/10/17/steve-jobss-iphone-sdk-letter/ adresinden erişilebilir.

2. ENISA, "Vulnerabilities - Separating Reality from Hype" (Zaaflar - Gerçek ile Abartıyı Ayırmak), *Avrupa Birliği Siber Güvenlik Ajansı*, 24 Ağustos 2016.

3. Griffin, Robert Jr., "Study on Mobile Device Security" (Mobil Aygıt Güvenliği Çalışması), *ABD İç Güvenlik Bakanlığı*, Nisan 2017.

4. Nokia, "Threat Intelligence Report 2020" (Tehdit İstihbaratı Raporu 2020), *Nokia*, 2020.

5. Johnson, Dave, "Can iPhones get viruses? Here's what you need to know" (iPhone'lara virüs bulaşır mı? İşte bilmeniz gerekenler), *Business Insider*, 4 Mart 2019.

6. Symantec, "Internet Security Threat Report, Volume 23" (İnternet Güvenliği Tehdit Raporu, 23. Sayı), Nisan 2018.

7. Golovin, Igor, "Malware in Minecraft mods: story continues" (Minecraft modlarındaki kötü amaçlı yazılımlar: Hikaye devam ediyor), *Kaspersky*, 9 Haziran 2021.

8. Lunden, Ingrid, "Google removes 3 Android apps for children, with 20M+ downloads between them, over data collection violations" (Google toplam 20 milyondan fazla kez indirilen, çocuklara yönelik 3 Android uygulamasını veri toplama ihlalleri nedeniyle kaldırdı), *Tech Crunch*, 23 Ekim 2020.

9. Henry, Josh, "Malicious Apps: For Play or Prey?" (Kötü Amaçlı Uygulamalar: Eğlence mi? Tuzak mı?) *United States Cybersecurity Magazine*, 2021.

10. Schwartz, Jaime-Heather, "How to protect your Android phone from ransomware – plus a guide to removing it" (Android telefonunuzu fidye yazılımlarından korumanın yolları ve fidye yazılımı silme kılavuzu), *Avira*, 13 Ağustos 2020.

11. Seals, Tara, "Emerging Ransomware Targets Photos, Videos on Android Devices" (Yeni Fidye Yazılımları Android Aygıtlarındaki Fotoğrafları ve Videoları Hedef Alıyor), *ThreatPost*, 24 Haziran 2020.

12. Owaida, Amer, "Beware Android trojan posing as Clubhouse app" (Clubhouse uygulaması gibi görünen Android trojan yazılımına dikkat edin), *ESET'ten WeLiveSecurity* , 18 Mart 2021.

13. Desai, Shivang, "SpyNote RAT posing as Netflix app" (SpyNote RAT, Netflix uygulaması gibi görünüyor), *Zscaler*, 23 Ocak 2017.

14. Peterson, Andrea, "Beware: New Android malware is 'nearly impossible' to remove" (Dikkat: Kötü amaçlı yeni Android yazılımını kaldırmak 'neredeyse imkansız'), *The Washington Post*, 6 Kasım 2015.

15. Palmer, Danny, "This Android trojan malware is using fake apps to infect smartphones, steal bank details" (Bu kötü amaçlı Android trojan yazılımı sahte uygulamalarla akıllı telefonlara bulaşıp banka bilgilerini çalıyor), *ZDNet*, 1 Haziran 2021.

16. O'Donnell, Lindsey, "Banking.BR Android Trojan Emerges in Credential-Stealing Attacks" (Kimlik Bilgilerini Çalmaya Yönelik Saldırılarda Banking.BR Android Trojan Yazılımı Ortaya Çıktı), *ThreatPost*, 21 Nisan 2020.

17. Stefanko, Lukas, "Android Trojan steals money from PayPal accounts even with 2FA on" (Android Trojan yazılımı iki faktörlü kimlik doğrulama özelliği açık PayPal hesaplarından bile para çalıyor), **ESET'ten** *WeLiveSecurity* , 11 Aralık 2018.

18. Cybereason Nocturnus Team, "FakeSpy Masquerades as Postal Service Apps Around the World" (FakeSpy Dünyanın Çeşitli Yerlerinde Posta Hizmeti Uygulamalarını Taklit Ediyor), *Cybereason*, 1 Temmuz 2020.

19. Stefanko, Lukas, "New ransomware posing as COVID-19 tracing app targets Canada; ESET offers decryptor," (COVID-19 takip yazılımı gibi görünen yeni bir fidye yazılımı Kanada'yı hedef alıyor; ESET şifre çözücü sunuyor), *ESET'ten WeLiveSecurity*, 24 Haziran 2020.

20. Yaswant, Aazim, "New Advanced Android Malware Posing as 'System Update'" (Yeni ve Gelişmiş Bir Kötü Amaçlı Android Yazılımı 'Sistem Güncellemesi' Gibi Görünüyor), *Zimperium*, 26 Mart 2021.

21. Aamir, Humza, "Beware of this newly discovered Android spyware that pretends to be a system update" (Sistem güncellemesi gibi görünen bu kötü amaçlı yeni Android yazılımına dikkat edin), *TechSpot*, 29 Mart 2021.

22. Koetsier, John, "The Mobile Economy Has A $17.5B Leak: App Piracy" (Mobil Ekonomide 17,5 Milyar dolar Kayıp: Korsan Uygulamalar), *Forbes*, 2 Şubat 2018.

23. Koetsier, John, "App Developers Losing $3-4 Billion Annually Thanks To 14 Billion Pirated Apps" (Uygulama Geliştiriciler 14 Milyar Korsan Uygulama Yüzünden Yılda 3-4 Milyar Dolar Kaybediyor) *Forbes*, 24 Temmuz 2017.

24. Maxwell, Andy, "Cheat Maker Agrees to Pay Pokémon Go Creator $5m to Settle Copyright Infringement Lawsuit" (Hile Üreticisi Telif Hakkı İhlali Davasında Anlaşmak için Pokémon Go Geliştiricisine 5 Milyon Dolar Ödemeyi Kabul Etti) *TorrentFreak*, 8 Ocak 2021.

25. Reklamsız Çocukluk İçin Kampanya, "Apps which Google rates as safe for kids violate their privacy and expose them to other harms" (Google'ın çocuklar için güvenli olarak derecelendirdiği uygulamalar gizliliği ihlal ediyor ve çocukları başka tehlikelere açık hale getiriyor), 12 Aralık 2019.

26. J.P. Morgan, "2020 E-commerce Payments Trends Report: Japan" (2020 E-ticaret Ödeme Eğilimleri Raporu: Japonya) *J.P. Morgan*, 2020.

27. Deloitte, "Trust: Is there an app for that? Deloitte Australian Privacy Index 2019" (Güven: Bunun için bir uygulama var mı? Deloitte Avustralya Gizlilik Endeksi 2019), 2019.

28. Gikas, Mike, "How to Protect Your Privacy on Your Smartphone" (Akıllı Telefonunuzda Gizliliğinizi Nasıl Korursunuz) *Consumer Reports*, 1 Şubat 2017.