2023 McAfee Tüketicileri Hedef Alan Mobil Tehditler Raporu

Artık her şey dijital ortamda: Telefonlarımız da bunlara ulaşmamıza yardımcı oluyor. Riskleri nasıl azaltacağınızı öğreneceksiniz.

İçindekiler

2023 McAfee Tüketicileri Hedef Alan Mobil Tehditler Raporu

Artık her şey dijital ortamda: Telefonlarımız da bunlara ulaşmamıza yardımcı oluyor. Riskleri nasıl azaltacağınızı öğreneceksiniz.

Telefonunuza en son ne zaman baktınız? Araştırmalar, çoğumuzun günümüzün yaklaşık üçte birini mobil cihazlarla geçirdiğini gösteriyor.[1] Telefonlarımız ve diğer mobil cihazlarımız üzerinden bağlantıda kaldığımızı, faturalarımızı ödediğimizi, oyunlar oynadığımızı ve hayatımızı planladığımızı düşünürsek buna şaşırmamak gerek.

2022'nin sonunda OpenAI'nin ChatGPT sohbet botu ve DALL-E 2 görüntü oluşturma uygulaması gibi oyunun kurallarını değiştiren bazı uygulamalar kullanıma sunuldu. Bu araçlar, yapay zekanın gücünü kitlelerle buluşturdu. Bu gelişmeler sadece bize değil, siber suçlulara da yenilik ve üretkenlik açısından heyecan verici fırsatlardan yararlanma imkanı sağladı.

McAfee'nin Tehdit Araştırma Ekibi, günümüzün mobil tehditlerine siber suçluların gözünden bakma avantajına sahip. Bu içgörüleri kullanarak riskleri ve kendinizi nasıl koruyabileceğinizi daha iyi anlamanıza yardımcı olmak için bu raporu hazırladık. Bu sayede telefonların sunduğu özgürlük, denetim, erişim ve eğlence gibi olanaklardan faydalanırken siber suçluların hazırladığı potansiyel tuzaklardan kaçınabilirsiniz.

Bu raporun dijital hayatınızı, mobil cihazlarınızı ve ailenizi korumak için yararlı bir kaynak olacağını ve çevrimiçi hayatınızı güvenle yaşamanızı sağlayacağını umuyoruz.

Steve Grobman
Kıdemli Başkan Yardımcısı ve Teknolojiden Sorumlu Başkan, McAfee

Fernando Ruiz
Kıdemli Güvenlik Araştırmacısı, McAfee Mobil Tehditler Araştırma Ekibi

Bu rapor dört ana başlığa ayrılmıştır ve her başlığın altında çeşitli bulgulara yer verilmiştir:

- **Birinci Başlık**-Tehdit: Güvenilir görünen uygulamalara güvenme
- **İkinci Başlık**-Tehdit: DM atan dolandırıcılar
- **Üçüncü Başlık**-Tehdit: Kişisel telefonunuzu iş için kullanma
- **Dördüncü Başlık**-Zorluk: Telefon sahibi çocuklara ve gençlere modern ebeveynlik yapma
- **En yaygın görülen 10 kötü amaçlı yazılım ailesi**
- **2023 Tehdit tahminleri**

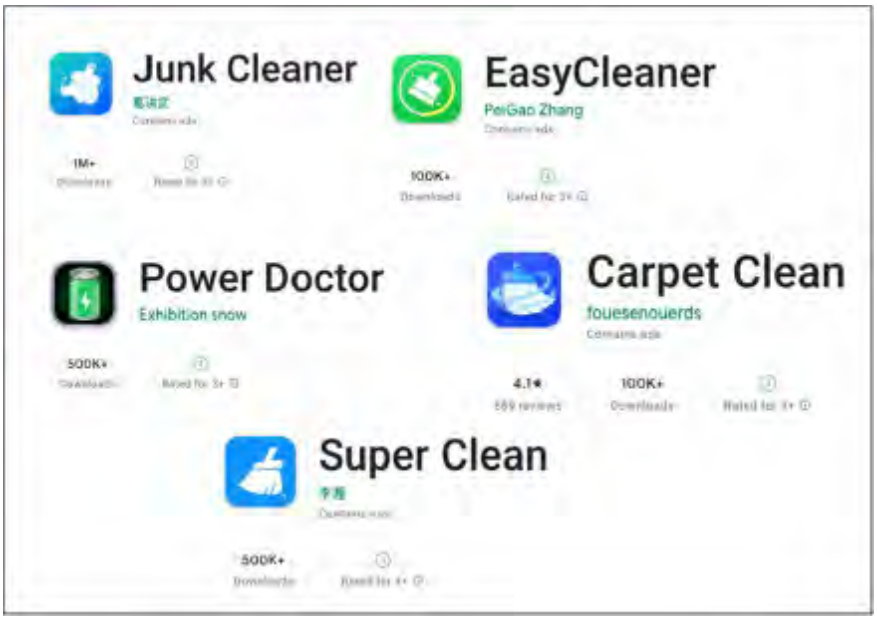
Birinci Başlık: Tehdit

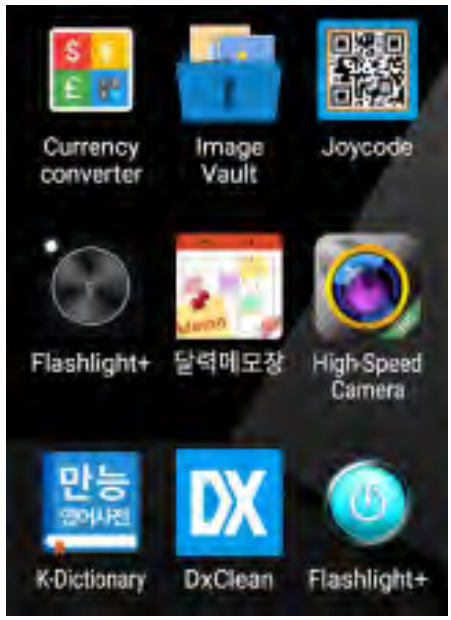
Güvenilir görünen uygulamalara güvenme

Tehdit: Güvenilir görünen uygulamalara güvenme

Mobil uygulamalar hayatımızın büyük bir parçası ve A noktasından B noktasına ulaşma, sosyal medyada içerik paylaşma veya bütçe yönetimi gibi pek çok alanda bize yardımcı oluyorlar. Peki güvenilir uygulamaları diğerlerinden nasıl ayırt ediyorsunuz? Uygulama mağazalarının inceleme süreçlerinin, kötü amaçlı uygulamaları kimse indirmeden yakalayıp sileceğine güvenmemeniz gerekir. Kötü adamlar, uygulamalarını mağazalara gizlice eklemek için her geçen gün daha akıllı hamleler yapıyor. Bu nedenle cihazınızı ve verilerinizi güvende tutmak için izlemeniz gereken birkaç adım var.

Ne tür uygulamalar var?





Şekil 1. McAfee tarafından kötü amaçlı olduğu tanımlanan çeşitli mobil uygulamalar. (Gösterilen uygulamalar Google Play'den kaldırılmıştır.)

Kötü amaçlı uygulamalar genellikle birkaç ortak özelliğe sahiptir: popüler, kullanımı kolay ve görünüşte zararsız. Doğru, bunlar aynı zamanda ilgilendiğiniz birçok uygulamanın da özelliği ve asıl sorun da burada başlıyor. Bu nedenle özellikle şu tür uygulamaları indirirken çok dikkatli olun:

- Resim düzenleme uygulamaları ve fotoğraf filtreleri
- İş ve telefon için yardımcı programlar
- Oyun ipuçları ve hileler
- Sosyal medya araçları

Mağazaya nasıl giriyorlar?

Burada teknik ayrıntılara ve kodlama tekniklerine girmeyeceğiz ancak dolandırıcıların, kötü amaçlı kodlarının incelemelerden geçmesi için kullandığı birkaç numara vardır. Bu püf noktaları hakkında bilgi sahibi olmak kötü uygulamalardan kaçınmanıza veya bunları yükledikten hemen sonra fark etmenize yardımcı olabilir.

Öncelikle kötü amaçlı uygulamaların çoğu aslında bazı normal işlevler sunar. İndirdiğiniz ücretsiz fotoğraf düzenleyicinin veya sosyal medya takip aracının çalışıyor olması arka planda bir şeyler saklamadığı anlamına gelmez. Suçlular, kötü amaçlı kodlarının incelemelere takılmamasını sağlamak için genellikle şifreleme kullanır veya kötü amaçlı kodları gecikmeli olarak ekleyerek uygulama testleri geçene kadar ortaya çıkmamasını sağlar. Başvurdukları diğer bir hile de cihazın konumunu kontrol etmek ve kötü amaçlı kodun sadece belirli ülkelerde çalışmasını sağlamaktır. Bazıları da uygulama yüklendikten sonra ek kod indirilmesini sağlayarak kötü amaçlı kodun incelemeye hiç girmemesini amaçlar. Son olarak suçlular bazen kodlarını bir sonraki yazılım güncellemesine otomatik olarak dahil edilen üçüncü taraf kod kitaplığına yerleştirerek normal uygulamaları kötü amaçlı uygulamaya dönüştürmeyi başarırlar.

Dolayısıyla karşınıza çıkan hemen her uygulama kötü amaçlı olabilir ve bu nedenle telefonunuzu, tabletinizi ve dijital hayatınızı kötü adamlardan korumak için bazı ek adımlar atmanız gerekir.

Bu uygulamalar nasıl kötülükler yapıyor?

Dolandırıcılar genellikle paranın veya paraya çevirebilecekleri verilerin peşindedir. Dolandırıcılık amaçlı reklamlara tıklanmasını sağlamak veya bu tür reklamlar oluşturarak kullanıcıların kimlik bilgilerini çalmak, bu tür uygulamaların denediği en yaygın yöntemlerden bazılarıdır. Çoğu arka planda gerçekleştiğinden bu işlemlerin farkında bile olmayabilirsiniz.

Bir uygulamayı yüklerken, kurarken veya kullanırken aşağıdakilere benzer olaylarla karşılaşırsanız hemen kurulumu durdurun veya uygulamayı bulup silin:

- Uygulamanın gereksiz izinler istemesi
- Kurulumun ardından uygulama simgesinin menüden kaybolması
- Ana ekran veya kilit ekranı gibi uygulamanın bağlamı dışındaki yerlerde reklam gösterilmesi
- Web tarayıcısının sizi bilmediğiniz bir web sitesine yönlendirmesi
- Telefonunuzun kamerayı, mikrofonu veya konum servislerini açmak gibi beklenmedik işlemler gerçekleştirmesi
- Varsayılan ana sayfanız veya arama motorunuz gibi ayarların değiştirilmesi

Yapay zeka dolandırıcılara nasıl yardımcı oluyor?

Geçen yılın sonunda OpenAI, yapay zeka destekli görüntü oluşturma uygulaması DALL-E 2'nin kullanıma açılmasıyla manşetlerde kendisine yer buldu. Bu uygulama, fotoğraflara dayalı sanatsal görüntüler oluşturabilen yapay zeka tabanlı mobil uygulamalar dalgasını başlattı. Lensa gibi uygulamalar güvenilir olsa da diğer uygulamalar yapay zeka alanındaki en son gelişmelerinden yararlanmak isteyen kötü amaçlı uygulamalar olabilir.

ChatGPT'nin yeni sürümü bazı endişeleri de beraberinde getiriyor. ChatGPT, insanlarla hemen hemen aynı şekilde sohbet edip metin yazabilen bir yapay zeka programı ve dolandırıcıların yazım ve dil bilgisini geliştirmelerine yardımcı olabilir.

Telefonunuzda kötü amaçlı bir yazılımın çalışıyor olabileceğine dair diğer işaretler:

- Beklediğinizden daha fazla mobil veri tüketimi
- Cihazı kullanmamanıza rağmen pilin çabuk bitmesi veya cihazın aşırı ısınması
- Sosyal medyada bilginiz dışında gerçekleştirilen işlemler, farklı yerlerden giriş yapılması, gönderi paylaşılması, beğeni atılması vb.
- Bilginiz dışında eklenen yeni kişiler veya takvim etkinlikleri
- İzniniz olmadan yüklenen yeni uygulamalar veya ana ekranda görünen yeni simgeler
- Gönderdiğini hatırlamadığınız ücretli SMS mesajları
- Bilginiz dışında başlatılan ücretli operatör hizmeti abonelikleri

Telefonunuzda kötü amaçlı uygulama olduğunu düşünüyorsanız şunları yapabilirsiniz:

- Telefonunuzu güvenli moda alın (yalnızca Android telefonlar için)
- Güvenilir bir güvenlik uygulamasıyla virüs taraması yapın; ucuz veya ücretsiz olduğu için daha önce adını hiç duymadığınız bir uygulamayı indirmeyin
- İşletim sisteminiz güncel değilse güncelleyin
- Cihazınızı yeniden başlatın
- Şüphe uyandıran tüm uygulamaları silin
- Bu yöntemlerin hiçbiri işe yaramazsa son aşamada telefonunuzu fabrika ayarlarına sıfırlamanız gerekebilir. Bunu yaptığınızda tüm sorunların giderilmesi gerekir.

Kendinizi sahte uygulamalardan korumak için kullanabileceğiniz ipuçları

McAfee ve App Defense Alliance topluluğunun diğer üyeleri, kötü amaçlı uygulamaların resmi uygulama mağazalarına ulaşmasını önlemeye yardımcı olmak için işbirliği yapıyor ancak tüketicilerin yapması gereken bazı işlemler de var:

Biraz araştırma yapın

Uygulamanın kaynağı güvenilir mi? Geliştiricinin diğer uygulamalarına göz atın. Söz konusu olan bir bankacılık veya benzeri bir finans uygulamasıysa şirketin web sitesine gidin ve resmi geliştirici hesabı tarafından yayınlanan resmi uygulamayı indirdiğinizden emin olun.

Yorumlara göz atın

Olumsuz veya 1 yıldızlı yorumları okuyun. Dolandırıcılar genellikle "Güzel uygulama" gibi çok sayıda kısa ve standart 4/5 yıldızlı yorumlar yayınlar ve ardından çok sayıda sahte oyla bu yorumları listenin en üstüne taşır.

Gerçek olamayacak kadar güzel mi görünüyor?

Siber güvenlikte genelgeçer bir yaklaşım vardır. Gerçek olamayacak kadar güzel görünüyorsa muhtemelen gerçek değildir. Uygulamanın normalden daha yüksek bir yatırım getirisi vaat etmesi veya sosyal medya hesabınızı ücretsiz olarak hızla büyütebileceğinizi söylemesi büyük olasılıkla farklı bir şekilde bedel ödeyeceğinizi gösterir.

İzinlere dikkat edin.

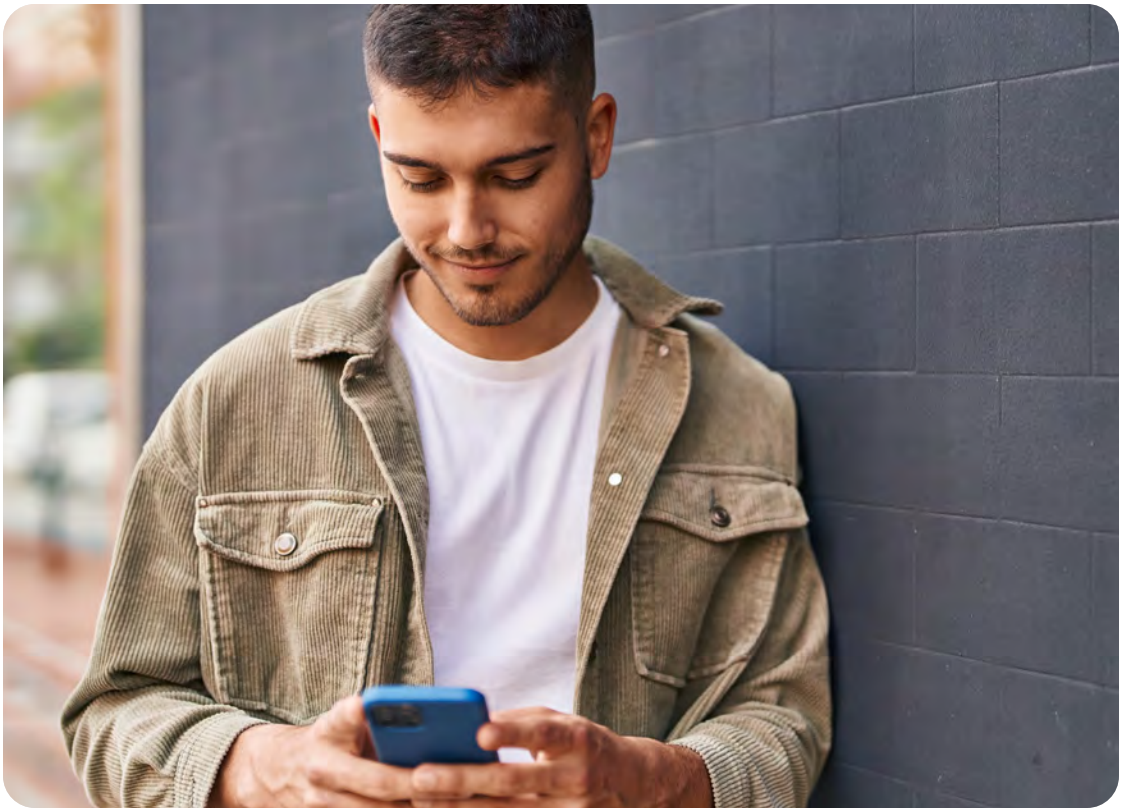
Bir el feneri uygulamasının gerçekten de ses kaydetmesi veya kişilerinize erişmesi gerekir mi? Android telefonlarda "Ayarlar" sayfasından "Uygulamalar"a ve ardından uygulamaya tıklayıp "İzinler" listesine göz atabilirsiniz. iPhone'da "Ayarlar"a ve ardından "Gizlilik ve Güvenlik" girişine tıklayın. Uygulamaya vermek istediğiniz izinleri ve engellemek istediklerinizi seçebiliyor olmanız gerekir. En başında uygulamanın bu izinlerden bazılarına neden ihtiyaç duyduğunu sorgulamayı unutmayın.

Doğrulanmış mağazalardan şaşmayın

Kötü amaçlı uygulamalar tüm uygulama mağazalarına sızmayı başarabilir ancak Google Play ve Apple App Store gibi resmi platformlar hem uygulamaları yayınlanmadan önce incelemek hem de yayınlandıktan sonra keşfedilen kötü amaçlı uygulamaları belirleyip kaldırmak için katı süreçlere sahiptir. Üçüncü taraf uygulama mağazalarda bu süreçler zorunlu olarak uygulanmayabilir ve hatta bu mağazalardan bazıları mobil kullanıcılara kasıtlı olarak kötü amaçlı yazılım dağıtmak için tasarlanmış olabilir.

İkinci Başlık:
Tehdit

DM atan dolandırıcılar



Tehdit: DM atan dolandırıcılar

Doğrudan mesajlar veya DM'ler, kişilerin arkadaşları ve takipçileri tarafından görülemeyen özel sohbetler yapmak için kullandığı popüler bir yöntem. Bunlar ister basit metin veya SMS mesajları, ister iMessage ve WhatsApp gibi mesajlaşma uygulamaları veya bir sosyal medya platformunun eklentileri olsun, suçlular tarafından kötü amaçlı bağlantılar göndermek veya insanları daha büyük dolandırıcılıklara yönlendirmek için kullanılıyor. Mesajların güvenli veya şifrelenmiş olması, karşı tarafta bir dolandırıcı olmasına engel değildir!

Ne tür mesajlar var?

Your Netflix account has been suspended, because we're having some trouble with your current account information.

Recovery your Netflix account immediately by click link bellow:

[redacted]

Please take action on your account within 48 hours to avoid permanent suspension.

Best regard,
Netflix, Inc.

Venmo,

Your Venmo account has been suspended, because we're having some trouble with your current account information.

Validate your account information by click link bellow:

[redacted]

Please take action on your account within 24 hours to avoid permanent suspension.

Best regards,
Venmo. Inc

Reminder: Take action on your PayPal account

Your PayPal acount is currently limited, We noticed that you've been using your PayPal account in a questionable manner. To understand this better, we need more information from you.

To help keep your account secure, immediately by click link bellow and perform the required tasks.

[redacted]

Please take action on your account within 24 hours to avoid permanent suspension.

Best regards,
PayPal Pte. Ltd.

FBsej1

Amazon :

Your account has been locked due suspicious activity.

All of your last orders and subsription has been on hold until this issues fixed.

Click link below to unlock your account :

[redacted]

If you do not complete the verification process before 24 hours, your Amazon account will be terminated.

Sincerely,
Amazon Team

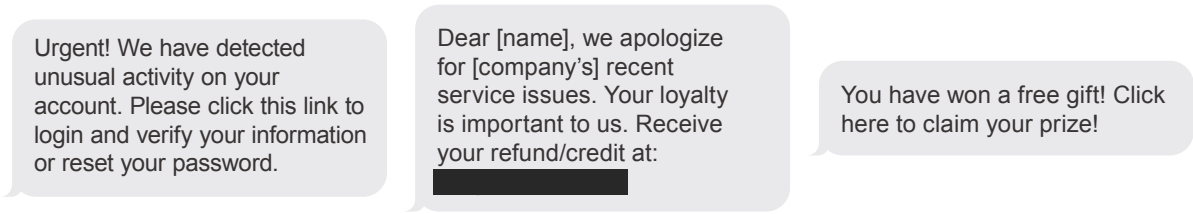
Çoğu mesaj güvenli olsa da bir bağlantıya tıklamadan veya bir DM'e yanıt vermeden önce gerçek olduğundan emin olmak için birkaç saniyenizi ayırmanız önemlidir. Dolandırıcılar sahte mesajlar kullanarak sizi kandırıp kötü amaçlı bir bağlantıya tıklamanızı ve ardından giriş bilgilerinizi veya hesap numaralarınızı girmenizi veya kişisel bilgilerinizi paylaşmanızı sağlamaya çalışır. Bu mesajlarda bazen yazım veya dil bilgisi hataları ya da garip ifadeler yer alabilir.

Yapay zeka dolandırıcılara yardım ediyor:
ChatGPT gibi yapay zeka araçlarının kullanıma sunulmasıyla birlikte dolandırıcılar, yazım ve dil bilgisi hatalarını düzeltebiliyor ve bu da dolandırıcılık amaçlı mesajların içerikteki hatalar sayesinde tespit edilmesini zorlaştırıyor.

Dikkat edilmesi gereken diğer bazı uyarı işaretleri şunlardır:

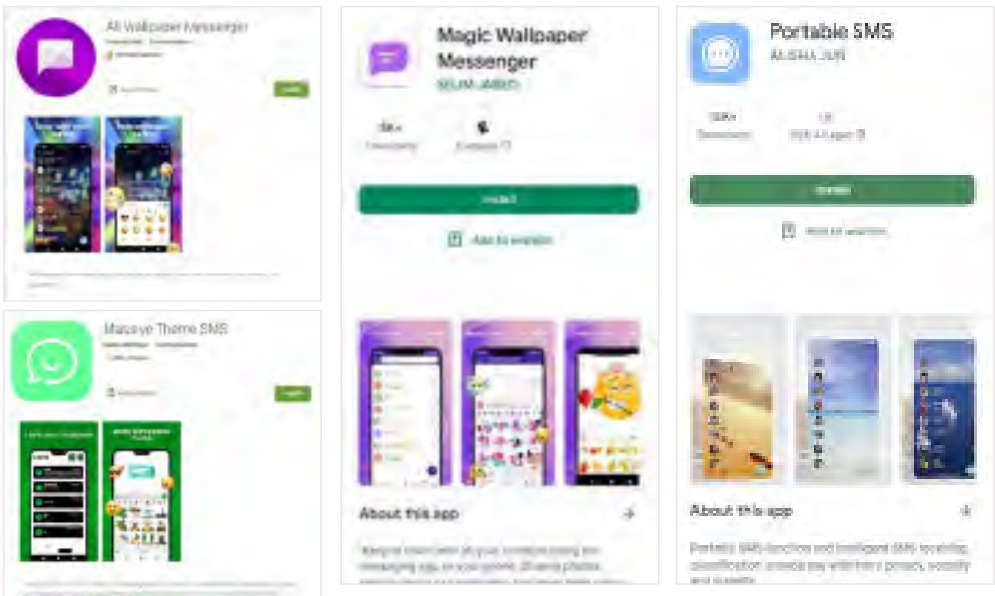
- Bilinmeyen bir numaradan veya güvenilir bir kuruluşa ait gibi görünen bir numaradan beklenmeyen mesajlar
- Kişisel bilgilerinizi vermediğiniz takdirde hesabınızın kapatılacağına dair uyarı gibi acil veya tehdit edici ifadeler içeren mesajlar
- Kişisel bilgilerinizi güncellemek veya hesabınıza giriş yapmak için bir bağlantıya tıklamanızı isteyen mesajlar
- Bonus, ödül veya para iadesi teklifleri
- Peşin işlem ücreti veya idari ücret talepleri

Tipik örnekler şunlardır:



MoqHao olarak bilinen kötü amaçlı yazılım ailesi en yaygın mobil tehditlerden biridir ve genellikle SMS mesajlarıyla bulaşır. MoqHao, 2022'de dünya çapında 573.000'den fazla cihaza bulaştı ve özellikle Japonya, Fransa, Güney Kore, İspanya, Türkiye ve Amerika Birleşik Devletleri'ndeki kurbanları etkiledi. Ancak MoqHao, dünyanın farklı noktalarındaki cihazlara bulaşmayı da başardı.

McAfee'nin 2022'de Google Play'de tespit ettiği tehditlerin %6,2'si "İletişim" kategorisindeydi ve bunların çoğu sahte SMS Mesajlaşma uygulamalarıydı. Joker kötü amaçlı yazılımı, sahte SMS uygulamaları arasındaki en yaygın ailedir. Bu kötü amaçlı yazılım, telefon sahibinin bilgisi olmadan SMS mesajları gönderip özel numaraları arayarak telefon faturasını şişirir ve suçluların bundan pay almasını sağlar. Bu yöntem genellikle "ücretli numara dolandırıcılığı" olarak bilinir.



Şekil 2. McAfee'nin 2022'de tespit ettiği kötü amaçlı iletişim uygulaması örnekleri.
Denenmiş ve doğrulanmış uygulamalardan şaşmamak en iyi seçenektir. (Gösterilen uygulamalar Google Play'den kaldırılmıştır.)

"Yemleme" yöntemini duydunuz mu?

"Yemleme", suçluların kurbanın parasını çalmadan önce onu beslediği dolandırıcılık mesajları için kullanılan bir terimdir. Bu girişimlerde genellikle suçlular "Merhaba" veya "geçen hafta ne eğlendik" gibi basit bir mesaj atar ve karşıdan "yanlış numara" yanıtının gelmesini bekler. Bu mesajın ardından dolandırıcı yeni bir arkadaş bulmuş gibi davranır ve karşı tarafın güvenini kazanmak için bir sohbet başlatır. Başarılı bir borsacı olduğunu söyleyebilir ve kripto paralar gibi bazı özel yatırımlarla çok para kazandığından bahsedebilir. Burada amaç, kurbanın sahte bir yatırım uygulaması indirmesini veya güvenilir görünen bir yatırım hesabı açmasını ve buraya bir miktar para aktarmasını sağlamaktır.

Bu uygulamalar veya web siteleri oldukça iyi tasarlanmıştır ve dolandırıcılar bazen yatırım fırsatıyla ilgili görüntülü görüşme yapar veya kurbanı daha kolay kandırmak için sahte kazancının küçük bir bölümünü çekmesine izin verir. Ardından suçlular kurbanın giderek daha fazla para yatırmasını ister ve hatta bunu yapmak için karşı tarafı borç almaya ve kredi çekmeye teşvik eder. Dolandırıcıların amacı kurbanın cebindeki son kuruşa kadar alıp sonra kaçmaktır. Arka planda suç örgütlerinin bunları büyük ölçekte yürütmesini kolaylaştıran, genellikle zorla çalıştırılan kişileri veya insan kaçakçılığı kurbanlarını istismar eden ayrıntılı senaryolar ve yöntemler vardır.

Bu dolandırıcılıklardan uzak durmak için en iyi tavsiye, kısa sürede zengin olma planlarına veya istenmeyen yatırım fırsatlarına çok şüpheci yaklaşmaktır. Kulağa gerçek olamayacak kadar güzel geliyorsa genellikle gerçek değildir!

QR kodların getirdiği risklerin farkında mısınız?

Siyah ve beyaz piksellerden oluşan kare kutular olan QR kodlar, mobil cihazların bir kamerayla okuyabildiği ve bir mesaja veya eyleme dönüştürebildiği "hızlı yanıt" barkodlarıdır. Bu kodlar özellikle pandemi sırasında restoran menüleri gibi bilgilerin dokunmadan paylaşılmasını sağladıkları için popüler oldular.

Her QR kod 4.000 karakterden fazla veri tutabildiğinden bir web sayfasını açmak, mesaj göndermek ve bir uygulama indirme bağlantısı sağlamak gibi birçok işlem için kullanılabilir. Yüksek esneklik sunan bu teknoloji birçok farklı amaçla kullanılabilir, örneğin:

- Menüyü görüntülemeye ek olarak restoranda sipariş verme ve ödeme yapma
- Paylaşılan Wi-Fi ağlarına kolay erişim
- Ürün ambalaj içeriği ve ürün bilgileri
- Sosyal medya bağlantıları
- Müze ve sanat galerisi sergi bilgileri
- Etkinlik bilgileri, toplu taşıma tarifeleri
- Mobil ödemeler

Ancak diğer birçok dijital araç gibi bunlar da suçlular veya kötü amaçlı kişiler tarafından kullanılıyor. Dolandırıcılar, QR kodları web siteleri, sosyal medya, kısa mesajlar aracılığıyla paylaşabilir ve hatta orijinal QR kodların üzerine çıkartmalar yapıştırabilir.

Kodlara yerleştirilen bağlantılar şunları yapabilir:

- Kullanıcıları, kişisel bilgileri çalmak için tasarlanmış sahte sitelere yönlendirme
- Kötü amaçlı yazılım indirme
- Güvenliği ihlal edilmiş bir Wi-Fi ağına bağlanma
- Banka kimlik bilgileri veya diğer değerli kişisel bilgiler için kimlik avı yapma

Kendinizi nasıl koruyabilirsiniz? Kötü amaçlı kodların kurbanı olmamak için:

- Almayı beklemediğiniz QR kodları tararken dikkatli olun
- QR kodun sizi yönlendirdiği web sitesinin URL'sini kontrol edin
- Güvenilir bir kaynak tarafından yayınlanan güvenilir bir QR kod okuma uygulamasını kullanın ve indirmeden önce yorumlara göz atın
- Kişisel bilgilerinizi koruyun, nerede ve kiminle paylaştığınıza dikkat edin
- Uygulamaları doğrudan QR kodlardan indirmeyin, gerçek kodlar resmi uygulama mağazasına yönlendirecektir

Kendinizi DM dolandırıcılıklarından korumak için kullanabileceğiniz ipuçları

Özetlemek gerekirse paranızı ve kişisel bilgilerinizi DM dolandırıcılığından korumak için buradaki ipuçlarından yararlanabilirsiniz.

Sahte DM'lerdeki uyarı işaretlerine dikkat edin

Bilinmeyen kişilerden gelen mesajlara, acil uyarılara, para iadesi tekliflerine veya hesabınıza giriş yapma isteklerine şüpheyle yaklaşın. Tıklamadan önce mesajdaki bağlantıları dikkatlice inceleyin. Mesajda verilen bağlantıya tıklamak yerine doğrudan şirketin web sitesine gidin.

Modlara dikkat edin

Doğrudan mesajlaşma uygulamaları için ekstra özellikler sunan veya bazı ülkelerde iletişim engellerini aşmanın yollarını sunan birçok "mod" vardır. Bu modlar sık sık kötü amaçlı veya casus yazılımların hedefi olur.

"Yemleme" girişimlerine dikkat edin

Birikimlerinizi çalmak isteyen suçluların sizi yemleyerek kandırmasına izin vermeyin. Kime para gönderdiğinize dikkat edin ve kendi isteğinizle dahil olmadığınız yatırım tekliflerini araştırın. Güvenilir yatırım şirketleri resmi makamlara kayıtlı olur ve yüksek getiri vaat edemez veya bu yönde bir garanti sunamaz.

QR kodlara dikkat edin

Herhangi bir QR kodun bağlandığı web sitesi adresini dikkatlice inceleyin ve gerçek olduğundan emin olun. Telefonunuzun donanım veya yazılım geliştiricisi tarafından yayınlanan veya telefonunuzun kamerasında bulunan güvenilir bir QR kod okuyucu kullanın. Kişisel bilgilerinizi paylaşırken son derece dikkatli olun.

Üçüncü Başlık: Tehdit

Kişisel telefonunuzu iş için kullanma

Tehdit: Kişisel telefonunuzu iş için kullanma

Birçoğumuz, işle ilgili önemli bir telefon veya e-posta beklerken telefonsuz kalmanın getirdiği o panik duygusunu yaşamışızdır. İş hayatımızla kişisel hayatımız elektronik ortamda iç içe geçmiş durumda. Arabada, spor salonunda ve hatta yatakta bile e-postalarımızı kontrol etmekten geri kalmıyoruz.

Cep telefonları insanların üretkenlik uygulamalarına ve iletişim araçlarına erişmesini, aynı zamanda masalarına bağlı kalmadan işlerini yapmalarını sağlayan güçlü bir iş aracıdır. Ancak bu davranışla şirketlerimizi nasıl riske atıyoruz?

Yapılan son araştırmalara göre çoğumuz mobil cihazları hem iş hem de kişisel amaçlı olarak kullanıyoruz. İş cihazlarında kişisel e-postalarımızı kontrol ediyor, bazen de tam tersini yapıp kişisel cihazlarımızdan iş e-postalarımıza bakıyoruz. İş cihazları teorik olarak işverenler tarafından yönetiliyor ve BT departmanları güvenlik açıklarını kapatıp uygulamaları güncelliyor. Peki iş cihazınızın ne kadar güvenli olduğunu biliyor musunuz? İşvereniniz kişisel cihazınızın güvenliğini de yönetiyor mu? Yoksa iki tarafı da riske mi atıyorsunuz?

Risk değerlendirmesi: İşi ve kişisel görevleri birlikte yürütme

Birçok insan için kişisel cihazlar ve iş cihazları arasında bir ayrım yoktur. Daha büyük şirketler size bir cihaz verebilir veya sizi işte kişisel telefonunuzu veya tabletinizi kullanmaya teşvik eden Kendi Cihazını Getir (BYOD) politikasına sahip olabilir. Daha küçük işletmeler, girişimciler veya ortak araç kullanan sürücüler ya da köpek gezdiriciler gibi serbest çalışanlar büyük ölçüde kişisel mobil cihazlarını kullanır.

Hangi gruba dahil olursanız olun bu raporda yer verilen DM dolandırıcılıkları veya uygulama mağazası güvenlik sorunları gibi mobil tehditler evde olduğu kadar işte de geçerlidir. Acil bir proje için hediye kartı almanızı veya şirketten para transferi yapmanızı isteyen bu mesaj gerçekten patrondan mı geliyor? Çeşitli görevlerinizi yönetmenize yardımcı olması için indirdiğiniz uygulama gerçek ve güvenilir mi? Şirketinizi güvenlik tehditlerine ve dolandırıcılık girişimlerine açık hale getirmemek için iş uygulamalarına veya veritabanlarına güvenli bir şekilde giriş yapıyor musunuz?

Mobil cihazlara yönelik iş uygulamaları (PDF düzenleyiciler, VPN'ler, mesajlaşma yöneticileri, belge tarayıcılar, pil güçlendiriciler ve bellek temizleyiciler gibi kategoriler) üretkenliğinizi artırmanıza yardımcı olabilir. Bu tür uygulamalar tipik erişim profilleri nedeniyle kötü amaçlı yazılımların hedefi olur. Bu tür bir uygulamanın depolama, mesajlaşma, takvimler, kişiler, konum ve hatta sistem ayarları için izin istemesi alışılmadık bir durum değildir ve bu da dolandırıcıların işle ilgili her türlü bilgiyi almasına olanak tanır.

Sosyal mühendislik ve dolandırıcılık girişimleri

Teknik Destek dolandırıcılığı uzun yıllardır kullanılan bir yöntem olsa da uzaktan çalışmanın yaygınlaşmasıyla birlikte yerinde destek yerine telefon üzerinden destek yöntemine daha çok başvurulması siber suçluların bu alandaki girişimlerinin artmasına neden oldu. Bu dolandırıcılıklarda genellikle arayan kişiler sizin farkında olmadığınız bir sorun için teknik destek sunma teklifinde bulunur. Birçoğu kişisel bilgisayarınızı düzeltme konusunda yardım etmeyi teklif edebilir. Bu tür bilgileri şirketinizin yardım masası da talep edebileceğinden dikkatli olmanız gerekir. Bu dolandırıcılıkların nasıl gerçekleştiğini ve yapmanız gerekenleri öğrenmek için buraya göz atın.

Teknoloji daha esnek bir şekilde çalışmamızı sağladı ancak bu esneklik, sorumluluğu da beraberinde getiriyor. Yalnızca kişisel dijital hayatlarımızın değil aynı zamanda profesyonel dijital hayatlarımızın da güvenliğini de sağlamamız gerekiyor.

McAfee'nin 2022'de Google Play'de tespit ettiği tehditlerin %23'ü "Araçlar" kategorisinde yer alıyordu ve bu kategori Eğlence, İletişim ve Kişiselleştirme Uygulamaları dahil olmak üzere tüm uygulama kategorileri arasında en yüksek yüzdeye sahipti.

İş cihazlarını ve kişisel cihazları çapraz tehditlere karşı korumak için ipuçları

Kişisel cihazınızda gerçekleştirebileceğiniz işlemler

- Telefonunuzun kilidini açmak için şifre girilmesi gerektirdiğinden emin olun ve makul bir otomatik kilitleme süresi ayarlayın.
- Yanlışlıkla ifşa etme olasılığını azaltmak için iş ve kişisel görevler için farklı uygulamalar kullanmayı veya mobil cihazınızdaki bir klasörü veya ekranı "yalnızca iş" uygulamalarına ayırmayı değerlendirin.
- Bilinen güvenlik sorunlarından ve güvenlik açıklarından kaynaklanan riskleri azaltmak için uygulamalarınızı ve mobil işletim sisteminizi sürekli güncel tutun.
- Herkese açık veya bilinmeyen Wi-Fi ağlarına bağlanıyorsanız VPN kurun ve kullanın.
- Cihazınıza yeni uygulamalar yüklerken dikkatli olun.

Dikkat etmeniz gerekenler

- Dolandırıcılık veya kimlik avı mesajlarına ve hangi hesaba gönderildiklerine dikkat edin. Kişisel e-posta adresinizi iş arkadaşlarınızla paylaştınız mı? Paylaşmadıysanız bu adresi nereden buldular?
- Gönderenin kimliğini doğrulamak için zaman ayırın ve kişisel e-posta veya SMS yoluyla sizinle iletişime geçmelerinin mantıklı olup olmadığını değerlendirin.
- Mümkün olduğunda çok faktörlü kimlik doğrulamasını kullanın ve dolandırıcılık girişimlerine karşı dikkatli olun. Suçlular, gerçek gibi görünen ve kimlik doğrulaması koduyla doğrulama yapmanızı isteyen kısa mesajlar gönderebilir ve daha sonra bu kodu kullanarak hesabınıza giriş yapmaya çalışabilir.

İş tarafında doğrulanması gerekenler

- Kuruluşunuzun bir BYOD politikası olup olmadığını kontrol edin ve güvenlik gereksinimlerine uygun hareket ettiğinizden emin olun.
- İş uygulamalarına veya veritabanlarına bağlanırken ya da herkese açık veya bilinmeyen Wi-Fi ağlarını kullanırken şirket onaylı VPN uygulamasını kurun ve kullanın.

Dördüncü Başlık: Zorluk

Telefon sahibi çocuklara ve gençlere modern ebeveynlik yapma

Zorluk: Telefon sahibi çocuklara ve gençlere modern ebeveynlik yapma

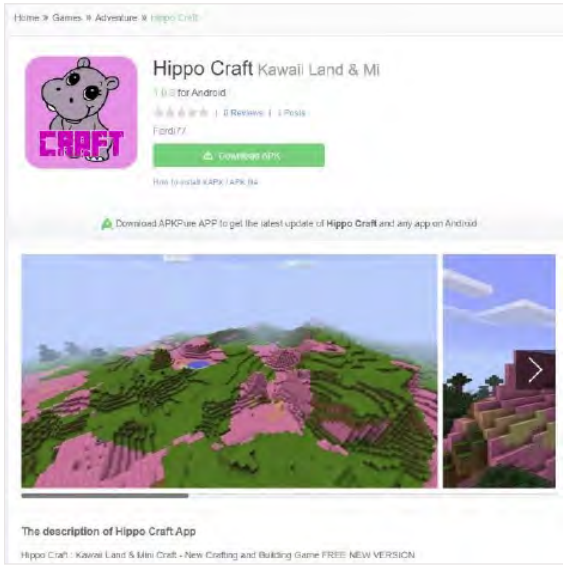
Dijital çağda ebeveynlik yapmak bazı zorlukları da beraberinde getirir. Cep telefonları, ebeveynlerin ve çocukların iletişim halinde kalmasına yardımcı olma açısından faydalı olsa da bu cihazlar potansiyel tehlikelerin kaynağı da olabilir. Ebeveyn denetimleri, çocukların dijital hayatlarını korumaya yardımcı olabilir. Ancak onları çevrimiçi ortamda tamamen güvende tutmak için hem çocukların hem de ebeveynlerinin teknolojilerden, şahsen takip etme olanaklarından ve bu alanlarla ilgili sunulan eğitimlerden faydalanmaları gerekir.

Kötü amaçlı uygulamalardan daha fazlası

Kötü amaçlı uygulamalar genellikle oyun oynamak, video çekmek ve sosyal medya hesaplarını yönetmek gibi çocukların ve gençlerin sevdiği faaliyetleri hedefler. Uygulamalardan kaynaklanan tehdidi raporun ilk bölümlerinde inceledik ancak çocukların telefonlarına yeni uygulamaları indirmesinin kısıtlandığından ya da bu konuda bilgi sahibi olduklarından ve şüpheli uygulamaları sorgulayıp dolandırıcılık amaçlı olanları tespit edebildiğinden emin olmak önemlidir. McAfee'nin 2022'de Google Play'de tespit ettiği tehditlerin %9'u Basit Eğlence, Arcade ve Aksiyon gibi uygulama kategorilerindeki Oyunlardı.

Zararlı uygulamalar ve aşırı reklam gösteren kötü amaçlı veya reklam amaçlı uygulamalar TikTok, Instagram ve YouTube gibi çocuklar ve gençler arasında popüler olan sosyal medya platformlarında öne çıkarılır. Bu uygulamalar, Minecraft ve Roblox gibi oyunlarla ilgili kanalları hedefler. Hatta bazen resmi uygulama mağazalarında bile kötü amaçlı oyunlar ve oyun modları ortaya çıkabilir. Bu uygulamalar genellikle güvenlik sürecinde yakalanıp kaldırılır ancak ilgili uygulamalar indirilmiş oldukları telefonlardan silinmeyebilir. Bu nedenle çocuklarınızın cihazlarında zararlı uygulamaları anında tanımlayıp işaretleyebilen ve hatta kaldırabilen güvenlik korumasına sahip olmaları önemlidir.

Şekil 3. Bu örnekte sosyal medya şifrelerini çalan bir oyun gösterilmiştir. Uygulama yüklendikten sonra Facebook üzerinden kimlik doğrulaması yapılmasını ister ve hesap bilgilerini ele geçirir. (Gösterilen uygulama Google Play'den kaldırılmıştır.)



Şekil 4. Bu, blok işleme oyun modu olarak dağıtılan HiddenAds kötü amaçlı yazılım kategorisine bir örnektir. (Modlar, orijinal oyunu değiştirerek oyuncular için daha ilginç, daha kolay veya daha zorlayıcı hale getirebilir.) Bu uygulama Google Play'den kaldırıldı ancak üçüncü taraf pazarlarda hâlâ mevcut.

2022'de oyun kategorisinde tespit edilen en yaygın tehdit türleri, uygulamayı kullanırken ve hatta kullanmadığınız zamanlarda bile aşırı reklam görüntüleyen aşırı reklam uygulamalarıydı. Bu tür uygulamalar telefonun performansını etkileyebilir ve kullanımı çok sinir bozucu hale getirebilir. Reklam yazılımlarının en popüler örneklerinden biri, reklam görüntüleyen ve pazarlama amacıyla kullanıcı verilerini toplayan HiddenAds Trojan yazılımıdır. Reklam yazılımları ayrıca kişisel verileri toplayabilir ve başta diğer arkadaşlarıyla olan etkileşimleri olmak üzere çocuğun etkinliklerini takip edebilir ve bu sayede daha fazla cihaza bulaşabilir.

Ancak çocukların ve ebeveynlerinin dijital dünyada dikkat etmesi gereken sadece zararlı uygulamalar ve kötü amaçlı yazılımlar değildir. Sosyal medya; influencer kültürü, tehlikeli veya yasa dışı popüler "akımlar" ve siber zorbalık gibi dikkat edilmesi gereken bir dizi yeni kavramı da beraberinde getirir. İlgili uygulama ve kanalların çoğu reklam gelirleriyle desteklendiğinden çocuklar ve gençler yüksek hacimli hedefli reklamlara ve gizli ya da öyle olduğu açıkça beyan edilmeyen sponsorlu ürünlere maruz kalıyor.

Influencer'lar, akımlar ve zorbalık

Sosyal medya birçok çocuğun ve gencin hayatında büyük bir rol oynar ve birçok farklı artıları ve eksileri vardır. Bu araçların aile üyeleri ve arkadaşlarla ilişkileri geliştirmeye, sosyal çevreler arasında bağlantı kurmaya ve insanları yeni kavram ve kültürlerle tanıştırmaya katkıda bulunabileceği kabul edilen bir gerçek. Ancak siber zorbalık, akran baskısı ve bilgisiz takipçileri kandırmak isteyen kötü niyetli kişiler için bol miktarda hedef sunan ortamlar haline geldiler.

Influencer'lar ve benlik algısı

Her yaştan çocuk, ilham ve motivasyon için kendine rol modeller arar. Ancak günümüzün beğeni, takip ve paylaşımları temel alan popülerlik ölçütleri genç beyinleri motive etmek yerine onları zehirleyebilir. Çocuklarınızla influencer'lar hakkında konuşmak zor olabilir. Çocuklara kimi takip ettiklerini, bu kişi hakkında neleri beğendiklerini ve benzer bir durumda olsalar nasıl davranacaklarını sormanızı öneriyoruz. Influencer'ı doğrudan eleştirmek yerine değerleri ve hedefleri keşfetmeye odaklanın.[2]

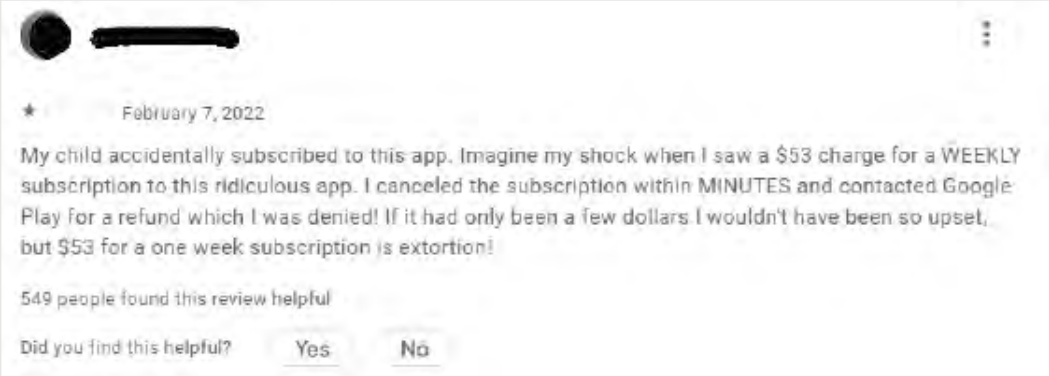
Tehlikeli veya yasa dışı "akımlar"

TikTok son zamanlarda potansiyel gizlilik ihlalleriyle ilgili çok sayıda habere konu oldu. Ancak bu ve diğer uygulamalardaki çocuklara yönelik en büyük tehditlerden biri, viral olan ve tehlikeli ya da yasa dışı olabilen "akımlardır". Son örnekler arasında çok miktarda tarçın yemek, halüsinasyon görme noktasına gelene kadar Benadryl içmek veya bir arabaya USB kabloyla düz kontak yapmak (ve çalmak) yer alıyor. TikTok'un güvenlik merkezi, gençlerin dört aşamalı bir eleştirel düşünme süreci geliştirmelerine yardımcı olmayı öneriyor: Dur, Düşün, Karar Ver ve bunları yaptıktan sonra Harekete Geç.[3]

Ancak takip ve paylaşımları temel alan popülerlik ölçütleri genç beyinleri motive etmek yerine onları zehirleyebilir.

Abonelikler ve mobil ödemeler

Kötü adamların çocuklardan ve gençlerden faydalanma yöntemlerinden biri, belirsiz veya yanıltıcı uygulama içi satın almalar ve aboneliklerdir. Çocuklar, şartları ve koşulları veya tam olarak neyi kabul ettiklerini anlamayabilir veya umursamayabilir. Bu da uygulamanın değerinin çok ötesinde aşırı yüksek ödemeler yapılmasına neden olabilir.



Şekil 5. Google Play'deki bir kullanıcı yorumunun ekran görüntüsü.

Siber zorbalık

Yakın tarihli bir McAfee Bağlantılı Aile Raporu, çocukların %60'ının siber zorbalık konusundaki endişelerinin bir önceki yıla göre arttığını gösterdi. Rapor, dünya genelinde dört çocuktan birinden fazlasının ırkçılık kaynaklı siber zorbalığa uğradığını, sekiz çocuktan birinin fiziksel tehdit şeklinde siber zorbalığa uğradığını ve altı çocuktan birine müstehcen mesajlar veya resimler gönderildiğini tespit etti.[4]

Siber zorbalığın etkileri kalıcıdır. Çocuklara bu konular hakkında konuşabilecekleri ve çözümler geliştirebilecekleri güvenli bir ortam yaratmak, onları dijital bağlantılara sahip bir dünyada güvende tutmanın en önemli bileşenlerinden biridir.

Hedefli reklamcılık ve sponsorlu içerik

Sosyal medyanın ücretsiz olmasının nedeni, şirketlerin her türlü kişisel veriyi toplamasıdır. Pazarlamacılar, belirli kitleleri hedeflemek ve kullanıcıları ürün haline getirmek için bu verilerden yararlanır. Kişiselleştirilmiş reklamlar, sponsorluklar ve ürün yerleştirme bazen faydalı olsa da yanıltıcı olabilir ve bazı durumlarda hizmeti satın almadığınız veya abone olmadığınız takdirde kendinizi dışlanmış hissetmenize veya kendinize olan saygınızı yitirmenize neden olabilir.

Çocuklarınızla takip ettikleri influencer'larla bağlantılı ürün yerleştirmeleri ve sponsorluklar hakkında konuşmanız önemlidir. Sonuçta bunlar örnek aldıkları ve hatta taklit etmek isteyebilecekleri kişilerdir. Çocukların, sosyal medya influencer'larının bazen kendilerine para ödendiği için ilgili ürünleri kullandığını veya tanıttığını söylemeleri ve bu konuda yeterli açıklama yapmaları gerekse de bunu herkesin yapmadığını anlamaları önemlidir.

Son olarak çocuğunuz kamera önüne geçiyorsa kendi gönderilerinde sponsorlu ürün veya hizmetlere yer vermenin getirdiği sorumluluklar hakkında sohbet etmenizde fayda vardır. ABD Federal Ticaret Komisyonu'nun (FTC) marka sponsorlukları veya mali ilişkiler hakkında ne zaman ve nasıl açıklama yapılacağına ilişkin faydalı bir kılavuzu vardır.

Çocuklarınızı telefonlarında güvende tutmaya yönelik ipuçları

Çocuğunuzun gizliliğini ve çevrimiçi etkinliğini korumanıza yardımcı olacak bazı önemli ipuçlarını burada bulabilirsiniz.[5]

Etkinliklerini takip edin

Hiçbir çocuk dijital hayatının ebeveynleri veya velileri tarafından incelenmesini istemez. Ancak çevrimiçi ortamda neler yaptıklarını, ilgilendikleri yeni uygulamaları veya güncel sosyal medya trendlerini ara sıra kontrol etmek önemlidir. YouTube'da neleri izliyorlar, TikTok'ta neler oluyor veya Instagram'da gönderi paylaşıyorlar mı?

Çocuklarınızı ve kendinizi eğitin

Benzer şekilde kendinizin ve çocuklarınızın gizlilik ayarlarını nasıl yapacağınızı bildiğinizden emin olun. İstemeden veya kasıtlı olarak paylaşabilecekleri kişisel bilgilerin nelere yol açabileceğini de anlatın. Bu herkesin daha güvenli ve daha bilinçli kararlar almasına yardımcı olmakla kalmaz, aynı zamanda gelecekte üniversiteye girerken, iş başvurusunda bulunurken ve hatta yeni insanlarla tanışırken de fayda sağlar. İşverenler, üniversiteler ve hatta yeni arkadaşlar ve iş arkadaşları sık sık ilgili kişileri sosyal medyada arar.

Var olan teknoloji araçlarını kullanın

Ebeveynlerin cihazlarda ekran süresini sınırlamak, belirli web sitelerini engellemek ve uygulamaları kısıtlamak için kullanabileceği faydalı araçlar vardır. Bunlar dijital ebeveynlikle ilgili tüm zorlukları çözmese de etkinliği takip etme ve bilinen kötü amaçlı sitelere erişimi engelleme konusunda kesinlikle yardımcı olabilir. Güvenlik yazılımları sahip oldukları gerçek zamanlı tehdit algılama, kimlik izleme ve gizlilik koruması özellikleriyle bir koruma katmanı daha ekler.

Çocuklarınızla sorunlar hakkında konuşun

Son olarak, çocuklarınızla sık sık sorunlar hakkında konuşmaya çalışın ve onların bakış açısını öğrenin. Açık ve dürüst iletişimi teşvik edin. Uygulamaları kendiniz kontrol edin. Çevrimiçi ortamda ne yaptıkları hakkında ne kadar çok şey bilirseniz bilinçli konuşma yapmak o kadar kolay olur. Onları kendi araştırmalarını yapmaları ve yorumlarıyla sorularını sizinle paylaşmaları konusunda teşvik edin. Dikkat edilmesi gerekenin yalnızca kötü amaçlı uygulamalar değil aynı zamanda zararsız uygulamalarda ortaya çıkabilen kötü amaçlı insanlar ve zararlı davranışlar olduğunu unutmayın.

En yaygın görülen 10 kötü amaçlı yazılım ailesi

En yaygın görülen 10 kötü amaçlı yazılım ailesi

McAfee araştırmacıları, müşterileri kötü amaçlı yazılımlardan korumak için çok çaba harcıyor. Peki kötü amaçlı yazılım nedir? Bir bilgisayar sistemine, ağa veya kullanıcı verilerine zarar vermek veya bunlardan yararlanmak için tasarlanmış HER TÜRLÜ yazılım veya kod bu başlık altında değerlendirilebilir.

Kötü amaçlı yazılımların verdiği zarar, kripto para madenciliği yapmak için bilgisayarınızdan faydalanmak gibi basit bir sıkıntıdan hassas bilgilerin çalınmasına ve hatta hesapların karşılığında fidye istenmesine kadar uzanabilir.

Araştırmacılar bu tehditleri "aileler" veya türler halinde gruplandırır. Aşağıda, McAfee'nin 2022'de tespit ettiği en yaygın görülen mobil kötü amaçlı yazılım ailelerinin listesi verilmiştir.

1 Dropper (Yükleyici)

Yükleyici, bir kurbanın cihazına kötü amaçlı yazılım indirmek ve yüklemek için kullanılan bir tür kötü amaçlı yazılımdır ve uzun yıllardır en yaygın görülen türdür. Genellikle bir saldırının ilk aşamasında kullanılır ve güvenlik sistemlerinden kaçınarak virüsten casus yazılıma ve fidye yazılımına kadar birçok farklı kötü amaçlı yazılımı yürütecek olan birincil "faydalı yükü" veya kötü amaçlı kodu yüklemek için tasarlanmıştır.

2 HiddenAds

HiddenAds adından da anlaşılacağı gibi bir kullanıcının cihazının arka planında onların bilgisi veya onayı olmadan reklam yayınlar (Gizli ifadesi bu özelliği niteler). Bu kötü amaçlı yazılım, üçüncü taraf reklamcılardan para kazanma amacıyla reklamlara hileli bir şekilde erişir ve cihazınızı yavaşlatmaktan çevrimiçi etkinliğinizi ve kişisel bilgilerinizi izlemeye kadar çeşitli sorunlara neden olabilir.

Reklam dolandırıcılığının sonuçları, HiddenAds türündeki kötü amaçlı yazılımları yükleyen kullanıcılarla sınırlı değildir. Sahte reklam gösterimleri şirketlerin ve reklamverenlerin paralarını boşa harcamalarına neden olduğundan işlevlerini finanse etmek için reklamlara bağımlı olan tüm uygulama ekosistemi bu durumdan etkilenir.

3 FakeApp (Sahte Uygulama)

Sahte Uygulamalar aslında sahip olmadıkları bir işleve sahipmiş gibi davranan kötü amaçlı uygulamalardır. Bu uygulamalar indirildikten sonra reklam yazılımı yayar veya kötü amaçlı davranışlar sergiler.

Bu rapordaki "Güvenilen Uygulamalar" makalesinde yapay zeka ve ChatGPT'nin son zamanlardaki yükselişiyle bağlantılı bu tür bir kötü amaçlı yazılım örneğinden bahsetmiştik. Pek çok kötü amaçlı Sahte Uygulama, kullanıcıların bunları indirmesini sağlamak için ChatGPT ile aynı yaratıcı yapay zekadan faydalandığını iddia ediyor ancak aslında bunların basit fotoğraf filtreleri olduğu ortaya çıkıyor.

4 HiddenApp (Gizli Uygulama)

Gizli Uygulamalar genellikle kullanıcının bilgisi olmadan sistemde kalmak için kurulumdan sonra simgelerini gizler. Bazı Gizli Uygulamalar, arka planda kötü amaçlı etkinlik gerçekleştirirken kullanıcının tespit etmemesi için görünmez veya zararsız görünen bir simgeye sahiptir. Kullanıcılar bunun bir sistem yardımcı programı, yazılım güncellemesi veya normalde çalışması gereken bir şey olduğunu düşünebilir veya hiç fark etmeyebilir.

Bu nedenle uygulamaları Google Play veya Apple Store gibi resmi uygulama mağazalarından indirmeniz çok önemlidir. Kişisel bilgilerinizi paylaşıyorsanız erişmek istediğiniz hizmetin resmi web sitesindeki uygulama bağlantısına tıklamanız en iyi seçenektir.

5 MoqHao

MoqHao, başlangıçta Asya ve Avrupa'da SMS ile kimlik avı yoluyla dağıtılan ve sunucu tarafında çok biçimli olan bir banka truva atıdır. "Bu kelimelerin hepsini biliyorum ama anlatılmak isteneni anlamıyorum" diye düşünüyorsanız yalnız değilsiniz. Bu ifadeyi parçalara ayırarak inceleyelim:

Sunucu tarafında çok biçimli kötü amaçlı yazılım, zaman içinde "mutasyona uğrayacak" veya değişecek şekilde programlanan ancak yine de temeldeki kötü amacı koruyan yazılımdır. Bu değişiklikler değişmeyen kodu veya "imzayı" temel alan geleneksel güvenlik önlemlerinin tespit edilmesini zorlaştırır. MoqHao, kötü amaçlı yazılımı barındıran sunucudan indirme sırasında meydana gelen mutasyonlar nedeniyle sunucu tarafında çok biçimlidir.

Banka Truva Atı, finans kurumunuzla ilgili olabilecek meşru bir dizi kullanışlı özelliğe sahipmiş gibi görünen program veya uygulamadır. Gerçekte amacı banka giriş bilgilerinizi çalmak veya finansal bilgilerinize erişim elde etmek olan kötü amaçlı bir "faydalı yük" içerir.

Yani MoqHao için "sunucu tarafında çok biçimli olan bir banka truva atı" ifadesi kulağa mantıklı geliyor mu? Bir banka soyguncusunu üzerindeki kıyafetlere göre yakalamaya çalıştığınızı düşünün. Polis, mavi takım elbiseli ve kravatlı bir zanlının peşine düşmüş olabilir ancak zanlı binadan ayrılmadan önce üstünü değiştirip dışarıda tişört ve kot pantolonla dolaşıyorsa tutuklanmaktan kurtulmuş olur. MoqHao da giriş bilgilerinizi veya banka bilgilerinizi çalar ve "kılık değiştirerek" güvenlik çözümlerinden kaçmaya çalışır.

Syringe (Şırınga)

Şırınga ailesindeki kötü amaçlı yazılımlar, Android sistemlerinde çalışan işlemlere kötü amaçlı kod ekler. Hedefi para olan bu yazılımlar genellikle yeniden paketlenen ve üçüncü taraf mağazalarda (ana uygulama mağazalarında değil) dağıtılan uygulamalarla birlikte gelir ve amacı hassas bilgileri çalmak veya başka kötü amaçlı yazılımlar yüklemektir.

İşlemlere kod eklemek, saldırganların kötü amaçlı talimatlarını doğrudan başaramayacakları görevleri gerçekleştirebilen diğer programlara (genellikle sistem hizmetleri) iletmesine olanak tanıyan bir yöntemdir. Android, işleme kod eklemek için standart bir yöntem sunmadığından geçerli tek yöntem telefona yönetici düzeyinde erişim elde etmek veya diğer güvenlik açıklarından yararlanmaktır.

İşleme kod ekleyen yazılımların, kasaya erişimi olan bir banka çalışanına "bankayı soy" emrini veren suçlular olduğunu hayal edebilirsiniz.

Banker (Bankacı)

Bu kötü amaçlı yazılım ailesi, kimlik bilgilerinizi veya kişisel bilgilerinizi çalmayı hedefleyen banka truva atıdır.

Mobil bankacılık truva atları her geçen gün gelişiyor ve paranızı çalma konusunda daha yetenekli hale geliyor. Android'in yeni sürümlerinin bu kötü amaçlı yazılımın becerilerini sınırlamak için uygulamaya koyduğu güvenlik politikalarını ve sınırlamaları, özellikle de ek katman saldırılarını (aşağıda bu konuda daha fazla bilgi verilmiştir) ve telefonunuzdaki Erişilebilirlik hizmetlerini kötüye kullanma engellerini aşmak için sürekli kendini yeniliyor.

Banka Truva Atları tarafından geniş çapta kötüye kullanıldığı için Google Play, Erişilebilirlik gibi güçlü izinlere erişebilecek uygulamalara kısıtlama getirdi. Bu nedenle Google Play'de banka Truva Atı yazılımlarına ender rastlanır. Genellikle SMS ile kimlik avı yöntemiyle veya kimlik avı yapan bankacılık siteleri gibi kötü amaçlı üçüncü taraf kaynaklarla dağıtılır.

Ek katman saldırısı, kötü amaçlı uygulamalar tarafından kullanılan ve banka uygulamanızda oturum açarken yazdıklarınızı takip edebilen veya bildirimde bulunmaksızın gerçek olanın üzerine kötü amaçlı uygulama yerleştiren görünmez öğe katmanlarından oluşan bir tekniktir.

Erişilebilirlik hizmetleri görme, motor beceri veya işitme gibi engelleri olan kullanıcılara yardımcı olmak için tasarlanmıştır. Bu nedenle erişilebilirlik hizmetleri kullanıcı arayüzünü kontrol edebilir ve ekran eylemlerini simüle edebilir. Bu beceriler, güvenlik önlemlerini atlayıp ikinci kimlik doğrulama faktörlerini, oturum açma kimlik bilgilerini ve hassas verileri çalarak banka hesabınızı boşaltmak için kullanılabilir.

Bu kötüye kullanımı önlemek için bu güçlü Erişilebilirlik erişim izinlerine yalnızca kesinlikle ihtiyaç duyan uygulamaların erişmesine izin vermek önemlidir.

8 SpyAgent

SpyAgent bir kullanıcının konumu, kişileri, mesajları veya kişisel verileri hakkında bilgi toplayan ve bunları cihaz kullanıcısının bilgisi olmadan üçüncü taraflara aktaran kötü amaçlı yazılımlardır. Bu üçüncü taraflar, bu bilgileri kendi çıkarları için kullanan bilgisayar korsanlarını, takipçileri veya dolandırıcıları kapsar. Casus yazılımlar, adından da anlaşılabileceği gibi casusluk yapan yazılımlardır.

Kötüye kullanmak isteyen saldırganların faydalanabileceği çok miktarda hassas kullanıcı verisini toplama girişiminde bulunan yaygın görülen casus yazılımlar vardır. (Bu kişisel bilgileri tutan sunucular güvenli değildir ve birçoğuna yapılan saldırıların sonucunda veriler sızdırılmıştır.) Bununla birlikte bu tür kötü amaçlı yazılımların en yaygın kullanım alanı hedefli saldırılar ve bir kişiyi gözetlemek için ticari casus yazılım yazılımlarının kullanılmasını kapsayan takip yazılımı (SpyAgent ailesinde bulunan bir tür kötü amaçlı yazılım) kullanımıdır.

9 Clicker (Tıklayıcı)

Tıklayıcı, hemen fark etmeyebileceğiniz ve hatta kendinizi kurbanı olarak göremeyeceğiniz ailelerden biridir. Bu örnekte farkında olmadan suç ortağı olmuş olursunuz.

2022'de tıklayıcı kötü amaçlı yazılımı çoğunlukla el feneri ve görev yöneticileri gibi sistem araçları gibi görünen uygulamalarla dağıtıldı ancak bu kategorilerle sınırlı değildi. Dolandırıcılar, genellikle üçüncü taraf mağazalarda (ana uygulama mağazalarında değil) bulunan bu kötü amaçlı yazılımı bazen Google Play'e eklemeyi de başardı.

Tıklayıcı kötü amaçlı yazılımı yüklendikten sonra arka planda çalışır ve saldırgan için gelir sağlayan reklamlara (gizli reklamlar, açılır pencereler, videolar) veya bağlantılara tekrar tekrar tıklar. Bu süreçte cihazın sahibi telefonun işleyişinde veya pil ömründe yalnızca küçük bir değişiklik fark edebilirsiniz.

10 FaceStealer (Face Hırsızı)

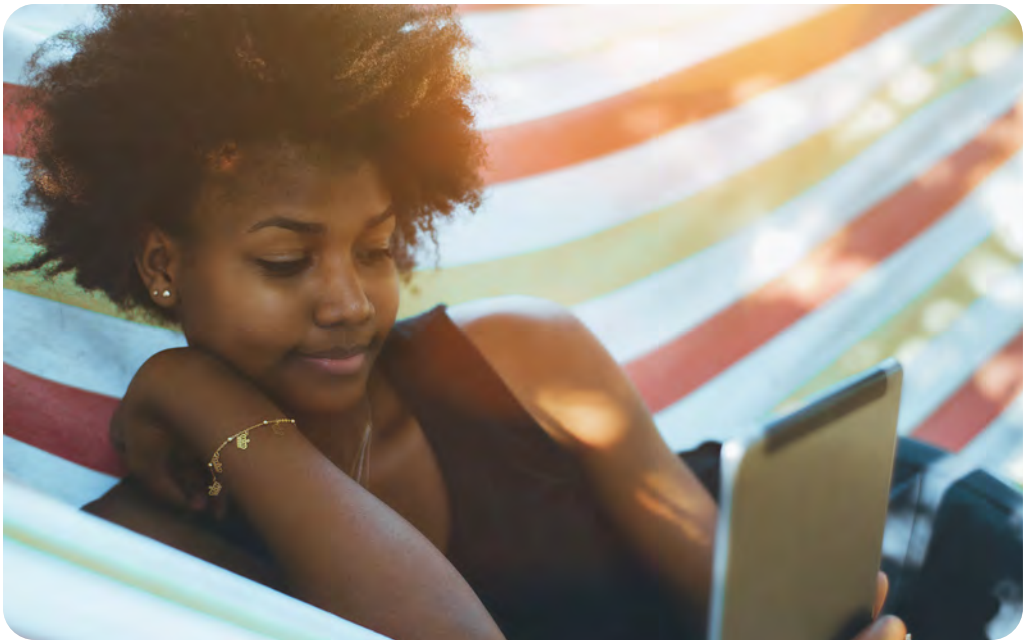
Sosyal medya hesabı ele geçirilip "Kripto paralara yatırım yaparak nasıl zengin oldum?" diye paylaşım yapan arkadaşınız var mı? Belki de arkadaşınıza Facebook, Instagram ve WhatsApp Meta platformlarını hedef alarak sosyal medya hesaplarını çalabilen bir tür kötü amaçlı yazılım olan Face Hırsızı bulaşmıştır. Hesaplar ele geçirildiğinde sizin gibi davranarak kişilerinizden para istemek, başka hesapları takip etmek ve (kötü) reklam kampanyalarını yaymak gibi diğer dolandırıcılık türleri için kullanılabilir.

2022'de Face Hırsızını bir "Mod" uygulaması olarak dağıtan ve Instagram hesaplarını çalan iki kampanyayla ilgili bir blog gönderisi yayınladık. McAfee, dünya genelinde 110.000'den fazla cihazı etkileyen yaklaşık 20.000 benzersiz Face Hırsızı örneği (veya sürümü) tespit etti.

Kendimi ve ailemi nasıl koruyabilirim?

Burada birçok farklı kötü amaçlı yazılım türüne yer verdik ancak güvende kalma tavsiyelerimiz çoğu için geçerli. Sonuçta ilk ve en iyi savunma hattı SİZSİNİZ ve her zaman durumlara makul ölçüde şüpheyle yaklaşmanız gerekiyor. Bir uygulama veya web sitesi kimlik bilgilerinizi veya farklı bilgilerinizi istediğinde aşağıdaki ipuçlarını gözden geçirmeniz yeterlidir. Uygulamaları ne kadar çok inceler ve ne kadar çok soru sorarsanız süreç o kadar kolaylaşır:

- **Her adımı sorgulayın.** Bu göndereni tanıyor muyum? Bu mesajı veya bağlantıyı bekliyor muydum? Bu kişi normalde para veya bilgi vereceğim biri mi?
- **Bu kim?** Kaç kez kim olduğunuzu biliyormuş gibi görünen bilinmeyen bir numaradan mesaj aldınız? Peki bu bilinmeyen numara şirketinizin CEO'su gibi davranıyorsa ne yapmanız gerekir? Sosyal mühendislik taktiklerinin farkında olun ve hattın diğer ucunda kimin olduğunu sormaktan çekinmeyin. En kötü ne olabilir? Karşıdaki gerçekten CEO'dur ve konuya özenli yaklaşımınızı takdir eder.
- **Bu istek gerçek mi?** Bir saniyenizi ayırın ve kendinize talebin mantıklı olup olmadığını sorun. İçgüdülerinizi hafife almayın. Ayrıca kişisel bilgilerinizi isteyen çoğu kuruluşun düzenlemelere tabi olduğunu, resmi sitesinin yanı sıra telefonla ulaşabileceğiniz gerçek bir yetkilisinin bulunduğunu unutmayın. Örneğin bankanız HİÇBİR ZAMAN size ulaşıp kullanıcı adınızı ve şifrenizi istemez.
- **Dolandırıcılığa karşı bağışıklık geliştirin!** Her an karşınıza çıkabilecek dolandırıcılıkların farkında olun. Bunları nasıl tespit edeceğinizi, bunlardan nasıl kaçınacağınızı ve hem yeni ortaya çıkan hem de kendini geliştiren dolandırıcılık vektörlerini nasıl anlayabileceğinizi öğrenin.
- **Hangi izinleri verdiğinize dikkat edin!** Bazı izinler (mesajlar ve konum gibi) telefonunuzda tek bir yerden yönetilebilir. Ancak uygulamalara ayrı ayrı bakıp hangi bilgileri izlediklerini ve sizi GERÇEKTEN bu kadar yakından izlemeleri gerekip gerekmediğini değerlendirmek çok iyi bir fikirdir.
- **Acele etmeyin!** Bu, verebileceğimiz en önemli tavsiyedir. Saldırganlar bu aciliyet duygusuna hitap etmeye çalışır ve bu sayede karar mekanizmanızın sağlıklı çalışmasını engellemeyi hedefler. Durun, değerlendirme yapın ve yukarıdaki adımları uygulayın.



2023 Tehdit tahminleri

2023 Tehdit tahminleri

Gelecekte bizi neler bekliyor? Bunu kimse kesin olarak bilemez ama McAfee'nin Mobil Araştırma Ekibi bazı mantıklı tahminlerde bulundu.

2022'nin sonunda önceden yapay zekanın daha iyi anlaşılmasını ve yüksek bütçeler ayrılmasını gerektiren teknolojilere erişimle ilgili bazı etkileyici gelişmeler kaydedildi. OpenAI'nin ChatGPT yapay zeka sohbet botu ve DALL-E 2 yapay zeka destekli görüntü oluşturucu gibi uygulamalar sayesinde artık internete erişimi olan herkes yapay zekanın gücünden yararlanabiliyor. Bu heyecan verici bir teknolojik gelişme olsa da tehdit ortamını da değiştiriyor. Bu gelişmeler küresel ekonomik belirsizlikle bir araya geldiğinde dolandırıcılar için hedef bolluğu açısından verimli bir ortam yaratıyor.

Aşağıda araştırma ekibimizin 2023 yılına dair ilgili tahminlerinin yanı sıra kendinizi ve ailenizi korumak için faydalanabileceğiniz bazı yöntemlere yer verilmiştir.

Yeni uygulamalar tehdit ortamını değiştirecek

Bu yapay zeka destekli yeni uygulamaların doğrudan etkilerinden biri geleneksel kimlik avı girişimlerini tespit etmeyi zorlaştırmasıdır. Geleneksel kimlik avı kampanyalarının (birden çok kurban toplamak için geniş bir ağa yayılan kampanyaların) ayırt edici özelliklerinden biri basit yazım ve dil bilgisi hatalarıydı. ChatGPT'nin kullanıma sunulmasıyla bu kimlik avı e-postalarını yazan kişilerin doğru dil bilgisi ve yazım konusunda endişelenmesine gerek kalmadı. ChatGPT sizin için kolayca dil bilgisi açısından doğru bir e-posta yazabilir. Kötü aktörlerin tek yapması gereken istedikleri mesajı yazmak, çevirisini yaptırmak ve programın mesajı oluşturmasını beklemektir.

Yalan haberler ve deepfake (derin sahte) videolar

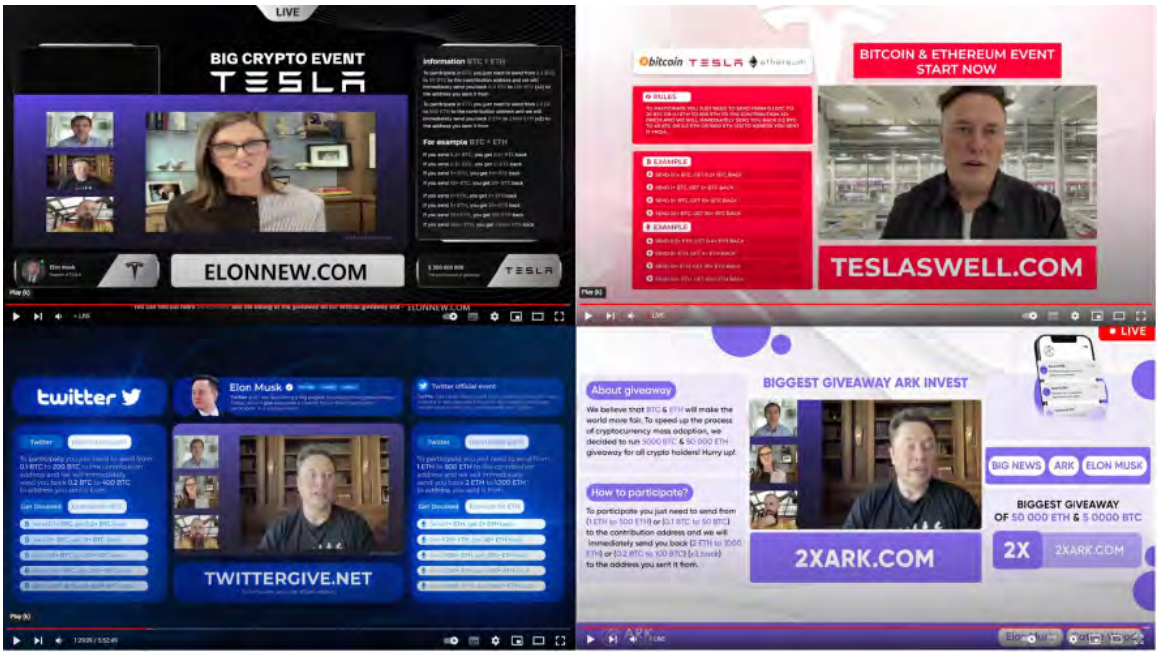
Yalan haberler ve sahte görüntüler, seçimler söz konusu olduğunda hem devletlerin hem de siber güvenlik çevrelerinin endişe kaynağı olmuştur. Montaj fotoğraflar ve yalan haberler, propaganda tekniklerinin yaygın olarak kullanıldığı uluslarda standart bir uygulama olmuştur.

Günümüzde sahte görüntüler ve videolar üretmek için derin öğrenme adı verilen yapay zeka biçimini kullanan ve derin sahte olarak adlandırılan içerikler mevcut. ChatGPT gibi bunu daha kolay hale getiren ve bazı alanlardaki siber güvenlik endişelerini artıran uygulamalar kullanıma sunuluyor. Örneğin, DALL-E 2 (metin istemlerine dayalı olarak görüntüler oluşturan bir yapay zeka sistemi) gibi gelişen teknolojiler, kripto para dolandırıcılıklarını daha inandırıcı kılmak için kullanılabilir. Örneğin paranızı ikiye katlayan kripto para dolandırıcılığında yem olarak eski bir Elon Musk videosu kullanıldı. Bu tür dolandırıcılık tekniklerinin 2023 yılında daha da gelişmesini ve kurbanları kandırıp bin bir güçlükle kazandıkları paraları ellerinden almak için derin sahte videolardan ve seslerden faydalanılacağını öngörüyoruz.

Yatırım dolandırıcılıkları

2023 birçok insan için finansal açıdan belirsizliğini koruyor. Böyle zamanlarda insanlar genellikle fazladan para kazanmanın yollarını ararlar ve bu nedenle çok az yatırımla büyük finansal kazançlar vadeden sosyal medya mesajlarına ve çevrimiçi reklamlara karşı savunmasız kalabilirler.

FBI İnternet Suçları Şikayet Merkezi'nin 2021 raporuna göre yatırım dolandırıcılığı kaynaklı kayıplar 2020 yılında 336.469.000 ABD dolarından 2021'de 1.455.943.193 ABD dolarına yükseldi. Bu veriler, bu tür dolandırıcılıkların katlanarak arttığını gösteriyor ve bu trendin devam etmesini bekliyoruz.



Şekil 6. YouTube'da derin sahte videolarla yapılan kripto para dolandırıcılığı girişimlerinin görüntüleri.

Sahte krediler

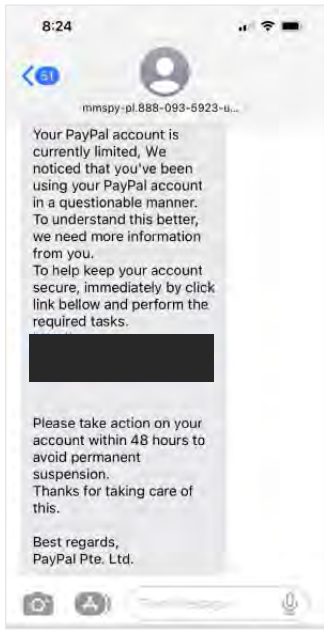
Ne yazık ki dolandırıcılar genellikle en savunmasız kişileri hedef alır. Sahte kredi dolandırıcılığı, suçluların çaresiz şekilde kredi aradıkları ve bu nedenle ön ödeme isteme gibi uyarı işaretlerine daha az tepki verdikleri bir dönemde yapılan dolandırıcılık türüdür. 2023 yılında bu tür dolandırıcılıklarda büyük bir artış olacağını tahmin ediyoruz. Kredi almak isterseniz her zaman güvenilir bir sağlayıcı kullanın ve internette gördüğünüz reklamlara tıklarken dikkat edin.

Metaverse

Facebook'un Horizon'ı gibi metaverse'ler, kullanıcılarının daha önce hayal bile edilemeyen çevrimiçi dünyaları keşfetmelerini sağlar. Bu platformların başlangıç dönemlerinde kötü amaçlı kişiler genellikle bu sistemin nasıl çalıştığına dair yeterli bilgi sahibi olmayan kişilerden faydalanmaya ve onları dolandırmaya çalışacaktır. 2022'de bu platformların kullanıcılarını hedefleyen kimlik avı kampanyaları gözlemledik ve 2023'te platformlara kaydolan kullanıcı sayısı arttıkça kimlik avı saldırılarının hacminin önemli ölçüde artmasını bekliyoruz.

Sosyal mühendislik

Telefonunuz ele geçirilebilir ancak suçluların bunun için zaman ve çaba harcaması gerekir. Sosyal mühendislik yöntemlerini kullanan yaygın bir saldırının hedefi olma olasılığınız katlanarak artıyor. Mesajlar aracılığıyla yapılan bu saldırıların sıklığı, hızı ve kolaylığı her geçen gün artıyor. Bankanızdan, PayPal'dan veya Venmo'dan geliyor gibi görünen bu mesajların amacı sizi kandırarak hesap bilgileriniz gibi kişisel verilerinizi paylaşmaya ikna etmektir.



Şekil 7. YouTube'da derin sahte videolarla yapılan kripto para dolandırıcılığı girişimlerinin görüntüleri.

Mobil cihazınızı geleceğe hazırlama

Siber suçlular tarafından kullanılan teknolojiler ve uygulamalar onlarca yıldır sürekli olarak gelişiyor. Bu raporda kendinizi ve ailenizi güvende tutmanın yöntemlerini paylaştık ve bu yöntemler gelecekteki tehditler için de geçerli olmaya devam edecek.

- Beklemediğiniz e-postalara, kısa mesajlara veya DM'lere şüpheyle yaklaşın ve bağlantılara tıklamadan önce iki kez düşünün.
- Bu dolandırıcılıkların çoğunun işe yaramasının nedeninin sahte bir aciliyet duygusu yaratmaları veya yoğun duygulardan faydalanmaları olduğunu unutmayın. Özellikle bilinmeyen veya beklenmedik bir göndericiden gelen tehdit edici veya acil mesajlarla etkileşime geçmeden önce durup düşünün.
- Gerçek olamayacak kadar güzelse muhtemelen gerçek değildir.
- Mobil cihazınızın McAfee Security uygulaması gibi cihazınızı izleme ve olası kötü amaçlı bağlantıları ve yazılımları engelleme özelliklerine sahip olan bir yazılımla korunduğundan emin olun.

Her zaman olduğu gibi suçlular daha akıllı ve daha yaratıcı olmaya devam ederken işledikleri suçların kapsamı da her geçen gün artacak. Teknoloji kullanıcıları olarak bizler de her geçen gün daha akıllı olacağız.

1. https://www.data.ai/en/go/state-of-mobile-2023/
2. https://www.mcafee.com/blogs/family-safety/helping-kids-think-critically-about-influencers-they-follow-online/
3. https://www.mcafee.com/blogs/family-safety/tiktok-update-dangerous-viral-challenges-age-restrictions/
4. https://www.mcafee.com/content/dam/consumer/en-us/docs/reports/rp-cyberbullying-in-plain-sight-2022-global.pdf
5. https://www.mcafee.com/blogs/family-safety/getting-your-kids-ready-for-school-and-their-smartphones-too/
   https://www.mcafee.com/blogs/family-safety/does-your-child-have-an-unhealthy-relationship-with-social-media/

2023 tehdit tahminlerimiz hakkında daha fazla bilgi edinmek ister misiniz?
www.mcafee.com/blogs/security-news/mcafee-2023-threat-predictions-evolution-and-exploitation/

Telefonunuzu ve içindeki bilgileri koruyun
McAfee Security mobil uygulamasını Apple veya Google Play uygulama mağazasından telefonunuza veya tabletinize indirmek için bu QR kodu tarayın.

McAfee™

6220 America Center Drive
San Jose, CA 95002
888.847.8766
www.mcafee.com