Android Cihazda Trojan Tasarimi Ve Uygulama Güvenliği

Ezel KOÇ

June 2017

1 Giriş

Sensor Tower tarafından yayınlanan bir rapor, 2016 birinci çeyrek döneminde Google Play Store'da indirilen uygulama sayısını gözler önüne seriyor. Rapora göre birinci çeyrek döneminde (ocak-mart) Play Store 11.1 milyar uygulama indirme gerçekleşti. Geçtiğimiz yıl aynı dönemler karşılaştırıldığında uygulama indirme sayısında %6.7'lik bir artış söz konusu. Pazar araştırma kuruluşu Gartner, 2016 ikinci çeyrek dönemine ait akıllı telefon satışlarının yer verildiği raporunu yayınlandı. Toplamda 344 milyon akıllı telefonun satıldığı üç aylık dilimde Android tabanlı akıllı telefonlar pazarın büyük bölümünü oluşturuyor. Nisan-Haziran döneminde toplam 296.9 milyon Android işletim sistemine sahip akıllı telefon satışı gerçekleşti. Android'in ikinci çeyrek sonunda pazardaki kullanım oranı ise %86.2 olarak açıklandı. Geçen yıl bu oran %82.2 seviyesindeydi.

Cisco 'nun 2014 güvenlik raporuna göre, 2013 yılında yapılan mobil kötücül saldırıların %99'u Android'i hedeflemektedir. Benzer şekilde Sophos firmasının 2014 yılında hazırladığı Mobil Güvenlik Tehdit Raporu da son bir yıl içerisinde Android kötücül yazılım sayısında 6 kat artış olduğunu ortaya koymaktadır. Android tabanlı kötücül yazılımlar[5], kullanıcıların kişisel bilgilerini toplamak (grayware) ve yetkisiz işlem yapmak (malware) gibi kötücül hedeflere sahiptir. Play Store'daki kötücül yazılım oranı yapılan çalışmalara göre son yıllarda ciddi bir artış göstermektedir. Bu artışın başlıca sebepleri olarak Android'in açık kaynak kodlu yapısı ve uyguladığı pasif koruma yöntemi gösterilebilir.

Android, izin tabanlı güvenlik mekanizmasına sahiptir. İzinler, uygulamaların SMS gönderimi, yer bildirimi gibi telefonun çeşitli kaynaklarını kullanabilmesi için ihtiyaç duyduğu onaylardır. Kullanıcılar uygulamaları yüklerken app store, uygulamanın kullanıcından talep ettiği izinleri listelemektedir. Bu izinler uygulamanın sahip olacağı kabiliyetleri kullanıcıya bildirmek için kullanılmaktadır. Bu aşamadan sonra kullanıcı kendi değerlendirmesine göre yüklemeye devam edebilmekte veya yüklemeyi iptal edebilmektedir. Üstelik bu izinler, yükleme işlemi tamamlandıktan sonra kullanıcıya bir daha sunulmamaktadır. Felt[14] ve arkadaşları tarafından yapılan çalışmada kullanıcıların yalnızca %17'sinin bu izinleri dikkate aldığı ve %42'sinin ise izinler hakkında bilgisinin olmadığı ortaya çıkmıştır. Yapılan diğer çalışmalarda da Android izin bildirimlerinin kullanıcılar tarafından yok sayıldığı ortaya çıkmaktadır. Literatürde bu eksiklikleri hedef alan çeşitli Android kötücül yazılım tespit ve koruma sistemleri mevcuttur.

2 Kötü Amaçlı Yazılım

Çok fazla sayıda zararlı yazılım uygulaması[6] vardır bu nedenle, bu uygulamalara bakıp zararlı yazılım uygulmalarını dört gruba ayırıyoruz. İlk grup, kendilerinin iddia ettiği gibi casus yazılım olarak kabul edilirler ve amaçlarına göre kurbanın telefonlarına yüklenmek istemektedirler. GPSSMSSpy[13], kurbanın şimdiki konumunu kaydetmek ve yüklemek için SMS tabanlı komutları dinleyen bir örnektir.[1][2][11][8][9][4][3]

İkinci grup, doğru/meşru görünen uygulamalarla örtüşen ancak kullanıcıların kimlik bilgilerini çalmak veya arka planda SMS mesajları göndermek gibi kötü niyetli işlemleri gerçekleştiren kötü amaçlı kod içeriyor. FakeNetflix, bir kullanıcının Netflix hesabını ve parolasını çalan bir örnektir. Netflix uygulamasının yeniden paketlenmiş bir sürümü olmadığını ancak bunun yerine aynı kullanıcı arabirimine sahip Netflix uygulamasını kılık değiştirdiğini unutmayın. FakePlayer, film uygulaması olarak taklit edilen ancak reklamı yapılan işlevi hiç sunmayan başka bir örnektir. Tek yapmanız gereken, kullanıcı farkında olmadan, ücret alınacak yerlere SMS mesajları göndermektir.

Üçüncü grup, kasıtlı olarak kötü amaçlı işlevler içeriyor (örneğin, yetkisiz SMS mesajları göndermek veya bazı hizmetlere otomatik olarak abone olmak) gibi uygulamaları içeriyor. Ancak ikinci gruptan farkı, sahte olmaması bunun yerine, iddia ettiği işlevselliği sağlayabilirler. Ancak kullanıcılar tarafından bilinmeyen bazı zararlı işlevleri de vardır. Örneğin, bir RogueSPPush örneği bir astroloji uygulamasıdır. Bu uygulama otomatik olarak kullanıcı tarafına gelen SMS mesajlarını otomatik yanıtlayarak ücretli hizmetlere abone olurlar. Son grubun, iyi çalışması için root ayrıcalığına dayanan uygulamalar içeriyor. Bununla birlikte, kullanıcıdan bu uygulamalara root yetkisi vermesini istemeden, built-in security sandboxdan kaçmak için bilinen root exploitlerini ortadan kaldırır. Bu uygulamalar kötü amaçlarını açıkça görünmese de,root exploitleri kullanıcı izni olmaksızın kötü amaçlı işlevleri yerine getiriyor. Bu gruptaki örnekler arasında Asroot ve DroidDeluxe bulunmaktadır.

2.1 Kötü Amaçlı Yazılımlarda İzin Kullanımı

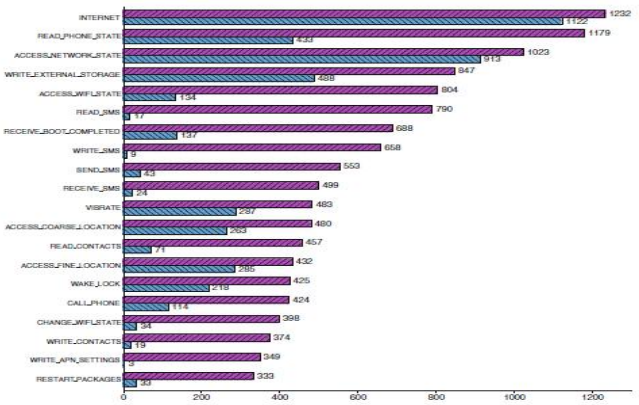


Fig. 2.4 The comparison of top 20 requested permissions by malicious apps (the *bar*) and benign apps (the *bar*)

Tehlikeli uygulamalar ve tehlikesiz uygulamaları temel alan istenen 20 izini karşılaştırma

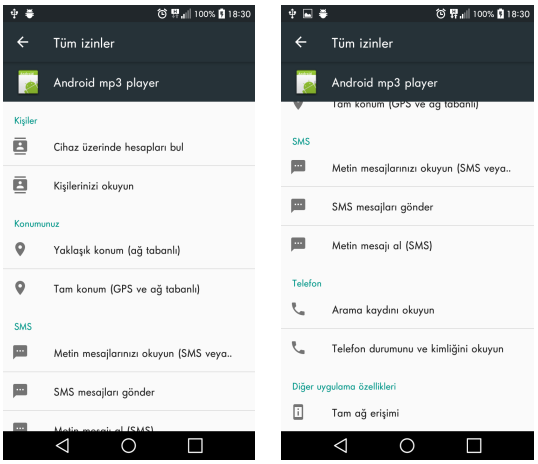
Detaylı açıklamalar içermeyen Android uygulamaları için uygulamanın yetenekleri, kullanıcıların onlara verdiği izinlerle sınırlandırılır. Bu nedenle, veri kümesindeki bu kötü amaçlı uygulamalar

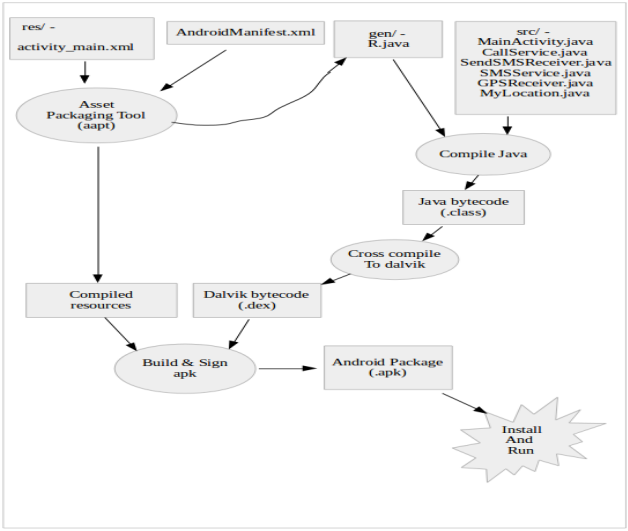
tarafından istenen izinlerin, en çok istenen izinlerle karşılaştırılması ilginç olacaktır. Bu amaçla, 2011 yılının Ekim ayının ilk haftasında resmi Android Market'ten indirilen 1260 adet en iyi ücretsiz uygulama seçilmiştir. Şekildeki karşılaştırmaya dayanarak, İNTERNET, READ_PHONE_STATE, ACCESS_NETWORK_STATE ve WRITE_EXTERNAL_STORAGE gibi Android izinleri hem tehlikeli hem de tehlikesiz uygulamalar tarafından istenir. Ancak, kötü amaçlı uygulamalar, READ_SMS, WRITE_SMS, RECEIVE_SMS ve SEND_SMS gibi SMS ile ilgili izinleri daha sık talep etme eğilimindedir. Veri setinde READ_SMS iznini isteyen 790 örnekden (%62.7), 17 tehlikesiz uygulama (%1.3) bu izni talep ediyor. Bu sonuçlar, SMS ile ilgili tehlikeli fonksiyonlara sahip olan veri grubumuzdaki 28 malware ailesinin (örneklerin %45,3'ü) gerçeği ile tutarlıdır. Ayrıca, 688 malware örneğinin RECEIVE_BOOT_COMPLETED iznini talep ettiğini gözlemliyoruz. Bu sayı, zararsız uygulamalardan beş kat daha fazla (137 örnek). Bu, malware, kullanıcının müdahalesi olmaksızın arka plan servislerini çalıştırma ihtimalinin yüksek olması gerçeğine bağlı olabilir. CHANGE_WIFI_STATE izni isteyen 398 malware örneğinin, zararsız uygulamalardan (34 örnek) daha çok istendiğini unutmayın. Bunun nedeni, Exploid root istismarının, bu izinle ilgili olan WIFI durumunun değiştirilmesi gibi bazı etkin ek olayları gerektirmesidir. Son olarak, kötü amaçlı uygulamaların iyi olanlardan daha fazla izin talep etme eğiliminde olduğunu fark ettik. Veri setinde, kötü amaçlı uygulamaların talep ettiği ortalama izin sayısı 11 iken, iyi uygulamlar tarafından istenenlerin ortalama sayısı ise 4'tür. En çok kullanılan 20 izin arasından 9'u ortalama olarak kötü niyetli uygulamalar tarafından talep edilirken aynı zamanda da ortalama 3'ü zararsız uygulamalar tarafından talep edilmektedir.

3 PROJE NE YAPIYOR?

Android'in uygulamalarının belirli izinler verildiğinde çok fazla kişisel bilgiye erişebileceğini biliyoruz. Uygulamalar, kişileri okuyabilir ve düzenleyebilir, metin ve telefon görüşmeleri gönderip alabilir, telefon numaranızı ve e-posta hesap bilgilerinizi okuyabilir, fiziksel konumunuzu izleyebilir ve çok daha fazlasını yapabilir.

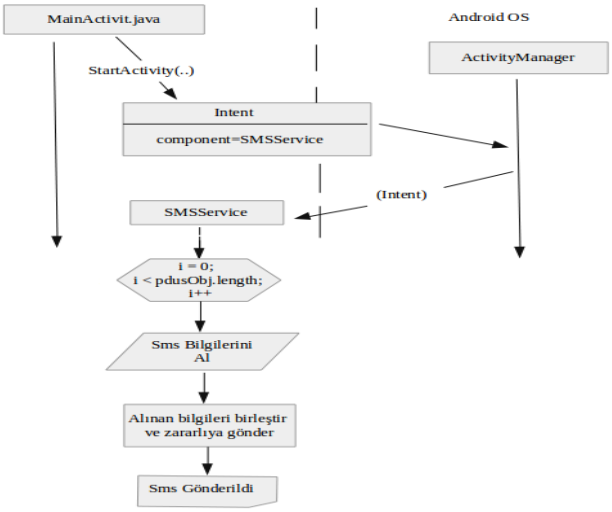
Çoğu durumda, bu izinler kullanıcıya olumlu bir hizmet sunarlar. Bununla birlikte, bu izinler sessizce kişisel bilgileri toplamak ve çok kötü niyetle hareket etmek için kolayca istismar edilebilir. Android Truva atı projesi, Android uygulamalarına yaygın olarak verilen izinlerin bazılarının kötü niyetli bir şekilde nasıl kullanılabileceğini göstermek amaçlı tasarlanmıştır. Uygulamadaki kötü amaçlı kod parçaları herhangi bir Android uygulamasına gömülebilir ve zararlı olmayan bir uygulamanın arkasında sessizce çalışır. Bu trojanın çalışma mantığını göstermek amaçlı temel düzeyde tasarlanmış bir mp3 player[1] kullanıldı ve gerekli yerlerine bu zararlı kod parçaları gömülmüştür. Kötü amaçlı kod tamamen arka planda çalışır ve kullanıcıya ulaşmaz. Mp3 player yüklenir yüklenmez trojan sahip olduğu izinlerle hedefin telefonunu dinlemeye alır ve tetiklenmeyi bekler. Bu trojan, kullanıcının telefon rehberine ve metin mesajlarına erişebilir; eriştiği her mesajı hedefe gönderir[2][10]. Uygulama yayılmak için bir sosyal mühendislik içermektedir ve gelen arama ile tetiklenir, arama sonlandıktan belli bir süre sonra o kişiye uygulamanın indirme linkini içeren bir oltalama mesaj gönderilir. Ayrıca uygulama tetiklendikten 5 dk sonra her 15 dakikada bir kullanıcının GPS bilgilerini okur ve hedefe gönderir. Uygulamanın kötü kod parçaları açılışta direk çalışmamaktadır bir tetikleme üzerine çalışmaya başlamaktadır bu sayede de antivirus programları tarafından yakalanmamaktadır. Tasarlarken düşündüğüm başka bir şey ise telefonun ısınma sorunu ve batarya sorunu olmuştur bunları da aynı şekilde optimize ettiğim için kullanıcı tarafından takibi zorlaşmıştır.



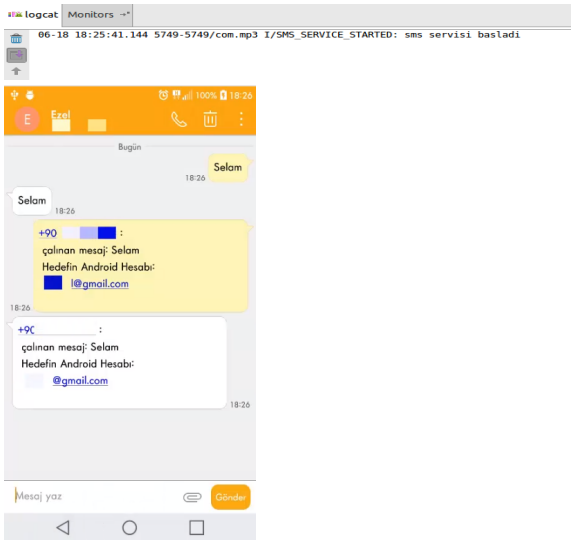


[1]https://www.hrupin.com/2010/12/simple-android-mp3-media-player
[2]https://www.tutorialspoint.com/android/android_sending_sms.htm

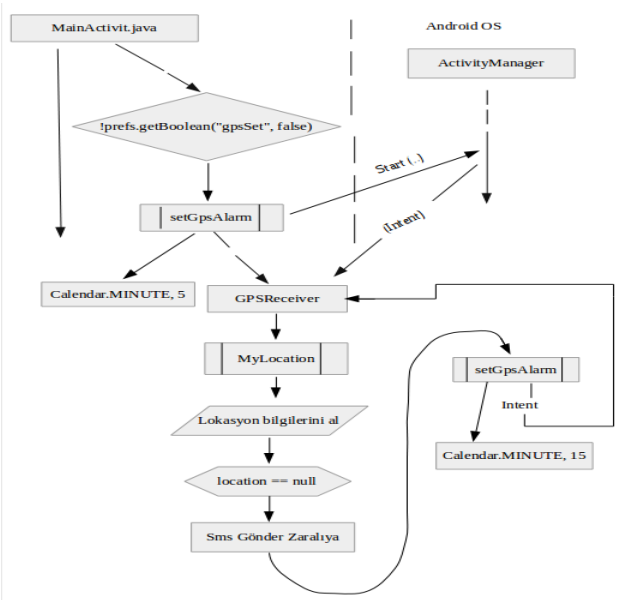
3.1 SMSService.java



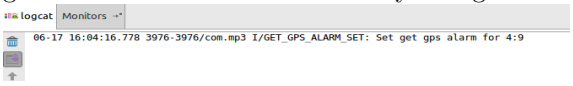
Bu java dosyası kullanıcının hiçbir şeyin farkında olmadan çalışması için bir android servisi olarak tanımlıyorum. Servis kullanmamın sebebi; taşınabilir cihazların en büyük problemi enerji. Bir akıllı telefonda çalışan bir uygulamayı aktif pencere olmaktan çıkardığınızda uygulama işleyişi duruyor (örneğin youtube'da müzik dinlerken epostalarınıza bakamazsınız). Ancak service interface'i bu engeli aşıyor, yani aktivite view'ı arka plana atılsa da çalışmaya devam ediyor. Bu servisin tetiklenmesi için mainActivity içinde bir intent tanımlıyorum. Servisin içinde tanımladığım kodları açıklamak gerekirse bir BroadcastReceiver'ı programatik olarak tanımladım. BroadcastReceiver'ın onReceive metodunda da receiver'ın aldığı intent içinde bulunan verilerin SMS alınmasıyla mesaj nesnesini ve bu nesne içinde bulunan gönderenin telefon numarası bilgisini alıyoruz. Son olarak sızdıracağımız bilgiyi mesajı gönderen telefon numarası ve mesaj içeriğini birleştirerek oluşturuyoruz ayrıca zararlıya sahip kullanıcının google hesap bilgisini de bu mesaj yardımıyla alıyorum ve SMS mesajını hardcoded olararak yazdığımız telefon numarasına gönderiyoruz. Çalışması aşağıda gösterilmiştir.[7][12]

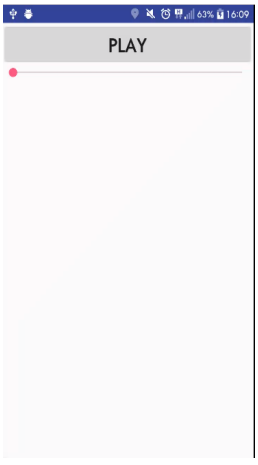


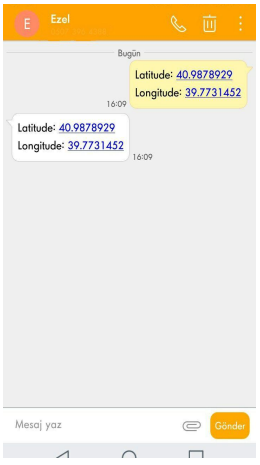
3.2 GPSReceiver.java

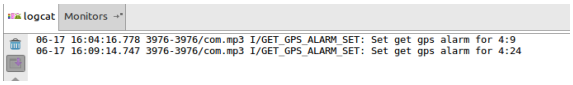


Bu java dosyasının tetiklenmesi için ilk önce mainActivty içine bir alarm ayarlıyorum bu alarm ile 5 dakika içinde konum bilgisini alıyoruz bu şekilde sürekli kendini tetikleyerek çalışabilecek. Java dosyamının içinde tanımladım kodlara gelirsem işletim sisteminden gelen sinyalleri dinlemek için BroadcastReceiver özelliği ekliyorum. BroadcastReceiver'ın onReceive metodunda da ilk önce java2s[3] sayfasından aldığım hazır MyLocation.java dosyamı çağırıyorum bu java dosyası hedefin lokasyon bilgisini çıkartıyor ve bir while döngüsü ile kullanıcı bulunana kadar veya zaman aşımına uğradıcınya kadar döngüde kalıyor ve daha sonra alınan enlem ve boylam bilgisini zararlı kullanıcıya gönderiyor ardından tanımladığım alarm ile 15 dk sonrasına tetiklenmek üzere ayarlanıyor. Logchat görüntülerinde bu saatler detaylıca gösterilmiştir.

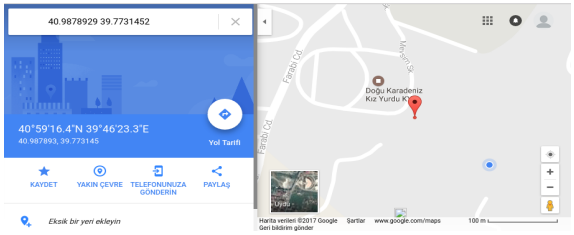


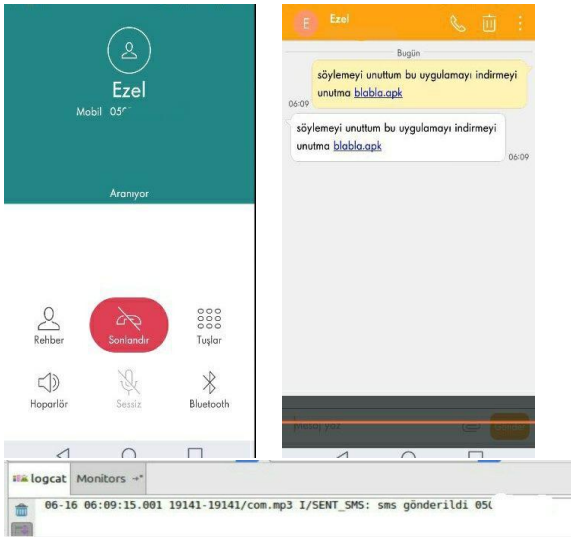




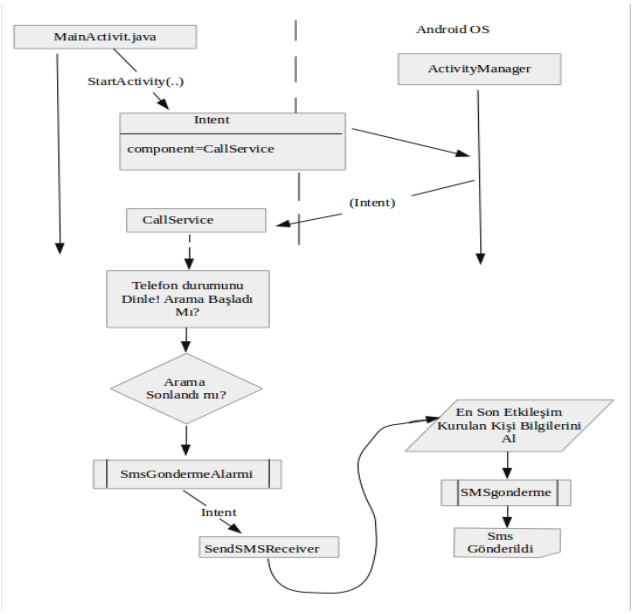


[3]http://www.javased.com/index.php?source$_dir = Cura/src/com/cura/security/MyLocation.java$

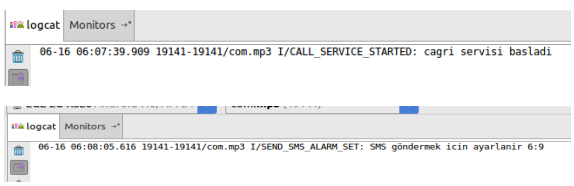




3.3 CallService.java



Bu java dosyası önceden bahsettiğim sebeplerden dolayı arka plan servisi olarak oluşturulmuştur. Bu servis kötü amaçlı kodu yaymak için tasarlanmıştır. Hiçbir şeyden habersiz kullanıcının telefon konuşması bittikten sonra çalışacak ve android cihazadaki en son etkileşim kurulan kişinin kullanıcı bilgisi alınıp 1dk içinde ona bir sosyal mühendislik saldırıcı içeren bir mesaj gönderecektir. MainActivity içinde bu servisin tetiklenmesi için bir intent oluşturulmuştur. Java dosyasında ise telefonu dinlemeye alarak arama durumunu dinlemektedir arama sona erdiğinde ise SmsGondermeAlarmi fonksiyonununu çağırarak hem 1 dk içinde sms göndermek için ayarlanacak hem sms gönderecek SendSMSReceiver.java dosyasını çağıracaktır. SendSMSReceiver.java dosyası SMSService.java dosyasına benzer yapıdadır ve sosyal mühendislik saldırısı gerçekleştirecek mesaj tanımlı olup en son konuşma yapılan kişinin telefon bilgilerini alan bir dosyadır. Logchat görüntülerinde çalışması detaylı gösterilmiştir.



3.4 AndroidManifest.xml

Bu proje ait daha net görülmesi için zararlı kod eklemeden önceki manifest dosyası ve zararlı eklendiken sonra oluşan zararlı dosyası gösterilecektir.

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="com.mp3">
    <application
        android:allowBackup="true"
        android:icon="@drawable/icon"
        android:label="Android mp3 player"
        android:supportsRtl="true"
        android:theme="@style/AppTheme">
        <activity android:name=".MainActivity">
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />

                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
    </application>

</manifest>
```

Orjinal manifest dosyası

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest xmlns:android="http://schemas.android.com/apk/res/android"
    package="com.mp3">

    <uses-permission android:name="android.permission.INTERNET" />
    <uses-permission android:name="android.permission.GET_ACCOUNTS" />
    <uses-permission android:name="android.permission.READ_CALL_LOG" />
    <uses-permission android:name="android.permission.READ_PHONE_STATE" />
    <uses-permission android:name="android.permission.READ_CONTACTS" />
    <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />
    <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
    <uses-permission android:name="android.permission.READ_SMS" />
    <uses-permission android:name="android.permission.SEND_SMS" />
    <uses-permission android:name="android.permission.RECEIVE_SMS" />

    <application
        android:allowBackup="true"
        android:icon="@drawable/icon"
        android:label="Android mp3 player"
        android:supportsRtl="true"
        android:theme="@style/AppTheme">
        <activity android:name=".MainActivity">
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />

                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
        <receiver android:name=".GPSReceiver"/>
        <receiver android:name=".SendSMSReceiver" />

        <service
            android:name=".CallService"
            android:label="Call Service" />
        <service
            android:name=".SMSService"
            android:enabled="true"
            android:exported="true" />
    </application>

</manifest>
```

Riskli izinler barındıran manifest dosyası

4 Alınacak Önlemler

Saldırıya uğramış android telefonun belirtileri:

- Cihazınız yeni ise ve garip bir şekilde davranıyorsa, tehlikede demektir. Örneğin,

bazı uygulamalar kendi izniyle açılıp kapanabilir veya kullanıcı izni olmaksızın metin mesajları gönderebilir vs. bunlar saldırıya uğramış android cihazı işaret eder.

- Telefonunuzun hızı çok yavaşsa ve otomatik olarak yeniden başlatılıyorsa, içinde bir malware olduğunu söylenebilir. Bu durumda, kötü niyetli kişi telefon sistem dosyalarını değiştirmeye çalıştığı düşünülebilir. Telefonun bataryası her zamankinden çok hızlı bitiyorsa, telefonda malware bulunma ihtimali var demektir. Çünkü o zararlı kod arkada casus olarak çalışır ve telefonun pilini çok çabuk tüketir. Ancak bazen, telefonun pil değiştirilmesi de gerekebilir.

- Yapmadığınız aramalar, hiç göndermediğiniz metinlerde veya uzun bir telefon faturası alıyorsanız, telefonunuzda kötü amaçlı yazılım bulunma olasılığı vardır. Aynı şey hiç gerçekleştirmediğiniz banka işlemleri için de geçerlidir. Her ikisi de mobil verilerinizin bazı zamanlarda veya başka bir noktada tehlikeye atıldığının işaretleridir.

Telefonunuzu nasıl güvende tutabilirsiniz:[4]

- Üçüncü taraf uygulama mağazalarına erişimin kıstlandığından emin olun; Android cihazınıza her zaman Google Play Store'dan uygulamaları indirin/yükleyin. Diğer tüm üçüncü taraf uygulama mağazalarından asla uygulama yüklemeyin. Ayrıca, android platformuyla uyumlu uygulama sağlayan bazı kötü niyetli web siteleri de bulunmaktadır. Bu tip web siteleri arka kapının ev sahasindadir. Kullanıcılar bu sitelerin indirme linkine tıkladığında, otomatik olarak kötü amaçla çalışan bir kod çalıştırılır ve telefonun donanımında otomatik olarak saklanır. Bunlar güvenilmez kaynaklardır. Kullanıcı ayrıca Google Play'deki tüm satın alma işlemlerini yapmak için ayrı bir PIN de ayarlayabilir. Bu, yetkisiz satın alımları durdurmak için faydalı bir adımdır.

- Telefonunuzu/uygulamalarınızı düzenli olarak güncelleyin; Eski mobil işletim sistemlerinin yazılımı, kilit döngülerden biridir. Akıllı telefonunuzu güncelleyerek, bilgisayar korsanlarına ve kötü amaçlı yazılımlara karşı kullanıcının tehlike riskini otomatik olarak azaltacaktır. Dolayısıyla, kullanıcı telefonda herhangi bir güncelleme bildirimi gördüyse hemen güncellemesi gerekir.

- Veri şifreleme; Verileri korumak için cihazınızdaki şifreleme ayarlarını kullanın. Kullanıcının Google hesaplarını, uygulama verilerini ve indirme bilgilerini korur. Kullanıcı şu adımları kullanarak etkinleştirebilir: Ayarlama / Güvenlik / Şifrelemeyi etkinleştir.

- Otomatik tamamlama özelliğine kapatın; Kullanıcı android akıllı telefonda otomatik tamamlama özelliğini kapatması gerekiyor. Kullanıcılar için her seferinde verileri yazmak can sıkıcı olsa da, bunun bilgiyi bilgisayar korsanlarından koruyacak en iyi seçenek olduğunu anlamamız gerekir. Hassas bilgileri her seferinde elle doldurun. Benzer şekilde, bir dizi uygulama ve web sitesi için kullanılabilen 'şifreyi göster' özelliğini kullanmaktan da kaçının.

- Telefonlarınızı genel şarj noktalarında şarj etmeyin; Cep telefonlarının düzenli kullanılması bataryayı boşaltır. Bu nedenle, bazen kullanıcı, kiosks, özellikle de hareket halindeyken cep telefonunu şarj ediyor. Burada kullanıcı, kendisine bağlı güç kaynağı kablolarıyla birlikte bir shoebox boyutunda sahte şarj noktalarının olduğunu anlamalıdır. Bunlar telefonunuza erişebilmek için Juice jacking tarafından yerleştirilir.

- Bluetooth'u kapatın; Bluetooth'u kullandıktan sonra lütfen kapatın. Açılırsa, bilgisayar korsanları, cihazınıza erişmek için korumasız Bluetooth şebekeleri kullanabilirler. Başka bir cihazla eşleştirmek isterseniz şifre kodunu kullanın. Telefon kullanıcısının güvenliği için herhangi bir cihazın telefonuyla otomatik olarak eşleştirmesine izin verilmemelidir. Bu, veri hırsızlığına ve kötü amaçlı kod aktarmaya neden olabilir.

- Şifrelerinizi bir uygulamada saklamayın; Kullanıcıların şifrelerini depolamak için kullandığı bazı uygulamalar vardır. Bu uygulamalar, kullanıcının uygulama şifrelerini, e-posta hesaplarını, Sosyal Medya hesaplarını ve hatta kredi kartı veya mobil/net bankacılık gibi farklı kategorilerde şifreleri depolamasına izin verir. Bu tür uygulamaların geliştiricilerine nasıl güvenebilirsiniz? Uygulama kaliteli olmasına ve çeşitli güvenlik özellikleri ve işlevleri ile birlikte olsa da, günün sonunda değiştirilebilen bir yazılımdır.

- public/free Wi-Fi'ye bağlanmayın; Ücretsiz Wi-Fi kesinlikle teknolojinin bize verdiği avantajlardan biridir. Ancak ücretsiz Wi-Fi bağlantısını kullanmadan önce iki kez düşünün. Güvenli olmayan Wi-Fi şebekesi üzerinden kişisel verilerinizi gönderiyorsanız, bu sizin için tehlikelidir. Bu android telefonunuzun bilgisayar korsanlarına karşı şimdiye kadar olduğundan daha tehlikeli olmasını sağlayabilir. Bağlanmadan önce tarama geçmişinizi silin: Önbellek geçmişi ve kayıtlı şifreler gibi göz atma geçmişinizi silmeniz gereklidir. Sanal ayak izinizi kaldırmak, özel bilgilerinizin gizli kalmasına ve bilgisayar korsanından uzakta olmanıza yardımcı olur. Telefonunuzda geçici dosya varsa bunları kaldırın. Bunu düzenli olarak yapabilirsiniz.

[4] https://www.cyberintelligence.in/tips-for-a-safe-android-phone/

- Browse safely(Detaylı göz at); Kullanıcılar İnternet'te hiçbir şeyin güvenli olmadığını anlamalıdır. Kullanıcılar internet kullandıklarında bir takım hatalar yapar. Bazen acele eden bir kullanıcı aceleyle farkında olmadan bazı bağlantılara tıklar. Bu, bilginiz olmadan Truva atlarını, casus yazılımları cihazınıza indirmeye neden olabilir.

5 Sonuçlar

Android OS için bu Truva Atının oluşturulmasından, Android'de çalışan uygulamaların çok sayıda kişisel veriye erişebildiğini ve bu erişimi de kolaylıkla kötü niyetli bir şekilde kullanabileceği sonucunu çıkarabiliriz. Bu uygulamayla, kullanıcının sms mesajlarını, e-posta bilgisini ve GPS konumunu, arka planda sessizce çalışarak, kullanıcıdan habersiz bir şekilde bu verileri toplayabilir. Ayrıca kötü niyetli bu uygulamayla sosyal mühendislik ilkelerini kullanarak, sms yoluyla yaymanın ne kadar basit olduğunu gördüm. Truva Atının kullanıcıdan bağımsız, kötü amaçlı olmayan herhangi bir uygulamaya gömülebilmesi, hızlı yazılması ve sosyal mühendisliği mümkün kılan bilgilere erişim yeteneği nedeniyle son derece tehlikelidir. Android kullanıcılarının bu tür Truva Atlarından kendilerini korumalarının tek yolu, yeni uygulamalar yüklerken her zaman uygulama izinlerini okumak ve yalnızca güvenilir kaynaklardan uygulamalar yüklemektir. Bir şey size garip veya şüpheli geliyorsa o uygulamayı kurmaktan kaçınmalısınız.

References

[1] İbrahim Alper DOĞRU Anıl UTKU. Mobil kötücül yazılımlar ve güvenlik Çözümleri Üzerine bir İnceleme. http://dergipark.gov.tr/download/article-file/229776, 2016.

[2] Joany Boutet. Malicious android applications: Risks and exploitation. https://www.sans.org/reading-room/whitepapers/threats/malicious-android-applications-risks-exploitation-33578, 2010.

[3] Ken Dunham. Mobile malware attacks and defense. http://libgen.io/book/index.php?md5=2691EB95040FEECC1AAC4FC22E979A2F, 2010.

[4] Ken Dunham. Android malware and analysis. http://libgen.io/book/index.php?md5=2AECCA3C7D9950C6DABB900D6FFC412D, 2014.

[5] Bakır Emre. Turk finans sektorunu hedef alan mobil zararlı yazılım: Mobil sube. https://github.com/bemre/mobil_sube.apk, Haziran 2015.

[6] Bakır Emre. slempo android bot-bankalarbirligi sahte flash player zararlı yazılım analizi. https://github.com/bemre/bankalarbirligi, Haziran 2016.

[7] Jimmy Su Jinjian Zhai. What are you doing? – dsencrypt malware. https://www.fireeye.com/blog/threat-research/2014/06/what-are-you-doing-dsencrypt-malware.html, 2014.

[8] O'Reilly Media. Application security for the android platform. http://it-ebooks.info/book/546/, 2011.

[9] Bernhard Mueller. Hacking soft tokens advanced reverse engineering on android. https://gsec.hitb.org/materials/sg2016/whitepapers/Hacking%20Soft%20Tokens%20-%20Bernhard%20Mueller.pdf, 2016.

[10] Grayson Milbourne & Armando Orozco. Android malware exposed. https://www.webroot.com/shared/pdf/Android-Malware-Exposed.pdf, 2012.

[11] SANS. Reverse engineering of malware on android. https://www.sans.org/reading-room/whitepapers/pda/reverse-engineering-malware-android-3376, 2011.

[12] Spreitzenbarth. Detailed analysis of android.fakeregsms.b. https://forensics.spreitzenbarth.de/2012/02/03/detailed-analysis-of-android-fakeregsms-b/, 2012.

[13] Xuxian Jiang & Yajin Zhou. Android malware. http://libgen.io/book/index.php?md5=0FD8A86F819B36A87755EAD5DD135F90, 2013.

[14] Abdullah Talha KABAKUŞ & İbrahim Alper DOĞRU & Aydın ÇETİN. Android kötücül yazılım tespit ve koruma sistemleri. http://dergipark.gov.tr/download/article-file/236041.