Akıllı Telefonlarda Güvenlik

Ulusal Siber Olaylara Müdahale Merkezi (USOM -TRCERT)
Bilgi Teknolojileri ve İletişim Kurumu
Telekomünikasyon İletişim Başkanlığı
Tel: (0312) 586 53 05
Web: www.usom.gov.tr
E-posta: usom@usom.gov.tr

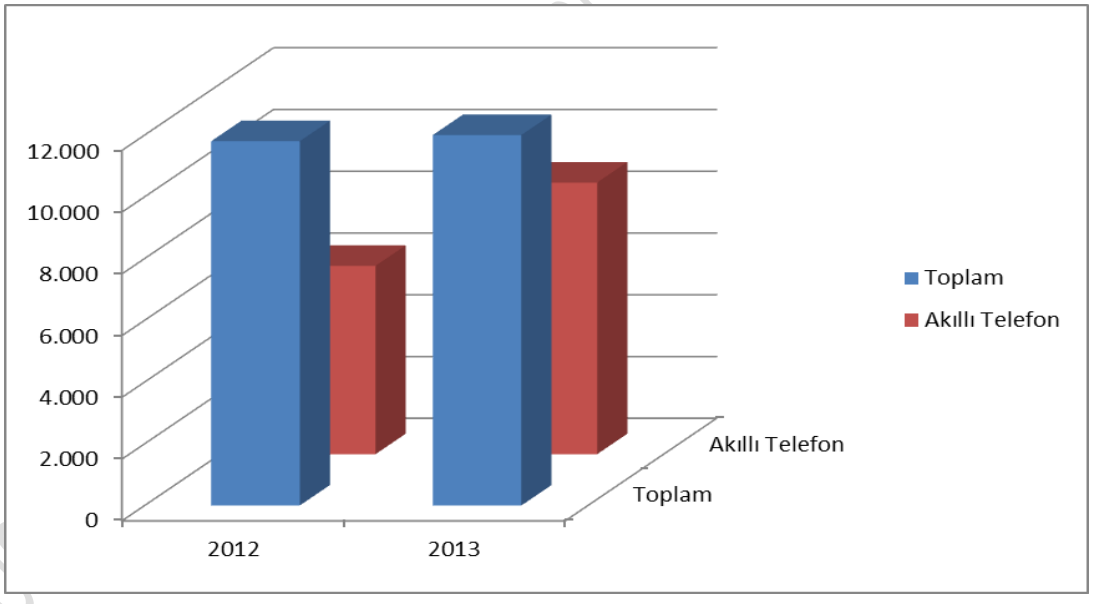
Temmuz 2014
UR.RHB.002

İÇİNDEKİLER

1. MOBİL İLETİŞİM VE AKILLI TELEFONLARLA İLGİLİ İSTATİSTİKLER

Yakın geçmişte başlayan mobil iletişim, günümüzde artık elektronik iletişimin en temel unsuru haline gelmiştir. Son dönemde yapılan bir araştırmaya göre 2017 yılı sonu itibariyle piyasada yer alan akıllı telefon ve tablet sayısı, günümüzde mevcut cihaz sayısının yaklaşık iki katına çıkacaktır. Bununla beraber kişisel bilgisayarların gerek oransal ve gerek sayısal olarak da düşüş göstereceği tahmin edilmektedir. Bu öngörüler ışığında dünya genelinde çok yakın gelecekte kullanıcıların çoğunun internete bağlanmak için tabletler ve akıllı telefonlarını kullanacakları görülmektedir [1].

Mobil telefon satış oranlarının toplamda yaklaşık 9 katına denk gelen büyümesi sonucunda, mobil telefonların %55'ini akıllı telefonların oluşturduğu görülmektedir [2]. Tüm dünyada akıllı telefonların pazar payı hızla büyürken, Türkiye'de büyüme oranları daha da yüksek çıkmaktadır.

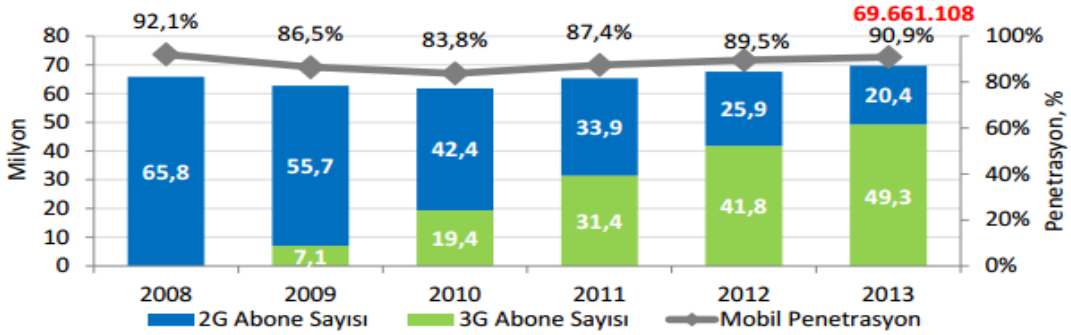


Şekil 1: Türkiye mobil telefon satış oranları [3]

Ülkemizde mobil telefon satış oranlarına ilişkin istatistikler Şekil 1'de görülmektedir. 2013 yılında toplam cihaz satışları bir önceki yıla göre %1'lik bir artış göstermiş ve 12 milyona ulaşmıştır. Bu satışların %74'ünü ise akıllı telefonlar oluşturmuştur. Bu oranlardan 2013 yılında Türkiye'de 8,8 milyon akıllı telefon satıldığı anlaşılmaktadır.

Tüm yıl gerçekleşen akıllı telefon satışlarında da 2012'ye göre yaklaşık %44'lük bir artış yaşanmıştır [3].

Dünya genelinde ve Türkiye'deki satış rakamları incelendiğinde, kullanıcıların artık tercihlerini akıllı telefondan yana kullandıkları açıkça görülmektedir. Bu durum da piyasada bulunan normal mobil telefonların yerini gittikçe akıllı telefonlara bıraktığını göstermektedir. Özellikle Türkiye'de mobil abone sayısı artış oranı akıllı telefon kullanımı artış oranına göre oldukça düşük kalmaktadır. Şekil 2'de de görüldüğü üzere mobil kullanıcı sayısı artışı düşük seviyededir. Ancak akıllı telefonların kullanımında ise tersi bir durum gözlemlenmektedir. Bu veriler ışığında Türkiye'de kullanıcıların büyük bir hızla akıllı telefon kullanımına geçtiği görülmektedir.



Şekil 2: Toplam mobil abone sayısı ve 3G kullanım oranı [4]

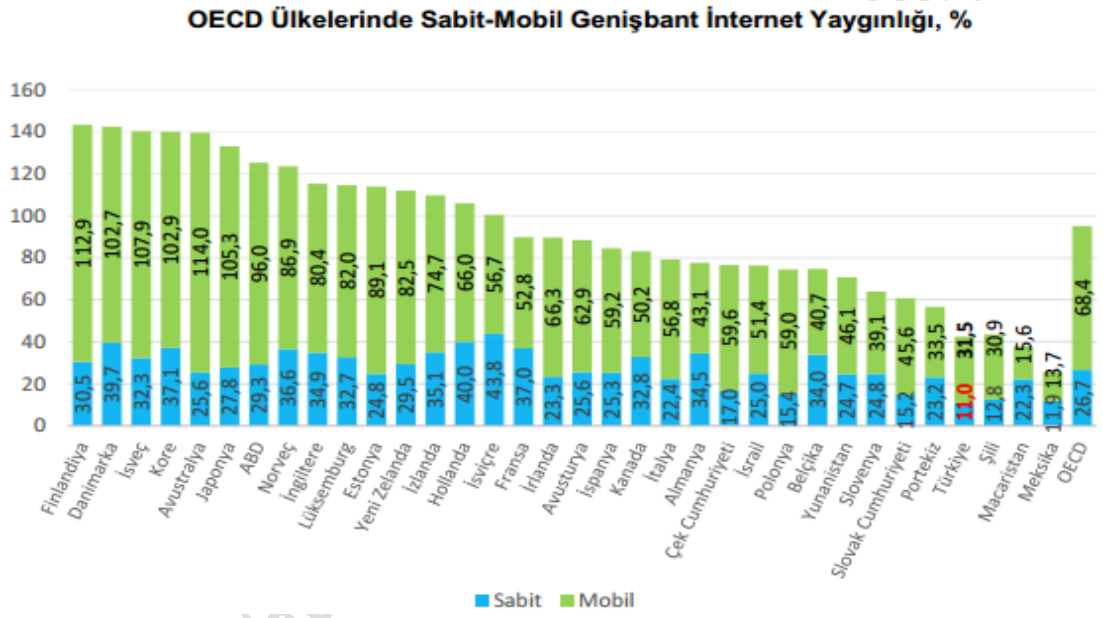
Mobil kullanıcı sayısında büyük bir artış olmamasına karşın, akıllı telefonların kullanımında ve 3G kullanımında büyük bir artış görülmektedir. Bu veriler ışığında Türkiye'de kullanıcıların internet kullanımının hızlı bir şekilde kişisel bilgisayarlardan akıllı telefonlara yöneldiği anlaşılmaktadır.

	2011-4	2012-3	2012-4	2013-4
3G Abone Sayısı	31.375.507	40.251.883	41.798.432	49.266.163
Mobil Bilgisayardan İnternet[20]	1.547.421	1.875.653	1.909.530	1.701.014
Mobil Cepten İnternet[18]	4.907.380	9.685.926	10.252.370	22.472.129
Mobil İnternet Kullanım Miktarı, TByte	10.458	18.618	21.590	43.686

Şekil 3: 3G hizmeti kullanıcı verileri [4]

Şekil 3'te de görüldüğü üzere, akıllı telefonlardan internet kullanıcı sayısı 2011 yılına oranla 2013 yılında 4 kattan fazla artmıştır. Kullanıcı sayısındaki artışın yanında yeni teknolojilerin gelişmesi ve mobil bağlantı hızlarının da artmasıyla beraber mobilden internet trafiğinin kullanımının da hızla arttığı görülmektedir.

2012 yılı son çeyreğinde mobilden internet kullanımı 21.590 TByte iken, 2013 yılı son çeyreğinde iki katına çıkarak 43.686 TByte olmuştur [4]. Son bir yıl içerisinde mobil internet kullanımının iki katına çıkması, akıllı telefonların ne sıklıkla hayatımızda yer aldığını en net ortaya koyan göstergedir.



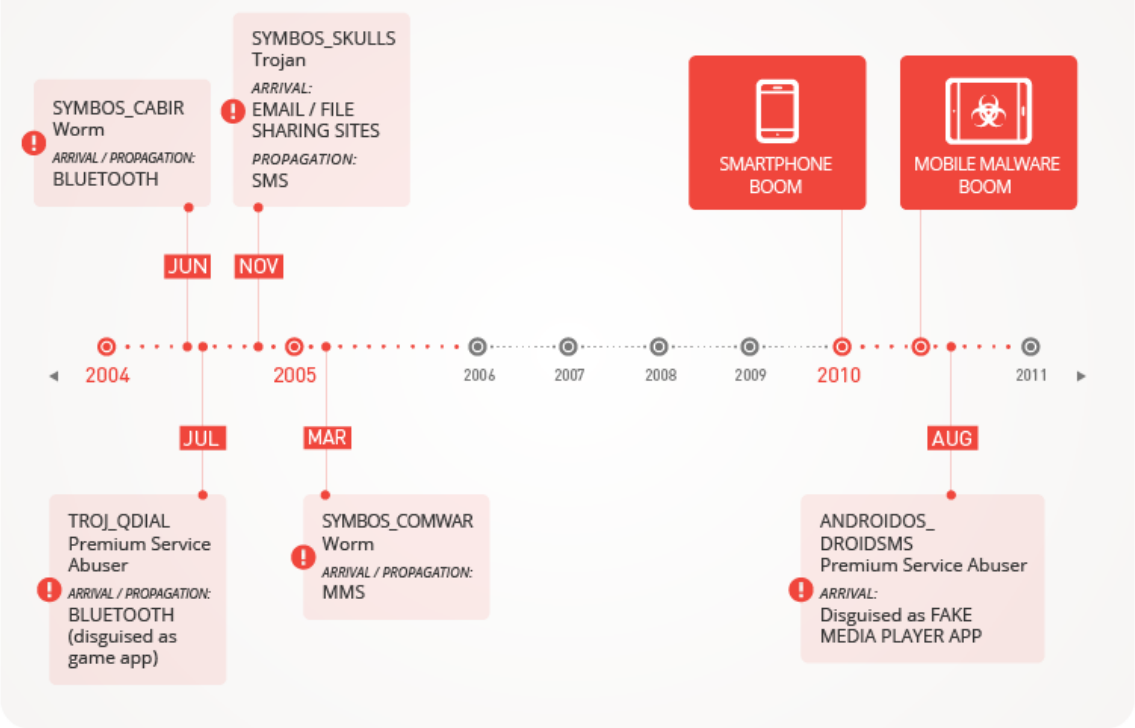
Şekil 4: OECD Ülkelerinde Sabit-Mobil Geniş bant İnternet Yaygınlığı [4].

OECD ülkelerinde mobil internet kullanımının ülkemize oranla yüksek olduğu Şekil-4'te görülmektedir. Türkiye'nin gelişmekte olan ülke olması sebebiyle, gelecekte ülkemizde kullanıcıların daha çok mobilden internete erişecekleri sonucuna erişmek mümkündür. Bankacılık hizmetlerinden iletişime, haberlerin takibinden sosyal medya kullanımına kadar birçok alanda akıllı telefonların daha çok kullanılacağı öngörülmektedir.

2. AKILLI TELEFONLARDAKİ GÜVENLİK RİSKLERİ

Mobil iletişimin ve akıllı telefonların yaygınlaşması ve kullanıcıların bir çok alanda günlük işlerini de bu cihazlar üzerinden yürütmesi, kişisel bilgisayarlarda olduğu gibi, kötü niyetli program geliştiricilerin ilgisini mobil dünyaya doğru çekmiştir.

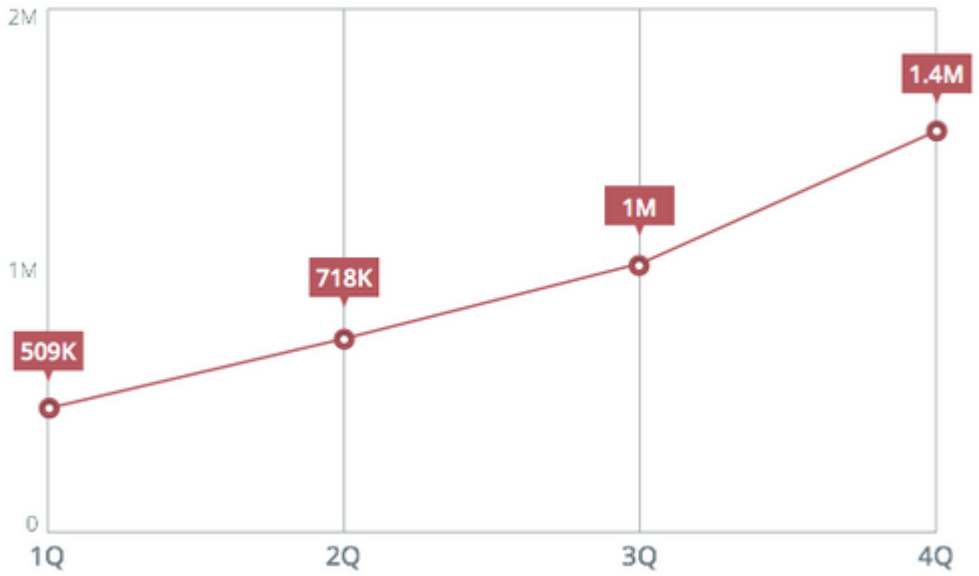
Akıllı telefonların kullanıcıların hayatına girmesinden çok önce mobil telefonlarda güvenlik riski ve zararlı yazılımlar yerini almıştır. 2004 yılında ortaya çıkan SYMBOS_CABIR isimli kötücül yazılım mobil zararlı yazılımların öncüsü olarak nitelendirilmektedir [5].



Şekil 5: Mobil Kötücül Yazılımların Gelişimi [5]

Şekil 5'te görüldüğü üzere, öncelikle Symbian işletim sistemine yönelik kötücül yazılımlar ortaya çıkarken, iOS ve ardından Android işletim sistemli telefonların piyasada ağırlık kazanmaları ile bu mobil işletim sistemlerine yönelik zararlı yazılımlarda artış görülmektedir. Günümüz akıllı telefonlarına kıyasla daha zayıf kabiliyetleri olan eski telefonlardaki zararlı yazılımların etkileri ve yayılma yöntemleri

de, telefonların kapasiteleri ile orantılı olarak daha zayıf kalmaktadır. Ancak akıllı telefonların yaygınlaşması ve bu telefonlardaki gerek işletim sistemlerinin gerekse donanım özelliklerinin hızla gelişmesi ile bu alana yönelik zararlı yazılımların da gelişmesinde artış meydana gelmiştir. Nerdeyse kişisel bilgisayar performansı ve kabiliyeti gösteren akıllı telefonlardaki yazılımların kapasitelerinin de aynı oranda gelişmesi kaçınılmaz olmuştur.



Şekil 6: 2013 yılı Zararlı Yazılım İstatistikleri [6]

Şekil 6'da 2013 yılı içerisinde mobil zararlı yazılımların artışı görülmektedir. 2013 yılı ilk çeyreğinde 509.000 civarında saptanan mobil zararlı yazılımların sayısı, yıl sonu itibariyle neredeyse 3 katına çıkarak 1,4 milyon sayısına ulaşmıştır. Bu sayının içerisinde kullanıcılara istekleri dışında reklam sunan uygulamalar olduğu gibi, kullanıcı bilgilerini sunucularına veya kullanıcıdan habersiz başka noktalara gönderen yazılımlar da bulunmaktadır [6]. Zararlı yazılımların bir yıl gibi kısa bir süre içerisinde üç katına çıktığı gerçeği göz önünde bulundurulacak olursa, akıllı telefonlardaki güvenlik riskinin ne denli kritik seviyede olduğu da görülmüş olacaktır.

Akıllı telefonlardaki riskler için şu şekilde sınıflandırma yapılabilmesi mümkündür. 1- İşletim sistemi bazlı riskler, 2- Uygulama yetkilerinden kaynaklı riskler, 3- Amacı tamamen istihbarat toplamak olan yazılımlardan kaynaklı riskler.

2.1. İŞLETİM SİSTEMİNDEN KAYNAKLANAN RİSKLER

Akıllı telefonlardaki risklerin başında mobil işletim sistemlerinden kaynaklanan problemler gelmektedir. Burada kullanıcıların alabileceği önlemler çok kısıtlı olduğu ve her cihazda işletim sistemi yüklü bulunduğu için, etkilenen kullanıcı sayısı çok daha geniş olmaktadır.

Bu risk grubuna örnek olarak Carrier IQ programı verilebilir. iOS, Android, Blackberry ve Symbian işletim sistemine sahip telefonlarda yüklü olarak gelen bu programın kullanıcı verilerini kendi veri merkezine gönderdiği bilinmektedir. Carrier IQ şirketi, kendilerine ait internet adresinde, "milyonlarca cihazı destekleyecek gömülü analiz yazılımı sunan firma" ve "mobil üreticilere eşi görülmemiş müşterileri anlayabilme sağlıyoruz" şeklinde tanıtım yapmaktadır [7] Şirketin kendine ait bu tanıtımda yer alan ifadeler bile açıkça kullanıcıların bilgilerinin kendilerinden habersiz üretici dahil farklı merkezlere verildiğini göstermektedir.

Android, Blackberry ve Symbian işletim sistemine sahip telefonlarda hali hazırda yüklü ve çalışır durumda gelen Carrier IQ uygulaması, iOS işletim sistemli cihazlarda ise yüklü ancak kapalı durumda gelmektedir. Ancak müşteri memnuniyeti için verileriniz değerlendirilmesi gibi bir seçeneğin aktif edilmesi durumunda, uygulama çalışır duruma gelmektedir.

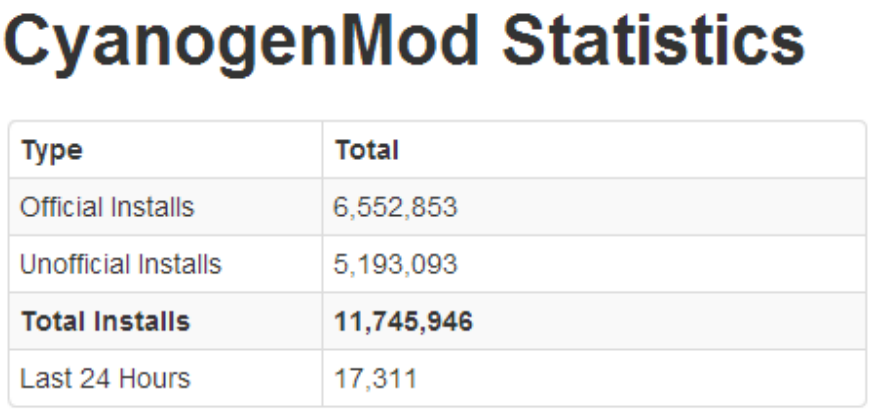
Carrier IQ uygulaması telefonun en alt seviyesinde yüklü olarak bulunmaktadır. Yani bu şekilde kullanıcı böyle bir uygulamanın yüklü olduğundan ve çalıştığından haberdar değildir. Ayrıca, uygulamanın çalışmasından kaynaklı herhangi bir uyarı da kullanıcıya verilmemektedir. Kullanıcının uygulaması bulması ve ardından da bunu kaldırması kesinlikle mümkün olmamaktadır.

Hali hazırda yüklü gelen ve telefondan kaldırılamayan uygulamanın çalışma mantığı ise şu şekildedir. Uygulama kullanıcı ve telefonda yüklü diğer uygulamalar arasında bulunmaktadır. Böylece, ne kadar güvenlik önlemleri alınmış olursa olsun, uygulama kullanıcı tarafından yapılan tüm işlemleri yakalayıp kayıt edebilmektedir. Kullanıcının bulunduğu yerden, internet tarayıcısında girdiği internet adreslerine kadar, uygulamalarda kullandığı şifrelerden paylaştığı mesajların içeriklerine kadar tüm

bilgiler uygulama tarafından yakalanabilmektedir. Carrier IQ firması bu iddiaları yalanlamış olsa da, işletim sistemi bazında takip edilen kayıtlar göstermektedir ki, kullanıcı bilgileri Carrier IQ'ya ait eşsiz bir kod ile tutulmaktadır. SSL gibi güvenli protokoller ile oluşturulan bağlantılardaki trafik ve bu trafiğin içeriği bile uygulama tarafından açık bir şekilde yakalanabilmektedir.

İşletim sisteminden kaynaklı risklerden bir diğeri de, değiştirilmiş işletim sistemleri kullanılmasıdır. Android işletim sistemi için bu tip değiştirilmiş yazılımlara kısaca "Custom ROM" denirken, iOS için "Jailbreak" tanımı kullanılmaktadır.

Custom ROM ve Jailbreak gibi, içeriği farklı kullanıcılar tarafından değiştirilmiş işletim sistemlerinde yazılımın nasıl çalışacağı tamamen işletim sisteminin kodlarını değiştirenlerin inisiyatifinde olmaktadır. Google tarafından geliştirilen bir Android veya Apple tarafından geliştirilen bir iOS işletim sistemi yerine, dünyanın herhangi bir yerinde bulunan bir yazılımcı tarafından ve tamamen kendi isteğine göre tasarlanarak geliştirilen bir işletim sistemi kullanmanın ne derece büyük riskler doğurabileceği ise açıktır.



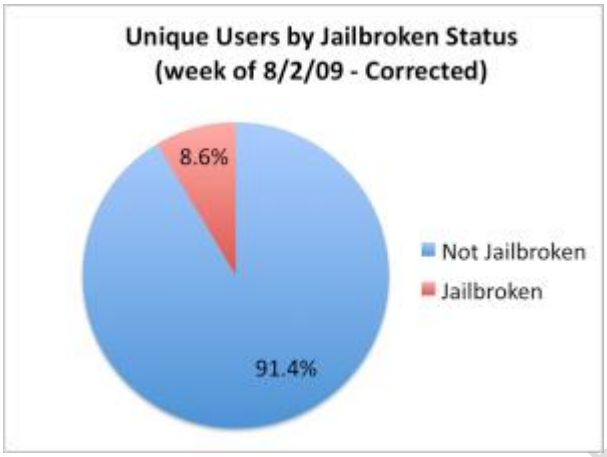
CyanogenMod Statistics

Type	Total
Official Installs	6,552,853
Unofficial Installs	5,193,093
Total Installs	**11,745,946**
Last 24 Hours	17,311

Şekil 7: CyanogenMod ROM Yükleme İstatistikleri [8]

Şekil 7'de Android Custom ROM'lar arasında en popüleri olan CyanogenMod istatistikleri ve Şekil 8'de de Jailbreak kullanım oranları verilmiştir. Bu şekillerden anlaşıldığı üzere, milyonlarca kullanıcı, akıllı telefonlarının işletim sistemlerinin

kontrollerini asıl cihaz üreticilerinin değil, tamamen başkalarının eline bırakmış durumdadır.

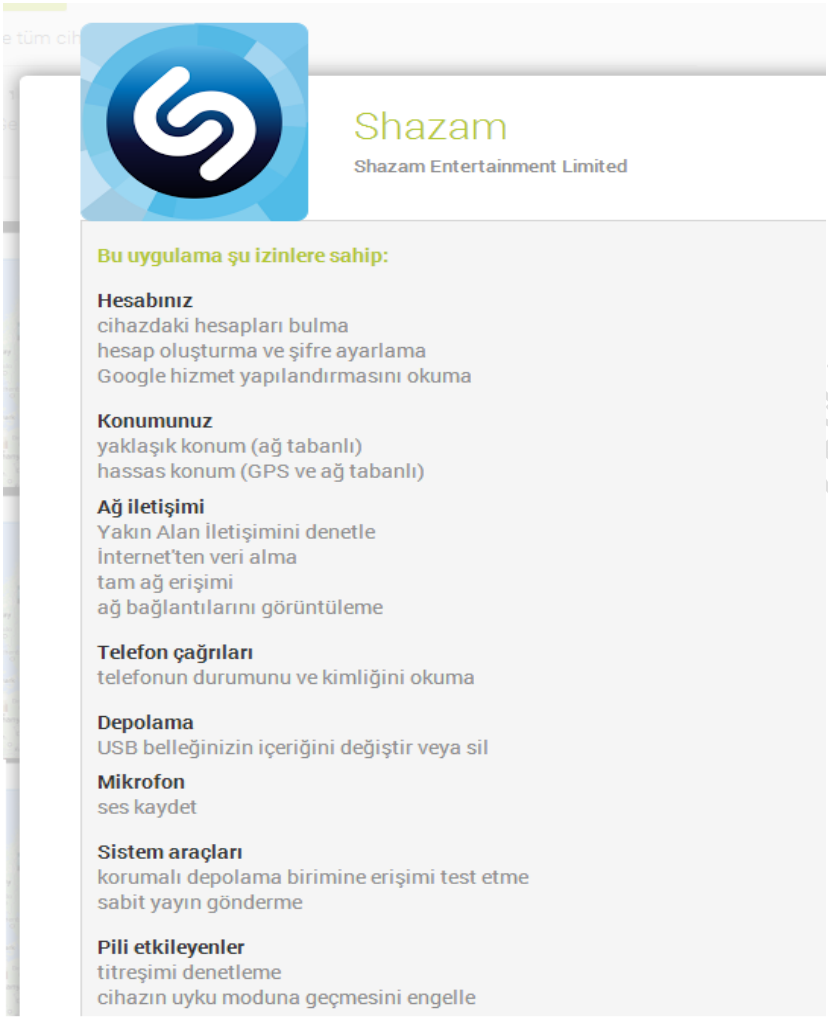


Şekil 8: Jailbreak Yükleme İstatistikleri [9]

2.2. UYGULAMA YETKİLERİNDEN KAYNAKLANAN RİSKLER

Akıllı telefonlardaki risklerden bir diğeri de yüklenen uygulamalarda kaynaklanan risklerdir. Bu kategoride, uygulamalar fonksiyonlarını yerine getirirken, aynı zamanda uygulamanın çalışma alanı dışında kullanıcı bilgilerini de elde etmektedirler. Örnek olarak, bir telefonda yüklü bir kelime oyunu oyun fonksiyonunu yerine getirirken aynı zamanda telefonda bulunan rehber bilgilerini ya da girilen internet adresi bilgilerini de alıp kendi veri merkezine gönderebilmektedir.

Yapılan araştırmalar göstermektedir ki, iOS ve Android uygulamalarının neredeyse yarısı, kullanıcı bilgilerini alıp bunları kendi veri merkezlerine göndermektedir. Kullanıcılara ait alınan bu veriler reklam şirketlerine ya da talep eden firmalara belirli ücretler karşılığında satılmaktadır. Bu şekilde kullanıcı bilgilerini alan popüler uygulamalar arasında tüm dünyada milyonlarca kullanıcısı olan “Angry Birds” oyunu ve “Shazam” uygulaması da bulunmaktadır. Araştırması gerçekleştirilen 101 uygulamadan 56’sı telefona ait kullanıcı bilgilerini ticari firmalara telefona ait tekil UDID bilgisi ile beraber verdiklerini göstermektedir. 47’si ise telefonun konu bilgisi, kullanıcının cinsiyet ve yaş bilgisi gibi diğer kişisel bilgilerini de ticari firmalara vermektedir [10].



Şekil 9: Shazam Uygulama Yetkileri [11]

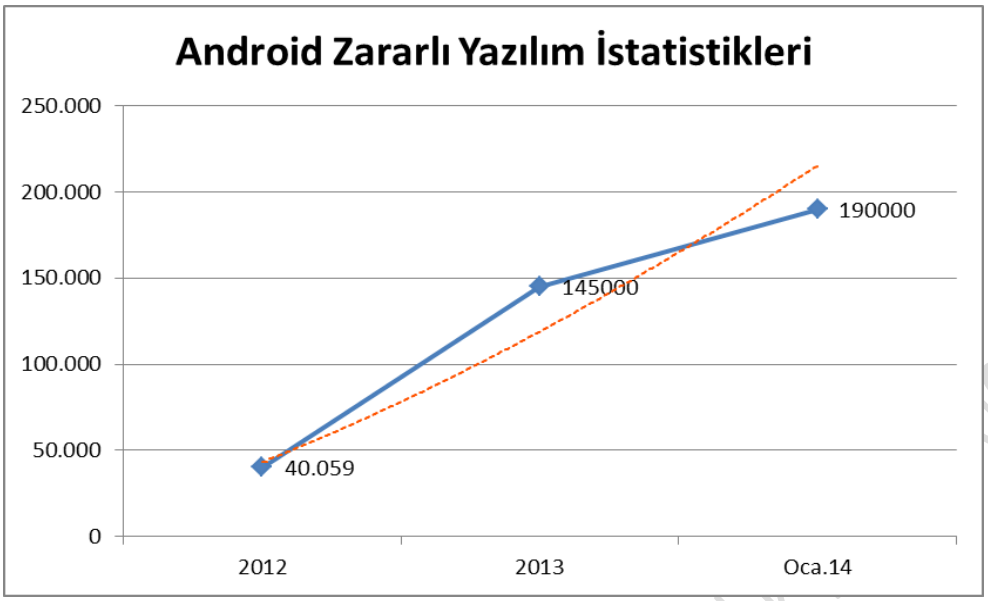
Şekil 9'da Shazam uygulamasının telefona yüklenmeden önce kullanıcı tarafından kabul etmesi istenen özellikler görülmektedir. Burada da görüldüğü üzere telefon çağrılarından rehber bilgilerine, internette girilen adreslerden kullanıcının GPS konum bilgisine kadar bir çok bilginin uygulama tarafından elde edilebileceği yazılmaktadır. Amacı sadece dinlenen şarkının adını bulmak olan bu uygulamanın bu kadar çok yetkiyi istemesi açıkça göstermektedir ki, kullanıcı bilgileri bu uygulamalar tarafından elde edilmektedir.

Popüler uygulamaların dışında ayrıca kullanıcılar için büyük risk oluşturan diğer bir kategori de yanıltıcı uygulamaların uygulama marketlerinde bolca bulunmasıdır. Bu kategorideki uygulamalar kullanıcılara çok basit bir fonksiyonu gösterir şeklinde

sunum yaparken, aslında arka planda kullanıcıya ait kişisel verileri elde etmektedirler. Android işletim sistemine yönelik uygulama marketi olan "Google Play Store" yüklenen uygulamaların kontrolünü gerçekleştirmediği için bu şekilde kullanıcıları yanlış bilgilendiren kötü amaçlı uygulamalar Android marketinde çokça bulunmaktadır. iOS için uygulama marketi olan "Apple Store"'da uygulamaların kontrolü daha sıkı gerçekleştirildiğinden bu markette riskli uygulamaların bulunma ihtimali düşük olsa da yine de kullanıcıların yükleyecekleri uygulamalarda dikkatli davranmaları gerekmektedir.

Şekil10'da bir örneği görüldüğü üzere, amacı sadece wallpaper yüklemek olan bir uygulama internet erişim bilgilerinden telefon çağrılarına, kullanıcıya ait kişisel bilgileri içeren sosyal iletişim bilgilerinden telefonun sistem bilgilerine ait bir çok bilgiye erişim yetkisi istemektedir. Bu kategorideki uygulamalar şekilde de görüldüğü üzere kullanıcıları kandırabilmek için cinselliği ya da oyunları ön planda tutmaktadır. Cinsel görsellerle kullanıcıları etkilemeye çalışan bu uygulamaların tek hedefi kullanıcılara ait kişisel verilerin elde edilebilmesidir.

Şekil 10: Wallpaper Uygulama Yetkileri [11]



Şekil 11: Android Zararlı Yazılım İstatistikleri [12]

Online güvenlik şirketi Kaspersky'ın gerçekleştirdiği bir araştırmadan elde edilen sonuçlara göre, 2013 yılı içerisinde akıllı telefonlara yönelik 145.000'e yakın kötü amaçlı yazılım tespit edilmiştir. Bu rakam 2012 yılına oranla üç kat artış göstermiş Ocak 2014 itibariyle de 190.000'e ulaşmıştır. Ayrıca Android tabanlı cihazlarda mobil kötü amaçlı yazılım dağıtmak yaklaşık 4 milyon uygulama kullanıldığı ifade edilmektedir [12].

2.3. CASUS YAZILIMLARDAN KAYNAKLANAN RİSKLER

Akıllı telefonlarda en büyük güvenlik riski içeren uygulamalar bu kategoride bulunmaktadır. Bu sınıftaki uygulamaların nihai amacı kullanıcıya ait tüm bilgilerin bir merkezde toplanması ve bunu talep eden kullanıcıya online olarak gönderilmesidir. Bu sınıftaki uygulamaların en önemli özelliği telefonda yüklü olup olmadıklarının tespit edilememesidir. Aynı zamanda uygulamanın kaldırılması da mümkün olmamaktadır [13].

Bu sınıftaki uygulamaların kendilerine ait internet sayfalarında genellikle; çocuklarınızın güvenliği için takip edin, telefonunuzun çalınması durumunda verilerinizi ve telefonunuzu takip edin, çalışanlarınızın iş telefonlarını takip edin, gibi

tanıtımlarla casus yazılımların reklamı yapılmaktadır. Casus yazılımlar ile yapılabilecekler aşağıdaki gibi listelenebilir.

Ortam Dinlemesi: Telefonun mikrofonu kullanılarak, kullanıcının haberi olmadan ortamda bulunan sesler kaydedilebilir ve bunlar belirlen hedefe yüklenebilir. Yapılabilecek ayarlamalar ile kaydedilecek ses süresi dahil belirlenebilmektedir.

Gizli Kamera: Telefonun kamerası kullanılarak bulunan ortamın fotoğrafı gizlice çekilebilir. Çekilen bu fotoğraflar belirlenen hedefe yüklenebilir ve buradan kullanıcı fotoğrafları temin edebilmektedir.

Kısa Mesaj Bilgileri: Telefona gelen ve telefondan gönderilen tüm kısa mesajlar kaydedilir ve program sahibi bunları takip edebilir.

Konum Bilgileri: Telefonun bulunduğu konum anlık ve sürekli olarak kayıt altına alınabilir. Böylece telefon sahibinin coğrafi olarak takibi de gerçekleştirilebilir.

Arama Bilgileri: Telefona gelen ve telefondan yapılan tüm aramaların kayıtları tutulabilir. Görüşmeye ait telefon bilgisi, zaman ve süre bilgisi tüm detaylar bu kayıtlar ile tutulabilmektedir.

İnternet Bağlantı Bilgileri: Kullanıcının telefondan girdiği tüm internet adresleri ve bu internet adreslerinde kullandığı kullanıcı adı, şifre gibi tüm bilgiler takip edilebilmektedir.

Dosya Bilgileri: Telefonun dahili hafızasında bulunan fotoğraf ve video gibi tüm dosyalar belirlenen hedefe yüklenerek buradan takip gerçekleştirilebilmektedir.

Sosyal Medya Bilgileri: Kullanıcının telefonunda kullandığı Facebook, Twitter, Whatsapp gibi sosyal paylaşım uygulamalarında paylaştığı tüm bilgiler, gönderdiği ve gelen tüm mesajlar takip edilebilmektedir.

E-Posta Bilgileri: Telefonun e-posta uygulaması ile gönderilen ve gelen tüm e-posta bilgileri takip edilebilmektedir.

Uygulama Bilgileri: Telefona yüklenen tüm uygulamalara ait uygulamanın yüklenme tarihi, versiyonu gibi tüm bilgiler takip edilebilmektedir.

Rehber Bilgileri: Telefon rehberine kayıt edilen tüm kişilere ait bilgiler, telefonda bulunan şekliyle kayıt edilip takip edilebilmektedir.

Takvim Bilgileri: Telefona takviminde bulunan tüm olaylar ve önemli tarihler, kayıt edilen bilgiler takip edilebilmektedir.

Uygulama Engelleme: Telefona yüklenen bazı uygulamaların ya da telefonda yüklü bulunan bazı uygulamaların çalışması engellenebilmektedir.

Uzaktan Program Kaldırma: Casus yazılım ihtiyacının ortadan kalkması durumunda bu uygulama uzaktan telefondan kaldırılabilmektedir.

Kısa Mesaj ile Kontrol: Telefonu kilitleme, kilidi açma, anlık GPS konumunu öğrenme gibi anlık bilgi talebi durumunda, bunlar kısa mesaj ile telefonun kontrolü sağlanarak gerçekleştirilebilmektedir.

Uyarı Sistemi: Telefonda veya kullanıcının bazı hareketlerinde anında bilgilendirilmek istendiği durumlarda uyarı sistemi kullanılabilmekte ve belirlenen şartların oluşması durumunda uyarı program sahibine gönderilebilmektedir.

Telefonlarda kullanılacak casus yazılımlar ile gerçekleştirilebilecek işlemler, neredeyse kullanıcıya ait tüm bilgilerin takibini sağlamaktadır. Kullanıcının farkında olmadan gerçekleştirdiği faaliyetler, programlar sayesinde anlık olarak takip edilip kayıt altına alınabilmektedir.

Piyasada casus yazılımların genelde özelliklerine ve kabiliyetlerine göre fiyatları bulunmaktadır. Bununla beraber, daha az kabiliyetli olmalarına rağmen ücretsiz uygulamaların temin edilmesi de mümkün olmaktadır.

Casus yazılımlarla aynı kabiliyetlere sahip ancak farklı amaçlar için kullanılan programlar da akıllı telefon marketlerinde bulunabilmektedir. Bunlara örnek olarak “Color”, “Shopkick” ve “IntoNow” uygulamaları verilebilir. Bu uygulamalar ortamdaki sesleri dinleyip, bulunulan ortamın neresini olduğunu, buralarda yayın yapılan gizli

ses kodları ile anlayabilmekte ve bulunulan mekana göre reklam ya da tanıtım mesajlarını kullanıcıya iletmektedir [14].

Casus yazılımlar gerek uygulama marketlerinde bulunabileceği gibi, daha profesyonel firmaların kendi internet adresleri vasıtasıyla da satın alınabilmektedir. İnternet adreslerinde uygulamaların özellikleri ve kabiliyetleri listelenmektedir.

2.4. AKILLI TELEFONLAR İÇİN GÜVENLİK İPUÇLARI

Kullanıcıların günlük hayatında bu kadar önemli yer edinen ve bir o kadar da önemli riskleri barındıran akıllı telefonlarda birkaç basit önlemle bu risklerin azaltılması mümkün olabilmektedir. İşletim sisteminden bağımsız olarak tüm akıllı telefonlarda uygulanabilecek önlemler aşağıda listelenmiştir.

Ekran Koruyucu Şifre: Telefonun kaybolması veya çalınması gibi durumlarında, telefonun izinsiz kullanımını önlemek için telefonun ana ekranına şifre/PIN/ekran koruması yapılması gerekmektedir [16].

Cihazın Temel Güvenlik Ayarları: Güvenlik ayarları üzerinde değişiklik yapılmaması tavsiye edilir. Telefonun fabrika ayarlarının ve işletim sisteminin ayarlarının değiştirilmesi (jailbreak, rooting) gibi işlemler, akıllı telefonun siber saldırılara karşı daha duyarlı yaparken, işletmeci ve akıllı telefon tarafından sunulan güvenlik özelliklerini zayıflatmaktadır [17].

Telefonun Yedeklenmesi ve Veri Güvenliği: Telefonda saklanan bütün verilerin (rehber öğeleri, belgeler, fotoğraflar vb.) yedeklenmesi tavsiye edilir. Söz konusu bu veriler kişisel bilgisayarlarda, harici depolama aygıtlarında veya bulut ortamında saklanabilir [17].

Uygulama Erişim Yetkilerinin Kontrolü: Uygulamaların, akıllı telefonlarınızda bulunan kişisel bilgilerinize erişme yetkisi konusunda dikkatli olmanız tavsiye edilir. Aksi halde indireceğiniz uygulama ile kişisel bilgileriniz (örneğin konum veriniz) üzerinde işlem yapılmasına izin vermiş olabilirsiniz. Ayrıca yüklemeden önce her uygulama için gizlilik ayarlarını kontrol ettiğinizden emin olun [17].

Güvenilir Kaynaklardan Uygulama Yüklenmesi: Bir uygulamayı indirmeden önce, uygulamanın yasal ve güvenilir olduğundan emin olmak için araştırma yapılmalıdır. Akıllı telefonlara indirilecek uygulamaları, işletim sisteminin resmi uygulama ortamından edinilmesi önemle tavsiye edilir [17].

Uzaktan Erişim ile Silmeyi Etkinleştirecek Güvenlik Uygulamaları: Akıllı telefonlarda, uygulama olarak edinilebilecek veya varsayılan olarak yaygın olarak kullanılan önemli bir güvenlik özelliği; telefonun GPS'i kapalı olsa bile, telefonunuzda depolanan tüm verilere uzaktan erişebilmeye ve söz konusu verileri silebilmeye imkân sağlamasıdır. Bu durumda telefonunuzu kaybettiğinizde, telefonunuz sessiz olsa bile bazı uygulamalar yüksek sesli bir alarmı aktif edebilir. Bu uygulamalar aynı zamanda telefonunuzu kaybettiğinizde daha kolay bulabilmenize yardımcı olabilir [17].

Açık Wi-Fi Bağlantıları: Şifresiz herkese açık kablosuz ağ trafiği bu hizmeti bedava veren kişi tarafından dinleniyor olabilir. Halka açık ağ kullanımını kısıtlamalı ve onun yerine güvenebileceğiniz bir operatöre ait güvenli Wi-Fi veya kablosuz mobil bağlantı kullanmalısınız [16].

Yazılım Güncellemelerinin Yapılması: Otomatik güncellemeleri etkinleştirerek, telefonunuzun işletim sistemini güncel tutmalısınız veya servis sağlayıcınızdan, işletim sistemi sağlayıcınızdan, cihaz üreticisinden ve uygulama sağlayıcınızdan gelen güncellemeleri kabul etmelisiniz. İşletim sisteminizi güncel tutarak, siber tehditlere maruz kalma riskinizi azaltabilirsiniz [17].

Telefon Verilerinin Silinmesi: Telefonunuzu satmak istemeniz durumunda, akıllı telefonunuzda kişisel verileriniz olabileceğini unutmayın. Gizliliğinizi korumak için, verileri tamamen silin veya telefonunuzu fabrika ayarlarına sıfırlayın. Aynı zamanda sıfırlama işleminin; telefonunuzda yer alan uygulamalar, mesajlar, arama geçmişi, müzik, fotoğraf gibi içeriklerin silinmesini de kapsadığını unutmayınız [17].

Çalınan Telefonun Bildirilmesi: Telefonunuzun çalınması veya kaybolması durumunda, hattınızı kapatmak için işletmenize başvurun. Telefonunuzun ülkemizde kullanımını engellemek için durumu Bilgi Teknolojileri ve İletişim Kurumu'na (BTK) (*www.btk.gov.tr*) bildirebilirsiniz [17].

Uygulama Marketinde Kredi Kartı Kullanımı: Sadece ücretsiz uygulamaları kullanıyorsanız telefonunuzun uygulama marketinde kullanıcı oluştururken bunu sizden talep etse de kredi kartı bilgilerinizi girmeyiniz. Uygulama satın almayı düşünüyorsanız limiti düşük sanal kart bilgilerinizi kullanmalısınız. Ek olarak kredi kartı ekstrenizi düzenli olarak takip edin [16].

Telefondaki Verilerin Şifrelenmesi: Eğer telefonunuzun veri şifreleme özelliği varsa bu özelliği kullandığınızdan emin olun. Böyle biz özellik yoksa, veri şifreleyen uygulama kullanmanız tavsiye edilir. Telefonun çalınması ya da kaybolması durumunda veriler ele geçirilse bile ilgili şahıs tarafından kullanılamayacak ve anlaşılamayacaktır [18].

KAYNAKLAR

[1] Atalay, A.H. *Mobil İletişim ve Siber Güvenlik*.

http://www.globalnet.com.tr/blog/377-mobil-iletisim-ve-siber-guvenlik.html

[2] Türkiye'deki akıllı telefon pazarı büyüme oranı dünyayı solladı

http://www.marketingturkiye.com.tr/index.php?option=com_content&view=article&id=12646:tuerkiyedeki-akll-telefon-pazar-bueyueme-oran-duenyay-sollad&catid=65:guencel-haberler&Itemid=160

[3] Türkiye'de 9 milyon akıllı telefon satıldı

http://www.computerworld.com.tr/haberler/turkiyede-9-milyon-akilli-telefon-satildi/

[4] Türkiye Elektronik Haberleşme Sektörü – Üç Aylık Pazar Verileri Raporu

http://www.btk.gov.tr/kutuphane_ve_veribankasi/pazar_verileri/ucaylik13_4.pdf

[5] Mobile Malware: 10 Terrible Years

http://about-threats.trendmicro.com/us/mobile/monthly-mobile-review/2014-03-mobile-malware-10-terrible-years

[6] Trend Micro Mobile App Reputation Service: Beyond Anti-Malware

http://blog.trendmicro.com/beyond-anti-malware/

[7] Your Android Phone Is Secretly Recording Everything You Do

http://gizmodo.com/5863849/your-android-phone-is-secretly-recording-everything-you-do

[8] CyanogenMod Statistics

http://stats.cyanogenmod.com/

[9] 8.6% of iPhones are jailbroken, stats suggest…

http://9to5mac.com/2009/08/15/8-6-of-iphones-are-jailbroken-stats-suggest/

[10] How your smartphone is keeping track of you: Apps secretly monitor users to target advertising campaigns

http://www.dailymail.co.uk/sciencetech/article-1340107/How-smartphone-keeping-track-Apps-secretly-monitor-users-target-advertising-campaigns.html

[11] Shazam Uygulama Yükle

https://play.google.com/store/apps/details?id=com.shazam.android

[12] Zararlı yazılımlar evrimleşiyor

http://www.hurriyet.com.tr/teknoloji/25949565.asp

[13] Smartphone Apps Quietly Using Phone Microphones And Cameras To Gather Data

http://www.techdirt.com/blog/wireless/articles/20110417/21485513927/smartphone-apps-quietly-using-phone-microphones-cameras-to-gather-data.shtml

[14] Snooping: It's not a crime, it's a feature

http://www.computerworld.com/s/article/print/9215853/Snooping_It_s_not_a_crime_it_s_a_feature?taxonomyName=Privacy&taxonomyId=84

[15] Spy Agencies Tap Data Streaming From Phone Apps

http://www.nytimes.com/2014/01/28/world/spy-agencies-scour-phone-apps-for-personal-data.html?_r=11

[16] 10 Adımda Akıllı Telefon Güvenliği

http://www.siberguvenlik.org.tr/2013/12/10-admda-akll-telefon-guvenligi.html

[17] Tüketiciler İçin Akıllı Telefon Güvenlik İpuçları

https://tuketici.btk.gov.tr/haber/?id=76

[18] Security tips – for safer smartphone use

http://usa.kaspersky.com/internet-security-center/internet-safety/smartphones#.U1jDXPl_t4F