MAKÜ FEBED
ISSN Online: 1309-2243
http://dergipark.ulakbim.gov.tr/makufebed

Mehmet Akif Ersoy Üniversitesi Fen Bilimleri Enstitüsü Dergisi Özel Sayı 1: 88-96 (2017)
The Journal of Graduate School of Natural and Applied Sciences of Mehmet Akif Ersoy University Special Issue 1: 88-96 (2017)

Zararlı Yazılım Yayma Aracı Olarak Mobil Uygulamaların Kullanılması: Pokemon Go Örneği[a]

Mehmet Ali YALÇINKAYA, Besim ALTINOK, Mehmet GÜRDAL, Meryem AKDOĞAN, Ecir Uğur KÜÇÜKSİLLE

Süleyman Demirel Üniversitesi Mühendislik Fakültesi, Isparta

✉ *Sorumlu Yazar (Corresponding author)*: mehmetyalcinkaya@sdu.edu.tr*

ÖZ

Günümüz bilişim dünyasında mobil cihazlar, gün geçtikçe artan yetenekleri sayesinde bilgisayar sistemlerinin yerini almaya başlamıştır. Farklı donanımsal özelliklere ve fonksiyonelliğe sahip mobil cihazların kullanımı gün geçtikçe artmaktadır. Mobil cihazların kullanımındaki bu artış, söz konusu cihazlara yönelik gerçekleştirilen saldırılarda da aynı oranda artışa neden olmuştur. Saldırganlar tarafından mobil cihazlara yönelik olarak gerçekleştirilen saldırılardan biri de mobil uygulamaların içerisine zararlı yazılımların enjekte edilmesidir. Bu çalışmada mobil cihaz kullanımının artışına ve söz konusu cihazların saldırganlar tarafından hedef alınmasına değinilmiş, saldırganlar tarafından geliştirilen zararlı yazılım türleri incelenmiştir. Çalışmada ayrıca son günlerde mobil cihaz kullanıcıları arasında en popüler uygulamalardan biri olan Pokemon Go uygulaması incelenmiş, söz konusu uygulama içerisine enjekte edilmiş olan Droidjack zararlı yazılımı analiz edilmiştir. Gerçekleştirilen çalışma mobil cihaz kullanıcılarına yönelik güvenlik önlemlerinin sunulması ile tamamlanmıştır.

Anahtar Kelimeler: Mobil uygulama, malware, pokemon go, droidjack

Usage of Mobile Applications As a Malware Spreading Tool: Pokemon Go Example

ABSTRACT

Nowadays in the world of informatic, mobile devices have begun to take place of computer system due to ever increasing capabilities. The use of different hardware features and functionality of mobile devices is increasing day by day. This increase in the use of mobile devices, in attacks that also for such devices has led to an increase in the same ratio. One of the attacks carried out by attackers for mobile devices is to also inject malicious software into mobile applications. In this study, mentioned increasing use of the mobile devices and to be targeted these devices by the attackers. In this study also examined that Pokemon Go application is one of the most popular applications among mobile users in recent days and malware Droidjack which is injected into this application was analyzed. This research was completed by presenting security measures for mobile users.

Keywords: Mobile application, malware, pokemon go, droidjack

GİRİŞ

Yakın geçmişe kadar, bilişim dünyasında zararlı yazılımlar (malware) olarak nitelendirilen solucan, trojan, virüs ve reklam içerikli yazılımlar saldırganlar tarafından kişisel ya da kurumsal bilgisayarlara yönelik olarak geliştirilmiştir (Schmid et al., 2009). Günümüzde mobil cihazlar, iletişim kurmanın

[a] 11 -13 Mayıs 2017 tarihleri arasında Mehmet Akif Ersoy Üniversitesi tarafından düzenlenen "MESTEK 2017: 4. Ulusal Meslek Yüksekokulları Sosyal ve Teknik Bilimler Kongresi" kapsamında sunulmuştur.

ötesinde birçok farklı işlemi gerçekleştirebilecek teknolojiye ulaşmıştır. Mobil cihazların yeteneklerinde meydana gelen bu artış, söz konusu cihazların kullanımında da aynı oranda artışa neden olmuştur. Mobil cihazların kullanımında meydana gelen artışın bir diğer nedeni de; mobil cihazlar kullanılarak geleneksel masaüstü sistemler ile gerçekleştirilebilen işlemlerin birçoğunun halledilebilmesi, mobil cihazların taşıma vb. yönlerden daha kullanışlı sistemler olmasıdır.

Günümüzde akıllı telefonlar olarak nitelendirilen mobil cihazlar aracılığı ile bankacılık işlemleri, sosyal medya kullanımı, mail gönderme ve alma, kişisel verileri saklama, kişisel multimedya verilerinin saklanması gibi birçok işlem gerçekleştirilebilmektedir. Firmalar çalışanları arasında haberleşmeyi, kurdukları eposta sunuculara bağlı akıllı telefonlar ile gerçekleştirmekte, bankalar ise müşterilerini mobil internet bankacılığı kullanmaları yönünde teşvik etmektedir. Mobil bankacılık işlemleri kullanıcının oluşturduğu şifrelerin yanı sıra kullanıcıya iletilen tek kullanımlık SMS parolaları ile yapılmaktadır.

Günümüz bilişim dünyasında mobil cihazların bu denli yüksek önem içeriyor olması, mobil cihazları siber saldırganların en önemli hedeflerinden biri haline getirmiştir. Saldırganlar tarafından geliştirilen zararlı yazılımlar önceleri sadece bilgisayarlar için tehditken şimdilerde mobil cihazlar içinde ciddi tehdit oluşturmaktadır. Mobil cihazlara bulaşan söz konusu zararlı yazılımlar tüm rehber bilgisini ele geçirebilmekte, kullanıcıya ait mesajları okuyabilmekte, resim, video ve ses gibi multimedya dosyalarına erişebilmekte ve kullanıcıya ait konum bilgisini saldırganlara iletebilmektedir. Ayrıca sisteme bulaşmış olan zararlı yazılımlar, sahip oldukları yeteneklere göre; telefon görüşmelerini anlık olarak dinleme, kullanıcının bulunduğu ortamın dinlemesi, internet aktivitelerinin takip edilmesi gibi işlemleri gerçekleştirebilmektedir (Ekim, 2013).

Dünya genelinde 2014 yılında kişisel ya da iş amaçlı olarak dünyada 5.6 milyar mobil kullanıcı bulunmaktadır. 2018 yılında söz konusu miktarın 6.2 milyara ulaşması ön görülmektedir. Bu veriler 2018 yılında dünya nüfusunun %84'nün mobil cihaz kullanıcısı olacağı anlamına gelmektedir. Tablo 1' de yıllara ait bilinen ve gelecek yıllar için beklenen mobil kullanıcı ve mobil cihaz sayısı gösterilmektedir (Akalın ve Uluyol, 2016).

Tablo 1. Yıllara Göre Toplam Mobil Cihaz ve Toplam Kullanıcı Sayıları

	2014	**2015**	**2016**	**2017**	**2018**
Toplam Mobil Cihaz Kullanıcısı Sayısı	5,674	5,808	5,945	6,085	6,228
Toplam Mobil Cihaz Sayısı	7,733	8,627	9,628	10,825	12,165

Mobil uygulamalar aracılığı ile kullanıcılara ait bu denli kritik verilere erişilebiliyor olması saldırganların iştahını kabartmış, mobil cihazlara yönelik farklı yeteneklerde zararlı yazılımların geliştirilmesinde artışa sebep vermiştir. Saldırganlar geliştirmiş oldukları zararlı yazılımları, kullanıcıların mobil cihazlarına bulaştırabilmek için bilinen klasik sosyal mühendislik yöntemlerini kullanmışlardır. Saldırganlar gerçekleştirdikleri sosyal mühendislik saldırılarında kullanıcılara, tıklandığında zararlı yazılımın sisteme indirilmesine neden olan URL'ler içeren oltalama mailleri göndermişlerdir. Fakat günümüzde kullanıcıların oltalama maillerine karşı geçmişe göre nispeten daha bilinçli olmaları nedeniyle saldırganlar yeni yöntem arayışına girmişlerdir. Saldırganlar Google Playstore' da yer alan uygulamalara ait dosyaların içerisine geliştirmiş oldukları zararlı yazılımları enjekte ettikten sonra, söz konusu uygulamaları kendi web sitelerinde "ücretsiz API" adı altında paylaşmışlardır. Google Play içerisinde ücretli olarak sunulan uygulamaları, ücretsiz olarak söz konusu web sitelerinden indiren kullanıcılar, ilgili uygulamaların içerisine enjekte edilen zararlı yazılıma maruz kalmaktalardır. Gerçekleştirilen bu çalışmada, günümüz siber dünyasında saldırganların kurban mobil cihazlara zararlı yazılım bulaştırabilmek amacıyla mobil uygulamaları kullanmaları incelenmiştir. II. Bölümde zararlı yazılım türleri sıralanmış ve söz konusu zararlı yazılımlar davranışsal olarak incelenmiştir. III. Bölümde geçmişten günümüze kadar zararlı yazılımların mobil cihazlara bulaştırılması amacıyla saldırganlar tarafından izlenen politikalar incelenmiştir. IV. Bölümde günümüz mobil cihaz kullanıcıları arasında en popüler uygulamalardan biri olan Pokemon GO uygulamasının Google Play dışında internet sitelerinden elde edilen API dosyası üzerinde gerçekleştirilen malware analiz işlemi anlatılmış ve elde edilen sonuçlar detaylı olarak paylaşılmıştır. Gerçekleştirilen çalışma elde edilen sonuçların paylaşılması ile tamamlanmıştır.

MALWARE TÜRLERİ

Günümüzde mobil uygulamalar üzerinde farklı amaçları gerçekleştirebilmek adına saldırganlar tarafından geliştirilmiş farklı türde zararlı yazılımlar bulunmaktadır.

Söz konusu zararlı yazılımlara verilebilecek ilk örnek bilgi hırsızlığı amacı ile geliştirilmiş olan malware'lardır. Söz konusu zararlı yazılımlar bulaştıkları sisteme zarar vermek yerine söz konusu sistem üzerinden bilgi toplamayı amaçlamaktadır. Bu tip zararlılara örnek olarak keyloggerlar, bilgisayardan önemli parolaları toplayan zararlı yazılımlar ve ağ içerisindeki trafiği dinleyerek veri kaçıran zararlılar örnek gösterilebilmektedir.

Saldırganlar tarafından geliştirilen bir diğer malware türü ise, zararlı yazılım yükleyicilerdir. Söz konusu malwarelar bulaştıkları sisteme saldırganlar tarafından belirlenmiş diğer bir zararlı yazılımın indirilmesi için kullanılmaktadır. Bu malware türü çoğunlukla sisteme erişim hakkı kazanan saldırganlar tarafından yüklenmektedir.

Arka kapılar (backdoor) bir sisteme erişim sağlayan bir saldırgan tarafından, söz konusu sisteme istenildiği zaman erişim sağlanabilmesi amacı ile kullanılmaktadır.

Saldırganlar tarafından kullanılan bir diğer malware türü Botnet' lerdir. Botnetler, arka kapılar ile görev itibarıyla benzerlik göstermektedir. Ancak botnetleri, arka kapılardan ayıran en temel özellik, tek bir komuta merkezinden ele geçirilen tüm sistemlerin eş zamanlı olarak aynı görev için kullanılabilmesidir.

Launcher isimli zararlı yazılımlar ise, bulaşmış oldukları sistemler üzerinde diğer zararlı yazılımların başlatılması için kullanılmaktadır. Söz konusu zararlı yazılımlar gizli olmayı ve hedef alınan sisteme daha kalıcı erişim sağlamayı amaçlayan saldırganlar tarafından yayılma stratejisi olarak kullanılmaktadır.

Rootkitler hedef alınan sistem üzerinde çalışmakta olan zararlı yazılımların varlığının gizlenmesi amacıyla tasarlanmış zararlı yazılımlardır. Saldırganlar tarafından kullanılan son malware türü ise solucanlardır. Solucanlar bulaşmış oldukları sistem içerisinde kendilerini farklı noktalara ya da aynı networkte yer alan bir başka bilgisayara kopyalama yeteneğine sahiptir.

ZARARLI YAZILIMLARIN YAYILMA STRATEJİLERİ

Saldırganlar geliştirmiş oldukları zararlı yazılımları hedef aldıkları sistemlere bulaştırmak amacıyla farklı stratejiler uygulamaktadırlar. Bu stratejiler;

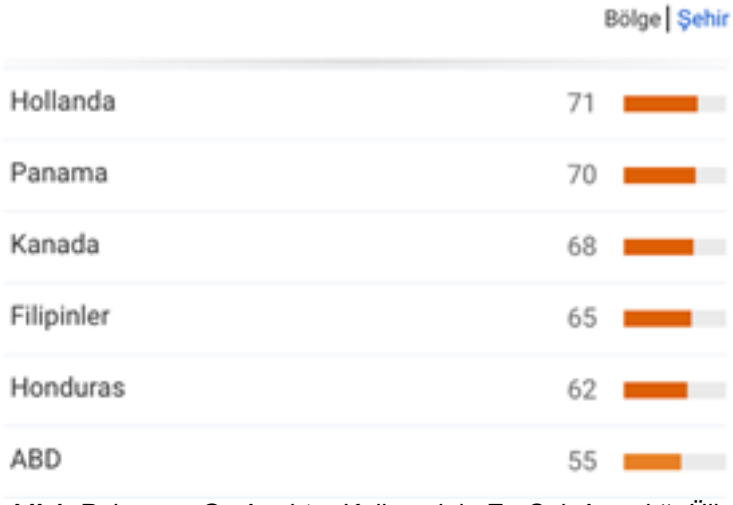
1) E-mail vektörü tabanlı yayılma teknikleri
   a) Oltalama (phishing) mailleri
   b) Sahte URL içeren mailler
   c) Zararlı ek dosyalar (zip, apk dosyaları vb.) içeren mailler
2) Web vektörü tabanlı yayılma teknikleri
   a) Web üzerinden yayılan exploit kitler
   b) Tarayıcı (browser) istismarı
   c) DNS yönlendirme
3) Diğer yayılma vektörleri
   a) Sosyal mühendislik saldırıları
   b) İşletim sistemlerinin istismarı
   c) Donanımsal saldırı cihazları olarak grup ve alt gruplara ayrılmaktadır.

Mobil cihazların kullanımının gün geçtikçe artması saldırganları, söz konusu cihaz kullanıcılarına yönelik farklı stratejiler geliştirmeye itmiştir. Günümüzde saldırganlar tarafından mobil cihazlara yönelik olarak kullanılmakta olan en temel strateji, mobil uygulama APK' larının içerisine zararlı yazılımların eklenmesidir. Çoğunlukla uygulama marketinde yer alan ücretli yazılımların APK dosyaları içerisine zararlı yazılımı enjekte eden saldırganlar, söz konusu uygulama APK' sını "ücretsiz" adı altında internet ortamında paylaşmaktadır. Markette ücretli olan bir uygulamanın, internet üzerinden ücretsiz olduğunu gören kullanıcılar, insan doğası gereği söz konusu APK dosyalarını mobil cihazlarına indirmekte ve çalıştırmaktadır. Zararlı yazılım enjekte edilmiş APK dosyasının mobil cihaz üzerinde çalıştırılması sonrasında söz konusu zararlı yazılım ilgili mobil cihaza bulaşmakta ve saldırgana hizmet

vermeye hazır duruma gelmektedir. Bu çalışmanın bir sonraki bölümünde günümüz mobil oyunları içerisinde en popüler uygulamalardan biri olan Pokemon GO uygulaması ve içerisine enjekte edilmiş Droidjack malware' ı analiz edilmiştir.

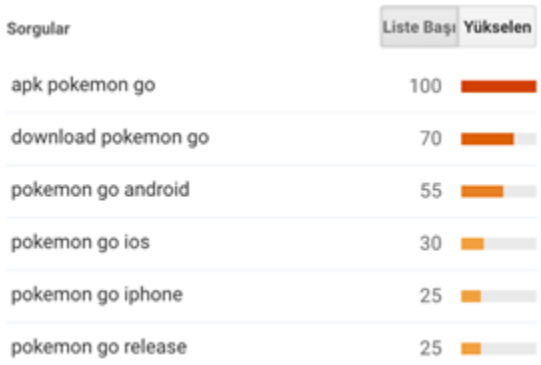
POKEMON GO MOBİL UYGULAMASININ ANALİZ EDİLMESİ

Pokémon GO Niantic firması tarafından geliştirilen ve The Pokémon Company tarafından yayımlanan, iOS ve Android tabanlı bir artırılmış gerçeklik oyunudur (Anderton,2016). Pokemon GO uygulaması Google Play üzerinde Latin Amerika, Avustralya, Belçika, Kanada, Almanya, İspanya, Fransa, İtalya, Hollanda, Portekiz, Rusya, Birleşik Krallık, İrlanda ve Amerika Birleşik Devletleri' nde yaşayan mobil kullanıcılar tarafından indirilip kullanılabilmektedir. Diğer dünya ülkeleri üzerinde yer alan kullanıcıların ise söz konusu uygulamayı kullanabilmeleri için Google Play dışında, internet üzerinde yer alan uygulamaya ait APK dosyasını indirmeleri ve yüklemeleri gerekmektedir. İnternet üzerinde güvenilir olmayan kaynaklarda yer alan bu APK dosyaları içerisinde zararlı yazılım enjekte eden saldırganlar, kullanıcıların söz konusu uygulamaya olan ilgilerini, onlara karşı kullanmaktalardır. Şekil 1' de "Pokemon Go" anahtar kelimesinin en çok arandığı ülkeler listelenmektedir.



Şekil 1. Pokemon Go Anahtar Kelimesinin En Çok Arandığı Ülkeler

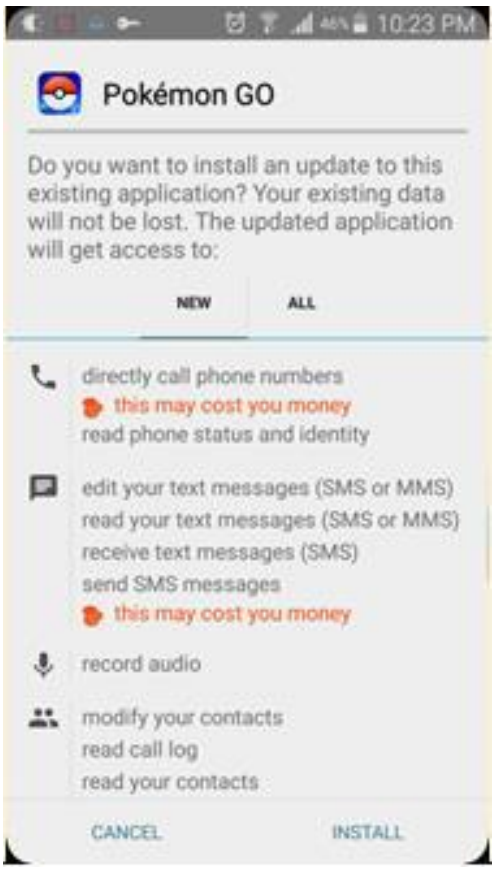
Listelenen ülkeler içerisinde Panama, Filipinler ve Honduras' da Pokemon Go uygulaması Google Play' den indirilememektedir. Dolayısıyla söz konusu ülkedeki kullanıcılar ilgili uygulamayı güvenilir olmayan kaynaklardan indirmektedir. Bir başka Google Trend verisi ise içerisinde "Pokemon go" ifadesi içeren Google aramalarıdır. Şekil 2' de söz konusu araştırmaya ait Google Trend verileri gösterilmektedir.



Şekil 2. Pokemon Go Anahtar Kelimesi Kullanılarak Yapılan Aramalar

Şekil 2' de gösterilmekte olan Google Trend verileri incelendiğine, içerisinde "Pokemon go" ifadesini içeren aramaların büyük çoğunluğu söz konusu uygulamaya ait APK dosyasının indirilmesi amacıyla gerçekleştirilmiştir. İlgili veriler, Google Play dışında yer alan APK dosyası içerisinde zararlı yazılım olduğu varsayılırsa, söz konusu zararlı yazılımın ne kadar geniş kitlelere yayıldığını göstermektedir.

Gerçekleştirilen çalışmada, Google Trend verilerinin incelenmesinden sonra, söz konusu APK dosyası indirilerek laboratuvar ortamında çalıştırılmıştır. İlk olarak söz konusu uygulamanın yüklenmesi sırasında erişim izni istediği noktalar incelenmiştir. Şekil 3' te ilgili APK' nın yüklenmesi sırasında istediği erişim izinleri gösterilmektedir.



Şekil 3. Zararlı Pokemon Go Uygulamasının Kurulum Esnasında İstediği İzinler

Söz konusu zararlı yazılım tarafından istenen izinler incelendiğinde doğrudan farklı numaraların aranması, SMS ve MMS mesajlarının okunması, değiştirilmesi ve alınması, SMS mesajı gönderilebilmesi, ses kaydı yapılabilmesi, rehberde yer alan kişilerin görüntülenmesi ve değiştirilmesi ve son olarak da arama geçmişinin okunabilmesidir. Söz konusu izinler incelendiğinde, güvenilir bir uygulama tarafından istenmeyen, kuşku uyandırıcı izinler olduğu görülmektedir.

Bu çalışma kapsamında gerçekleştirilen malware analiz işleminde sırası ile Apktool, Dex2Jar, MOBSF, Jd-gui ve Androguard analiz araçları kullanılmıştır. Gerçekleştirilen analizler kapsamında ilk olarak ilgili uygulama Dex2jar aracı ile açılarak .jar uzantılı dosyası elde edilmiştir. Söz konusu .jar uzantılı dosya daha sonra Jd-gui aracı ile incelendiğinde, güvenilir kaynaklardan indirilmeyen Pokemon Go uygulaması içerisinde Droidjack adlı bir zararlı yazılımın belirtileri gözlemlenmiştir. Jd-gui aracından elde edilen ekran görüntüsü Şekil 4' te gösterilmektedir.

Şekil 4. Jd-gui Aracı İle Pokemon Go Uygulamasından Elde Edilen .jar Dosyasının İncelenmesi

Gerçekleştirilen analiz işlemlerine Apktool aracı ile devam edilmiştir. Söz konusu araç kullanılarak Pokemon Go uygulaması decompile edilerek kaynak kodlarına erişim sağlanmıştır. Uygulama içerisinde yer akan "AndroidManifest.xml" dosyası incelendiğinde Droidjack yazılımının, Pokemon go yazılımına ek olarak bir takım izinlerin istendiği görülmüştür.

Apktool aracı kullanılarak belirlenen, Droidjack zararlı yazılımının istediği izinler;
- 'android.permission.READ_SMS',
- 'android.permission.RECEIVE_SMS',
- 'android.permission.RECORD_AUDIO',
- 'android.permission.ACCESS_WIFI_STATE',
- 'android.permission.READ_PHONE_STATE',
- 'android.permission.WRITE_SMS',
- 'android.permission.WRITE_CONTACTS',
- 'android.permission.READ_CONTACTS',
- 'android.permission.SEND_SMS',
- 'android.permission.READ_CALL_LOG',
- 'android.permission.WRITE_CALL_LOG',
- 'com.android.browser.permission.READ_HISTORY_BOOKMARKS',
- 'android.permission.RECEIVE_BOOT_COMPLETED',
- 'android.permission.CALL_PHONE',
- 'android.permission.GET_TASKS',
- 'android.permission.CHANGE_NETWORK_STATE',
- 'android.permission.CHANGE_WIFI_STATE' şeklindedir.

Söz konusu zararlı yazılım tarafından istenen izinler incelendiğinde, cihazın wifi, ağ durumunun değiştirilmesinden, sms alıp okuma, gönderme gibi işlemler bulunmaktadır.

Gerçekleştirilen analiz işlemlerine, Apktool aracı kullanılarak uygulama kaynak kodlarının analiz edilmesi ile devam edilmiştir. Şekil 5' te Droidjack zararlı yazılımına ait bir kaynak kod parçası gösterilmektedir.

```
package net.droidjack.server;

public class br
{
  protected static String a = "pokemon.no-ip.org";
  protected static int b = 1337;
  protected static byte c = -1;
}
```

Şekil 5. Droidjack Zararlı Yazılımına Ait Kaynak Kodları

Şekil 5' te gösterilmekte olan kaynak kodlar incelendiğinde, mobil sisteme bulaşmış Droidjack yazılımı, söz konusu kodda gösterilmekte olan hostun ilgili portuna bağlantı gerçekleştirmektedir. Bu bilgilerden sonra Apktool aracı kullanılarak zararlı yazılıma ait kaynak kodların analiz edilmesi işlemine devam edilmiştir. Şekil 6' da Droidjack yazılıma ait bir başka kaynak kod parçacığı gösterilmektedir.

```
private static boolean c()
{
  try
  {
    boolean bool = new File("/system/app/Superuser.apk").exists();
    return bool;
  }
  catch (Exception localException) {}
  return false;
```

Şekil 6. Droidjack Zararlı Yazılımına Ait Kaynak Kodları

Şekil 6' da gösterilmekte olan kaynak kodlar incelendiğinde, Droidjack zararlı yazılımı sisteme bulaşıp Şekil 5' te gösterilen host ile bağlantı kurduktan sonra ilk olarak bulaşmış olduğu mobil cihazın root erişiminin olup olmadığını kontrol etmektedir. Söz konusu zararlı yazılım root yetkisine erişmesi halinde gerçekleştirebileceği eylemlerde artış meydana gelmektedir. Gerçekleştirilen çalışma kaynak kodların analiz edilmesi işlemi ile devam etmiştir. Şekil 7' de Droidjack zararlı yazılımına ait bir başka kaynak kod parçası gösterilmektedir. Şekil 7' de gösterilmekte olan kaynak kodlar incelendiğinde Droidjack yazılımı sisteme bulaştıktan sonra üretici, model, versiyon bilgilerini "http://droidjack.net/storeReport.php" adresine göndermektedir. Bu işlem sayesinde zararlı yazılım bulaştığı sistem hakkında saldırganı bilgilendirmektedir.

Saldırgan Droidjack tarafından aldığı bilgilere göre kullanacağı exploitleri ve gerçekleştireceği işlemleri seçebilmektedir.

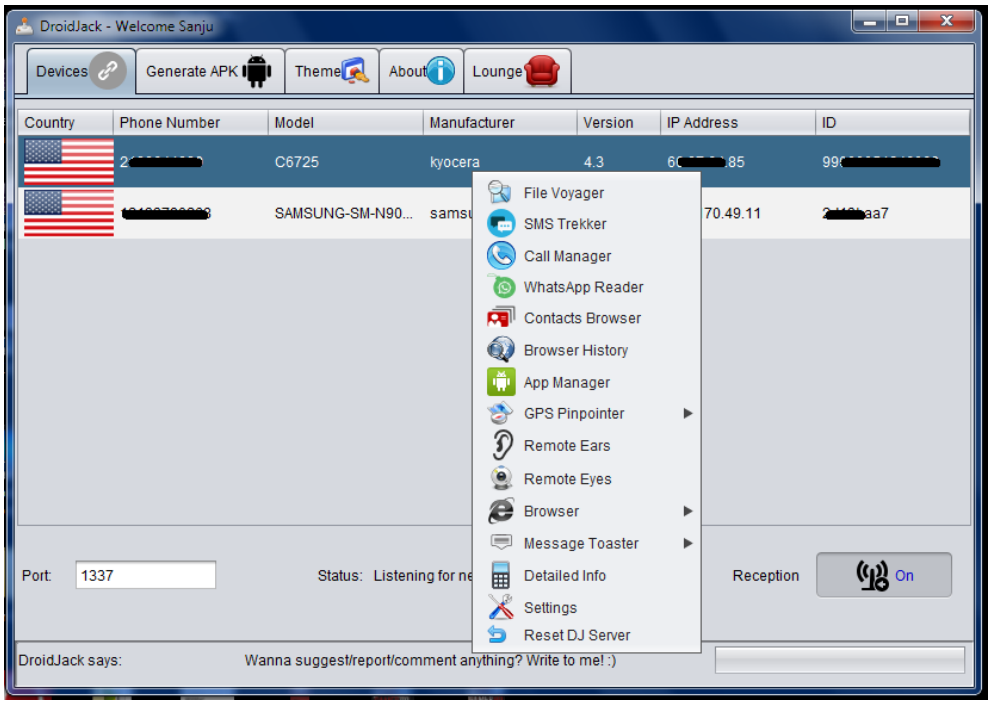
```
StringWriter localStringWriter = new StringWriter();
paramThrowable.printStackTrace(new PrintWriter(localStringWriter));
String str1 = localStringWriter.toString();
ArrayList localArrayList = new ArrayList();
DefaultHttpClient localDefaultHttpClient = new DefaultHttpClient();
HttpPost localHttpPost = new HttpPost("http://www.droidjack.net/storeReport.php");
localArrayList.clear();
String str2 = Build.BRAND;
String str3 = Build.MODEL;
String str4 = Build.VERSION.RELEASE;
localArrayList.add(new BasicNameValuePair("manufacturer", str2));
localArrayList.add(new BasicNameValuePair("model", str3));
localArrayList.add(new BasicNameValuePair("version", str4));
localArrayList.add(new BasicNameValuePair("stacktrace", str1));
localHttpPost.setEntity(new UrlEncodedFormEntity(localArrayList));
localDefaultHttpClient.execute(localHttpPost);
return;
```

Şekil 7. Droidjack Zararlı Yazılımına Ait Kaynak Kodları

Droidjack yazılımına ait kaynak kodları incelendiğinde bulaştığı android cihazın uzaktan kontrol edilmesi amacıyla kullanılan bir zararlı yazılım olduğu görülmüştür. Droidjack aracı kullanarak saldırganlar mobil cihazlar üzerinde

- SMS' lerin yönetilmesi,
- Cihaz üzerinde yer alan dosyaların yönetilmesi,
- Arama kayıtlarına doğrudan erişim sağlanması
- Kişi rehberinin yönetilmesi,
- Ön ve arka kamera aracılığı ile fotoğraf ve video çekilmesi,
- İnternet tarayıcının yönetilerek tarama geçmişinin listelenmesi
- İstenilen bir web ardesinin tarayıcı aracılığı ile açılması
- Cihazın GPS' inin aktifleştirilerek lokasyon bilgisinin alınması
- Cihaza ait IME, MAC adresi gibi bilgilerin çalınması işlemlerini gerçekleştirebilmektelerdir.

Şekil 8' de Droidjack zararlı yazılımının kontrol paneli gösterilmektedir. Saldırganlar söz konusu kullanıcı ara yüzü sayesinde çok çeşitli saldırıları kolaylıkla gerçekleştirebilmektedir.



Şekil 8. Droidjack zararlı yazılımı kontrol paneli (Cluley, 2015)

SON KULLANICI ODAKLI SAVUNMA ÖNERİLERİ

Günümüzde mobil cihazların tüm alanlarda etkin olarak kullanılması, söz konusu cihazları saldırganlar tarafından kullanılan en önemli saldırı vektörlerinden biri haline getirmiştir. Saldırganlar mobil cihazları hedef almak amacıyla bilinen en popüler uygulamalara ait APK dosyalarının içerisine zararlı yazılım enjekte etmekte ve bu zararlı yazılımların mobil cihazlara bulaşmasıyla hedeflerine ulaşmaktadırlar. Söz konusu saldırılara karşı mobil cihaz kullanıcılarının dikkat etmesi gereken bir takım işlemler bulunmaktadır. Günümüz mobil cihazlarında bilinmeyen kaynaklardan uygulama kurulmasını önlemek amacıyla bir güvenlik önlemi varsayılan olarak aktiftir. Kullanıcıların bilinmeyen kaynaklardan uygulama kurmak amacıyla bu güvenlik önlemini pasifleştirmemesi gerekmektedir.

Mobil cihazlarda yer alan USB hata ayıklama seçeneği çoğunlukla uygulama geliştiricileri tarafından mobil cihazlara yazılım yüklemelerinde kullanılmaktadır. Yazılım geliştirme amacı gütmeyen kullanıcıların USB hata ayıklama seçeneğini pasifleştirmesi gerekmektedir.

Kullanıcıların ayrıca cihazlarına mobil uygulama yükleme esnasında, uygulama tarafından istenen erişim izinlerine dikkat etmesi gerekmektedir. Kullanıcılar, uygulamalar tarafından kullanılan standart izinler dışında herhangi bir izin talebi ile karşılaşırsa, söz konusu uygulamaların güvenilir olduğuna emin olana kadar uygulamaları yüklememeleri gerekmektedir.

Google Play içerisinde yer alan uygulamalar içerisinde zararlı yazılım bulunma ihtimallerine taranmaktadır. Bu nedenle Google Play dışında bir kaynaktan yüklenen uygulamalar içerisinde zararlı yazılım olma ihtimali yüksektir.

Bu nedenle mobil cihaz kullanıcıları, uygulama yükleme için sadece Google Play' i tercih etmeli, bunun dışında internet üzerinde yayınlanan uygulama APK' larını kullanmamalılardır.

SONUÇLAR

Günümüz teknoloji dünyasında mobil cihazlar yavaş yavaş bilgisayarların yerini almaya başlamıştır. Mobil cihazlar sayesinde kullanıcılar, sosyal medya takibi, mail takibi, bankacılık işlemleri, oyun oynama, fotoğraf ve video çekme, film izleme gibi farklı alanlarda birçok işlemi

gerçekleştirebilmektedirler. Mobil cihazların kullanımının bu denli artması, söz konusu cihazların saldırganlar tarafından hedef alınmasına neden olmuştur. Günümüze kadar saldırganlar tarafından bilgisayar sistemlerine yönelik olarak geliştirilen zararlı yazılımlar, günümüzde mobil cihazlar içinde geliştirilmeye başlanmıştır. Saldırganlar mobil cihazlar için geliştirmiş oldukları zararlı yazılımları söz konusu cihazlara bulaştırabilmek için çeşitli yöntemler geliştirmişlerdir. Söz konusu yöntemlerden biri, popüler ya da ücretli uygulamaların içerisine geliştirmiş oldukları zararlı yazılımı ekledikten sonra, uygulama APK' larını internet üzerinde "ücretsiz" adı altında yayınlamaktır. Google Play içerisindeki ücretli bir uygulamayı, ücretsiz olduğu için internet üzerinden indiren kullanıcıların sistemleri, zararlı yazılımlara maruz kalmaktadır. Gerçekleştirilen bu çalışmada, mobil cihazların bilgisayar sistemlerinin yerini alma sürecine değinilmiş ve söz konusu sistemler için saldırganlar tarafından geliştirilen zararlı yazılım türleri listelenmiştir. Gerçekleştirilen çalışma, mobil uygulamalar içerisine zararlı yazılımların gömülmesine en güncel örneklerden biri olan Pokemon Go uygulamasının analiz edilmesi ile devam etmiştir. Analiz edilen Pokemon Go APK' sı içerisinde Droidjack isimli zararlı yazılım tespit edilmiştir. Tespit edilen zararlı yazılım çeşitli malware analiz araçları kullanılarak, istediği izinler, davranışsal olarak yetenekleri ve sistem üzerinde oluşturabileceği hasarlar yönünden incelenmiştir. Çalışmamız, malware yayma amacıyla mobil uygulamaların kullanılmasına yönelik olarak kullanıcılara savunma önerilerinin sunulması ile tamamlanmıştır.

KAYNAKLAR

Akalın, U., Uluyol, Ç. (2016). Mobil Cihazlarda Mobil Cihazlarda Adli İnceleme Ve Süreç Adımları. XVIII. Akademik Bilişim Konferansı, Ocak 30– Şubat 5, 2016, Aydın, Türkiye.

Anderton, K. (2016). Augmented Reality, The Future, And Pokemon Go. https://www.forbes.com/sites/kevinanderton/2016/11/14/augmented-reality-the-future-and-pokemon-go-infographic/#662cef507e98 [Erişim Tarihi: 6 Mayıs 2017].

Cluley, G., (2015), "Using DroidJack to spy on an Android?" http://www.welivesecurity.com/2015/10/30/using-droidjack-spy-android-expect-visit-police/ [Erişim Tarihi: 15 Mayıs 2017]

Ekim, A. (2013). Mobil Cihazlarda Adli Bilişim Ve Malware Analizi. 1st International Symposium on Digital Forensics and Security, May 20- 21, 2013, Elazığ, Turkey.

Schmidt, A., D., et al. (2009). Static Analysis Of Executables For Collaborative Malware Detection On Android. IEEE International Conference on Communication, June 14-18, 2009, Dresden, Germany.