Mobil Cihazlarda Adli Bilişim ve Malware Analizi

Ahmet EKİM

Özet— Akıllı telefonlar artan popülaritesi ve becerileri sonunda, hackerların yeni hedefi olmaya başladı. Milyonları aşan mobil uygulamalar hayatımıza kolaylık, eğlence ve heyecan katarken bir yandan da ciddi güvenlik tehditleri getirmiş durumda. İndirdiğiniz basit bir uygulamayla dahi cihazımıza bulaşabilen bu zararlı yazılımlar bazen bir mailin ekiyle bazen de bir bağlantıyı tıkladığınızda indirilen bir dosya ile sisteme efekte olabilmektedir. Bu bildiride adli bilişim donanım ve yazılımlarıyla mobil cihazlarda malware analizi yapılacaktır.

***Anahtar kelimeler*—Akıllı telefon, zararlı yazılım, enfekt olma**

Abstract— Smart phones at the end of the growing popularity, started to become new target of hackers. In excess of millions of mobile applications, while adding fun and excitement, on the other hand is brought serious security threats. The malicious software can infect the phone when you download a small application or a mail attachment. This paper will be performed malware analysis on mobile phones with forensic hardware and software.

Keywords— Smart phones, malicious software, infect

I. GİRİŞ

İngilizce orijinal ismi Computer Forensics olan adli bilişim, içerisinde sayısal bilgi barındıran her türlü elektronik cihazda sayısal delilin araştırılması ve değerlendirilmesi ile ilgilenir.

Adli bilişim özel inceleme ve analiz teknikleri kullanılarak, bilgisayarlar başta olmak üzere, tüm elektronik medya üzerinde yer alan potansiyel delillerin toplanması amacıyla, elektronik aygıtların incelenmesi süreci olarak açıklanmaktadır.[1] Bu süreç içerisinde günlük kullanımda önemi tartışılmaz bir hale gelen mobil cihazlarda adli bilişim incelemesi üzerinde duracağız.

Günümüzde mobil cihazlar, konuşmak gibi basit bir iletişim aracı olmanın çok ötesinde bir teknolojiye ulaşmıştır. Bu cihazlar; kızılötesi ve Bluetooth ile başlayan çevre cihazlar ile haberleşme yetileri, kablosuz ağlara bağlanabilmesinden GPS uydu sistemleri ile haberleşmeye kadar vardı. Birçok cep telefonu operatörünün düşündüğünün aksine henüz akıllı telefonlar ile yapılan bankacılık işlemleri beklendiği düzeye ulaşmadı. Ancak bu cihazlar hâlihazırda bir bilgisayarın yapabildiği, aklınıza gelebilecek hemen hemen ne varsa yapabilir duruma ulaştı. O kadar ki web göz atıcıları, mesajlaşma yazılımları ve şirket e-posta sunucularına erişim bu cihazların yapabildiği basit işler arasında görülmeye başlandı. Mobil teknolojinin sağladığı kolaylıklar beraberinde yeni güvenlik riskleri de oluşturmaktadır. Bu riskler, cihazların taşınabilir fiziksel özellikleriyle birlikte kullanım şeklinden kaynaklanabilecek unsurları da kapsamaktadır. [2]

Mobil cihazların artan kapasiteleri ile bir bilgisayarda saklanabilecek tüm verileri artık bu cihazlarda saklamak mümkündür. Son yıllarda, mobil araçların kullanışlılığı ve sundukları çözümlerin özellikleri nedeniyle, geleneksel masaüstü sistemlerden mobil araçlara doğru geçiş hızlanmıştır. Bunun sonucunda mobil araçların kullanımı yaygınlaşmıştır.[3]

Bugün akıllı telefonlarımızdan bankacılık işlemleri, mobil ödeme, mail hesapları ve sosyal medyayı kullanım oranında büyük oranda artış olmuştur. Şirketler çalışanlarınla haberleşmeyi kurdukları eposta sunuculara bağlı akıllı telefonlarla yapmakta, bankalar müşterilerine mobil internet bankacılığına teşvik etmektedir. Bankacılık işlemleri kullanıcının oluşturduğu şifre dışında SMS ile iletilen tek kullanımlık şifrelerle yapılmaktadır.

Zararlı yazılımlar önceleri sadece bilgisayarlar için tehditken şimdilerde mobil cihazlar içinde büyük tehdit oluşturmaktadır. Mobil cihazlara bulaşan bu zararlı yazılımlar tüm rehber bilgisini ele geçirebilmekte, mesajları okuyabilmekte, resim, video ve ses dosyalarına ulaşabilmekte, haberiniz olmadan mesaj gönderebilmekte hatta sizin nerelerde bulunduğunuza dair konum bilgisini kötü niyetli kişilere ulaştırabilmektedir. Zararlı yazılımların yaptığı işler tabiî ki bununla da sınırlı değil. Sisteme bulaşmış olan zararlı yazılımlar, becerisine göre; ikili görüşmeleri anlık dinleme, ortam dinlemesi, internet aktivitelerinin takibi ve en önemlisi de kişisel bilgiler ile birlikte kullanıcı adı ve parolaları da ele geçirebilmektedir. Ele geçirilen bu bilgiler bankaya ait kullanıcı adı ve parolalar ise yaşanan kayıplar daha da büyüyebilmektedir.

Günümüzde işlenen suçların %70'den fazlasında cep telefonları bir şekilde dahil olmaktadır. Böyle bir durumda suçu aydınlatmada mobil cihaz incelemelerinin önemi de artmaktadır. Eski nesil cep telefonlarından rehber, mesaj, multimedia mesaj, gelen giden ve cevapsız aramalar, notlar ve takvim bilgisi gibi sınırlı sayıda bilgi elde edilirken yeni nesil cep telefonlarda bu bilgilere ek olarak video, resim, ses, konum bilgisi, e-postalar, internet geçmişi, internet yazışmaları ve uygulama bilgilileri elde edilebilmektedir.

II. MOBİL ADLİ BİLİŞİME GİRİŞ

Öncelikle mobil cihazlarda adli bilişim inceleme diğer bilişim aygıtlarına oranla daha zor ve meşakkatli olduğunu bilinmelidir. Bunun temel sebepleri arasında;

- Çok sayıda marka ve model mobil cihazın olması,
- Her geçen gün bu cihazlara yenilerinin eklenmesi,
- Geniş işletim sistemi ve firma çeşitliği,
- İnceleme yapılan adli bilişim yazılım ve donanımlarının sürekli güncellemesi,
- Mevcut yazılım ve donanımların bütün telefonları desteklememesi,
- Farklı bağlantı aparatları ve şarj kabloları ile çalışmaları,
- Batarya problemleri
- Her telefonun her veriyi kaydetmemesi,
- Şifreli ve kirptolu mesajlar,
- Güvenlik ve açılış şifreleri gibi belli başlı sorunları söyleyebiliriz.

Bahsedilen bu sebepler dolayı mobil cihazlara özel adli bilişim yazılımları ve donanımları üretildiğini görmek mümkündür. Bu yazılım ve donanımlardan yazının devamında bahsedilecektir.

Mobil Cihazlarda Veri Alanları:

Mobil cihazlar 3 bölümde veri barındırırlar. Bu alanlar, mobil cihazın dahili hafızası, harici hafızası (Hafıza kartı) ve sim karttan oluşmaktadır.

A. Mobil Cihazın Dahili Hafızası:

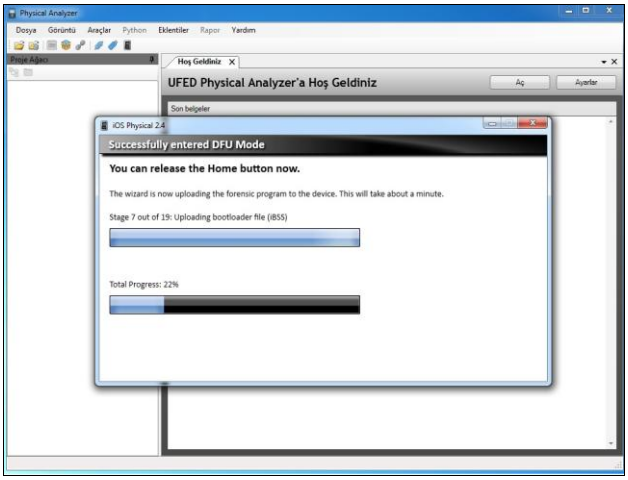
Bu alanda fiziksel ve mantıksal incelemeden bahsedebilir. Mantıksal incelemede cihazın ekranında görüntülenen verileri elde edilebilir. Fiziksel incelemede ise bit bit denilen kopyalama metodu ile cihazın içerinde ki tüm verilere ham haliyle anlamlandırılmamış olarak ulaşılması mümkündür. Bu alanda silinmiş verilerde elde edilebilir.

CelleBrite ile Logical (Mantıksal) İçerik Çıkartma



Şekil 1. CelleBrite cihazı

CelleBrite ile physical (Fiziksel) İçerik Çıkartma



Şekil 2. CelleBrite yazılımı

Mobil Cihazların Dahili Hafızasında Bulunan Veriler:

- Gelen aramalar
- Giden aramalar
- Cevapsız aramalar
- Kişi listesi (kişisel telefon rehberi)
- Metin mesajları (SMS)
- Sohbet kayıtları (IM)
- Fotoğraflar
- Video klipler
- Takvim
- E-postalar
- Özel bir zil sesi (Ayırt edici zil sesi ,bir soruşturmada tanık tarafından hatırlanabilir)
- Yer ve konum bilgisi
- Yüklü Uygulamalar



Şekil 3. Cep Telefonu

B.Bellek kartları (Memory Cards):

Taşınabilir elektronik kayıt araçlarıdır. Karttan güç kesildiğinde dahi bilgilerin kaydedilme riski yoktur. Hatta silinmiş imgelerin bellek kartından tekrar geri kurtarılması mümkündür. Bellek kartları, bazen kredi kartı boyutunda olmalarına rağmen, yüzlerce imgeyi saklayabilmektedirler. Bilgisayarlar, Mobil cihazlar, dijital kameralar ve avuç içi bilgisayarlar gibi birçok farklı aygıtta kullanılmaktadır. [4]

Bellek kartlarında bulunan veriler:

- Metin mesajları
- Anlık mesajlar
- Fotoğraflar
- Videolar
- Ses dosyaları



Şekil 4. Hafıza Kartı

C.Sim Kart:

SIM kart abone bilgilerini taşıyan, operatör ile bağlantı sağlayan akıllı kart olup, mobil cihaz içine takılmaktadır.

Sim kartlarda bulunan veriler:

- Kişi listesi
- Metin mesajları (SMS)
- Gelen aramalar
- Giden aramalar
- Cevapsız aramalar



Şekil 5. Sim kart

Mobil Adli Bilişim Yazılım ve Donanımları:

CelleBrite: Hem donanımsal hem de yazılımsal kullanılabilen ürün fiziksel ve mantıksal çıkarım yapabilmektedir. Kablo desteği sağlamaktadır.

XRY: Yazılımsal kullanılabilen ürün fiziksel ve mantıksal çıkarım yapabilmektedir. Kablo desteği sağlamaktadır.

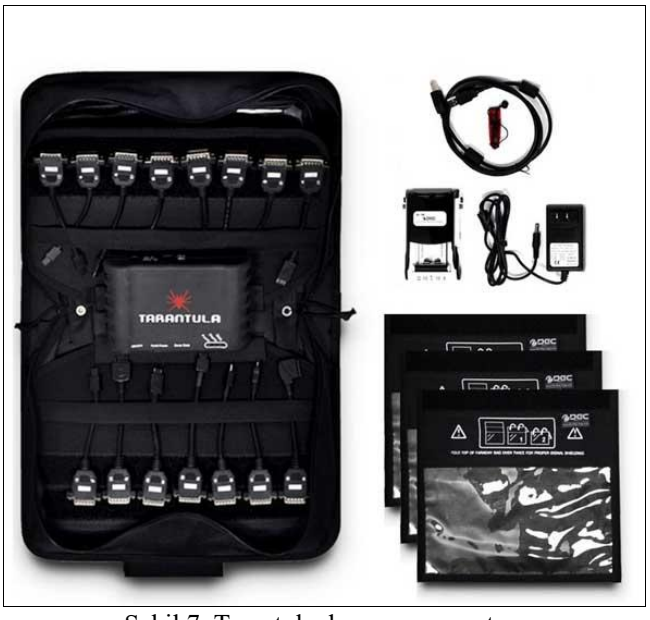


Şekil 6. XRY donanım ve çantası

Paraben: Yazılımsal kullanılabilen ürün fiziksel ve mantıksal çıkarım yapabilmektedir. Kablo desteği sağlamaktadır.

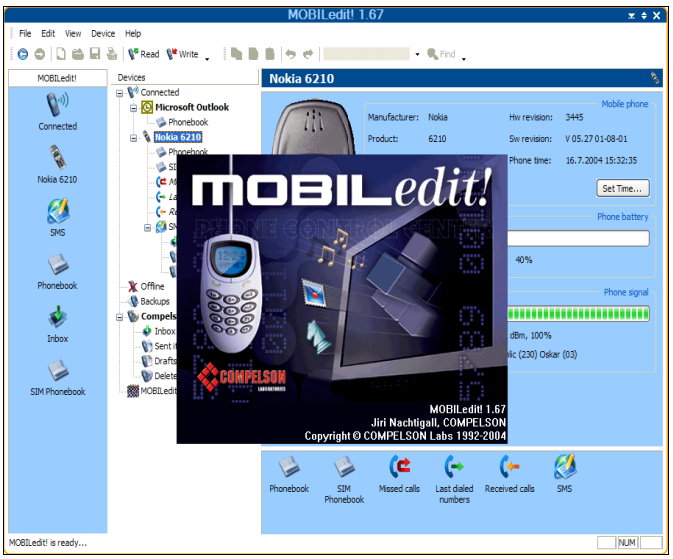
Oxygen: Yazılımsal kullanılabilen ürün fiziksel ve mantıksal çıkarım yapabilmektedir.

Tarantula: Yazılımsal kullanılabilen ürün fiziksel ve mantıksal çıkarım yapabilmektedir. Daha çok Çin malı mobil cihazları desteklemektedir. Kablo desteği sağlamaktadır.



Şekil 7. Tarantula donanım ve çantası

Mobil Edit: Yazılımsal kullanılabilen ürün fiziksel ve mantıksal çıkarım yapabilmektedir. Kablo desteği sağlamaktadır.



Şekil 8. Mobiledit Yazılımı

Flasher Box: Genelde cep telefonu servis ve tamircileri tarafından kullanılan, cep telefonu tamiri, sim ve güvenlik kilitlerini kırmak gibi çeşitli özelliklere sahip cihazlardır. Birden çok marka ve modeli destekleyebilmektedirler. Bu cihazların adli bilişim incelemelerde kullanılması sakınca oluşturabilmektedir. Doğru kullanılmadığında cihazın tüm verilerini silebilir ya da cihaz bir daha çalışmayabilir. Teknik açıdan kullanımı zor ve karmaşıktır. Çıkartılan bilgiler ham verilerdir.



Şekil 9. Flasher Box Cihazı

Faraday çantası

Cep telefonlarının açık kalması gereken durumlarda operatörle iletişimi engelleyen, ortamda bir sinyal kesici varmış gibi cihazın dış dünya ile bağlantısını kesmeye yarayan özel çantadır. Açık bir cep telefonda kapandığında güvenlik kilidi girme gereksinimi varsa bu çanta içerisine muhafaza edilen telefon açık kalabilmektir.



Şekil 10. Faraday Çantası

Mobil Cihazlarda İşletim Sistemleri:

Android:

Android, Google, Open Handset Alliance ve özgür yazılım topluluğu tarafından geliştirilen, Linux tabanlı, mobil cihaz ve cep telefonları için geliştirilmekte olan, açık kaynak kodlu bir mobil işletim sistemidir. Android, aygıtların fonksiyonelliğini genişleten uygulamalar yazan geniş bir geliştirici grubuna sahiptir. Android için halihazırda 250,000'den fazla uygulama bulunmaktadır. Google Play ise, Android işletim sistemi uygulamalarının çeşitli sitelerden indirilebilmesinin yanısıra, Google tarafından işletilen kurumsal uygulama mağazasıdır. Geliştiriciler, ilk olarak aygıtı, Google'ın Java kütüphanesi aracılığıyla kontrol ederek Java dilinde yazmışlardır. [5]

Windows Mobile:

Windows Mobile Microsoft şirketi tarafından PDA ve akıllı telefonlar gibi mobil cihazlar için tasarlanmış olan bir işletim sistemidir. Windows CE çekirdeği üzerine temellendirilmiştir.[6]

BlackBerry OS:

BlackBerryOS, Java tabanlı BlackBerry marka akıllı telefonlar için geliştirilen mobil işletim sistemidir. [7]

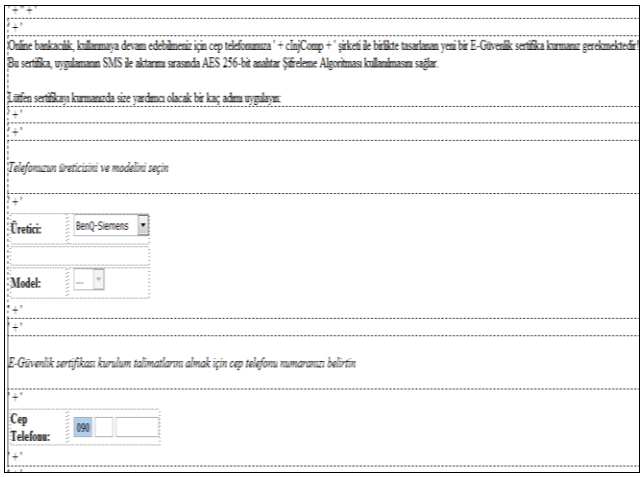
Apple ios:

iOS (eski adıyla iPhone OS) Apple'ın başlangıçta iPhone için geliştirdiği ancak daha sonra iPod Touch ve iPad'de de kullanılan mobil işletim sistemidir. Mac OS X'den türetilmiştir. iOS içinde 4 katman bulundurmaktadır: Core OS tabakası, Core Servisleri tabakası, Medya tabakası ve Cocoa Touch tabakası. Yazılım cihazın içinde 500 MB'lık bir alan kaplamaktadır. [8]

III. MOBİL CİHAZLARDA MALWARE ANALİZİ

Katlanarak büyüyen akıllı telefon kullanıcı sayısı, siber suçlular için cazip bir alan haline gelmektedir. Akıllı telefonlara, casus yazılım veya zararlı kodlar, e-posta eklerindeki bir fotoğrafın açılması, zararlı kod gömülü web sayfasının ziyaret edilmesi, bluetooth bağlantısı, çoklu multimedia mesajları ve mesaj içerisinde gelen bir linkin tıklanması ile bulaşabilmektedir. Siber suçluların akıllı telefonlara zararlı kod bulaştırmadaki en önemli nedenleri arasında bankacılık şifrelerine ulaşma amacı yatmaktadır. Geçmişte hackerlar kullanıcıların bilgisayarlarına sızarak internet bankacılığı bilgilerini (Banka hesap numarası ve kullanıcı şifresi) alabilmekteydi ancak günümüzde internet bankacılığı ve mobil bankacılık işlemleri kullanıcının oluşturduğu şifre dışında SMS ile iletilen tek kullanımlık şifrelerle yapılmaktadır. Hackerler bu şifrelere ulaşmak için zararlı yazılım bulaştırılmış bilgisayardan banka sitelerine girildiğinde, zararlı yazılım tarafından bankanın güvenlik uygulaması olduğunu belirten ancak hackerlara ait olan yeni bir pencere açmaktadır. Kullanıcıdan bu pencereye cep telefonu numarası, cep telefonu marka ve model bilgilerini girmesi istenmektedir. Kullanıcı kendisinden istenilen bu bilgileri ilgili kutucuklara girip formu yolladığında, kullanıcının cep telefonuna bir SMS geliyor ve SMS içerisinde "E-Güvenlik sertifika linkini içeren mesaj aldınız, kuruluma devam etmek için SMS mesajındaki linke tıklayın" şeklinde virüs linkinin olduğu bir mesaj geliyor. Mesaj içeriğindeki bağlantı linkini tıklayarak uygulamayı indiren kullanıcının cep telefonuna zararlı yazılım bulaşmış oluyor. Cep telefonlarına bulaştırılmış zararlı yazılım ile tek kullanımlık SMS şifrelerin farklı bir cep telefonu numarasına iletilmesi sağlanıyor.

Şekil 11'da gösterilen örnekte zararlı yazılım bulaştırılmış bir sistemden kullanıcının banka sitesine erişimi ile zararlı yazılım tarafından bankadan geliyormuş gibi sahte bir mesaj iletisi gösterilmektedir.



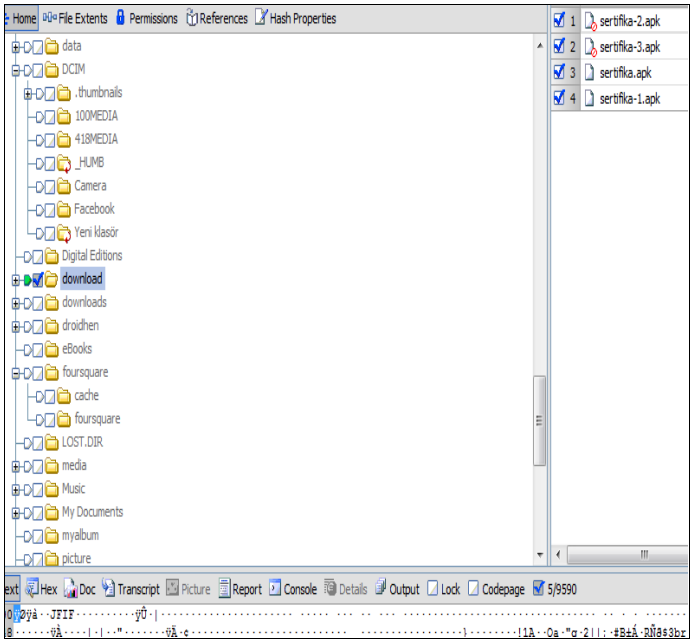
Şekil 11. Zararlı yazılım tarafından kullanıcıya gösterilen sahte ileti

Kullanıcı şekil 11'da gösterilen iletideki bilgileri doldurup gönder butonuna bastığında girmiş olduğu cep telefonuna link içeren bir SMS gelmektedir.



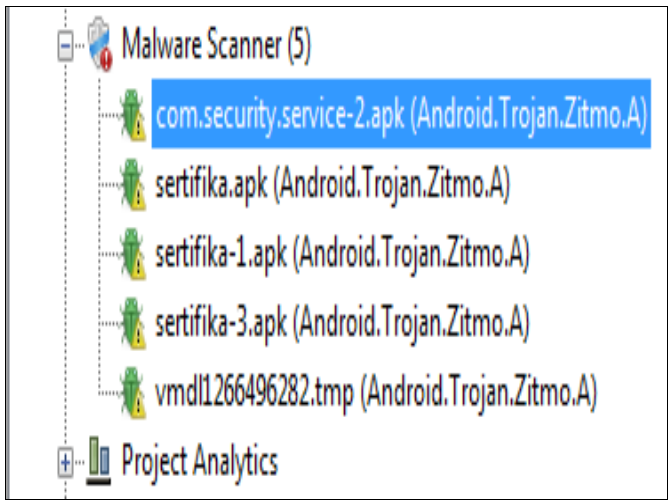
Şekil 12. Cep telefonuna gönderilen zararlı dosya linki içeren SMS

Kullanıcı şekil 12'de gösterilen SMS ile gelen linki tıkladığında zararlı yazılım cep telefonu dahili hafızası yada hafıza kartına inmiş oluyor.



Şekil 13. Cep telefonu bellek kartında zararlı yazılıma ait kayıtlar

Kullanıcıya ait cep telefonun fiziksel çıkarı üzerinde yapılan malware taraması sunucunda sms ile gelen linkte ve bellek kartında bulunan zararlı yazılımın cep telefonun dahili hafızasında da tespit edildiği Şekil 14'de görülmektedir.



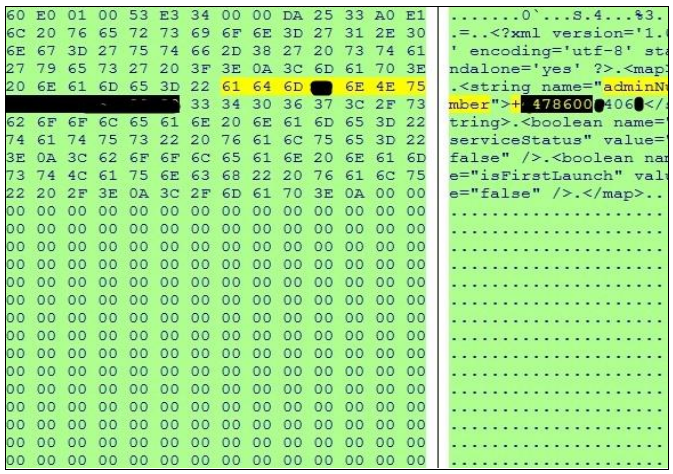
Şekil 14. Cep telefonun fiziksel çıkarımında zararlı yazılıma ait kayıtlar.

Zararlı yazılımın kullanıcıya ait cep telefonunda SMS yazma, gönderme ve alma yetkilerini kullandığı Şekil 15'de görülmektedir.

android.permission.RECEIVE_SMS
android.permission.SEND_SMS
android.permission.WRITE_SMS

Şekil 15. Cep telefonun fiziksel çıkarımında zararlı yazılıma ait kayıtlar.

Zararlı yazılımın kullanıcıya ait cep telefonunda bir numarayı Admin (Yönetici) olarak yetkilendirdiği, bu numaraya kullanıcıya gelen tüm mesajların bir kopyasını gönderdiği Şekil 16'da görülmektedir.



Şekil 15. Zararlı yazılımın atadığı admin numarası

IV. SONUÇ VE ÖNERİLER

Bilişim teknolojilerinin sağladığı kolaylıklar beraberinde yeni güvenlik riskleri de getirmiştir. Özellikle mobil teknolojinin gün geçtikçe artmasıyla birlikte, bu alandaki suçlarda da çok büyük artışlar görülmektedir. Teknoloji ve saldırganların artan becerileri suçu ve suçluyu tespit edilebilmede bu alanda yetiştirilmiş özel uzman personel ihtiyacını arttırmıştır. Çoğu akıllı telefonda özel donanım ve yazılım kullanılmadan kötü amaçlı yazılım tespit etmek neredeyse imkânsızdır. Bu donanım ve yazılımlar maliyet açısından pahalı, kullanımı açısından da son derece karmaşık ve zordur. Uzman sayısı arttırmak amacıyla eğitim programları, özel ekipmanlar ve laboratuar ortamları kurulmalıdır.

Topluma mobil cihazların karşı karşıya olduğu tehditler yeterli seviyede anlatılmalı, farkındalık oluşturulmalı, alınacak önlemler hakkında bilgi verilmelidir. Bu teknolojileri alt yapılarında kullanan firmaların gerekli güvenlik önlemlerini alması sağlanmalıdır.

KAYNAKLAR

[1] Keser Berber, Adli Bilişim, CMK md 134 ve Düşündürdükler, http://www.leylakeser.org/2008/07/adli-biliim-cmk-md-134-ve-dndrdkleri.html

[2] Mobil Cihazlarda Güvenlik Farkındalığı, Nisan 2013 http://web.ogm.gov.tr/birimler/merkez/bilgiislem/Dokumanlar/BilgiGuvenligi/Makale/MOBIL_CIHAZLARDA_GUVENLIK_FARKINDALIGI.pdf S.1.

[3] Handorean, R., Sen, R., Hackmann, G. and Roman, G.C., 'Automated code management in ad hoc Networks',http://www.cs.wustl.edu/mobilab/ Publications/ Papers/2004/ 04-17%20 (Automated %20Code%20

[4] KESER BERBER, L.(2004). Adli Bilisim. Ankara, Yetkin Yayınları, s.:58

[5] İnternet: ''Vikipedi Özgür Ansiklopedi'', http://tr.wikipedia .org/wiki/Android, Nisan 2013.

[6] İnternet: ''Vikipedi Özgür Ansiklopedi'',http://tr.wikipedia.org/wiki/Windows_Mobile, Nisan 2013

[7] İnternet: ''Vikipedi Özgür Ansiklopedi'',http://tr.wikipedia.org/wiki/BlackBerry_OS, Nisan 2013.

[8] İnternet: ''Vikipedi Özgür Ansiklopedi'',http://tr.wikipedia.org/wiki/IOS, Nisan 2013. -