Mobil Cihazları Etkileyen Zararlı Yazılımlar ve Korunma Yöntemleri

Assoc. Prof. Dr. Alper AYTEKİN[70]
Arş. Gör. Ahmet AYAZ[71]
Arş. Gör. Fatma TÜMİNÇİN[72]
Eda BEKTAŞ[73]

Özet

Mobil cihazlar günümüzde hayatın olağan bir parçası haline gelmiştir. Çıktığı ilk yıllarda amacı sadece iletişim kurmak olan mobil cihazlar için, arama yapmak, artık basit bir fonksiyondur. Alışverişten banka ödemelerine kadar birçok işlemin kolaylıkla yapılmasını sağlayan bu teknoloji, yanında önemli riskleri de beraberinde getirmektedir. Mobil cihazlar, henüz bilgisayarlar gibi ayrıntılı güvenlik duvarlarına sahip değildirler. Birçok mobil kullanıcısı da bu güvenlik eksiklerini bilmediği için, zararlı yazılımların, bilgisayar korsanlarının hedefi haline gelmektedir. Bu çalışmada mobil cihazlara çeşitli yollarla bulaşan zararlı yazılımlar araştırılmış ve bu yazılımların türleri analiz edilmiştir. Kullanıcıların bu zararlı yazılımlardan ne tür yöntemler ile korunması gerektiği hakkında bilgiler verilmiştir. Mobil cihazların herhangi bir zararlı yazılımın ve bilgisayar korsanının tehdidine maruz kalmaması için alacağı önlemler ve mobil cihazları korumak amacıyla kullanılabilecek uygulamalar hakkında bilgi verilmiştir.

Anahtar kelimler: Mobil cihazlar, Zararlı yazılımlar, Bilgisayar korsanı, Mobil tehditler

Harmful Software Affecting Mobile Devices and Protection Methods

Abstract

Mobile devices have become an ordinary part of life today. For mobile devices whose purpose was only to communicate in the first years of its used, making calls is now a simple function. This technology, which enables easy transactions from shopping to bank payments, brings important risks along with it. Mobile devices do not yet have detailed firewalls, such as computers. Since many mobile users do not know these security gaps, they become the target of malicious software and hackers. In this study, malicious software transmitted to mobile

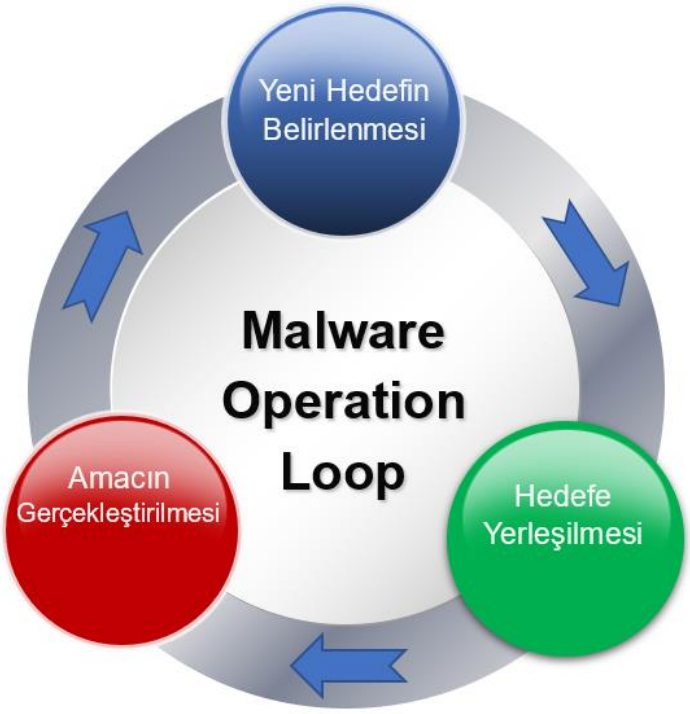
[70] Bartın Üniversitesi İktisadi ve İdari Bilimler Fakültesi, Yönetim Bilişim Sistemleri Bölümü
[71] Bartın Üniversitesi İktisadi ve İdari Bilimler Fakültesi, Yönetim Bilişim Sistemleri Bölümü
[72] Bartın Üniversitesi İktisadi ve İdari Bilimler Fakültesi, Yönetim Bilişim Sistemleri Bölümü
[73] Bartın Üniversitesi İktisadi ve İdari Bilimler Fakültesi, Yönetim Bilişim Sistemleri Bölümü

devices in various ways has been investigated and the types of these software have been analyzed. The users are informed about what methods they should use against this malware. Information is given about the precautions that mobile devices will take to prevent any malicious software and hackers from being threatened and the applications that can be used to protect mobile devices.

Keywords: Mobile devices, Malware, Hacker, Mobile threats

Giriş

Teknoloji çağının yaşanıldığı bu dönemde 7'den 70'e insanlar en az bir mobil cihaza sahipler ve farkında olmadan da olsa birçok tehdidin hedefindedirler. Bu tehditlerin başlıca sebebi zararlı yazılımlardır. Zararlı yazılım ise, bulaştığı sistemde veya cihazda yazılımı yapan kişinin istediği eylemleri gerçekleştirmesi amacıyla hazırlanmış kodlardır (1). Kullanıcı bilinçsizliği, bu hazırlanan yazılımların yanıltıcılığı gibi pek çok sebeplerle onların cihazlarına yerleşir ve onlardan daha fazla yetkiye sahip olurlar. Ana işleyiş 3 aşamalı bir döngü ile açıklanır. İlk olarak zararlı yazılım hedeflenen cihaza ulaşır ve yerleşir. Daha sonra ise bu cihaz üzerinde hedeflediği amacı gerçekleştirir. Son olarak aynı amacı gerçekleştirmek üzere yeni bir hedef belirler.



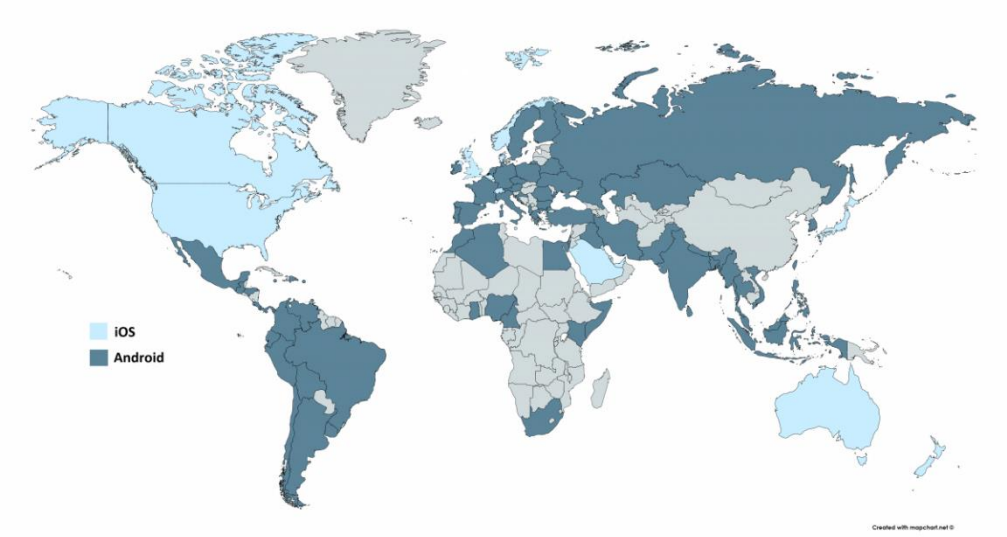
Şekil 1. Zararlı yazılımların işleyiş döngüsü (Malware's operating loop)

Kullanıcıya ait bir cihaz üzerinden, kullanıcının kredi kartı şifresinden adresine kadar bir sürü bilgi elde edilebilir (2). Mobil cihazlara yapılan saldırılarda bu verilere erişimi amaçlanmaktadır. Kullanıcıya ait bu veriler elde edildikten sonra ise saldırganın istediği her türlü amaçta illegal olarak kullanılabilmektedir (3). Bu işlemler sayesinde milyonlarca kullanıcı maddi ve manevi zararlar görür.

Bu sebeple, bu tür zararlarla karşılaşmamak için kullanıcılar bilinçlendirilmeli, tehditler ve çeşitlerinden haberdar olunmalı, sistematik zafiyetler giderilmeli ve bu önlemler saldırılar gerçekleştirilmeden alınmalıdır.

Mobil saldırganların asıl hedefleri işletim sistemi temelinde hazırlanan uygulamalardır. Dünyada en çok kullanılan mobil işletim sistemleri Android ve IOS'tur. %70 kullanım oranı ile Android işletim sistemi birinci sırada yer almaktadır. İkinci sırada ise %28,3 kullanım oranı ile IOS gelmektedir. Diğer işletim sistemleri ise %1,7 kullanım oranına sahiptir (4).

Dünyada ülkelerin IOS ve Android kullanımlarına göre yoğunluğu Şekil 2'de verilmiştir (5).



Şekil 2. Dünyada IOS ve Android Kullanım Yoğunluğu

Bu işletim sistemlerinin mağazalarındaki uygulama sayıları (6) ise; Android uygulamaları: 2,7 milyon, IOS uygulamaları: 2,2 milyon'dur. Gerçekte, uygulama sayıları en iyi ölçüm yöntemi değildir, çünkü çoğu kullanıcı çok az uygulama kullanır ve en popüler olanları her iki platformda da bulunur. Geleneksel olarak, IOS, geliştiriciler için daha kazançlı bir platform olmuştur, bu yüzden yeni uygulamaların ilk önce orada ortaya çıkma eğilimi olmuştur, ancak Android'in pazar payı artmaya devam ettikçe bu değişmektedir.

1. Mobil İşletim Sistemleri Güvenlik Analizi

Uzun zamandır IOS ve Android işletim sistemi karşılaştırmalarında IOS işletim sisteminin daha güvenli olduğu düşünülmektedir. Çünkü Apple'ın işletim sistemi kapalı kaynak kodlu bir sistemdir. Apple kaynak kodunu uygulama geliştiricilere bırakmaz ve iPhone'ların ve iPad'lerin sahipleri telefonlarındaki kodları değiştiremez. Bu, korsanların IOS destekli cihazlarda güvenlik açıkları bulmasını zorlaştırır.

Android cihazlar ise tam aksine açık kaynak kodlu bir sisteme sahiptir. Bu yapı, cihaz sahiplerinin kodlarda değişiklik yapmasına olanak sağlamaktadır. Eğer yeni çıkan bir cihazda güvenlik açığı varsa bunu mobil korsanlar bulabilir ve sisteme kendi isteğince müdahale edebilir.

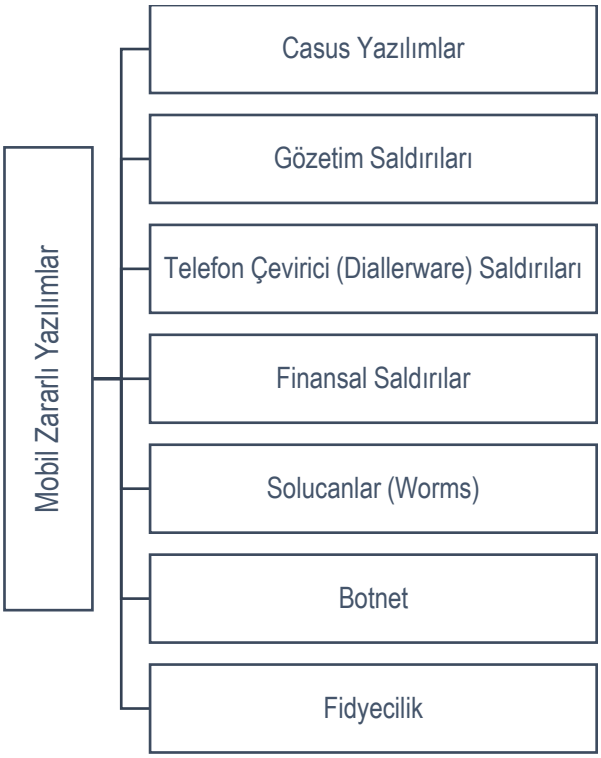
Android işletim sistemi günümüzde daha çok tercih edilen işletim sistemi olduğu için mobil korsanlar tarafından daha sık hedeflenmektedir. Android işletim sisteminin küresel popülaritesi, siber suçlular için daha çekici bir hedef haline gelmesine neden olmaktadır ve buna bağlı olarak da Android cihazlar, bu suçluların gönderdiği kötü amaçlı yazılımların saldırısına daha çok uğramaktadır.

Buradan yapılacak bir çıkarımla IOS daha güvenli olarak kabul edilebilir olsa da, siber suçluların iPhone'lara veya iPad'lere ulaşması imkansız değildir. Hem android hem de IOS cihazlarının sahiplerinin olası kötü amaçlı yazılım/virüslerin farkında olmaları ve üçüncü taraf uygulama mağazalarından uygulama indirirken dikkatli olmaları gerekmektedir. Sattıkları uygulamaları inceleyen Google Play ve Apple App Store gibi güvenilir kaynaklardan uygulamalar indirmek en güvenli yoldur.

Uygulamalar üzerinden yapılan saldırılar dışında, siber suçlular, kullanıcıların oturum açma, banka hesaplarına erişim bilgileri ve diğer kişisel verileri çalmak için çeşitli ikna yöntemleri kullanmaktadırlar. Bu tür saldırılar için birçok sosyal mühendislik içeren yöntemler geliştirmişlerdir. Hangi mobil işletim sistemi olursa olsun hem IOS hem de android bu tür kimlik avı saldırılarına karşı aynı derecede savunmasız olabilir.

2. Mobil Zararlı Yazılımlar

Zararlı yazılımlar genellikle sistemlere izinsiz erişmek ve eriştiği sistemlerden bilgi çalmak için yazılan kodlar veya programlardır. Bu zararlı yazılımların sistemlere erişebilmek için kullandığı birçok teknik vardır ve bu tekniklere göre adlandırılmışlardır (Şekil 2).



Şekil 2. Mobil Zararlı Yazılım Türleri (Types of Mobile Malware)

1.1. Casus Yazılımlar

Kullanıcının haberi olmadan gizlice sisteme erişen ve yerleşen, yerleştiği sistemden gizlice bilgiler toplayan zararlı yazılımlara casus yazılım denir. Casus yazılımlar, solucanlar ve virüsler gibi fazla yayılmaya gerek duymazlar. Casus yazılımın asıl hedefi, sistem içinde kendini gizleyerek istenilen bilgilere erişmektir (7). 2005 yılında FBI tarafından 2000'den fazla şirketle birlikte yapılan bir ankette, katılımcıların %64'ünün casus yazılımlar sebebiyle maddi kayıplar yaşadığı ortaya çıkmıştır. Bu kayıpların yaklaşık 62 milyon dolar olduğu tahmin edilmiştir (8). Mobil cihazlardan bu sitelere erişim sağlanmasıyla yazılımlar mobil cihazlara da yerleşmektedir.

1.2. Gözetim Saldırıları

Mobil cihazlarda var olan kamera, mikrofon, GPS gibi donanımlar kullanılarak kullanıcıların gözetlenmesi ve takibe alınmasıdır. Özel hayatın gizliliğine apaçık bir saldırı olan bu yazılımlar ile birçok insanın günlük hayatta neler yaptığı, kimlerle konuştuğu gibi bilgilere kolayca erişilir, hedef kullanıcının uygunsuz fotoğrafları çekilerek şantaj için kullanılır, mikrofon kullanılarak cihazın bulunduğu ortam dinlenir, GPS verileri kullanılarak hedef kullanıcının telefonunun istenilen zamanda nerde olduğu dinlenir ve zararlı yazılımlar sayesinde bu ve bunun gibi daha birçok eylemde bulunulur. Bu yazılımlar cihaza yerleştikten sonra kendini gizleyerek yakalanma şansını azaltır.

1.3. Telefon Çevirici (Diallerware) Saldırıları

Bu tür saldırılar, sıklıkla uluslararası telefon numaralarını, kurban olarak seçilen bilgisayar modeminin internet sağlayıcısının erişim numarasını değiştirilmesiyle gerçekleşir (9). Kullanıcının yüksek maliyetli SMS ve arama servisleriyle daha fazla ücret ödemesi sağlanmaktadır.

1.4. Finansal Saldırılar

Finansal saldırılar genellikle kredi kart bilgilerini hedef alan, kullanıcının online işlemlerinde bu bilgilere ulaşarak onları sızdıran saldırı çeşididir. Kaspersky Lab'ın 2015 1. çeyrek raporunda en az 29 bankacılık ve finans uygulamasına saldırma becerisine sahip SMS.AndroidOS.OpFake.cc adlı bir Trojan bulduğunu bildirmiştir. Bu Trojan'ın 2. çeyrek raporundaki en yeni sürümü ile 114 (dört kat fazla) bankacılık ve finans uygulamasına saldırma becerisine sahip olduğu belirtilmiştir (10).

1.5. Solucanlar (Worms)

Genelde kullanıcının sistemine e-posta, forum siteleri gibi çeşitli dosyalar ve ağlar üzerinden bulaşan, sisteme girdiklerinde kullanıcının herhangi bir hareketine ihtiyaç duymadan kullanacağı kaynakları bularak kendini kopyalayan ve diğer kullanıcılara çok hızlı bir şekilde ulaşan yazılımlardır.

1.6. Botnet Saldırısı

Bir ana sunucunun zararlı yazılımları bulaştırdığı tüm cihazları kontrol ederek istediği eylemleri yaptırdığı saldırı biçimidir. Zararlı yazılımların bulaştığı cihazlar (botnet) bir siteyi devre dışı bırakmak veya yasa dışı amaçlar için kullanılmak üzere daha tehlikeli eylemlerde kullanılabilirler.

1.7. Fidyecilik

Bu tür saldırılar genellikle bulaştığı cihazın ekranını kilitleyen veya dosyalarını şifreleyen saldırı biçimidir. Saldırgan kullanıcıdan para ister ve bunun karşılığında ekranı serbest bırakacağını veya şifreleri kaldıracağını söyler.

2. Korunma Yöntemleri

Zararlı yazılımların giderek çoğaldığı bu dönemde kullanıcıların artık bilinçlenmesi ve kişisel verilerinin korunması için önemler alması gerekmektedir. Kullanıcıların alacağı önlemler şu şekilde sıralanabilir:

1) Genel güvenlik bilgisine sahip olmak,
2) Anti-virüs programı indirmek,
3) Güvensiz sitelerden cihaza herhangi bir dosya, uygulama, belge indirmemek,
4) İndirilecek uygulamaları orijinal sitelerinden indirmek,
5) Uygulamaları indirirken uygulamanın izinlerine dikkat edip indirmek (11),
6) Şüpheli linklere tıklamamak,
7) Cihaz çalınma riskine karşı uzaktan yedek alma ve sıfırlama yazılımlarını indirmek (11).
8) Açık kablosuz ağlarda hassas bilgilerle ilgili işlemler yapmamak (11),
9) Hesapları için güçlü şifreler oluşturmak (12),
10) Cihazdaki verilerin yedeğini düzenli bir şekilde almak (12),

kullanıcının alacağı önlemler arasındadır.

Kullanıcı dışında aynı zamanda ağ operatörleri de müşterisine güvenilir bir ortam hazırlamalıdır. Operatörlerin gelen ve giden mesajlar için antivirüs yazılımları yüklemesi önemli bir adımdır Bir diğer önlem alması gereken uygulama geliştiriciler, uygulamalarının gerekli güvenlik önlemlerini alması gereklidir. Verilerin ağlardan şifreli gönderilmesi,

uygulama izinlerinin olabildiğince az olması, sadece gerektiğinde veri toplayacak şekilde uygulamalarını geliştirmelidir (11).

Son olarak uygulama marketleri piyasaya sürmeden uygulamaların kodlarını, güvenilirliklerini, zararlı olup olmadığını incelemelidir. Elde ettiği verilere göre uygulamayı piyasaya sürmelidir (13).

Sonuç

Teknoloji devrinin yaşandığı bu dönemde mobil cihazlar evlere hızla yayılmış, çocuğundan yaşlısına her bireyin elinde yer edinmeyi başarmıştır ve donanımları da artmıştır. Artık insanlar fatura ödemelerini, banka işlemlerini, sosyal medya takibini, fotoğraf video çekimlerini tek cihazda gerçekleştirmektedir ve bu da mobil cihazları saldırıların gözdesi haline getirmiştir. Bu çalışmada günümüzde gittikçe daha fazla yetenek kazanan mobil cihazların aynı zamanda kullanıcılarına bir tehdit olmaması için, cihazların yetenekleriyle doğru orantılı büyüyen zararlı yazılımlara hazırlıklı olmalarını sağlayacak bir ortam amaçlanmıştır.

Kötü amaçlı yazılımların hızla artmasıyla birlikte, ağ ve mobil cihazların güvenliğini sağlamak için proaktif yaklaşımlar uygulanmalıdır. Kötü amaçlı yazılımlara karşı algılama ve önlemenin çok önemli olduğu ve ana bilgisayarlardaki güvenlik açıklarından yararlanan yeni değişkenlere karşı mücadele etmek için yeni tekniklerin geliştirilmesi gerektiği açıktır.

Kaynakça

1) Canbek, G. (2005). Klavye dinleme ve önleme sistemleri analiz, tasarım ve geliştirme. *Unpublished master's thesis,* Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Ankara.

2) Su, Q., Tian, J., Chen, X., & Yang, X. (2005). A fingerprint authentication system based on mobile phone. *International Conference on Audio-and Video-Based Biometric Person Authentication* (pp. 151-159). Springer, Berlin, Heidelberg.

3) Shimonski, R., & Zenir, J. (2015). Mobile Phone Tracking. *Cyber Reconnaissance, Surveillance and Defense*, 113-143.

4) Teknoloskop, (2019). "Dünya'da en çok kullanılan mobil işletim sistemleri", https://www.teknoloskop.net/dunyada-en-cok-hangi-sistem-kullaniliyor/

5) DeviceAtlas, (2019). “Android v IOS market share 2019”, https://deviceatlas.com/blog/android-v-IOS-market-share.

6) DigitalTrends, (2019). “Android vs. IOS: Which smartphone platform is the best?”, https://www.digitaltrends.com/mobile/android-vs-IOS/

7) Hansen, J. B. & Young, S. (2003). The Hacker's Handbook, November 24, CRC Press.

8) State of Spyware Report – 2005, Webroot, 2006.

9) Gralla, P. (2002). *The complete idiot's guide to Internet privacy and security*. Penguin.

10) KasperSky, Mobil Zararlı Yazılımlar 2. Çeyrekte 3 Kat Arttı, https://www.kaspersky.com.tr/blog/mobil-zararli-yazilimlar-2-ceyrekte-3-kat-artti/1706/

11) Utku, A., & Doğru, İ. A. (2016). Mobil Kötücül Yazılımlar ve Güvenlik Çözümleri Üzerine Bir İnceleme. *Gazi Üniversitesi Fen Bilimleri Dergisi,* Part C. Tasarım ve Teknoloji, 4 (2), 49-64.

12) Canbek, G., & Sağiroğlu, Ş. (2007). Kötücül ve Casus Yazılımlar: Kapsamlı Bir Araştırma. *Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi, 22* (1).

13) Aydoğan, E. (2014). Genetik Programlama Kullanılarak Mobil Zararlı Yazılımların Otomatik Olarak Üretilmesi.