

FIRAT ÜNİVERSİTESİ
TEKNOLOJİ FAKÜLTESİ
Yazılım Mühendisliği

YMT311 – Bilgi Sistemleri ve Güvenliği Dersi
Proje Uygulaması

Casus Android Uygulaması

Proje Çalışma Grubu

10541511 Mustafa TUFAN

Proje Yürütücüleri

Yrd.Doç.Dr. Resul DAŞ
Arş.Gör. Fatih ÖZKAYNAK

Ocak – 2013

İçindekiler

1. Giriş.....	2
2. Casus Android Uygulamasının Amacı ve Kısa Tanıtımı	2
3. Casus Android Uygulamasının Tanımı ve Genel Özellikleri	2
4. Casus Android Uygulaması Virüs Tanımındaki Hangi Açıklıkları Kullanıyor.....	3
5. Casus Android Uygulaması Çalışmasının Akış Şeması	3
6. Casus Android Uygulaması Çeşitli Antivirüs Yazılımları ile Kontrolü ve Çıktıların Değerlendirilmesi 3	
7. Genel Değerlendirme ve Sonuçlar.....	3
8. Kaynaklar	4

1. Giriş

IDC firmasının yaptığı araştırmaya göre 2015 yılında akıllı telefonlar ve tablet bilgisayarlardan olan internet kullanımı masaüstü ve dizüstü bilgisayarları geride bırakacak.^[1] Bu da basitçe demek oluyor ki mobil sistemlerin güvenliği daha önemli bir pazar haline gelecek. Hali hazırda son kullanıcılar için güvenlik çözümleri sunan antivirüs yazılımları üreten şirketler bu platformlar için çoktan ürünler sunmuş durumda.^{[2][3][4][5]} Hemen hemen Windows için geliştirilmiş başarılı birçok anti-virüs yazılımının Android uygulaması yayınlandı. Bu uygulamalara Google Play Store'dan veya uygulama marketlerinden ulaşılabilir. Bu anti-virüs uygulamalarının var olmasının sebebi, elbette mobil sistemlerde cirit atan kötücül yazılımlar. Özellikle Android'in sicili bu konuda pek temiz değil. iOS geliştirici olmanın biraz zahmetli olması ve iOS cihazlara resmi olarak sadece AppStore'dan uygulama yüklenebilmesi iOS cihazlarda virüs sorununu engelliyor.

2. Casus Android Uygulamasının Amacı ve Kısa Tanıtımı

Uygulamanın sayfası: mustafatufan.com.tr/BilgiGuvenciligi.htm

Uygulamanın amacı kurbanların yerini gizlice bir yere/kişiye bildirmek ve bunu yaparken kısa mesaj servisini gizlice kullanarak kurbanı ekonomik zarara uğratmaktır.

Kısaca casus bir siteden yüklenen uygulamamız kurbanın Android cihazına bulaşıyor, normal kullanılabilir gibi görünen bu uygulama, işini yaparken aynı zamanda da arka planda kötücül faaliyetler yürütüyor.

3. Casus Android Uygulamasının Tanımı ve Genel Özellikleri

Casus Android Uygulaması bir trojan türüdür. Faydalı bir uygulama gibi görünür ancak arka planda cihaza veya kullanıcıya zarar verir.

Trojanlarla taşıdığı ortak özellik olarak kullanıcıyı kandıran bir siteden bulaşır.

mustafatufan.com.tr/BilgiGuvenciligi.htm sayfası, uygulamayı sanki yararlı bir ürün gibi sunan sayfadır.

Buradan uygulamayı indiren kişi kurban oluyor, nerede olduğu bilgisi kısa mesaj servisi ile bir başkasının eline geçiyor.

4. Casus Android Uygulaması Virüs Tanımındaki Hangi Açıklıkları Kullanıyor

Casus Android Uygulaması bir trojan türüdür. Trojanlar yararlı bir yazılımı gibi sisteme girerler ve casusluk etmeye ve sisteme ve de kullanıcıya zarar vermeye başlarlar. Bu projede de casus uygulama sanki bir matematiksel uygulamaymış gibi gözüküp arka planda kullanıcının nerede olduğunu ve bazı parametreleri kısa mesaj servisiyle bir yere/kişiye aktarmaktadır.

5. Casus Android Uygulaması Çalışmasının Akış Şeması

1. Kullanıcı casus siteden casus uygulamayı yükler.
2. Kullanıcı casus uygulamayı kullanır.
3. Kullanıcı uygulamayı kullandığında kullanıcının yer bilgileri kısa mesaj servisi ile belirli kişilerin eline geçer.

6. Casus Android Uygulaması Çeşitli Antivirüs Yazılımları ile Kontrolü ve Çıktıların Değerlendirilmesi

Casus Android Uygulaması bir mobil uygulama olduğundan dolayı herhangi bir mobil antivirüs uygulaması yüklü telefona yüklenememiştir. Mobil uygulamalarda alınması gereken uygulama içi izinlerden dolayı kötücül yazılımlar rahatlıkla tespit edilebilmektedirler.

7. Genel Değerlendirme ve Sonuçlar

Gelecekte biliyoruz ki son kullanıcılar için bilgisayar namına ne varsa mobil teknolojiler üzerinde yürütülecek. Masaüstü ve dizüstü bilgisayarlar yalnızca geliştiriciler arasında kendine yer bulacak. İnsanların %99,9'u bilgisayarla, bilgisayar olduğu için değil, bilgisayarla internete girebildiği, maillerini kontrol edebildiği, oyun oynayabildiği için vakit geçiriyor. Birkaç yıl içinde bunları da en az bilgisayar kadar iyi yapan tabletler çıktığında (Windows RT işletim sistemli Surface gibi) ve bunlar yaygınlaştığında insanların klasik anlamda bilgisayara ihtiyacı kalmayacak. O mobil cihazların mobil uygulamalarıyla da internete girebilecek, maillerini kontrol edebilecek ve oyunlarını oynayabilecekler.

Gelecekteki bu mobil kalabalığın günümüz kullanıcılarından daha iyi korunması gerekiyor. Çünkü bu kalabalık hemen hemen tüm kişisel verilerini bu cihazlar üzerinde tutuyor olacaklar. Bu cihazlar kişiselleştirilmiş olduğu için bir bilgisayardan daha fazla kişisel veri içerecek. Örneğin bugün basitçe birinin telefonunu alıp telefonundan Facebook şifresini değiştirebilirsiniz. Çünkü kimse telefonunda giriş yaptığı herhangi bir hesabı önemsemiyor.

Projemde de bu konuya değindim. Basitçe birinin nerede olduğu bilgisini, SMS'i karşı tarafa ödeterek edindim. Bütün bunlar olurken kullanıcının haberi dahi olmadı. Android'de her yıl buna benzer on binlerce uygulama ortaya çıkıyor ve kullanıcıları bu zararlı uygulamalardan koruyacak sistemler gerekiyor. Google Play Store kesinlikle bu konuda tek başına yetersiz.

8. Kaynaklar

- [1]<http://www.donanimhaber.com/tablet-pc/haberleri/iDC-ABD-capinda-tablet-ve-akilli-telefonlar-internet-kullaniminda-PCleri-2015de-gececek-.htm>
- [2]<https://play.google.com/store/apps/details?id=com.kms.free>
- [3]<https://play.google.com/store/apps/details?id=com.eset.ems>
- [4]<https://play.google.com/store/apps/details?id=com.symantec.mobilesecurity>
- [5]<https://play.google.com/store/apps/details?id=com.wsandroid.suite>