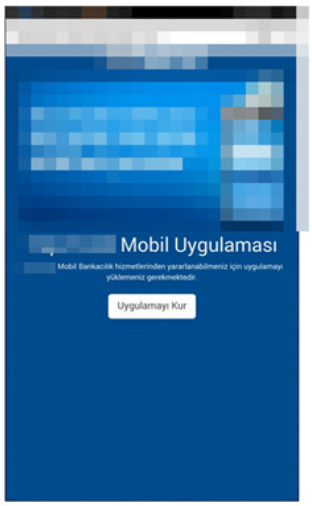
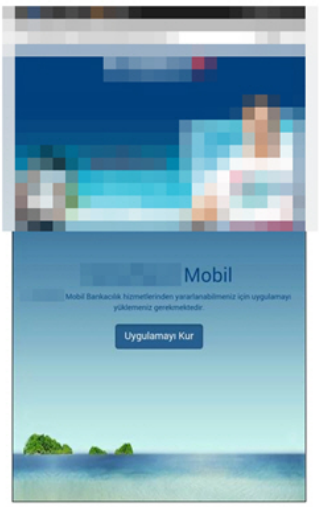
Android Bankacılık Casus Yazılımı

written by Mert SARICA | 5 November 2015

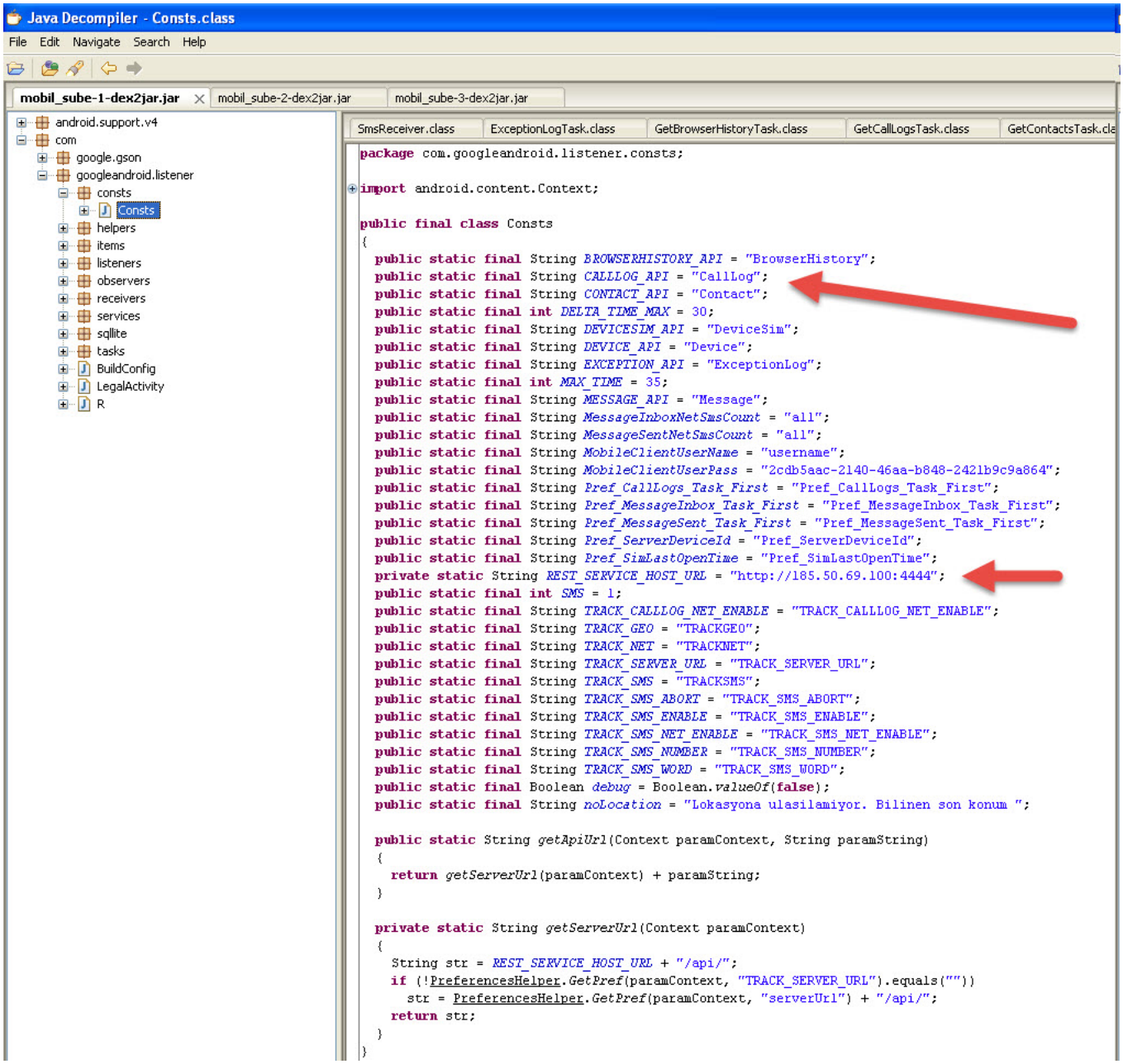
Nisan ayı başı gibi bazı banka müşterilerine SMS ile banka_adi.şüpheli_adres.com adında mesajlar gönderilmeye başlandı. Siteye Android akıllı cihazı ile bağlanan kullanıcıları, bankaya aitmiş gibi görünen güzel bir görsel karşılıyor ve kullanıcının bankanın mobil bankacılık hizmetinden yararlanabilmesi için ilgili uygulamayı kurması isteniyordu.



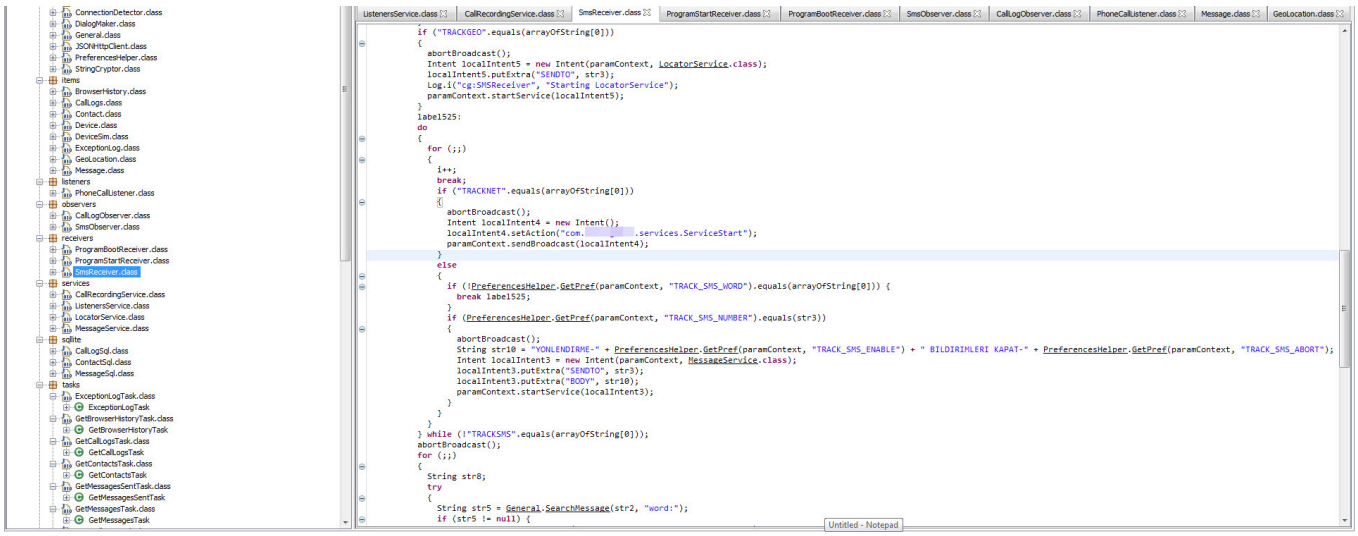


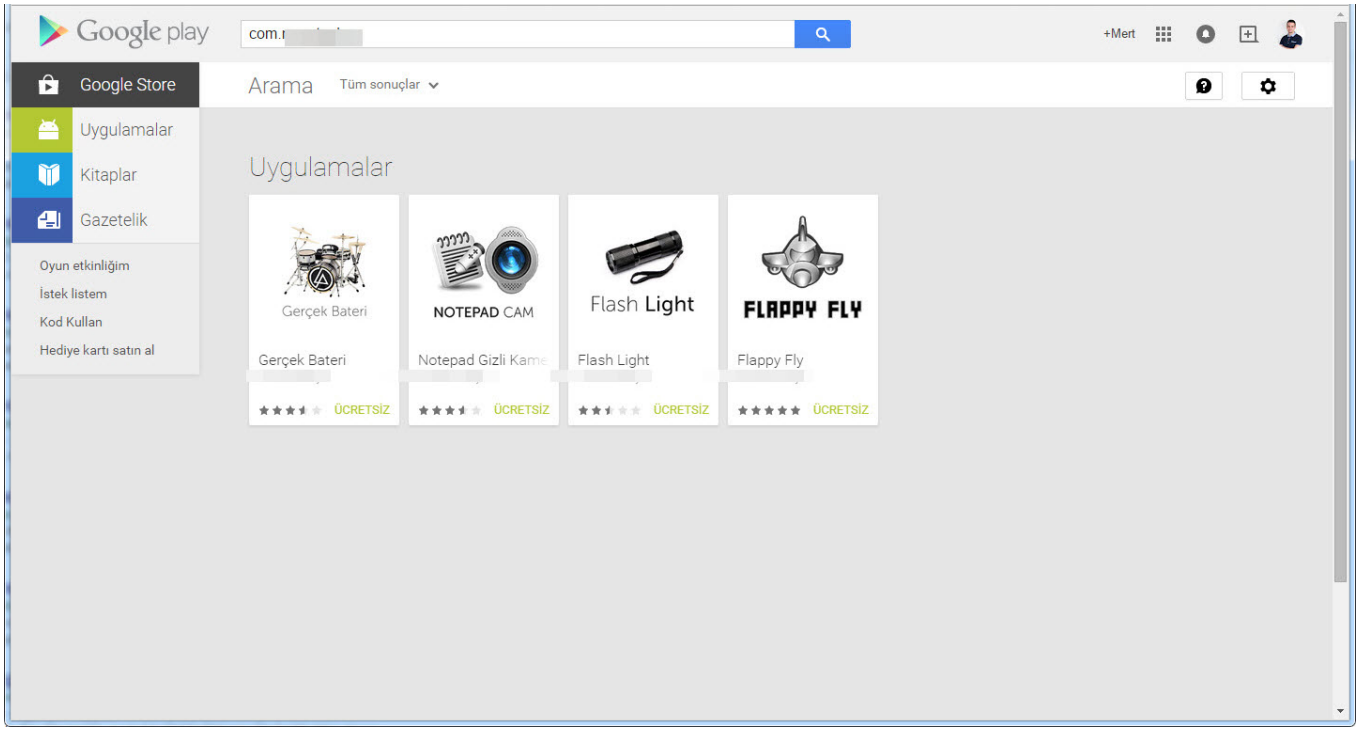
Siteyi masa üstü internet tarayıcısı ile ziyaret edenler ise bankanın ana sayfasına yönlendiriliyordu. Zararlı yazılımın zaman içinde birden fazla sürümüne erişme imkanım olduğu için ilk sürümü ile 2 ve 3. sürümlerini kıyaslama imkanım olmuştu.

İlk sürümde kod gizlemesi (obfuscation) gerçekleştirilmediği için zararlı yazılım, kaynak koda çevridiğinde bunun rehber, arama kaydı ve sms bilgilerini çalan, anahtar kelime ile sms yönlendirmesi yapabilen ve Türkiye'de 185.50.69.100 ip adresi ile 4444 numaralı bağlantı noktasından haberleşen bir casus yazılım olduğu rahatlıkla anlaşılıyordu.

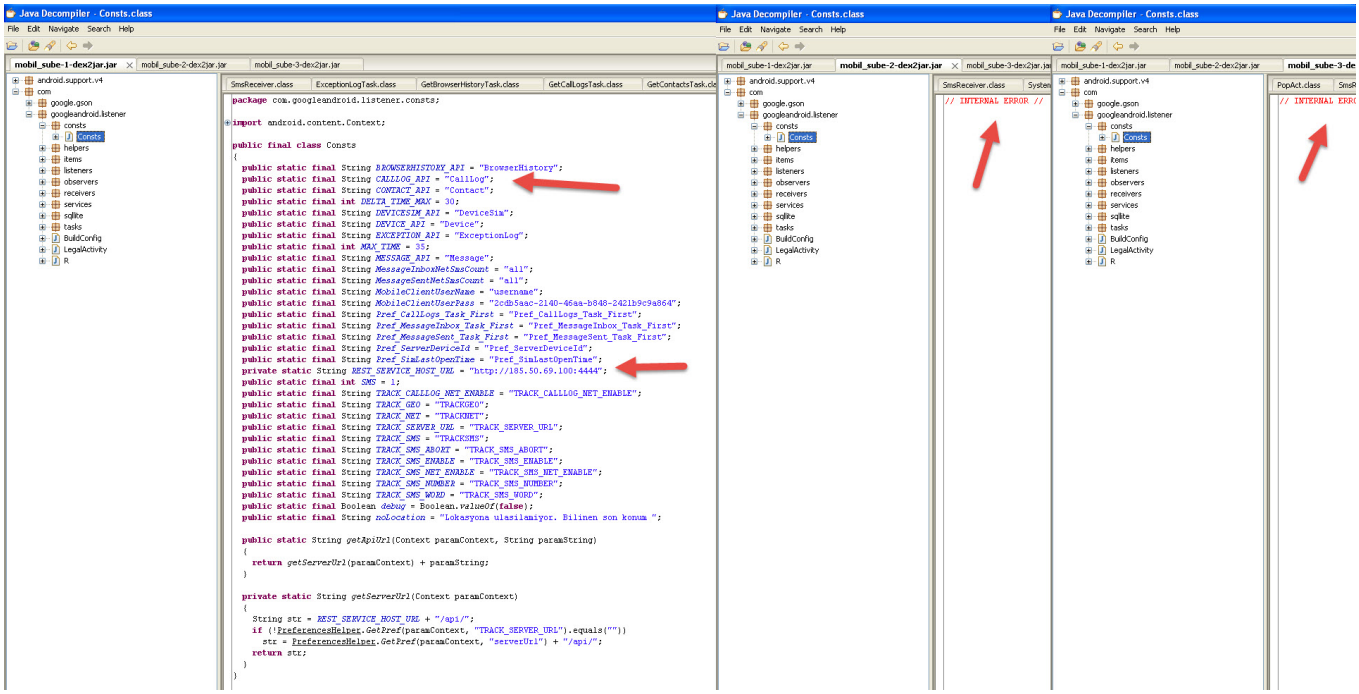


Yazılımı geliştiren kişinin kaynak kodun bir yerinde servis adı olarak isim.soyad bilgisine yer vermesi, kodun ya çalıntı ya da dikkatsizce başka bir koddan kopyalandığına işaret ediyordu.





İlerleyen sürümlerde ise bu zararlı yazılım haberleştiği ip adresi, kod gizleme yöntemi ile gizlendiği görülebiliyordu.

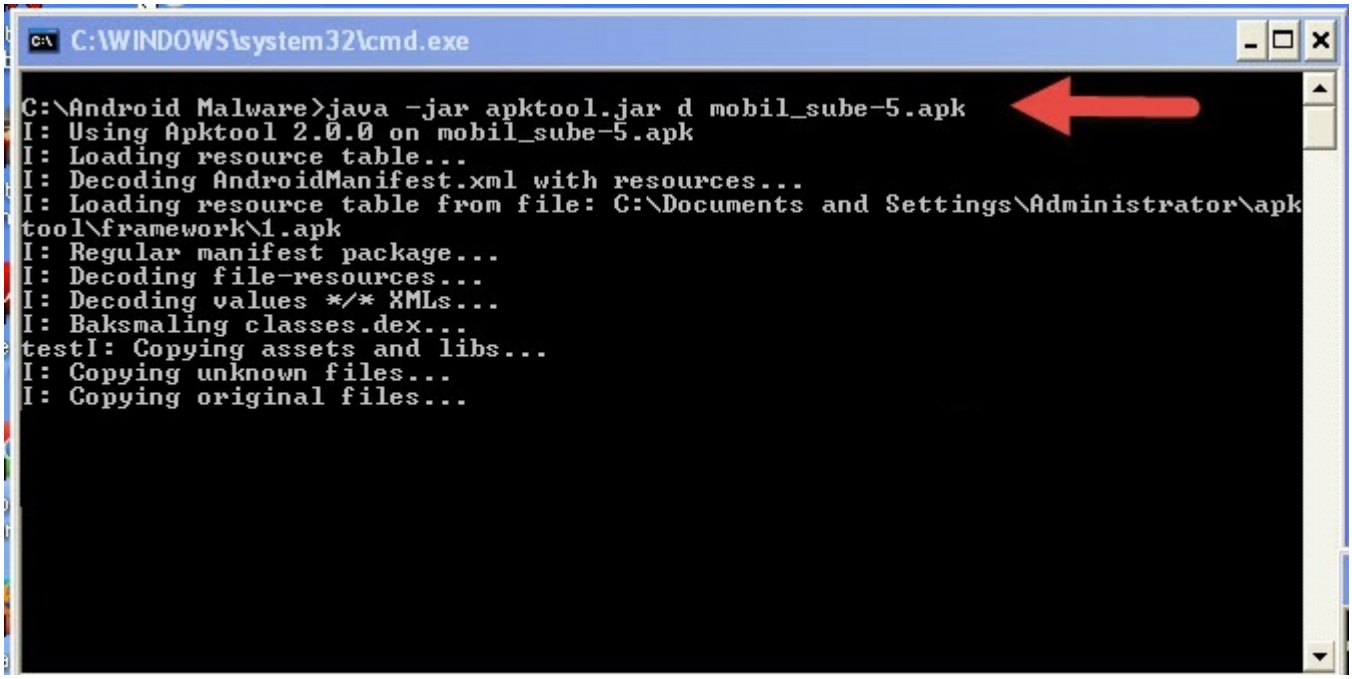


Yeri gelmişken bu tür zararlı yazılımlar ile karşılaşıldığı zaman, son kullanıcı da olsanız, güvenlik uzmanı da olsanız, Ulusal Siber Olaylara Müdahale Merkezi'ni (USOM) ihbar formu üzerinden bilgilendirmenin, ulusal ve kurumsal güvenlik adına oldukça önemli olduğunun altını çizmek isterim.

USOM'un hızla güncellediği zararlı bağlantılar listesi ve koordinasyon ile sektörel ve kurumsal SOME'lerin, güvenlik üreticilerinin kısa süre içinde bu zararlı adreslerden haberdar olarak, kullanıcıların mağdur olmasını kısa bir süre içinde engellediklerini unutmayın.

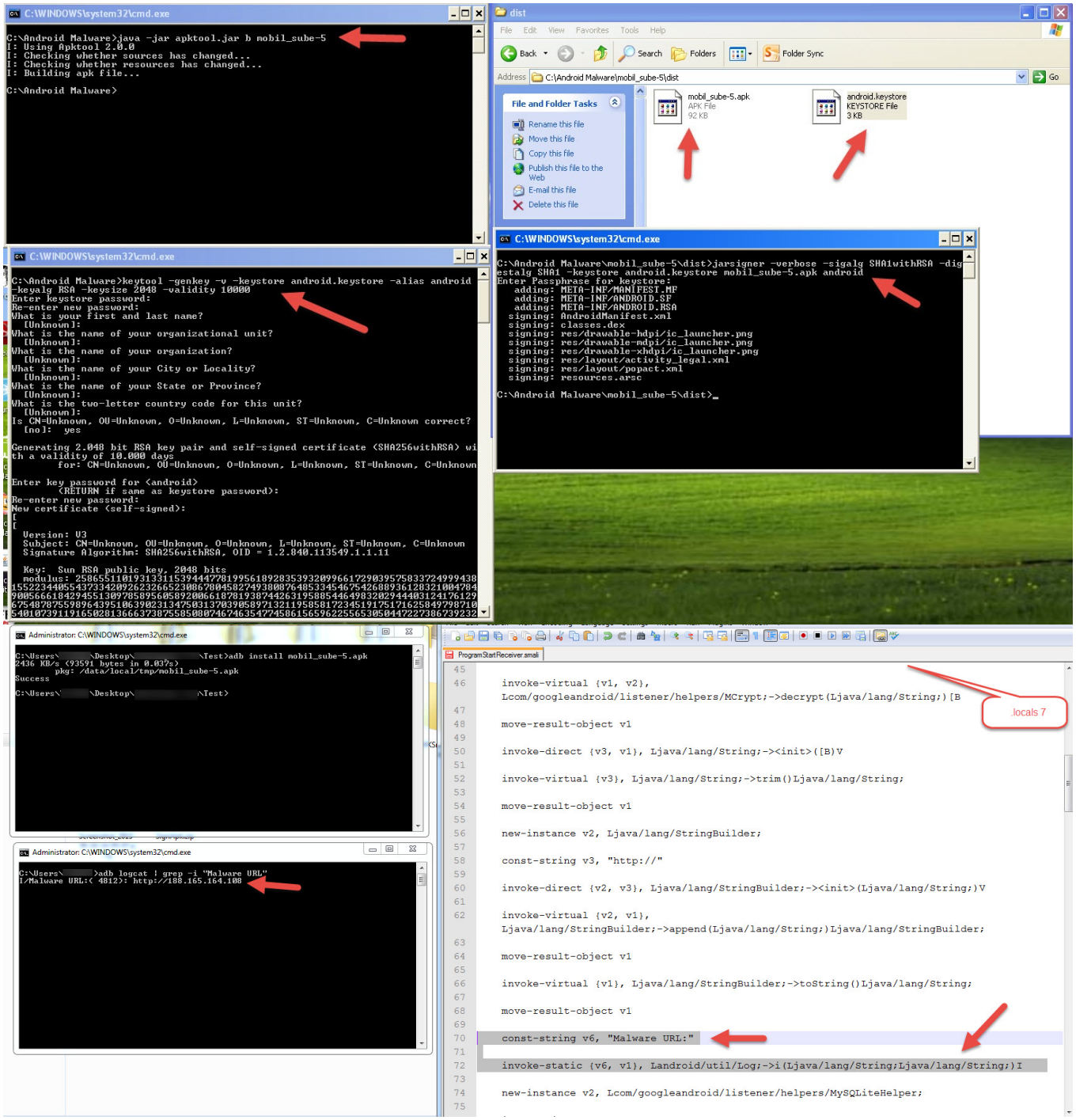
Devlet kurumudur, oldukça yavaş işler, hiç zahmet etmeyeyim gibi ön yargıları bir kenara koyabilirsiniz çünkü USOM'a yapmış olduğum bir bildirimin 2 saat gibi kısa bir süre içinde zararlı bağlantılar listesine eklendiğini geçtiğimiz günlerde tecrübe ettiğimi söyleyebilirim.

Daha önceki yazılarımdan da bildiğiniz üzere Android platformu için geliştirilen uygulamalar kolaylıkla bayt koduna ve kaynak koduna çevrilebilmektedir. Kaynak kodunun bu örnekte olduğu gibi okunaklı olmadığı durumlarda bayt kodunu analiz etmek tercih edeceğiniz en akıllıca yöntemlerden biri olacaktır.



Zararlı yazılımı apk-tool aracı ile bayt koduna (smali) çevirdikten sonra smali\com\googleandroid\listener\items\receivers\ klasörü içinde yer alan ProgramStartReceiver.smali dosyası dikkatimi çekti. Dosyayı incelediğimde şifrelenen komuta kontrol merkezi adresinin bu dosya içinde çözüldüğünü (decryption) gördüm.

Bu gibi (okunaklı olmayan kaynak kodu) durumlarda bayt kod üzerinde değişiklik yaparak programın akışını değiştirebilme imkanına sahip olduğunuz için ben de şifresi çözülmüş olan değişkeni aşağıdaki ekran görüntüsünde yer aldığı şekliyle LogCat'e yönlendirmeye karar verdim. Değişikliği yaptıktan sonra tekrar apk-tool aracı ile paketi derleyip, imzaladıktan sonra Android Emulator'e yükledim ve ardından gizlenmiş olan komuta kontrol merkezinin ip adresini görebildim.



Bu zararlı yazılımda olduğu gibi siz de kod gizleme yönteminden (obfuscation) faydalanan zararlı yazılımları analiz etmek istediğinizde benzer şekilde bayt kodu üzerinden ilerlemeyi alternatif bir yol olarak değerlendirebilirsiniz.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.