DTMF Hırsızlığı

written by Mert SARICA | 1 June 2017

15 Kasım 2016 tarihinde Hürriyet'te yayınlanan "Dolandırıcılıkta yeni yöntem: Dolandırılıyorsunuz; şifrenizi ekrana tuşlayın" başlıklı yazı dikkatimi çekti. Haberin detaylarını okuduğumda dolandıcıların yeni keşfettikleri akılalmaz bir yöntem ile dolandırıcılık yaptıklarına dem vuruluyordu. Şayet haberi derleyen kişi, haberi yayımlamadan önce en azından bir bilişim uzmanına danışmış olsaydı eminim bunun akıl almaz bir yöntem olmadığını öğrenmesi 5 dakikasını almaz ve dolandırıcıların kullandıkları yöntemi de açığa kavuşturarak çok sayıda vatandaşımızı, ilgilileri bu konuda aydınlatabilirdi. Durum böyle olmayınca ve yakın çevremden de bu konuya ilişkin sorular geldiği için iş başa düştü ve bu haberde yer alan yöntemi açığa çıkarmaya karar verdim.

Detaylara geçmeden önce ilk olarak Çift Tonlu Çoklu Frekans'tan (Dual Tone Multi-Frequency / DTMF) kısaca bahsetmek gerekiyor. DTMF, Bell Systems firması tarafından 1963 yılında geliştirilmiş ve telefon şebekesinde taraflar arası bilginin iletilmesini sağlayan bir kodlama türüdür. DTMF tuş takımları aşağıdaki gibi 16 tuştan oluşur. Tuşlu telefonlarda, tuş takımlı akıllı telefonlarda her bir tuşa basıldığında, aşağıdaki tabloya göre bir ton çifti oluşturulur ve telefonun diğer ucundaki tarafa sinyale dönüştürülerek iletilir. Örneğin bir bankayı aradığınızda sizi karşılayan robot, sizi tanıyabilmek için sizden müşteri numaranızı ve TCKN numaranızı girmenizi ister. Siz bu bilgileri tuşlamaya başladığınız zaman oluşan ve rahatlıkla duyabildiğiniz her ton çifti, robot tarafından Goertzel algoritmasına göre çözümlenerek sayısal değere çevrilir ve işlemlerinizi gerçekleştirilir.

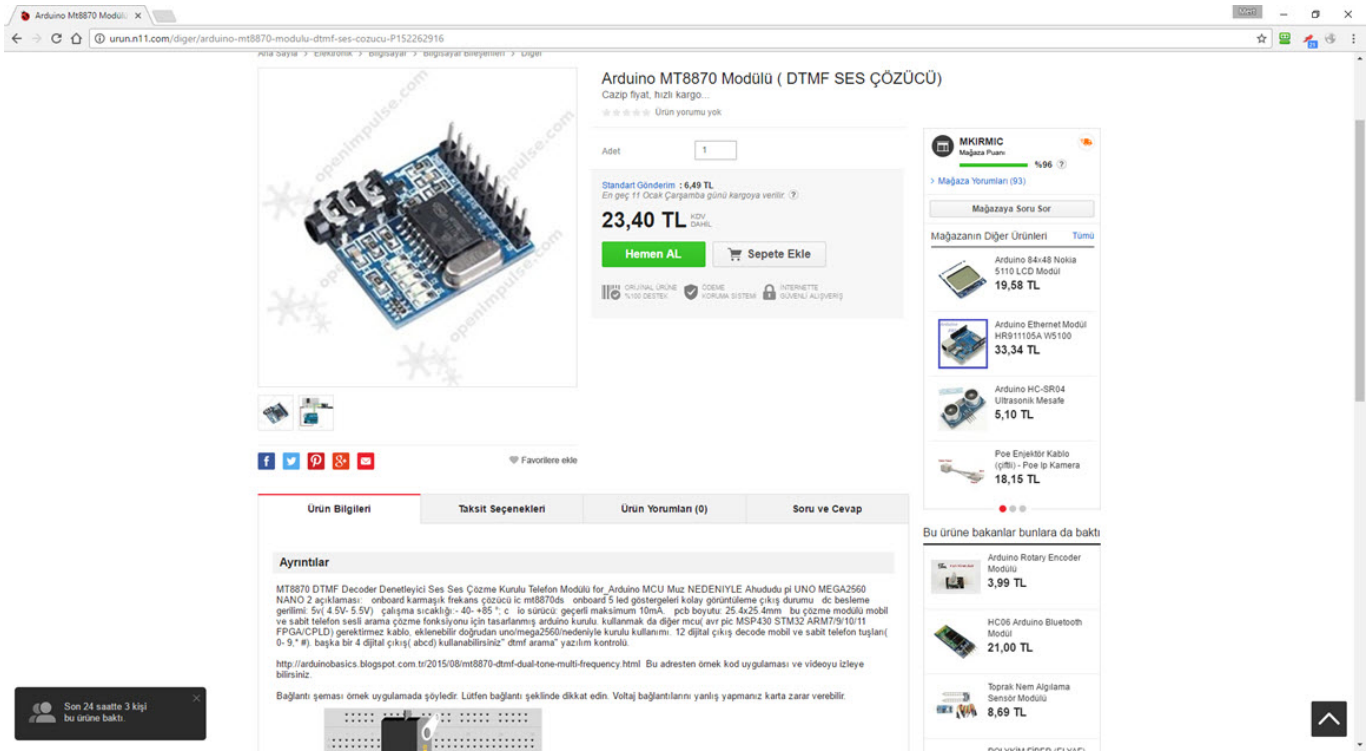
Frekanslar	1209 Hz	1336 Hz	1477 Hz	1633 Hz
697 Hz	1	2	3	A
770 Hz	4	5	6	B
852 Hz	7	8	9	C
941 Hz	*	0	#	D

Tablo 1 – DTMF kodlama frekansları

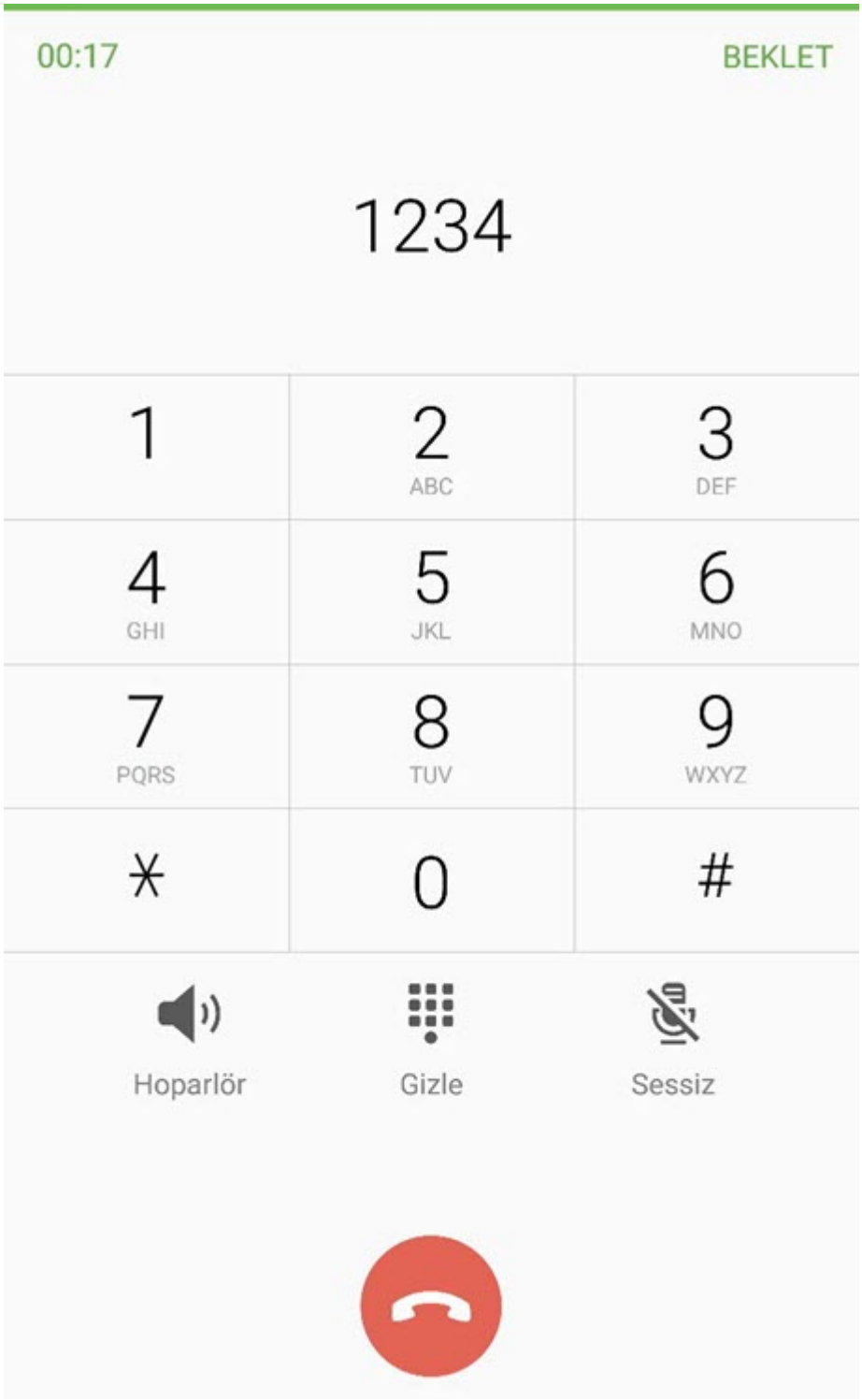
Yukarıdaki özet bilgi ışığında habere konu olan dolandırıcılık yönteminin pratikte nasıl gerçekleşebileceğine kısaca bir bakalım. İkna dolandırıcılığında, dolandırıcıların temel amacı karşı tarafın güvenini kazanararak kötü emellerini gerçekleştirmektir. Haberde de belirtildiği üzere bankadan aradıklarını söyleyen dolandırıcılar, vatandaşa parasının çekilmeye

çalışıldığını ve bu şüpheli işlemi durdurmak için kart PIN kodunu ekrana tuşlayarak durdurabileceğini söylemektedirler. Vatandaşın güveninini kazanarak yapılan bu dolandırıcılıkta, dolandırıcıların yaptığı işlem tahmin edeceğiniz üzere vatandaşın ekrana girerken bastığı tuşların oluşturduğu DTMF sinyalini çalmaktır.

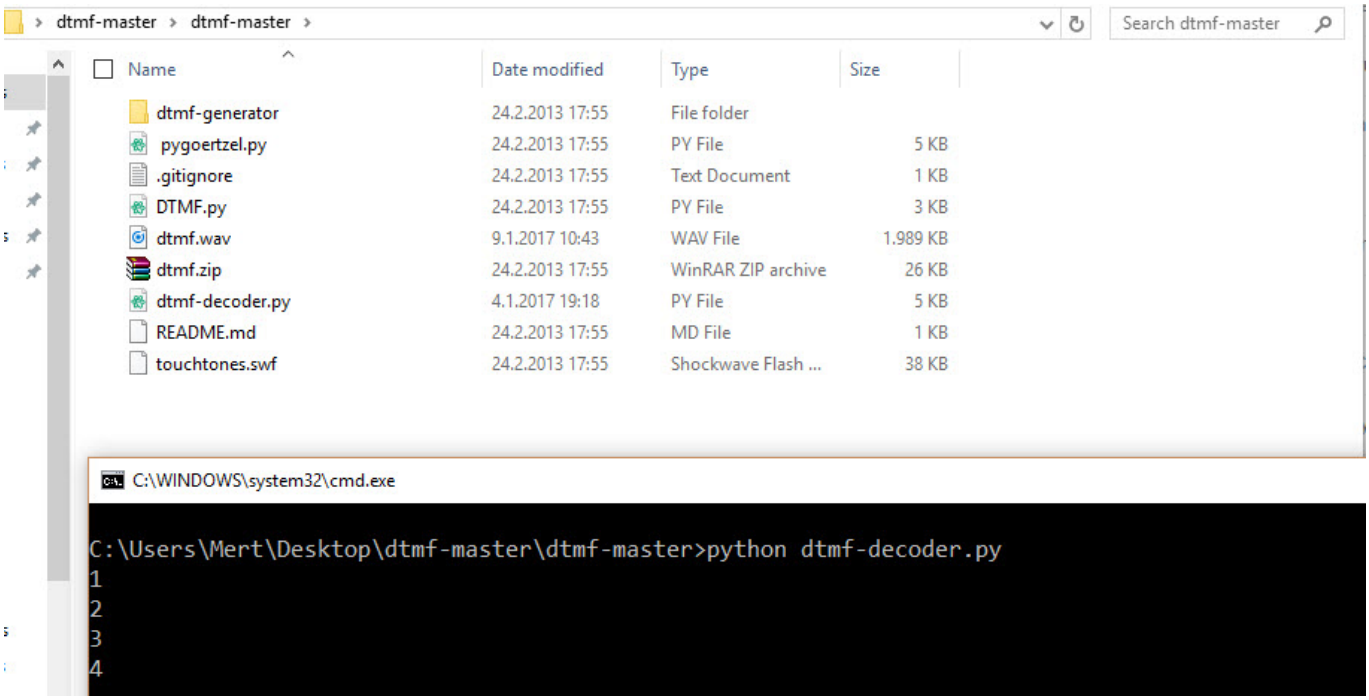
DTMF sinyalini çalmak ve sayısal değere dönüştürmek dolandırıcılar için ne kadar zor olabilir diye düşünmeye başladığımda, ilk olarak e-ticaret sitelerine girip “DTMF” anahtar kelimesi ile arama yapmaya karar verdim. Çok geçmeden DTMF sinyalini çözebilen Arduino modüllerinin 23 TL gibi uygun bir fiyata satıldığını gördüm. İlan üzerindeki bilgilere kısaca göz attığımda da, aşağıdaki video ile pratikte bu işin çok da zor olmayacağını öğrendim.



İşin içine modüller ve kablolar girdiğinde dolandırıcıların çok da bu yolu tercih etmeyeceklerini düşünerek başka yollar üzerine düşünmeye başladım ve Automatic Call Recorder gibi çağrı kaydı yapan akıllı telefon uygulamaları aklıma geldi. Uygulamayı yükleyip, çalıştırdıktan sonra eşime kendimi aratıp ekrana 1234 PIN kodunun tuşlandığı ufak bir parodi hazırladım.



Son olarak GitHub üzerinde kayıt altına aldığım ses dosyasındaki DTMF sinyalini sayısal değere dönüştürmek için program aramaya koyuldum ve 4 yıl önce DTMF sinyalini çözmek amacıyla geliştirilmiş olan bu araç ile karşılaştım. Ses dosyası (dtmf.wav) üzerinde bu aracı çalıştırdıktan kısa bir süre sonra eşimin telefonundan ekrana tuşladığım PIN kodunu (1234) programın çıktısında görebildim.



Sonuç itibariyle ikna dolandırıcılarının güveninizi kazanarak bilgilerinizi çalmak için çağrı merkezlerinde kullanılan robotları taklit ettiklerini ve arka planda ekrana tuşladığınız bilgileri DTMF sinyalleri üzerinden kolaylıkla çalabildiklerini görüyoruz. Güvenliğiniz için güvenilirliğinden emin olmadığınız hiç bir sisteme kart no, pin, müşteri no vb. bilgilerinizi telefon üzerinden tuşlamayınız.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.