Sponsorlu Dolandırıcılık

written by Mert SARICA | 1 October 2018

If you are looking for an English version of this article, please visit here.

Siber güvenlik dünyasında olan biteni Twitter’dan takip ettiği için bir gözü Twitter’da olan bir güvenlik araştırmacısı olarak, 2018 Ağustos ayı itibariyle Twitter’da karşıma banka müşterilerini hedef alan sponsorlu oltalama (phishing) reklamlarının çıkmaya başladığını farkettim. Başlarda bu tweetleri sadece Twitter’a bildirmekle yetinsem de, takipçilerimden gelen mesajların sayısının artması ve bu reklamların Ekim ayına kadar sürdüğünü görünce bu konuyla yakından ilgilenmeye karar verdim.

Tweet

11:29 · 18 Ağu 18

Sponsorlu

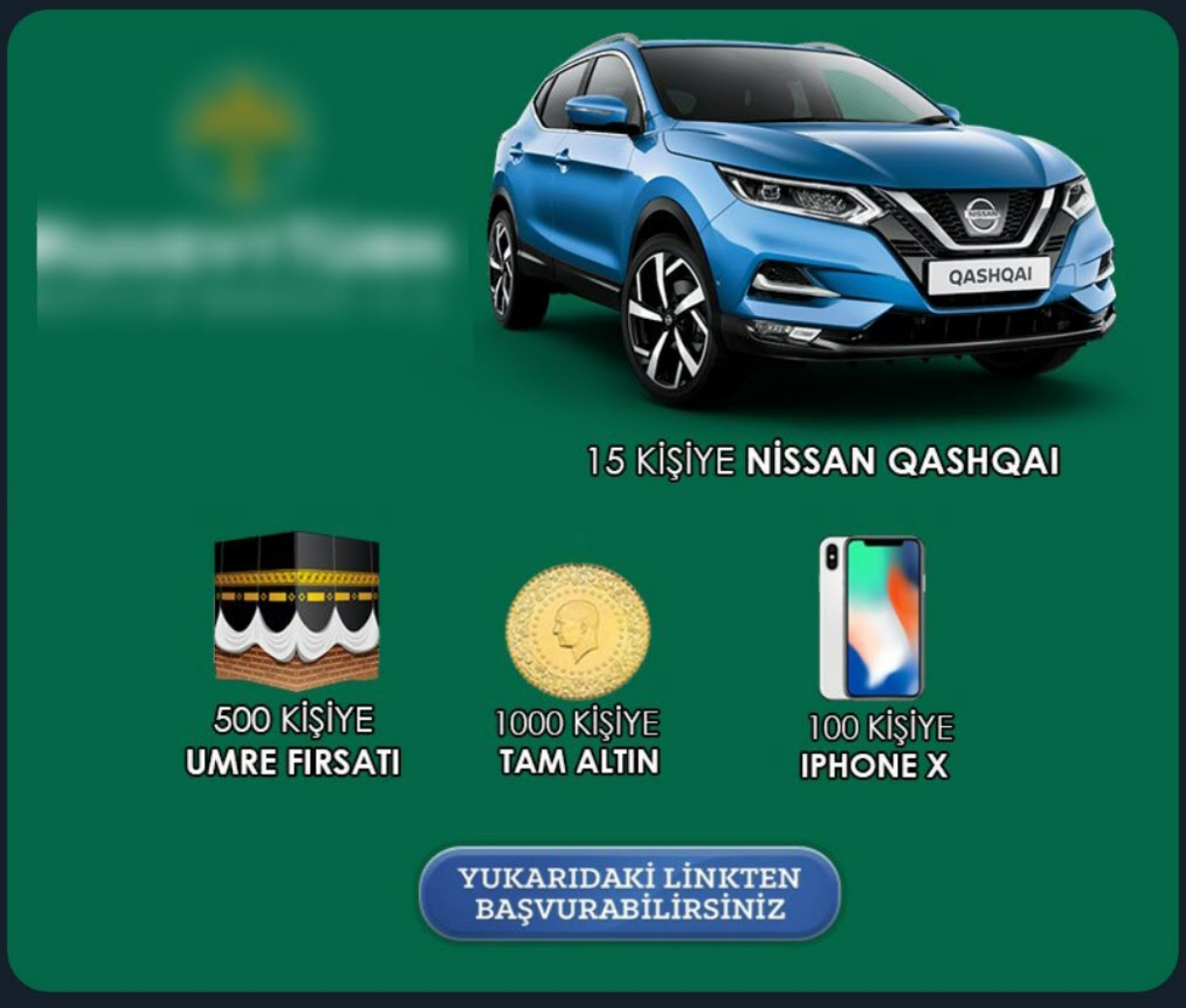
4 Beğeni

Tweet

12:32 · 29 Ağu 18

3 Beğeni

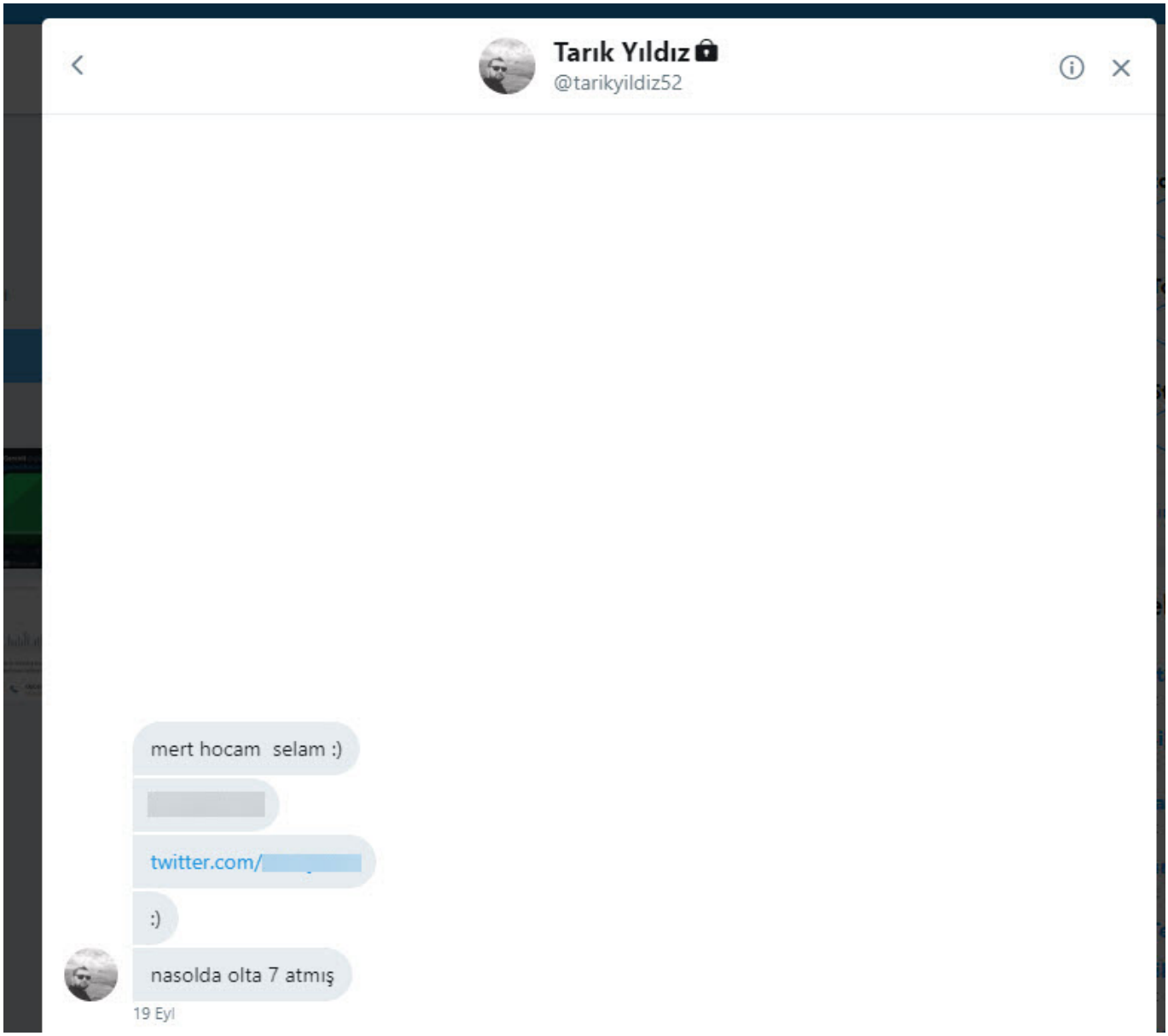
Tweet

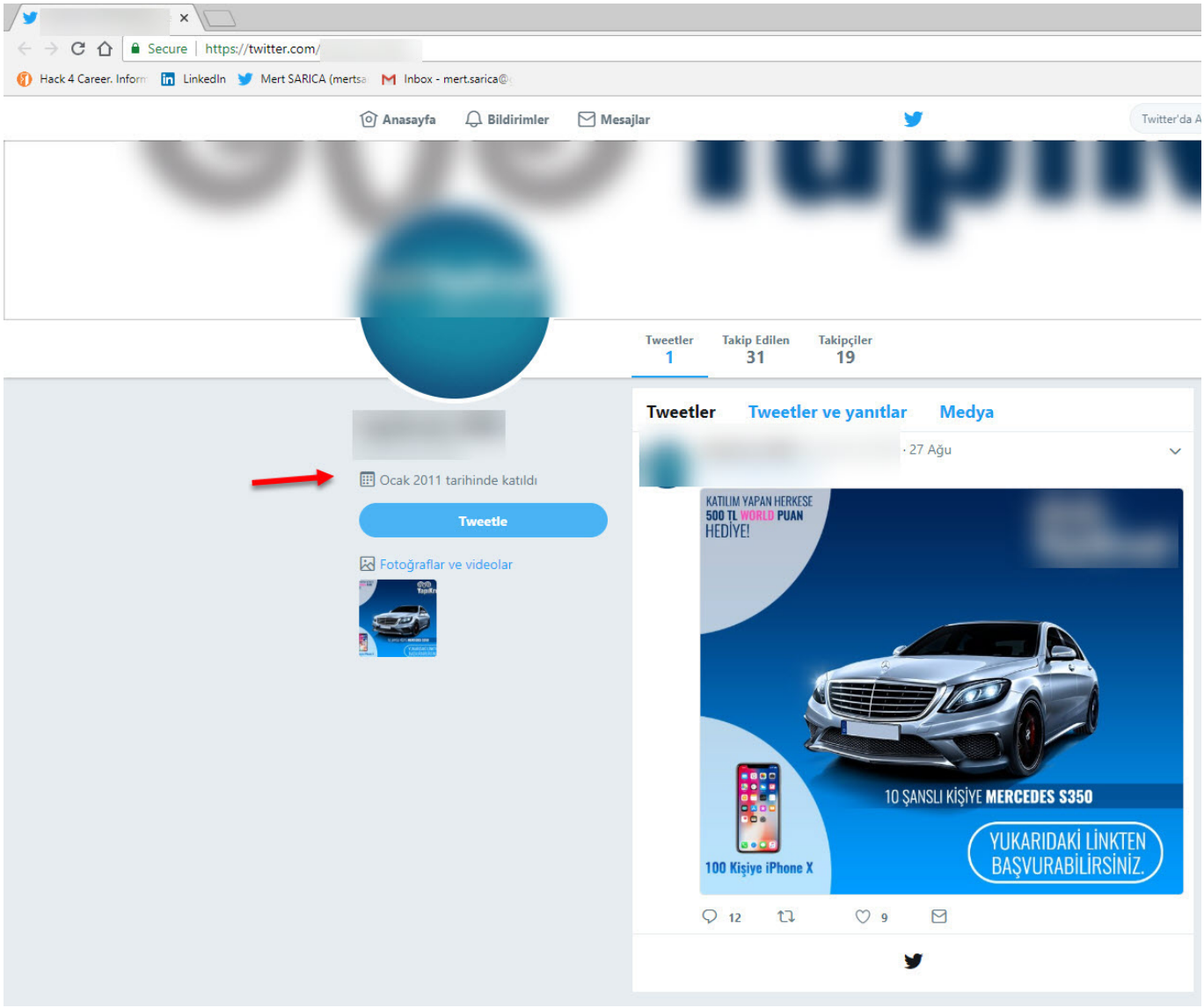


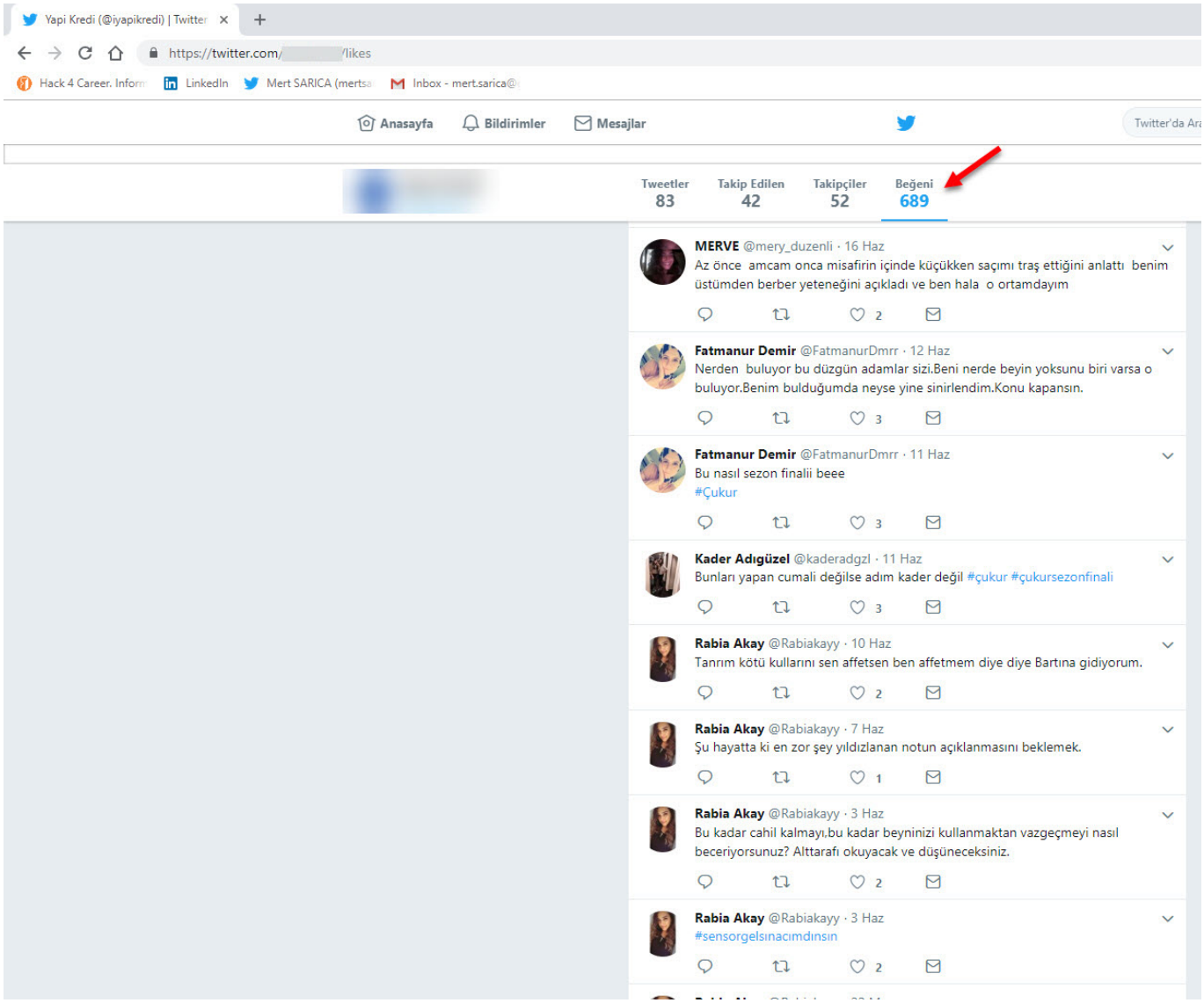
12:57 · 19 Eyl 18

4 Retweet **53** Beğeni

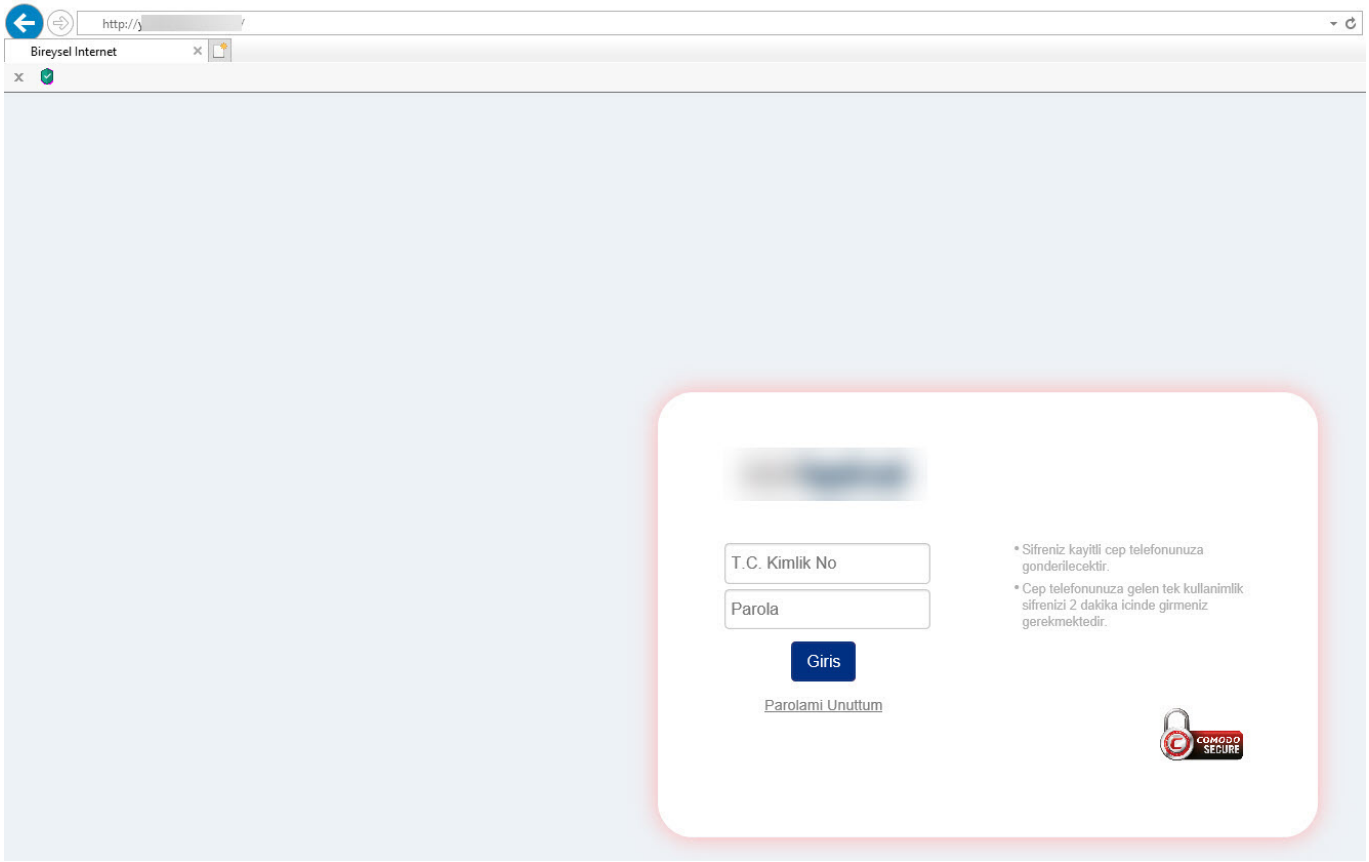

Nurseda ÖZDEMİR
@nursedaozdemr
Hocam bu yeni, size havale ediyorum 😂
twitter.com/...
8 Eyl
Aynen hocam, ilginç olan twitter'a katılım tarihleri 2013, 2016 vs.
Yeni hesap da değiller.
8 Eyl

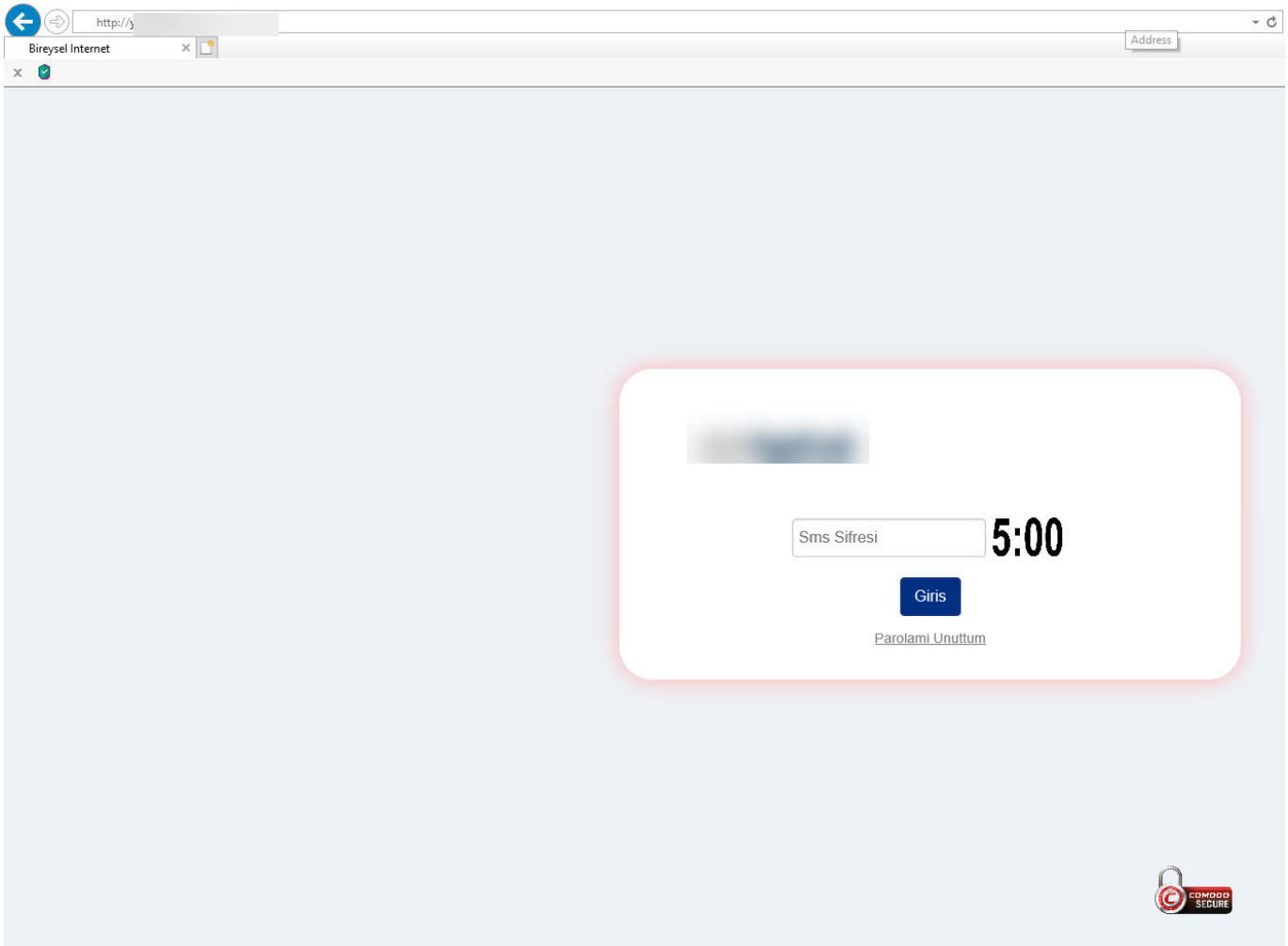

Tarık Yıldız
@tarikyildiz52
mert hocam selam :)
twitter.com/
:)
nasolda olta 7 atmış
19 Eyl

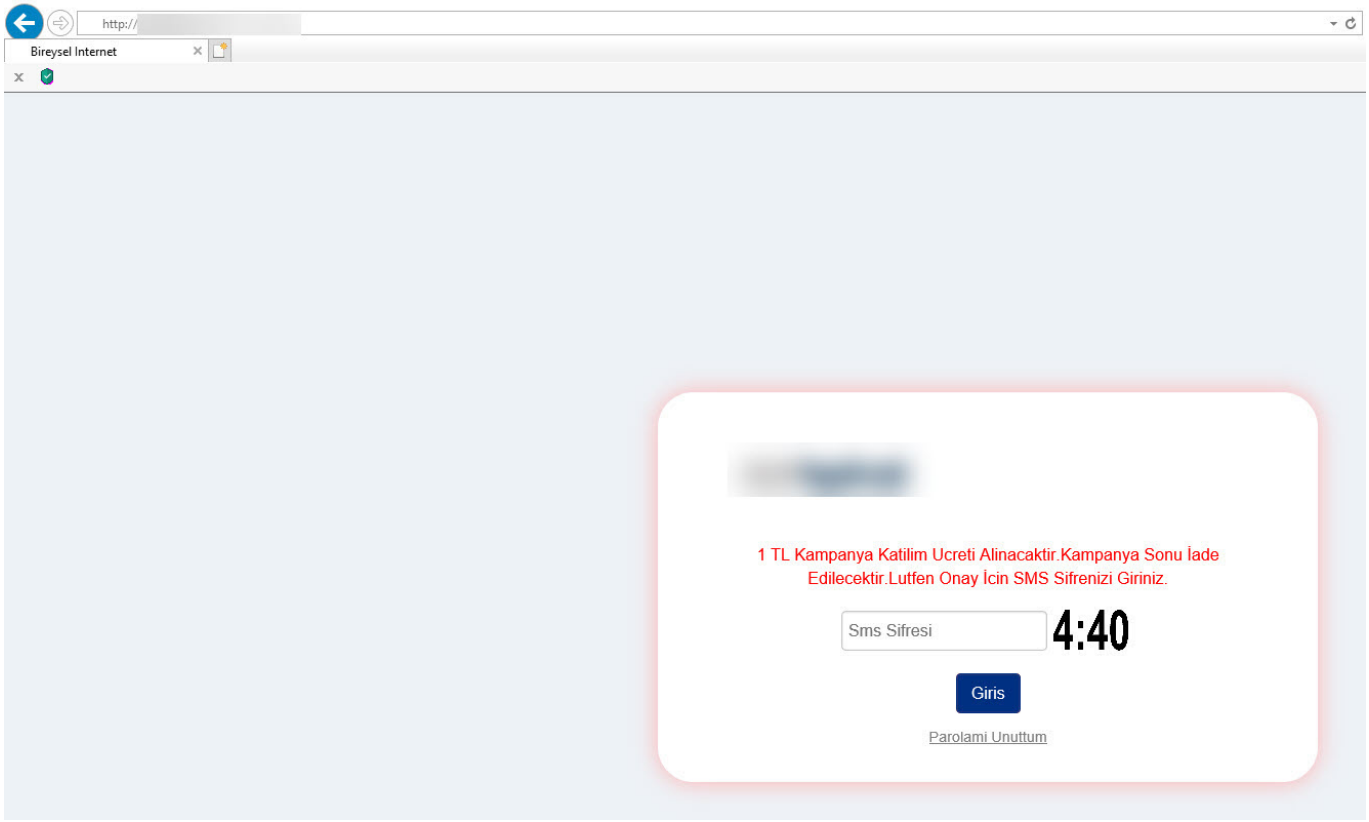

Secure | https://twitter.com/
Hack 4 Career. Inform
LinkedIn
Mert SARICA (mertsa
Inbox - mert.sarica@
Anasayfa
Bildirimler
Mesajlar
Twitter'da A
Tweetler 1
Takip Edilen 31
Takipçiler 19
Ocak 2011 tarihinde katıldı
Tweetle
Fotoğraflar ve videolar
Tweetler
Tweetler ve yanıtlar
Medya
· 27 Ağu
KATILIM YAPAN HERKESE
500 TL WORLD PUAN
HEDİYE!
10 ŞANSLI KİŞİYE MERCEDES S350
YUKARIDAKİ LİNKTEN
BAŞVURABİLİRSİNİZ.
100 Kişiye iPhone X
12
9

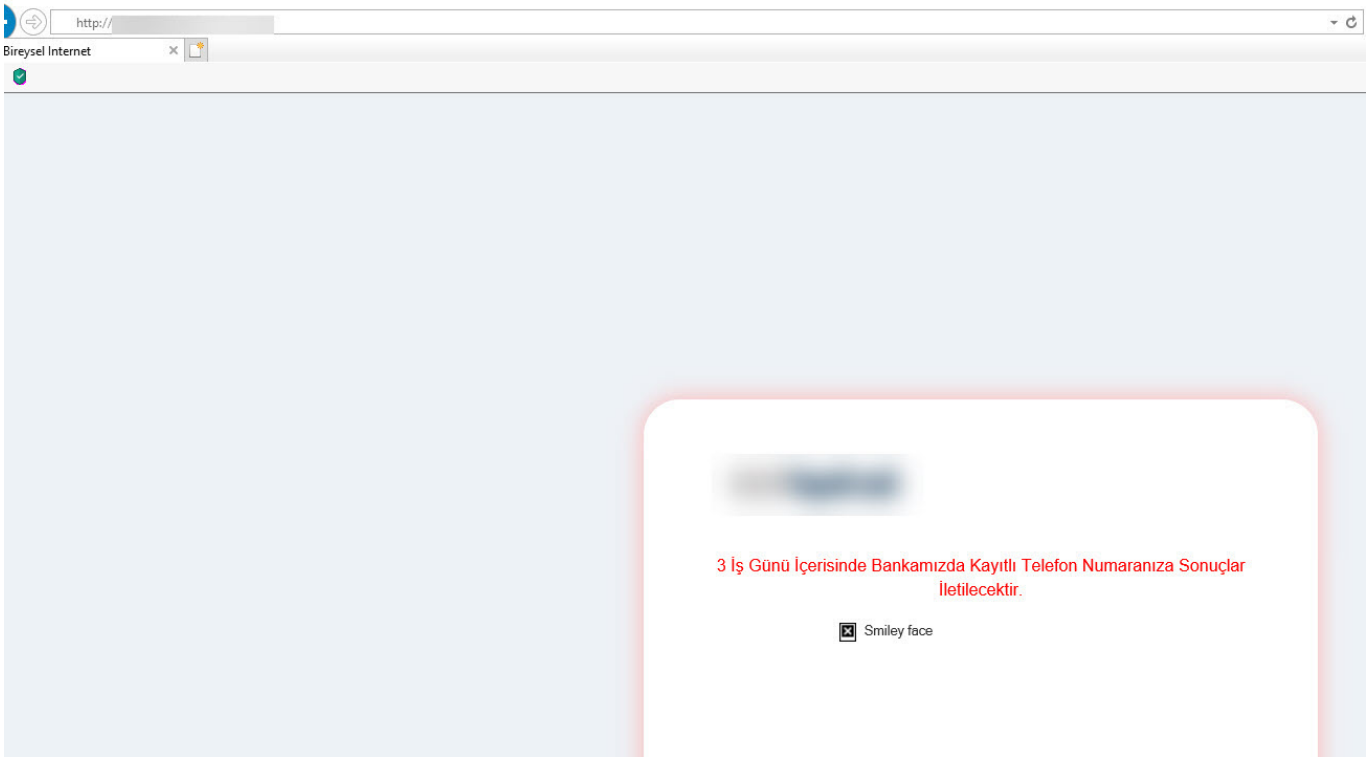


Oltalama tweetlerinden birinde yer alan bağlantı adresini takip ettiğimde dolandırıcıların, müşterinin internet bankacılığına giriş esnasında kullandığı kullanıcı adını, parolasını, sms ile gönderilen doğrulama kodunu ve ardından da para transferinde kullanılan sms doğrulama kodunu çaldıklarını gördüm.


Bireysel Internet
T.C. Kimlik No
Parola
Giris
Parolami Unuttum
• Sifreniz kayitli cep telefonunuza gonderilecektir.
• Cep telefonunuza gelen tek kullanimlik sifrenizi 2 dakika icinde girmeniz gerekmektedir.
COMODO SECURE


Bireysel Internet
Address
Sms Sifresi
5:00
Giris
Parolami Unuttum
COMODO SECURE



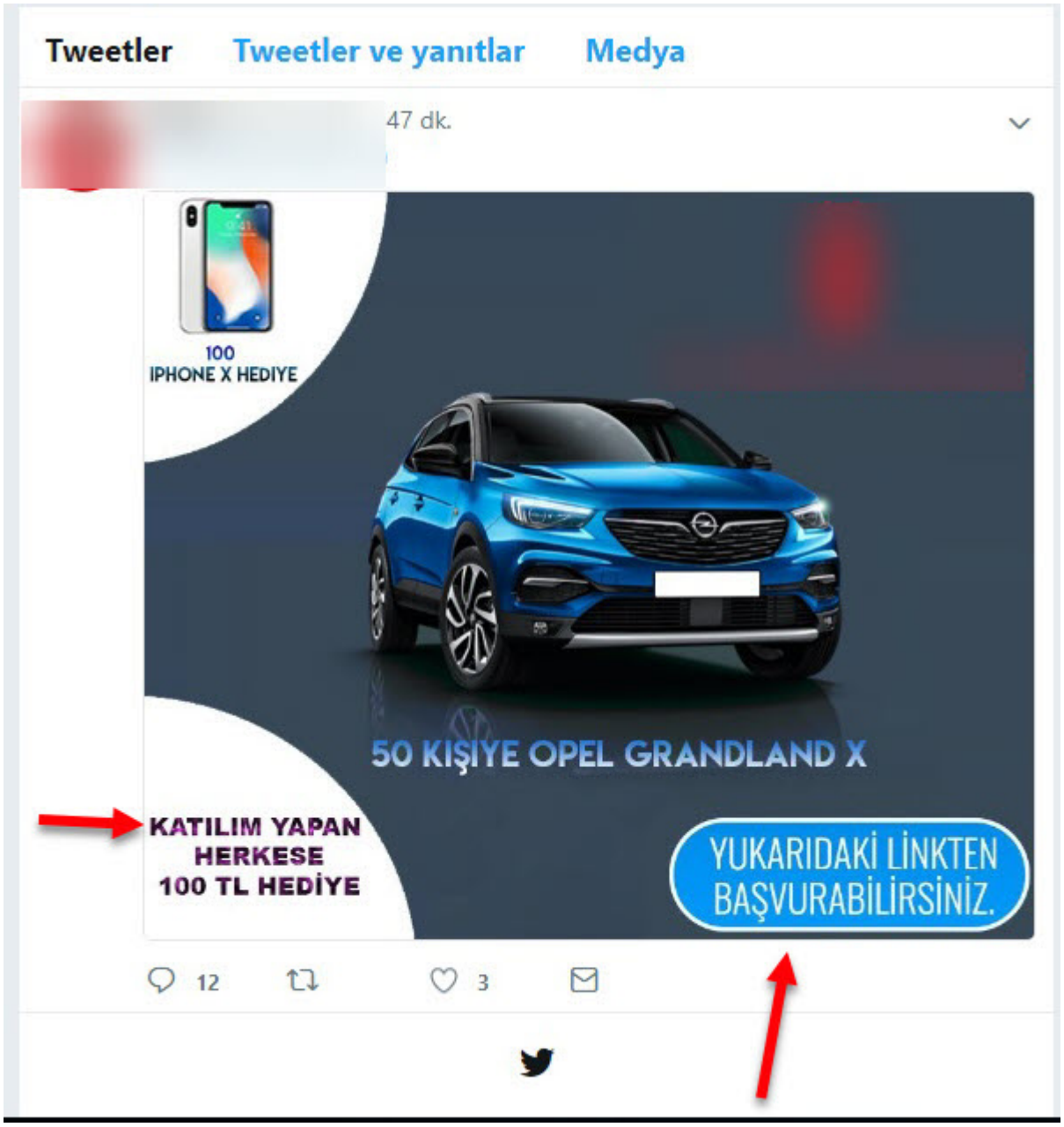


Çoğunuz gibi benim de Twitter'da bu sponsorlu oltalama reklamlarını gördükçe aklıma aşağıdaki bazı sorular ve yanıtları takıldı.

1. Twitter, aylardır birbirine fazlasıyla benzeyen, şikayet bildirimlerine konu olan bu oltalama reklamlarını engellemeye yönelik nasıl birşey yapamaz ?
2. Oltalama tweetleri için kullanılan hesapların bazıları nasıl olur da yıllar önce oluşturulmuş olabilir ?

3. Birbirine benzeyen bu oltalama tweetleri nasıl tespit edilebilir ?

Sorulara teker teker yanıt aramaya koyulduğumda, kendi kendime ilk soruya yanıt bulmam mümkün olamasa da, Twitter'ın bu oltalama reklamları karşısında bu kadar çaresiz (belki de vurdumduymaz) kalmasına oldukça şaşırdığımı söyleyebilirim. İkinci sorunun yanıtını bulmaya geldiğimde, oltalama için kullanılan hesapların eski tarihli olmasının muhtemel sebebi, Twitter'ın buradaki yardım sayfasında belirttiği üzere kullanıcı adının değiştirilmesine imkan tanımasıydı. Bu bilgiden yola çıkarak, oltalama tweetleri için kullanılan bu hesapların kuvvetle muhtemel hacklendiğini ve dolandırıcıların amaçları doğrultusunda kullanıldığını söyleyebiliriz. Sıra son soruya, oltalama tweetlerinin nasıl tespit edileceğine yanıt bulmaya geldiğinde, çoğu mesajda ortak olan kelimelerden (ŞANSLI KİŞİ, KATILIM YAPAN, YUKARIDAK) yola çıkarak Optik Karakter Tanıma (OCR) teknolojisi ile bu tweetleri tespit etme konusunda bir çalışma yapmaya karar verdim.



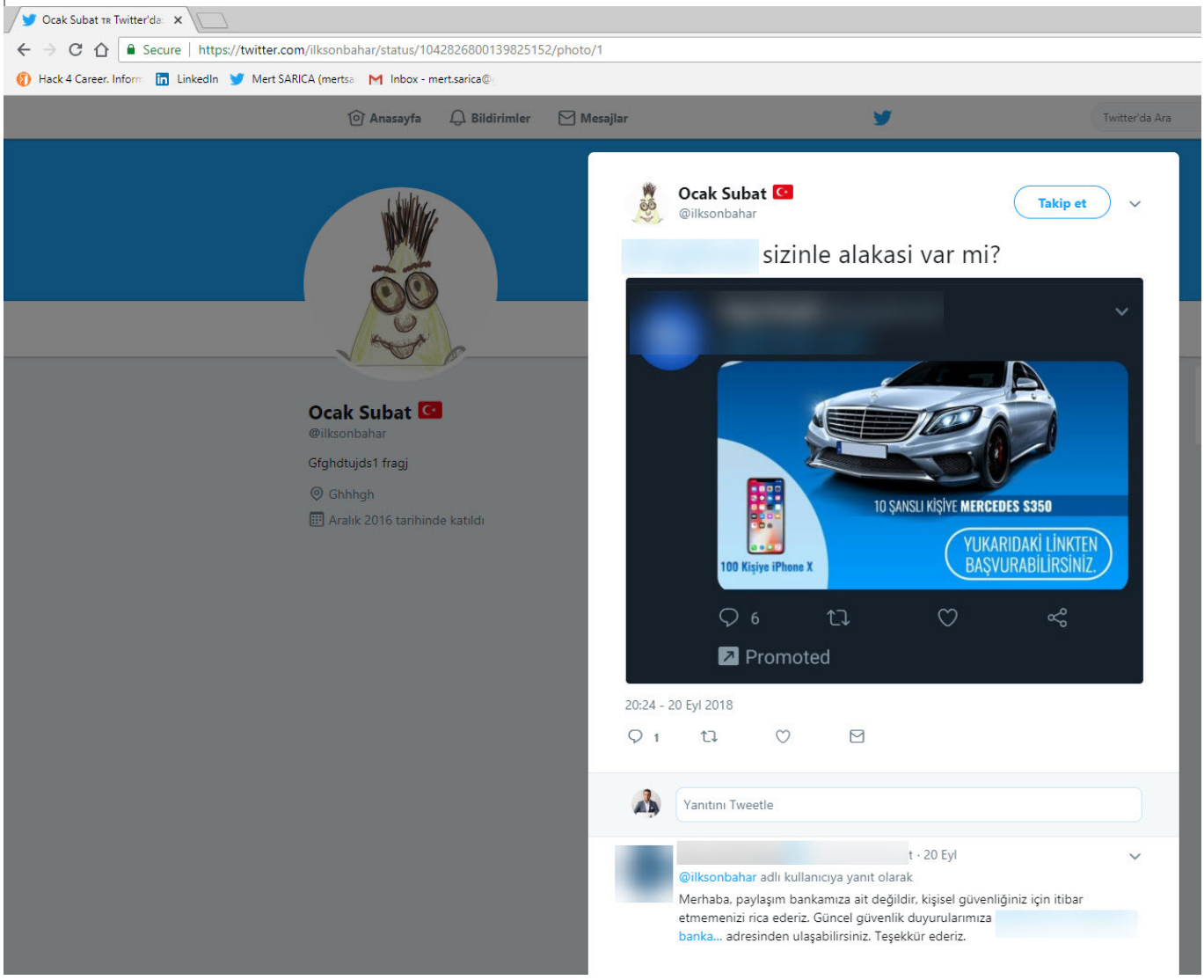
Çoğu banka müşterisinin karşılaştığı bu oltalama tweetlerini bankaların resmi Twitter hesapları ile paylaştığını gördükten sonra aracı hızlıca aklımda tasarlamaya başladım. Aracın temel olarak yapması gerekenler, Twitter'da banka isimlerini aramak, tweetlerde paylaşılan resimleri indirmek, OCR ile analiz etmek ve "ŞANSLI KİŞİ, KATILIM YAPAN, YUKARIDAK" kelimelerini tespit etmesi durumunda e-posta ile uyarmaktı. Uydurduğum, "Düşünmek, kodlamanın yarısıdır." sözünden yola çıkarak Python ile bu aracı kodlamaya başladıktan kısa bir süre sonra Tweepy isimli Python kütüphanesinden faydalanarak geliştirdiğim Phishing Tweet Detector aracı ortaya çıktı.

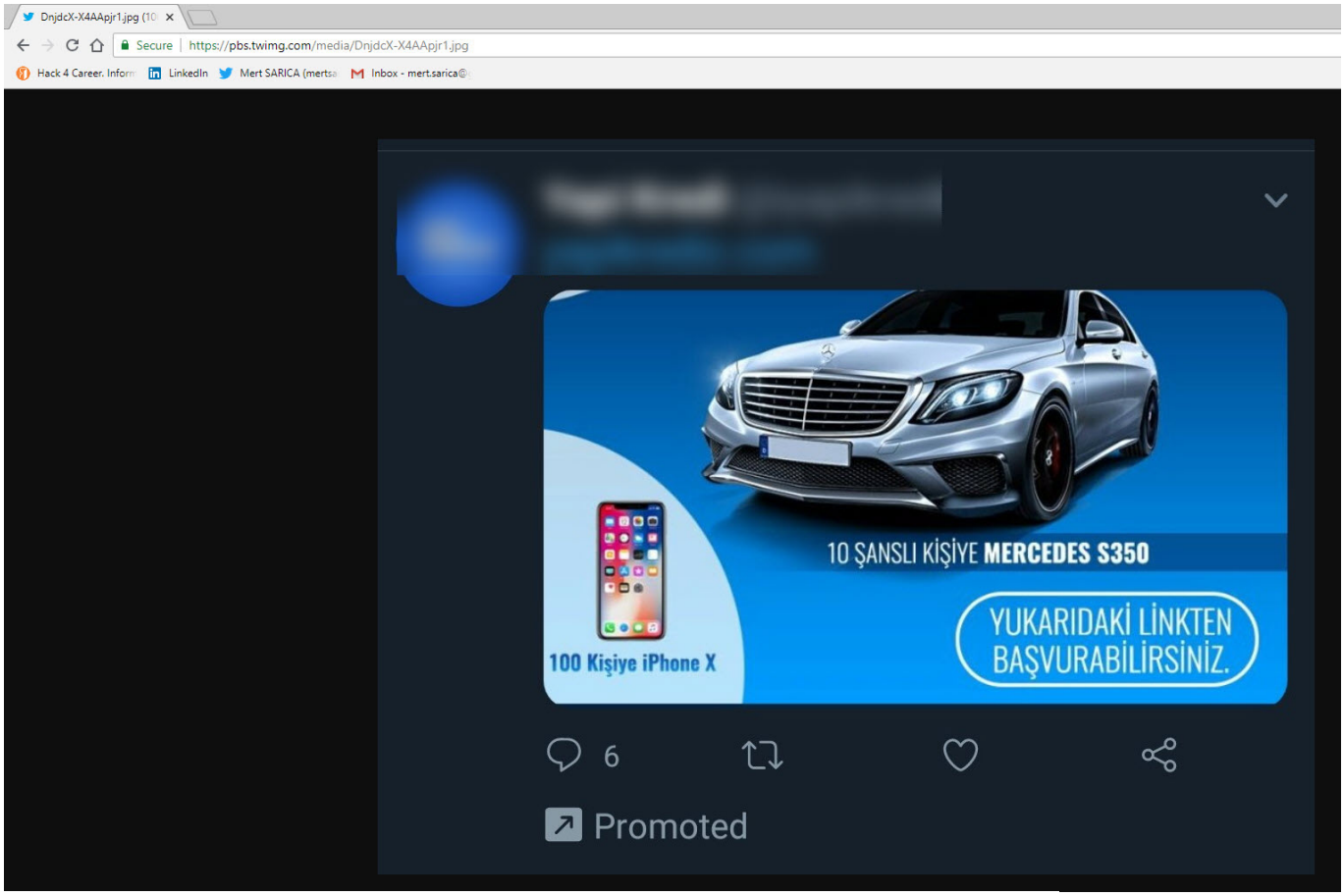
Aracı çalıştırdıktan kısa bir süre sonra bir Twitter kullanıcısının banka ile paylaştığı oltalama tweeti bu araç tarafından tespit edilmiş ve kurumların, vatandaşların bu tür dolandırıcılarla mücadele edebilmesine yardımcı olabilme adına ortaya koyduğum bir fikrim daha başarıyla hayata geçmiş oldu. :)

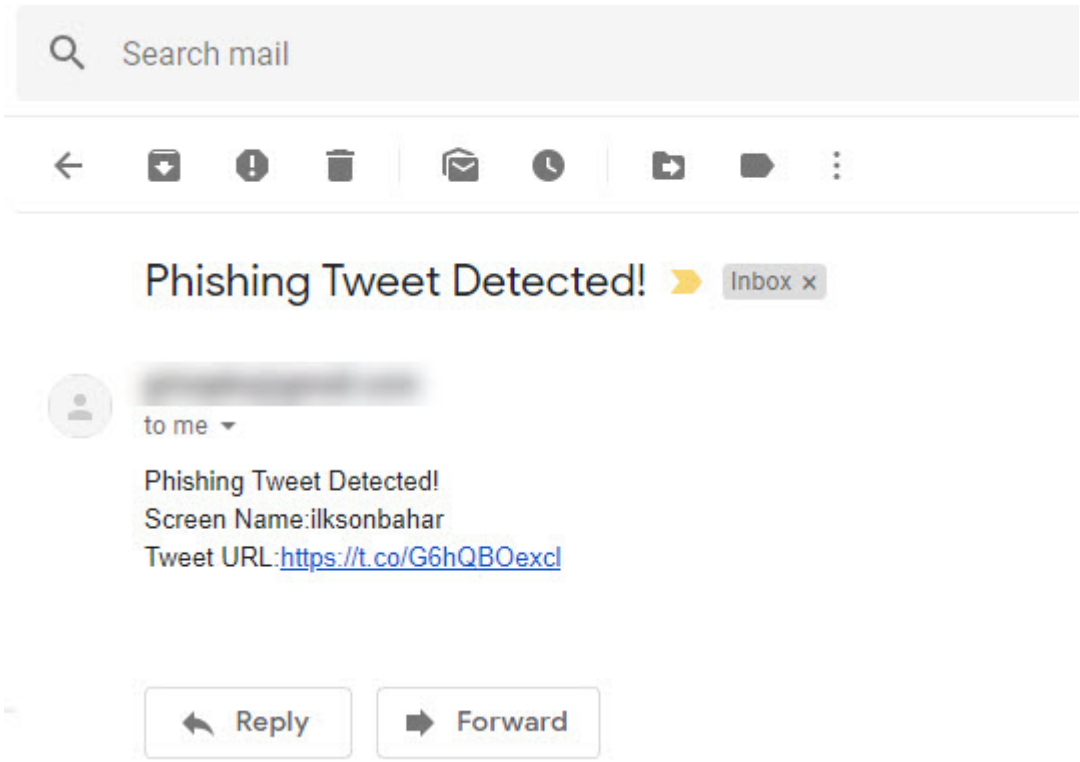
```
==========================================
Phishing Tweet Detector [https://www.mertsarica.com]
==========================================
[+] Checking tweets for keyword:
[+] Downloading image: http://pbs.twimg.com/media/DnpIE-TWwAAOlJy.jpg
[+] Running OCR on: DnpIE-TWwAAOlJy.jpg
[+] Downloading image: http://pbs.twimg.com/media/DnoYOGuXcAAoIOb.jpg
[+] Running OCR on: DnoYOGuXcAAoIOb.jpg
[+] Downloading image: http://pbs.twimg.com/media/DnoU-NjW4AEPnXK.jpg
[+] Running OCR on: DnoU-NjW4AEPnXK.jpg
[+] Downloading image: http://pbs.twimg.com/media/DnniAqAXoAAC2bW.jpg
[+] Running OCR on: DnniAqAXoAAC2bW.jpg
[+] Downloading image: http://pbs.twimg.com/media/DnmwLjzXOAA1Yc2.jpg
[+] Running OCR on: DnmwLjzXOAA1Yc2.jpg
[+] Downloading image: http://pbs.twimg.com/media/DnlsBWXV4AAhBQ5.jpg
[+] Running OCR on: DnlsBWXV4AAhBQ5.jpg
[+] Downloading image: http://pbs.twimg.com/media/DnkpKzkWOA4ueP4.jpg
[+] Running OCR on: DnkpKzkWOA4ueP4.jpg
[+] Downloading image: http://pbs.twimg.com/media/DnkF_mcW4AIJYSE.jpg
[+] Running OCR on: DnkF_mcW4AIJYSE.jpg
[+] Downloading image: http://pbs.twimg.com/media/DnjdcX-X4AApjr1.jpg
[+] Running OCR on: DnjdcX-X4AApjr1.jpg

[!] Phishing tweet detected! -> Screen Name: ilksonbahar Name: Ocak Subat ðŸ‡¹ðŸ‡· Media URL: http://pbs.twimg.com/media/DnjdcX-X4AApjr1.jpg Tweet URL: https://t.co/G6hQBOexcl

[+] Downloading image: http://pbs.twimg.com/media/DnjMsulWwAA6p_d.jpg
[+] Running OCR on: DnjMsulWwAA6p_d.jpg
[+] Downloading image: http://pbs.twimg.com/media/DnjIuTOWwAEqaMO.jpg
[+] Running OCR on: DnjIuTOWwAEqaMO.jpg
```







Yazıma son noktayı koymadan önce dolandırıcılarla mücadele için oltalama mesajları ile karşılaşanların bunları en kısa sürede bankalarına, bulunduğu sosyal ağ platformuna bildirmelerinin (Tweet'i bildir gibi) çok ama çok önemli olduğunun altını çizmek isterim.

21 Tweet

Haziran 2013 tarihinde katıldı

290 Takip edilen **110** Takipçi

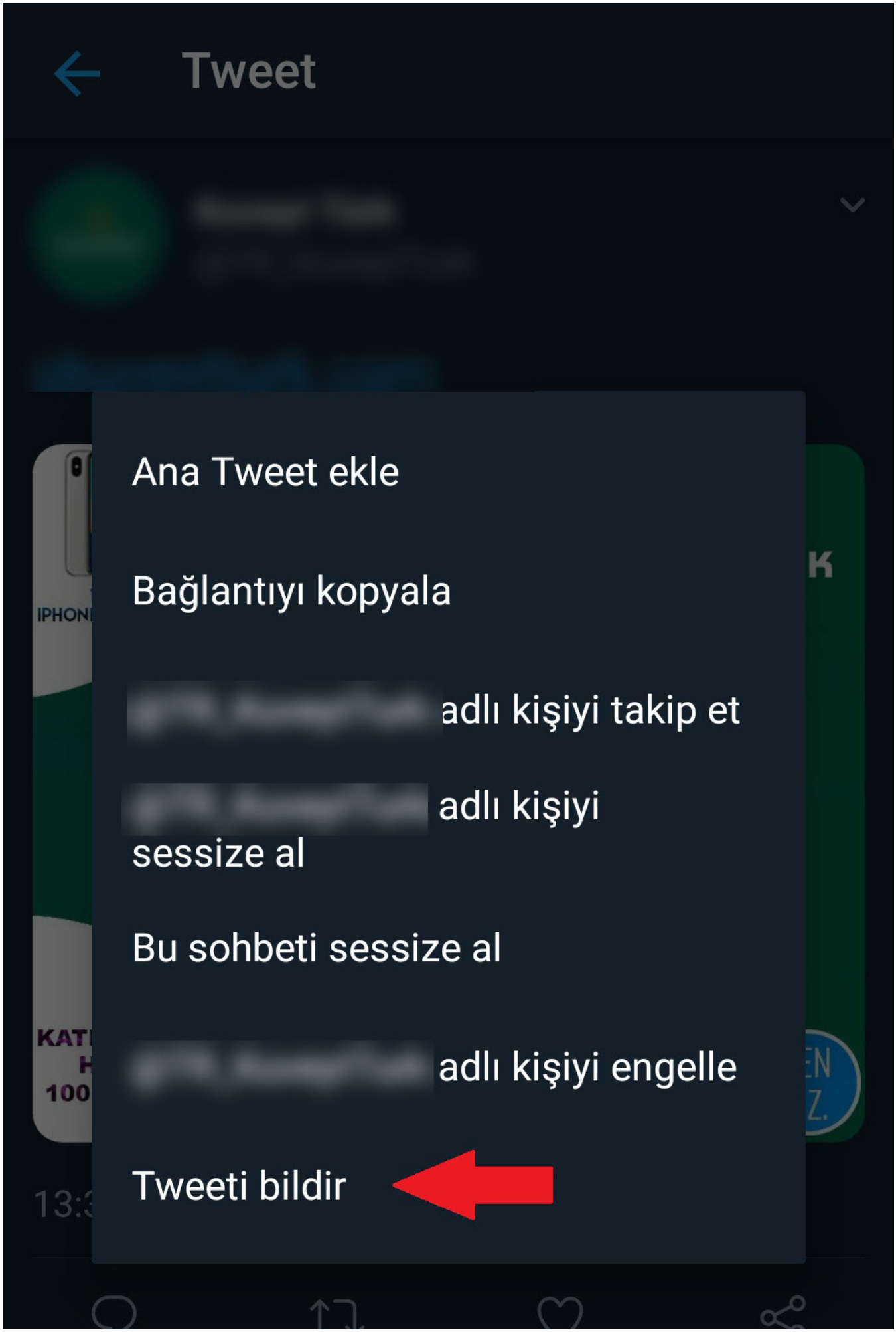
Tweet | Tweetler ve yanıtlar | Medya | Beğeni

· 18sa

5

· 18sa

47 39


Tweet
Ana Tweet ekle
Bağlantıyı kopyala
adlı kişiyi takip et
adlı kişiyi sessize al
Bu sohbeti sessize al
adlı kişiyi engelle
Tweeti bildir

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.