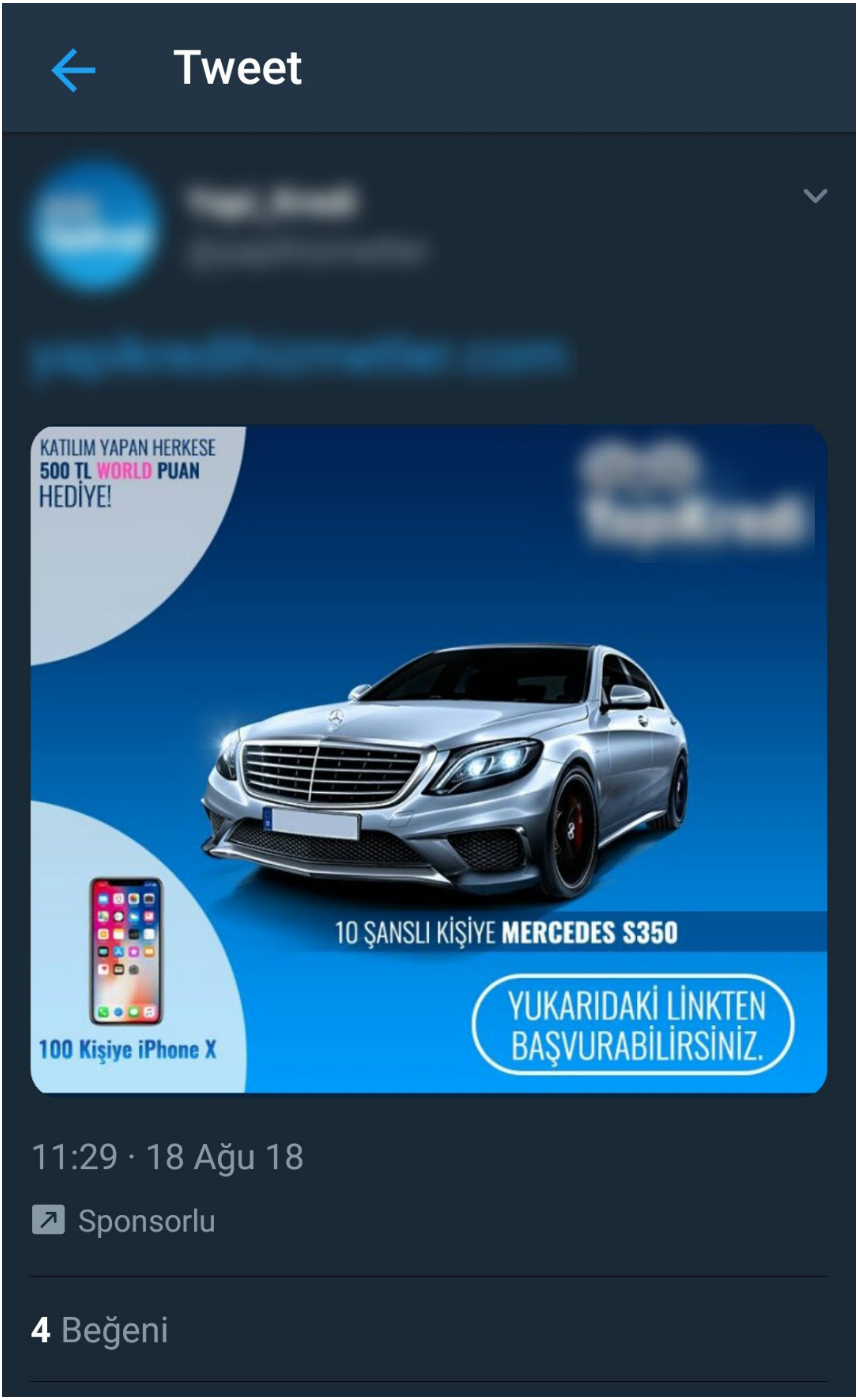
Sponsored Scamming

written by Mert SARICA | 1 October 2018

As a security researcher who keeps an eye on Twitter to stay informed about developments in the world of cyber security, I noticed that as of August 2018, phishing ads targeting bank customers began to appear on Twitter. At first, I only reported these tweets to Twitter, but as the number of messages from my followers increased and these ads continued until October, I decided to take a closer look at this issue.



Tweet

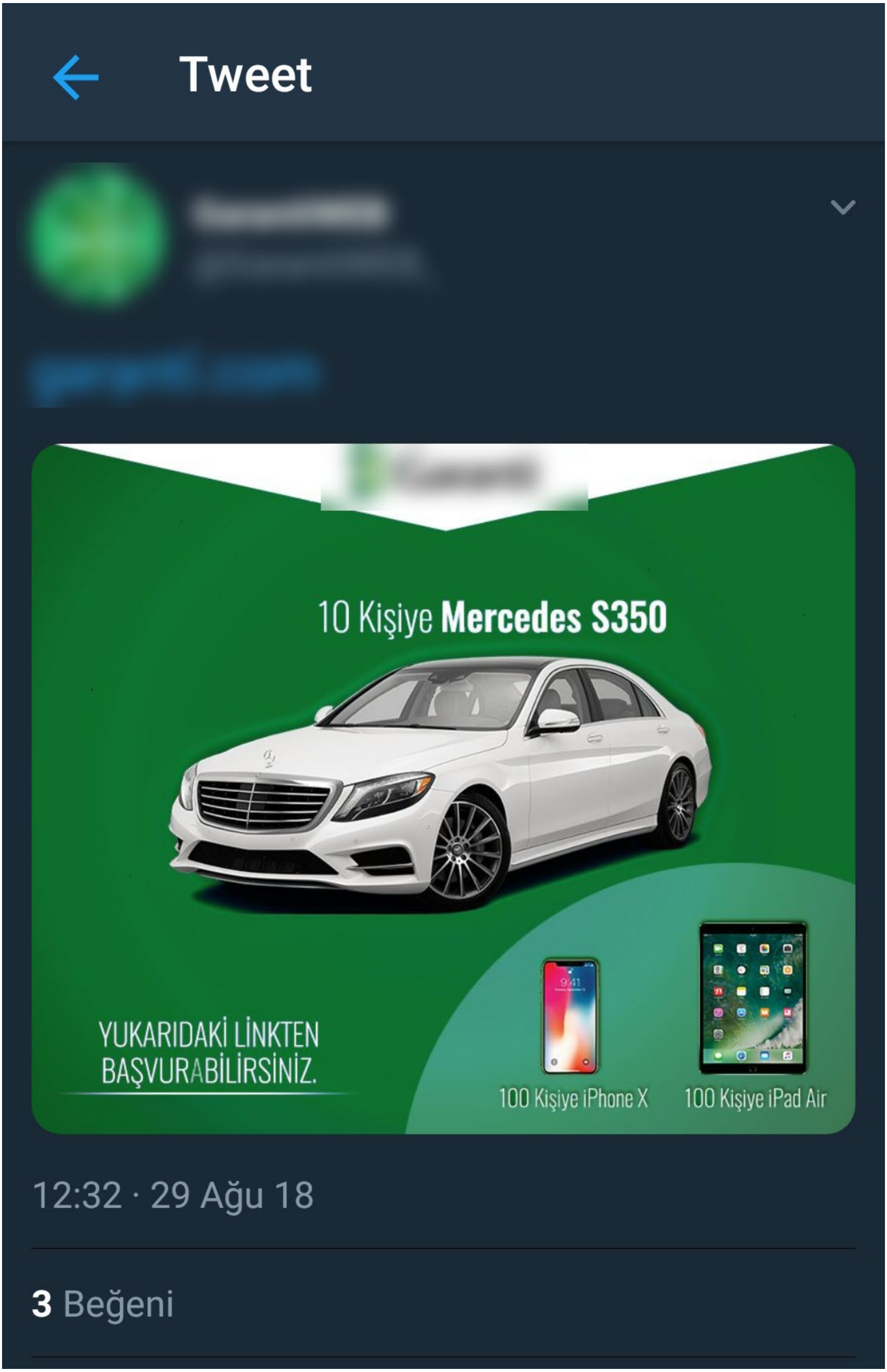
[redacted]

[redacted]

11:29 · 18 Ağu 18

Sponsorlu

4 Beğeni



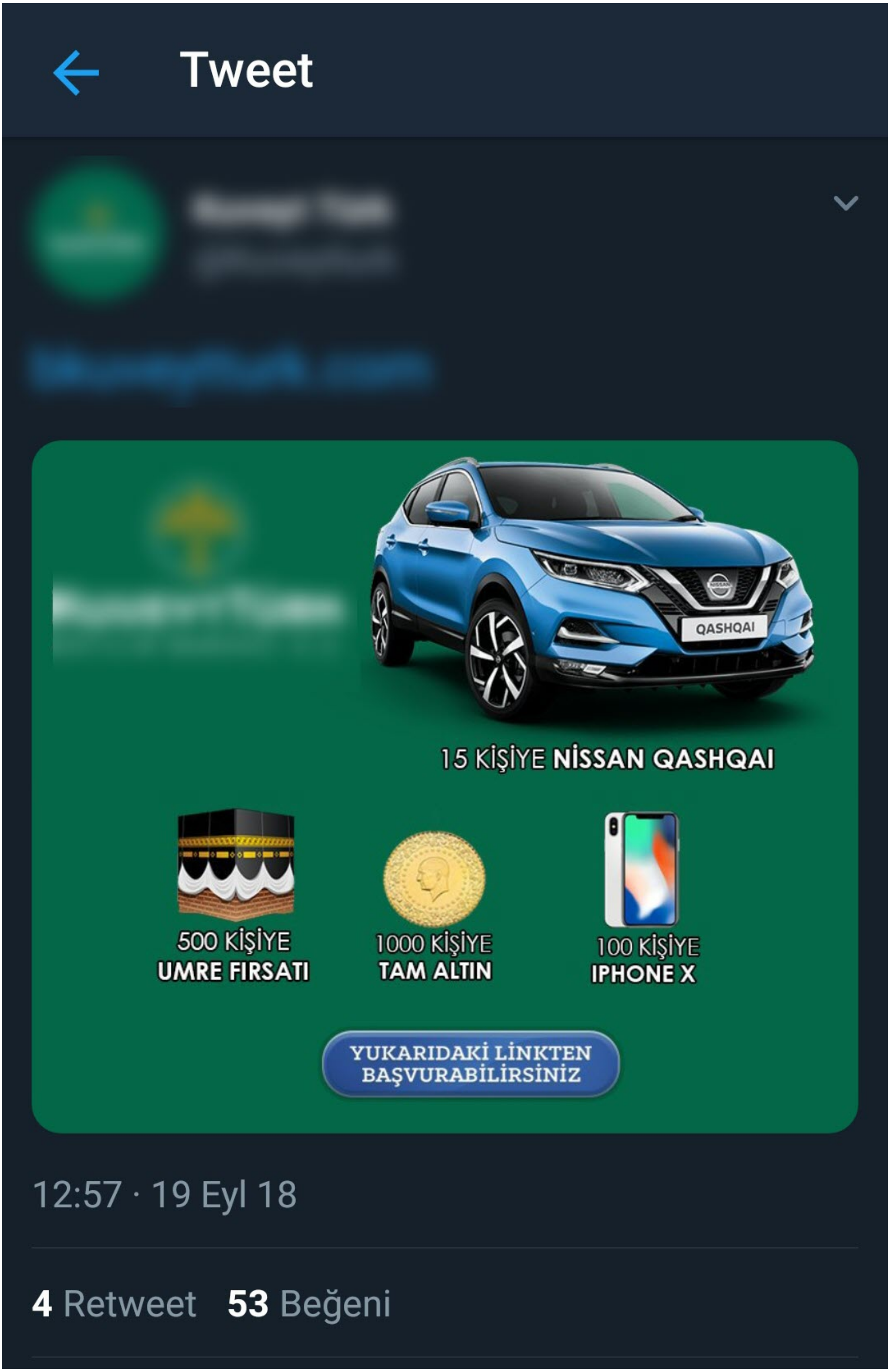
Tweet

[redacted]

[redacted]

12:32 · 29 Ağu 18

3 Beğeni



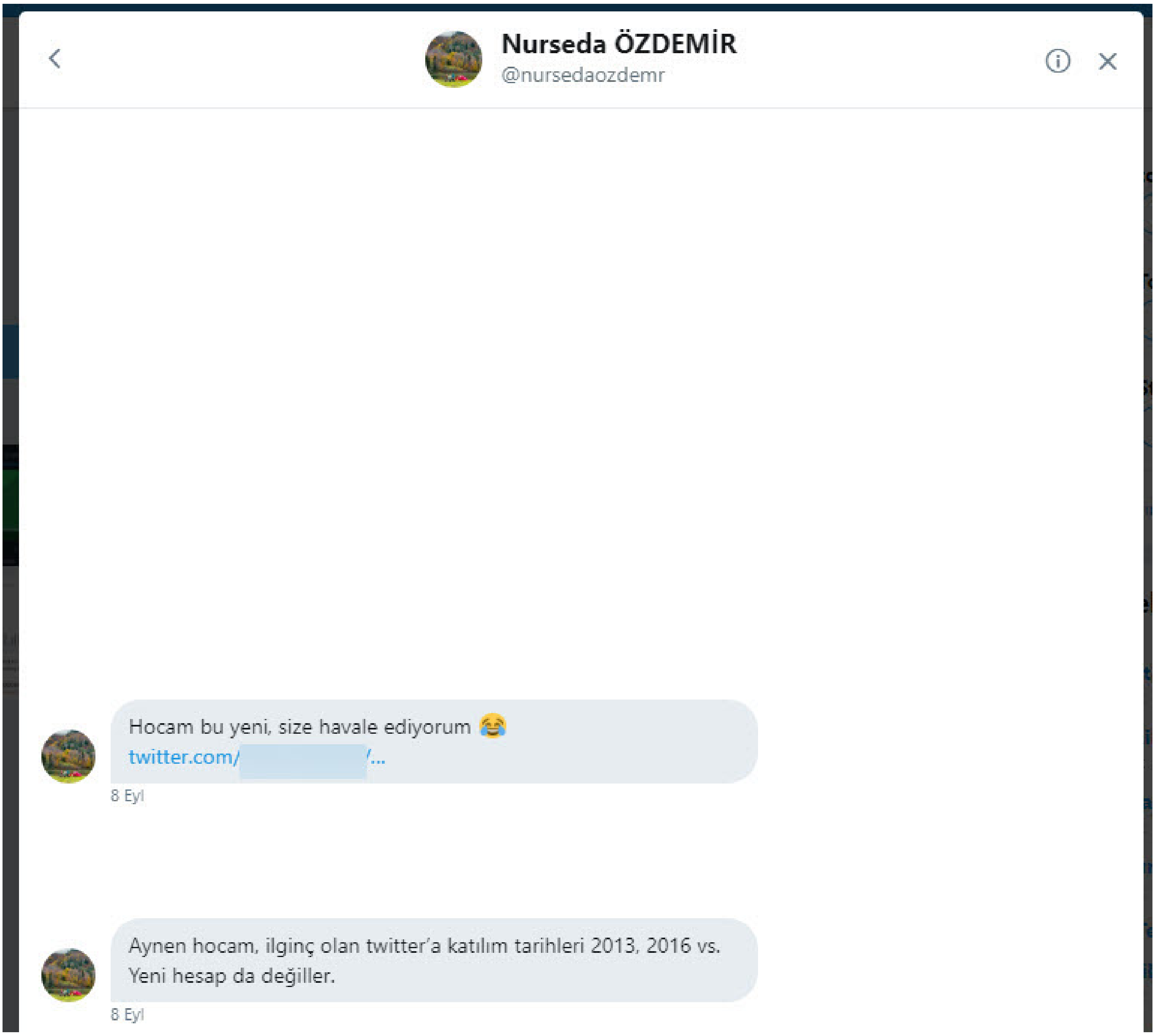
Tweet

[redacted]

[redacted]

12:57 · 19 Eyl 18

4 Retweet 53 Beğeni



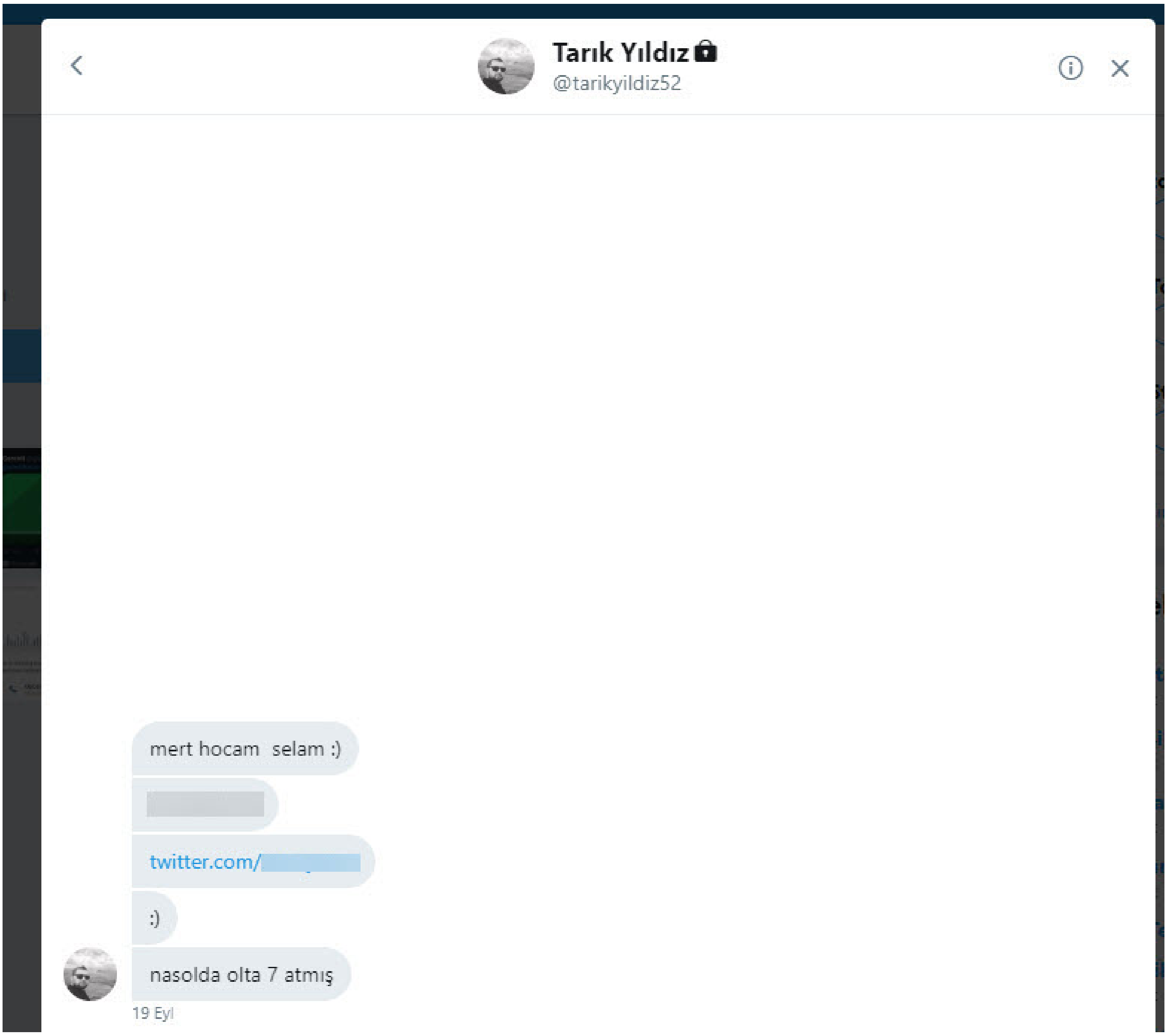
Nurseda ÖZDEMİR
@nursedaozdemr

Hocam bu yeni, size havale ediyorum 😂
twitter.com/[redacted]/...

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 :)

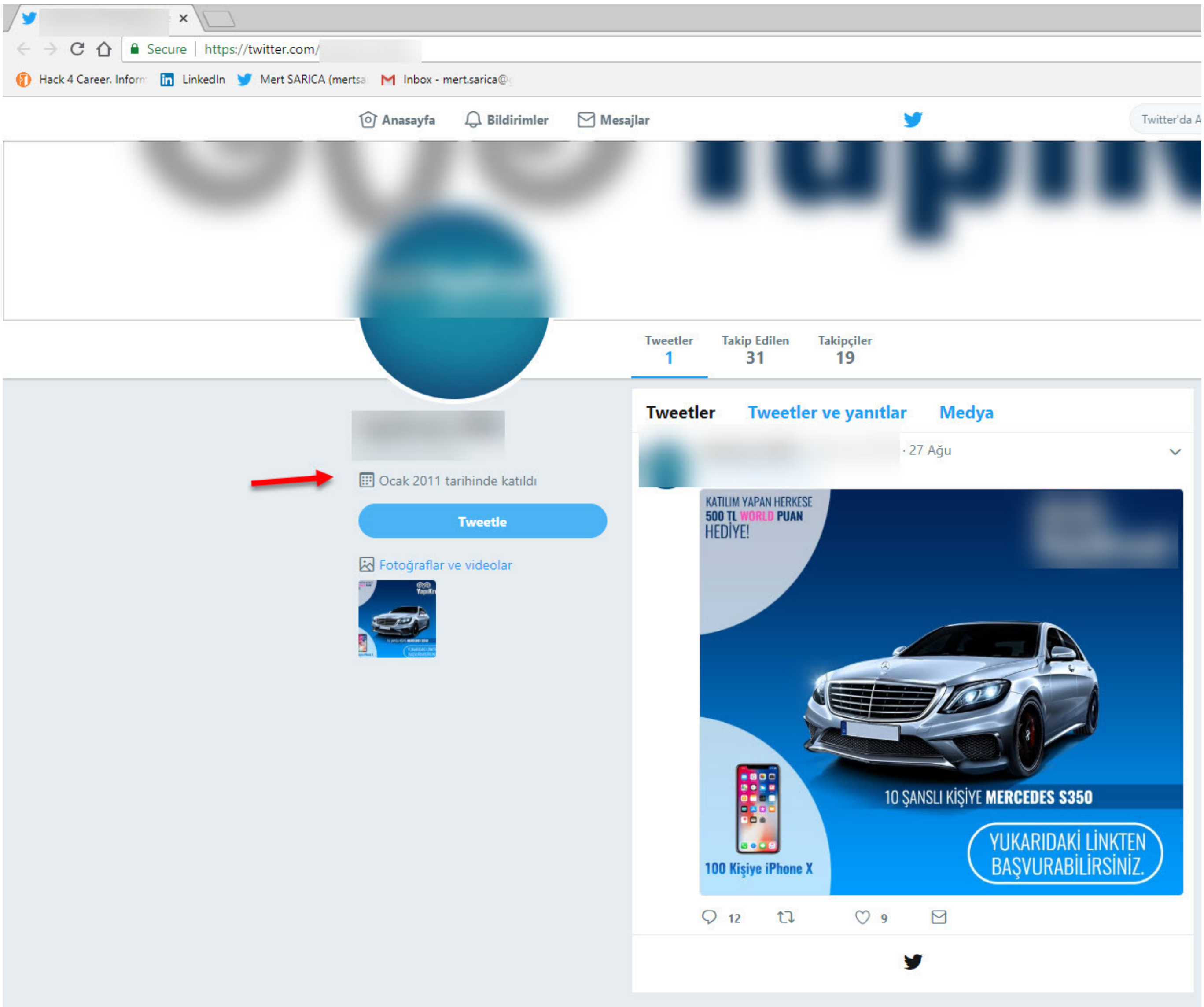
[redacted]

twitter.com/[redacted]

:)

nasolda olta 7 atmış

19 Eyl



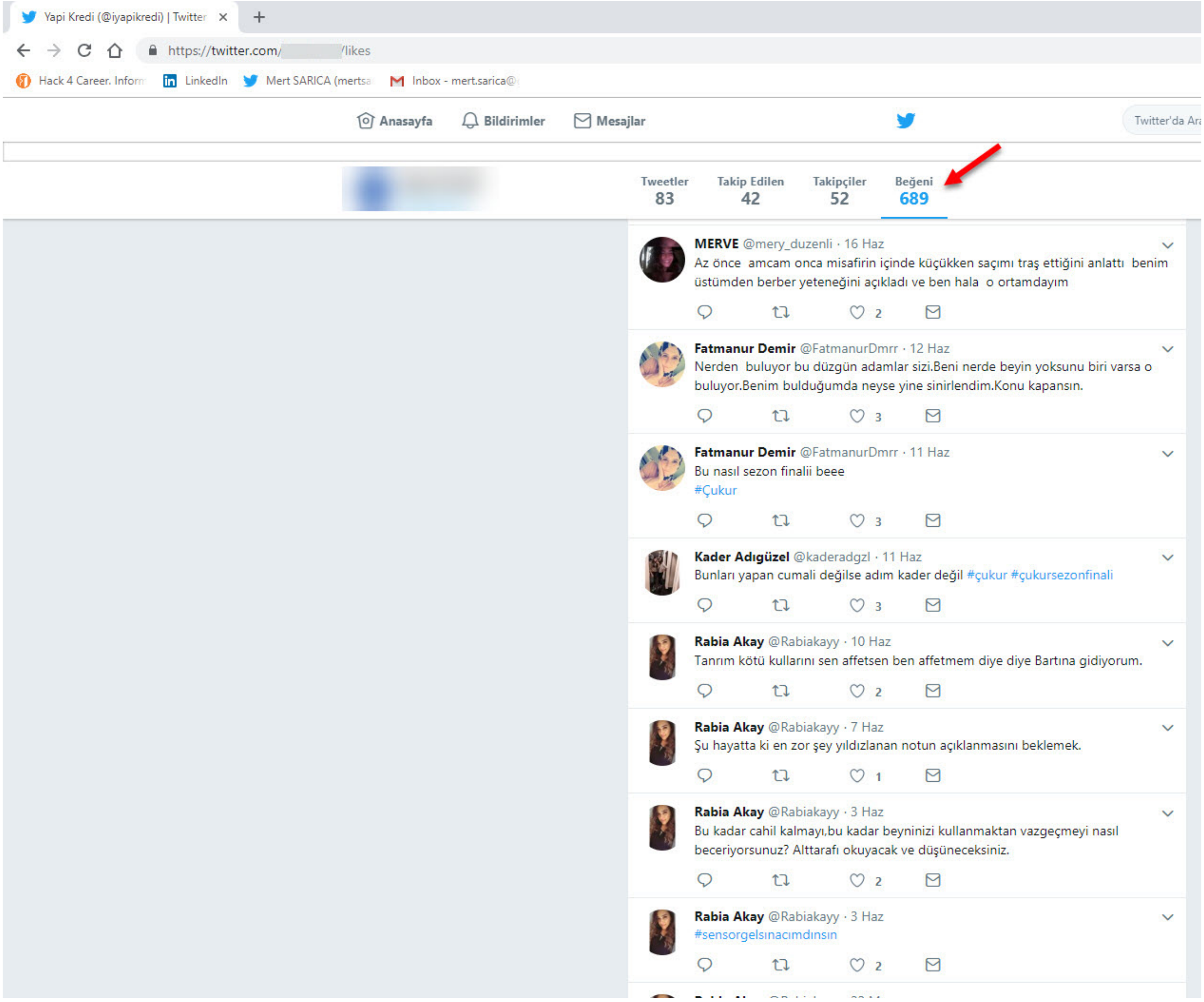
Tweetler 1 | Takip Edilen 31 | Takipçiler 19

[redacted]

Ocak 2011 tarihinde katıldı

[redacted] · 27 Ağu

12 · 9



[redacted]

Tweetler 83 · Takip Edilen 42 · Takipçiler 52 · Beğeni 689

MERVE @mery_duzenli · 16 Haz
Az önce amcam onca misafirin içinde küçükken saçımı traş ettiğini anlattı benim üstümden berber yeteneğini açıkladı ve ben hala o ortamdayım
2

Fatmanur Demir @FatmanurDmrr · 12 Haz
Nerden buluyor bu düzgün adamlar sizi.Beni nerde beyin yoksunu biri varsa o buluyor.Benim bulduğumda neyse yine sinirlendim.Konu kapansın.
3

Fatmanur Demir @FatmanurDmrr · 11 Haz
Bu nasıl sezon finalii beee
#Çukur
3

Kader Adıgüzel @kaderadgzl · 11 Haz
Bunları yapan cumali değilse adım kader değil #çukur #çukursezonfinali
3

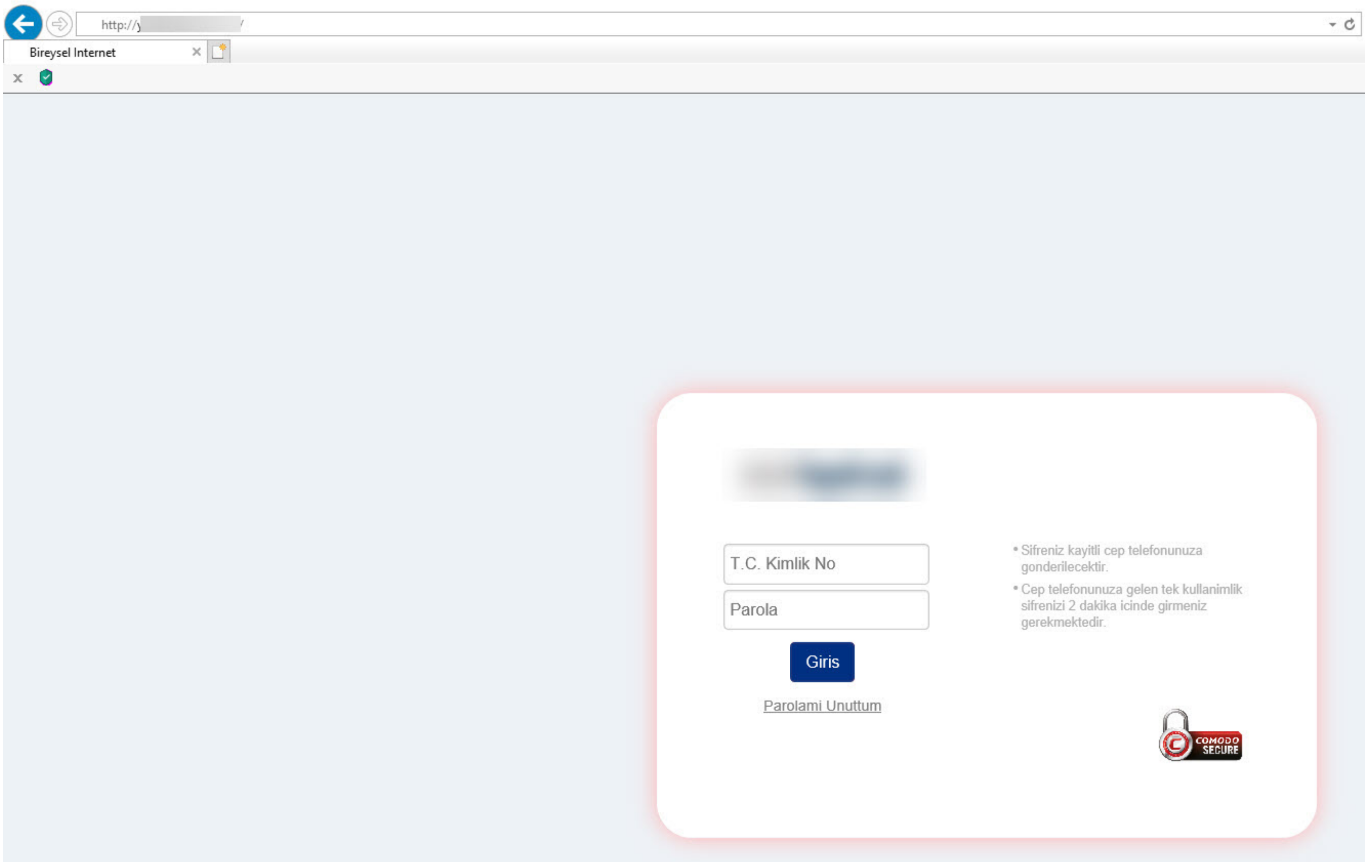
Rabia Akay @Rabiakayy · 10 Haz
Tanrım kötü kullarını sen affetsen ben affetmem diye diye Bartına gidiyorum.
2

Rabia Akay @Rabiakayy · 7 Haz
Şu hayatta ki en zor şey yıldızlanan notun açıklanmasını beklemek.
1

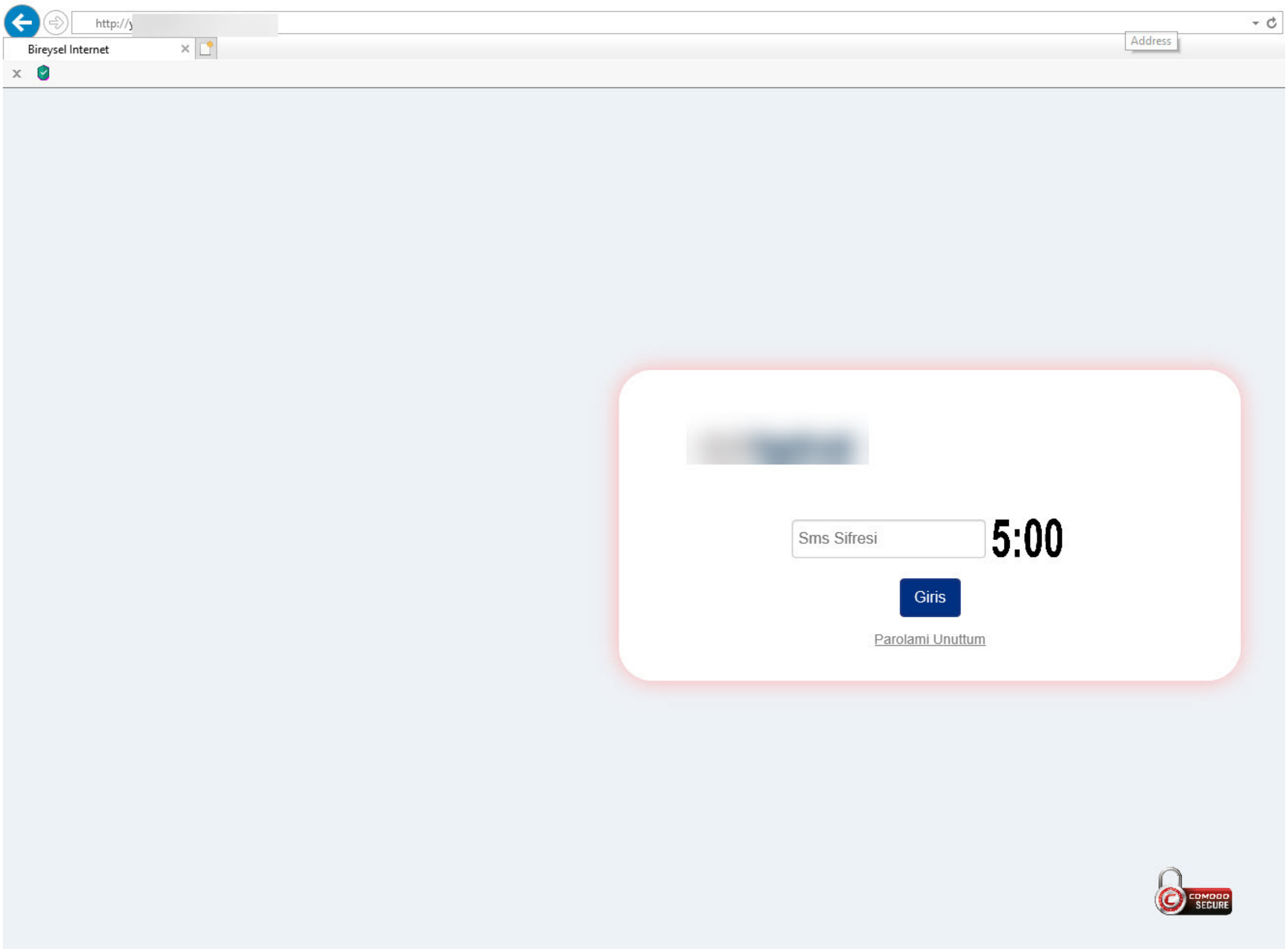
Rabia Akay @Rabiakayy · 3 Haz
Bu kadar cahil kalmayı,bu kadar beyninizi kullanmaktan vazgeçmeyi nasıl beceriyorsunuz? Alttarafı okuyacak ve düşüneceksiniz.
2

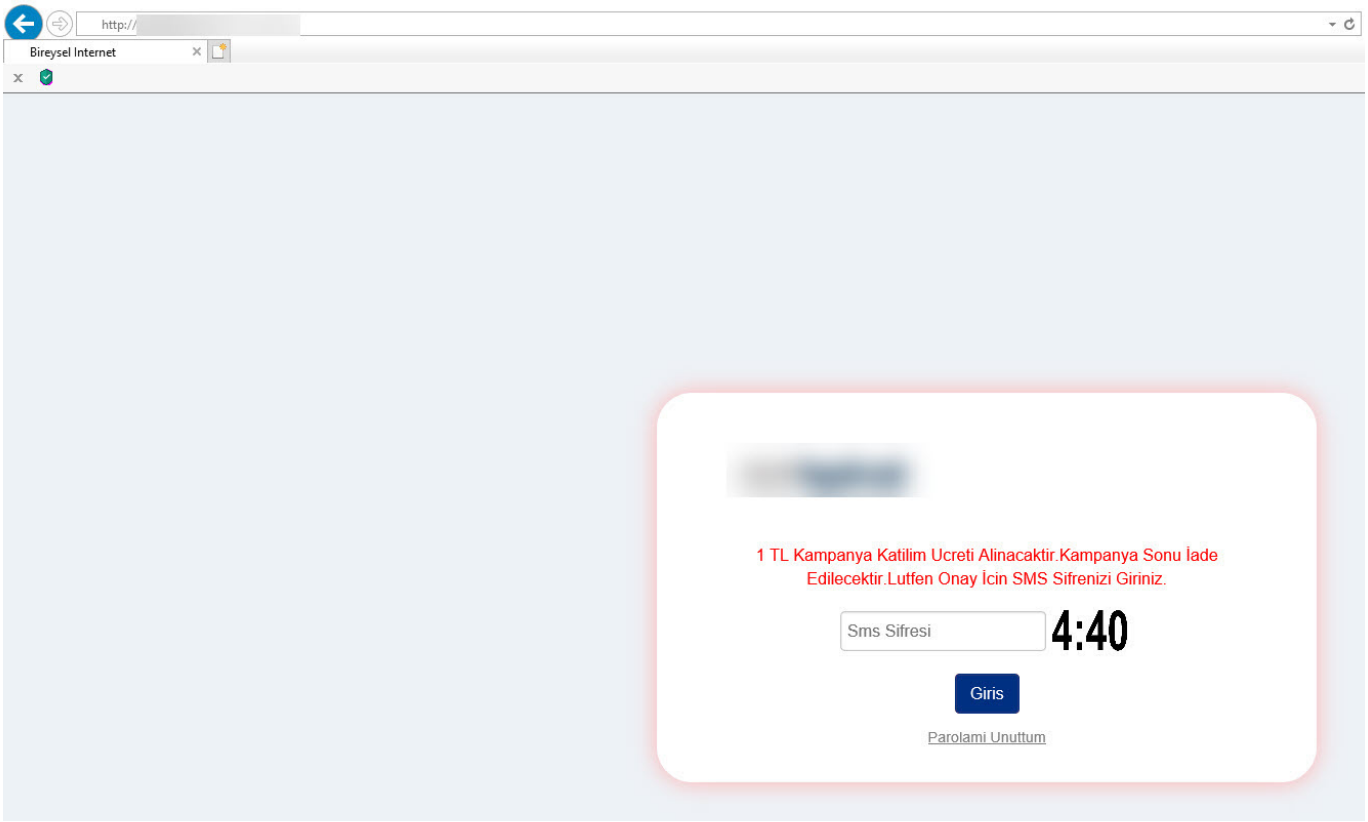
Rabia Akay @Rabiakayy · 3 Haz
#sensorgelsınacımdınsın
2

When I followed the link in one of the phishing tweets, I found that the scammers were stealing the customer’s username, password, verification code sent via SMS, and transfer verification code used during internet banking login.



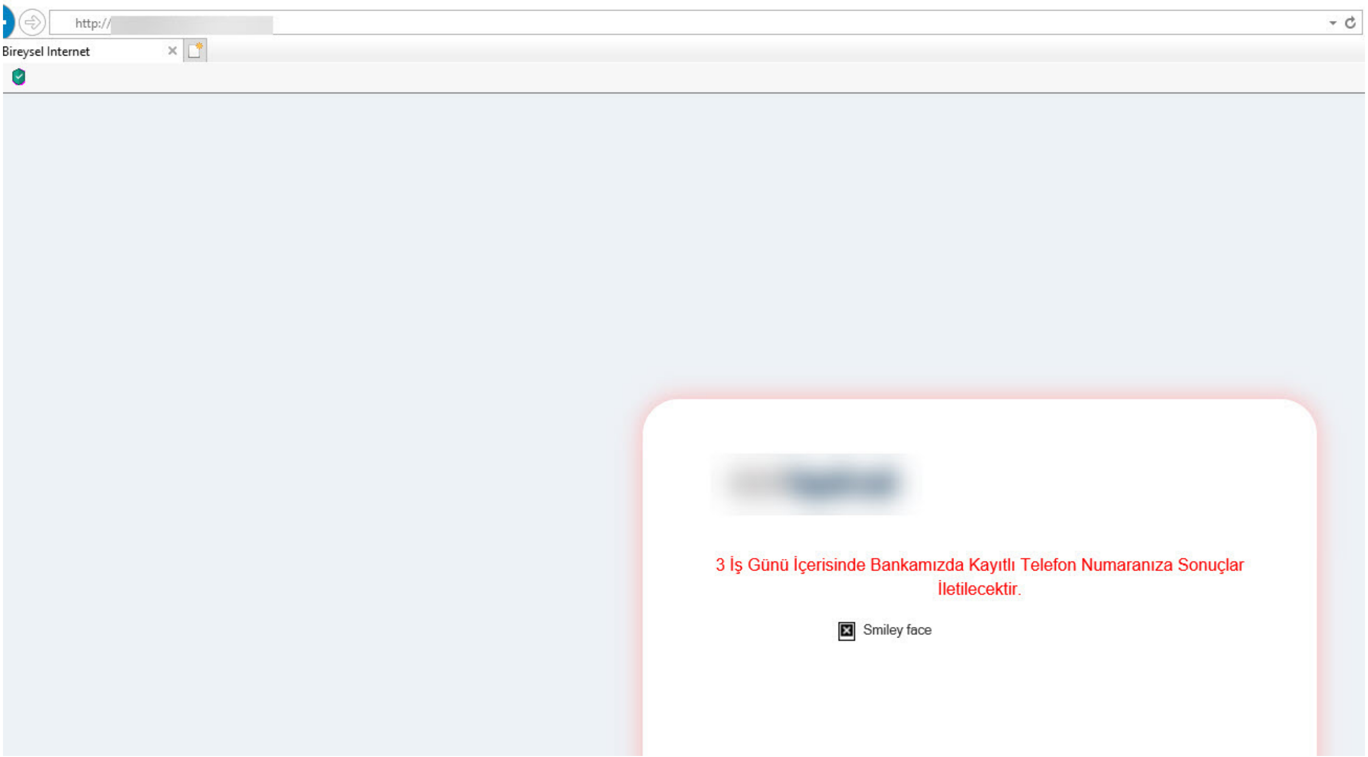
- Sifreniz kayitli cep telefonunuza gonderilecektir.
- Cep telefonunuza gelen tek kullanimlik sifrenizi 2 dakika icinde girmeniz gerekmektedir.





1 TL Kampanya Katilim Ucreti Alinacaktir.Kampanya Sonu İade Edilecektir.Lutfen Onay İcin SMS Sifrenizi Giriniz.

Sms Sifresi 4:40



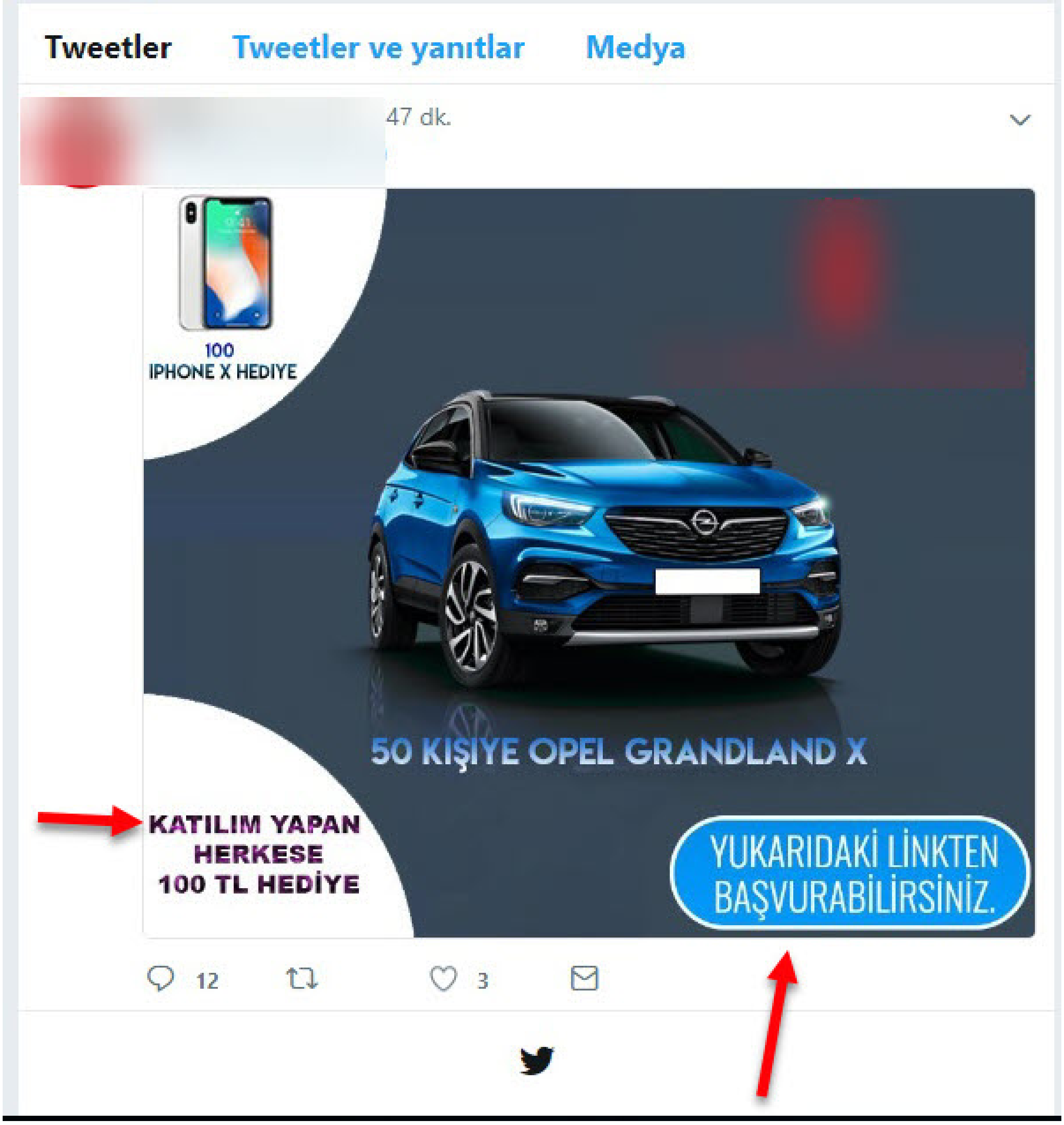
3 İş Günü İçerisinde Bankamızda Kayıtlı Telefon Numaranıza Sonuçlar İletilecektir.

Like many of you, when I see these sponsored phishing ads on Twitter, I have some questions and answers that come to mind:

1. Why can’t Twitter take action to block these phishing ads that have been the subject of complaint reports for months and look very similar to each other?
2. How is it possible that some of the accounts used for phishing tweets were created years ago?

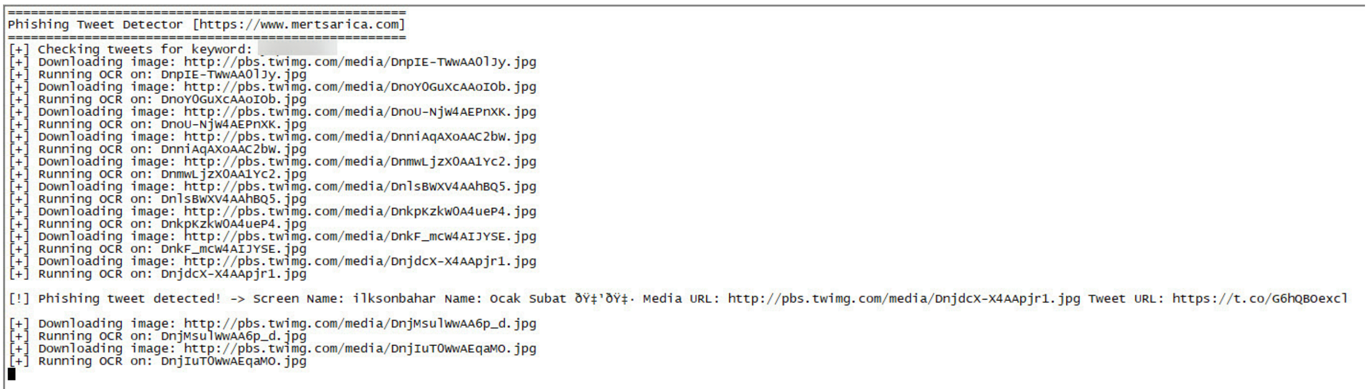
3. How can similar phishing tweets be detected?

As I looked for answers to these questions one by one, I can say that while I was unable to find an answer to the first question, I was surprised that Twitter appeared to be so helpless (or perhaps indifferent) in the face of these phishing ads. When I came to answer the second question, the likely reason that these accounts used for phishing are old, as stated on Twitter’s help page, was that they allow users to change their username. Based on this information, it can be said that these accounts used for phishing are probably hacked and used by scammers for their own purposes. As for the third question, how to detect phishing tweets, I decided to conduct a study using Optical Character Recognition (OCR) technology by identifying common keywords in Turkish such as “LUCKY” , “PARTICIPANT”, “ABOVE” in most messages.



After seeing that most bank customers are facing these phishing tweets and shared by official Twitter accounts of the banks, I quickly started to design a tool in my mind. The basic things the tool had to do were to search for bank names on Twitter, download the images shared in the tweets, analyze them using OCR, and send an email warning when the keywords “LUCKY” , “PARTICIPANT” , “ABOVE” were detected. I began coding this tool using Python, taking advantage of the Tweepy library, and a short time later, my Phishing Tweet Detector was developed.

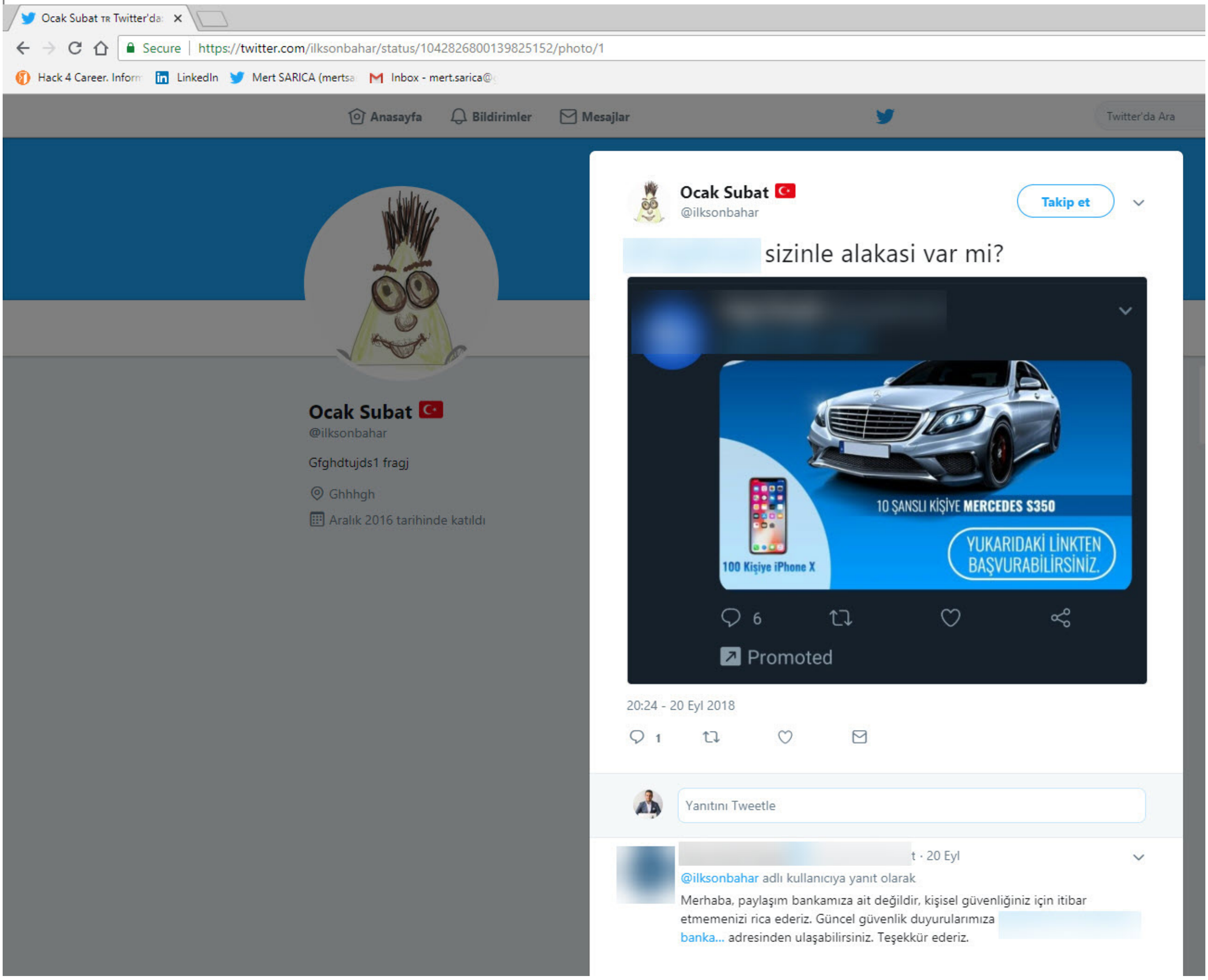
After running the tool, a short time later, it was able to detect a phishing tweet shared by a Twitter user with a bank, and this helped the institution to fight against such scammers, thus my idea of helping citizens and institutions to fight against these types of scammers was successfully implemented. :)



```
=====================================================
Phishing Tweet Detector [https://www.mertsarica.com]
=====================================================
[+] Checking tweets for keyword: [redacted]
[+] Downloading image: http://pbs.twimg.com/media/DnpIE-TWwAA0lJy.jpg
[+] Running OCR on: DnpIE-TWwAA0lJy.jpg
[+] Downloading image: http://pbs.twimg.com/media/DnoY0GuXcAAoIOb.jpg
[+] Running OCR on: DnoY0GuXcAAoIOb.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/DnmwLjzX0AA1Yc2.jpg
[+] Running OCR on: DnmwLjzX0AA1Yc2.jpg
[+] Downloading image: http://pbs.twimg.com/media/DnlsBWXV4AAhBQ5.jpg
[+] Running OCR on: DnlsBWXV4AAhBQ5.jpg
[+] Downloading image: http://pbs.twimg.com/media/DnkpKzkW0A4ueP4.jpg
[+] Running OCR on: DnkpKzkW0A4ueP4.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‡'ðŸ‡· 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
```



Ocak Subat
@ilksonbahar
Gfghdtujds1 fragj
Ghhhgh
Aralık 2016 tarihinde katıldı

Ocak Subat
@ilksonbahar

[redacted] sizinle alakasi var mi?

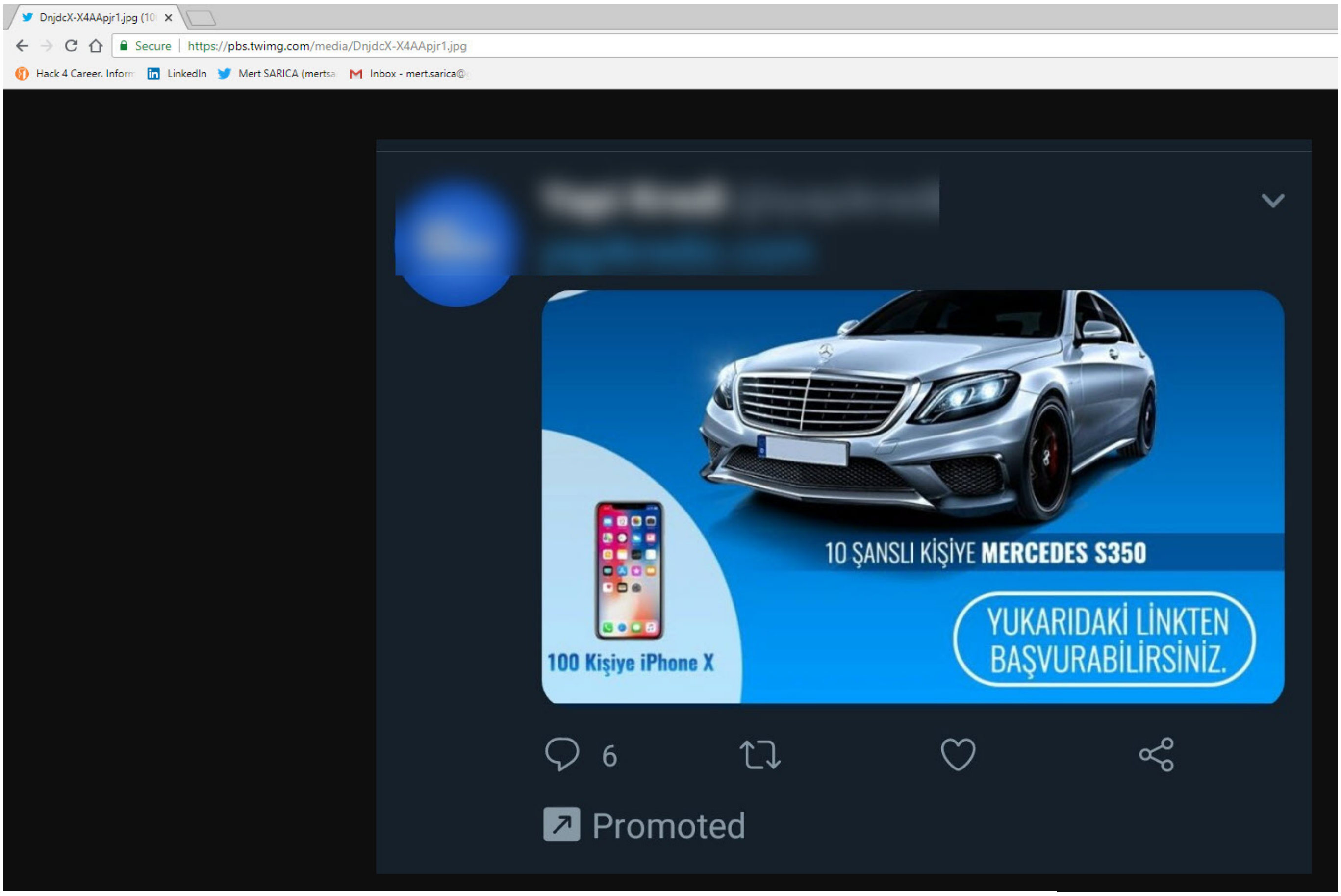
10 ŞANSLI KİŞİYE MERCEDES S350
100 Kişiye iPhone X
YUKARIDAKİ LİNKTEN BAŞVURABİLİRSİNİZ.
6
Promoted

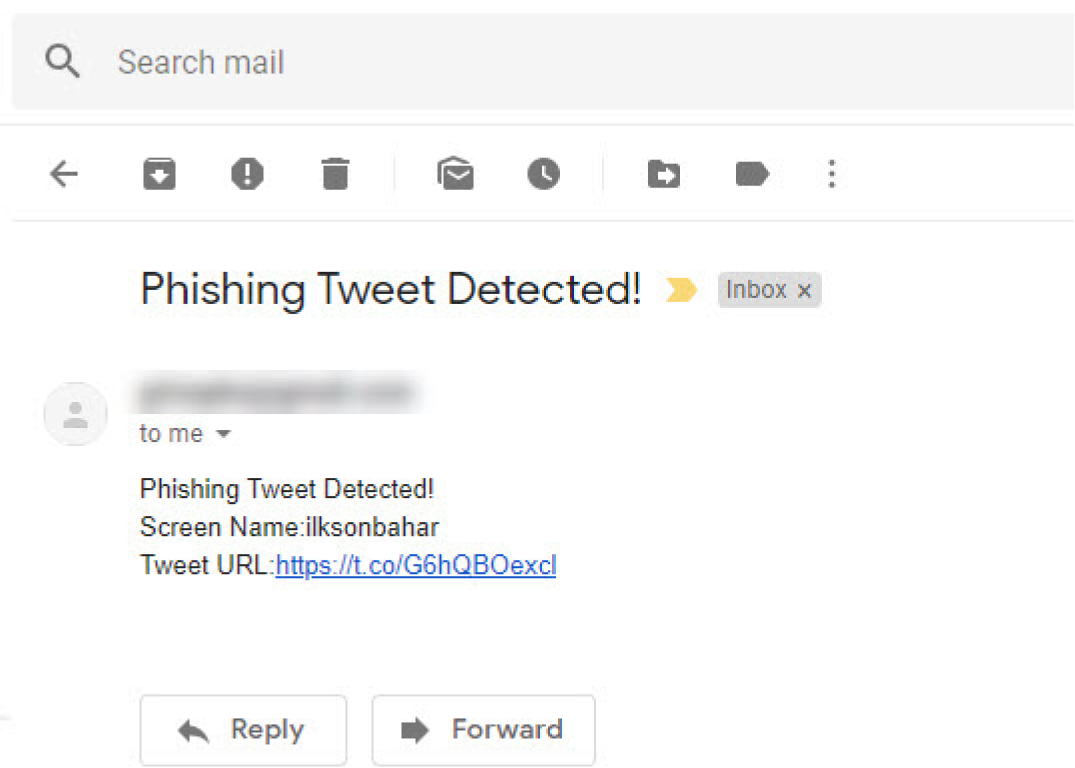
20:24 - 20 Eyl 2018

[redacted] · 20 Eyl

@ilksonbahar adlı kullanıcıya yanıt olarak

Merhaba, paylaşım bankamıza ait değildir, kişisel güvenliğiniz için itibar etmemenizi rica ederiz. Güncel güvenlik duyurularımıza [redacted] banka... adresinden ulaşabilirsiniz. Teşekkür ederiz.



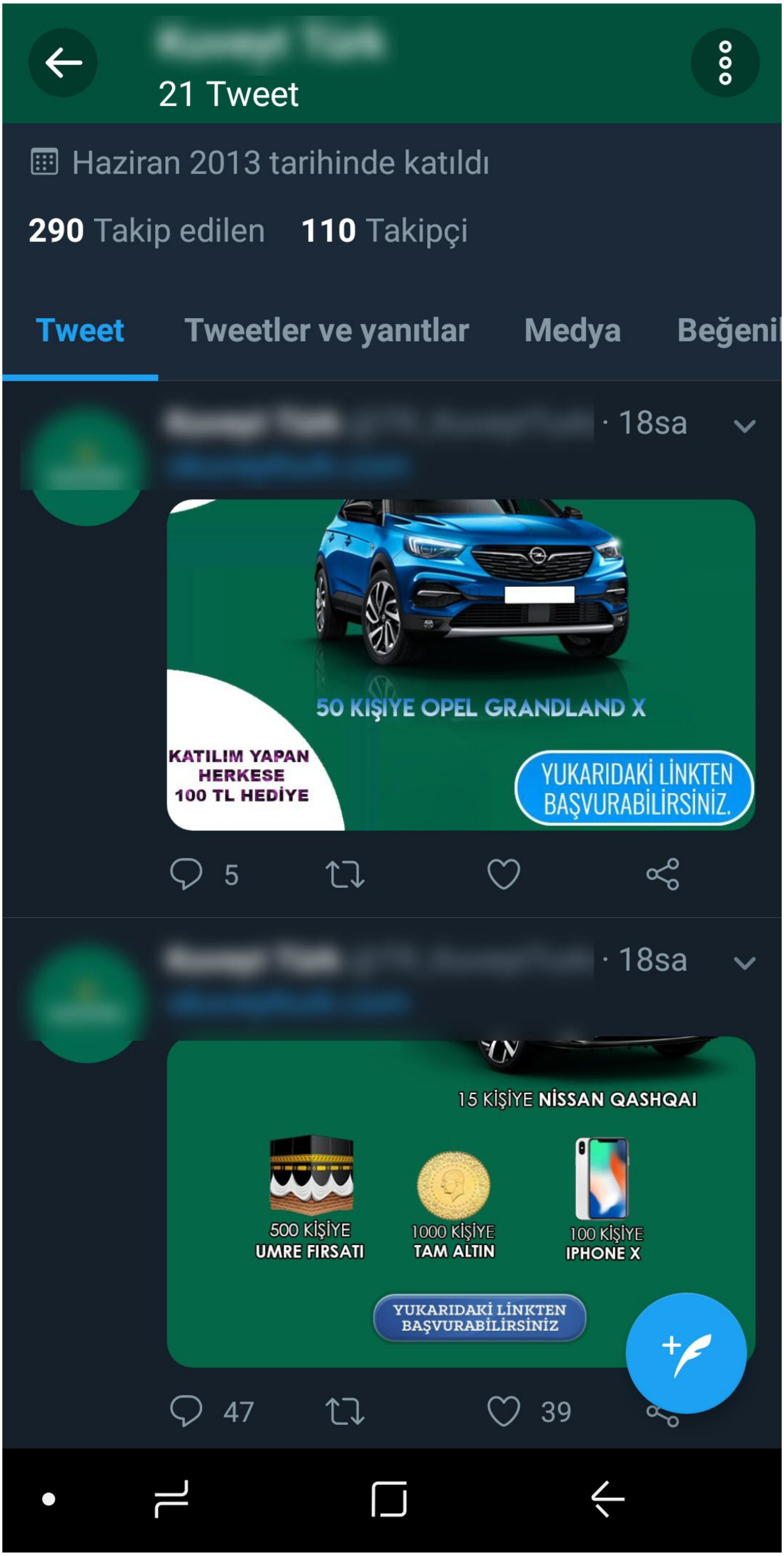


Phishing Tweet Detected!

[redacted]

Phishing Tweet Detected!
Screen Name:ilksonbahar
Tweet URL:https://t.co/G6hQBOexcl

Before I put an end to my article, I would like to emphasize that it is very, very important for those who come across phishing messages to report them to their banks and the social media platform as soon as possible (just like reporting a Tweet).



[redacted]
21 Tweet

Haziran 2013 tarihinde katıldı

290 Takip edilen **110** Takipçi

Tweet Tweetler ve yanıtlar Medya Beğeni

[redacted] · 18sa

50 KIŞIYE OPEL GRANDLAND X

KATILIM YAPAN HERKESE 100 TL HEDİYE

YUKARIDAKİ LİNKTEN BAŞVURABİLİRSİNİZ.

5

[redacted] · 18sa

15 KİŞİYE NİSSAN QASHQAI

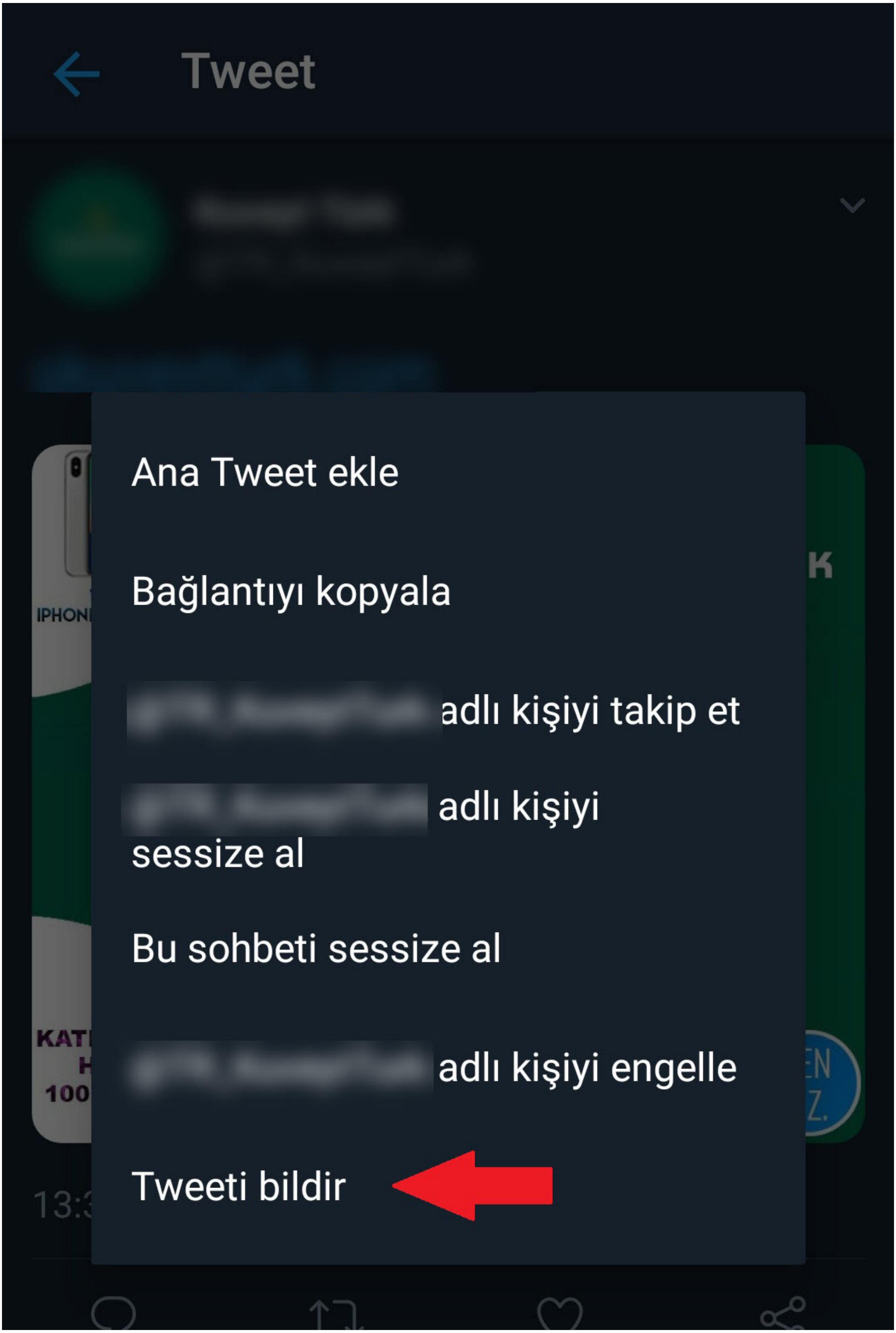
500 KİŞİYE UMRE FIRSATI

1000 KİŞİYE TAM ALTIN

100 KİŞİYE IPHONE X

YUKARIDAKİ LİNKTEN BAŞVURABİLİRSİNİZ

47 39



Tweet

[redacted]

Ana Tweet ekle

Bağlantıyı kopyala

[redacted] adlı kişiyi takip et

[redacted] adlı kişiyi sessize al

Bu sohbeti sessize al

[redacted] adlı kişiyi engelle

Tweeti bildir

Hope to see you in the following articles.