

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 ettiđi için bir gözü Twitter'da olan bir güvenlik arařtırmacısı 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



Yeni Akademi
@YeniAkademi



KATILIM YAPAN HERKESE
500 TL **WORLD PUAN**
HEDİYE!



10 ŞANSLI KİŞİYE **MERCEDES S350**



100 Kişiyeye iPhone X

YUKARIDAKİ LİNKTE
BAŞVURABİLİRSİNİZ.

11:29 · 18 Ağu 18

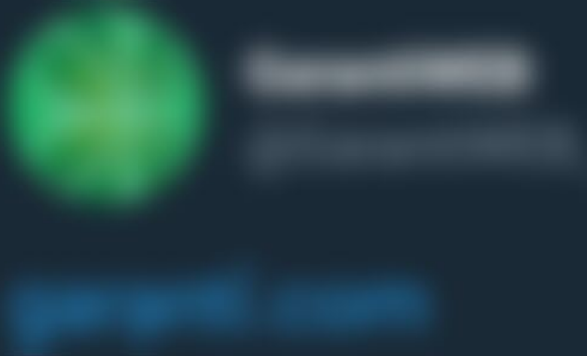


Sponsorlu

4 Beğeni



Tweet



10 Kişiyeye Mercedes S350



YUKARIDAKİ LINKTEN
BAŞVURABİLİRSİNİZ.



100 Kişiyeye iPhone X



100 Kişiyeye iPad Air

12:32 · 29 Ağu 18

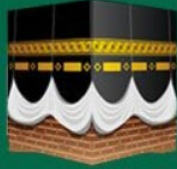
3 Beğeni



Tweet



15 KİŞİYE NISSAN QASHQAI



500 KİŞİYE
UMRE FIRSATI



1000 KİŞİYE
TAM ALTIN



100 KİŞİYE
IPHONE X

YUKARIDAKİ LİNKTE
BAŞVURABİLİRSİNİZ

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 :)

[Redacted]

twitter.com/

:)



nasolda olta 7 atmış

19 Eyl

Yapi Kredi (@yapikredi) | Twitter x

https://twitter.com/ /likes

Hack 4 Career. Inform LinkedIn Mert SARICA (mertsarica) Inbox - mertsarica@

Anasayfa Bildirimler Mesajlar

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

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.

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

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

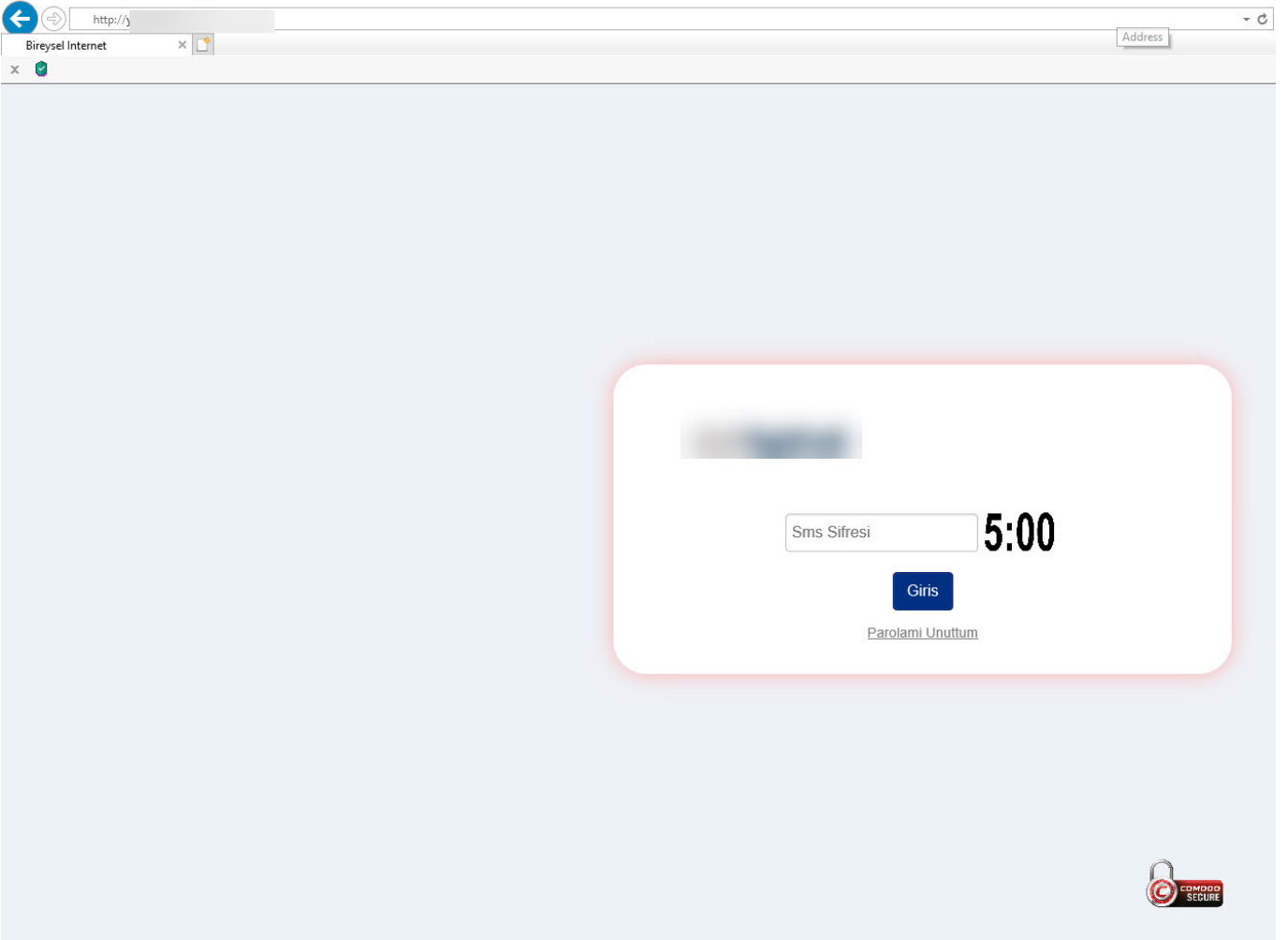
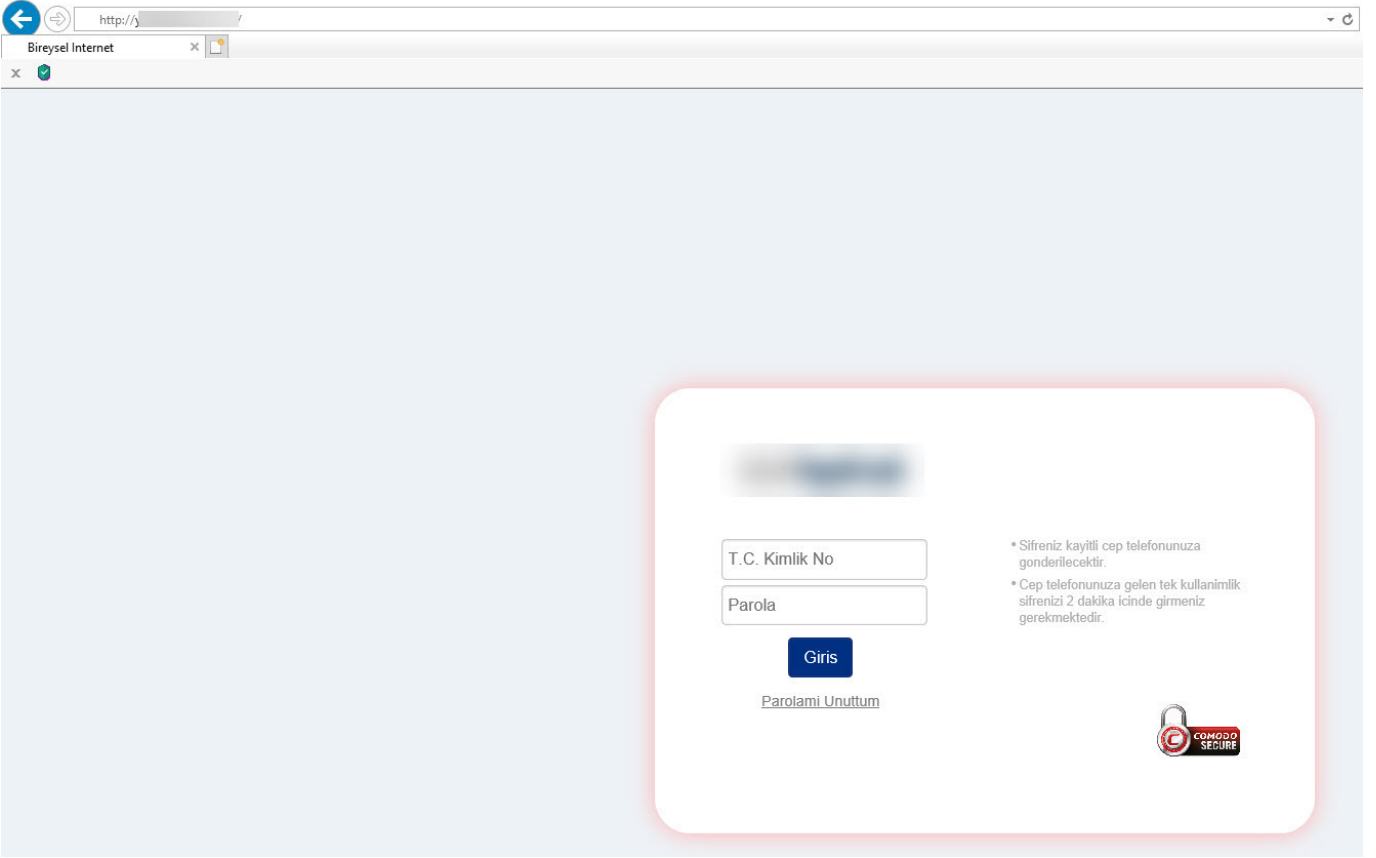
Rabia Akay @Rabiakayy · 10 Haz
Tanrım kötü kullarını sen affetsen ben affetmem diye diye Bartına gidiyorum.

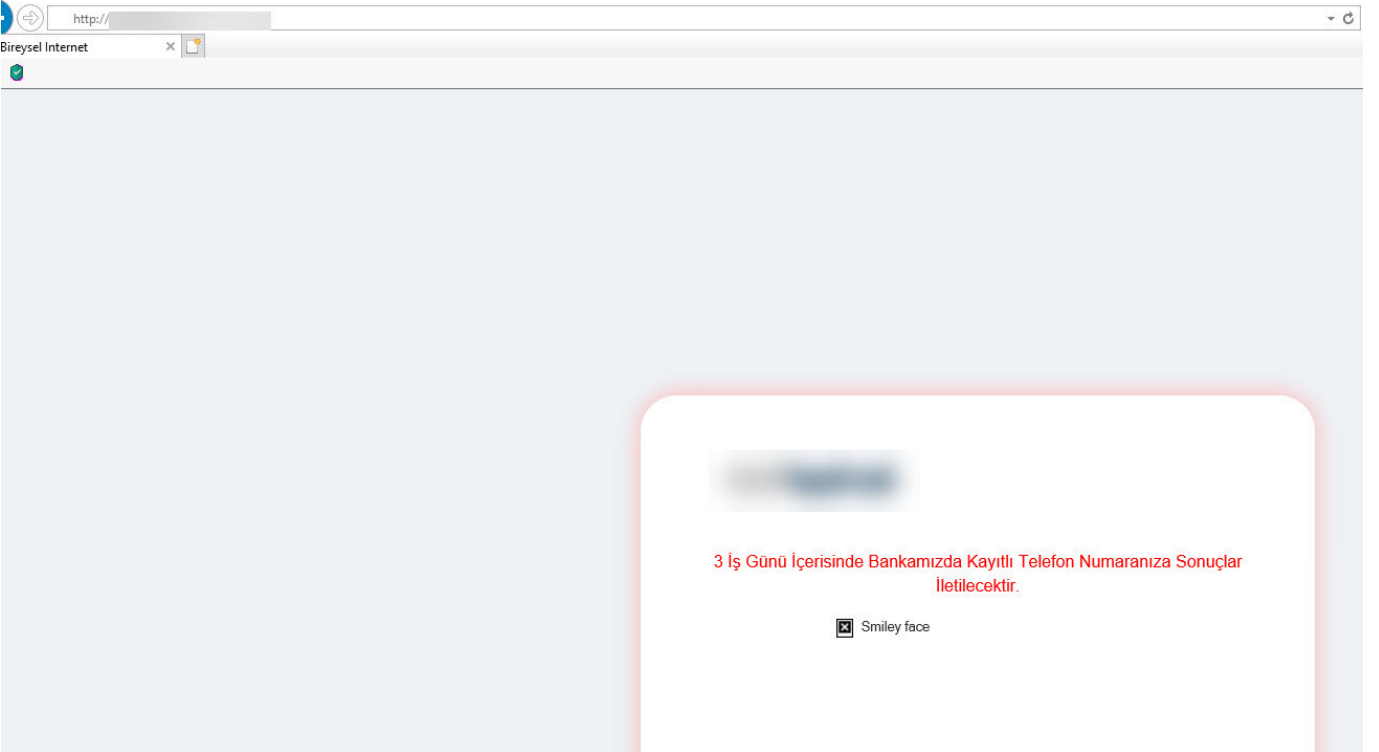
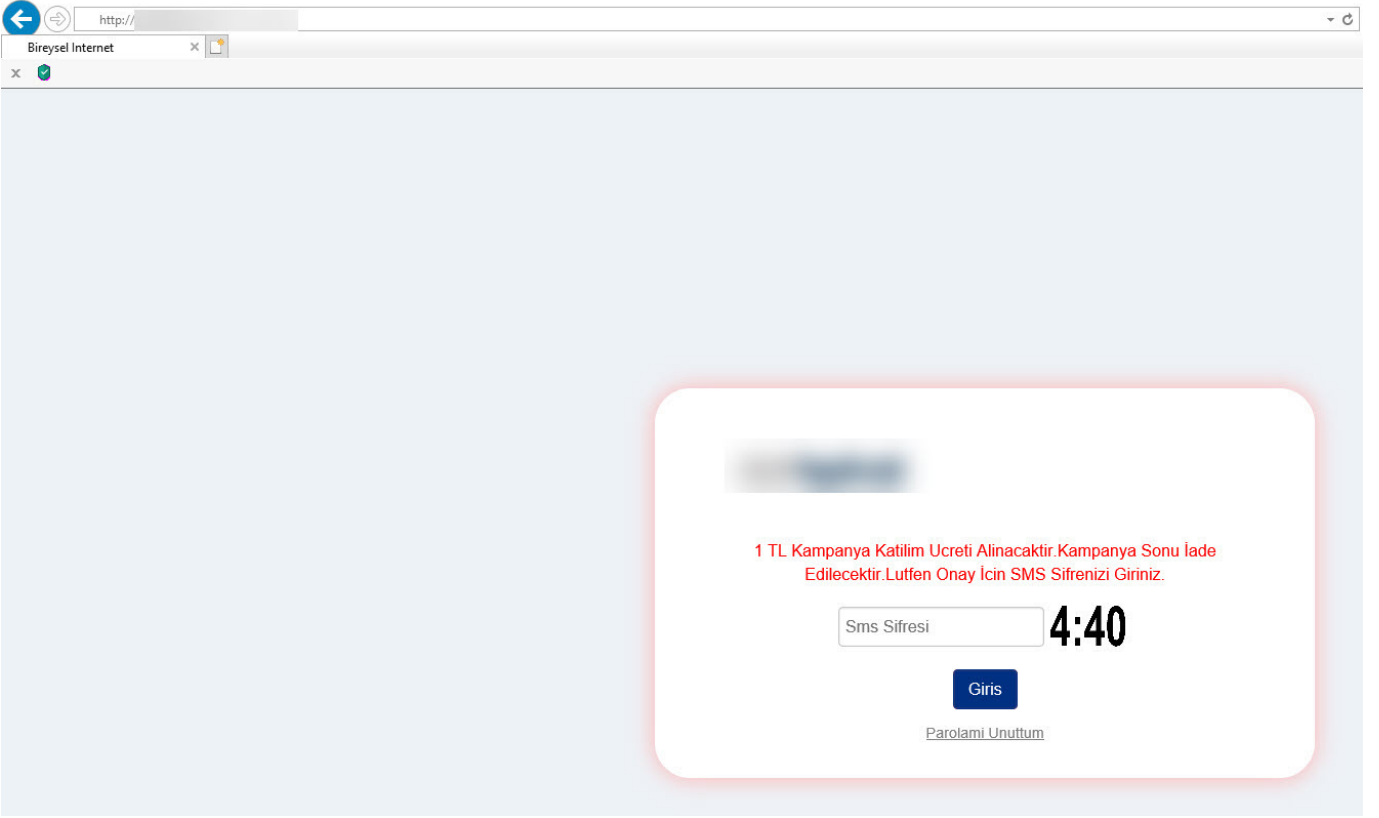
Rabia Akay @Rabiakayy · 7 Haz
Şu hayatta ki en zor şey yıldızlanan notun açıklanmasını beklemek.

Rabia Akay @Rabiakayy · 3 Haz
Bu kadar cahil kalmayı.bu kadar beyninizi kullanmaktan vazgeçmeyi nasıl beceriyorsunuz? Altıtarafı okuyacak ve düşüneneceksiniz.

Rabia Akay @Rabiakayy · 3 Haz
#sensorgelsinacimdinsin

Ortalama 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.





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

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

3. Birbirine benzeyen bu ortalama tweetleri nasıl tespit edilebilir ?

Sorulara teker teker yanıt aramaya koyulduğumda, kendi kendime ilk soruya yanıt bulmam mümkün olamasa da, Twitter'ın bu ortalama reklamları karşısında bu kadar çaresiz (belki de vurdumduymaz) kalmasına oldukça şaşırdığımı söyleyebilirim. İkinci sorunun yanıtını bulmaya geldiğimde, ortalama için kullanılan hesapların eski tarihli olmasının muhtemel sebebi, Twitter'ın buradaki yardım sayfasında belirttiği üzere kullanıcı adının değiştirilmesine imkan tanınmasıydı. Bu bilgiden yola çıkarak, ortalama tweetleri için kullanılan bu hesapların kuvvetle muhtemel hacklendiğini ve dolandırıcıların amaçları doğrultusunda kullanıldığını söyleyebiliriz. Sıra son soruya, ortalama 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 ortalama 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, YUKARIDAKİ" kelimelerini tespit etmesi durumunda e-posta ile uyarmaktır. 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 ortalama 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-TwAA013y.jpg
[+] Running OCR on: DnpIE-TwAA013y.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/Dn1sBwXV4AAhBQ5.jpg
[+] Running OCR on: Dn1sBwXV4AAhBQ5.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 0v4'0v4. Media URL: http://pbs.twimg.com/media/DnjdcX-X4AApjr1.jpg Tweet URL: https://t.co/G6hQBOexc1

[+] Downloading image: http://pbs.twimg.com/media/DnjMsulwAA6p_d.jpg
[+] Running OCR on: DnjMsulwAA6p_d.jpg
[+] Downloading image: http://pbs.twimg.com/media/DnjIuT0WwAEqAM0.jpg
[+] Running OCR on: DnjIuT0WwAEqAM0.jpg
```

Okac Subat 11 Twitter'da: X

Secure | https://twitter.com/ilksonbahar/status/1042826800139825152/photo/1

Hack 4 Career. Inform LinkedIn Mert SARICA (mertsarica) Inbox - mertsarica@

Anasayfa Bildirimler Mesajlar Twitter'da Ara

 Ocak Subat  @ilksonbahar

Gfghdtujds1 fragj

Ghhgh

Aralık 2016 tarihinde katıldı

sizinle alakasi var mi?



10 Şanslı Kişiye MERCEDES S350

100 Kişiye iPhone X

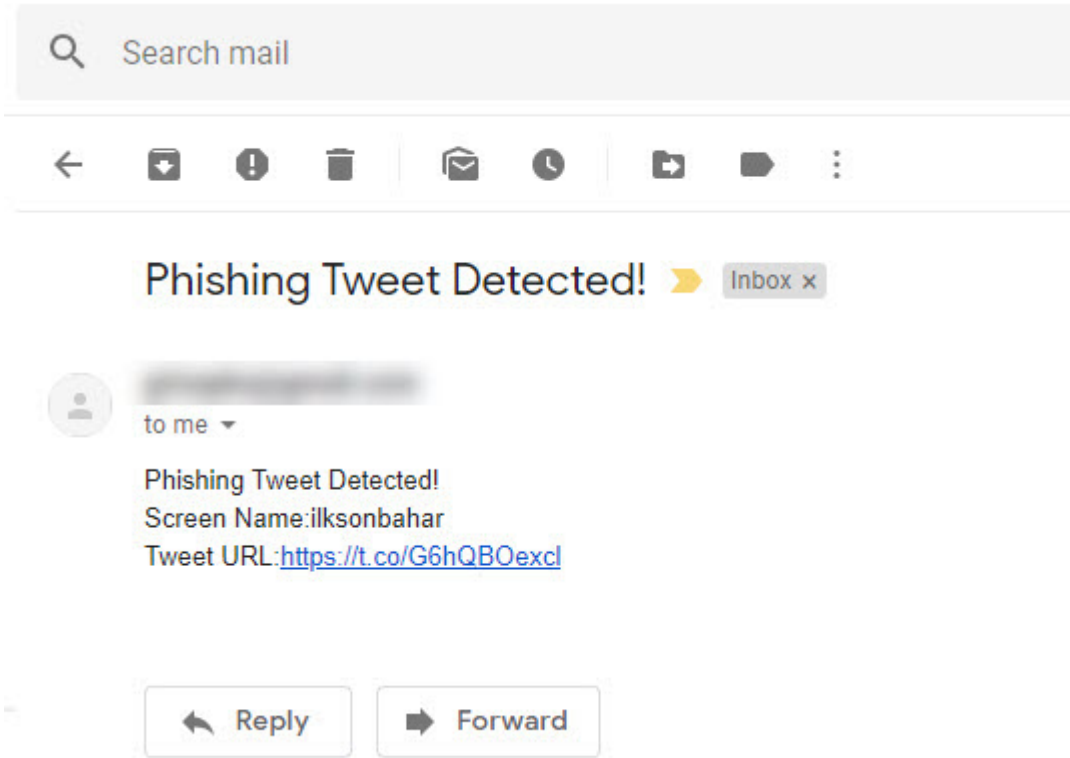
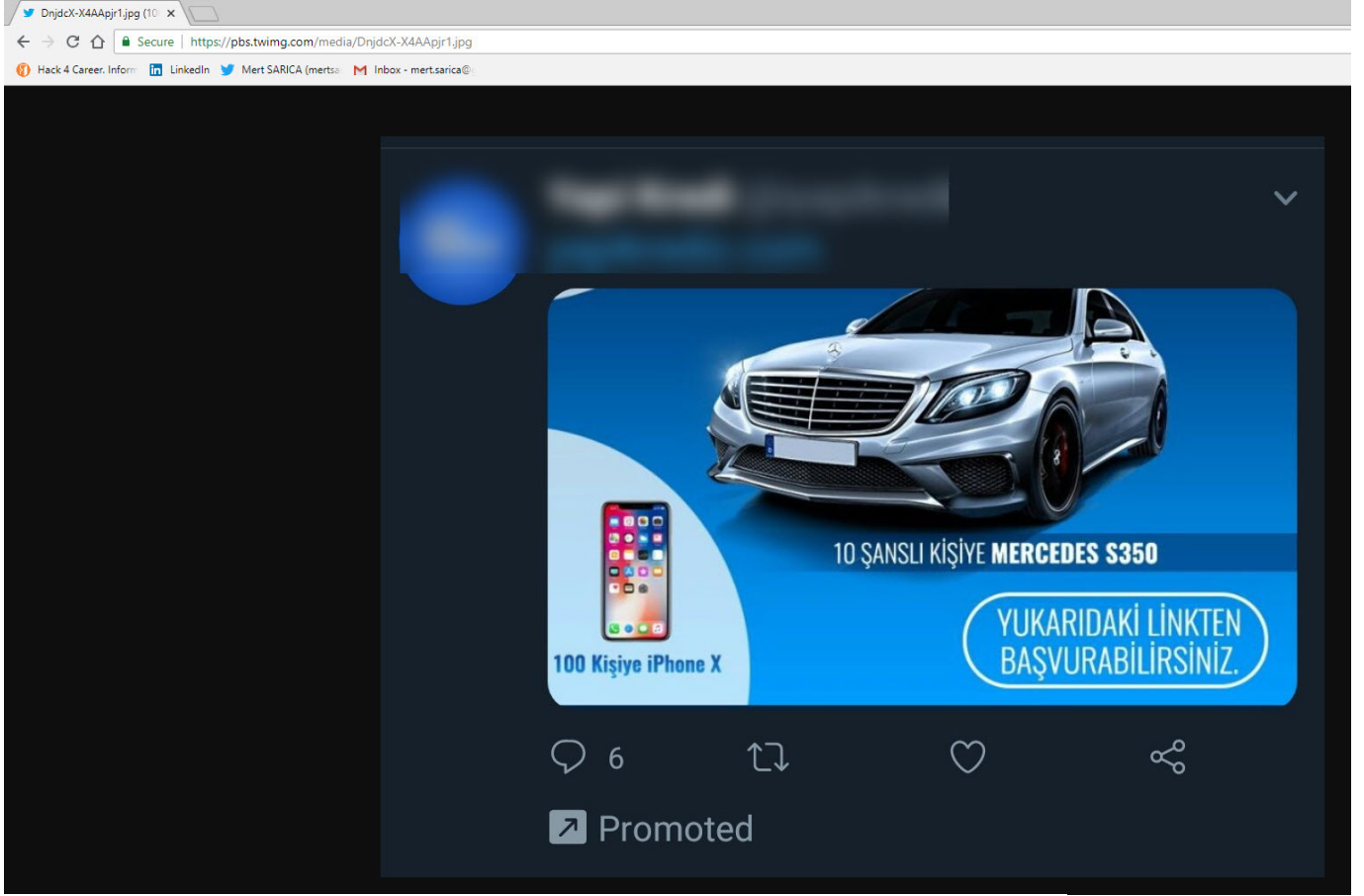
YUKARIDAKİ LİNKTE BAŞVURABİLİRSİNİZ.

6 1 20 Eyl 2018

Yanıtını Tweetle

@ilksonbahar adlı kullanıcıya yanıt olarak

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



Yazıma son noktayı koymadan önce dolandırıcılarla mücadele için ortalama 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

[blurred] adlı kişiyi takip et

[blurred] adlı kişiyi
sessize al

Bu sohbeti sessize al

[blurred] adlı kişiyi engelle

Tweeti bildir



Bir sonraki yazıda g r  mek dileęiyle herkese güvenli g nler dilerim.