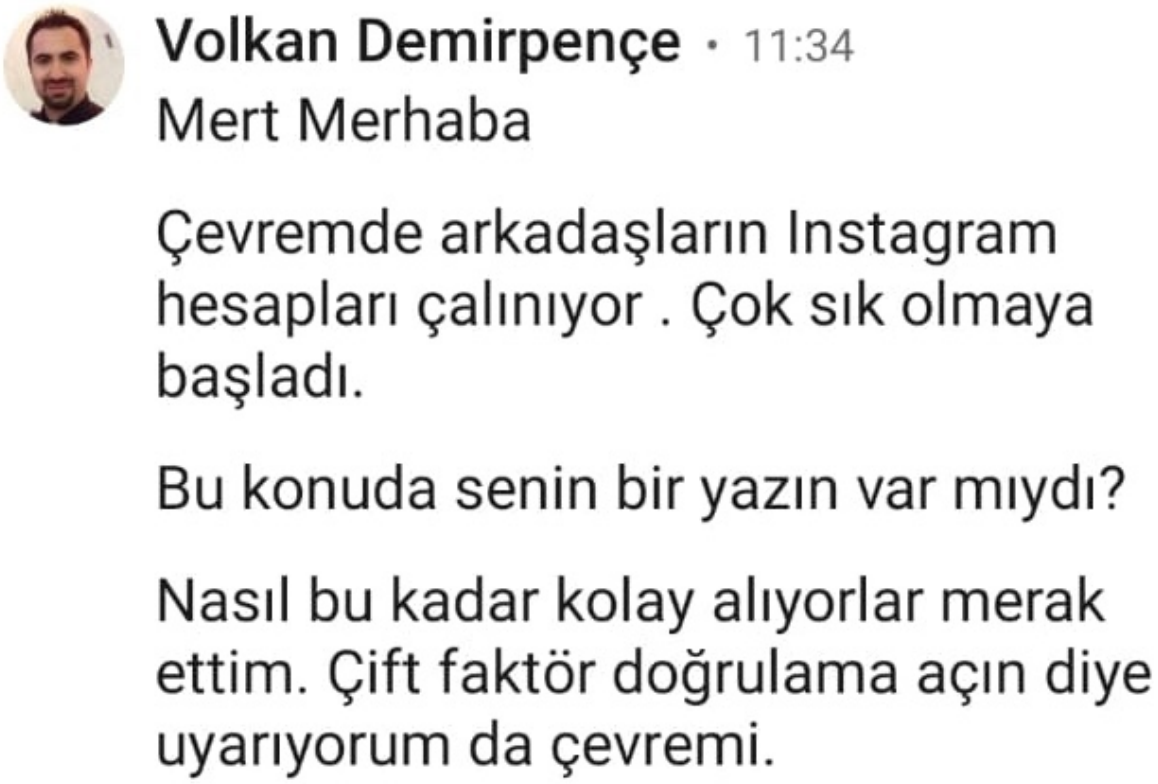
Instagram Scammers

written by Mert SARICA | 1 December 2021

Those of you who have read my previous blog posts titled “Sponsored Scamming” “LinkedIn Scammers” and “Who Viewed My Profile?” have learned that social media platforms are effectively used by scammers. However, what surprised me the most after writing these articles was that almost 2 years later, after almost 2 years, the “LinkedIn Scammers” blog post was still receiving comments about the ongoing activities of fraudsters.

After writing three articles on this topic, I had decided to leave myself to fate, but in September 2021, in the face of the following message I received from Volkan DEMİRPENÇE on LinkedIn, I decided not to be indifferent and asked my spouse and friends to share any suspicious messages they received on Instagram with me.



As time passed and I was able to examine the phishing messages that came my way and learn how they hacked Instagram accounts, I decided to write about this topic in order to raise awareness for friends like Volkan.

In one of the phishing messages, the scammer sent a message to an Instagram user via the Facebook account Messenger under the name Telif Hakları stating that a copyright infringement had been committed and requesting that the user visit the web address userhelpconfirm[.]site-tr[.]site, which has the shared IP address 116[.]202[.]53[.]12, to confirm their account and fill out a form.

Telif Hakları
Bugün aktif

Telif Hakları
Facebook

Profili Gör

Dün 22:24

İnstagram telif hak ihlali !

Güvenliğiniz bizim sorumluluğumuz.

Hesap incelendi ve telif ihlali gerçekleştirdiği anlaşıldı.

Hesabınızı doğrulamadığınız taktirde 24 saat içinde hesabınız tarafımızca askıya alınacaktır. Ortaklığımızı devam ettire bilmemiz için hesabın kullanıcısı olduğunuzu doğrulamamız gerekmektedir.

Hesabınız bu şartlar yerine getirildikten sonra , bir doğrulama kodu gönderilerek güvenli hale getirilecektir. Verilen formda gerekli bilgileri doldurarak ortaklığınızı devam ettirebilirsiniz. Doğrulama kodunuz, formu doldurduktan sonraki 24 saat içinde hesabınıza tarafımızca gönderilecektir.

Form: **https://userhelpconfirm .site-tr.site/**

Verified Badges | Help Center
Merhaba, Hesabınız telif haklarını ihlal ettiği gerekçesiyle 24 saat içinde Kapatılacaktır. Bunun Bir Hata Olduğunu Düşünüyorsanız İ...

Ara

Telif Hakları

Arkadaşı Ekle | Mesaj | ...

... Telif'in Hakkında Bilgilerini Gör

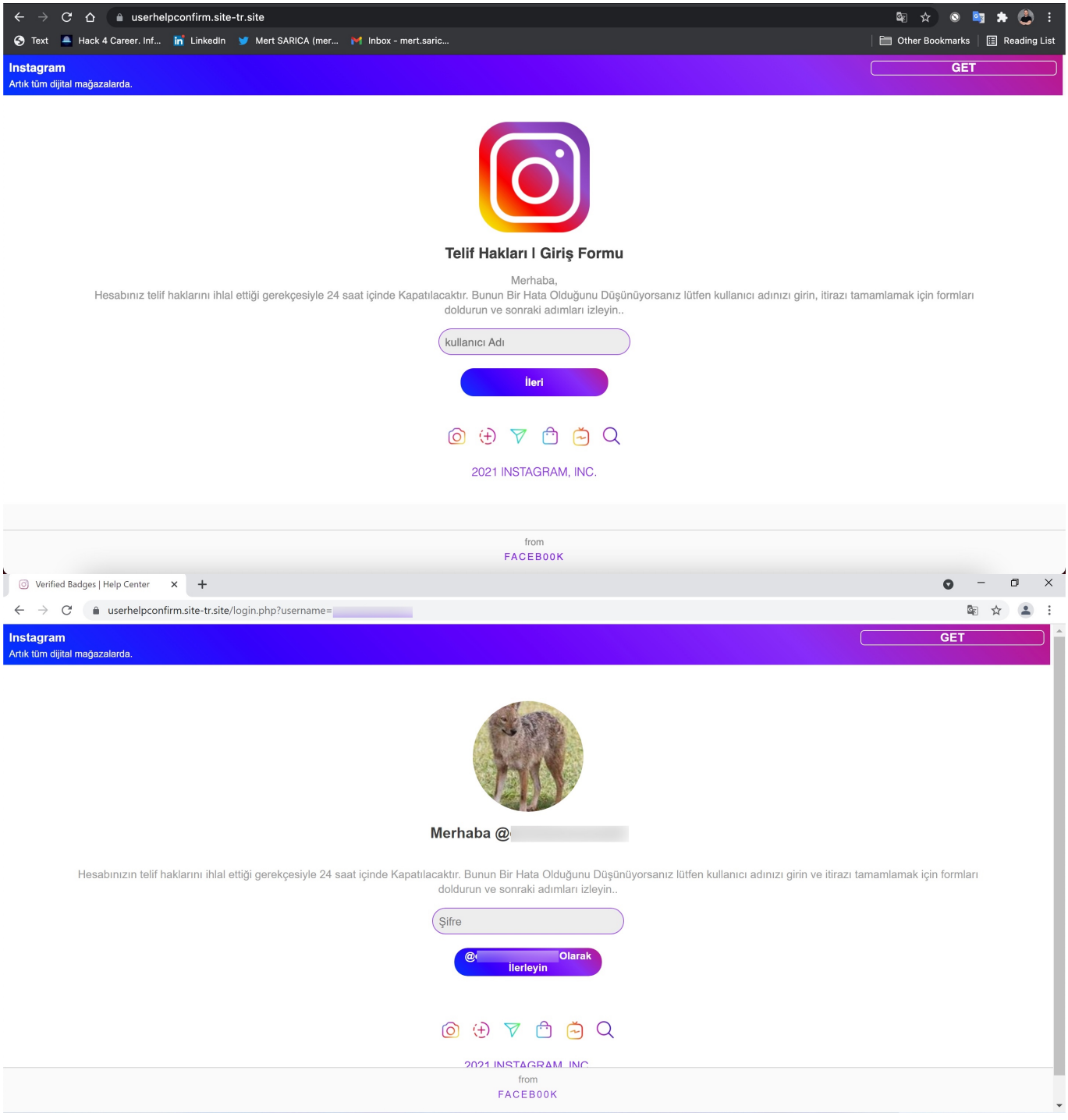
Arkadaşlar

Gönderiler

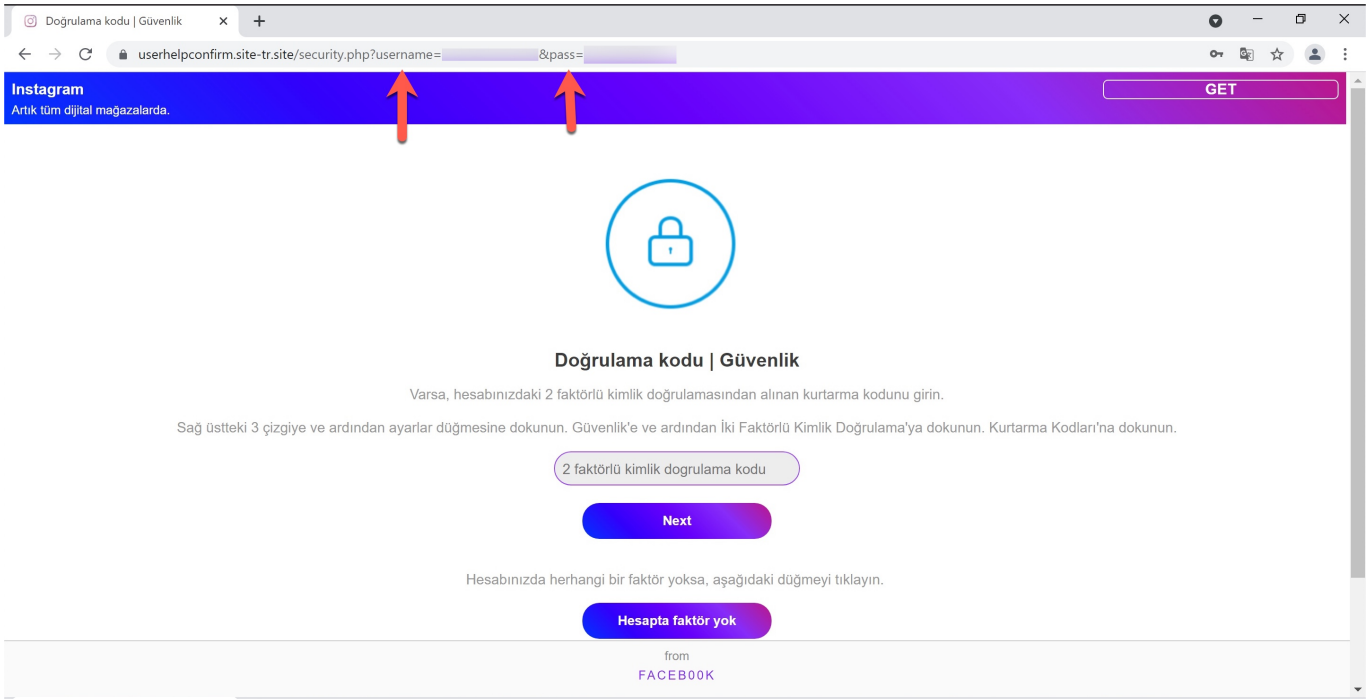
Fotoğraflar

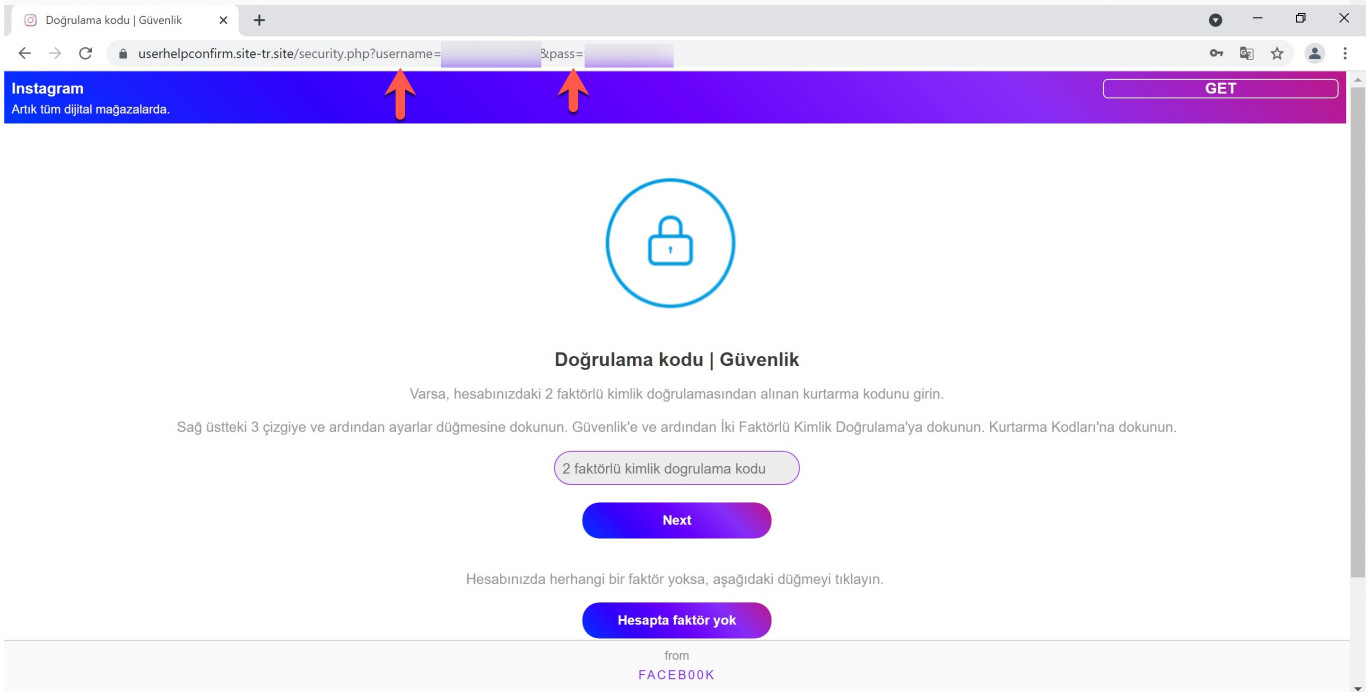
Telif Hakları profil resmini güncelledi.
31 Ağu, 23:08 •

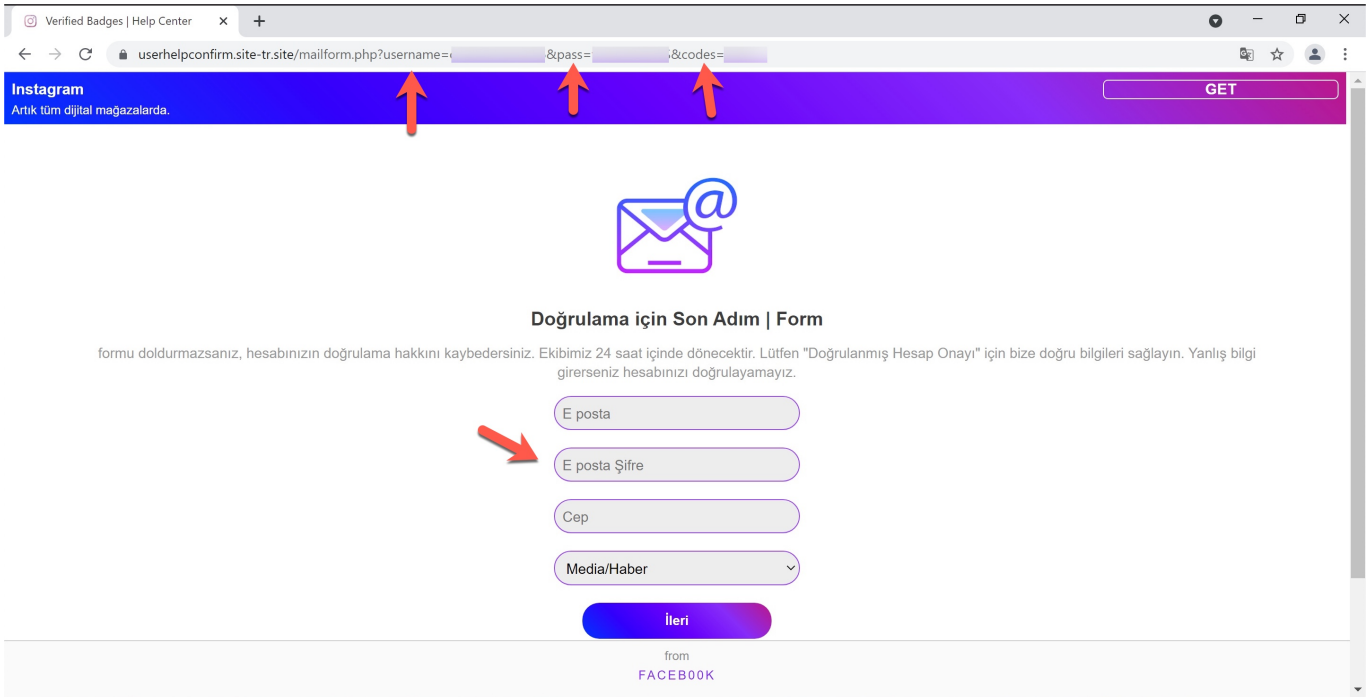
When the user’s Instagram username was entered on the website, in order to increase credibility, the user’s profile picture was also downloaded and displayed in the background through the dumpor.com website when the password was requested on the page.



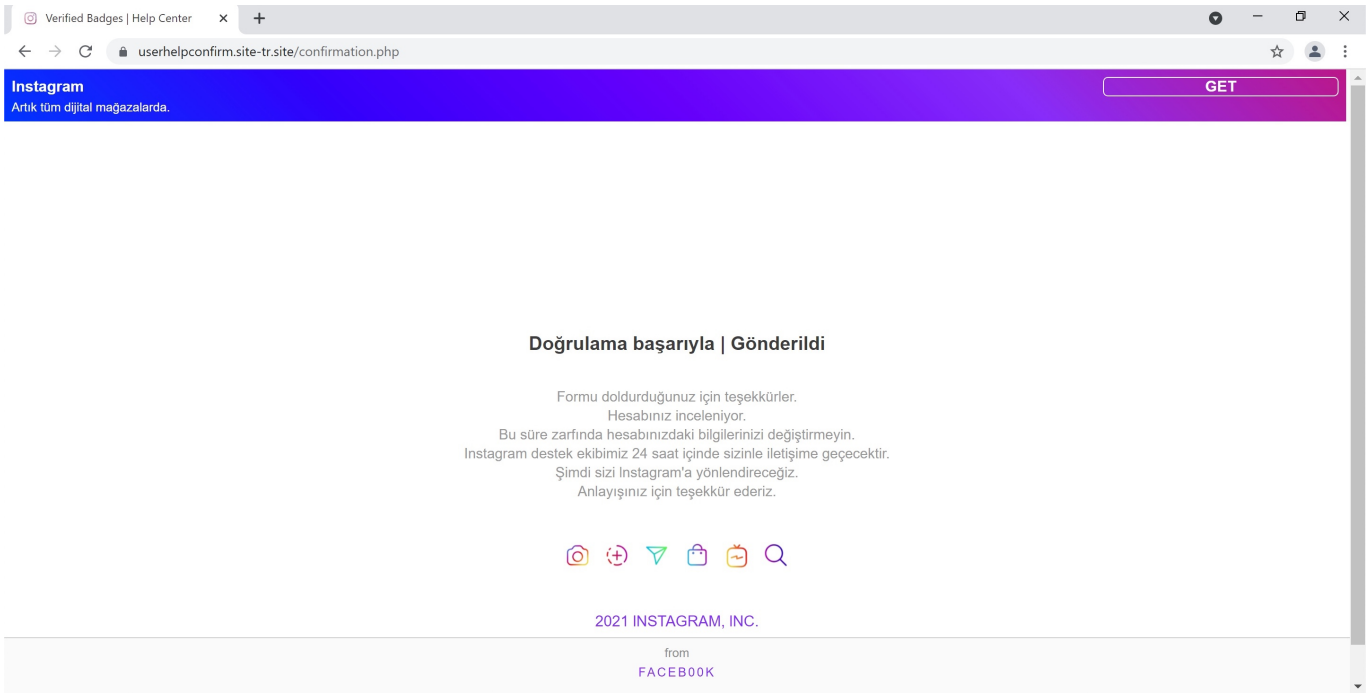
If the account is protected with two-factor authentication (which I strongly recommend using), after the correct password is entered on the phishing page, the user is asked to enter the verification code (SMS or login code) and, as if that were not enough, their email address and password as well.


Doğrulama kodu | Güvenlik
userhelpconfirm.site-tr.site/security.php?username=&pass=
Instagram
Artık tüm dijital mağazalarda.
GET
Doğrulama kodu | Güvenlik
Varsa, hesabınızdaki 2 faktörlü kimlik doğrulamasından alınan kurtarma kodunu girin.
Sağ üstteki 3 çizgiye ve ardından ayarlar düğmesine dokunun. Güvenlik'e ve ardından İki Faktörlü Kimlik Doğrulama'ya dokunun. Kurtarma Kodları'na dokunun.
2 faktörlü kimlik dogrulama kodu
Next
Hesabınızda herhangi bir faktör yoksa, aşağıdaki düğmeyi tıklayın.
Hesapta faktör yok
from
FACEB00K


Doğrulama kodu | Güvenlik
userhelpconfirm.site-tr.site/security.php?username=&pass=
Instagram
Artık tüm dijital mağazalarda.
GET
Doğrulama kodu | Güvenlik
Varsa, hesabınızdaki 2 faktörlü kimlik doğrulamasından alınan kurtarma kodunu girin.
Sağ üstteki 3 çizgiye ve ardından ayarlar düğmesine dokunun. Güvenlik'e ve ardından İki Faktörlü Kimlik Doğrulama'ya dokunun. Kurtarma Kodları'na dokunun.
2 faktörlü kimlik dogrulama kodu
Next
Hesabınızda herhangi bir faktör yoksa, aşağıdaki düğmeyi tıklayın.
Hesapta faktör yok
from
FACEB00K



Once all the information is entered, the scammers have obtained all the information they need to take over the Instagram account and achieve their nefarious goals. Although what they can do from there is limited only by their imagination, I created a fake Instagram account in order to understand their intentions and obtain the IP addresses of the system used by the scammers, and began waiting for them to hack my account by entering my information on this page, but I probably failed to attract their interest due to the low number of followers, and therefore was unable to allow them to access my account.



I can hear some of my readers saying, ‘Well, who would believe these phishing messages anyway?’ I asked myself the same question and continued to examine the phishing messages for a while.

In another phishing attack, I encountered a cold-blooded scammer who was very cautious in order not to be caught by the security controls of the phishing site, did not hesitate to use sweet talk to persuade, and did not shy away from using a sensitive topic such as “No to Violence Against Women” in their scenario to achieve their sinister goals.

On October 21, the scammer, who hid behind the gamzedemirel.avk account with a fake name, surname, and profile photo, and entered into communication with the target user pretending to be a lawyer, stated that they were in an endless struggle against violence against women and children and wanted to talk for 2 minutes.

gamzedemirel.avk

Gamze Demirel

gamzedemirel.avk · Instagram

4,5 B takipçi · 52 gönderi

Seni takip ediyor

Profili Gör

21 Eki 11:24

[redacted] merhaba iyi günler rahatsızlık vermiyorum umarım

21 Eki 16:17

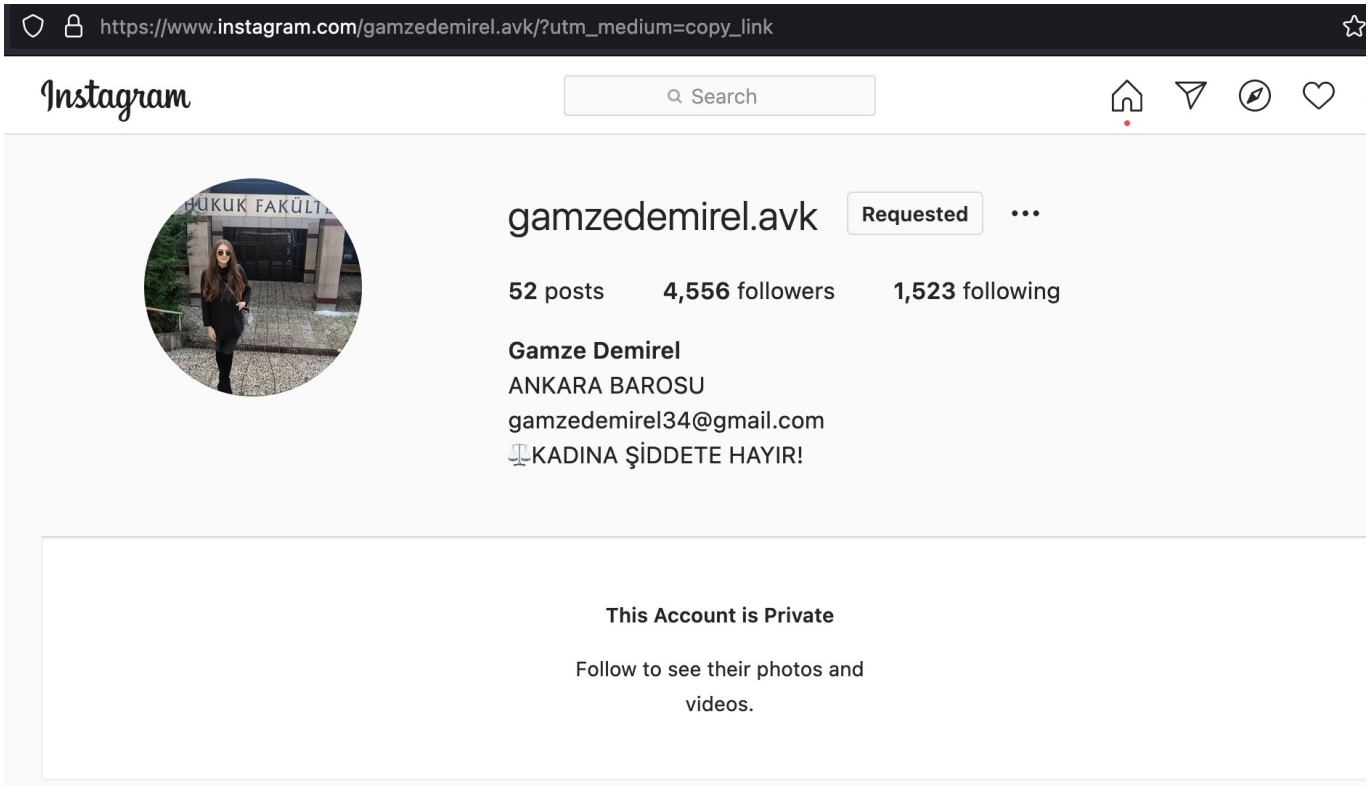
[redacted]

Türkiyede son dönemlerde kadınların ve çocukların hedef olduğu şiddet olaylarını haberlerde izliyorsunuzdur mutlaka, bu durumlara farkındalık yaratmak için devlet kadınlarımız ve çocuklarımızın yanında olmak adına bir destek platformu oluşturduk. Sizde katılıp destek verirseniz en azından manevi anlamda yanımızda durursanız bizi çok mutlu edersiniz. Kadınlara ve çocuklara uygulanan şiddetin her türlüsüne karşı bir avukat olarak sonsuz bir mücadele içindeyim adı geçen her failin en yüksek cezayı almasi için elimden gelen gayreti göstermekteyim. Sizden ricam sadece birkaç dakikanızı ayırmanız

[redacted]

Duyarlı olduğunuz için minnettarım size,duyarlı olmak,bilinçi olmak, hayvana, kadına şiddete her türlü şiddete dur demek ve bunu yapanlara en yüksek mertebeden cezalar vermek için mücadelemiz 2 dk vaktinizi ayıracağınız için çok teşekkür ederim 🙏🥰

21 Eki 18:25



After six days, when the scammer realized that they had not received a response from the target user, they contacted them again on October 26 and shared that they had not seen the name of the target user among the supporters and asked for support through the kadinlaradestek[.]com/home.php website hidden behind Cloudflare.

gamzedemirel.avk

teşekkür ederim 🙏🥰

21 Eki 18:25

🙏

Bugün 11:19

https://www.kadinlaradestek.com/home.php

Kadın Şiddetine Hayır

Kadına şiddet insanlık suçudur! Kadına yönelik her türlü şiddetin karşısında, şiddet mağduru kadınlarımızın da her zaman yanı...

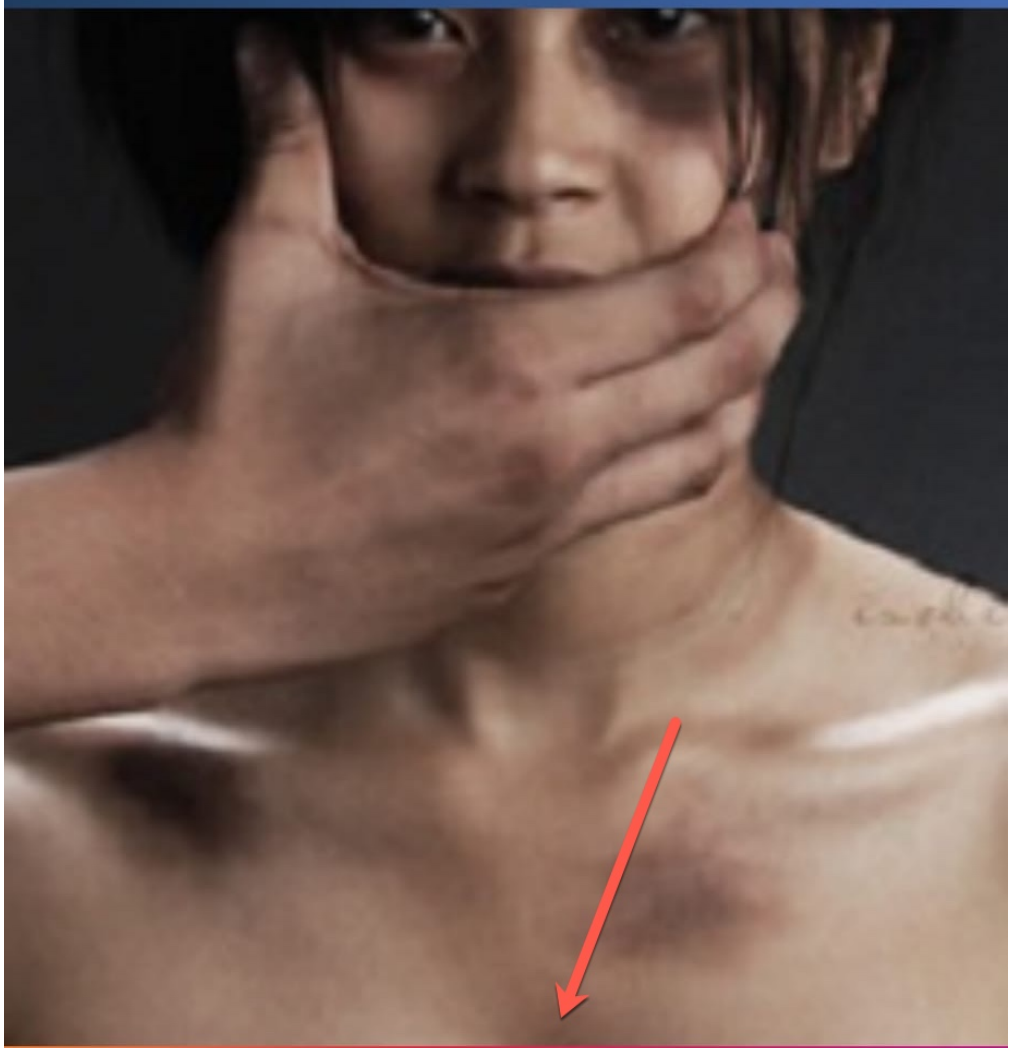
Merhaba iyi günler efendim listede adınızı göremedim destek olmamışsınız da, umarım bu duruma duyarsız kalmayıp desteğinizi gerçekleştirirsiniz. Kampanyamızın süresinin dolmasına çok az bir süre kaldı😊🙏

kadinlaradestek.com/ho

30

KADINA ŞİDDETE DUR!

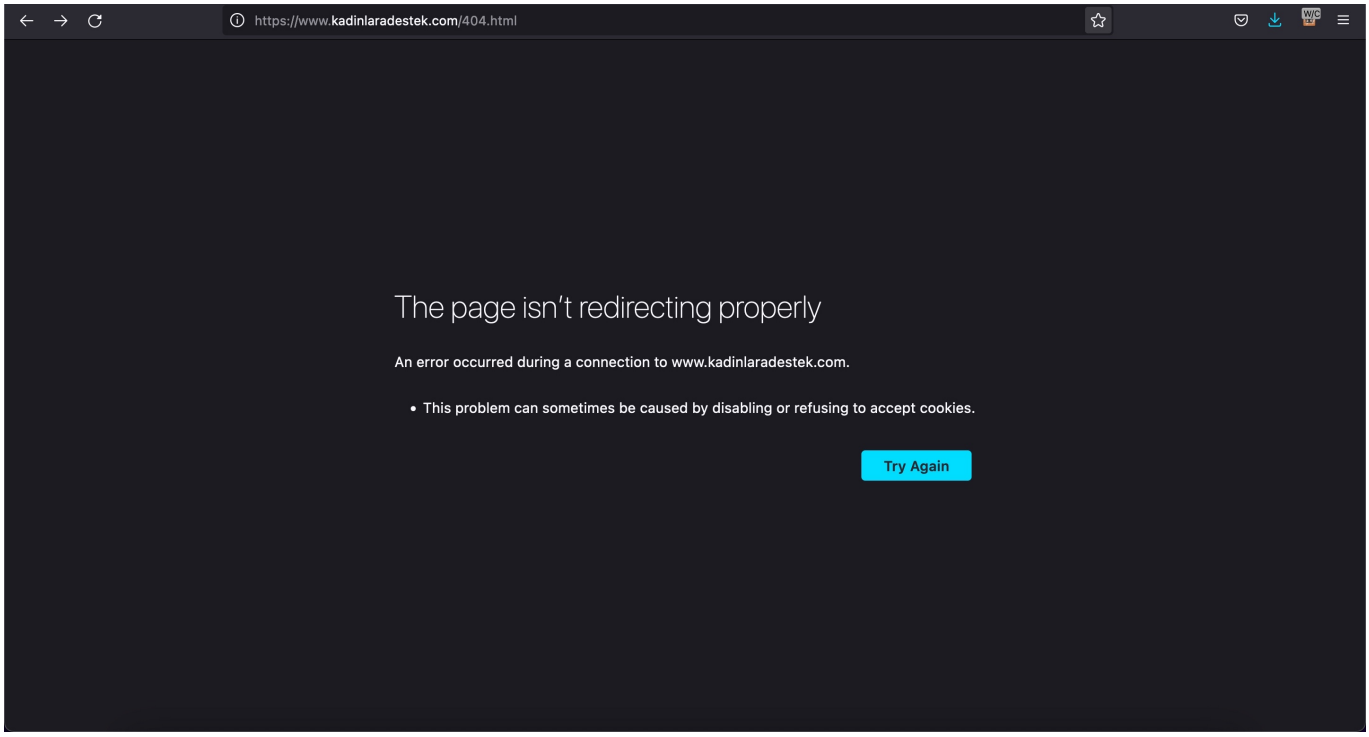
Kadına şiddet insanlık suçudur! Kadına yönelik her türlü şiddetin karşısında, şiddet mağduru kadınlarımızın da her zaman yanındayız. Destek olarak bizlere katıl!

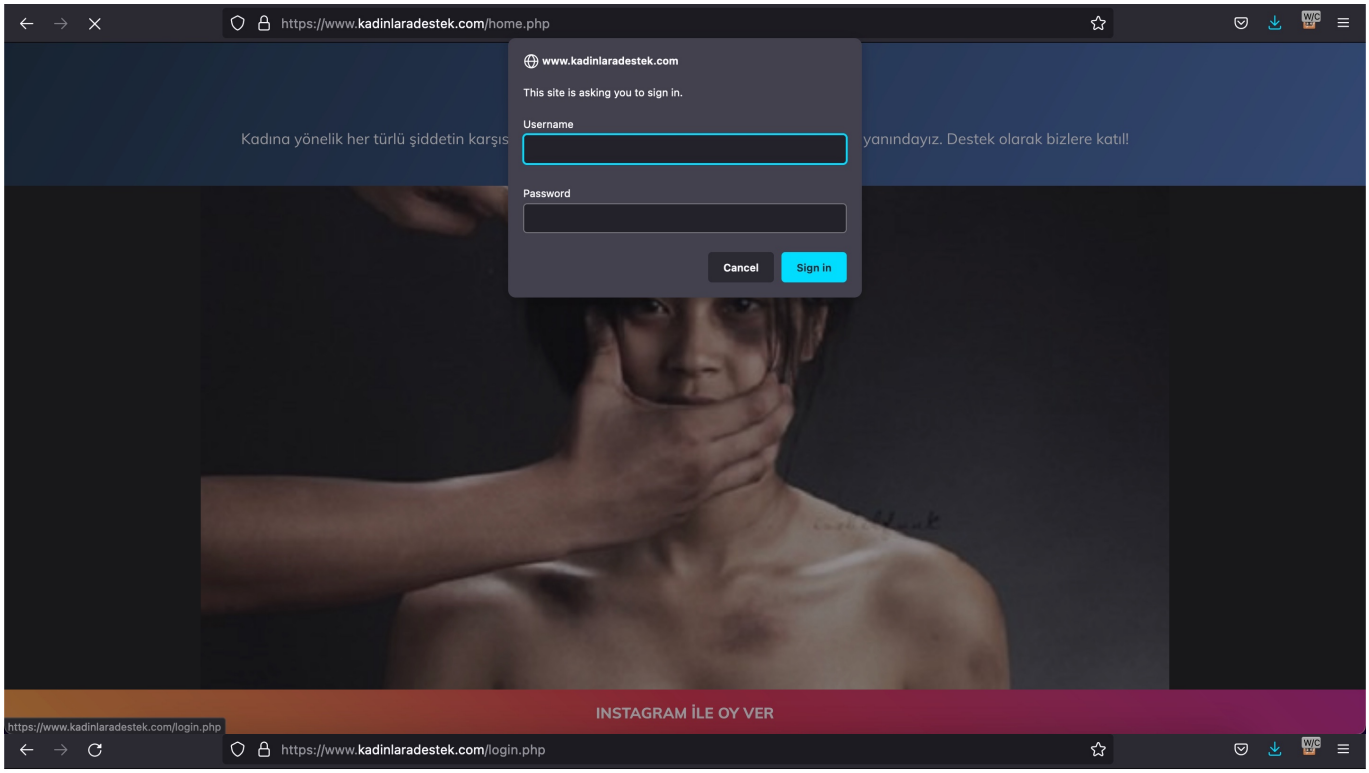


INSTAGRAM İLE OY VER

When I visited the website, I noticed that the scammer had taken various technical measures in order to continue their operation for a long time. When I tried to go directly to https://kadinlaradestek[.]com, the website entered a 404 (page not found) error loop and would not open. To access the site, it was necessary to visit the direct address https://kadinlaradestek[.]com/home.php.

Another point that caught my attention was that when you went to the site through an Instagram private message and pressed the INSTAGRAM İLE OY VER button at the bottom of the page, you were confronted with a form that steals your information through https://kadinlaradestek[.]com/login.php, but if you try to go directly to https://kadinlaradestek[.]com/login.php through your internet browser, you encounter a box that asks for a username and password instead of a form, and if you press the CANCEL button, you encounter a fake error page. In short, it was clear that the scammer took various measures to prevent these types of phishing sites from being detected by scanning tools of cybersecurity companies.





{ "error": { "message": "You did not provide an API key. You need to provide your API key in the Authorization header, using Bearer auth (e.g. "Authorization: Bearer YOUR_SECRET_KEY"). See https://stripe.com /docs/api#authentication for details, or we can help at https://support.stripe.com/.", "type": "invalid_request_error" } }

Like a lion focused on its prey, the scammer closely monitored whether they were able to steal the information of the target user, and contacted them again on October 28 and November 1.

Per 11:07

Merhabalar, zamanınız olmadı galiba

Per 12:18

Tamam efendim

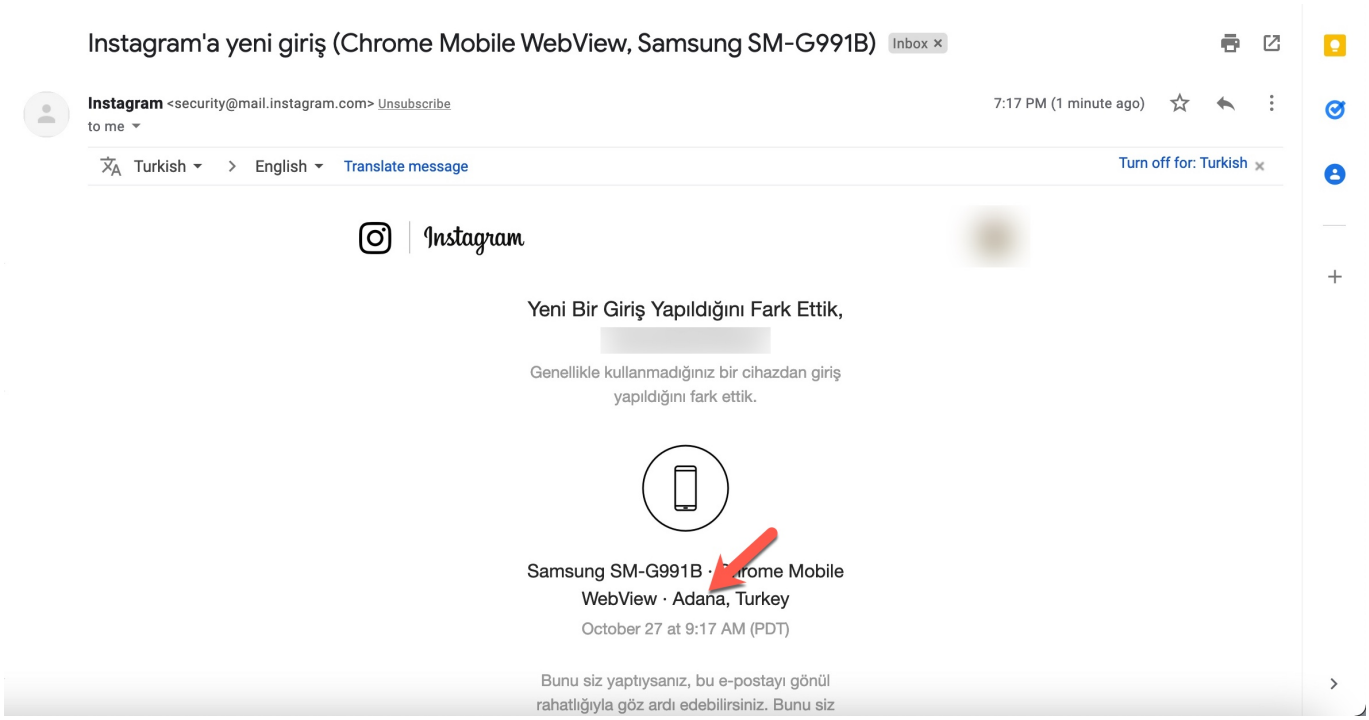
Bugün 15:09

Sizi rahatsız ediyorum sürekli kusura bakmayın

Müsaitliğiniz sağlanmadı galiba

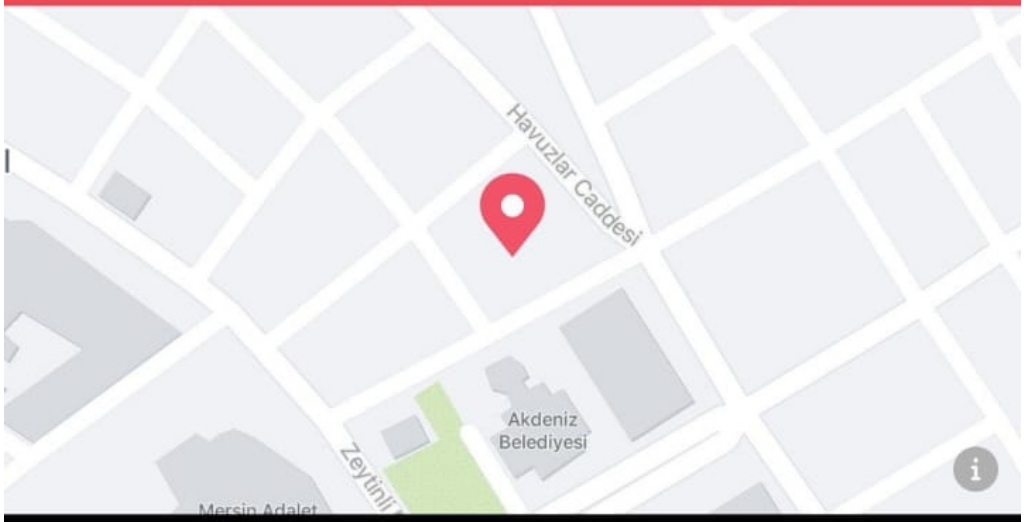
Mesaj...

As before, I began entering the information of the fake Instagram account I created in order to understand the intentions of the scammer and obtain the IP address, into the form on this page, and waiting for them to hack my account at certain intervals. As soon as I entered my information, I received warning messages from Instagram stating that my account had been accessed from Adana and Mersin and that two-factor authentication had been turned off. The fact that the transactions were carried out so quickly by the scammers indicated that the stolen information was being automatically processed with the help of a script in the background.



Instagram

Şüpheli Giriş Denemesi



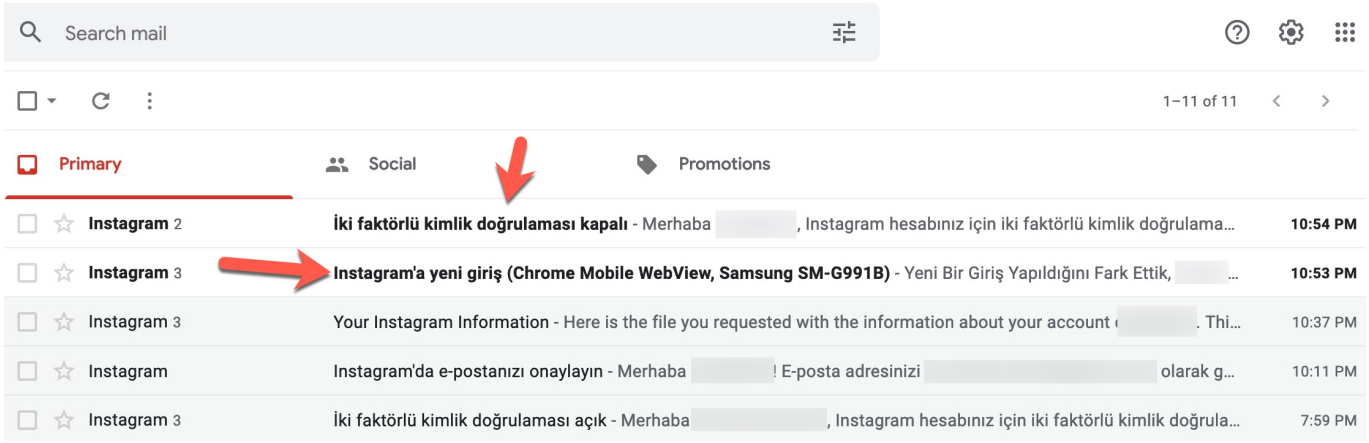
Olağandışı Bir Giriş Denemesi Saptadık

Android | 27.10.2021 22:01
Mersin

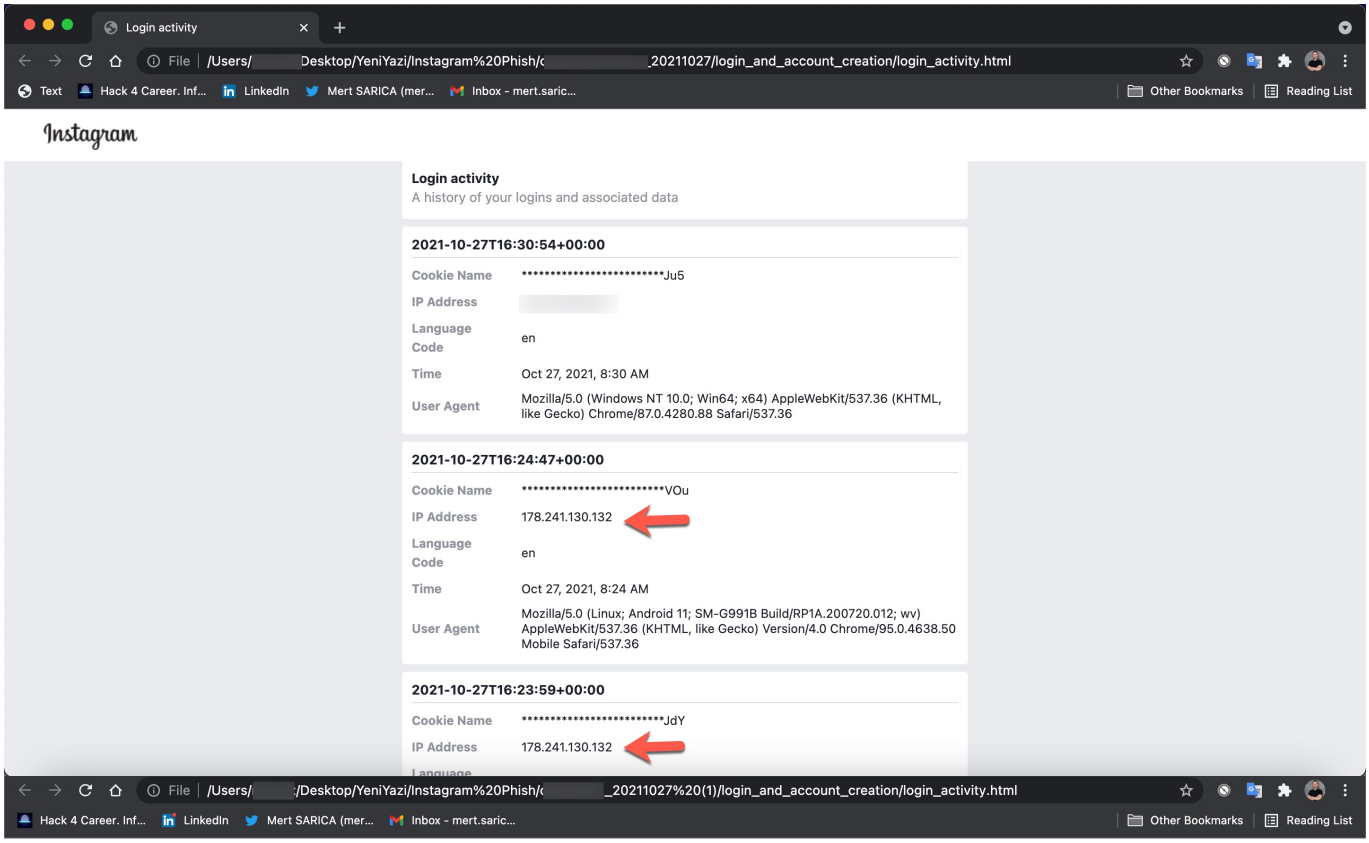
Hesabını güvene almak için bunu yapanın sen olduğunu bize bildir.

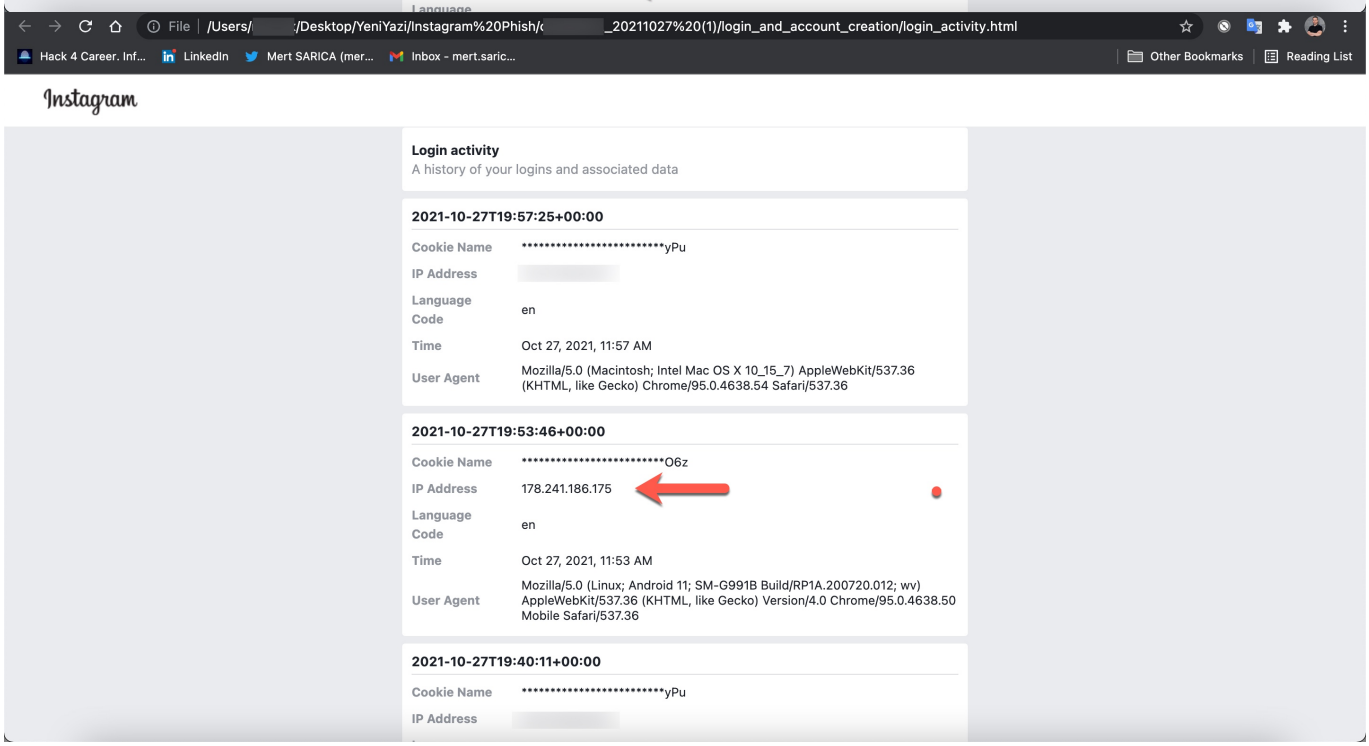
Bunu Ben Yapmadım

Bunu Ben Yaptım



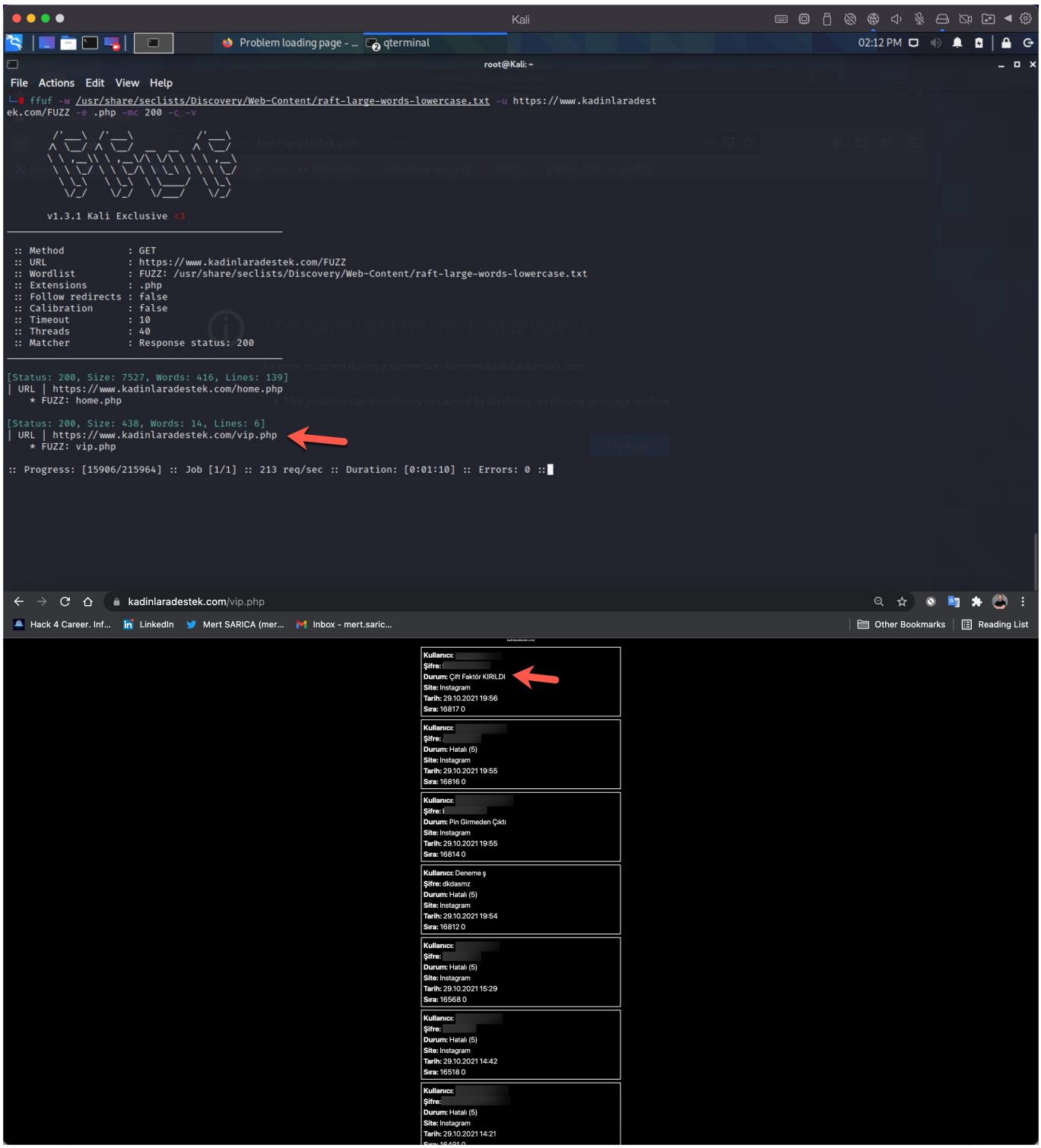
When it came time to find the IP addresses of the scammers who logged in, I first had to request information related to my Instagram account through the Settings -> Security -> Download Data steps in the Instagram mobile app. After receiving an email from Instagram stating that the information was ready, I downloaded the relevant ZIP file. After opening the ZIP file, I looked at the login_activity.html file in the login_and_account_creation folder and saw that the scammers had accessed my account from a different dynamic IP address belonging to Turkcell each time. When I examined the IP addresses, I saw that the 178.241.130.132 IP address belonged to the Diyarbakir IP pool and the 178.241.186.175 IP address belonged to the Kayseri IP pool. The fact that the IP addresses were dynamic and changed each time suggested the possibility that these operations were being carried out with the help of a script on a rooted phone or mobile device in the background. The fact that the scammers did not change the password after logging into the Instagram account indicated that they wanted to use it to access hacked accounts for a long period of time and achieve their goals.





Lastly, when it came to identifying the innocent users who had fallen victim to these scammers, I began using ffuf, a tool well-known to offensive security experts, to discover PHP files on the website. It didn't take long for ffuf to identify a file called vip.php on the website. When I visited the address https://kadinlaradestek[.]com/vip.php where the file was located, I was able to access a list of accounts that had been hacked by scammers since October 26th. Upon reviewing the list, it became clear that between October 26th and November 25th, the scammers had successfully targeted over 70 Instagram users specifically for their networks. Upon reviewing the number of

followers of the targeted Instagram accounts, it was also revealed that approximately 200,000 Instagram users were at risk of being subjected to an attack or scam through these hacked accounts.



```
================================================================
Show Hacked Instragram Accounts v1.0 [https://www.mertsarica.com]
================================================================
Unfortunately 73 Instagram accounts have been hacked!

Date: 25.11.2021 12:38 Username:
Date: 23.11.2021 20:10 Username:
Date: 22.11.2021 13:32 Username:
Date: 22.11.2021 11:37 Username:
Date: 19.11.2021 21:44 Username:
Date: 19.11.2021 20:35 Username:
Date: 19.11.2021 15:54 Username:
Date: 18.11.2021 18:36 Username:
Date: 17.11.2021 18:30 Username:
Date: 16.11.2021 20:57 Username:
Date: 16.11.2021 19:58 Username:
Date: 16.11.2021 19:48 Username:
Date: 16.11.2021 16:44 Username:
Date: 16.11.2021 14:35 Username:
Date: 16.11.2021 13:28 Username:
Date: 15.11.2021 12:46 Username:
Date: 13.11.2021 15:02 Username:
Date: 13.11.2021 13:23 Username:
Date: 13.11.2021 12:01 Username:
Date: 12.11.2021 15:15 Username:
Date: 11.11.2021 12:28 Username:
Date: 11.11.2021 12:04 Username:
Date: 10.11.2021 20:07 Username:
Date: 10.11.2021 19:50 Username:
Date: 10.11.2021 11:40 Username:
Date: 10.11.2021 11:21 Username:
Date: 09.11.2021 22:32 Username:
Date: 09.11.2021 19:00 Username:
Date: 09.11.2021 17:39 Username:
Date: 09.11.2021 17:18 Username:
Date: 08.11.2021 21:11 Username:
Date: 08.11.2021 20:30 Username:
Date: 08.11.2021 19:35 Username:
Date: 08.11.2021 19:09 Username:
Date: 08.11.2021 16:48 Username:
Date: 08.11.2021 13:16 Username:
Date: 08.11.2021 12:50 Username:
Date: 08.11.2021 10:32 Username:
Date: 07.11.2021 21:22 Username:
Date: 07.11.2021 18:39 Username:
Date: 07.11.2021 09:16 Username:
Date: 06.11.2021 18:07 Username:
Date: 06.11.2021 13:14 Username:
Date: 06.11.2021 12:47 Username:
Date: 06.11.2021 11:17 Username:
Date: 06.11.2021 07:29 Username:
```

In conclusion, as I have also emphasized in my previous articles, I recommend that all readers do not click on links from unknown sources (emails, SMS, private messages, etc.), do not enter passwords, two-factor authentication

codes, or other sensitive information on websites or forms that they do not know, use two-factor authentication on all accounts whenever possible, follow the guidelines on this page to ensure the security of their Instagram accounts, visit Instagram's support page to recover hacked accounts, and finally, share this article with friends and acquaintances who use social media to raise awareness.

On the occasion of this being my final article of the year, I would like to wholeheartedly wish all my readers a happy new year, and I hope that 2022 brings health, happiness, and abundance to everyone.