

Who Viewed My Profile?

written by Mert SARICA | 1 October 2020

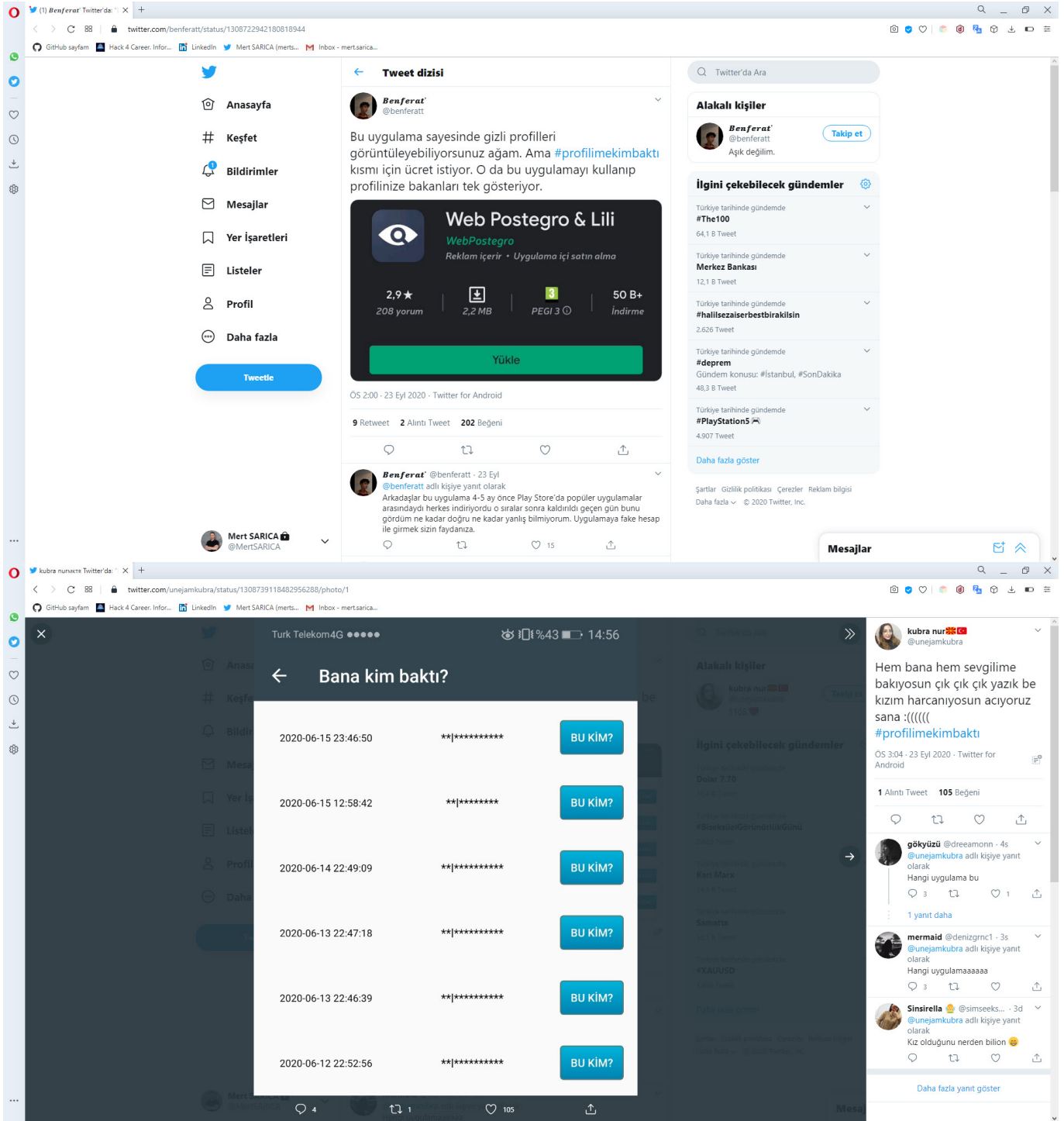
On September 23, 2020, while browsing cybersecurity-related news on Twitter, I noticed the hashtag #profilimekimbaktı in the trending topics. I decided to check the accounts sharing this hashtag as it raised suspicion. One of the accounts had written in their message that the Android app Web Postegro & Lili showed who viewed their profile.

Q Twitter'da Ara

İlgini çekebilecek gündemler

- Türkiye tarihinde gündemde 
#çöktü
Gündem konusu: Ali Babadan, Dolar 7.68
9.839 Tweet
- Türkiye tarihinde gündemde 
#BiseksüelGörünürlükGünü
Gündem konusu: #BiVisibilityDay
- Türkiye tarihinde gündemde 
#XAUUSD
1.524 Tweet
- Türkiye tarihinde gündemde 
#KemalizmiYikacaz
17,2 B Tweet
- Türkiye tarihinde gündemde 
#profilimekimbaktı 
2.264 Tweet

[Daha fazla göster](#)



Except for LinkedIn, I have always approached social networks like Twitter, Facebook, and Instagram with skepticism because I know that they do not share the information of profile viewers. I downloaded and analyzed this Android application and wrote about it to understand if my suspicions were justified. I started by reviewing the page of the Android application Web Postegro & Lili on Google Play. As of September 24, I did not see any permissions that raised any suspicions when I looked at the permissions used by this mobile application, which has been downloaded over 100,000 times. However, when I looked at the comments, I saw some suspicious comments from users claiming

that there were unauthenticated logons to their accounts from unknown sources. Although the developer replied to one of the comments stating that it is stated in their security policy that connections may be made from abroad, I could not find such kind of statement in their policy.

Web Postegro & Lili - Google Play

play.google.com/store/apps/details

GitHub sayfam Hack 4 Career. Infor... LinkedIn Mert SARICA (merts... Inbox - mert.sarica...

Google Play Ara

Kategoriler Ana Sayfa Üst sıralar Yeni yayınlar

Uygulamalarım Mağaza

Oyunlar Aile Editörün Seçimi

Hesap Ödeme yöntemleri Aboneliklerim Kullan Hediye kartı satın al İstek listem Oyun etkinliğim Ebeveyn Rehberi

Web Postegro & Lili

WebPostegro Sosyal 248

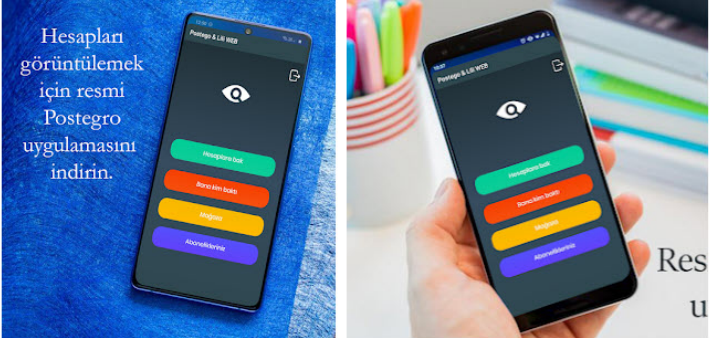
PEGI 3

Reklam içeriyor

Bu uygulama tüm cihazlarınızla uyumlu.

İstek Listesi'ne ekle

Yükle



Hesapları görüntülemek için resmi Postegro uygulamasını indirin.

Açıklama, Google Çeviri kullanılarak Türkçe (Türkiye) diline çevrilsin mi? Çevir

Web Postegro & Lili ile tüm hesapları arayın ve görüntüleyin. Hesapları görüntülemek için resmi uygulamayı indirin.

Uygulamalar

Kategoriler Ana Sayfa Üst sıralar Yeni yayınlar

Uygulamalarım

Mağaza

Oyunlar

Aile

Editörün Seçimi

Hesap

Ödeme yöntemleri

Aboneliklerim

Kullan

Hediye kartı satın al

İstek listem

Oyun etkinliğim

Ebeveyn Rehberi

Web Postegro & Lili ile tüm hesapları arayın ve görüntüleyin. Hesapları görüntülemek için resmi uygulamayı indirin.

Web Postegro & Lili kolayca video ve fotoğraf kaydetmenize yardımcı olur. Yalnızca tek tıklamayla doğrudan cihazınıza hikâye kaydedebilirsiniz. Kaydedilen video ve fotoğrafları, kendi hesabınızda yeniden paylaşın.

Müthiş Özellikler

- ✓ Hikâyelerini ve gönderilerini görüntüleyin
- ✓ Videoları ve fotoğrafları yeniden paylaşın
- ✓ %100 güvenli.
- ✓ Birden çok hesabı destekler
- ✓ Kullanıcıları aratın ve hikâyelere göz atın
- ✓ Sık kullandığınız hesapları yer imlerine ekleyin
- ✓ Arayüzü sade ve kullanımı kolay
- ✓ Yerleşik oynatıcıyla videoları izleyin
- ✓ Hafif hikâye kaydedici
- ✓ En iyi kaydedici ve video indirici

Web Postegro & Lili uygulaması yardımcı oluyorsa, lütfen uygulamaya puan verin **★★★★★**
Yeni özellikler için bildirim ve önerilere ihtiyacınız varsa, lütfen webpostegro@gmail.com adresine e-posta gönderin

Web Postegro & Lili Sorumluluk Reddi

- * Video veya fotoğrafları yeniden paylaşmadan önce sahibinden lütfen İZİN alın;
- * Video veya fotoğrafların izinsiz yeniden paylaşımlarından doğan hiçbir fikri mülkiyet ihlalden biz sorumlu değiliz;
- * Bu uygulama, hiçbir sosyal medya platformu ile ilişkili değildir.

DARALT

YORUMLARI AR

Yorum Politikası

Web Postegro & Lili - Google Play Store

play.google.com/store/apps/details

Uygulamalar Kategoriler Ana Sayfa Üst sıralar Yeni yayınlar

Uygulamalarım Mağaza

Oyunlar Aile Editörün Seçimi

Hesap Ödeme yöntemleri Aboneliklerim Kullan Hediye kartı satın al İstek listem Oyun etkinliğim Ebeveyn Rehberi

Türkiyedeyiz ve şifreyi girdiğiniz anda hesabınıza yabancı ülkeden giriş yapıyor. İndirmeyin bence

WebPostegro 22 Eylül 2020

Merhaba. Hesabınıza yabancı ülkeden giriş yapılmasının nedeni bizim uygulamada vpn hizmetinin çalışmasıdır ve bunlar uygulamanın düzgün çalışabilmesi içindir. Bizim için en önemli şey kullanıcılarımızın güvenliği ve rahatlığıdır bunun için de, elimizden geleni yapıyoruz.

TÜM İNCELEMELERİ OKU

EK BİLGİ		
Güncellendi	Boyut	Yükleme sayısı
8 Eylül 2020	2,5M	50.000+
Mevcut Sürüm	Gereken Android sürümü	İçerik Derecelendirmesi
1.0	5.0 ve sonrası	PEGİ 3 Daha Fazla Bilgi
Etkileşimli Öğeler	İzinler	Rapor
Sınırsız İnternet	Ayrıntıları göster	Uygunsuz olarak işaretle
Sunan:	Geliştirici	
WebPostegro	webpostegro@gmail.com Gizlilik Politikası	

©2020 Google | Site Hizmet Şartları Gizlilik Geliştiriciler Google Hakkında | Konum: Türkiye Dil: Türkçe Tüm fiyatlara KDV dahildir. Bu öğeyi satın alarak Google Payments ile işlem yapıyorsunuz ve Google Payments Hizmet Şartları ile Gizlilik Uyarısı'nı kabul etmiş oluyorsunuz.

Web Postegro & Lili - Google Play Store

play.google.com/store/apps/details

Uygulamalar Kategoriler Ana Sayfa Üst sıralar Yeni yayınlar

Uygulamalarım Mağaza

Oyunlar Aile Editörün Seçimi

Hesap Ödeme yöntemleri Aboneliklerim Kullan Hediye kartı satın al İstek listem Oyun etkinliğim Ebeveyn Rehberi

Merhaba. Gonderilerde beğenileri gösterme sorunu bir kaç gün içinde hall edilecektir. Şu an için uygulamaya girşte hiç bir sıkıntı yoktur. Eğer herhangi sorun yaşıyorsanız lütfen destek ekibimize iletişime geçin.

Enes Kuzu ★★★★★ 14 Eylül 2020
Adminler selamun aleykum öncelikle sizden ricamız lütfen bize bakanlar ücretsiz yapılırsanız çok makbule geçer yorumu okuduğunuz ve değerlendirdiğiniz için teşekkürler iyi günler.

WebPostegro 22 Eylül 2020
Merhaba. Eğer uygulama ortalaması 4.4 ve üzeri olursa herkese bana kim baktı paketini hediye edeceğiz. Yorumunuz için teşekkürler.

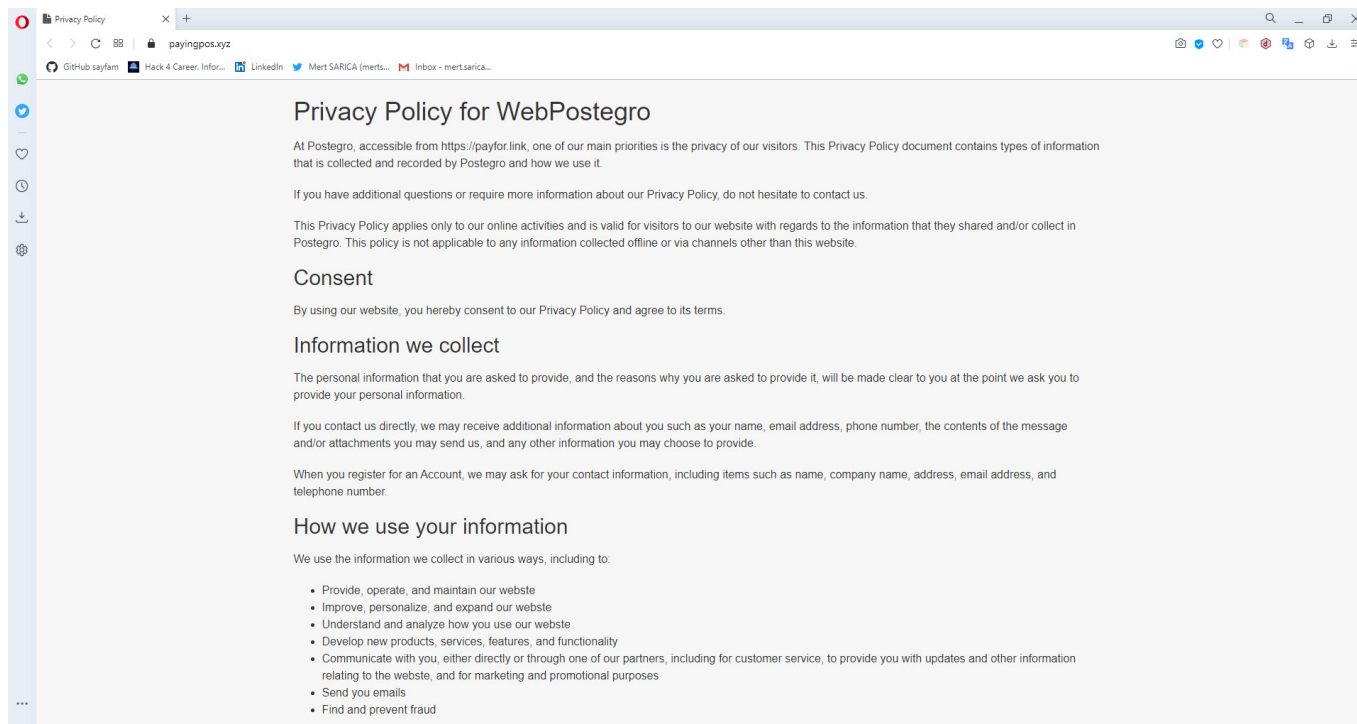
Musa Yakıcı ★★★★★ 19 Eylül 2020
Uygulama hiç güvenilir değil. Hesabıma bir anda Londra dan giriş yaptı. Kesinlikle indirmeyin. Anında şifreyi değiştirmek zorunda kaldım.

WebPostegro 22 Eylül 2020
Merhaba. Uygulama tam güvenlidir buna emin ola bilirsiniz. Bizim için en önemli şey kullanıcılarımızın güvenliği ve bunun için elimizden geleni yapıyoruz. Daha fazla ayrıntı için lütfen Kullanıcı Şartlarımızı ve Güvenlik Politikamızı inceleyiniz.

Elif Gürcan ★★★★★ 20 Eylül 2020
Yüklediğiniz ve şifreyi girdiğiniz anda hesabınıza yabancı ülkeden giriş yapıyor. İndirmeyin bence

WebPostegro 22 Eylül 2020
Merhaba Hesabınıza yabancı ülkeden giriş yapılmasının nedeni bizim uygulamada vpn hizmetinin çalışmasıdır ve bunlar uygulamanın düzgün çalışabilmesi içindir. Bizim için en önemli şey kullanıcılarımızın güvenliği ve rahatlığıdır bunun için de, elimizden geleni yapıyoruz.

TÜM İNCELEMELERİ OKU



After collecting the preliminary information from the Google Play page, I downloaded the Web Postegro & Lili application from the APKPure website to analyze it. When I uploaded the APK file to VirusTotal, I found no evidence that this application was malicious.

Then, I installed this application on the GenyMotion emulator and began recording the HTTP traffic generated during usage, using Charles Proxy, one of my favorite tools. In the first response from the payingpos[.]xyz web server that the application communicated with, I saw an Instagram account belonging to the application's developer, postegro.llc. One of the photos shared on the account caught my attention, as it mentioned that the application had been removed from Google Play previously. When I visited the website registered on September 5, which was listed on the Instagram account, I learned that I could directly download the Web Postegro & Lili application (39.apk) from the website.



Home » Apps » Social » Web Postegro & Lili

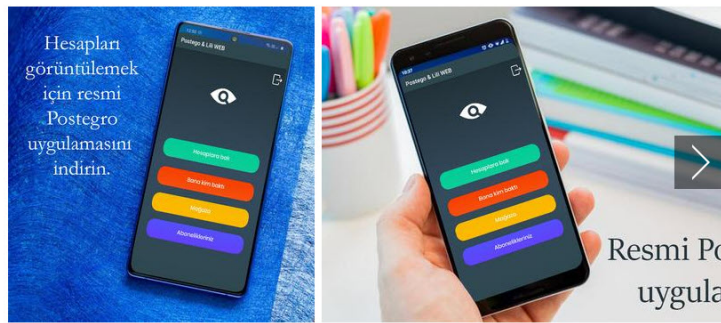


Web Postegro & Lili

1.0 for Android
★★★★★ | 0 Reviews | 0 Posts
WebPostegro

Download APK (2.5 MB) Versions

Using APKPure App to upgrade Web Postegro & Lili, fast, free and save your internet data.



Discover More »

- Netflix**
7.74.1 build 26 35115
Netflix, Inc.
- Microsoft Edge**
45.08.4.5072
Microsoft Corporation
- SoundCloud**
2020.09.22-release
SoundCloud
- Google Chrome: Fast & Secure**
85.0.4183.120
Google LLC
- Girls' Frontline**
2.0600_351
Darkwinter Software Co., Ltd.
- HERE WeGo**
2.0.14622
HERE Apps LLC
- Standoff 2**
0.13.6
Axlebolt

Charles 4.5.4 - Session 1 *

Structure Sequence

- https://www.googleapis.com
- https://infinitedata-pa.googleapis.com:443
- https://payingpos.xyz
 - api
 - versions
 - 1.php?processName=getInformations
- https://fonts.gstatic.com
- http://connectivitycheck.gstatic.com
- https://www.google.com
- https://android.clients.google.com
- https://android.googleapis.com
- https://people-pa.googleapis.com
- https://reminders-pa.googleapis.com:443
- https://play.googleapis.com
- https://graph.facebook.com
- https://phonedeviceverification-pa.googleapis.com:443
- https://r3---sn-u0g3uxax3-pnud.gvt1.com
- https://playatoms-pa.googleapis.com

Overview Request Response Summary Chart Notes

```
{  "processName": "getInformations",  "status": "success",  "message": "User not found",  "update_app": false,  "update_app_url": "-",  "update_message": "",  "update_size": "0.00",  "needLogout": "1",  "purchased_packages": [],  "purchased_packages_label": "",  "hasNewMessage": 0,  "hide_status": 0,  "all_in_one": 0,  "loadTimeAfterhasAllInOne": 0.055053949356079102,  "terms_url": "https://payingpos.link/terms-of-service",  "privacy_url": "https://payingpos.link/Privacy_Policy_files",  "iv": "fedcba9876543210",  "instagram_username": "postegro.llc",  "loadTimeAftergetPrices": 0.055055856704711914}
```

Postegro & Lili (@postegro) X +
www.instagram.com/postegro.llc/
GitHub sayfam Hack 4 Career. Infor... LinkedIn Mert SARICA (merts... Inbox - mert.sarica...

Instagram Search Log In Sign Up

postegro.llc Follow
17 posts 87.5k followers 2 following
Postegro & Lili
indirme linki
postegro.net

POSTS IGTV TAGGED

Web Postegro & Lili
WebPostegro
Reklam için - Uygulama içi satın alma
2.2 MB 3+ için derecelendirildi 100+ indirme
Yükle

Lütfen uygulamayı silip ve yeniden bu sitemizden yükleyin
https://postegro.net/

Postegro domaini ile bağlı sıkıntı var ve farkındayız. Teknik ekibimiz yeni domain üzerinde çalışıyor ve 48 saat arzında yeni güncelleme ile sorun hall edilecektir. Merak etmeyin tüm aboneliklerinizde hiç bir sorun olmayacaktır.

Merhaba. Teknik ekibimizin yoğun çalışmaları sonucu tüm sorunlar çözüldü ve uygulamayı rahatlıkla kullanabilirsiniz. Kullanıcılarımızın isteklerini dikkate alarak

Arkadaşlar şu anlık sunucumuzda güncelleme ve geliştirme işlemleri yaptığımız için sorunlar devam ediyor. Teknik ekibimizin verdiği bilgilere göre bu sorunlar 2, 3 gün devam edecektir. Bu işlemler

halkının ve tüm İslam alemlerinin bayramını Postegro ekibi adından kutluyoruz

Log In to Instagram
Log in to see photos and videos from friends and discover other accounts you'll love.
Log In Sign Up

Postegro - View hidden in: X +
postegro.net
GitHub sayfam Hack 4 Career. Infor... LinkedIn Mert SARICA (merts... Inbox - mert.sarica...

POSTEGRO

Home About us Screenshots Price

POSTEGRO APP

DOWNLOAD APK Google Play Web Version

You can view any instagram profile with our product
It is free
And you will enjoy it

When I examined the traffic recorded with Charles Proxy, I saw that the Web Postegro Lili (Web Postegro Lili_v1.0_apkpure.com.apk) application communicated with the payingpos[.]xyz, webpostegro[.]net, and postegro[.]net servers during use.

When I uploaded the APK file 39.apk to VirusTotal, I did not receive any warning about it being malicious, similar to previous result. When I used the Web Postegro & Lili (39.apk) application, I saw that it communicated with the postegro202039348[.]com, imagecropper2020[.]com, postegro[.]net, and the inactive postegro[.]com servers. Because the postegro[.]com address was not working, and the general functions of the Web Postegro & Lili (39.apk) application, such as viewing profiles that are hidden and viewing profile viewers were not functioning, so I continued my analysis using the Web Postegro & Lili (Web Postegro Lili_v1.0_apkpure.com.apk) application.

When I ran the Web Postegro & Lili application, I saw menus that allowed me to view profiles set to private (View accounts) and view profile viewers (Who viewed me). When I clicked on the View accounts menu, the application communicated with the instagram.com server through its own interface and brought up the login page where the Instagram username and password were entered. As soon as I logged in with my osmentosman24 Instagram username and password, which I created specifically for this investigation, I noticed that the application sent my session information, which was generated after verification with the instagram.com server, to the payingpos[.]xyz address using the cookie parameter and recorded this and more information in the /data/data/com.web.lilipostegro/shared_prefs/com.web.lilipostegro_preferences.xml file!



Hesaplara bak

Bana kim baktı

Mağaza

Abonelikleriniz



Instagram

Log In

OR

 Log in with Facebook

[Forgot password?](#)

Don't have an account? [Sign up](#)

Get the app.



The screenshot shows the Charles Proxy interface with a list of network requests. A red arrow points to the 'app_version' field in the request details, which has the value '1.0'. Another red arrow points to the search results in the 'Find in Session 1' dialog, highlighting a response header containing the token 'KIQTSigH9TPuAx5576rF1mRcH4eOY0'.

Code	Method	Host	Path	Start	Duration	Size	Status	Info
200	POST	www.instagram.com	/ajax/bz	18:02:47	164 ms	680 bytes	Complete	
200	POST	www.instagram.com	/logging/falco	18:02:47	164 ms	1.90 KB	Complete	
200	GET	www.instagram.com	/accounts/onetap/?next=%2F	18:02:48	309 ms	12.46 KB	Complete	
200	POST	graph.instagram.com	/logging_client_events	18:02:48	122 ms	5.70 KB	Complete	
200	GET	www.instagram.com	/static/bundles/es6/OneTapUpsell.js/d47af31ad21.js	18:02:49	35 ms	1.66 KB	Complete	
200	GET	www.instagram.com	/static/bundles/es6/OneTapUpsell.css/c312629c297e.css	18:02:49	36 ms	667 bytes	Complete	
200	GET	www.instagram.com	/graphql/query/?query_hash=7223fb3559610ca97900c019401669e7&variables=%7B%22only_stories%22%3Atrue%2C...	18:02:50	293 ms	498 bytes	Complete	
200	GET	www.instagram.com	/graphql/query/?query_hash=ed76c36f16156cfdb12233b4ee43b43&variables=%7B%22has_threaded_comments%22...	18:02:50	546 ms	628 bytes	Complete	
200	POST	www.instagram.com	/ajax/bz	18:02:51	191 ms	901 bytes	Complete	
200	POST	graph.instagram.com	/logging_client_events	18:02:51	170 ms	6.57 KB	Complete	
200	GET	www.instagram.com	/static/bundles/es6/ActivityFeedBox.js/8f6003baeb70.js	18:02:51	42 ms	31.41 KB	Complete	
200	POST	payingpos.xyz	/api/versions/1.php?processName=login	18:02:51	2.18 s	1.05 KB	Complete	
200	GET	www.instagram.com	/static/bundles/es6/ActivityFeedBox.css/3893332a2b8f.css	18:02:51	35 ms	1.85 KB	Complete	

To be able to use the application, I had to follow at least 10 people or have 10 people follow me, so I quickly started following Instagram accounts that followed back and made them follow me as well. After increasing my follower count and stopping following all the accounts I was following, I started exploring the menus of the application and could view the content of profiles that were set to private and hidden. This application generates income by charging a certain fee to remove limits on the application (such as removing ads, unlimited viewing of stories, unlimited viewing of accounts, and the uncensored display of names of profile viewers).

You have to minimum 10 following or 10 followers. Your following count are 0 and followers count are 0

OK

- Open GAPP
- Lock
- GPS
- Camera
- Rotation
- ID
- Microphone
- Wi-Fi
- Notifications
- Share
- Volume Up
- Volume Down
- Refresh
- Clipboard
- Home
- Power

Web Postegro

webpostegro.net/store#tab=monthly

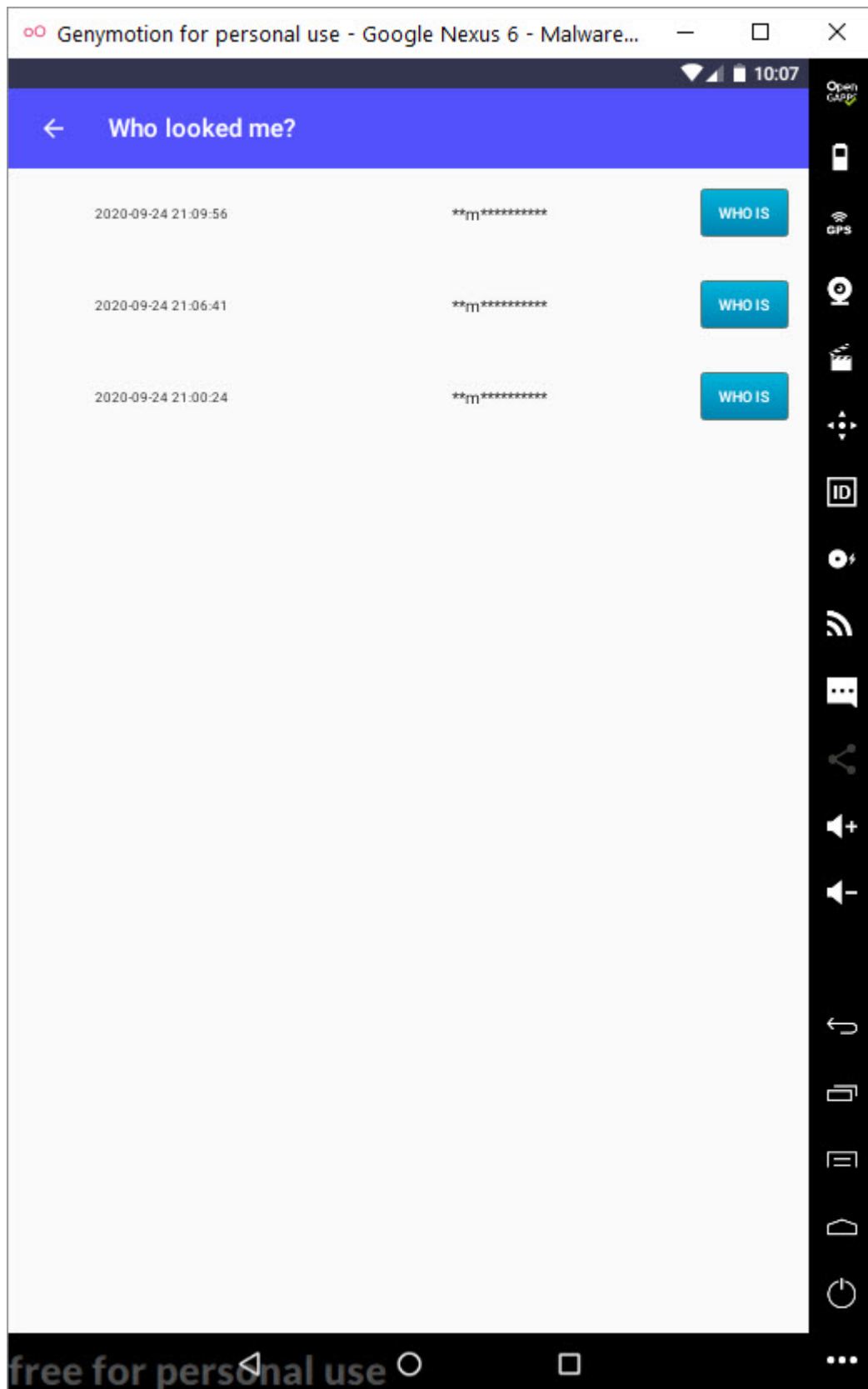
Mağaza monthly

Aylık Yıllık Abonelikler

Reklamları kaldırın Reklamları kaldırın 14.5₺	Hikayelere sınırsız bakın Hikayelere sınırsız bakabilirsiniz. (günlük hikayeler de dahil) 20.9₺
Hesaplara sınırsız bakın Gizli hesaplara sınırsız bakabilirsiniz. 27.9₺	Gizli mod Gizli modda hesaplara bakabilirsiniz (Hedef kullanıcı bu konuda bilgilendirilmez) 69.8₺
Bana kim baktı? Hesabınızı kimlerin görüntülediğini öğrenebilirsiniz. 95.8₺	Hepsi birinde Gizli hesapların gönderilerine ve hikayelerine sınırsız bakın, tüm reklamları kaldırın, Hesabınızı kimlerin görüntülediğini öğrenin ve tüm hesaplara gizli moda bakın (Hedef kullanıcı bu konuda bilgilendirilmez) + Bu zamana kadar baktığınız gizli hesaplardan sizin onları görüntüleme geçmişiniz silinecek + Ayarlar bölümünde 'Profili mi gizle' bölümü etkinleşecek 209.2₺

TURKISH ENGLISH

free for personal use



Generally, when an application with a secure architecture wants to access your Instagram information, it uses the OAuth protocol to request authorization from you. However, the Web Postegro & Lili application does not have a section that asks for permission or approval from the user. Therefore, to allow this application to view and list hidden profiles, it must constantly access the information of all accounts belonging to users who log

in through the application by connecting to the Instagram servers with session information belonging to those users. (session hijack) To understand that this method is being used, I conducted a test using Burp Suite over VPN to determine if the session information sent by the Web Postegro & Lili application to the payingpos[.]xyz address with the cookie parameter was sufficient to access my Instagram account. When I logged in to Instagram again through the Web Postegro & Lili application and made a request through Burp Suite to my Instagram account's Login Activity page (https://www.instagram.com/session/login_activity/), I was able to successfully receive a response from the server. When I rechecked the Login Activity page to see if there was a way for Instagram to understand those who accessed the account in this way, unfortunately, my access from abroad using VPN was not shown.

The screenshot shows the Burp Suite interface with a request and response for the URL https://www.instagram.com/session/login_activity/. The request is a GET request with various cookies and headers. The response is a JSON object containing user profile data, including the user's name, phone number, profile picture URL, and session information. A red callout box points to the response, stating: "Login Activity sayfası İstanbul'dan geçerli bir çerez/oturum ile çağrıldı." (Login Activity page called with a valid cookie/session from Istanbul). Another red callout box points to the response, stating: "Ülke kodu TR olarak görünüyor, problem yok." (Country code is seen as TR, no problem).

```
GET /session/login_activity/ HTTP/1.1
accept-language: en-US,en;q=0.9,tr;q=0.8,az;q=0.7
cookie: ig_ds=0218593-3668-4876-8321-88B10040F02; mid=Y2uWhvABAAE2PpYUQV4w0kDN5la; csrftoken=Tp7AbtaIMJ3QUkFFKUBaopkFBRp04fa; ds_user_id=42200448532; sessionid=4220044853243ae6bb2ad7P7F9A3AS; rus=FTW; uzigen=({"78.1.1.1": 9121});lk1r:1k1RdxjFVYGdof_IB8-yM_3rqdo
accept: */*
x-requested-with: XMLHttpRequest
user-agent: Mozilla/5.0 (Linux; Android 6.0; Nexus 5 Build/MRA58N) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Mobile Safari/537.36
Host: www.instagram.com
Connection: Keep-Alive
Accept-Encoding: gzip
```

```
{
  "config": {
    "csrf_token": "Tp7AbtaIMJ3QUkFFKUBaopkFBRp04fa",
    "viewer": {
      "biography": "",
      "external_url": null,
      "full_name": "Osman",
      "has_phone_number": false,
      "has_public_story": false,
      "id": "42200448532",
      "is_joined_recently": true,
      "is_private": true,
      "profile_pic_url": "https://instagram.fsa2-2.fna.fbcdn.net/v/t51.2885-19/11994171_612518468094701_2321684948211249007_n.jpg?nc_ht=instagram.fsa2-2.fna.fbcdn.net/u00260eb909edcfc4000f91b004488b3f5c49e/u00260ee5934889b",
      "profile_pic_url_hd": "https://instagram.fsa2-2.fna.fbcdn.net/v/t51.2885-19/11994171_612518468094701_2321684948211249007_n.jpg?nc_ht=instagram.fsa2-2.fna.fbcdn.net/u00260eb909edcfc4000f91b004488b3f5c49e/u00260ee5934889b",
      "username": "osmantam28",
      "badge_count": 0,
      "badge_count_at_rest": 1600887836360,
      "viewer_id": "42200448532",
      "country_code": "TR",
      "language_code": "en-US",
      "entry_data": {
        "SettingsPages": {
          "data": {
            "suspicious_logins": {
              "id": "17882550514782929",
              "location": "Istanbul, Turkey",
              "latitude": "41.0079",
              "longitude": "28.9781",
              "device": "Android",
              "timestamp": "1600886548",
              "sessions": {
                "id": "5:1600886548",
              "location": "Istanbul, Turkey",
              "latitude": "41.0079",
              "longitude": "28.9781",
              "device": "This Android",
              "timestamp": "1600886548",
              "login_timestamp": "1600886548",
              "is_current": true,
              "login_id": "17882550514782929",
              "id": "20:1600874283",
              "location": "Istanbul, Turkey",
              "latitude": "41.0079",
              "longitude": "28.9781",
              "device": "Android",
              "timestamp": "1600874283",
              "is_current": false,
              "login_id": "1788852172068483",
              "id": "18:1600873369",
              "location": "41.0079",
              "longitude": "28.9781",
              "device": "Android",
              "timestamp": "1600873369",
              "is_current": false,
              "login_id": "18102969367168473",
              "id": "17:16008733169",
              "location": "41.0079",
              "longitude": "28.9781",
              "device": "Windows",
              "timestamp": "16008733169",
              "is_current": false,
              "login_id": "17852530976265431",
              "hostname": "16008733169",
              "deployment_stage": "02",
              "platform": "android",
              "nonce": "41a997c",
              "server_cookies": {
                "life": true,
                "knox": true,
                "24": true,
                "25": true,
                "26": true,
                "27": true,
                "28": true,
                "29": true,
                "30": true,
                "31": true,
                "32": true,
                "33": true,
                "34": true,
                "35": true,
                "36": true,
                "37": true,
                "38": true,
                "39": true,
                "40": true,
                "41": true,
                "42": true,
                "43": true,
                "44": true,
                "45": true,
                "46": true,
                "47": true,
                "48": true,
                "49": true,
                "50": true,
                "51": true,
                "52": true,
                "53": true,
                "54": true,
                "55": true,
                "56": true,
                "57": true,
                "58": true,
                "59": true,
                "60": true,
                "61": true,
                "62": true,
                "63": true,
                "64": true,
                "65": true,
                "66": true,
                "67": true,
                "68": true,
                "69": true,
                "70": true,
                "71": true,
                "72": true,
                "73": true,
                "74": true,
                "75": true,
                "76": true,
                "77": true,
                "78": true,
                "79": true,
                "80": true,
                "81": true,
                "82": true,
                "83": true,
                "84": true,
                "85": true,
                "86": true,
                "87": true,
                "88": true,
                "89": true,
                "90": true,
                "91": true,
                "92": true,
                "93": true,
                "94": true,
                "95": true,
                "96": true,
                "97": true,
                "98": true,
                "99": true,
                "100": true,
                "101": true,
                "102": true,
                "103": true,
                "104": true,
                "105": true,
                "106": true,
                "107": true,
                "108": true,
                "109": true,
                "110": true,
                "111": true,
                "112": true,
                "113": true,
                "114": true,
                "115": true,
                "116": true,
                "117": true,
                "118": true,
                "119": true,
                "120": true,
                "121": true,
                "122": true,
                "123": true,
                "124": true,
                "125": true,
                "126": true,
                "127": true,
                "128": true,
                "129": true,
                "130": true,
                "131": true,
                "132": true,
                "133": true,
                "134": true,
                "135": true,
                "136": true,
                "137": true,
                "138": true,
                "139": true,
                "140": true,
                "141": true,
                "142": true,
                "143": true,
                "144": true,
                "145": true,
                "146": true,
                "147": true,
                "148": true,
                "149": true,
                "150": true,
                "151": true,
                "152": true,
                "153": true,
                "154": true,
                "155": true,
                "156": true,
                "157": true,
                "158": true,
                "159": true,
                "160": true,
                "161": true,
                "162": true,
                "163": true,
                "164": true,
                "165": true,
                "166": true,
                "167": true,
                "168": true,
                "169": true,
                "170": true,
                "171": true,
                "172": true,
                "173": true,
                "174": true,
                "175": true,
                "176": true,
                "177": true,
                "178": true,
                "179": true,
                "180": true,
                "181": true,
                "182": true,
                "183": true,
                "184": true,
                "185": true,
                "186": true,
                "187": true,
                "188": true,
                "189": true,
                "190": true,
                "191": true,
                "192": true,
                "193": true,
                "194": true,
                "195": true,
                "196": true,
                "197": true,
                "198": true,
                "199": true,
                "200": true,
                "201": true,
                "202": true,
                "203": true,
                "204": true,
                "205": true,
                "206": true,
                "207": true,
                "208": true,
                "209": true,
                "210": true,
                "211": true,
                "212": true,
                "213": true,
                "214": true,
                "215": true,
                "216": true,
                "217": true,
                "218": true,
                "219": true,
                "220": true,
                "221": true,
                "222": true,
                "223": true,
                "224": true,
                "225": true,
                "226": true,
                "227": true,
                "228": true,
                "229": true,
                "230": true,
                "231": true,
                "232": true,
                "233": true,
                "234": true,
                "235": true,
                "236": true,
                "237": true,
                "238": true,
                "239": true,
                "240": true,
                "241": true,
                "242": true,
                "243": true,
                "244": true,
                "245": true,
                "246": true,
                "247": true,
                "248": true,
                "249": true,
                "250": true,
                "251": true,
                "252": true,
                "253": true,
                "254": true,
                "255": true,
                "256": true,
                "257": true,
                "258": true,
                "259": true,
                "260": true,
                "261": true,
                "262": true,
                "263": true,
                "264": true,
                "265": true,
                "266": true,
                "267": true,
                "268": true,
                "269": true,
                "270": true,
                "271": true,
                "272": true,
                "273": true,
                "274": true,
                "275": true,
                "276": true,
                "277": true,
                "278": true,
                "279": true,
                "280": true,
                "281": true,
                "282": true,
                "283": true,
                "284": true,
                "285": true,
                "286": true,
                "287": true,
                "288": true,
                "289": true,
                "290": true,
                "291": true,
                "292": true,
                "293": true,
                "294": true,
                "295": true,
                "296": true,
                "297": true,
                "298": true,
                "299": true,
                "300": true,
                "301": true,
                "302": true,
                "303": true,
                "304": true,
                "305": true,
                "306": true,
                "307": true,
                "308": true,
                "309": true,
                "310": true,
                "311": true,
                "312": true,
                "313": true,
                "314": true,
                "315": true,
                "316": true,
                "317": true,
                "318": true,
                "319": true,
                "320": true,
                "321": true,
                "322": true,
                "323": true,
                "324": true,
                "325": true,
                "326": true,
                "327": true,
                "328": true,
                "329": true,
                "330": true,
                "331": true,
                "332": true,
                "333": true,
                "334": true,
                "335": true,
                "336": true,
                "337": true,
                "338": true,
                "339": true,
                "340": true,
                "341": true,
                "342": true,
                "343": true,
                "344": true,
                "345": true,
                "346": true,
                "347": true,
                "348": true,
                "349": true,
                "350": true,
                "351": true,
                "352": true,
                "353": true,
                "354": true,
                "355": true,
                "356": true,
                "357": true,
                "358": true,
                "359": true,
                "360": true,
                "361": true,
                "362": true,
                "363": true,
                "364": true,
                "365": true,
                "366": true,
                "367": true,
                "368": true,
                "369": true,
                "370": true,
                "371": true,
                "372": true,
                "373": true,
                "374": true,
                "375": true,
                "376": true,
                "377": true,
                "378": true,
                "379": true,
                "380": true,
                "381": true,
                "382": true,
                "383": true,
                "384": true,
                "385": true,
                "386": true,
                "387": true,
                "388": true,
                "389": true,
                "390": true,
                "391": true,
                "392": true,
                "393": true,
                "394": true,
                "395": true,
                "396": true,
                "397": true,
                "398": true,
                "399": true,
                "400": true,
                "401": true,
                "402": true,
                "403": true,
                "404": true,
                "405": true,
                "406": true,
                "407": true,
                "408": true,
                "409": true,
                "410": true,
                "411": true,
                "412": true,
                "413": true,
                "414": true,
                "415": true,
                "416": true,
                "417": true,
                "418": true,
                "419": true,
                "420": true,
                "421": true,
                "422": true,
                "423": true,
                "424": true,
                "425": true,
                "426": true,
                "427": true,
                "428": true,
                "429": true,
                "430": true,
                "431": true,
                "432": true,
                "433": true,
                "434": true,
                "435": true,
                "436": true,
                "437": true,
                "438": true,
                "439": true,
                "440": true,
                "441": true,
                "442": true,
                "443": true,
                "444": true,
                "445": true,
                "446": true,
                "447": true,
                "448": true,
                "449": true,
                "450": true,
                "451": true,
                "452": true,
                "453": true,
                "454": true,
                "455": true,
                "456": true,
                "457": true,
                "458": true,
                "459": true,
                "460": true,
                "461": true,
                "462": true,
                "463": true,
                "464": true,
                "465": true,
                "466": true,
                "467": true,
                "468": true,
                "469": true,
                "470": true,
                "471": true,
                "472": true,
                "473": true,
                "474": true,
                "475": true,
                "476": true,
                "477": true,
                "478": true,
                "479": true,
                "480": true,
                "481": true,
                "482": true,
                "483": true,
                "484": true,
                "485": true,
                "486": true,
                "487": true,
                "488": true,
                "489": true,
                "490": true,
                "491": true,
                "492": true,
                "493": true,
                "494": true,
                "495": true,
                "496": true,
                "497": true,
                "498": true,
                "499": true,
                "500": true,
                "501": true,
                "502": true,
                "503": true,
                "504": true,
                "505": true,
                "506": true,
                "507": true,
                "508": true,
                "509": true,
                "510": true,
                "511": true,
                "512": true,
                "513": true,
                "514": true,
                "515": true,
                "516": true,
                "517": true,
                "518": true,
                "519": true,
                "520": true,
                "521": true,
                "522": true,
                "523": true,
                "524": true,
                "525": true,
                "526": true,
                "527": true,
                "528": true,
                "529": true,
                "530": true,
                "531": true,
                "532": true,
                "533": true,
                "534": true,
                "535": true,
                "536": true,
                "537": true,
                "538": true,
                "539": true,
                "540": true,
                "541": true,
                "542": true,
                "543": true,
                "544": true,
                "545": true,
                "546": true,
                "547": true,
                "548": true,
                "549": true,
                "550": true,
                "551": true,
                "552": true,
                "553": true,
                "554": true,
                "555": true,
                "556": true,
                "557": true,
                "558": true,
                "559": true,
                "560": true,
                "561": true,
                "562": true,
                "563": true,
                "564": true,
                "565": true,
                "566": true,
                "567": true,
                "568": true,
                "569": true,
                "570": true,
                "571": true,
                "572": true,
                "573": true,
                "574": true,
                "575": true,
                "576": true,
                "577": true,
                "578": true,
                "579": true,
                "580": true,
                "581": true,
                "582": true,
                "583": true,
                "584": true,
                "585": true,
                "586": true,
                "587": true,
                "588": true,
                "589": true,
                "590": true,
                "591": true,
                "592": true,
                "593": true,
                "594": true,
                "595": true,
                "596": true,
                "597": true,
                "598": true,
                "599": true,
                "600": true,
                "601": true,
                "602": true,
                "603": true,
                "604": true,
                "605": true,
                "606": true,
                "607": true,
                "608": true,
                "609": true,
                "610": true,
                "611": true,
                "612": true,
                "613": true,
                "614": true,
                "615": true,
                "616": true,
                "617": true,
                "618": true,
                "619": true,
                "620": true,
                "621": true,
                "622": true,
                "623": true,
                "624": true,
                "625": true,
                "626": true,
                "627": true,
                "628": true,
                "629": true,
                "630": true,
                "631": true,
                "632": true,
                "633": true,
                "634": true,
                "635": true,
                "636": true,
                "637": true,
                "638": true,
                "639": true,
                "640": true,
                "641": true,
                "642": true,
                "643": true,
                "644": true,
                "645": true,
                "646": true,
                "647": true,
                "648": true,
                "649": true,
                "650": true,
                "651": true,
                "652": true,
                "653": true,
                "654": true,
                "655": true,
                "656": true,
                "657": true,
                "658": true,
                "659": true,
                "660": true,
                "661": true,
                "662": true,
                "663": true,
                "664": true,
                "665": true,
                "666": true,
                "667": true,
                "668": true,
                "669": true,
                "670": true,
                "671": true,
                "672": true,
                "673": true,
                "674": true,
                "675": true,
                "676": true,
                "677": true,
                "678": true,
                "679": true,
                "680": true,
                "681": true,
                "682": true,
                "683": true,
                "684": true,
                "685": true,
                "686": true,
                "687": true,
                "688": true,
                "689": true,
                "690": true,
                "691": true,
                "692": true,
                "693": true,
                "694": true,
                "695": true,
                "696": true,
                "697": true,
                "698": true,
                "699": true,
                "700": true,
                "701": true,
                "702": true,
                "703": true,
                "704": true,
                "705": true,
                "706": true,
                "707": true,
                "708": true,
                "709": true,
                "710": true,
                "711": true,
                "712": true,
                "713": true,
                "714": true,
                "715": true,
                "716": true,
                "717": true,
                "718": true,
                "719": true,
                "720": true,
                "721": true,
                "722": true,
                "723": true,
                "724": true,
                "725": true,
                "726": true,
                "727": true,
                "728": true,
                "729": true,
                "730": true,
                "731": true,
                "732": true,
                "733": true,
                "734": true,
                "735": true,
                "736": true,
                "737": true,
                "738": true,
                "739": true,
                "740": true,
                "741": true,
                "742": true,
                "743": true,
                "744": true,
                "745": true,
                "746": true,
                "747": true,
                "748": true,
                "749": true,
                "750": true,
                "751": true,
                "752": true,
                "753": true,
                "754": true,
                "755": true,
                "756": true,
                "757": true,
                "758": true,
                "759": true,
                "760": true,
                "761": true,
                "762": true,
                "763": true,
                "764": true,
                "765": true,
                "766": true,
                "767": true,
                "768": true,
                "769": true,
                "770": true,
                "771": true,
                "772": true,
                "773": true,
                "774": true,
                "775": true,
                "776": true,
                "777": true,
                "778": true,
                "779": true,
                "780": true,
                "781": true,
                "782": true,
                "783": true,
                "784": true,
                "785": true,
                "786": true,
                "787": true,
                "788": true,
                "789": true,
                "790": true,
                "791": true,
                "792": true,
                "793": true,
                "794": true,
                "795": true,
                "796": true,
                "797": true,
                "798": true,
                "799": true,
                "800": true,
                "801": true,
                "802": true,
                "803": true,
                "804": true,
                "805": true,
                "806": true,
                "807": true,
                "808": true,
                "809": true,
                "810": true,
                "811": true,
                "812": true,
                "813": true,
                "814": true,
                "815": true,
                "816": true,
                "817": true,
                "818": true,
                "819": true,
                "820": true,
                "821": true,
                "822": true,
                "823": true,
                "824": true,
                "825": true,
                "826": true,
                "827": true,
                "828": true,
                "829": true,
                "830": true,
                "831": true,
                "832": true,
                "833": true,
                "834": true,
                "835": true,
                "836": true,
                "837": true,
                "838": true,
                "839": true,
                "840": true,
                "841": true,
                "842": true,
                "843": true,
                "844": true,
                "845": true,
                "846": true,
                "847": true,
                "848": true,
                "849": true,
                "850": true,
                "851": true,
                "852": true,
                "853": true,
                "854": true,
                "855": true,
                "856": true,
                "857": true,
                "858": true,
                "859": true,
                "860": true,
                "861": true,
                "862": true,
                "863": true,
                "864": true,
                "865": true,
                "866": true,
                "867": true,
                "868": true,
                "869": true,
                "870": true,
                "871": true,
                "872": true,
                "873": true,
                "874": true,
                "875": true,
                "876": true,
                "877": true,
                "878": true,
                "879": true,
                "880": true,
                "881": true,
                "882": true,
                "883": true,
                "884": true,
                "885": true,
                "886": true,
                "887": true,
                "888": true,
                "889": true,
                "890": true,
                "891": true,
                "892": true,
                "893": true,
                "894": true,
                "895": true,
                "896": true,
                "897": true,
                "898": true,
                "899": true,
                "900": true,
                "901": true,
                "902": true,
                "903": true,
                "904": true,
                "905": true,
                "906": true,
                "907": true,
                "908": true,
                "909": true,
                "910": true,
                "911": true,
                "912": true,
                "913": true,
                "914": true,
                "915": true,
                "916": true,
                "917": true,
                "918": true,
                "919": true,
                "920": true,
                "921": true,
                "922": true,
                "923": true,
                "924": true,
                "925": true,
                "926": true,
                "927": true,
                "928": true,
                "929": true,
                "930": true,
                "931": true,
                "932": true,
                "933": true,
                "934": true,
                "935": true,
                "936": true,
                "937": true,
                "938": true,
                "939": true,
                "940": true,
                "941": true,
                "942": true,
                "943": true,
                "944": true,
                "945": true,
                "946": true,
                "947": true,
                "948": true,
                "949": true,
                "950": true,
                "951": true,
                "952": true,
                "953": true,
                "954": true,
                "955": true,
                "956": true,
                "957": true,
                "958": true,
                "959": true,
                "960": true,
                "961": true,
                "962": true,
                "963": true,
                "964": true,
                "965": true,
                "966": true,
                "967": true,
                "968": true,
                "969": true,
                "970": true,
                "971": true,
                "972": true,
                "973": true,
                "974": true,
                "975": true,
                "976": true,
                "977": true,
                "978": true,
                "979": true,
                "980": true,
                "981": true,
                "982": true,
                "983": true,
                "984": true,
                "985": true,
                "986": true,
                "987": true,
                "988": true,
                "989": true,
                "990": true,
                "991": true,
                "992": true,
                "993": true,
                "994": true,
                "995": true,
                "996": true,
                "997": true,
                "998": true,
                "999": true,
                "1000": true
              }
            }
          }
        }
      }
    }
  }
}
```


Instagram Login Activity

Was This You?

Istanbul, Turkey
25 minutes ago - Android

This Was Me | This Wasn't Me

Where You're Logged in

- Istanbul, Turkey
Active now - This Windows
- Istanbul, Turkey
25 minutes ago - Android
- Istanbul, Turkey
3 hours ago - Android
- Istanbul, Turkey
4 hours ago - Android

İstanbul'dan giriş yaptığım için kayıtlarda bir hata görünmüyor.

WhatIsMyIP.com

My Public IPv4 is: 37.1

My Public IPv6 is: Not Detected

Location: Rome, 62 IT

ISP: Secure Data Systems SRL

My IP Information

IP Address Lookup

Recent Articles

Protect Yourself With Two-Factor Authentication

Two-Factor authentication simply adds a second step to the log-in process to verify yourself. This extra verification usually takes the form of a numeric code that is sent to your phone.

Ways to Prevent Hacking

Because of TV and movies, most of us have a similar picture of a hacker: a young, thin, and somewhat nerdy-looking person sitting at a computer screen in a dark room, typing furiously.

İtalya, Roma'ya VPN yapıldı.

What Is My IP?

WhatIsMyIP.com® is the industry leader in providing REAL IP address information. We have extensive tutorials that show users how to perform an Internet Speed Test, IP address lookup, proxy detection, IP Whois Lookup, and more. We have extensive tutorials that show users how to trace an email address, how to change IP addresses, and how to hide their IP information. Knowing your IP address is crucial for online gaming, tech support, using remote desktop connections, connecting to a security camera DVR, anonymity or even running an email server. If you've got questions about IP addresses and can't find the answer on our site, feel free to post your question in our IP Address Q & A section.

What Is An IP Address?

This number is an exclusive number on all information technology devices (printers, routers, modems, etc) use which identifies and allows them the ability to communicate with each other on a computer network. [Read more...]

What Is IPv6?

IPv6 or Internet Protocol version 6 is the replacement for IPv4. An IPv6 address looks like this 2600:1005:b062:61e4:74d7:f292:802c:cfbd and an IPv4 address looks like this 76.133.323.355. [Read more...]

The image shows a Burp Suite interface with a session hijack and a screenshot of the Instagram Login Activity page. The Burp Suite interface displays a request and response for a session hijack. The response shows a session ID and a location in Istanbul, Turkey. The Instagram Login Activity page shows a location in Istanbul, Turkey, with a note that the user is logged in from there. Red callouts explain the session hijack, the location change, and the VPN usage.

Oturum başarıyla kuruldu. (session-hijacked)

Ülke kodu değişti fakat lokasyon bilgileri hala değişmedi.

Daha önceki çerez, oturum ile VPN üzerinden İtalya'dan Login Activity sayfasını çağırdım.

Roma yazması gerekirken hala İstanbul yazıyor.

VPN ile İtalya, Roma'dan giriş yapmama rağmen hala İstanbul görünüyor.

Despite repeatedly explaining the situation to Facebook's security team with screenshots, they were unable to understand what they needed to do in the face of even the most basic fraudulent scenario (if an Instagram account is accessed from two different countries within 5 minutes, the user will be warned and the Login Activity page will show which country the connection was made from).

In order to regain control of my account and find out whether the Web Postegro & Lili app developer was still able to access my account after logging out, I accessed my Instagram account from a Windows device and

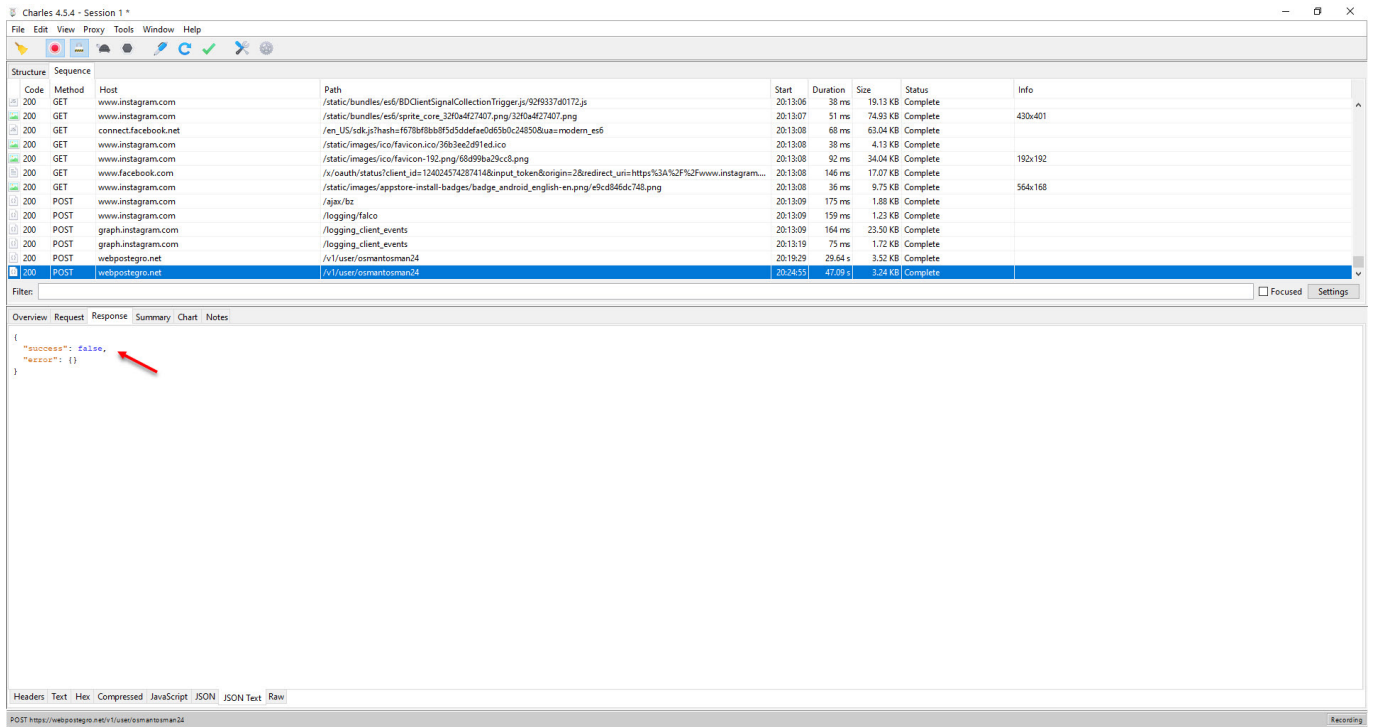
increased the number of people I followed by 1. Then, when I asked the webpostegro[.]net server to bring me the current information belonging to the user, it could also get me the information of the person I had most recently started following, meaning that access was still continuing.

The screenshot shows the Charles 4.5.4 interface with a network log table and a detailed view of a POST request to webpostegro.net. The log table includes columns for Code, Method, Host, Path, Start, Duration, Size, Status, and Info. The selected request is a POST to /v1/user/osmantosman24, returning a JSON object with user details.

Code	Method	Host	Path	Start	Duration	Size	Status	Info
200	GET	connect.facebook.net	/en_US/sdk.js	20:13:06	100 ms	18.86 KB	Complete	
200	GET	www.instagram.com	/static/bundles/esd/6DClientSignalCollectionTrigger.js/929327d0172.js	20:13:06	38 ms	19.13 KB	Complete	
200	GET	www.instagram.com	/static/bundles/esd/sprite_core_32f0e427407.png/32f0e427407.png	20:13:07	51 ms	74.93 KB	Complete	430x401
200	GET	connect.facebook.net	/en_US/sdk.js?hash=f678bf8b8f5d5d4e0d65b0c248506aa=modern_es6	20:13:08	68 ms	63.04 KB	Complete	
200	GET	www.instagram.com	/static/images/ico/favicon-ico/36b3e2d91ed.ico	20:13:08	38 ms	4.13 KB	Complete	
200	GET	www.instagram.com	/static/images/ico/favicon-192.png/68d99ba29c8.png	20:13:08	92 ms	34.04 KB	Complete	192x192
200	GET	www.facebook.com	/x/oauth/status/client_id=124024374287414&input_token&origin=2&redirect_uri=https%3A%2F%2Fwww.instagram.com	20:13:08	146 ms	17.07 KB	Complete	
200	GET	www.instagram.com	/static/images/appstore-install-badges/badge_android_english-en.png/e9c846d-748.png	20:13:08	36 ms	9.75 KB	Complete	564x168
200	POST	www.instagram.com	/api/v1/bz	20:13:09	173 ms	1.88 KB	Complete	
200	POST	www.instagram.com	/logging/fatco	20:13:09	159 ms	1.23 KB	Complete	
200	POST	graph.instagram.com	/logging_client_events	20:13:09	164 ms	23.50 KB	Complete	
200	POST	graph.instagram.com	/logging_client_events	20:13:19	75 ms	1.72 KB	Complete	
200	POST	webpostegro.net	/v1/user/osmantosman24	20:19:29	29.64 s	3.52 KB	Complete	

```
{
  "success": true,
  "user_id": "4200448830",
  "is_private": true,
  "username": "3170e4159885532a02566e6c056da49d",
  "user_data": {
    "username": "osmantosman24",
    "full_name": "Osman",
    "biography": "",
    "followers": 20,
    "post_count": 0,
    "profile_image": "https://content-lax3-1.cdninstagram.com/v/t51.2885-19/4320x320/119994171_612618466094701_202169498211249007_n.jpg?nc_h=content-lax3-1.cdninstagram.com_nc_obc=apF4FVOM9RvAX04G1g0sobw01e6E6272w56w879w26145a56c9b32waa0w5F958BF63",
    "is_private": true
  }
}
```

While I was thinking about how to prevent the Web Postegro & Lili application and its developer from accessing my Instagram account and session, I decided to see if changing my Instagram password would work and, whether or not I changed it, I confirmed that they couldn't access my account through webpostegro[.]net and ended my research here.



Brief summary of my research is:

1. The Web Postegro Lili Android app, which is used to see who views your profile, has access to your entire Instagram account by taking your session information when accessing your Instagram account.
2. Even if you log out or delete the Web Postegro Lili app, the developer's access to your Instagram account will continue. To prevent this, you will need to change your Instagram password.

As a personal recommendation, if you come across a person, application, website, etc., that promises to show you who views your profile, be aware that this feature does not exist among the features of the social media applications.

Hope to see you in the following articles.