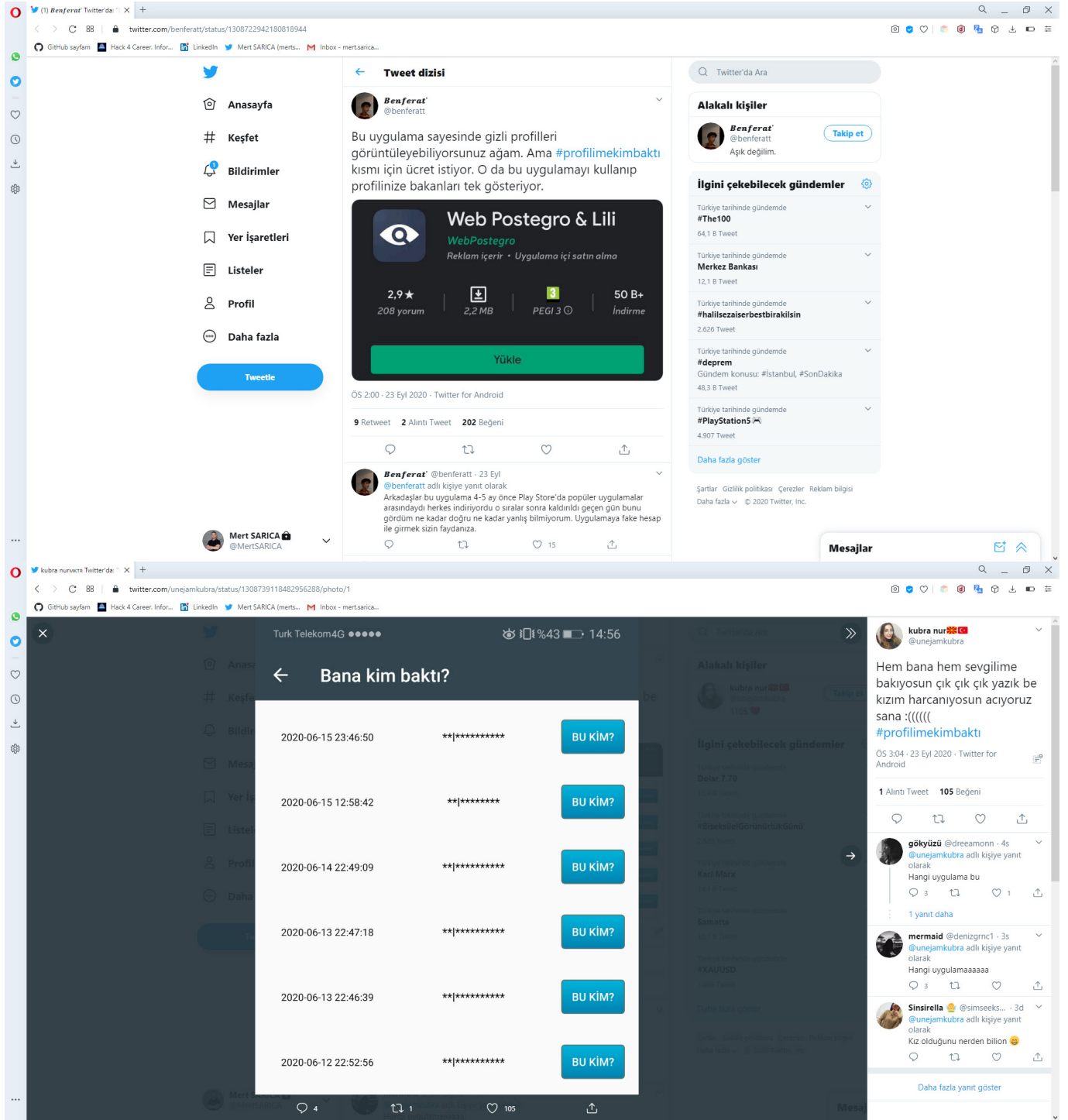


Who Viewed My Profile?

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.





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

Uygulamalar

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

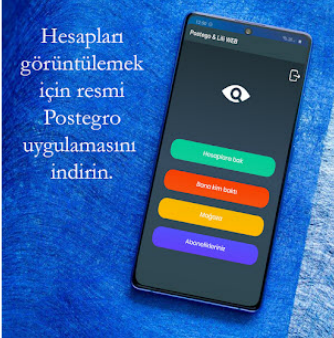
PEGI 3


Reklam içeriyor

Bu uygulama tüm cihazlarınızla uyumlu.

İstek Listesi'ne ekle

Yükle





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.

Web Postegro & Lili - Google Play

play.google.com/store/apps/details

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

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 geri 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 ihlalinin biz sorumlu değiliz;

* Bu uygulama, hiçbir sosyal medya platformu ile ilişkili değildir.

DARALT

YORUMI AR

Yorum Politikası

Web Postegro & Lili - Google Play Store

play.google.com/store/apps/details

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

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

Türkiyedeymiş 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 | Uyumsuz olarak işaretler |
| Sunan: | Geliştirici | |
| WebPostegro | webpostegro@gmail.com Gizlilik Politikası | |

©2020 Google Site Hizmet Şartları Gizlilik Geliştiriciler Google Hakkında | Konum: Türkiye Dil: Türkçe Tüm fiyatlarla 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

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

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. Gönderilerde beğenileri gösterme sorunu bir kaç gün içinde hall edilecektir. Şu an için uygulamaya girişte hiçbir sıkıntı yoktur. Eğer herhangi sorun yaşıyorsanız lütfen destek ekibimize iletişime geçin.

Enes Kuzu ★★★★★ 14 Eylül 2020

Adminler selamun aleykum öncelikle sizden ricamız lütfen bize bakanları ücretsiz yapabilirseniz çok makbule geçer yorumu okuduğunuz ve değerlendirdiğiniz için teşekkürler iyi günler.

WebPostegro 22 Eylül 2020

Merhaba. Eğer uygulama ortalama 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.

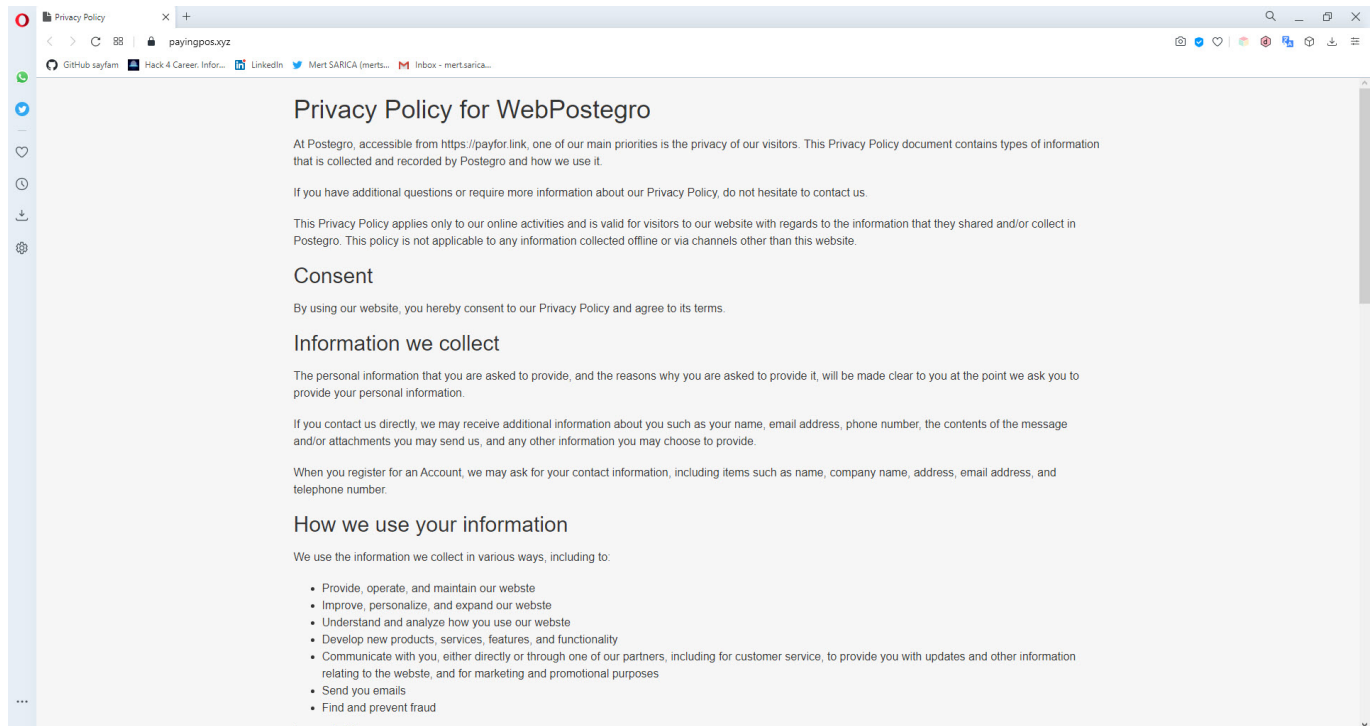
Elif Gürcan ★★★★★ 20 Eylül 2020

Yüklediniz 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.

Web Postegro & Lili for Android

apkpure.com/store/apps/details

GitHub sayfam Hack 4 Career. Infor... LinkedIn Mert SARIKA (merts... Inbox - mertsarika...

Apkpure GAMES APPS TOPICS PRODUCTS

Search... EN

Facebook Twitter YouTube

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.

Hesapları görüntülemek için resmi Postegro uygulamasını indirin.

Resmi Postegro uygulaması

Discover More »

Netflix
7.74.1 build 26 35115
Netflix, Inc.

Microsoft Edge
45.0.4.5072
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 *

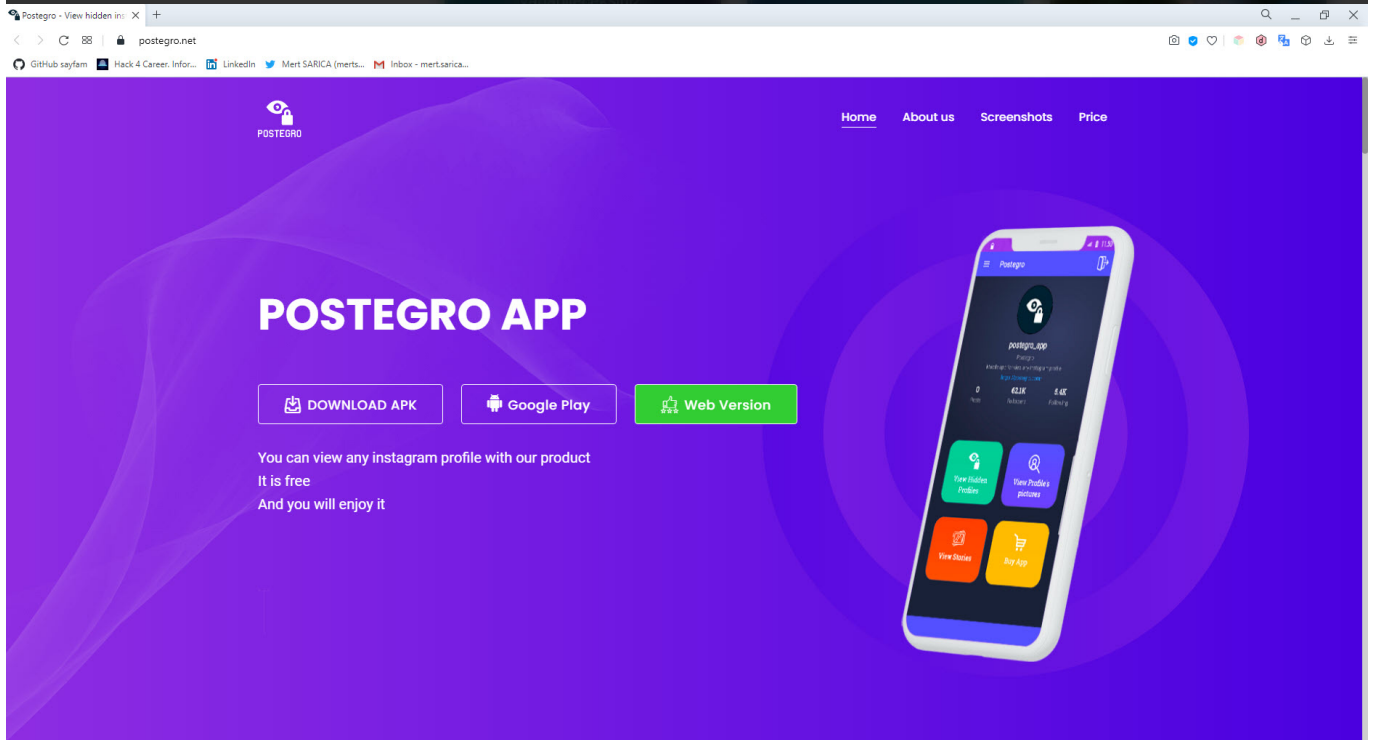
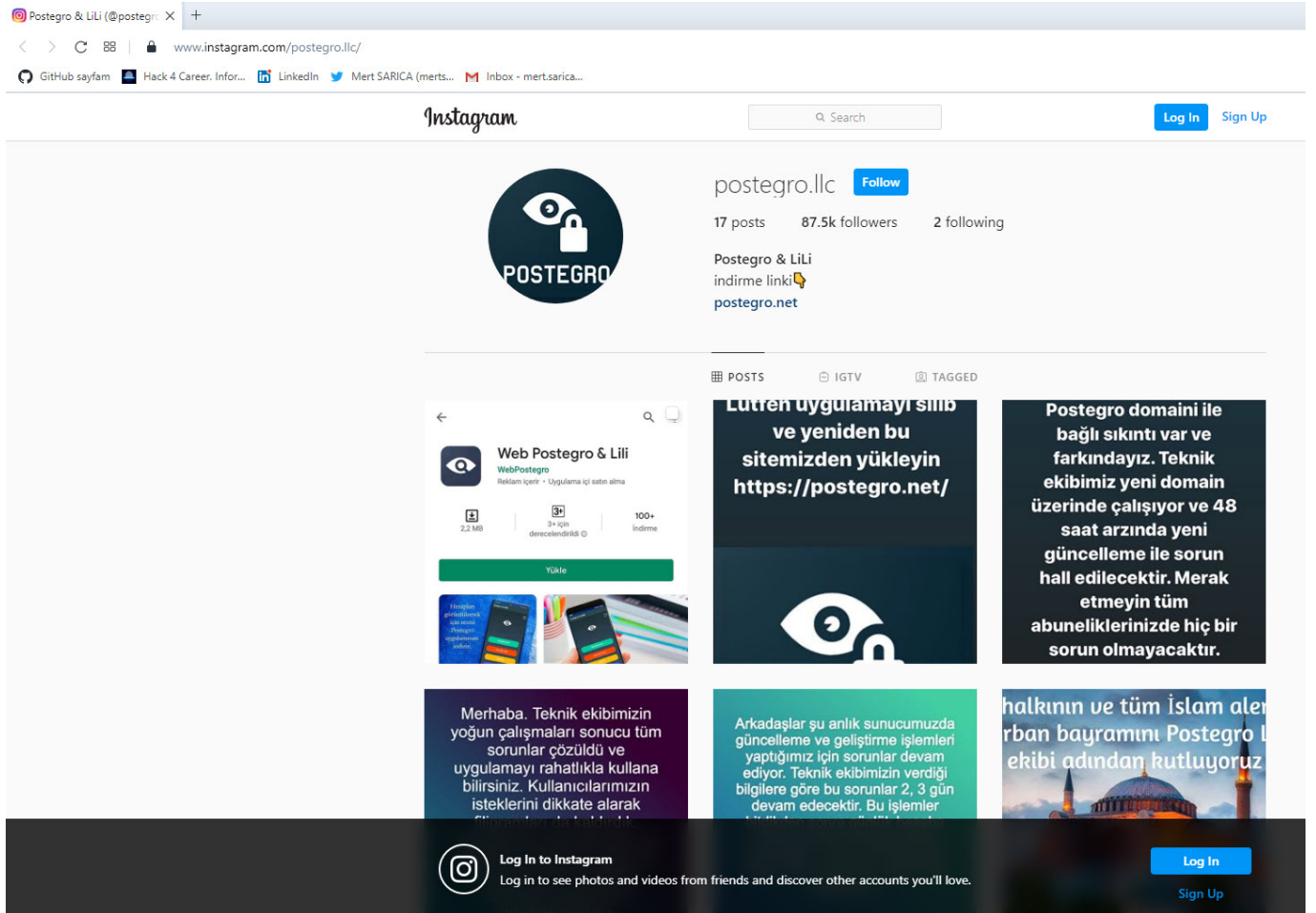
File Edit View Proxy Tools Window Help

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
}
```



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 osmantosman24 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

Phone number, username, or email

Password

Log In

OR

 Log in with Facebook

[Forgot password?](#)

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

Get the app.



[ABOUT](#) [HELP](#) [PRESS](#) [API](#) [JOBS](#) [PRIVACY](#) [TERMS](#)
[LOCATIONS](#) [TOP ACCOUNTS](#) [HASHTAGS](#) [LANGUAGE](#)

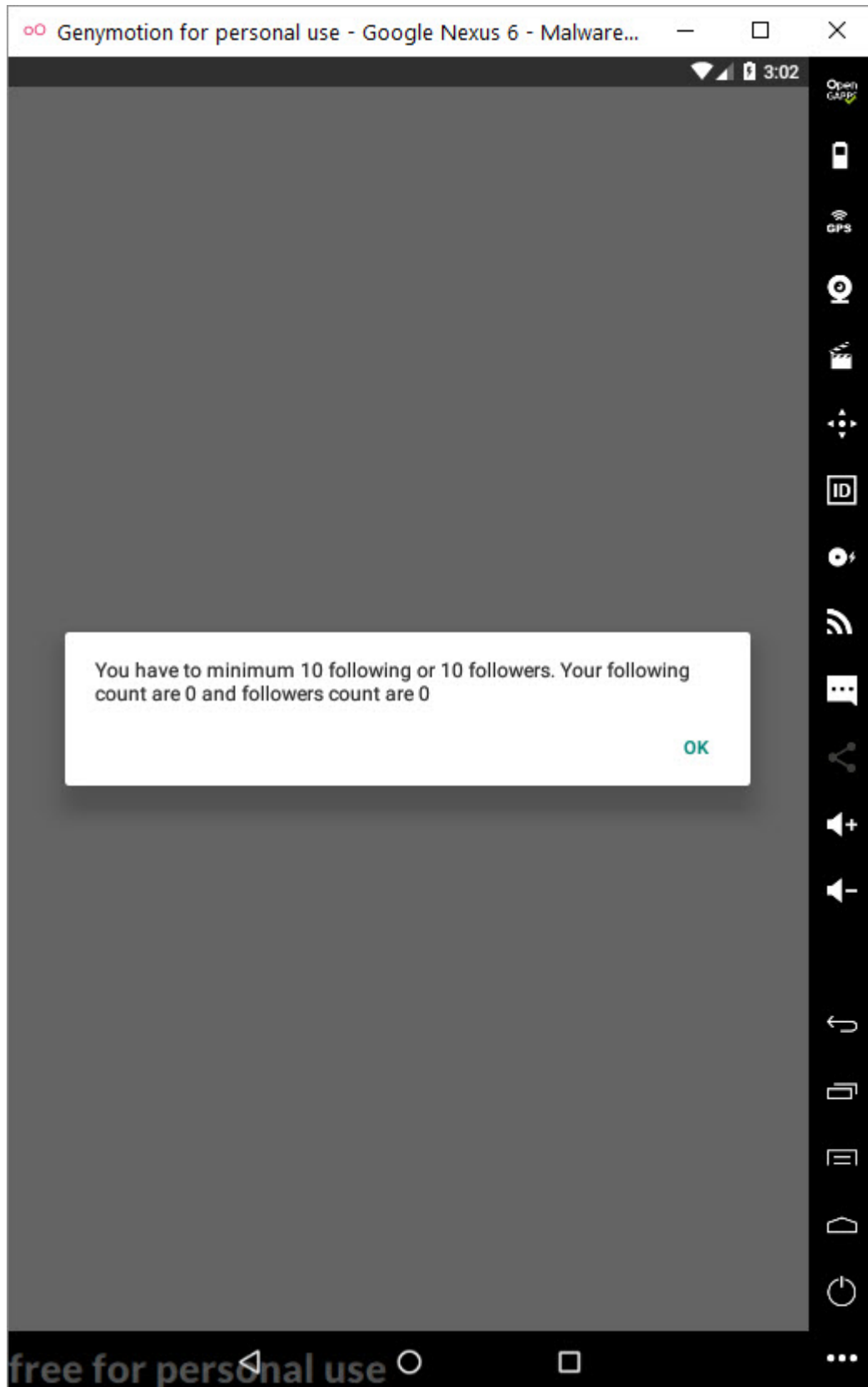
© 2020 INSTAGRAM FROM FACEBOOK

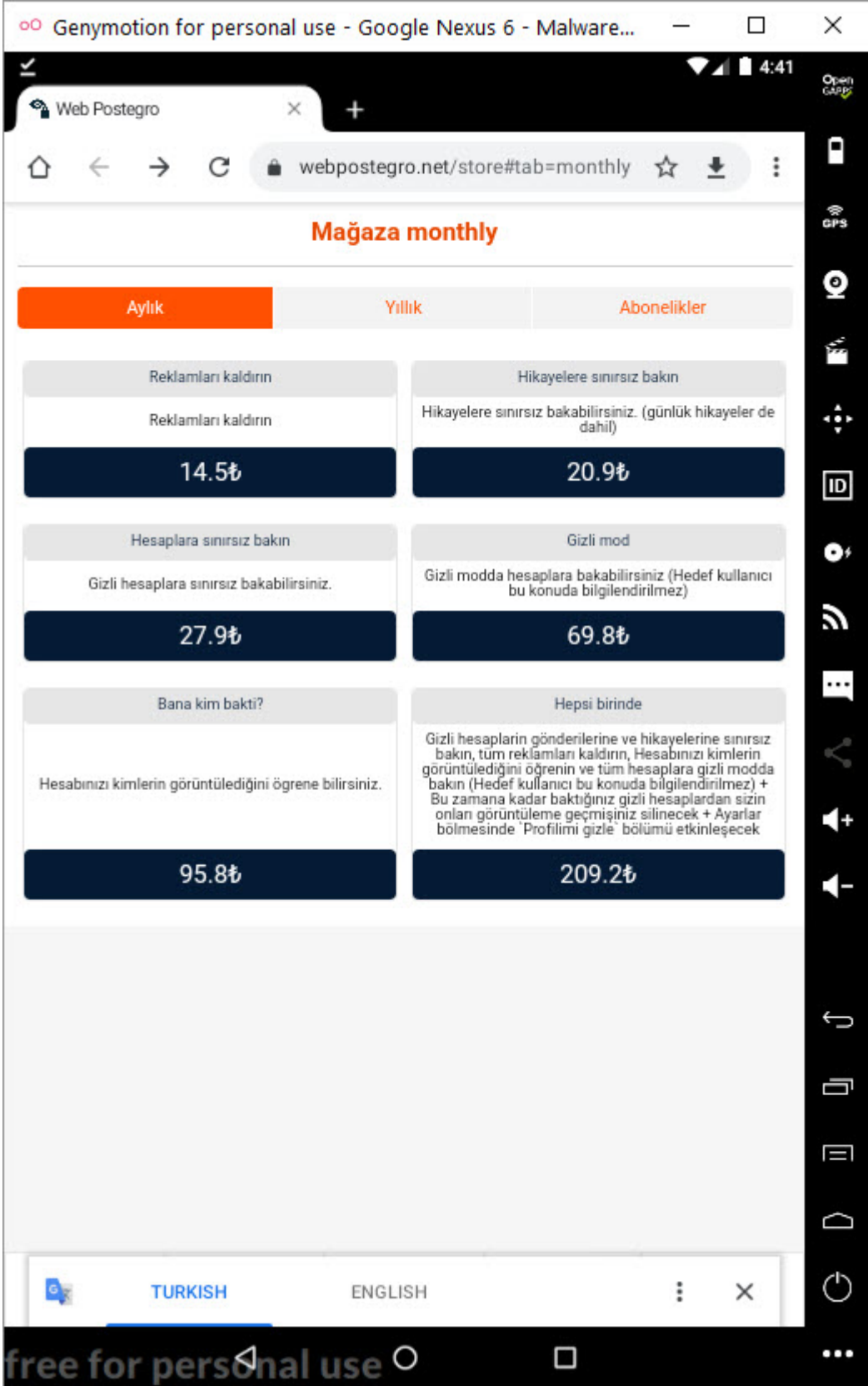


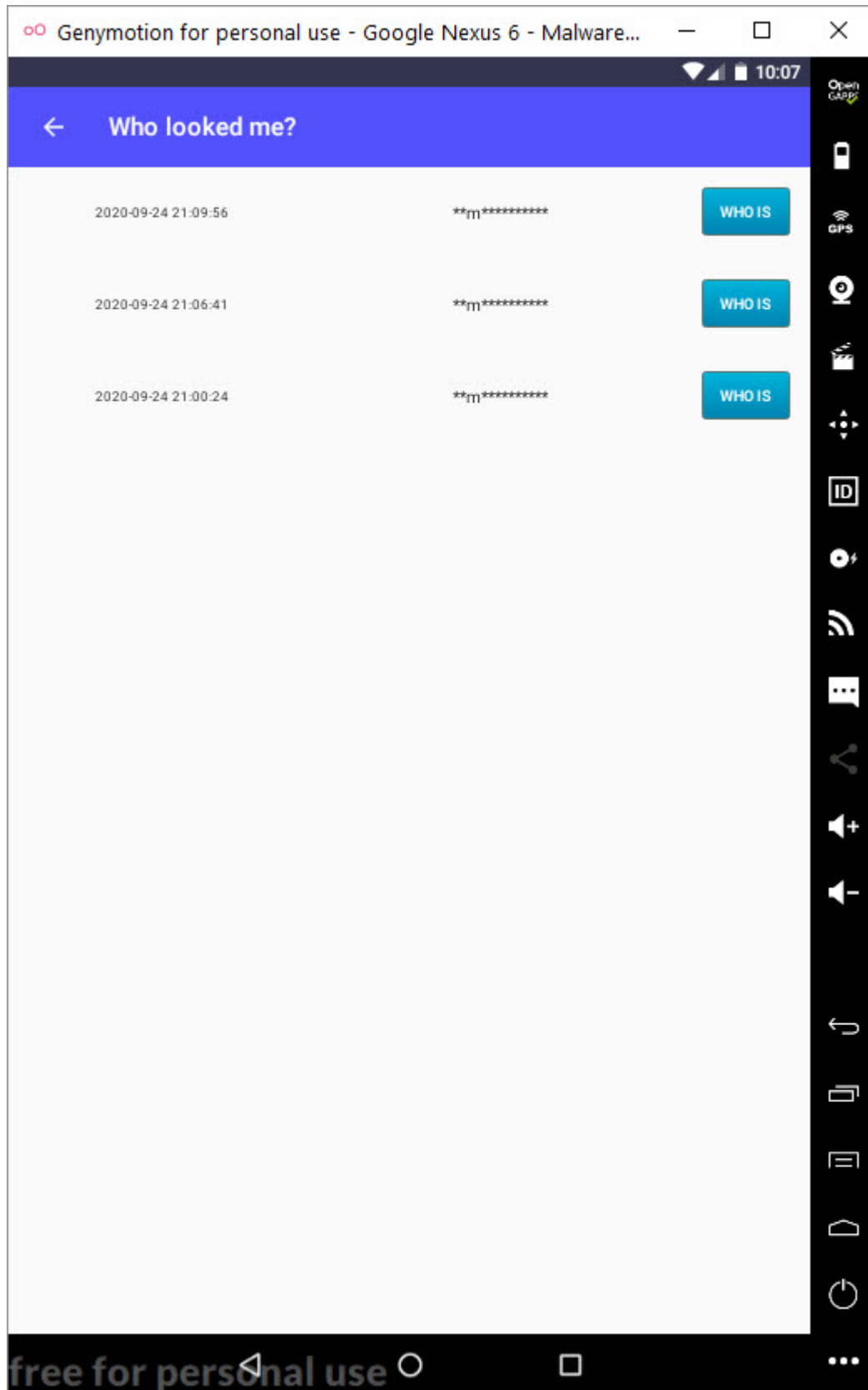
The screenshot shows the Charles 4.5.4 web proxy tool interface. The top pane displays a list of network requests. The bottom pane shows the details of a selected request, including headers, query string, and response body. A search window is open, displaying 41 results for the text `KIQTSigH9TPuA5576rFnmRCerHeOY0`. The search results are filtered by the 'Response Header: 2259' and the 'Content-Type: application/json' header. The search results list includes `https://payingpos.xyz/` (1 match), `https://www.instagram.com/` (37 matches), `accounts` (7 matches), `login` (1 match), `ajax` (1 match), `get_encrypted_credentials` (3 matches), `onemap` (3 matches), `static` (6 matches), `ajax` (5 matches), and `looinio` (6 matches).

| 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/onemap/?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/esf/OneTapUpsell.js/dd7af31ad1.js | 18:02:49 | 35 ms | 1.66 KB | Complete | |
| 200 | GET | www.instagram.com | /static/bundles/esf/OneTapUpsell.css/c312629c297e.css | 18:02:49 | 36 ms | 667 bytes | Complete | |
| 200 | GET | www.instagram.com | /graphql/query/?query_hash=7223fb3559610cad7900c019401669e78&variables=%7B%22only_stories%22%3Atrue%2C... | 18:02:50 | 293 ms | 498 bytes | Complete | |
| 200 | GET | www.instagram.com | /graphql/query/?query_hash=ed7dc3bf16156cfdb12233b4ee03b43&variables=%7B%22has_threaded_comments%22... | 18:02:50 | 546 ms | 628 bytes | Complete | |
| 200 | POST | www.instagram.com | /ajax/bz | 18:02:51 | 181 ms | 801 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/esf/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/esf/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).







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.

Request

```
GET /session/login_activity/ HTTP/1.1
Host: www.instagram.com
Accept-encoding: gzip
Cookie: ig_ds=0218569-1668-1476-8321-88310040702; mld=V3uWhuABAAZFPyUTQV4wKDN5la; csrf_token=Tp7AbtaIWJ3gUkFFKUBaopkF8Rpr04fa; ds_user_id=42200448532; sessionid=4220044853243Ae6cbW2ad7PT7F83AS; ruz=FTW; uzigen=178.1.1.1; 91211:1kL91r:SnRdxYFVYGdCoF_I88-yM_3rqdo
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
Connection: Keep-Alive
Accept-Encoding: gzip
```

Response

```
<link rel="stylesheet" href="/static/bundles/es6/ConsumerUICommons.css/5bf847374baf.css" type="text/css" crossorigin="anonymous" />
<link rel="stylesheet" href="/static/bundles/es6/ConsumerUICommons.css/0732f0d98130.css" type="text/css" crossorigin="anonymous" />
<script type="text/javascript">window._sharedData =
({
  "config": {
    "csrf_token": "Tp7AbtaIWJ3gUkFFKUBaopkF8Rpr04fa",
    "viewer": {
      "biography": "",
      "external_url": null,
      "full_name": "Osmann",
      "has_phone_number": false,
      "has_profile_pic": true,
      "has_tabbed_inbox": false,
      "id": "42200448532",
      "is_joined_recently": true,
      "is_private": true,
      "profile_pic_url": "https://instagram.fsa2-2.fna.fbcdn.net/v/t51.2885-19/15106150/119984171_612518466094701_2321684948211249007_n.jpg?nc_ht=instagram.fsa2-2.fna.fbcdn.net/u0026_nc_oh=457upTXoTWAX_T7qLc/u0026oh=eb9c9edcfc400c0f91b004488b3f5c49e/u0026oe=593489B",
      "profile_pic_url_hd": "https://instagram.fsa2-2.fna.fbcdn.net/v/t51.2885-19/6320x320/119984171_612518466094701_2321684948211249007_n.jpg?nc_ht=instagram.fsa2-2.fna.fbcdn.net/u0026_nc_oh=457upTXoTWAX_T7qLc/u0026oh=eb9c9edcfc400c0f91b004488b3f5c49e/u0026oe=593489B",
      "username": "osmanna204",
      "badge_count": 1,
      "badge_count": 0,
      "badge_count_at_me": 160088783660
    },
    "viewer_id": "42200448532",
    "country_code": "TR",
    "language_code": "en",
    "locale": "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": "17888521720688483",
                  "id": "18:1600873369",
                  "location": "Istanbul, Turkey",
                  "latitude": 41.0079,
                  "longitude": 28.9781,
                  "device": "Android",
                  "timestamp": 1600873369,
                  "is_current": false,
                  "login_id": "18102969367168473",
                  "id": "17:1600873369",
                  "location": "Istanbul, Turkey",
                  "latitude": 41.0079,
                  "longitude": 28.9781,
                  "device": "Windows",
                  "timestamp": 1600873369,
                  "is_current": false,
                  "login_id": "17852530976265431",
                  "hostname": "1600873369",
                  "bot": false,
                  "deployment_stage": "02",
                  "platform": "android",
                  "nonce": "14nw97c",
                  "data": {
                    "cache_schema_version": 3,
                    "server_checks": {
                      "life": true,
                      "knox": true,
                      "24": true,
                      "25": true,
                      "26": true,
                      "27": true,
                      "28": true,
                      "29": true,
                      "30": true,
                      "36": false,
                      "37": true,
                      "38": 25000,
                      "39": true,
                      "4": false,
                      "to_cache": {
                        "gatekeeper": "113",
                        "102": true,
                        "103": false,
                        "104": true,
                        "105": true,
                        "106": true,
                        "107": false,
                        "108": true,
                        "114": true,
                        "116": true,
                        "119": false,
                        "12": false,
                        "120": true,
                        "123": false,
                        "126": true,
                        "132": false,
                        "137": true,
                        "14": true,
                        "140": false,
                        "142": false,
                        "146": true,
                        "147": false,
                        "151": false,
                        "152": true,
                        "153": false,
                        "154": true,
                        "156": false,
                        "157": false,
                        "158": false,
                        "159": false,
                        "16": true,
                        "160": false,
                        "32": true,
                        "34": false,
                        "35": false,
                        "38": true,
                        "4": true,
                        "40": true,
                        "41": false,
                        "43": true,
                        "5": false,
                        "59": true,
                        "6": false,
                        "61": false,
                        "62": false,
                        "63": false,
                        "64": false,
                        "65": false,
                        "67": true,
                        "68": false,
                        "69": true,
                        "7": false,
                        "73": false,
                        "74": false,
                        "75": true,
                        "78": true,
                        "79": false,
                        "8": false,
                        "81": false,
                        "82": true,
                        "84": false,
                        "86": false,
                        "8": false,
                        "91": false,
                        "95": true,
                        "97": false,
                        "qe": {
                          "app_upsell": {
                            "q": "",
                            "p": {}
                          },
                          "control": {
                            "p": {
                              "is_enabled": true,
                              "blacklist": "fbcr_124024574287414",
                              "felix_creation_duration_limits": {
                                "q": "dogfooding",
                                "p": {
                                  "maximum_length_seconds": 3600
                                }
                              }
                            }
                          }
                        }
                      }
                    }
                  }
                }
              ]
            }
          ]
        }
      }
    }
  }
})
```

Login Activity sayfası İstanbul'dan geçerli bir çerez/oturum ile çağrıldı.

Ülke kodu TR olarak görünüyor, problem yok.

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 lone, hooded figure sitting in a dark room, typing furiously on a computer screen in the dim light of a monitor.

İtalya, Roma'ya VPN yapıldı.

What Is My IP?

WhatIsMyIP.com® is the industry leader in providing REAL IP address information. We provide the premium IP address lookup service that allows users 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 76.433.323.355. [Read more...]

Burp Suite Community Edition v2.1.04 - Temporary Project

Burp Project: Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

Send Cancel

Request

Raw Params Headers Hex

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_id=C21D59C9-3668-44F6-9521-BEB1C040F02; mld=X2uWhvABAAZPDUOTQVw0kDN01a;
csrf_token=7P7AbtaIKJ3gUkzFKUbaopkPBRp04fz; ds_user_id=42200448532; sessionid=42200448532; 3Ae6cbW2ad7PTFN3AS;
sur=FW; usigen=({\"37\":..., \"9121\":1K191zISrSrdxyFVYGD0Gf_I88-yM_3eqda\"
accept: */*
x-requested-with: XMLHttpRequest
user-agent: Mozilla/5.0 (Linux; Android 6.0; Nexus 5 Build/MRA58N) AppleWebKit/537.36 (KHTML, like Gecko)
Host: www.instagram.com
Connection: Keep-alive
Accept-Encoding: gzip

Response

Raw Headers Hex HTML Render

Target: https://www.instagram.com

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.

Instagram

Manage Contacts

Privacy and Security

Login Activity

Emails from Instagram

Where You're Logged in

Istanbul, Turkey
Active now - This Windows

Istanbul, Turkey
15 minutes ago - Android

Istanbul, Turkey
55 minutes ago - Android

Istanbul, Turkey
4 hours ago - Android

Istanbul, Turkey
4 hours ago - Android

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 - Session 1 interface. The top panel displays a list of network requests. The bottom panel shows the details of a selected POST request to webpostegro.net.

| 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/80ClientSignalCollectionTrigger.js/929337d0172.js | 20:13:06 | 38 ms | 19.13 KB | Complete | |
| 200 | GET | www.instagram.com | /static/bundles/esd/sprite_core_32f0a427407.png/32f0a427407.png | 20:13:07 | 51 ms | 74.93 KB | Complete | 430x401 |
| 200 | GET | connect.facebook.net | /en_US/sdk.js?hash=f678bfbbf8fd5d5defad65b0c248508a&modem_es6 | 20:13:08 | 68 ms | 63.04 KB | Complete | |
| 200 | GET | www.instagram.com | /static/images/ico/favicon.ico/36b3ee2d91edico | 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_tokenorigin=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/e1cd846dc748.png | 20:13:08 | 36 ms | 9.75 KB | Complete | 564x168 |
| 200 | POST | www.instagram.com | /api/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/osmanosman24 | 20:19:29 | 29.64 s | 3.52 KB | Complete | |

Filter: [] Focused Settings

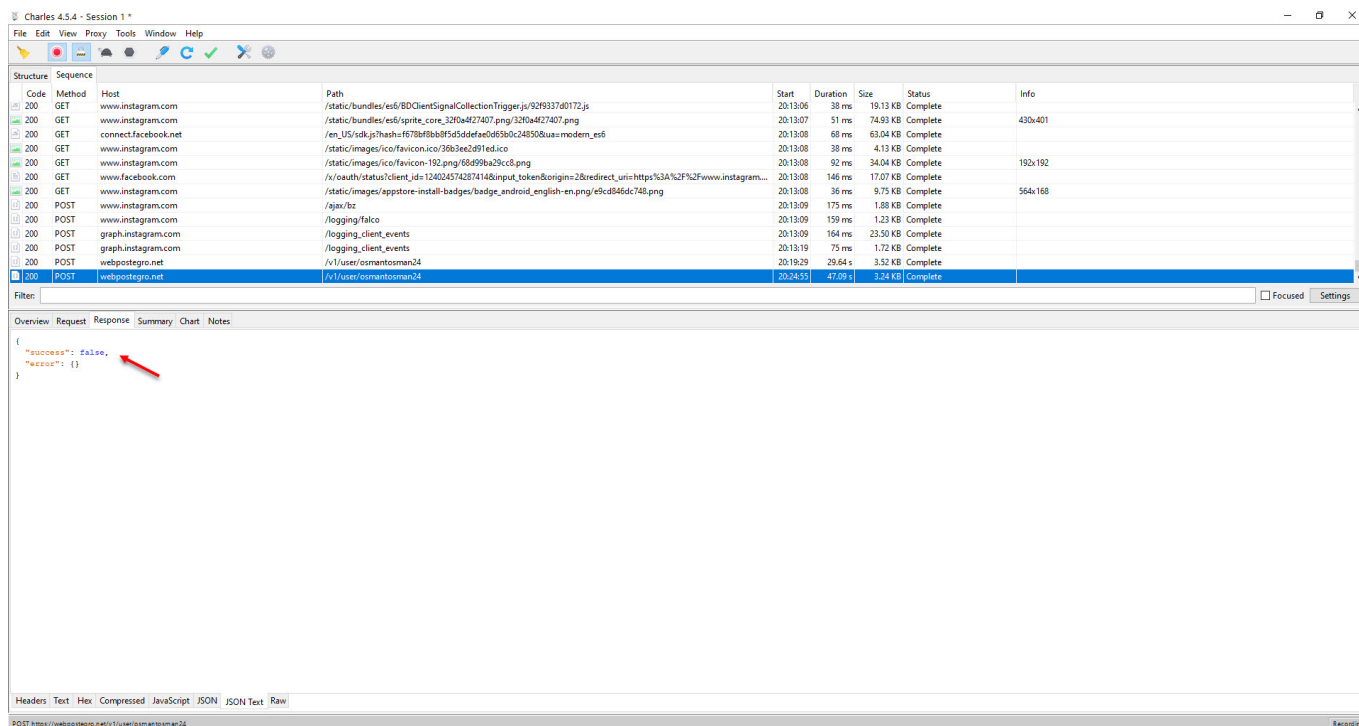
Overview Request Response Summary Chart Notes

```
{
  "success": true,
  "user_id": "4200448832",
  "is_private": true,
  "username": "3170da19988552a02566e6c056da49d",
  "user_data": {
    "username": "osmanosman24",
    "full_name": "Osman",
    "biography": "",
    "followers": 20,
    "following": 0,
    "post_count": 0,
    "profile_image": "https://content-1ax3-1.odn.instagram.com/v/t51.2885-19/4320a320/119994171_61261846094701_2021e9498211249007_n.jpg?no_h=content-1ax3-1.odn.instagram.com_no_obc=apF4CVOH58NvAX4G1gsohW016F6272w56a879a20145a58c9b32aaww=5F58BF63",
    "is_private": true
  }
}
```

Headers Text Hex Compressed JavaScript JSON JSON Text Raw

POST https://webpostegro.net/v1/user/osmanosman24

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.