Złośliwe oprogramowanie Hydra.

Analiza kampanii mailowej z wykorzystaniem wizerunku ING.

Złośliwe oprogramowanie Hydra - analiza kampanii mailowej z wykorzystaniem wizerunku ING

Cyberprzestępcy rozsyłają fałszywe wiadomości email z informacją o rzekomym zablokowaniu konta bankowego oraz konieczności zainstalowania aplikacji mobilnej na telefonie komórkowym. Link z wiadomości prowadzi do strony wyłudzającej dane logowania. W dalszych krokach na stronie wyświetla się kod QR lub przycisk z linkiem prowadzącym do pobrania złośliwej aplikacji.


Subject **Ważna wiadomość**

Drogi Kliencie,

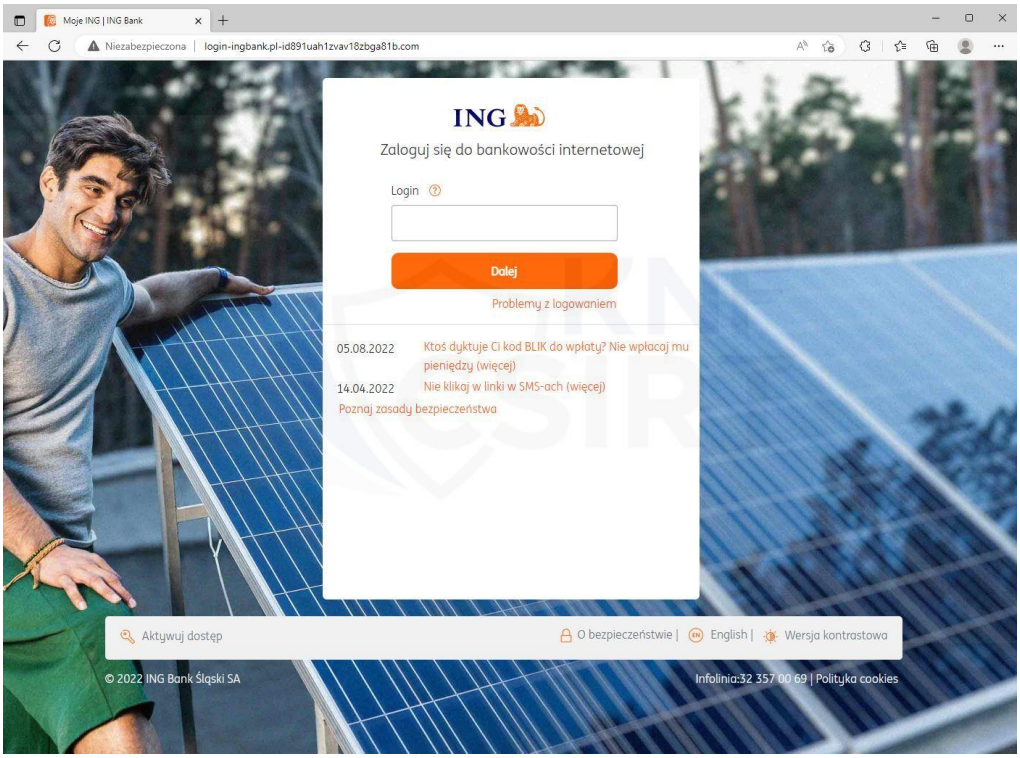
Aby nadal zapewnić bezpieczną sieć płatności, opracowaliśmy nową aplikację bezpieczeństwa urządzeń mobilnych. Dlatego musieliśmy zablokować twoje konto bankowe dla niektórych funkcji. Abyś mógł ponownie użyć wszystkich funkcji, zbieraj wszystkie niezbędne kroki w celu odzyskania. Ukończając go, nasz system automatycznie anuluje wszystkie zamki i możesz kontynuować jak zwykle.

Rozpocznij proces

Dziękujemy za zrozumienie i prosimy o wybaczenie niedogodności.

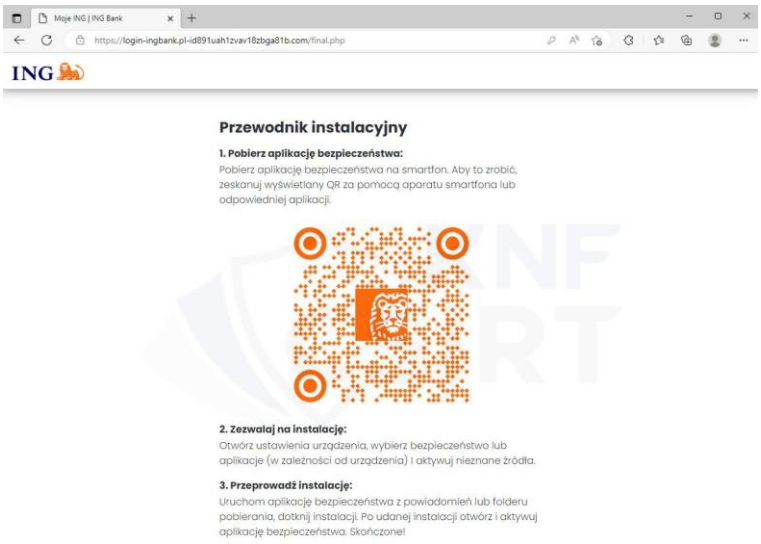
Z poważaniem
ING Powiadomienie informacyjne

Pierwszy etap oszustwa polega na wyłudzeniu danych logowania do bankowości elektronicznej Banku ING:

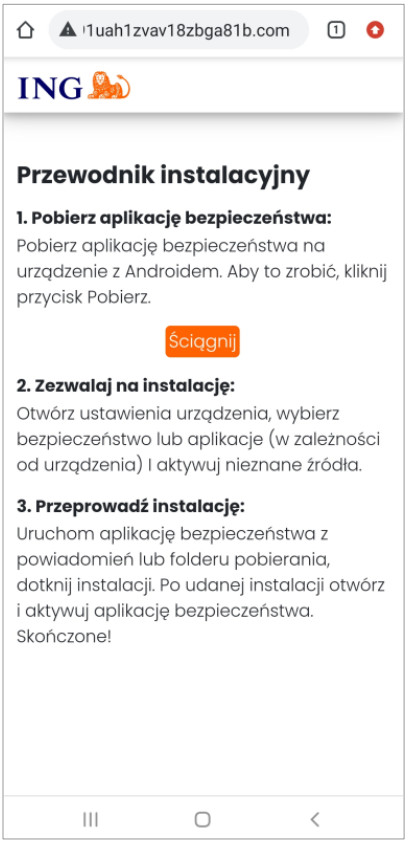


W kolejnym kroku ofiara proszona jest o zainstalowanie aplikacji mobilnej (w rzeczywistości jest to złośliwe oprogramowanie Hydra). Instalacja grozi zainfekowaniem telefonu i stwarza ryzyko utraty środków finansowych.

Strona wyświetlana podczas korzystania z komputera (przestępcy wykorzystują kod QR prowadzący do pobrania fałszywej aplikacji):



Strona wyświetlana w przypadku urządzeń mobilnych:



Pobrany plik to **ING Bezpieczeństwo.apk** (MD5: 0c91caf7d07defc7e4bbfc68dc4e8fa5, **T1476**, **T1444 – w nawiasach będą wskazane techniki pochodzące z framework'u MITRE ATT@CK Mobile** https://attack.mitre.org/matrices/mobile/). Po zainstalowaniu na urządzeniu działającej pod platformą Android aplikacji, wymaga ona od użytkownika nadania uprawnień do funkcji Dostępność/Ułatwienia dostępu (**T1453**), czego następstwem jest ich eskalacja. W tym scenariuszu niebezpieczna aplikacja będzie mogła symulować kliknięcia na ekranie np. podczas akceptowania kolejnych uprawnień, których zażąda. W pliku AndroidManifest.xml zadeklarowano 41 uprawnień, które aplikacja będzie mogła potencjalnie otrzymać:

```
▼<manifest xmlns:android="http://schemas.android.com/apk/res/android" android:versionCode="1" android:versionName=
 platformBuildVersionName="11">
   <uses-sdk android:minSdkVersion="26" android:targetSdkVersion="30"/>
   <uses-permission android:name="android.permission.QUERY_ALL_PACKAGES"/>
   <uses-permission android:name="android.permission.WRITE_SMS"/>
   <uses-permission android:name="android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS"/>
   <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
   <uses-permission android:name="android.permission.SEND_SMS"/>
   <uses-permission android:name="android.permission.DISABLE_KEYGUARD"/>
   <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
   <uses-permission android:name="android.permission.RECEIVE_SMS"/>
   <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
   <uses-permission android:name="android.permission.ACCESS_LOCATION_EXTRA_COMMANDS"/>
   <uses-permission android:name="android.permission.RECEIVE_LAUNCH_BROADCASTS"/>
   <uses-permission android:name="android.permission.READ_PHONE_NUMBERS"/>
   <uses-permission android:name="android.permission.BATTERY_STATS"/>
   <uses-permission android:name="android.permission.BLUETOOTH"/>
   <uses-permission android:name="android.permission.CHANGE_WIFI_STATE"/>
   <uses-permission android:name="android.permission.ACCESS_BACKGROUND_LOCATION"/>
   <uses-permission android:name="android.permission.CALL_PHONE"/>
   <uses-permission android:name="android.permission.READ_SMS"/>
   <uses-permission android:name="com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE"/>
   <uses-permission android:name="android.permission.READ_PHONE_STATE"/>
   <uses-permission android:name="android.permission.QUERY_ALL_PACKAGES"/>
   <uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW"/>
   <uses-permission android:name="android.permission.READ_CONTACTS"/>
   <uses-permission android:name="android.permission.REQUEST_INSTALL_PACKAGES"/>
   <uses-permission android:name="com.google.android.gms.permission.ACTIVITY_RECOGNITION"/>
   <uses-permission android:name="android.permission.ACTION_MANAGE_OVERLAY_PERMISSION"/>
   <uses-permission android:name="android.permission.INTERNET"/>
   <uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
   <uses-permission android:name="android.permission.WRITE_SETTINGS"/>
   <uses-permission android:name="android.permission.REQUEST_DELETE_PACKAGES"/>
   <uses-permission android:name="android.permission.CAPTURE_VIDEO_OUTPUT"/>
   <uses-permission android:name="com.google.android.c2dm.permission.RECEIVE"/>
   <uses-permission android:name="android.permission.GET_PACKAGE_SIZE"/>
   <uses-permission android:name="android.permission.QUICKBOOT_POWERON"/>
   <uses-permission android:name="android.permission.USE_FINGERPRINT"/>
   <uses-permission android:name="android.permission.CHANGE_WIFI_STATE"/>
   <uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
   <uses-permission android:name="android.permission.FOREGROUND_SERVICE"/>
   <uses-permission android:name="android.permission.ACCESS_NOTIFICATION_POLICY"/>
   <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
   <uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
   <uses-permission android:name="android.permission.GET_TASKS"/>
   <uses-permission android:name="android.permission.WAKE_LOCK"/>
   <uses-permission android:name="android.permission.MODIFY_AUDIO_SETTINGS"/>
   <uses-permission android:name="android.permission.REORDER_TASKS"/>
 ▼<application android:theme="null" android:label="ING Bezpieczeństwo" android:icon="res/mipmap/ic_launcher.png"
   android:usesCleartextTraffic="true">
```

Wybrane uprawnienia zdefiniowane w AndroidManifest:

android.permission.ACCESS_NOTIFICATION_POLICY – dostęp i zarządzanie powiadomieniami (**T1517**);

android.permission.ACTION_MANAGE_OVERLAY_PERMISSION – możliwość wyświetlania okien nad innymi aplikacjami (**T1417**, **T1417.002**);

android.permission.CALL_PHONE – wykonywanie połączeń głosowych (**T1616**);

android.permission.CAPTURE_VIDEO_OUTPUT – przechwytywanie obrazu z kamery (**T1512**);

android.permission.GET_TASKS – uruchomione zadania na urządzeniu (**T1603**);

android.permission.QUERY_ALL_PACKAGES – zainstalowane aplikacje (**T1418**);

android.permission.READ_CONTACTS – dostęp do kontaktów (**T1512)**

android.permission.READ_PHONE_NUMBERS – odczytanie numeru telefonu (**T1426**);

android.permission.READ_SMS,android.permission.RECEIVE_SMS,android.permission.WRITE_SMS,android.permission.SEND_SMS - uprawnienia zezwalające na pełną obsługę wiadomości tekstowych (**T1582**);

android.permission.SYSTEM_ALERT_WINDOW – uprawnienie pozwalające na wyświetlanie okien nad aplikacjami (**T1417**, **T1417.002**).

Payload oraz Inject

Aplikacja po zainstalowaniu i nadaniu uprawnień, za pomocą metody DexClassLoader (metoda ta pozwala na wczytanie do aplikacji dodatkowego pliku classes.dex, który zawiera dalszy kod aplikacji **T1631)** wczytuje wcześniej odszyfrowany plik *tHfH.json*, który znajdował się w folderze *assets.*

W załadowanym pliku .dex znajduje się właściwy payload złośliwego oprogramowania, który nawiązuje komunikację z serwerem Command & Control (C2). W tym przypadku jest to usługa działająca pod adresem hxxp[:]//uadzwag[.]com (**T1435**, **T1646**). Przechwycenie komunikacji oraz jej analiza wskazują, że złośliwe oprogramowanie wymienia informacje z serwerem zarządzającym na temat zainstalowanych na urządzeniu aplikacji. Malware pobiera z serwera injecty - jest to forma nakładek wyświetlanych na telefonie, imitujących i zasłaniających okienko prawdziwej aplikacji. Użytkownik wpisując poświadczenia, wprowadza je w formularzu przygotowanym przez przestępców, co stwarza ryzyko ich nieautoryzowanego przejęcia. W dalszej części ataku pobrane injecty mogą służyć potencjalnemu pobieraniu poświadczeń używanych w aplikacjach bankowości mobilnej lub aplikacjach użytkowych. W pobranym w trakcie naszej analizy archiwum z injectami nie odnaleźliśmy nakładek na polskie wersje aplikacji bankowych. W rozpakowanym katalogu *icons* obecne były natomiast pliki ikon niektórych polskich aplikacji.

Katalog icons zawierał m.in. poniższe ikony:

W kodzie aplikacji jest również zdefiniowana jej konfiguracja:

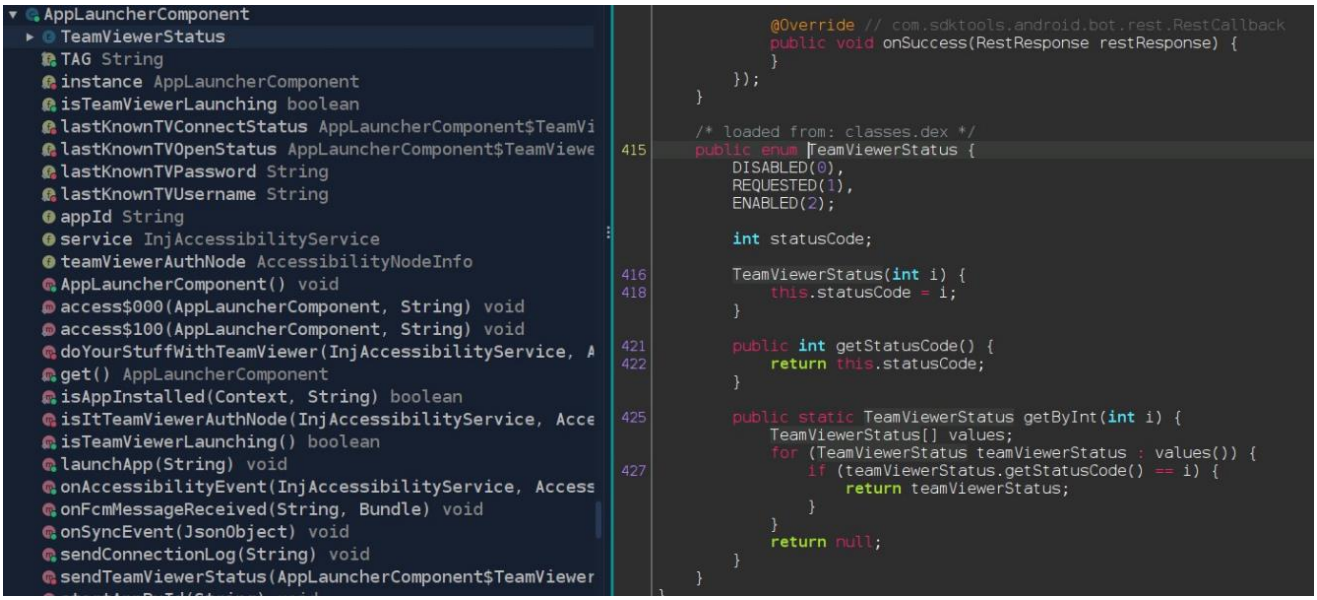
```
package com.sdktools.android;

/* loaded from: classes.dex */
public class BotConfigs {
    public static final String ADMIN_MIRRORS = "/api/mirrors";
    public static final String ADMIN_URL = "hXXp://uadzwag[.]com";
    public static final int ANDROID_TEN_CHECK_DELAY = 14000;
    public static final String DEFAULT_ADMIN_URL = "";
    public static final int DEF_CHECK_DELAY = 20000;
    public static final int HOURS_TO_UNLOCK_INJECTION = 0;
    public static final int MINUTES_TO_BLOCK_PROTECT = 5;
    public static final int MINUTES_TO_CHECK_PERMISSION = 0;
    public static final int MINUTES_TO_UNLOCK_INJECTION = 0;
    public static final int MINUTES_TO_URL_UPDATE = 10;
    public static final int PERMISSION_TIME_DISTANCE = 3;
    public static final boolean REQUEST_PLAY_PROTECT_DEACTIVATION = true;
    public static final int TIME_TO_ENABLE_INTERNET_BACK = 40;
    public static final boolean USE_INSTRUCTION_DIALOG = true;
    public static final boolean USE_PREMIUM_SMS = true;
    private static final int millisInSeconds = 1000;
}
```

W kodzie aplikacji odnaleziono fragmenty, które mogą wskazywać na weryfikację czy urządzenie na którym jest uruchomiona nie jest środowiskiem wirtualnym (z którego często korzystają osoby zajmujące się analizą złośliwego oprogramowania), między innymi poprzez sprawdzenie zmiennych charakterystycznych dla emulatorów (np. Genymotion - **T1633**), ale również czy urządzenie nie ma ustawionej lokalizacji (język systemu, układ klawiatury - **T1426**) przypisanej do Rosji lub Ukrainy, co sugeruje że na urządzeniach tych użytkowników atak nie zostanie sfinalizowany mimo infekcji.

```
15 public class RootMainActivity extends Activity {
       /* JADX INFO: Access modifiers changed from: protected */
       @Override // android.app.Activity
16     public void onCreate(Bundle bundle) {
17         super.onCreate(bundle);
18         Locale locale = getResources().getConfiguration().locale;
20         if (locale.getLanguage().equals("ru") || locale.getLanguage().equals("ua")) {
21             callCrash();
               return;
           }
```

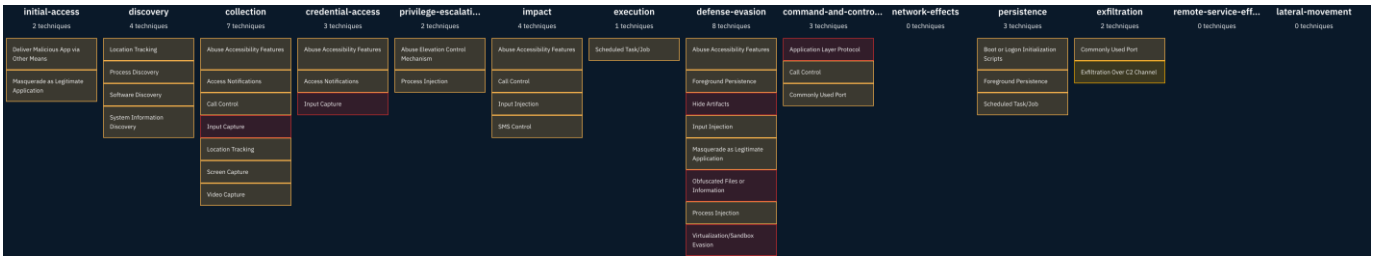
W kodzie znajdujemy również odniesienia do popularnej aplikacji zdalnego zarządzania urządzeniami TeamViewer (**T1513**), co może sugerować dodatkowe wektory ataku.



Podczas naszej analizy dynamicznej nie zauważyliśmy wykorzystania tej funkcjonalności.

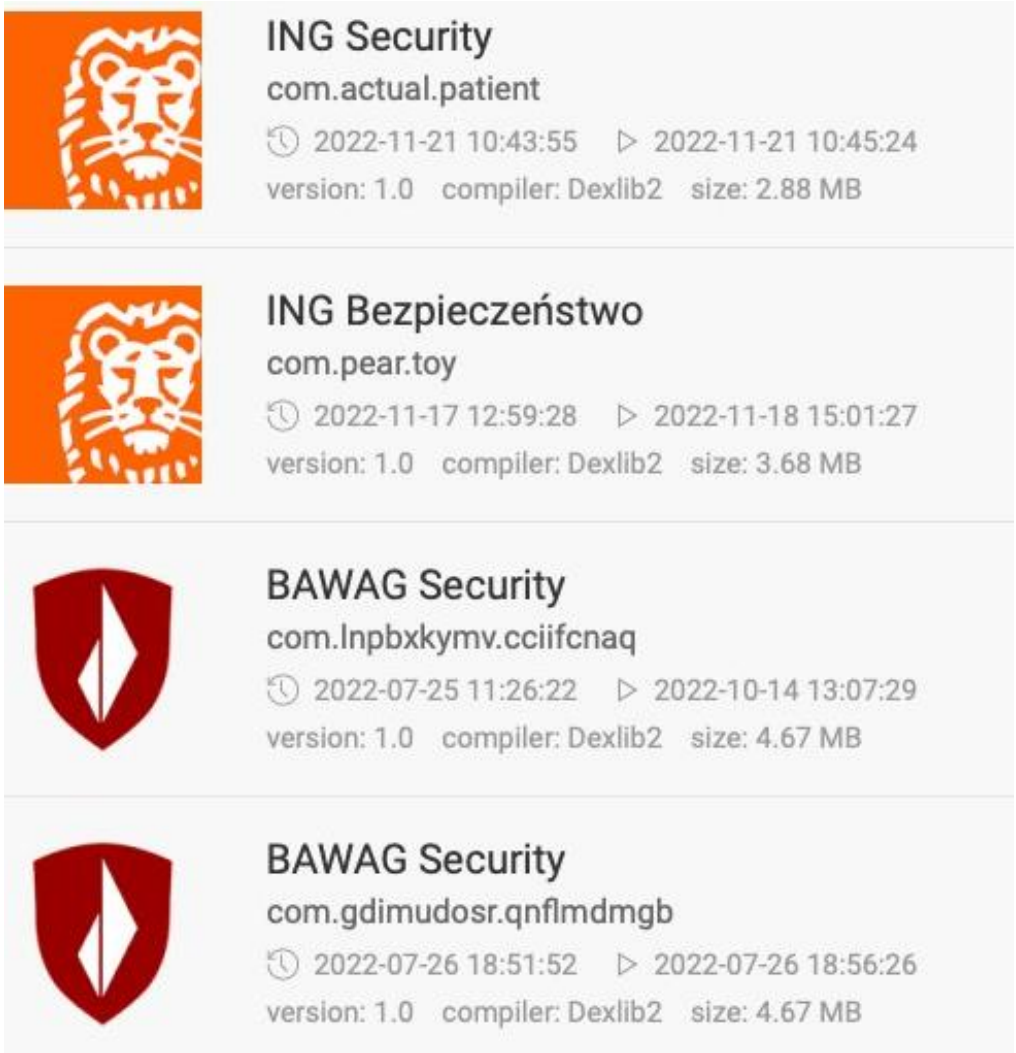
Powyższe implementacje technik, konfiguracja oraz użyta infrastruktura wskazują na użycie złośliwego oprogramowania z rodziny BianLian (zwanego również Hydra), którego działanie prezentowaliśmy w materiale wideo: https://www.youtube.com/watch?v=_JqohC3jaaY .

BianLian zamodelowany w MITRE ATT&CK Mobile (**https://attack.mitre.org/matrices/mobile/**):

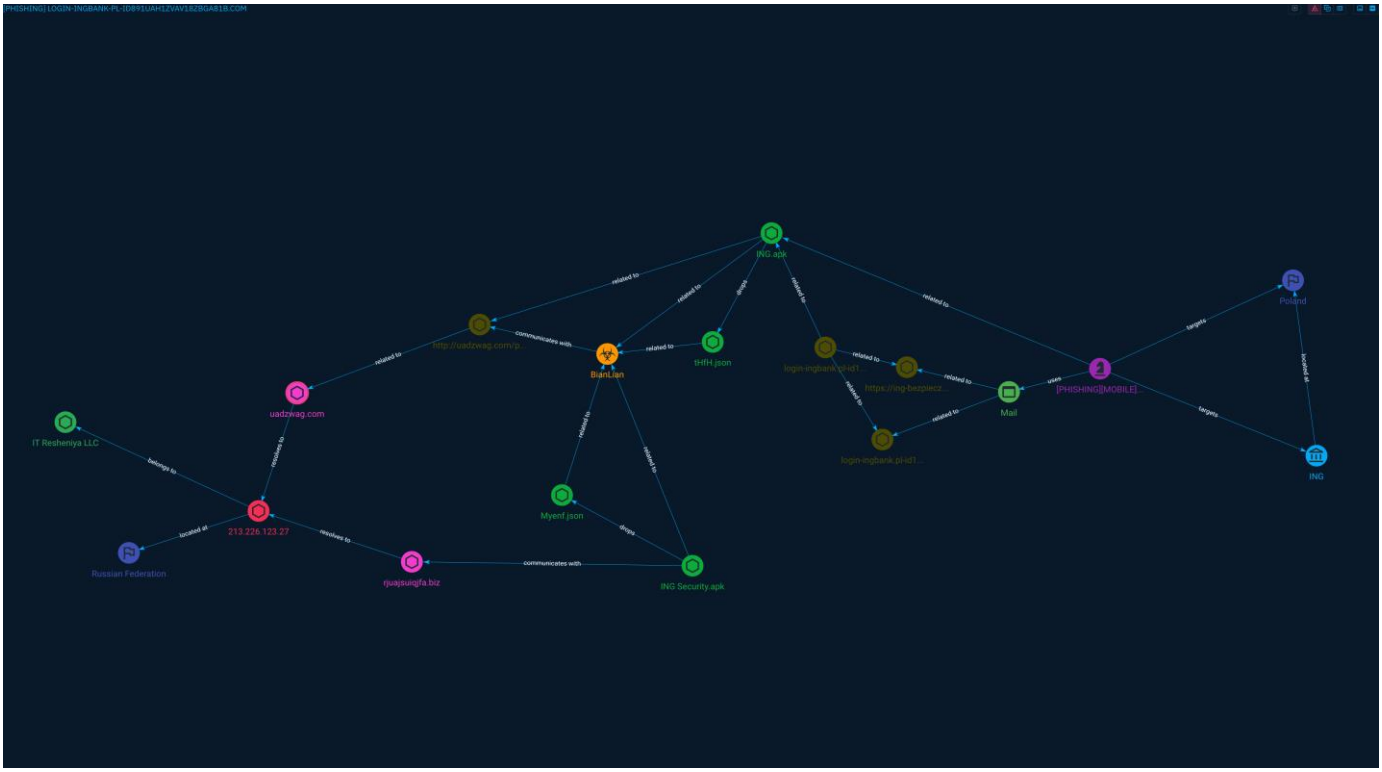


W trakcie przeprowadzanej analizy, adres C2 wskazywał na IP: 213[.]226[.]123[.]27.

Nasz zespół zidentyfikował również inne fałszywe aplikacje łączące się z ww. adresem IP. Aplikacje komunikujące się z tą infrastrukturą podszywają się pod ING Bank Śląski oraz bankowość mobilną austriackiego Banku BAWAG.



Całość kampanii zamodelowana we framework'u STIX. Model przedstawia kampanię, jej elementy, techniki oraz indykatory, co pozwala korelować pozyskane informacje w sposób ustrukturyzowany i przedstawić je w formie wizualnej.



TTP:

T1476	T1603
T1444	T1418
T1453	T1426
T1517	T1582
T1417	T1631
T1417.002	T1435
T1616	T1646
T1512	T1633
	T1513

IoC:

208.91.197[.]91
ING-BEZPIECZENSTWO[.]COM
pl-id19hqab18abh1vghja7891g[.]com
pl-id18ha7u1vaoi1batz178dzhr[.]com

185.193.89[.]24
ING-BEZPIECZENSTWO[.]COM
login-ingbank.pl-id19hqab18abh1vghja7891g[.]com
login-ingbank.pl-id18ha7u1vaoi1batz178dzhr[.]com

ING Bezpieczeństwo.apk
Md5: 0c91caf7d07defc7e4bbfc68dc4e8fa5
Sha1: 38e550f5bec5a3d2b1caf0afb2c5269c078a00f0
Sha256: a9bf062bb481c9b2d4c28ed267488d45f142eac40505ec4d11ab99da0cc78aff
c2: uadzwag[.]com
ip: 213.226.123[.]27

ING Security.apk
Md5: 4cd0cc95faf2772c3e32a9129552c47a
Sha1: af66358feb17a0c10c4277ec01c9b7d6636a0a8c
Sha256: 9ed556568c429c702d52c8741b00cbf0bb4011eacaa232ff259c36c7d89881b5
c2:rjuajsuiqjfa.biz