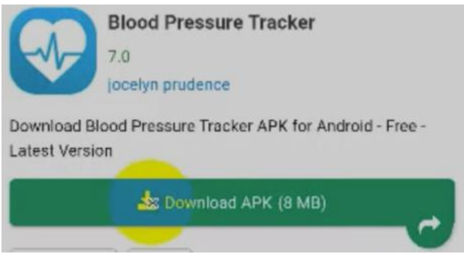
MCP MOBILE MALWARE UPDATE
App Malware Reads Notifications Blood Pressure Tracker App

As a leading mobile compliance and fraud specialist company, MCP Insight continually tests and validates potential issues coming from websites or malicious applications.

Our objective in this document is to reflect on a recent discovery of a malicious application called “Blood Pressure Tracker App”.



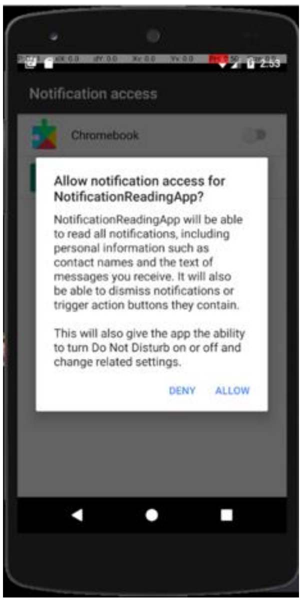
Blood Pressure Tracker
7.0
jocelyn prudence

Download Blood Pressure Tracker APK for Android - Free - Latest Version

The malicious nature of the application enables it to open an offer on a website within the app, complete the offer and finally validate the paid for subscription. The unique element highlighted in this discovery relates to the malicious application’s ability to control the mobile phone by directly using the ‘notification receiver’, even before the notification message shows up in the notification area on mobile phone.

App Security

Android Malware is not a new phenomenon but the degree to which criminals manipulate applications is a constant evolving battle. Newer versions of Android security have increased the complexity for malicious applications to act on certain vulnerabilities within the android environment, as well as Google-Play-Protect. App platforms operate sophisticated security systems to combat Android Malware, but the cat and mouse game goes on, with an ongoing mission to eliminate malware from the ecosystem as new applications are published on the Play-Store and Non-Play-Store sites daily.



Notification access

Chromebook

Allow notification access for NotificationReadingApp?

NotificationReadingApp will be able to read all notifications, including personal information such as contact names and the text of messages you receive. It will also be able to dismiss notifications or trigger action buttons they contain.

This will also give the app the ability to turn Do Not Disturb on or off and change related settings.

App Permissions

Newer Android security features request specific permissions or user consent on the device as a safety feature. One of the most common user consent requests for android applications is, “Notification Access” under Android System Settings.

The Notification Access can be manipulated by fraudsters by forcing the permission or consent requirement regarding legal, regulatory or for the application to function correctly. Users generally disregard this consent or are led to believe that this is important for the application to perform.

MCP Insight – App Test Process

To support our understanding of particular fraudulent applications, MCP search and install suspect apps from the Google Play-Store and Non-Play-Store sites on a daily basis for in-depth analysis.

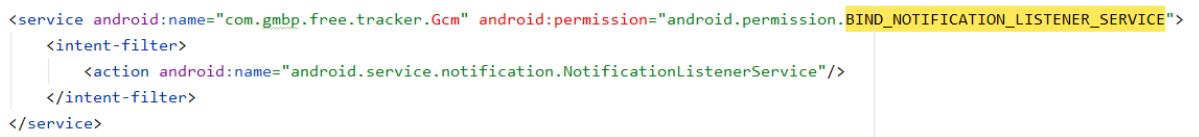
MCP first detected this malicious Blood Pressure Tracker App in our anti-fraud platform MCP Shield. Our platform determined that fraudulent activity was originating from the app and started blocking attempted transactions to our clients' services.

MCP identified that the Blood Pressure Tracker app was available on the Play-Store (before being taken down, based on our feedback to Google), so we downloaded it for observation.

Blood Pressure Tracker App – MCP Analysis

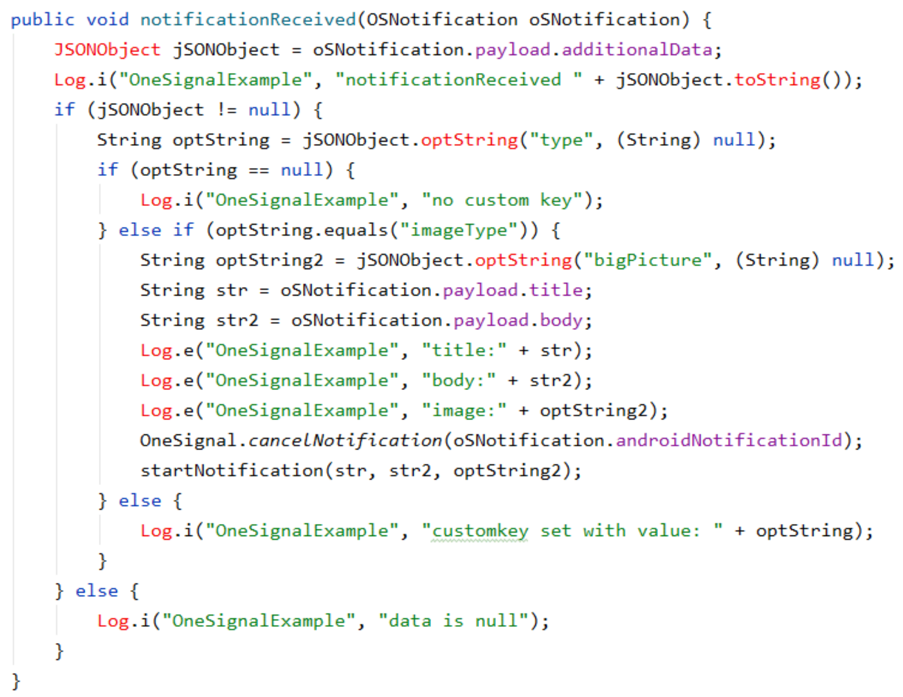
Upon installing the Blood Pressure Tracker app on the mobile phone, the application requires notification receiving and listening permission/consent from the user. This was 'allowed' and the phone we were using for the test was subscribed to 6 different services and a further 7 over the next 24hrs.

By analyzing the log information, we were able to establish that once notification access permission is granted, the application sets up a background service which continues to check for notification messages, ensuring that all notifications would be seen by the Blood Pressure Tracker app before the notification panel receives the notification (see snippet below).



```
<service android:name="com.gmbp.free.tracker.Gcm" android:permission="android.permission.BIND_NOTIFICATION_LISTENER_SERVICE">
    <intent-filter>
        <action android:name="android.service.notification.NotificationListenerService"/>
    </intent-filter>
</service>
```

The snippet below shows how the malicious application receives the notification.



```
public void notificationReceived(OSNotification oSNotification) {
    JSONObject jSONObject = oSNotification.payload.additionalData;
    Log.i("OneSignalExample", "notificationReceived " + jSONObject.toString());
    if (jSONObject != null) {
        String optString = jSONObject.optString("type", (String) null);
        if (optString == null) {
            Log.i("OneSignalExample", "no custom key");
        } else if (optString.equals("imageType")) {
            String optString2 = jSONObject.optString("bigPicture", (String) null);
            String str = oSNotification.payload.title;
            String str2 = oSNotification.payload.body;
            Log.e("OneSignalExample", "title:" + str);
            Log.e("OneSignalExample", "body:" + str2);
            Log.e("OneSignalExample", "image:" + optString2);
            OneSignal.cancelNotification(oSNotification.androidNotificationId);
            startNotification(str, str2, optString2);
        } else {
            Log.i("OneSignalExample", "customkey set with value: " + optString);
        }
    } else {
        Log.i("OneSignalExample", "data is null");
    }
}
```

In the snippet you can also see the notification being cancelled, so the user has no visibility of any interaction (see below extract).

```
OneSignal.cancelNotification(oSNotification.androidNotificationId);
```

The malware enables the application to extract data, read the pin code, suppress the notification message and use the PIN to complete the subscription element of a service.

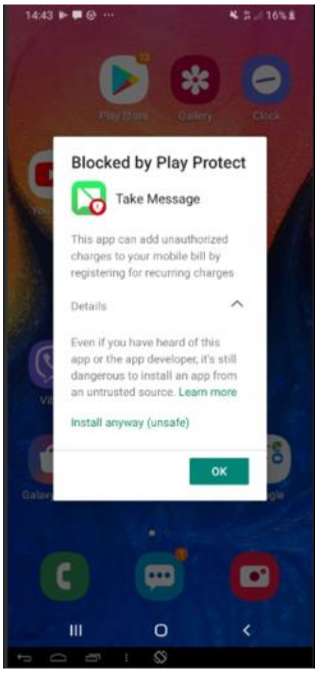
Consumer Harm

To the unassuming User, the app looks innocuous and offers a perceived value – in this case the ability to track blood pressure for 'free'. Often typical apps like this show 10,000 – 1,000,000+ downloads from the Play store. Our test shows the potential downside. Where malware is present, once downloaded and without the user's knowledge, the application opens an offer on a website within the application, requests to subscribe to the offer and finally validates the subscription by reading the pin that was sent to the device. The consumer is defrauded.

Security Partners

Once the app malware analysis has been conducted, MCP work with security partners (in this case Google) to share documented fraudulent activity, sharing knowledge and in order for the partner to take down the malicious app from the app store.

MCP understands the brand damage such fraud does to the mobile payments Industry and we will work with partners to ensure that fraud and the malicious operators perpetrating fraud, are shut down.



Blocked by Play Protect

Take Message

This app can add unauthorized charges to your mobile bill by registering for recurring charges

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

On Google Play, the Blood Pressure Tracker App can no longer be downloaded.

The Blood Pressure app can still be downloaded from certain non-Google third-party app stores, which emphasizes the value of consumers using approved app stores where security management is more robust. MCP work helps mitigate the impact of malicious activity, whilst also showing the importance of anti-fraud solutions and the role they play protecting business and consumers alike.