

No Joking Around with JOKER

Published: 2021-05-05 · Archived: 2026-04-05 19:37:33 UTC

The Joker malware family has been consistently targeting Android users since it was discovered in 2017 and is one of the most active malware families on the Google Play Store. It continues to find new tricks and tactics to stay undetected by doing small changes in its code or changing the payload download techniques.

The family name “Joker” was derived from the Command and Control (C2) domain name it used in its early days. This malware attempts to steal SMS messages, contacts from the victim’s device and silently signs up its victims to the premium services without their knowledge.

At K7 Labs, we recently noticed a new Joker malware sample on Google Play Store, which utilizes Android packers like “Tencent’s Legu” and “ijiami” packers to evade detection.

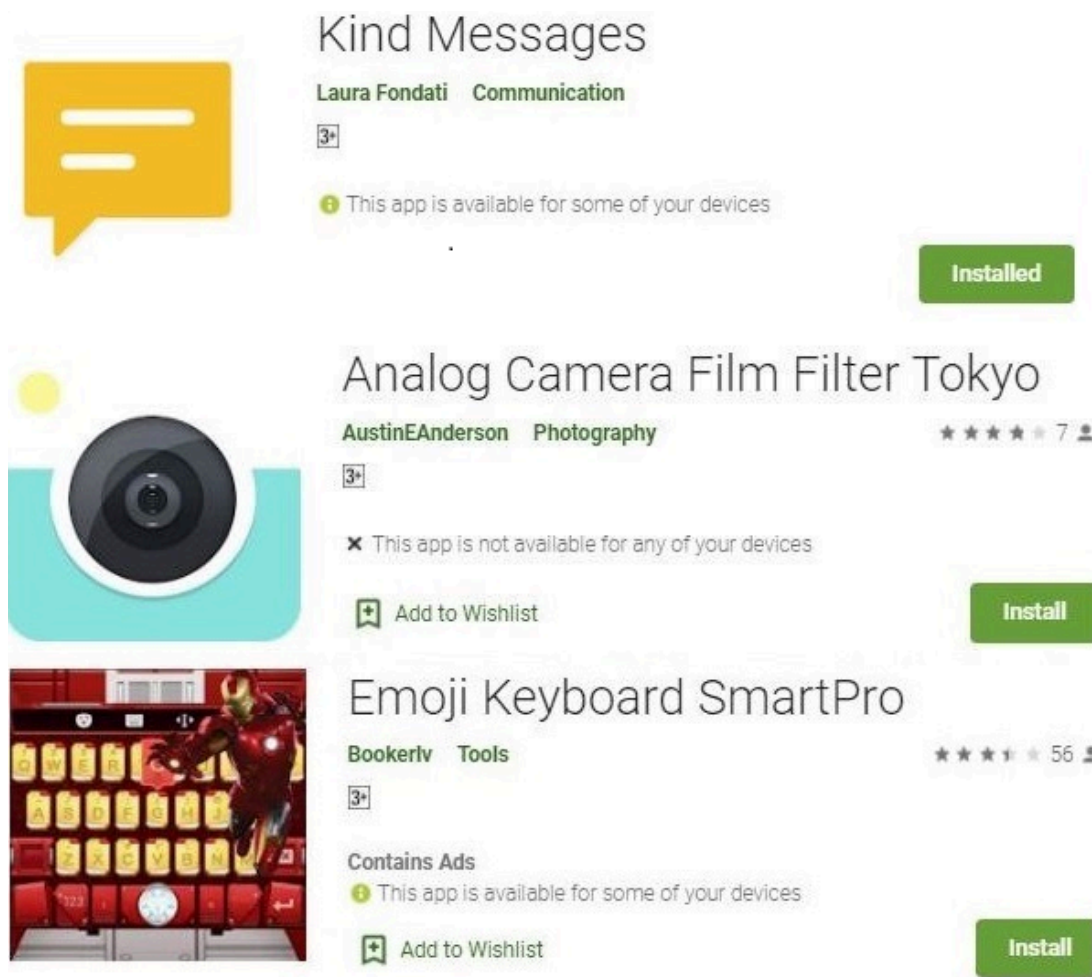
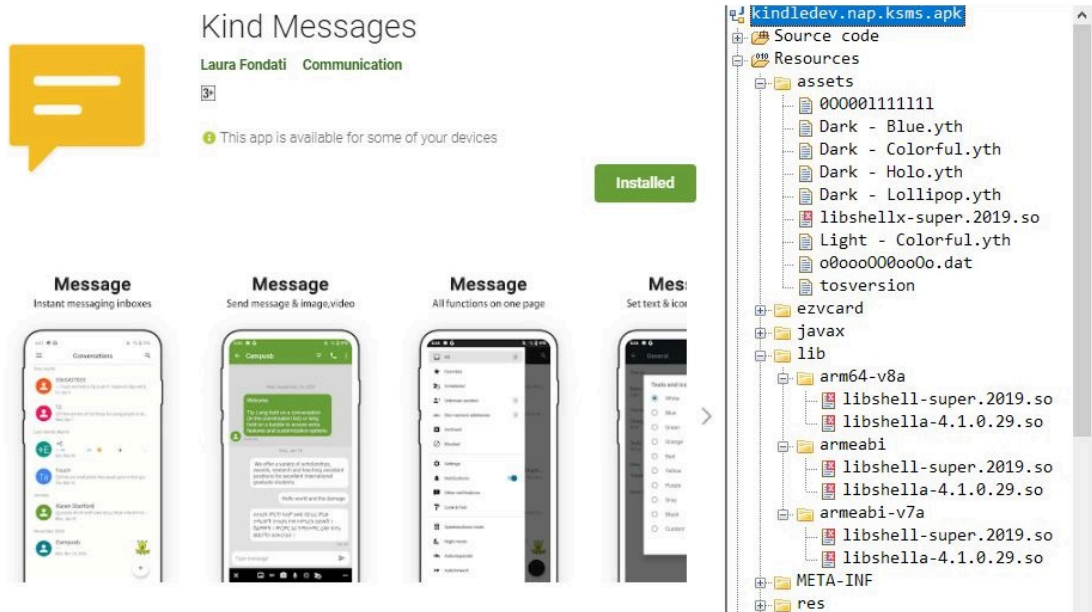


Figure 1: Malicious Joker Apps from Google Play Store Protected with Packer

In this blog, we will be analyzing the sample **kindledev.nap.ksms** which uses Tencent’s Legu Packer to hide its malicious payload functionality as shown in Figure 2.



Provides powerful short message (SMS&MMS) function. Keep in touch with friends, share photos to them, send audio, emojis and stickers. Personalize the screen and chat bubbles with custom colors and fonts.

Figure 2: APK Protected with Tencent's Legu Packer

Technical Analysis

Once launched, at runtime it unpacks the malicious Android Package (APK) and contacts the C2 server to download a malicious Dalvik Executable (DEX) file payload as shown in Figure 3, which enables the malware and adds other capabilities.

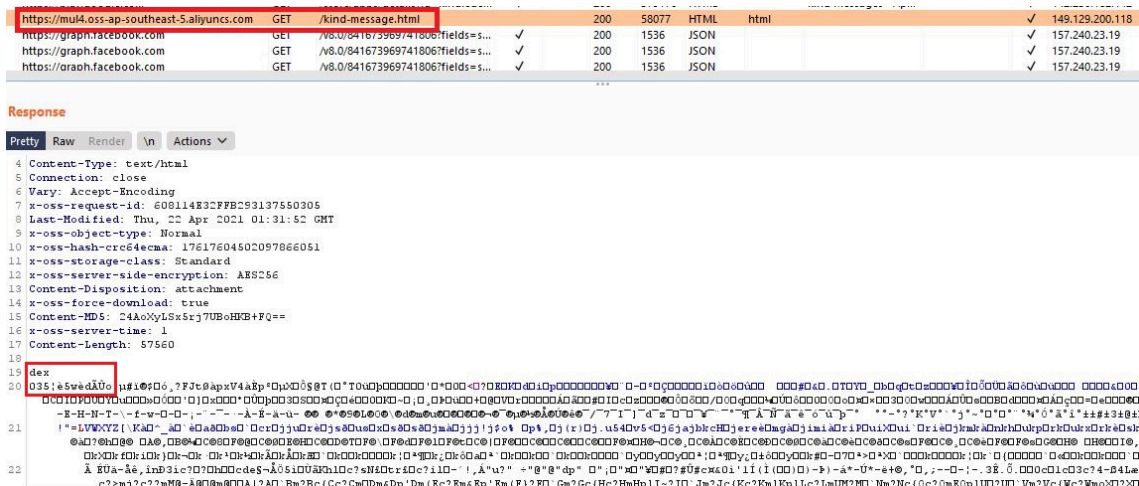


Figure 3: Malicious Payload from C2 Server

This malicious payload continuously sends POST requests to **hxxp[://161].[117].[146].[164]/svhyqj/mjcxzy** for communication as shown in Figure 4.

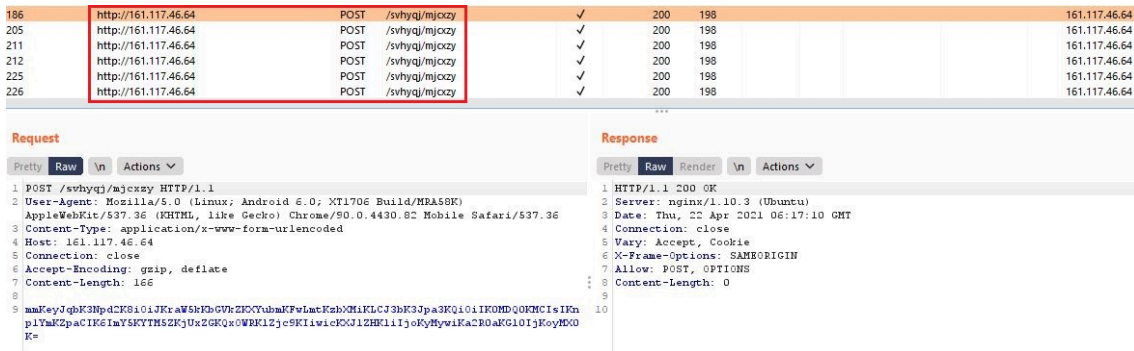


Figure 4: Encrypted Data sent to C2 in POST

This Joker Trojan attempts to intercept SMS messages notifications as shown in Figure 5.

```

public static boolean b(Context paramContext)
{
    boolean bool = false;
    String str = Settings.Secure.getString(paramContext.getContentResolver(), "a.v");
    if ((str != null) && (str.contains(paramContext.getPackageName())))
    {
        j = 1;
        if (j == 0) {
            if (paramContext.getPackageManager().checkPermission("android.permission.RECEIVE_SMS", paramContext.getPackageName()) != 0) {
                break label66;
            }
        }
    }
    label66:
    for (int j = 1; j = 0)
    {
        if (j != 0) {
            bool = true;
        }
        return bool;
        j = 0;
        break;
    }
}

public static boolean c(String paramString)
{
    String str = "sendSms:" + paramString;
    Log.e("a.g", str);
    try
    {
        paramString = paramString.split("a.d");
        SmsManager.getDefault().sendTextMessage(paramString[0], null, paramString[1], null, null);
        bool = true;
    }
    catch (Exception paramString)
}
    
```

Figure 5: Intercept SMS Messages

This Trojan also silently signs up the victim for the WAP (Wireless Application Protocol) fraud as shown in Figure 6.

)
cc.lask.as	b3a7042186cb7957726b468bc1024d6b	Tencent's Legu	Trojan (0001140e1)
inksms.beatmessages.messaging	ac2f1708ba265b2152aed0c43b7be2ea	Tencent's Legu	Trojan (0001140e1)
com.translate2021.forall.language	bf84acfd727c8aead7f81d73fc41082	Tencent's Legu	Trojan (0001140e1)
com.multicamera.coolwending.translator	fcc657d5e61d53ceff6943e7263f8d3	Tencent's Legu	Trojan (0001140e1)
com.alltxt.translate.photo.convert	8668549e97b60bfccfb4082f2bb9fc62	Tencent's Legu	Trojan (0001140e1)
com.sophisticated.gifmakermax	c5eb32e4ff466702fd95429b8a367686	Tencent's Legu	Trojan (0001140e1)
everysearch.artifact	f9b089e22514f1824a0e0c0bee4248ce	Tencent's Legu	Trojan (0001140e1)
com.kong.toouch.ass.iphoea	0f9f4d088a69659a4791ef5d883c0487	ijiami	Trojan (0057931a1)
livepictures.livebackground.lightningwallpaper	652d67cfb68278306e22545c551ac64d	Tencent's Legu	Trojan (0001140e1)
com.camscanner.docscanner.multidocscanner	8cb23726b1438e734ba3708995ae36c2	Tencent's Legu	Trojan (0001140e1)
cplus.mirzatext.translateapp	33b6a1a6d1d31a63c33666ba6a8be8d3	Tencent's Legu	Trojan (0001140e1)
com.freecollger.make.photocollage	f53560912c64f236bbd71995204b4962	Tencent's Legu	Trojan (0001140e1)

com.wandaretech.flashinterpreter	d595f2c5b39728269a531bd018740484	Tencent's Legu	Trojan (00579d201)
----------------------------------	----------------------------------	----------------	--------------------

Payload URLs

- mul4[.oss-ap-southeast-5.aliyuncs[.com
- hwayt[.oss-us-east-1.aliyuncs[.com
- wansgo[.oss-ap-southeast-5.aliyuncs[.com
- selct[.oss-ap-southeast-2.aliyuncs[.com
- scanlucky[.oss-us-east-1.aliyuncs[.com
- banca[.oss-us-east-1.aliyuncs[.com
- biggerone[.oss-us-east-1.aliyuncs[.com
- lucky-bird[.oss-me-east-1.aliyuncs[.com
- linchen-bucket[.oss-us-east-1.aliyuncs[.com
- breezea[.oss-us-east-1.aliyuncs[.com
- fronta[.oss-us-west-1.aliyuncs[.com
- warriorss[.oss-us-west-1.aliyuncs[.com

Final C2 Servers

161[.117.226.98
161[.117.250.158
161[.117.62.127
161[.117.46.64

Source: <https://labs.k7computing.com/?p=22199>