Malicious code in APKPure app

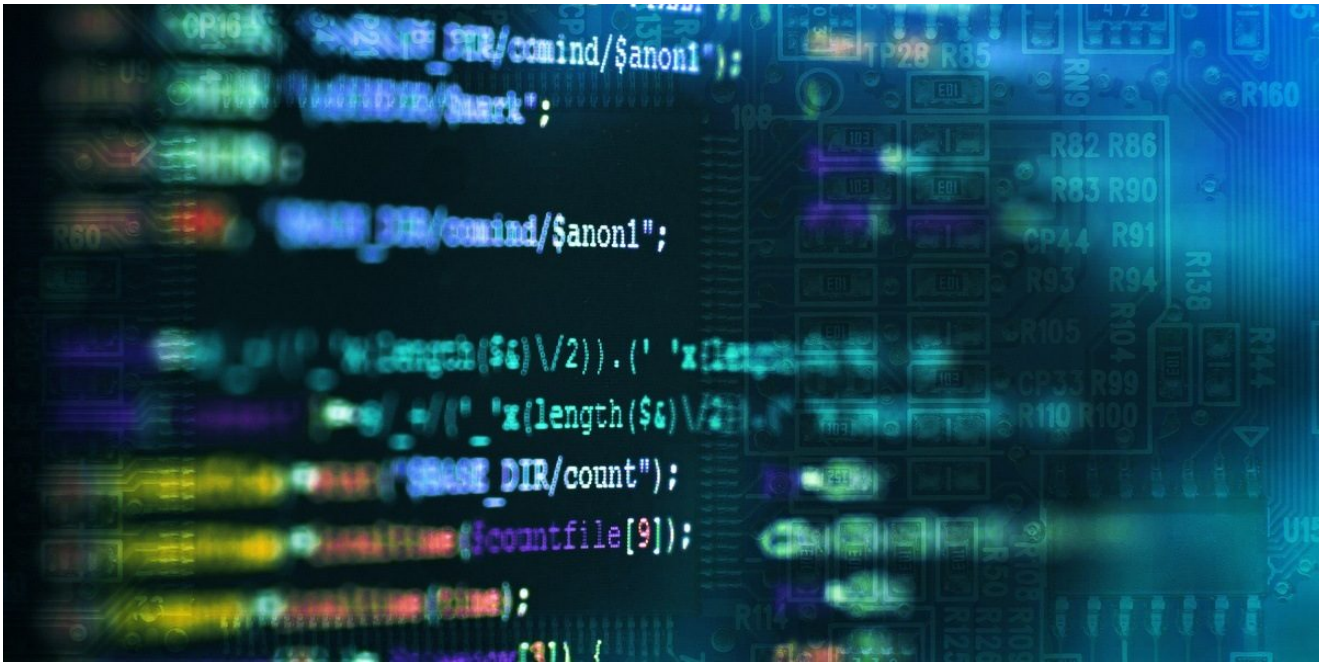
securelist.com/apkpure-android-app-store-infected/101845/

Incidents

Incidents

09 Apr 2021

minute read



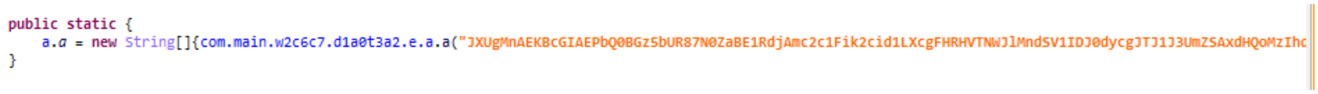
Authors

- Expert Igor Golovin
- Expert Anton Kivva

Recently, we’ve found malicious code in version 3.17.18 of the official client of the APKPure app store. The app is not on Google Play, but it is itself a quite a popular app store around the world. Most likely, its infection is a repeat of the CamScanner incident, when the developer implemented a new adware SDK from an unverified source.

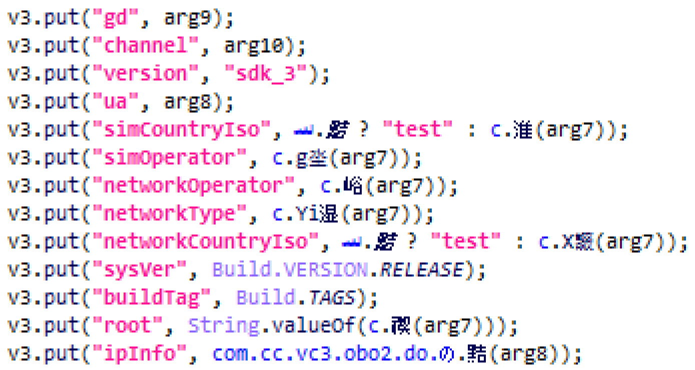
We notified the developers about the infection on April 8. APKPure confirmed the issue and promptly fixed it with the release of version 3.17.19.

In terms of functionality, the malicious code embedded in APKPure is standard for this type of threat. When the app starts, the payload is decrypted and launched. In this case, it is located in a long string in the app code.



```
public static {
    a.a = new String[]{com.main.w2c6c7.d1a0t3a2.e.a.a("JXUgMnAEKBcGIAEPbQ0BGz5bUR87N0ZaBE1RdjAmc2c1Fik2cid1LXcgFHRHVTNWJlMndSV1IDJ0dycgJTJ1J3UmZSAxdHQoMzIhc
}
```

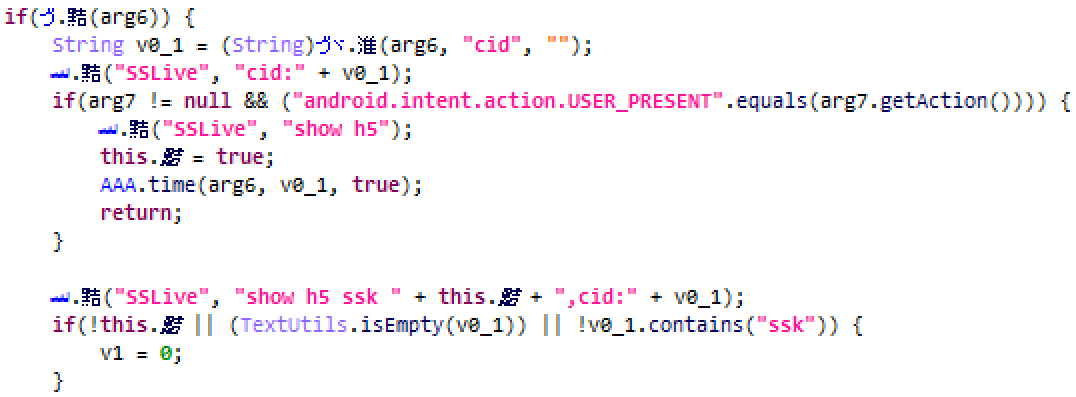
The payload collects information about the user device and sends it to the C&C server.



```
v3.put("gd", arg9);
v3.put("channel", arg10);
v3.put("version", "sdk_3");
v3.put("ua", arg8);
v3.put("simCountryIso", ↵.髫 ? "test" : c.淮(arg7));
v3.put("simOperator", c.g垩(arg7));
v3.put("networkOperator", c.峪(arg7));
v3.put("networkType", c.Yi湿(arg7));
v3.put("networkCountryIso", ↵.髫 ? "test" : c.X纇(arg7));
v3.put("sysVer", Build.VERSION.RELEASE);
v3.put("buildTag", Build.TAGS);
v3.put("root", String.valueOf(c.褉(arg7)));
v3.put("ipInfo", com.cc.vc3.obo2.do.の.黠(arg8));
```

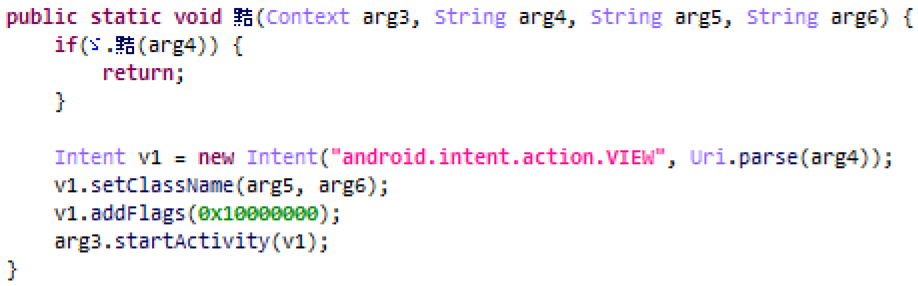
Next, depending on the response received, the malware can:

Show ads when the device is unlocked.



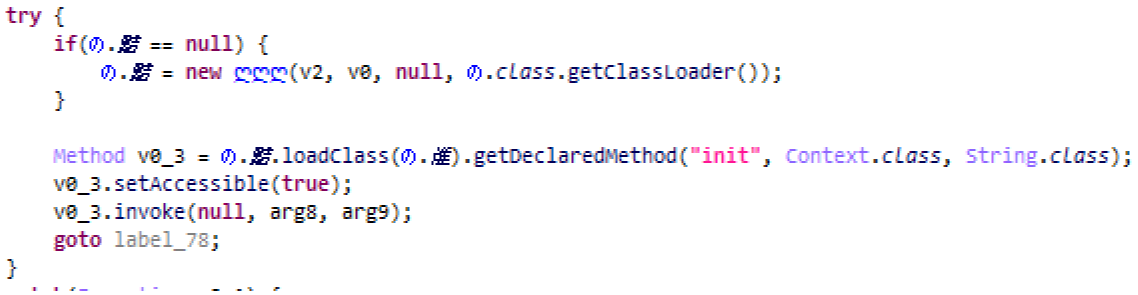
```
if(ゔ.黠(arg6)) {
    String v0_1 = (String)ゔヾ.淮(arg6, "cid", "");
    ↵.黠("SSLive", "cid:" + v0_1);
    if(arg7 != null && ("android.intent.action.USER_PRESENT".equals(arg7.getAction()))) {
        ↵.黠("SSLive", "show h5");
        this.髫 = true;
        AAA.time(arg6, v0_1, true);
        return;
    }

    ↵.黠("SSLive", "show h5 ssk " + this.髫 + ",cid:" + v0_1);
    if(!this.髫 || (TextUtils.isEmpty(v0_1)) || !v0_1.contains("ssk")) {
        v1 = 0;
    }
```

Open browser pages with ads repeatedly.



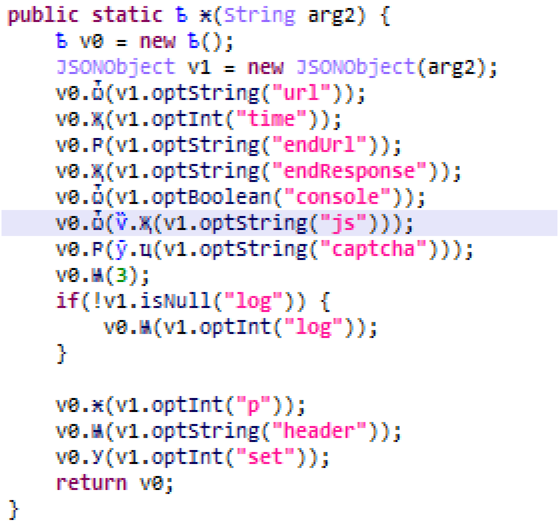
```
public static void 黠(Context arg3, String arg4, String arg5, String arg6) {
    if(ゞ.黠(arg4)) {
        return;
    }

    Intent v1 = new Intent("android.intent.action.VIEW", Uri.parse(arg4));
    v1.setClassName(arg5, arg6);
    v1.addFlags(0x10000000);
    arg3.startActivity(v1);
}
```

Load additional executable modules.

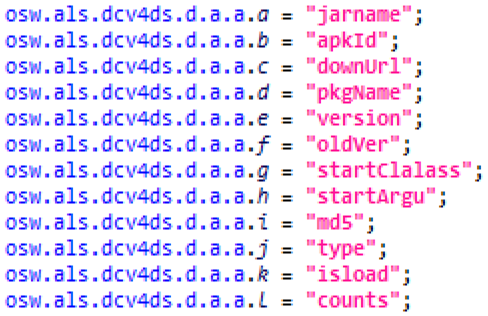


```
try {
    if(の.鬙 == null) {
        の.鬙 = new ღღღ(v2, v0, null, の.class.getClassLoader());
    }

    Method v0_3 = の.鬙.loadClass(の.雈).getDeclaredMethod("init", Context.class, String.class);
    v0_3.setAccessible(true);
    v0_3.invoke(null, arg8, arg9);
    goto label_78;
}
```

In our case, a Trojan was loaded that has much in common with the notorious Triada malware and can perform a range of actions: from displaying and clicking ads to signing up for paid subscriptions and downloading other malware.



```
public static ѣ ж(String arg2) {
    ѣ v0 = new ѣ();
    JSONObject v1 = new JSONObject(arg2);
    v0.ǒ(v1.optString("url"));
    v0.Җ(v1.optInt("time"));
    v0.Р(v1.optString("endUrl"));
    v0.Җ(v1.optString("endResponse"));
    v0.ǒ(v1.optBoolean("console"));
    v0.ǒ(ṽ.Җ(v1.optString("js")));
    v0.Р(ў.ц(v1.optString("captcha")));
    v0.Ӊ(3);
    if(!v1.isNull("log")) {
        v0.Ӊ(v1.optInt("log"));
    }

    v0.ж(v1.optInt("p"));
    v0.Ӊ(v1.optString("header"));
    v0.у(v1.optInt("set"));
    return v0;
}
```



```
osw.als.dcv4ds.d.a.a.a = "jarname";
osw.als.dcv4ds.d.a.a.b = "apkId";
osw.als.dcv4ds.d.a.a.c = "downUrl";
osw.als.dcv4ds.d.a.a.d = "pkgName";
osw.als.dcv4ds.d.a.a.e = "version";
osw.als.dcv4ds.d.a.a.f = "oldVer";
osw.als.dcv4ds.d.a.a.g = "startClalass";
osw.als.dcv4ds.d.a.a.h = "startArgu";
osw.als.dcv4ds.d.a.a.i = "md5";
osw.als.dcv4ds.d.a.a.j = "type";
osw.als.dcv4ds.d.a.a.k = "isload";
osw.als.dcv4ds.d.a.a.l = "counts";
```

Depending on the OS version, the Trojan can inflict various forms of damage on the victim. APKPure users with current Android versions mostly risk having paid subscriptions and intrusive ads appear from nowhere. Users of smartphones who do not receive security updates are less fortunate: in outdated versions of the OS, the malware is capable of not only loading additional apps, but installing them on the system partition. This can result in an unremovable Trojan like xHelper getting onto the device.

Kaspersky solutions detect the malicious implant as HEUR:Trojan-Dropper.AndroidOS.Triada.ap.

If you use APKPure, we recommend immediately deleting the infected app and installing the "clean" 3.17.19 version. In addition, scan the system for other Trojans using a reliable security solution, such as Kaspersky Internet Security for Android.

IOCs

APKPure app
2cfaedcf879c62f5a50b42cbb0a7a499
718aecd85e9f1219f3fc05ef156d3acf
ceac990b3df466c0d23e0b7f588d1407
deac06ab75be80339c034e266dddbc9f
f64d43c64b8a39313409db2c846b3ee9

Payload
31e49ac1902b415e6716bc3fb048f381

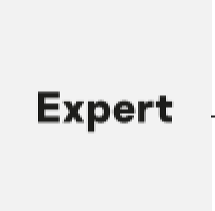
Downloaded malware
5f9085a5e5e17cb1f6e387a901e765cf

C&C
https://wcf.seven1029[.]com
http://foodin[.]site/UploadFiles/20210406052812.apk

- Code injection
- Google Android
- Malware Technologies
- Trojan

Authors

-

Igor Golovin
- 

Anton Kivva

Malicious code in APKPure app

Your email address will not be published. Required fields are marked *

GReAT webinars

13 May 2021, 1:00pm

GReAT Ideas. Balalaika Edition

26 Feb 2021, 12:00pm
17 Jun 2020, 1:00pm
26 Aug 2020, 2:00pm
From the same authors

Mobile subscription Trojans and their little tricks

Triada Trojan in WhatsApp mod

Pig in a poke: smartphone adware

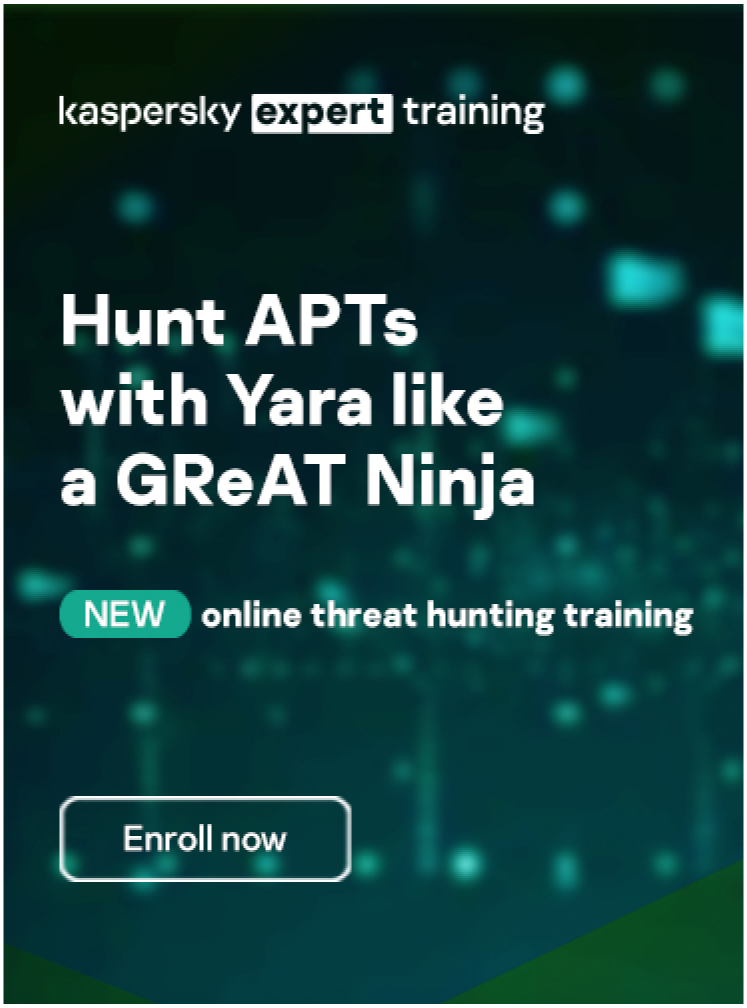
Aggressive in-app advertising in Android

Unkillable xHelper and a Trojan matryoshka

Subscribe to our weekly e-mails

The hottest research right in your inbox

-


kaspersky expert training
Hunt APTs with Yara like a GReAT Ninja
NEW online threat hunting training
Enroll now

Reports

APT trends report Q1 2022

This is our latest summary of advanced persistent threat (APT) activity, focusing on events that we observed during Q1 2022.

Lazarus Trojanized DeFi app for delivering malware

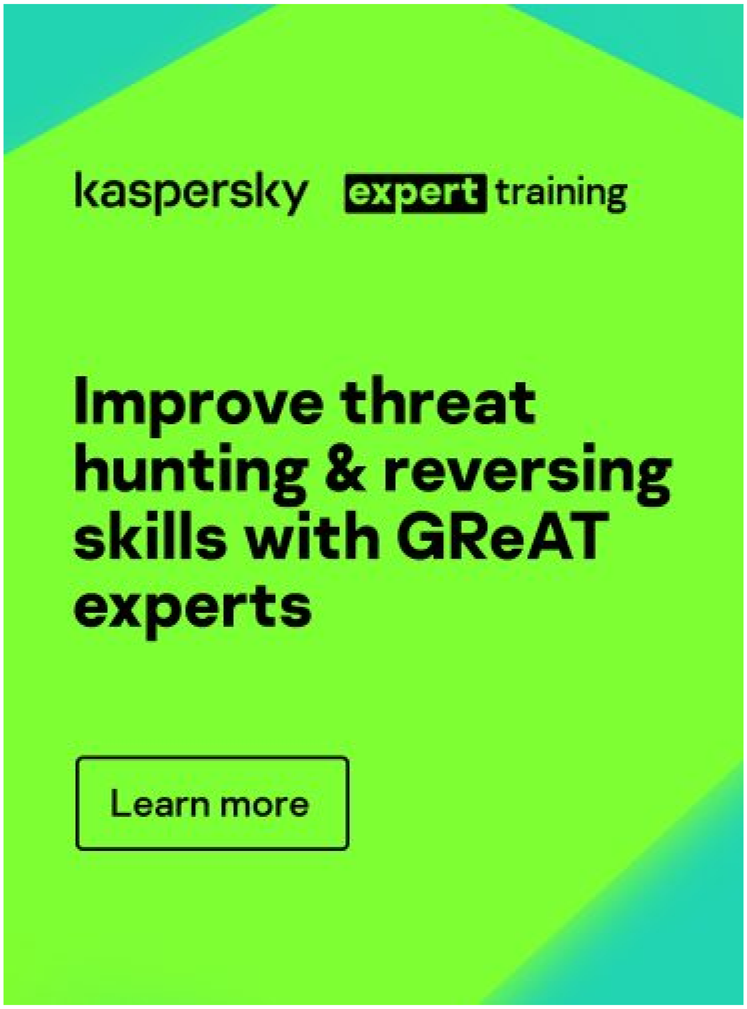
We recently discovered a Trojanized DeFi application that was compiled in November 2021. This application contains a legitimate program called DeFi Wallet that saves and manages a cryptocurrency wallet, but also implants a full-featured backdoor.

MoonBounce: the dark side of UEFI firmware

At the end of 2021, we inspected UEFI firmware that was tampered with to embed a malicious code we dub MoonBounce. In this report we describe how the MoonBounce implant works and how it is connected to APT41.

The BlueNoroff cryptocurrency hunt is still on

It appears that BlueNoroff shifted focus from hitting banks and SWIFT-connected servers to solely cryptocurrency businesses as the main source of the group’s illegal income.


kaspersky
expert training
Improve threat hunting & reversing skills with GReAT experts
Learn more