

Infected Zoom Apps for Android Target Work-From-Home Users

B labs.bitdefender.com/2020/03/infected-zoom-apps-for-android-target-work-from-home-users

Anti-Malware Research

5 min read



Oana ASOLTANEI

March 31, 2020

One product to protect all your devices, without slowing them down.

[Free 90-day trial](#)



Most of the world's population has been under lockdown for more than two weeks, forced to work from the safety of their own homes.

Many have turned to video-conferencing software to keep businesses open, to attend classes or just to stay connected. It was just a matter of time until cyber-criminals started to trick users into installing tainted video-conferencing apps to capitalize on the expanded pool of users.

Malicious Zoom clones for the unaware

Zoom has been in the spotlight lately as one of the booming applications for video conferencing, despite its issues with end-to-end encryption and liberalized data sharing with Facebook. It did not take long for cyber-criminals to re-package it, disseminate it on third-party markets and wait for new victims to install it. The samples documented in this article spread outside of the Google Play Store and exclusively target users who sideload applications on their Droids.


























*Analyzed sample: **30a1a22dcf7fa0b62809f510a43829b1***

Packagename: us.zoom.videomeetings

Detection: Android.Trojan.Downloader.UJ

App label: Zoom

This piece of malware has components injected in the repackaged Zoom application, as shown in figure 1 below.

- ▼  us.zoom
 - >  androidlib
 - >  cptshare
 - >  net
 - >  template
 - >  thirdparty.login
 - >  util
 - ▼  videomeetings
 - ▼  byfsl
 - >  us.zoom.videomeetings.byfsl.Pkipn
 - >  us.zoom.videomeetings.byfsl.Qrfde
 - >  us.zoom.videomeetings.byfsl.Qwkso
 - >  us.zoom.videomeetings.byfsl.Qxohs
 - >  us.zoom.videomeetings.byfsl.a
 - >  us.zoom.videomeetings.byfsl.b
 - >  us.zoom.videomeetings.byfsl.c
 - >  us.zoom.videomeetings.byfsl.d
 - >  us.zoom.videomeetings.byfsl.e
 - >  us.zoom.videomeetings.byfsl.f
 - >  us.zoom.videomeetings.byfsl.g
 - >  us.zoom.videomeetings.BuildConfig
 - >  us.zoom.videomeetings.Manifest
 - >  us.zoom.videomeetings.R
 - >  us.zoom.videomeetings.ZMBuildConfig
 - >  us.zoom.videomeetings.ZMPreferencesProvider

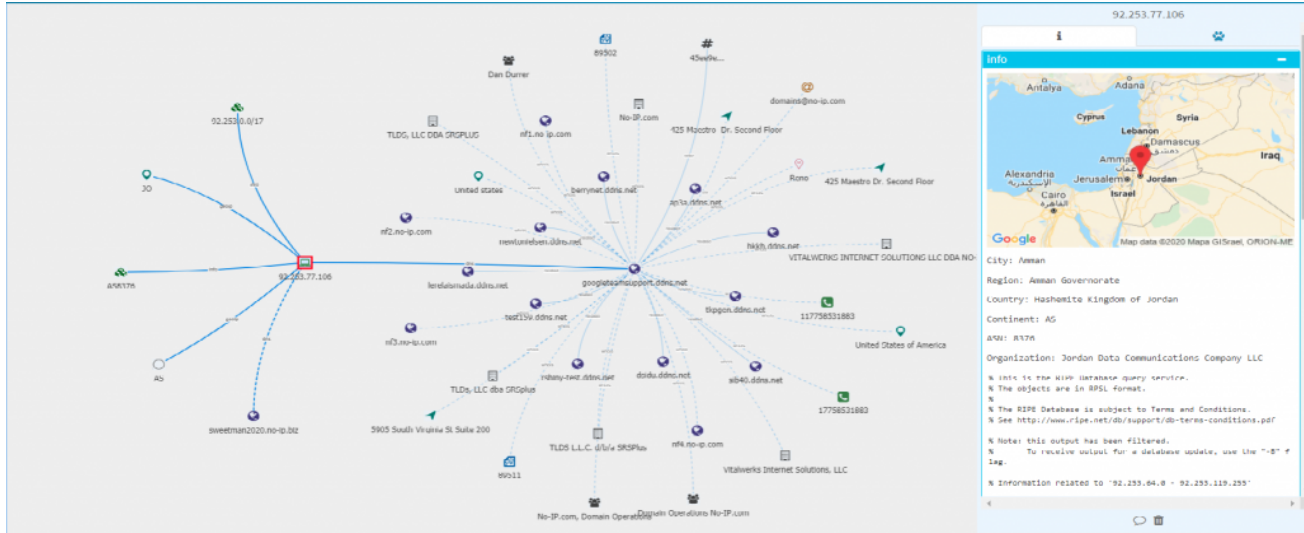
While the user interface is identical with the original application, it comes with extra “functionality” that the user did not sign up for. The malware tries to download its main payload from a command-and-control infrastructure at `tcp[://googleteamsupport[.]ddns.net:4444`

The choice of domains is likely not random, as it could indicate what the attackers might target next (the Google TeamSupport application is a business-to-business collaborative platform that is also surging during the COVID-19 isolation).

Update (04/01/2020): We have investigated the `googleteamsupport[.]ddns.net` domain and uncovered some interesting historical details.

This is a dynamic DNS service that allows an user with a dynamic IP address to map it to a subdomain, so they can offer a service without interruption, even when their dynamic IP address changes.

Our domain history shows that this subdomain was pointed at an IP address in Jordan (92.253.77.106) that seems to also have resolved sweetman2020[.]no-ip[.]biz.



We were able to link the sweetman2020 subdomain as a command and control server for SandoRAT / DroidJack, an Android remote access tool. Last year, security researcher Dancho Danchev also linked this subdomain to several **targeted** attacks using remote access tools.

The sample has the same package name as the original Zoom application and the developers have taken even subtle measures to keep the Certificate details as close as possible to the original Zoom app.

Application	Certificate details
Original Zoom	C=US, O=Zoom Video Communications Inc.
Malicious Zoom	C=US, O=Zoom Video Communications Inc.

Aggressive adware gangs can't miss the show

Bitdefender researchers have also uncovered a tainted Zoom APK that specifically targets Chinese users. Once sideloaded, the application asks for phone, location and photo permissions on start.

Analyzed sample: **fb5243138a920129dd85bb0e1545c2be**

Packagename: us.zoom.videomeetings

Detection: Android.Adware.Downloader.BC

App label: Zoom

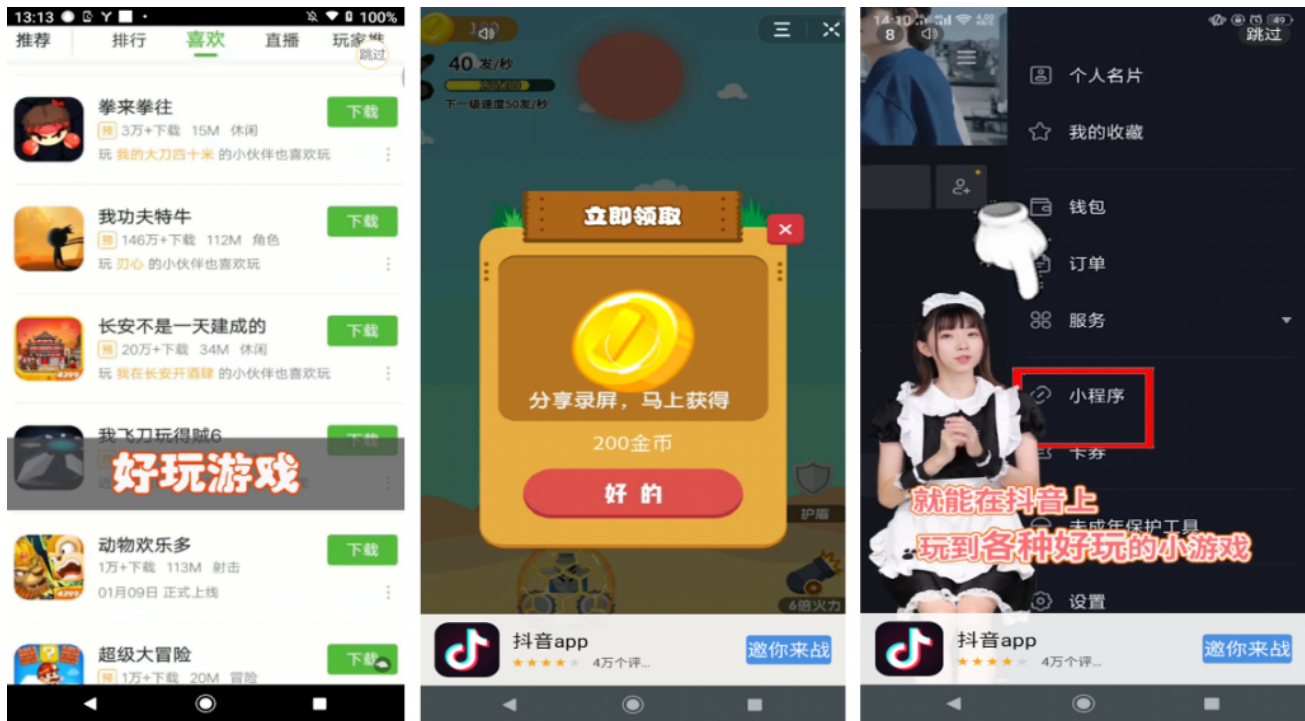
Targets: China

When the victim taps the app icon, the application either does nothing, or it briefly displays an ad before closing itself.

The piece of code below shows that the main activity is transparent:

```
<activity android:name="com.kdssa.sdk.csj.SplashActivity"
android:theme="@android:style/Theme.Translucent.NoTitleBar"> <intent-filter> <action
android:name="android.intent.action.MAIN"/> <category
android:name="android.intent.category.LAUNCHER"/> </intent-filter> </activity>
```

As soon as the app opens, a native ad is loaded and displayed on the screen for just a second.



When the application finally starts, the victim is presented with ads as soon as they try to Join a Meeting. They will keep receiving these ads until they press the X button.

The APK we analyzed retrieves adware info from:

[https://sf3-ttcdn-tos.pstatp\[.\]com/obj/ad-pattern/renderer/package.json](https://sf3-ttcdn-tos.pstatp[.]com/obj/ad-pattern/renderer/package.json) (the sf3 prefix part is different across various apps with the same SDK)

```
{ "name": "ad-pattern-renderer", "version": "1.0.124", "main": "https://sf3-ttcdn-tos.pstatp[.]com/obj/ad-pattern/renderer/99093f/index.html", "resources": [{"url": "https://sf3-ttcdn-tos.pstatp[.]com/obj/ad-pattern/renderer/99093f/index.html", "md5": "f0d70a91b5035cd0a11b99fe8182ca42", "level": 1}, {"url": "https://sf3-ttcdn-tos.pstatp[.]com/obj/ad-pattern/renderer/99093f/index.js", "md5": "0f4eef8f4ebfa230471c43dbf2e8bae", "level": 1}
```

Hardcoded links:

[http://sf3-ttcdn-tos\[.\]pstatp.com/](http://sf3-ttcdn-tos[.]pstatp.com/)

More Zoom badware

This is another malicious sample that attempts to impersonate the Zoom application and lure victims into installing it.

Analyzed sample: **9930b683d4b31a3398da0fb75c27d056**

Packagename: app.z1_android_421120320_app_original_file

Detection: Android.Trojan.HiddenAds.AJR

App label: ZOOM Cloud Meetings

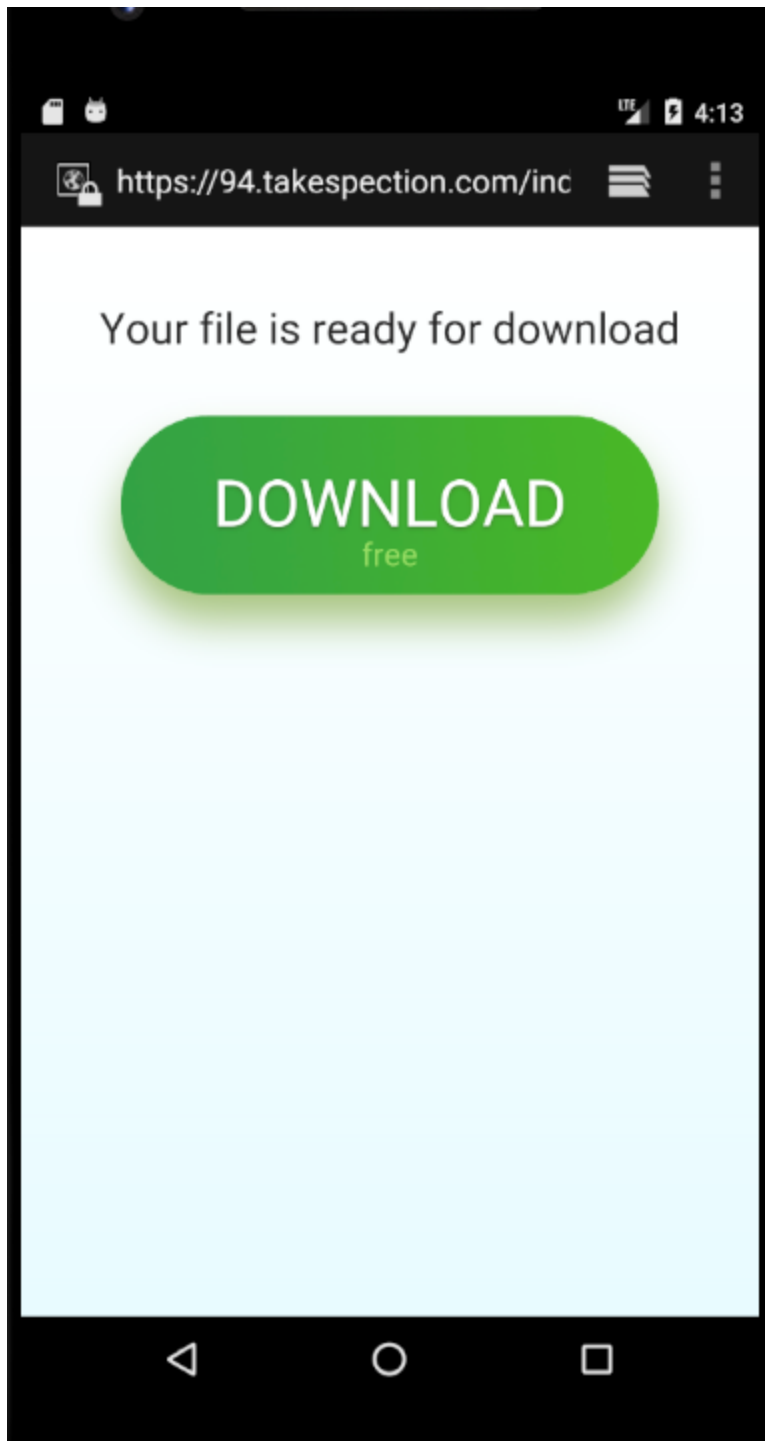
When opened, the application initially hides itself from the menu. It then starts a repeating alarm that randomly sends an intent to an Ad Service. This service subsequently starts an AdActivity that opens an ad. The link can be found in the resources: adsforapp1[.]com

```
public static void a(Context context, String str) {
    Random random = new Random(System.currentTimeMillis());
    int parseInt = Integer.parseInt(context.getString(R.string.interval_click));
    int nextInt = (random.nextInt((parseInt * 2) / 24) + parseInt) * 1000;
    ((AlarmManager) context.getSystemService("alarm")).setRepeating(0, ((long) (Istr.equals("new") ? nextInt :
}

public void onCreate(Bundle bundle) {
    super.onCreate(bundle);
    setContentView(R.layout.activity_ads);
    this.c = (WebView) findViewById(R.id.webViewAds);
    this.d = (ProgressBar) findViewById(R.id.progressBar);
    this.c.clearCache(true);
    this.c.getSettings().setJavaScriptEnabled(true);
    this.c.setVisibility(4);
    this.c.loadUrl("https://" + getString(R.string.domain_ads));
    this.c.setWebViewClient(new a());
}
```

The malicious app proceeds with checking for another hard-coded string in assets, called 'admin'. If the string is true, it asks for device admin rights. If the value is set to false (as in our case), it tries to download another file (the **apk** entry).

When opened, the app redirects to download the extra component.



As of the moment of writing, this sample has been seen in the wild in the United States.

The sample bundles functionality to ask for device admin permissions in English or Russian, based on the default language of the mobile phone. The malware also has the ability to start itself when the device is powered on.

Bitdefender Mobile Security for Android detects and blocks these applications as Android.Trojan.Downloader.UJ, Android.Adware.Downloader.BC and Android.Trojan.HiddenAds.AJR. In order to minimize risks of getting compromised, Android

users are advised to install a security solution and to limit their downloads to vendor-recommended application stores.

TAGS

[anti-malware research](#)

AUTHOR

