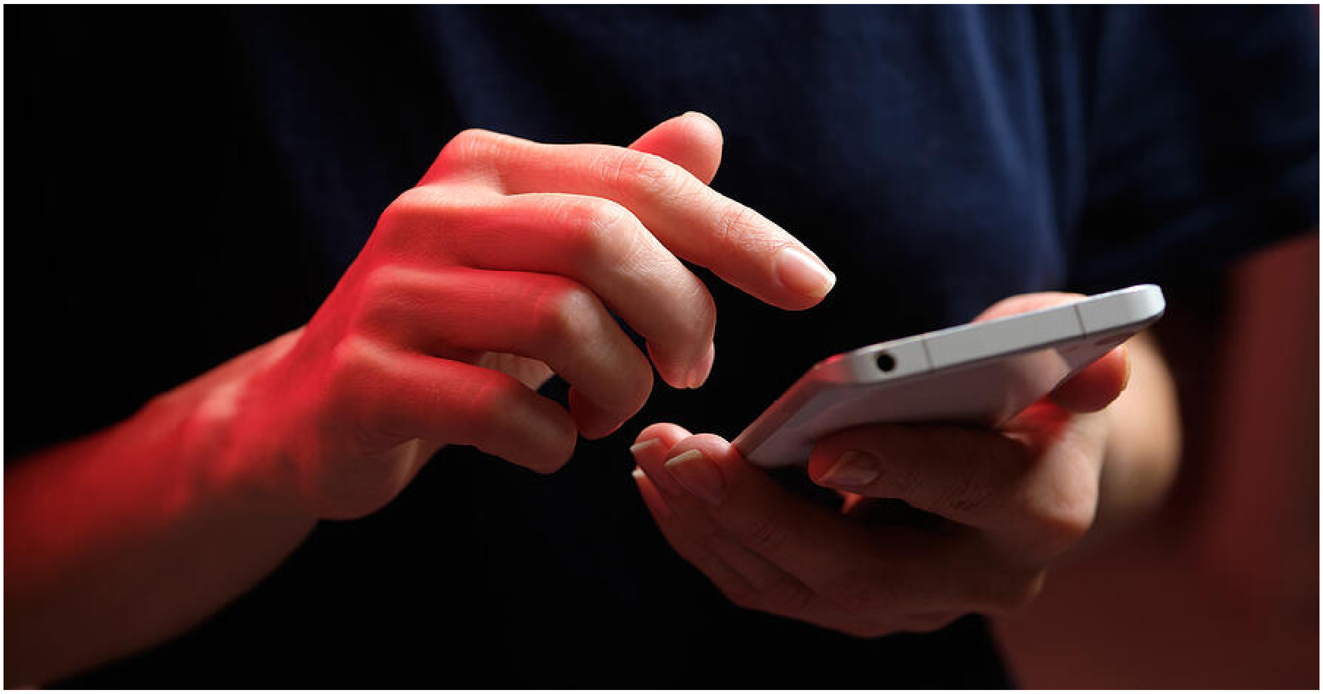
SMSFactory Android Trojan producing high costs for victims

blog.avast.com/smsfactory-android-trojan



Jakub Vávra 1 Jun 2022

Avast protected more than 165,000 people across the globe from this threat within a year.

Avast has been tracking a wide-spread malware campaign consisting of TrojanSMS malware, which we are calling SMSFactory. SMSFactory sneakily siphons money from victims around the world, including Russia, Brazil, Argentina, Turkey, Ukraine, US, France and Spain, among others, by sending premium SMS and making calls to premium-rate phone numbers. These numbers appear to be part of a conversion scheme, where the SMS includes an account number, identifying who should receive the money for the messages sent. Undetected, it can rack up a high phone bill, up to $7 per week or $336 per year, leaving an unpleasant surprise for victims. One version we found is also capable of extracting victims' contact lists, likely to spread the malware further.

We have dubbed the malware SMSFactory due to its functions, as well as class names in its code, one of which is called SMSFactory.

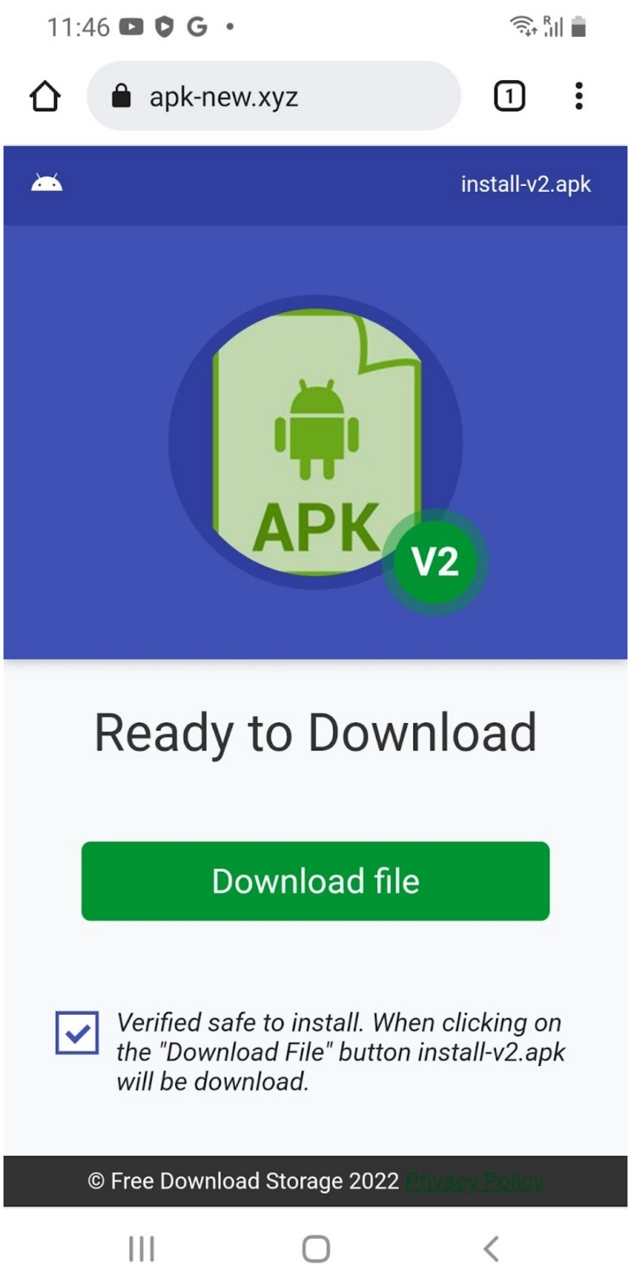
According to my research, the malware is spreading through malvertising, push notifications, and alerts displayed on sites offering game hacks, adult content, or free video streaming sites, serving the malware disguised as an app in which users can access gaming, videos, or adult content. Once installed, the malware hides itself, making it nearly impossible for victims to detect what is causing the charges on their phone bills.

A series of websites have been set up with the purpose of spreading and remote control of the malware. Avast has protected more than 165,000 Avast users from SMSFactory in the past year (May 2021-May 2022), with the highest number of users protected in Russia, Brazil, Argentina, Turkey and Ukraine.

Silently sending $ignals

The bad actors behind SMSFactory rely on malvertising to drive their campaign. Malvertising refers to the misuse of adverts to redirect users to sites with malware payloads, and can often appear on websites providing free streaming of films and TV shows, adult content, or torrent aggregators, but may occasionally appear on mainstream sites as well.

The redirect in this case leads to a website such as the one in the screenshot below. The user is prompted to download a file that is made to resemble the site the user was redirected from. This can, for example, be a game hack app, an adult content app, a free video streaming app or similar.


11:46

apk-new.xyz

install-v2.apk

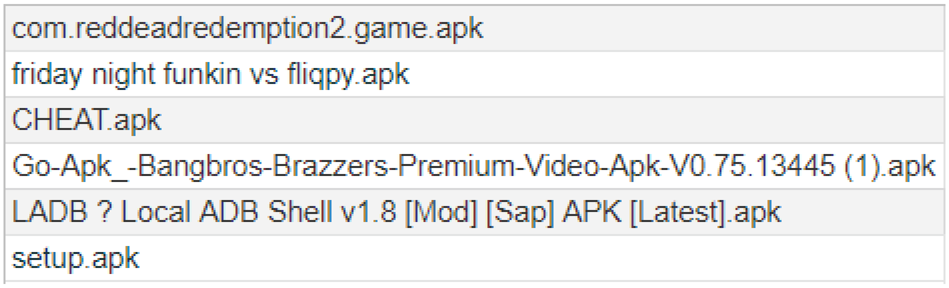
Ready to Download

Download file

☑ *Verified safe to install. When clicking on the "Download File" button install-v2.apk will be download.*

© Free Download Storage 2022 Privacy Policy

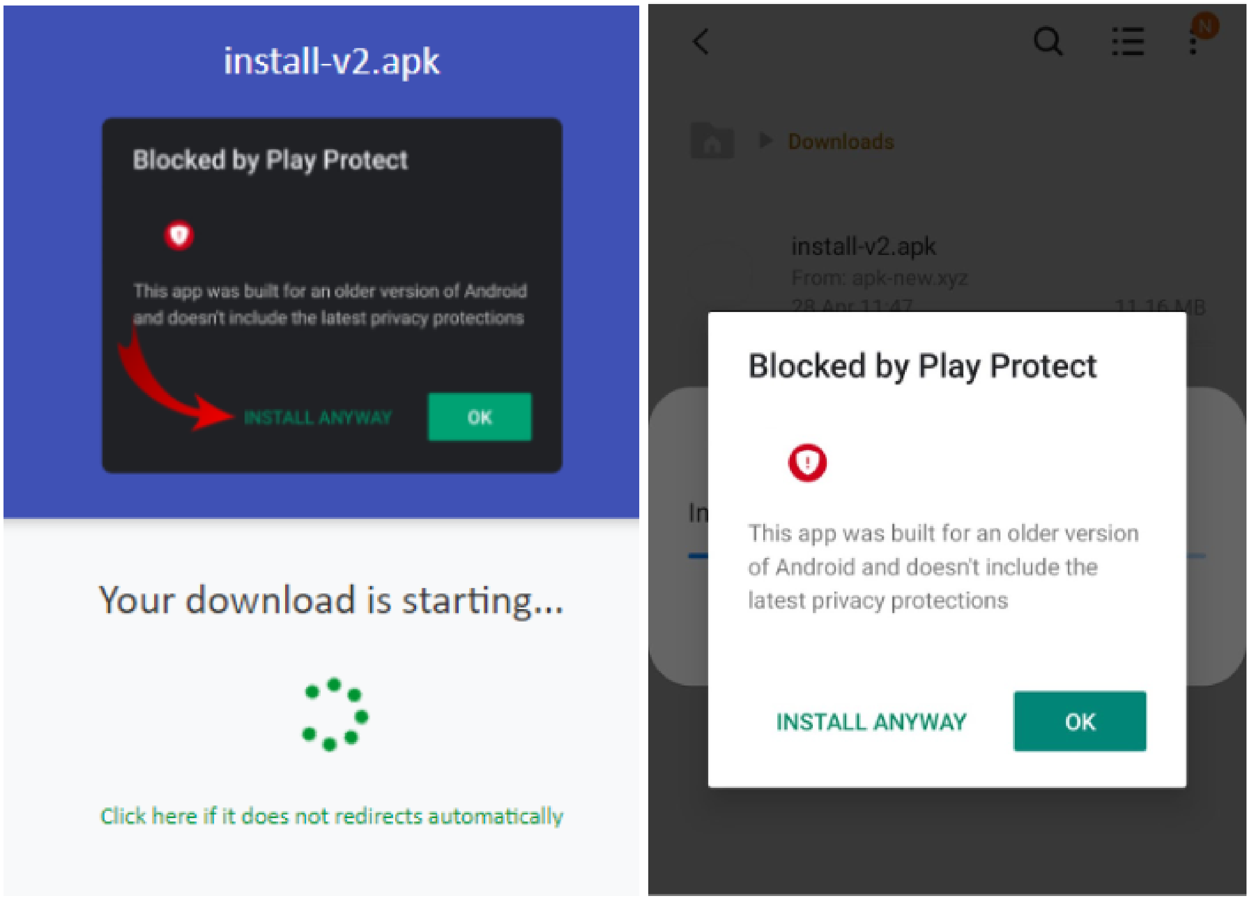
Redirect landing page with dynamic name visible in the top right corner



com.reddeadredemption2.game.apk
friday night funkin vs fliqpy.apk
CHEAT.apk
Go-Apk_-Bangbros-Brazzers-Premium-Video-Apk-V0.75.13445 (1).apk
LADB ? Local ADB Shell v1.8 [Mod] [Sap] APK [Latest].apk
setup.apk

Examples of different names for the same SMSFactory app

Once the user clicks on Download, the malicious app is downloaded. As it comes from a third party source, the website prompts the user to ignore Android's inbuilt Play Protect warning and go ahead with the installation.



install-v2.apk

Blocked by Play Protect

This app was built for an older version of Android and doesn't include the latest privacy protections

Your download is starting...

Click here if it does not redirects automatically

Downloads

install-v2.apk

From: apk-new.xyz

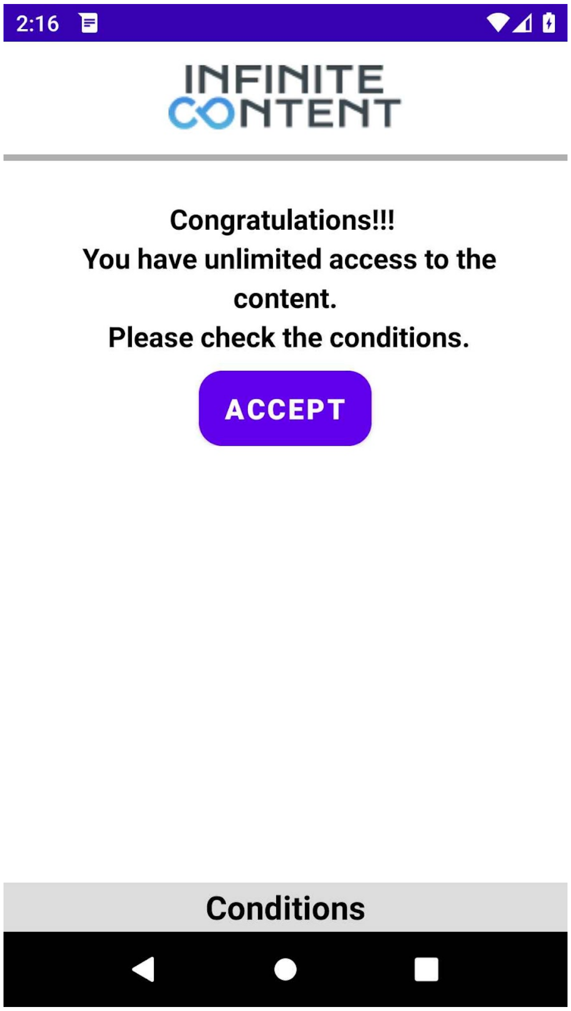
28 Apr 11:47 11.16 MB

Blocked by Play Protect

This app was built for an older version of Android and doesn't include the latest privacy protections

Screenshots showing how SMSFactory prompts the user to disable/ignore Play Protect in order to install the malware

Once installed, the user is met with a welcome screen. Clicking accept will activate the app's malicious behavior. The app then presents the user with a basic menu of videos, adult content and games that don't work or aren't available most of the time.

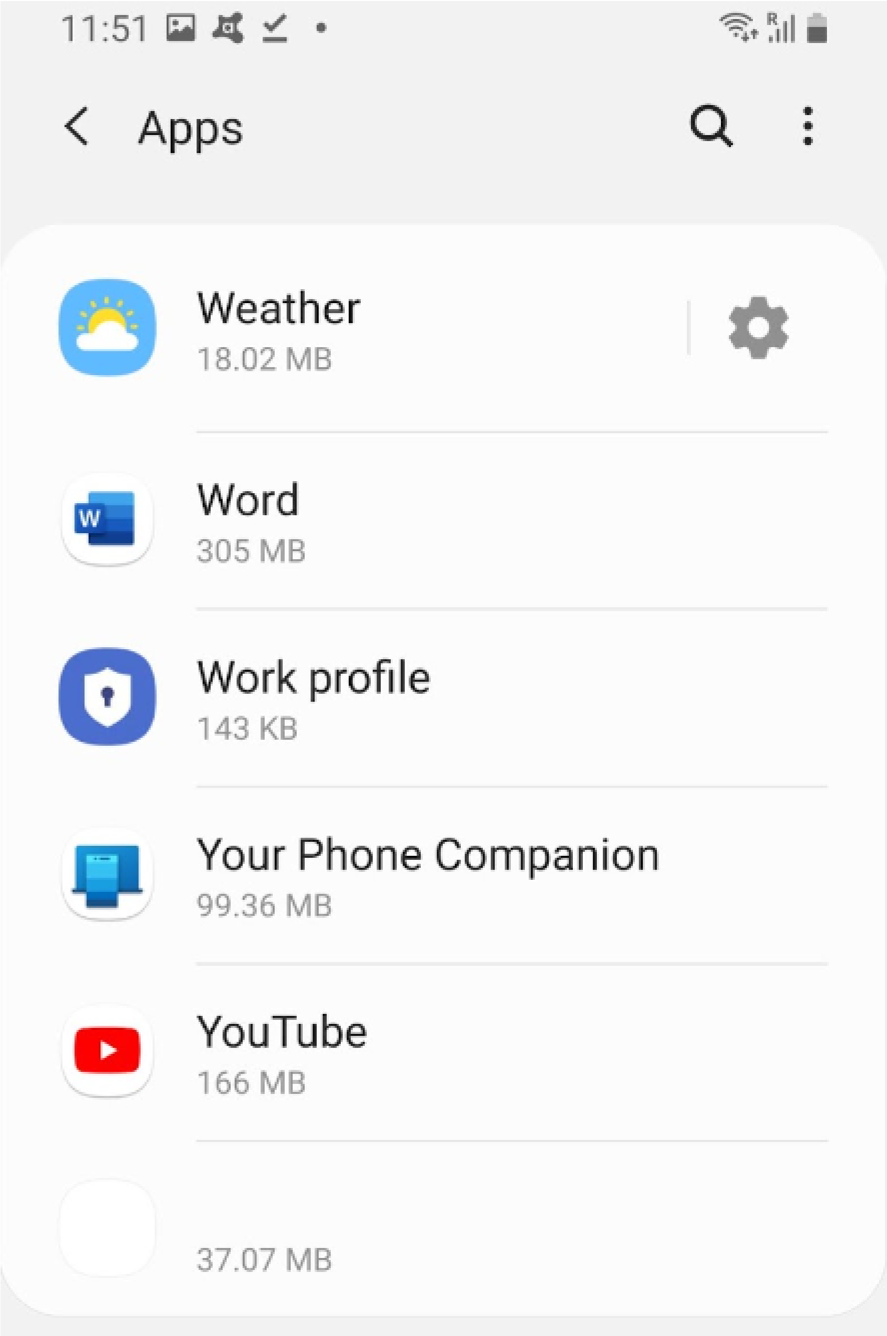


Congratulations!!!
You have unlimited access to the content.
Please check the conditions.

Example of an SMSFactory app upon installation

Ready or not, here come the charges!

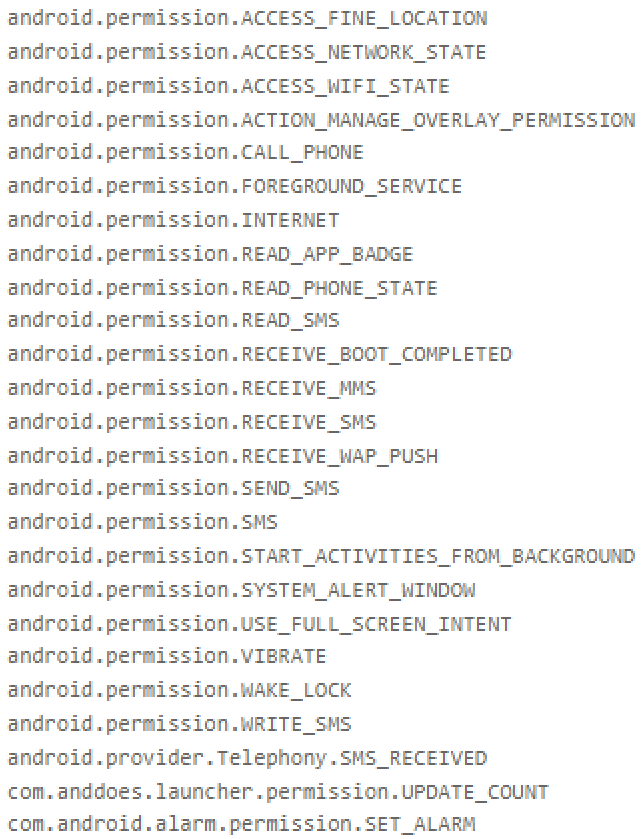
SMSFactory uses several tricks to stay on the victim’s device and remain undetected. It has a blank icon and it is able to hide its presence from the user by removing its app icon from the home screen. Additionally, it comes with no application name, making it more difficult for the user to discover the offending application and remove it. It is evident the malware relies on the user forgetting the app on their phone.



A blank icon and lack of app name are used to disguise the apps

Once hidden, the malware communicates with a pre-set domain. It sends a unique ID allocated to the device, its location, phone number, operator information, and model of the phone. If the actors behind this campaign deem the victim's device usable, the domain sends back instructions to the device. This will either be a list of phone numbers to which the malware will send premium SMS or a specific number which the application will attempt to call.

Both will result in excessive charges for the victim. The exact amount depends on the command sent by the actors behind SMSFactory — in our testing, we've seen a daily $1 charge through ten SMS messages sent, which can rack up to $28 per month. Assuming the victims don’t notice or forget the app is installed, this could result in an extortionate phone bill.



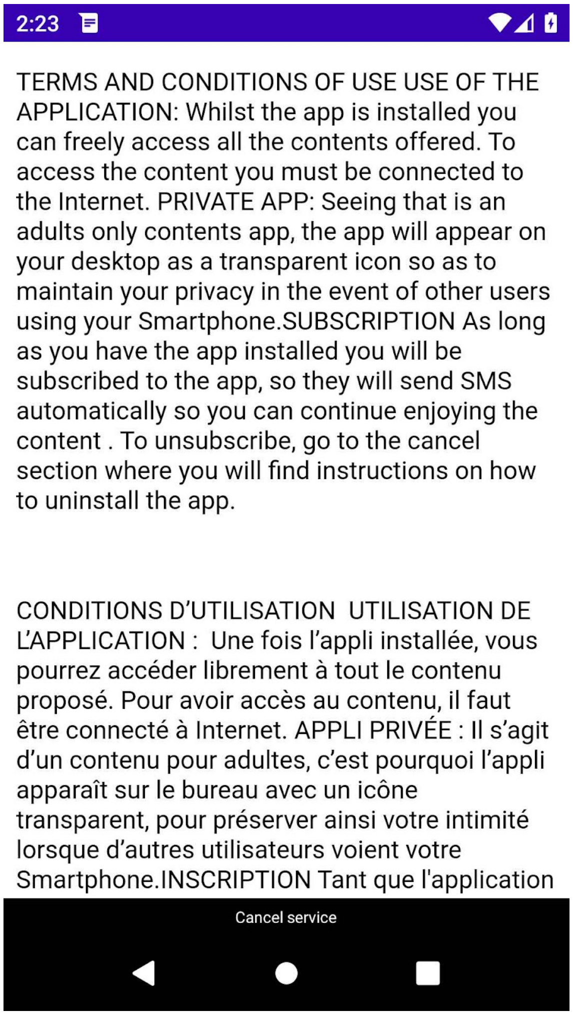
```
android.permission.ACCESS_FINE_LOCATION
android.permission.ACCESS_NETWORK_STATE
android.permission.ACCESS_WIFI_STATE
android.permission.ACTION_MANAGE_OVERLAY_PERMISSION
android.permission.CALL_PHONE
android.permission.FOREGROUND_SERVICE
android.permission.INTERNET
android.permission.READ_APP_BADGE
android.permission.READ_PHONE_STATE
android.permission.READ_SMS
android.permission.RECEIVE_BOOT_COMPLETED
android.permission.RECEIVE_MMS
android.permission.RECEIVE_SMS
android.permission.RECEIVE_WAP_PUSH
android.permission.SEND_SMS
android.permission.SMS
android.permission.START_ACTIVITIES_FROM_BACKGROUND
android.permission.SYSTEM_ALERT_WINDOW
android.permission.USE_FULL_SCREEN_INTENT
android.permission.VIBRATE
android.permission.WAKE_LOCK
android.permission.WRITE_SMS
android.provider.Telephony.SMS_RECEIVED
com.anddoes.launcher.permission.UPDATE_COUNT
com.android.alarm.permission.SET_ALARM
```

A portion of the permissions used by SMSFactory: SMS/MMS permissions as well as CALL_PHONE are used to siphon money away from victims by sending messages and making calls to premium rate numbers

Due to the nature of the malware, the user may be unaware of the financial damage until they receive their phone bill. SMSFactory could accrue significant charges in the meantime and it may be difficult for the user to identify the culprit due to the app hiding itself.

Different Factory versions

SMSFactory also appears to have several different versions with added features, which have appeared alongside this recent campaign. One such variation may create a new admin account on the Android device, making it potentially difficult to remove. Another variant copies the contact list of the victim and extracts it, likely to be used for further spread of the malware. Some versions redirect users to sites in order to get them to install another SMSFactory app onto their device.



TERMS AND CONDITIONS OF USE USE OF THE APPLICATION: Whilst the app is installed you can freely access all the contents offered. To access the content you must be connected to the Internet. PRIVATE APP: Seeing that is an adults only contents app, the app will appear on your desktop as a transparent icon so as to maintain your privacy in the event of other users using your Smartphone.SUBSCRIPTION As long as you have the app installed you will be subscribed to the app, so they will send SMS automatically so you can continue enjoying the content . To unsubscribe, go to the cancel section where you will find instructions on how to uninstall the app.

CONDITIONS D'UTILISATION UTILISATION DE L'APPLICATION : Une fois l'appli installée, vous pourrez accéder librement à tout le contenu proposé. Pour avoir accès au contenu, il faut être connecté à Internet. APPLI PRIVÉE : Il s'agit d'un contenu pour adultes, c'est pourquoi l'appli apparaît sur le bureau avec un icône transparent, pour préserver ainsi votre intimité lorsque d'autres utilisateurs voient votre Smartphone.INSCRIPTION Tant que l'application

Only a few SMSFactory samples contain a short 'Conditions' page

There are visual differences between these versions of SMSFactory as well. Older versions that posed as game hacks had an icon, while the newer versions removed the icon and app name altogether. The terms and conditions in the screenshot above, mentioning the background premium SMS/calls, are only present in one version of the malware I found, other versions don't include this information at all.

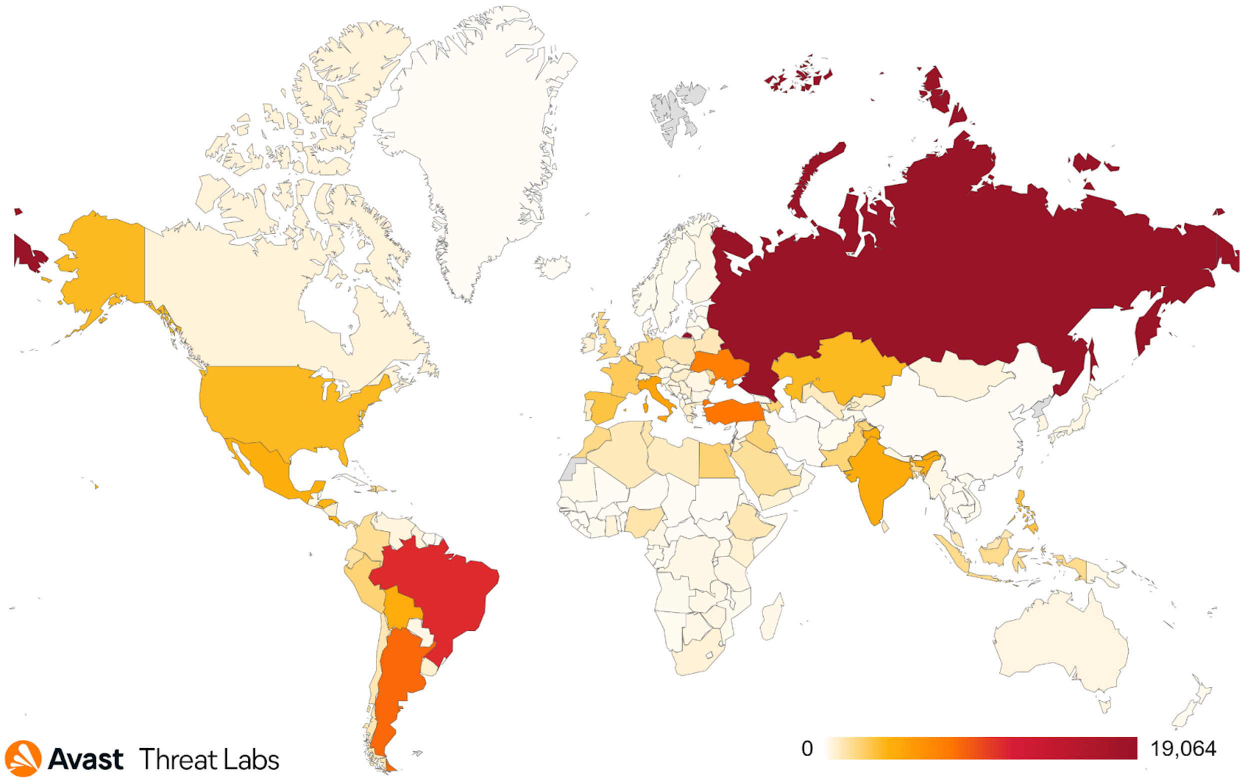
What makes SMSFactory unique

In contrast to recent TrojanSMS campaigns such as UltimaSMS or Grifthorse, the vector for spreading SMSFactory varies significantly. Its stealth features such as lack of app icon and name wouldn't be allowed on the Google Play Store, hence the bad actors have resorted to a reasonably intricate network of sites for delivery and subsequent communication with the malware.

Another departure is the intro screen that doesn't require the entry of a phone number to initiate the malware's functions, contrary to previous premium SMS malware. Where previous TrojanSMS campaigns subscribe the victim to premium services, SMSFactory simply sends a series of SMS to premium numbers to extract money.

Affected users

Despite its lack of presence on the Play Store, according to our data, we have protected over 165,000 Avast users from the malware in the last year alone. As evidenced by the high number of impacted users coupled with new versions recently surfacing, it is fair to say that SMSFactory is an active malware and likely to continue its spread.



Map showing number of Avast users protected from SMSFactory in the last year (May 2021 - May 2022)

As can be seen in the map above, the regions in which we protected the most Avast users from SMSFactory within the last year are located in Russia, Brazil, Argentina, Turkey, and Ukraine. It appears that SMSFactory isn't targeting a specific region or country, its aim is to spread to as many devices as possible.

Tips on how to avoid mobile malware like SMSFactory

Stick to official app stores. SMSFactory highlights the importance of using verified app stores to install applications. Third party stores or unknown sources may contain malware and aren't blocked by an authority, such as Google.

Install an antivirus on your mobile device. This is especially important if you want to install apps from unofficial sources. You can also be protected from malicious websites this way. Antivirus acts as a safety net, protecting even the most careful users.

- **Remain vigilant.** It's important to remain cautious when downloading new apps, especially apps advertised in short and catchy videos, or through push notifications in the browser.

- **Disable or limit premium SMS with your carrier.** While there are legitimate uses for premium SMS, recent SMS malware campaigns highlight the importance of control over potential charges on a user’s phone contract. Disabling premium SMS features or at least setting a limit significantly negates the potential impact of TrojanSMS campaigns. This step is especially important on children’s phones.

Want to know more? Explore the list of SMSFactory IOCs.