Android Apps and Malware Capitalize on Coronavirus

labs.bitdefender.com/2020/03/android-apps-and-malware-capitalize-on-coronavirus

Anti-Malware Research
12 min read

Oana ASOLTANEI
March 26, 2020

As new developments regarding the coronavirus outbreak emerge, Android developers (malware developers included) have started capitalizing the topic.

Bitdefender researchers have recently analyzed Android telemetry from Google Play – and other third-party marketplaces – regarding coronavirus-themed legitimate apps and malware in Europe, and found huge spikes in application scans containing “covid” or “corona” in the package name or file path — with over 2,100 scans during the first two weeks of March alone. The United States peaked at about 500 and Asia at about 1,000 applications scanned in March, containing the two keywords.

Interestingly, Bitdefender telemetry also shows that Android users have been more interested in downloading and installing medical applications from Google Play. For example, during the first two weeks of March, the number of scanned applications from the medical category increased more than 35 percent compared to February.

These numbers show that, as the novel coronavirus outbreak increased in severity throughout Europe and worldwide, the public sought out applications that provided information on procedures for avoiding infection, updates regarding COVID-19, and even medical appointment booking services.

In terms of analyzing applications from other, third-party marketplaces, while some applications have been repacked to include aggressive adware, others have been bundled with banking Trojans, SMS-sending malware, and even the money-siphoning Android malware named Joker Trojan.

Some malware developers have devoted more effort to financially capitalize on the coronavirus outbreak. For example, some applications have been bundled with the legitimate apps they're piggybacking, while others blatantly feature an obviously suspicious version name (e.g. "[SPY_NOTE_VERSION_OK]").

The next chapters include more information on findings from the Google Play store and coronavirus-themed Android malware.

Riding the Coronavirus Wave

Many apps contain the "coronavirus" keyword, or derivations of it, in their package name. Some news apps have also pushed an update containing an activity (UI component) dedicated to coronavirus (for example, a world map of confirmed cases).

Also, the popularity of medical appointment apps has increased, especially in the last few weeks. One such example is "Zocdoc Find A Doctor & Book On Demand Appointments." This app registered 867 scans between March 7 and March 16 (roughly 100 per day), out of which 97 percent were in the US. With more than 500,000 installs and 6,850 reviews, this medical appointment app has been highly popular in the United States where people are trying to set up appointments with doctors, potentially to be tested for COVID-19.

As of January 1, 2020, we found 579 applications that contain coronavirus-related keywords in their manifest (package name, activities, receivers, etc.). This means that a major component of the application was named in way – or the application contains strings – that relates it to the recent outbreak. Out of the total, 560 are clean, 9 are Trojans and 10 are Riskware. The distribution of such apps has increased dramatically from January 1st to March 17th, as can be noted from the histogram bellow.

Fig. 1 – Coronavirus-themed Android apps scanned between January and March

Most malicious apps found are bundle threats that range from ransomware, to SMS-sending malware, and even spyware designed to clean out the contents of victims' devices for personal or financial data.

Tweaking Content to Gain Google Play Ranking on Coronavirus

As soon as the coronavirus pandemic was officially declared, Google started making adjustments to Google Play searches to purposely filter or remove coronavirus apps.

For example, searching for keywords like "corona" or "coronavirus" would display no search results in the Apps section. This was in line with a blog post published by Google, explaining how these actions are meant to help offer only relevant information and applications that people in need might require.

They even set up a webpage within the Google Play marketplace where only legitimate and relevant applications that offered information about coronavirus or healthcare were displayed, in an attempt to steer users in the right direction.

Google likely anticipated a rise in opportunistic applications latching on to this topic of global interest and decided to clamp down on any potential abuse.

For instance, some apps have changed their name and description to capitalize on the coronavirus pandemic by including keywords that ensure their apps rank best when people search for coronavirus in Google Play. Some of these changes are skin-deep, in that only the application's page on Google Play has been updated, and not the app itself.

Bubble Shooter Merge (updated February 4th), is just one example where the developer twice updated the name of the application within Google Play to include the "coronavirus" and "stay home" keywords.

With these simple changes, apps become more "visible," taking advantage of the #coronavirus pandemic or the #stayhome challenge, although the app content wasn't related to COVID-19 in any way.

Another example is Galaxy Shooter – Falcon Squad, an arcade game with over 10 million installs. The recent update includes an "Anti Corona Event" in the application's title that's visible only to English-speaking countries, potentially to match #corona searches.

Another interesting finding involves a developer changing their application name on Google Play from "4K Wallpaper – only quality wallpapers!" to "Coronavirus (2019-nCov) – Protect yourself!."

The changes go a lot deeper. The developer even changed the original screenshots of the application that showcased some of the wallpapers available, replacing them with what seems to be a coronavirus infection map.

This means that the package name has remained completely the same ("com.thegosa.galaxythemes") with the developer simply leveraging coronavirus to boost an already impressive download count of over 500,000 installs.

At the moment, approximately 22 apps that use the "coronavirus" keyword are still online, most of them official and listed under the "Health and Fitness" or "Medical" categories.

However, about 280 applications have been removed from Google Play, likely because they infringed policies outlined by Google in terms of abusing the coronavirus pandemic.

Some of the apps removed from Google Play involve regional or global coronavirus trackers, with installs ranging from 5,000 to 50,000.

Coronavirus-Themed Bankers, Spyware, and Infostealers

Bitdefender researchers also took a look at some of the applications found on various third-party marketplaces or disseminated through phishing campaigns where users were instructed to manually download and install them directly from the attacker-controlled website.

As expected, most of these malicious applications leverage the coronavirus pandemic to scare users into installing the apps. Others use variations on coronavirus domains to hide their command and control infrastructure.

Anubis banker joins in on the corona mischief

For the first time, the Anubis banking Trojan has been spotted as part of an Android coronavirus malware campaign. The application imitates a Coronavirus information site and, on installation, asks for accessibility. If given access, it will request various other permissions and accept them by itself.

To throw users off track, it takes them to a coronavirus statistics website (https://coronatracker.com/) then proceeds to hide its icon while, in the background, it continues with an arsenal of functionalities, specific to Anubis.

Initially, Anubis targeted countries ranging from the US and India to France, Italy, Germany, Australia, and Poland, however this recent Android version seems to target Turkey, by impersonating the legitimate website to which it redirects users.

The “uygulama aktiflestirme onayi” message is translated into “application activation confirmation” (Turkish)

MD5:
b7070a1fa932fe1cc8198e89e3a799f3
64ebe4ecfb242019ee590d80740e6a46
Detection: Android.Trojan.Banker.OB

Abusing the infamous Iranian AC19 app

One such case abuses the now-famous Iranian corona information application AC19 (hxxps://cafebazaar.ir/app/co.health.covid), which stirred up quite a lot of controversy in Iran over fears of spying.

This application is installed by its malicious parent (*com.android.tester 8eb1a54389bd742b778e56fe9dd4b11d, application label: corona*). The sample asks for permissions to allow scanning for the coronavirus, but in fact will ask for sensitive Android application privileges that that malware uses to continue its malicious spying activities.

Spying and surveillance lot

Another malicious spying lot contains the legitimate corona live application (wrapper over the Johns Hopkins coronavirus tracker). While previous reports have covered some of the below-mentioned samples, Bitdefender researchers also found two more Crona named samples, showing that authors are clearly continuing this campaign with no end in sight.

Two of the new applications, were created with invalid package names and cannot install. The rush to milk the ongoing pandemic is quite high, which seems to make malicious actors prone to error.

All new application icons respect known variations of the family.

The legitimate application is stored, internally, in the **/res** folder of the APK; in **res/raw/MT_Bin or res/raw/google.apk**.

From the same malware family, we have found three newer variations that have only the application name corona viruse without carrying with them the legitimate sample. They simply hide the icon on launch.

An odd trait of these applications is that all three have the version name: **[SPY_NOTE_VERSION_OK]**

Coronavirus Tracker is the name, adware is the game

Another example of an application that abuses these times for ill-gotten gain bears the name **Coronavirus Tracker** (e423f61f1414eccd38649f20d018723d) and gives out adware to unsuspecting users.

At start-up, the application says it is “not available in your country” and hides itself. It will stay dormant for a time before actually starting to bombard the user with ads.

An interesting observation is that, in some cases, the application will not hide the icon on Xiaomi devices. While the reason is unknown, this could indicate that Xiaomi is a personal favorite of the malware authors.

Bitdefender also found the CnC from where it downloads configurations (api[.]jetrohe[.]pw), potentially to display customized apps.

MD5: e423f61f1414eccd38649f20d018723d
Detection: Android.Trojan.HiddenAds.ALB by Bitdefender.

It might get lonely in coronavirus times

Another interesting sample in the corona campaign is an application named CORONAVIRUS (com.MaCHIbuild.Ninjaclimbs.jumpout). At first, it seems to be a simple wrapper over the coronavirus information world map https://www.worldometers.info/coronavirus/.

Unexpectedly, the application has a different logic behind the scenes. It retrieves information from its CnC http[:]//contorl.okapk[.]website/AmineData.json and will either open the WebView with the world map, or an entirely different link, provided by the CnC.

For example, the CnC now returns:

```
{ "web_data": { "status": "0", "link": "https://google.com" }
```

With this logic, if the “status” is “0” then the application opens the coronavirus world map. At any given time, should the developers chose to change this, your trusty coronavirus-fighting app turns into something malicious.

Adware and adult content mostly likely come next. Within the application’s code, we see some partially implemented functions that load custom StartApp Ads, Ogury Ads and Admob Ads as well as the ability to open a Chrome tab with a custom provided link.

We estimate that adult content will be provided, because of another partially implemented part of the application. The application prepares a link to https[:]//t.grtyb[.]com (which redirects to hxxps://www[.]thepornstudy[.]com, a pornographic survey site) to be loaded into its own WebView. In this URL, the author will add specific tokens and referrals that will generate revenue for the application’s developer each time a victim visits the link.

MD5: 783277390d3fb1ad0fb7751d982d21ff
Detection: Android.Riskware.HiddenAds.GX

Iranian coronavirus apps

کرونا ویروس means coronavirus in Persian, and seems to be an informative app that helps users identify common symptoms of the illness while keeping in touch with news related to the outbreak.

The app was developed using a framework, as most parts of the code seem generated in an automatic fashion, making the code logic harder to grasp.

The core functionality of the app is found in the firebase messaging component, as the server communicates with the app through JSON objects.

The received JSON message is checked by the app and, based on what commands are received, the application’s behavior can be remotely controlled by messages received from the server.

The central functionality of the app is similar to apps identified with the detection Android.Riskware.HiddenApp.GN, but it has been adapted to contain information regarding the coronavirus, as it represents a major attraction point for Android users while also providing the opportunity to bombard them with popups.

One functionality of the app is the ability to redirect any link sent through firebase messaging to a browser.

Another interesting functionality is triggered when it receives a firebase command message containing Telegram. The provided link is used to open specific Telegram channels or groups.

The application will first search for the original Telegram application on the device. If it is not present, it searches for similar chat apps that are popular in Iran. The first one found is then opened, and the link can be seen as a popup in those applications.

Not only can it open webpages and chat apps but, depending on the issued command, it can also receive package names that it will try to open either on Google Play or on CafeBazaar, a popular Iranian Android market.

The application also has the ability to open any Instagram page received from firebase messaging:

In a nutshell, this coronavirus app can be much more than an informative application and its functionalities are likely to be used in a way that is harmful to users.

MD5s:
b0a418ce4f5439ddcb9c864e5ffd45a4
1897b6b9e3f2eab26d7175c14290129d
31092e0fefbe653d27479edb0e7f849a

Detection: Android.Riskware.HiddenAds.HZ

The Joke(r) is on you

It seems the Joker Trojan is also trying to capitalize on the corona outbreak. Although it only tries to hide its CnC using a coronavirus domain variation, the UI of the gaming application remains unchanged.

Distributed with the iFun Game (Android.Trojan.Joker.GC), the app is repackaged with the Joker malware, which downloads a payload from the **http[:]//coronavirus.oss-accelerate.aliyuncs[.]com** CnC.

Of course, Joker obfuscates the CnC so that static analysis does not identify it. However, as can be seen in the screenshot below, it simply shifts some letters.

The application can still be found on third party-marketplaces.

MD5: fed0a95f4e1936500e7c8c990666c7a6
Detection: Android.Trojan.Joker.GC

Additional Android banking malware

Additional Trojan Banking malware hijacking coronavirus news includes a banking Trojan designed to act as a RAT (Remote Access Trojan) enabling attackers to gain persistency on the victim’s device while syphoning sensitive information.

In some new instances the authors only bothered to change the application’s name from Coronavirus to CoronaVirus.

As people become more aware that they might be targeted with Corona-related scams, malware authors take this into consideration. For instance, while targeting Italian users, malware developers changed the name of the malware to Aggiornamento, which means “Update” in Italian.

One small difference with the malicious version of the Coronavirus Finder is related to the displayed UI. On installation, it takes users to accessibility settings. After activation, it opens different settings and automatically deactivates various things. It then opens an activity where victims are supposed to enter their credit card details.

If you try to go to the Settings menu, then hit Applications and scroll down, the malware will take you to the home screen, preventing victims from uninstalling the app. Of course, it can also hide its icon, just to make it even more annoying and difficult.

MD5:
2a4fe8c50de598066995bbfed2754c8f
dad9de0c3fa9b80dc1bc12535b851b5b
6815eb50505890c868f36649b07bc92d
a8dd3cd7860f3fd2d34a33b0c87bd615
d5ea5d3d9f6b44cf183ddd61c44c056e

Detection: Android.Trojan.Banker.MS

“Hacking” Pandemic: The Board Game

A fake app claims to provide a hack for “Pandemic: The Board Game” (which can be found on Google Play at https://play.google.com/store/apps/details?id=com.f2zentertainment.pandemic&hl=en) but it actually only shows adware, tries to get the user’s phone number, and advertises another popular Google Play game (https://play.google.com/store/apps/details?id=com.igg.android.lordsmobile&hl=en).

Besides all that, the malware we've detected as Android.Trojan.HiddenApp.AIT, also hides itself.

On launch the application shows a fake human verification step.

But in reality, pressing the indicated "free" option only displays more ads.

MD5: 5b22b1782f58081c2a6c94703268693e
Detection: Android.Trojan.HiddenApp.AIT

Final Thoughts

The Coronavirus pandemic might have everyone running around after information, searching for applications that offer live monitoring or even medical appointments to get tested. It's always recommended that you install only official apps from official marketplaces, and seek information only from official sources. Also, it's crucial to make sure you have a mobile security solution that can keep you and your device safe from malware and other online threats.

Note: This article is based in technical information provided courtesy of the Bitdefender Labs teams.

TAGS

anti-malware research

AUTHOR

Oana ASOLTANEI

Oana Asoltanei is a Security Researcher at Bitdefender. She focuses her research on Android malware and mobile security in general.

View all posts