Coronavirus Report: Popular Android Apps Impersonated by Malware
Foreword

It has been more than 30 days since Europe and North America have adopted serious isolation measures in an attempt to stop the Coronavirus pandemic. With most people safe at home in lockdown, human interactions are bridged by technology.

Whether it’s for working from home, online school courses or entertainment, people rely more than ever on smart devices to ease the effects of social distancing, and malware developers have been quick to adapt to the new reality.

Here at Bitdefender we keep a close eye on cyber-criminals’ techniques, and we develop mitigations for a safer experience at home, at the office or at school. For the past three months, we have monitored trending mobile applications and have looked for cloned applications rigged with malware.

Android Apps

To the best of our knowledge, none of these applications are available through official sources. The fact that they’re delivered through alternative channels does not make things any better though. Our past research reveals that one in 10 Android users install applications from alternative sources even when they are available on the Google Play Store for free. Here’s a non-exhaustive list of popular applications that cyber-criminals are using to compromise devices.
WORLD HEALTH ORGANIZATION

APK MD5: 9526c93bcfaa7b6f638181e100bc52fc
Detection: Android.Trojan.Obfus.II
Malware family: SpyNote
App label: World Health Organization
App icon:

As soon as the World Health Organization announced that it would develop an Android application to track COVID-19 infections, malware authors started exploiting this theme to peddle infected APKs.

This fake app hides its icon after the user opens it for the first time, then continues its malicious activities in the background. No visible GUI is available for the user.

The application's command and control server can be found at pharaoh.ddns.net (197.41.111.130), whose location can be tracked to Egypt's Al Mansurah city.

It can read text messages, make phone calls, read the contact list, get account information, record audio and access the device's camera, among many other capabilities.
## DISCORD

<table>
<thead>
<tr>
<th>APK MD5</th>
<th>App Label</th>
<th>Detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>692895885a1fc803f5062bdfbe3be9f0</td>
<td>Discord V.2 (Mods) Adrian</td>
<td>Android.Trojan.FakeApp.JE</td>
</tr>
<tr>
<td>2da8739af8d063c6c3d92f836ad32d53</td>
<td>Discord</td>
<td>Android.Trojan.SpyAgent.Q</td>
</tr>
<tr>
<td>6cbeb773921b80c132e0cb33824a78f9</td>
<td>Nitro Discord</td>
<td>Android.Trojan.Agent.AKD</td>
</tr>
</tbody>
</table>

### App icons:

![Discord icon](image)

The first application is a classic; it asks for accessibility and device admin permissions, hides itself and then spies in the background. At least it doesn’t block you from going to Settings - Applications to uninstall it.

The second app: On start, it shows a toast message with the text “CPU aquire.” Then, of course, it hides. Are we seeing a pattern here?

The third app fails to complete installation because it is signed improperly:

```
Failure [INSTALL_PARSE_FAILED_NO_CERTIFICATES: Failed to collect certificates from /data/app/vmdl1001754011.tmp/base.apk using APK Signature Scheme v3: APK content size did not verify]
```

Malware developers make mistakes, too. Just like that uTorrent icon on a Discord app.
The apps have been seen in the wild in the United States.

**Command and Control domain:** hostynamee.ddns.net
IP resolved at some point Location:
- 105.6.34.152 Morocco, Fes
- 199.66.93.173 Canada, Ontario
- 196.206.73.254 Morocco, Fes
- 41.248.117.142 Morocco, Fes
- 199.66.93.109 Canada, Ontario

Over time, this domain resolved to several different IPs, predominantly from Morocco and Canada.

**HANGOUTS**

**APK MD5:** 0eb9be2abb8f67046fa393eea97571db
**App Label:** hangouts
**Detection:** Android.Trojan.HiddenApp.AIB
App icon:

The app requests accessibility and device admin permissions, then proceeds to ignore all user attempts at opening it and instead chooses to perform its spying activities covertly.

The CnC server is located at 0{}.tcp{}.ngrok{}.io (18.223.41.243), which resolves to US, Columbus. *This same IP has been used to distribute variants of Gafgyt, a Linux-based cross-platform DDoS botnet family malware.*

*These apps have been found in the wild in the US and Germany.*
DELIVERY

Need a delivery service while in lockdown? The malware guys are quick to help you out. Simply accept their accessibility permission request and they’ll deliver you an Anubis Banker on the double.

**APK MD5:** 28c88cc3272ecdb84b78ce95a28e17a3  
**Package name:** rare.destroy.news  
**Detection:** Android.Trojan.FakeApp.JM  
**App Label:** Delivery club  
**App icon:**

Asks for accessibility settings. When granted, it opens Google Play automatically and starts Google's speech recognition to search on Play, possibly to trick the user into believing that accessibility access is needed for speech recognition. It hides its icon. Drops Anubis in the background from assets.

The Command and Control Server is [www[.happynewyear666[.xyz](mailto:www[.happynewyear666[.xyz)] that points to an IP 82.202.173.99 in Moscow, Russia.
SKYPE

Social apps with video call features are surging in popularity due to the social distancing measures imposed around the world, and Skype is no exception.

This is where Skype is most frequently used around the world (Bitdefender telemetry)

Over 100 new fake Skype apps have been found since countries have gone into lockdown and people around the world start to work from home or seek face time with loved ones.

App icons:

![App icons](image)

App labels:

- skype
- Skype
- skype-android
- Skype - free IM video calls Hack
- Skype для Android
- Skype 9.3
- Skype Mobile
- Skype_2.7.0.907
- Skype_Android
- skype注册拉人进群组
- skype自动语音广告
- skypelite
- skype轰炸
- skype轰炸eric
The most common malware family that tries to imitate the original Skype application is by far the one bundled with the `com.soft.android.appinstaller` package name, with 99 Skype-related applications.

Judging by the text and download link, this family of ransomware targets Russians. It attempts to get victims to download a possibly fake Skype app from http://amoby.ru/get/3ajKp (although the given link currently doesn't provide any applications) while trying to send “payment” text messages to various short codes (e.g. 7151, 8151, 2858).

“Confirm agreement with the Skype download rules. To continue to download, press Next.”

“Activation completed successfully. You will receive an SMS message with a link to Skype, after which the download will become available. If the message doesn't arrive, you can download Skype at http://amoby.ru/get/3ajKp or click next for automatic transition to download.”

InfoStealers, DroidJacks, Bankers and other FakeInstallers haven’t hesitated in targeting Skype either. We detect all of these applications with variants of Trojan.Fakelnst, Trojan.Banker, Trojan.SMSSend, Trojan.InfoStealer and Riskware.Agent. A full list of IoCs for APKs impersonating Skype is available in the Indicators of Compromise section.
NETFLIX

Netflix hasn’t gone unnoticed by cyber-criminals during the lockdown. Almost 100 fake apps trying to imitate the streaming service provider have been found, as more and more people tune into digital content to compensate for a lack of social interaction.

During the first three months of the Coronavirus pandemic, we’ve seen more Netflix malware in countries such as the United States and Germany. The following chart displays the geographic distribution of the malicious apps:

<table>
<thead>
<tr>
<th>App Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ChekerNetflix</td>
<td>Netflix Checker</td>
</tr>
<tr>
<td>free Netflix</td>
<td>Netflix Free</td>
</tr>
<tr>
<td>Free Netflix EN</td>
<td>Netflix hacked</td>
</tr>
<tr>
<td>Free Netflix Premium</td>
<td>Netflix hp</td>
</tr>
<tr>
<td>Netflix</td>
<td>Netflix Premium</td>
</tr>
<tr>
<td>netflix</td>
<td>Netflix Premium by APKMODY</td>
</tr>
<tr>
<td>NETFLIX</td>
<td>Netflix Premium by MODPLAY</td>
</tr>
<tr>
<td>NetFlix</td>
<td>NETFLIX UHD</td>
</tr>
<tr>
<td>Netflix-hacked</td>
<td>NETFLIX VPN V 2</td>
</tr>
<tr>
<td>Netflix-MOD-Final</td>
<td>Netflix.apk</td>
</tr>
<tr>
<td>Netflix 1</td>
<td>NetflixMOD</td>
</tr>
<tr>
<td>netflix 2</td>
<td>NetflixPlayer</td>
</tr>
<tr>
<td>Netflix 3</td>
<td>NetflixySpotify</td>
</tr>
<tr>
<td>Netflix App</td>
<td>pelis de netflix.com</td>
</tr>
<tr>
<td>Netflix by APKMODY</td>
<td></td>
</tr>
</tbody>
</table>

The fake applications come with various icons, some closer to the service’s visual identity than others:

A list of IoCs is available in the dedicated section at the end of this whitepaper.
SpyNote

Almost a third of these apps are different versions of the same app – the same family – and therefore have the same package name: `cmf0.c3b5bm90zq.patch`. They follow the malware author’s favorite behavior pattern: ask for accessibility, ask for device admin rights and hide their icon, as the application completely lacks usable features. Once the device is infected, the apps keep tabs on what victims do in the background, spy on text messages, install applications if instructed to do so by their CnC, record audio in the proximity of the device’s microphone, and more.
### Command and control servers:

<table>
<thead>
<tr>
<th>Domains</th>
<th>IPs</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>spydark.ddns.net</td>
<td>105.159.8.252</td>
<td>Morocco, Tangier</td>
</tr>
<tr>
<td>blueboxi.ddns.net</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>hajilsaad.ddns.net</td>
<td>160.176.32.70</td>
<td>Morocco, Agadir</td>
</tr>
<tr>
<td>a7aa.ddns.net</td>
<td>197.59.115.31</td>
<td>Egypt, Cairo</td>
</tr>
<tr>
<td>wordswag.ddns.net</td>
<td>41.111.108.252</td>
<td>Algeria, Messaad</td>
</tr>
<tr>
<td>0.tcp.ngrok.io</td>
<td>3.19.3.150</td>
<td>US, Columbus</td>
</tr>
<tr>
<td>7aga.ddns.net</td>
<td>197.38.178.119</td>
<td>Egypt, Cairo</td>
</tr>
<tr>
<td>hager44.ddns.net</td>
<td>94.47.27.189</td>
<td>Syria, Damascus</td>
</tr>
<tr>
<td>cracker012.ddns.net</td>
<td>196.90.134.217</td>
<td>Morocco, Agadir</td>
</tr>
<tr>
<td>hexohexo.ddns.net</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>STARLORD3307-62594.portmap.io</td>
<td>193.161.193.99</td>
<td>Russia, Saint Petersburg</td>
</tr>
<tr>
<td>hexo6664.ddns.net</td>
<td>41.104.38.17</td>
<td>Algeria, Sidi Moussa</td>
</tr>
<tr>
<td>arris05.ddns.net</td>
<td>141.255.146.118</td>
<td>France, Paris</td>
</tr>
<tr>
<td>spynoteaness2020.hopto.org</td>
<td>105.99.221.139</td>
<td>Algeria, Ras el Oued</td>
</tr>
<tr>
<td>azer123456.hopto.org</td>
<td>196.64.240.79</td>
<td>Morocco, Fes</td>
</tr>
</tbody>
</table>
Cerberus RAT

Another Android malware family that commonly targets Netflix is the Cerberus RAT (Remote Access Trojans). Bitdefender found almost 20 Cerberus Trojan files disguised as Netflix apps in the last month alone. Unlike the previously discussed family, Cerberus randomizes its application package names (e.g. ypcttczsahlwohemiyrygyapx.eea.uucsnrtjxfeykitgzyp), so one device can run multiple instances of this malware at the same time.

These applications request accessibility rights in terms of special requests to function. Once granted, the app uses the classic stealth mechanism of hiding their icon and will proceed to accept other permission requests by itself. Some versions disable Play Protect services to make sure it won't cause any problems in the future. The apps then wait for commands from their command and control servers.

The Cerberus family also uses accessibility features to protect itself from uninstallation by returning the device to the home screen if the user attempts to go to Settings -> Applications to uninstall an app.
WipeLocker

WipeLocker malware has also witnessed a spike lately, as operators strive to grab a share of the newly-available pool of victims looking for Netflix apps in the wrong place.

Immediately after being granted device admin rights, these fake apps wipe out their host’s memory card. Then, before locking the device screen (different samples use different pictures for this), they send an SMS message to every contact in the device’s list with a random text. One of them goes like this:

“HEY!!! <contact name> Please send me 220 bob kwaMpesa to this number [mobile-phone-number] I have Fuliza in my line. I am really stranded hapakwa stage. Nitakurefund please. “

The text seems to have random words switched to their Swahili equivalent, as “kwaMpesa” (probably a reference to the popular M-Pesa payment platform”, “hapakwa” to “here for” and “Nitakurefund” to “I will teach you”.

Other versions of the text are:

“Ralika 당신의모든범죄를잊을수없어. 나는너에게나를해칠수있게 할것이고 java html C ++이 너에게 올 것이다.” (Korean: “Ralika I can’t forget all your crimes. I will let you hurt me, java html c ++ will come to you”)

“Aki nimekwamahapa stage. Please send me hata 50 bob kwaMpesa to this number [mobile-phone-number] I have Fuliza in my line. Please nitakurefund. Will call you nkifika home”

“Please send me airtime to this number[mobile-phone-number]I have a debt in my line and I need to contact someone urgently I will appreciate.”

Some of the malware’s functionalities aren’t executed if an application with a certain package name exists on the device.

```java
public void keepRunningActivity(Context context) {
    DeviceManager deviceManager = new DeviceManager();
    if (!isPackageExisted(context, context.getResources().getString(R.string.packageName))) {
        new Async_sendSMS(context).execute(new Void[0]);
        getTopActivity(context);
        return;
    }
    try {
        if (deviceManager.isDeviceAdminActive(context)) {
            deviceManager.deactivateDeviceAdmin(context);
        }
    } catch (Exception e) {
        e.printStackTrace();
    }
}
```

The applications that the malware checks for include com.geo and com.hellboy. These two applications are utilities that search for package names associated with WipeLocker and uninstall the malware.

Other malware families discovered trying to take advantage of Netflix’s increasing popularity are DroidJack, AndroRAT and other types of spyware.
An up-to-date list of indicators is available to Bitdefender Advanced Threat Intelligence users. More information about the program is provided at Bitdefender.com/om/advanced-threat-intelligence.html.
Fake Skype apps

Fake Netflix apps

Bitdefender Whitepaper
Coronavirus Report: Popular Android Apps Impersonated by Malware

15
Why Bitdefender

Proudly Serving Our Customers
Bitdefender provides solutions and services for small business and medium enterprises, service providers and technology integrators. We take pride in the trust that enterprises such as Mentor, Honeywell, Yamaha, Speedway, Esurance or Safe Systems place in us.

- Leader in Forrester’s inaugural Wave™ for Cloud Workload Security
- NSS Labs “Recommended” Rating in the NSS Labs AEP Group Test
- SC Media Industry Innovator Award for Hypervisor Introspection, 2nd Year in a Row
- Gartner® Representative Vendor of Cloud-Workload Protection Platforms

Dedicated To Our +20,000 Worldwide Partners
A channel-exclusive vendor, Bitdefender is proud to share success with tens of thousands of resellers and distributors worldwide.

- CRN 5-Star Partner, 4th Year in a Row. Recognized on CRN’s Security 100 List. CRN Cloud Partner, 2nd year in a Row
- More MSP-integrated solutions than any other security vendor
- 3 Bitdefender Partner Programs - to enable all our partners – resellers, service providers and hybrid partners – to focus on selling Bitdefender solutions that match their own specializations

Trusted Security Authority
Bitdefender is a proud technology alliance partner to major virtualization vendors, directly contributing to the development of secure ecosystems with VMware, Nutanix, Citrix, Linux Foundation, Microsoft, AWS, and Pivotal.

Through its leading forensics team, Bitdefender is also actively engaged in countering international cybercrime together with major law enforcement agencies such as FBI and Europol, in initiatives such as NoMoreRansom and TechAccord, as well as the takedown of black markets such as Hansa. Starting in 2019, Bitdefender is also a proudly appointed CVE Numbering Authority in MITRE Partnership.

RECOGNIZED BY LEADING ANALYSTS AND INDEPENDENT TESTING ORGANIZATIONS

- CRN
- AV-TEST
- Gartner
- NSS Research

TECHNOLOGY ALLIANCES

- Microsoft
- Nutanix
- AWS
- Palo Alto Networks
- Citrix

DEDICATED TO OUR +20,000 WORLDWIDE PARTNERS

- A channel-exclusive vendor, Bitdefender is proud to share success with tens of thousands of resellers and distributors worldwide.

- CRN 5-Star Partner, 4th Year in a Row. Recognized on CRN’s Security 100 List. CRN Cloud Partner, 2nd year in a Row

- More MSP-integrated solutions than any other security vendor

- 3 Bitdefender Partner Programs - to enable all our partners – resellers, service providers and hybrid partners – to focus on selling Bitdefender solutions that match their own specializations

UNDER THE SIGN OF THE WOLF

A trade of brilliance, data security is an industry where only the clearest view, sharpest mind and deepest insight can win – a game with zero margin of error. Our job is to win every single time, one thousand times out of one thousand, and one million times out of one million.

And we do. We outsmart the industry not only by having the clearest view, the sharpest mind and the deepest insight, but by staying one step ahead of everybody else, be they black hats or fellow security experts. The brilliance of our collective mind is like a luminous Dragon-Wolf on your side, powered by engineered intuition, created to guard against all dangers hidden in the arcane intricacies of the digital realm.

This brilliance is our superpower and we put it at the core of all our game-changing products and solutions.