WHITEPAPER

Bitdefender

Security

Coronavirus Report: Popular Android Apps Impersonated by Malware

www.bitdefender.com

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.

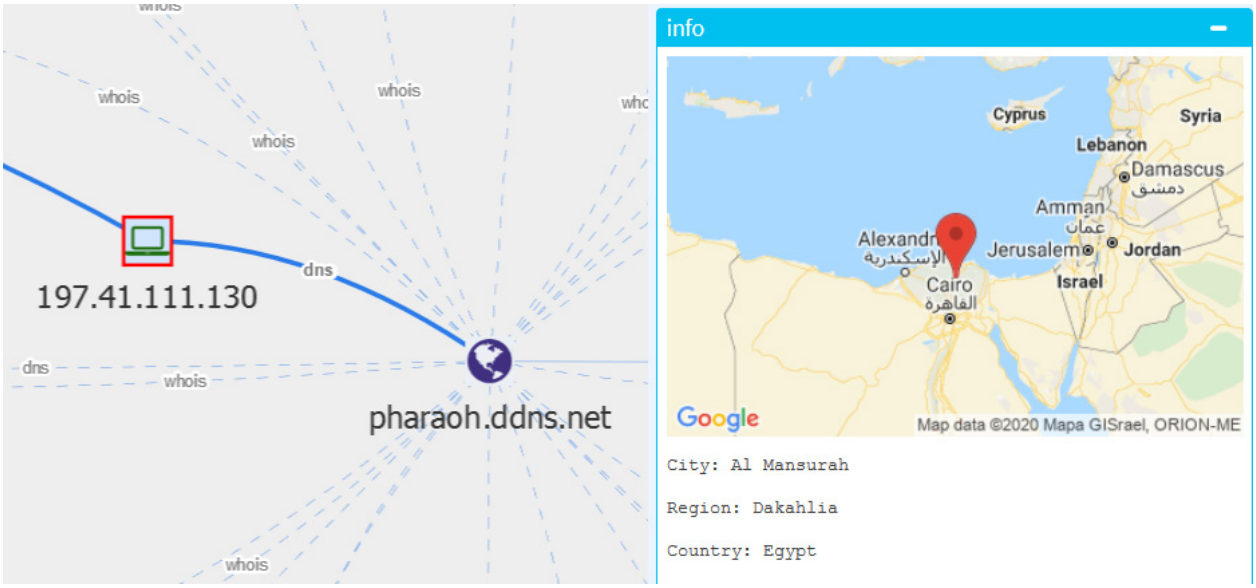
WORLD HEALTH ORGANIZATION

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.

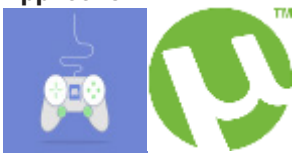


It can read text messages, make phone calls, read the contact list, get account information, record audio and access the device's camera, among many other capabilities.

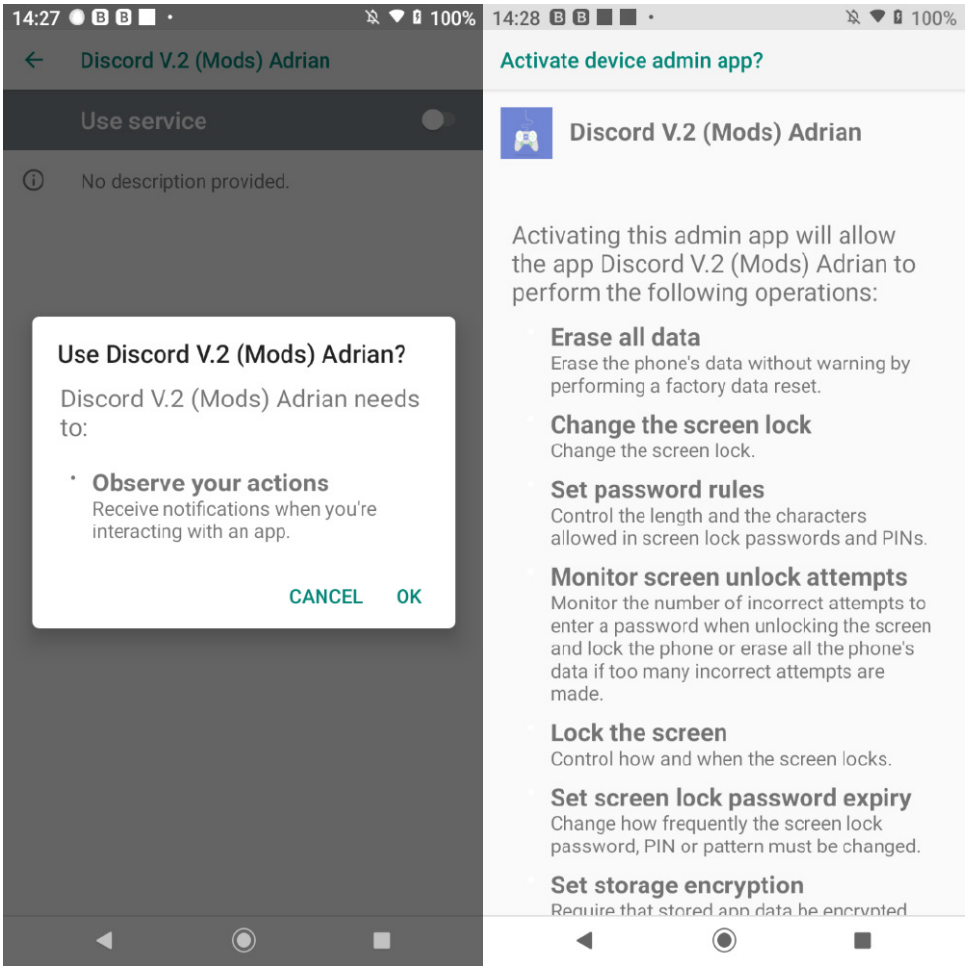
DISCORD

APK MD5	App Label	Detection
692895885a1fc803f5062bdfbe3be9f0	Discord V.2 (Mods) Adrian	Android.Trojan.FakeApp.JE
2da8739af8d063c6c3d92f836ad32d53	Discord	Android.Trojan.SpyAgent.Q
6cbeb773921b80c132e0cb33824a78f9	Nitro Discord	Android.Trojan.Agent.AKD

App icons:



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.

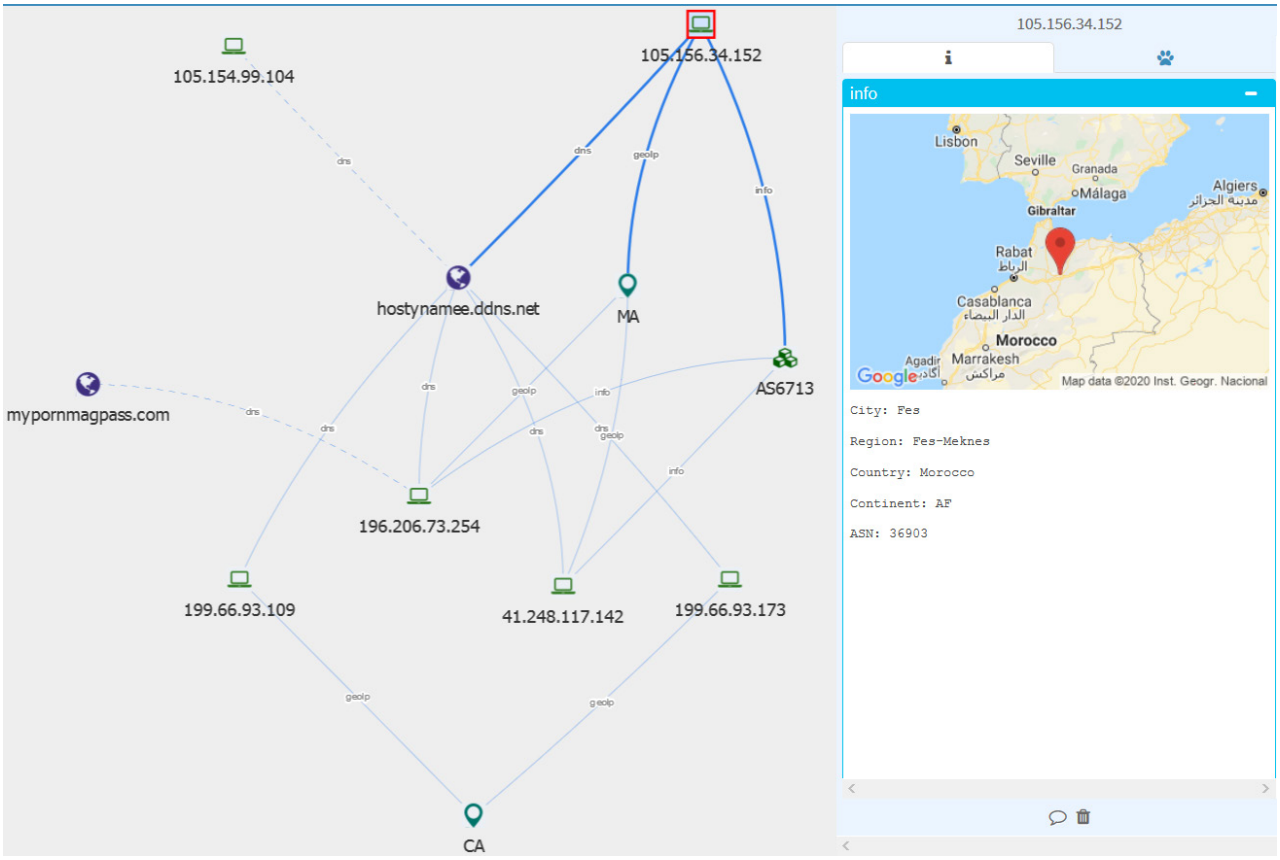


The second app: On start, it shows a toast message with the text "CPU aquire." Then, of course, it hides. Are we seeing a pattern here?

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.



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 CnCserver 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.***

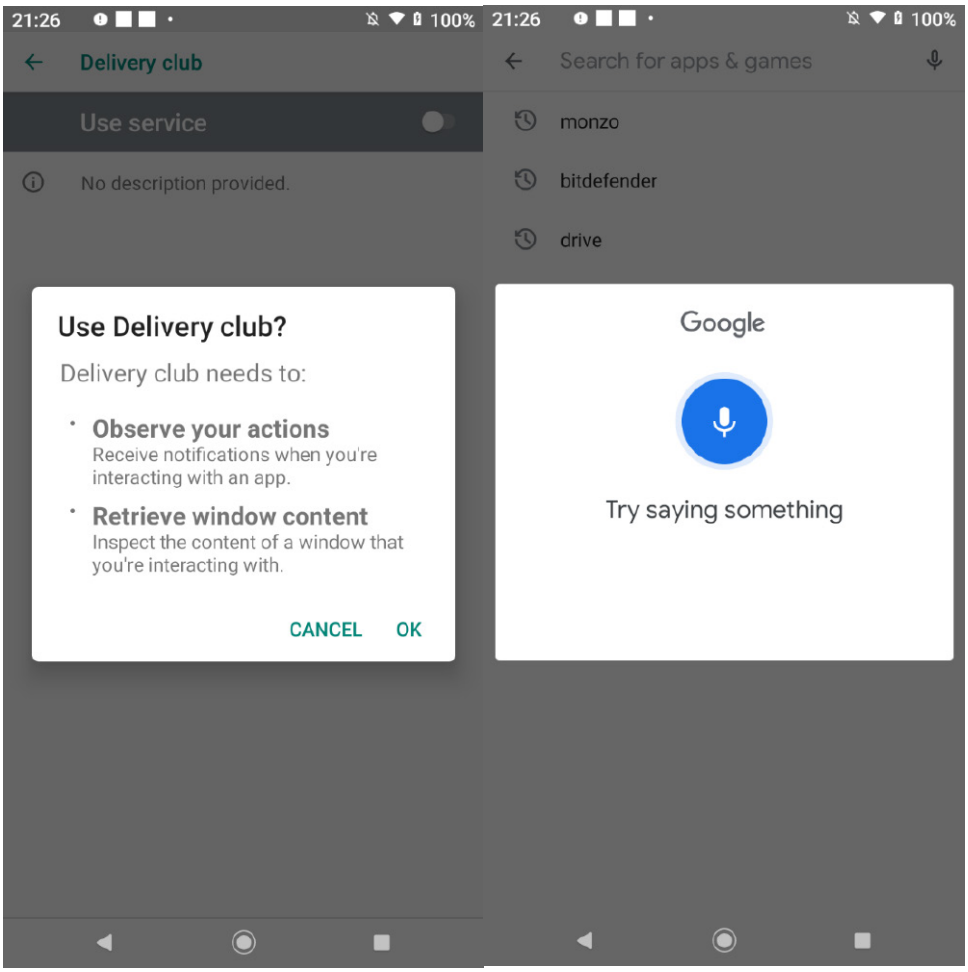
These apps have been found in the wild in the US and Germany.

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:

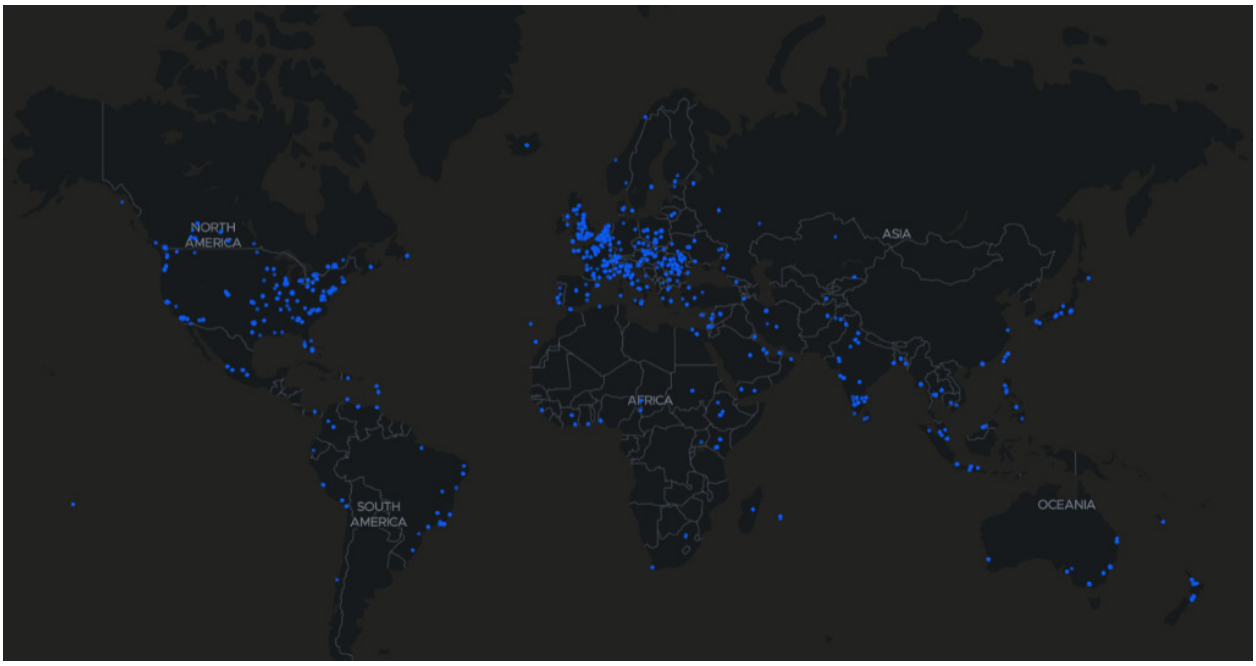
Asks for accessibility settings. When granted, it opens Google Play automatically and starts Google's speech recognition to search on Play, possibly to trick the user into believing that accessibility access is needed for speech recognition. It hides its icon. Drops Anubis in the background from assets.



The Command and Control Server is www[.]happynewyear666[.]xyz 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 labels:

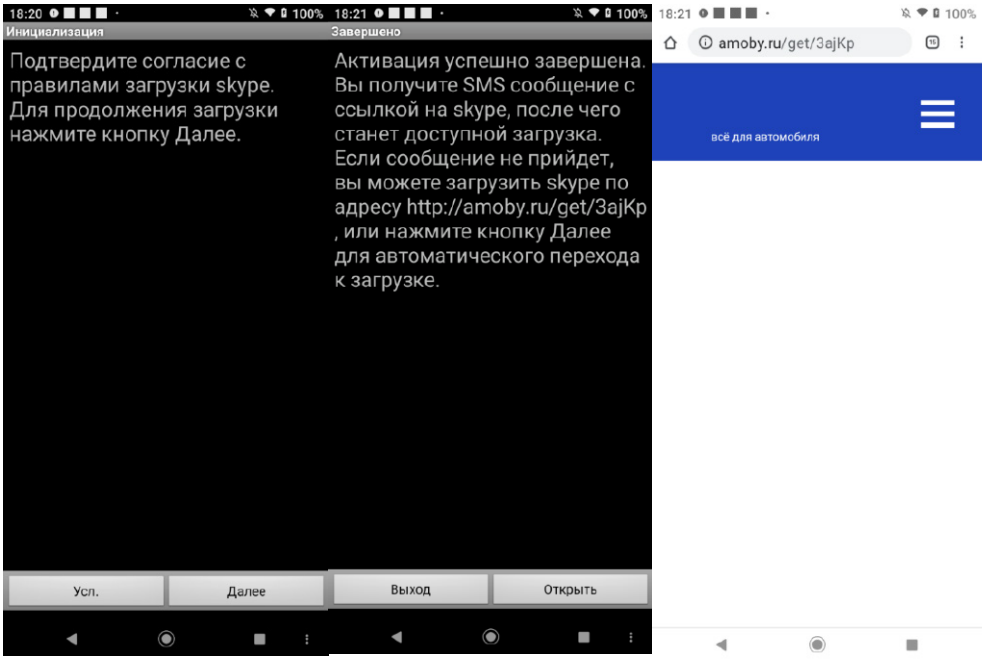
skype
Skype
skype-android
Skype - free IM video calls Hack
Skype для Android
Skype 9.3
Skype Mobile
Skype_2.7.0.907
Skype_Android
skype注册拉人进群组
skype自动语音广告
skypelite
skype改昵称
skype轰炸eric

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.FakeInst, 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.

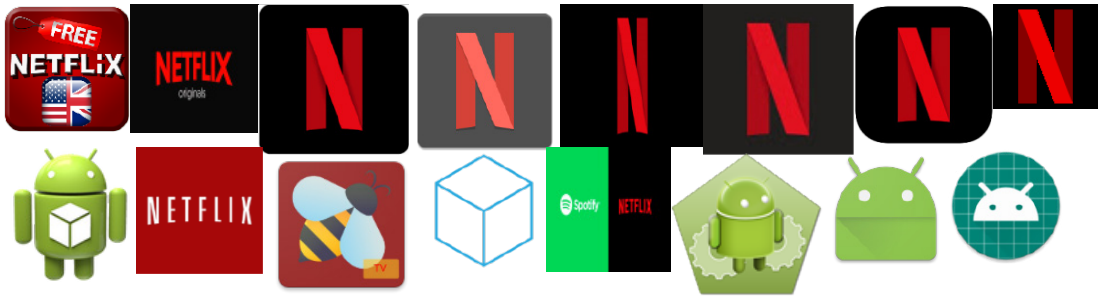
NETFLIX

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:

ChekerNetflix	Netflix Checker
free Netflix	Netflix Free
Free Netflix EN	Netflix hacked
Free Netflix Premium	Netflix hp
Netflix	Netflix Premium
netflix	Netflix Premium by APKMODY
NETFLIX	Netflix Premium by MODPLAY
NetFlix	NETFLIX UHD
Netflix-hacked	NETFLIX VPN V 2
Netflix-MOD-Final	Netflix.apk
Netflix 1	NetflixMOD
netflix 2	NetflixPlayer
Netflix 3	NetflixySpotify
Netflix App	pelis de netflix.com
Netflix by APKMODY	

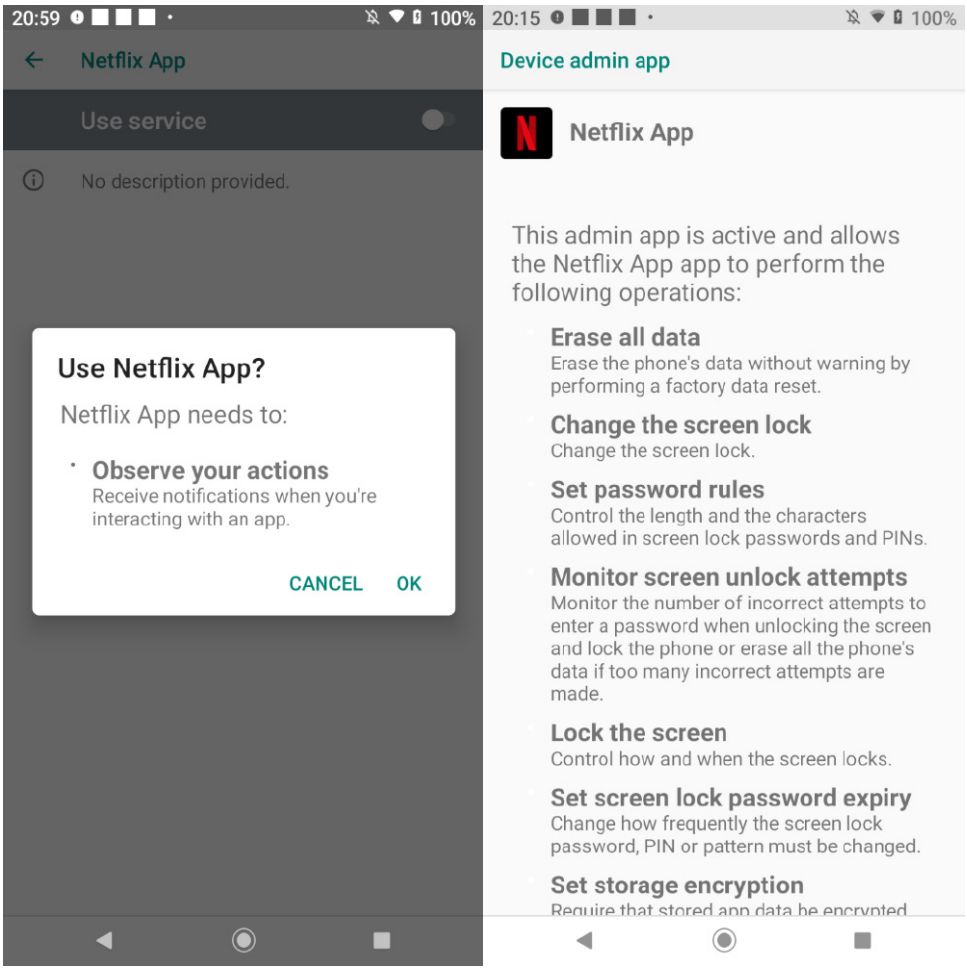
The fake applications come with various icons, some closer to the service's visual identity than others:



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:

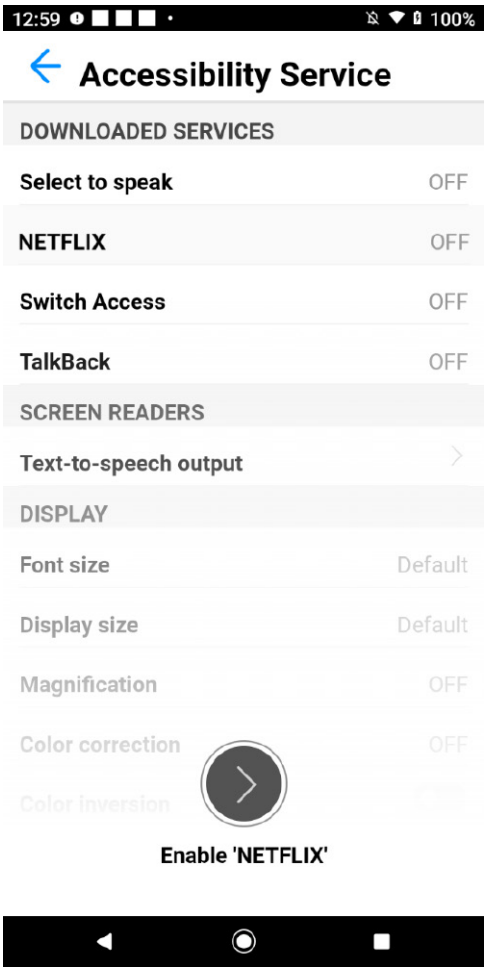
Domains	IPs	Location
spydark.ddns.net	105.159.8.252	Morocco, Tangier
blueboxi.ddns.net	-	-
hajilsaad.ddns.net	160.176.32.70	Morocco, Agadir
a7aa.ddns.net	197.59.115.31	Egypt, Cairo
wordswag.ddns.net	41.111.108.252	Algeria, Messaad
0.tcp.ngrok.io	3.19.3.150	US, Columbus
7aga.ddns.net	197.38.178.119	Egypt,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

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.uuclsnrtjxfeykitgzyp), 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*당신의모든범죄를잊을수는없어. 나는너에게나를해칠수있게 할 것이고*, 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.

```
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 Neflix's increasing popularity are DroidJack, AndroRAT and other types of spyware.

Indicators of Compromise

An up-to-date list of indicators of compromise is available to Bitdefender Advanced Threat Intelligence users. More information about the program is available at https://www.bitdefender.com/oem/advanced-threat-intelligence.html.

Fake Skype apps
092392cfde5823b7cfcb0231c125d2ca
6dc9504881a98bedaa1706a078935212
7f3ec9b57814a5e998bc6746c6d3c693
579255d3d98a94ce09981fd9d6f9ccaf
ad38eaf138bbdda5cfdf0c075b946c67
88ae31b95554cc3dc01e357bc3c87b74
2a75e863a608424d188af74d31b5ef1e
cac3a5ff4988499457138b11ecf265d8
23e062b7354560e6571d28749849ea11
58e06ea6a73cb56c51f423df7b411131
5bca7299fb146c4767349014dd2cf290
9aeb18dffc136ef1713f0ca949720cce
574363a1f8634ae5c0610a0987cd26fb
7e32eb63db3cfbe805486a62b62b0c21
3a1fb2d73b3bdc2fe01a689bd3e6b672
52670c7cd7fc1de383bc7fef5768571c
98b0d66c785c89f7de3ee82eb40d8857
453c218ac03d17ec5b820f7299a5244c
c6062b4c84ed293da92874654718d65a
ebd87e0227f4328eca606299c4c71c56
c7782fbb27ca989403b85df4e88fedc4
f98b1f682aeb34cd4c5d4e38620dfb29
fe72f991e3966aa4d12a598fb7cd2b93
f18dbe60f5b730f7d2acb2023a2676e0
d364262494d97a21d25b73b20e7b5bd3
e865d16eb974be99aff7a83531ab9289
e0dc1d5bbc73067c9f5bd01282660ba1
b62c93eaaa6b8def347bcee7d02bf693
8d79839cdbfcb6c3963270397cfef273
942c329e754b780a7b70571bc1711683
77448cfafac7f80d711f5324b7a4fb1f
345b91857efd4740a24dedd53222de09
e71c40a6c246c73d5c00a58719fd58e9
a00f1579e290fb19f5fa2d0f8135f877
cf4c7aa0e629d01d86f0ce5a00b99e4b
3daa21f0770eb4fd81c8e766b5e49512
d1181b043968f4d46f3643ce1dc591b8
445acb7e3c740b07877f69b043124582
a41c06fc1105f162b9ec35431bb01cad
47e34fac05cff612b5baa72beb753490
8626916dd40e1a43e3cebabd4f2969a5
798239e59688b9863e5c63cd650d1d43
3f954af5b772a8b6a4e625ff1a04c339
15d83d3295fd9daf20292d6e804ad94c
4d5984a83032a693fd702a7f4f16408f
7c0eca0fa4981d3d062accaeb48bb8fb
cfb5429fc32a8e68becd8068f904adce
15496dc7749a8fc06dde60898513f3c9
0fd9dd7a0d6dd3256c5319e215067faf
4be1c0a45302d5473ff78dcd90fa1e98
32e415a8b1d173e446251e866e94d70e
9e0e67a60cf2f8bd058d75404c5879a1

Fake Skype apps
3973f48cc9e4f4f2591e2478011520f9
a765ce1d9f9333425d300b5507b8d03b
3b911be1d14f3d497d4f854aad884c30
16c98b09ac9aa85bf2f90abfac3cdd66
0822fb4b48e358db7802fc4171828fb8
108ba6bbf981f1de7173e1e26aac60bc
52fffcece2cb701a2e4c98d30c27e184
cb2358c242687bd34da8b22a4a2b85b3
8d4ad2b2066ae3b4465dbc6109e03b14
c54155e444fa85925e026fb6329076cc
0c3def5d1573fe52bd5d90d5a25e6982
7695267f58acd4f0dcd85e457749946a
c0f6f4d88a39d6d081e78207b6daa2e0
8d2f9aaecf66f121dcadd63cf917b59b
0f55b59ef338441039d5e59b9cbb4be3
3fe0fd26c2476194510b3ab864561442
f87049c65418d7f6753b7e0f4a3455d0
78802229b62ad10fd99d69596e66aa90
f3b18a8175475d942308e86aaed5448e
18f425e3a15129a202b8cadb7c8706fe
b9b925793e7f41760bea40fac21da2b2
b1820532aa8bae01602ec65f1682fb61
fad9c7dde87abd247e35b96b16ffa844
34e0a1674c03e99b6a711bf2fdd019ba
418d3e507bb62a99e5c18dc3e89f103d
fc669416dd4b04f772e5cfd308abc3fc
fa40ce167b1b902554acb52e62bb7391
ca59cae18dff39d8f2ab588ee8ebec33
a8da3366be6be21391469c516dd48caa
db54ec7901457ff508abd94aa1dea97f
ae5d0f1eb7210355474a691d72b6b462
09461add8ab0f3045e181934c00682fa
40cd10ca7ae5e285526fd2c843ca47b3
7752ac5aee9199c6532a5faab22949cf
ae2038aace2f59fca7bbdc2b3e57fda2
7076a398d804985bb63b0ebc58f1204b
21353bdd143d60165a5e785eb64e352b
0d6100c81eb8ae1fd1a461962ff43850
31cb008a9eca28075c83bc99735c0b7c
9b4f54ba4b6f054f0c17aad8b6f25e05
7602b142b18795dc8450f6139b0cf2c8
146861b5951ebbe3b9a429dd6a9fc375
05184b8d66fff993d1298447def1cb65
f9dafbb8070eb27a16871ae5e35f305f
b66406cf2b6507f4e6fe8a19459f0146
117cfb772e162558bf3d50334288ef5b
3324102c6d15c445dea67fbc047f469a
8c9c95acb56cd50f07226dcce2dcb2ab
86c618e9b4e9a8f66998bedd2e247415
2d9337a1ad18ae79971d4414fd2f6da4
6e2c6f0258a5cff5cdea124f1a6e4b1e
c49212de0d0e737a1c94f7a08e2d7248

Fake Skype apps
6e50f05575a330e4744f7bc6ae29bce8
d80b8814b8e6e13678671a4ac6bf0d24
b10654fabd88e4775ac9dc3230a54afe
61c5aed9d34ec7fccc822aa48514d758
74f00f1abe6522445bd860877549a087
a871c4dc84a12546d733aabab9fd5c39
960a58f4df7257698f1ad66ebba5ef24
4790244354 71b8d81f825fa6c368bc76
75ee999642cbfe3b9fb912d1cd600e83
cf9e132734cd32fc2df64d1f80836ae5
b18ecdb18455271dcc7410f6338ffd3e
985afd6ae3d337ac915344080c8272b8
95aa24f62029ec095c69461173540b51
b0f55b5ea0f77510f81aa7f10760c3b3
49e3931b1ab6850571b4edd45c48cf5b
0c57d9c6db8234db8b5f84804538e491
099596be2ec82c0f5061a61fd3eca846
4759a1e683f6b7ce9b1abc97d6a5b446
9873485d9f13d60f381e4042d9ac3c50
d15cda7ae60ba96a243380f8904f56e3
edfc79a793648e59587a7d66387b69ee
ec9f401b7e84f4625fa058a05dd1aae4
48ff9bb66f4911f1c67ba709e623fb13
acba8fdc781923f3b4d9d51933134394
ce11a03e165d0ecfcd1b8259b16c43b8
157b93e5467aaa049a76ee5c3601dd74
6a640744ae3c2a5c1f1e25a76ec358d6
ab71fc8063abd72580ec9b190dc117e0
a2d6f4d0c7350eec0db19aa016b81a1b
c943a53c4c30d9a6205480508ce7a314
bc90f9a3f58795612ec85fa25911d0db
63562f10abd3f028c2dfbaedb75cc9b1
9dc567db812e5a85c43ab3d0c0a80809
c306eaf2e5175a0ac620e587a3ee560e
487d7c1705d43fbbc917990e86297d13
46106d08365116ad686df0c18a87ba9e
6d69e39f58bb3d54eb7f2dd46ac5953e
970772c9c53f8e6c0654ea572ff9758f
9d58fb2ae0327e602c3d7660440d55d4
9e7785e07755e831ee5b90c7271fcd6e
702d44c9654d45dff0fb2b263fb26785
b7828e18e78dd04be50a6758c4a214f1
239b1539b5214714fa07cd250d5e8f67
217e82c6e12c1a040f12fea6f54d703d
c999d3867d3dd483b9046e8f2871b779
3bc1a7c8ebdf2a162980cdb8ec1644b2
7e2db73b8389b19a63f53d7f088b6cf8
b6c5259f58522b3e4c579244df189aa7
3368de63d2e2762d5408056447db33d4
d63ed05792d23e6283a40c95ce1ce7c8
4e69b4472845f7556e7a2a205ac4179b
6cd34b4ecb762e6070645b32c90422ce

Fake Skype apps
612d37628bcffe45ba89ed62acdcdb15
6a27b55197c30f04c67f68061e20f424
13ce76ed40a4fdb00fa56c57904c5ffe
23d7c3dbdeabf3960ffbad8fc2038fc3
f58a3b2ffeb80a5e3a7b96519252a201
e6216c4ae5c66f855be3ccfa09f78b0c
3a74dfa62aaa0787ee5e4b09573e5ef0
81a98fd0446f51443f7e19ab5d34e4d1
d788b774ac06f9b66a25adfff988abc3
26c0e37a61e31a122b1c72006d78e148
a3b775c555b373a4b0c7c45d5094f391
543e1c6f2b643779a1d783d3bd39e15a
4d1bee08269b5f1c2813d345f98f0dc6
5cb3a9637d0323f872f59e1b803ff266
24312cc6cbb4dc4a342878d3230877db
fae54defd2f2395c36238bdc93a38d6a
70c17406f3711cadf577d04031d13735
1f86e06b91106ec80d0acdf3b3eeb747
d6bf72ee09a3d14cc421127bd43290f3
690631868055e865cc428a95a2fd7576
0e23f5725811bb1febb78799be0d3807
5da5a771b3946458bbc5418d5c736817
e34ee58df1a7e25dfa072ab67321605b
0e8b087dd0401abefeff04ba7e14a6e1
a96d5e9bf563b4d6b59db92488fac823
a8add46ff9e918725a45321182f91211
e920ce1c856eb5d15d5947f1b2aeadf6
5ec97182abc27effc0a8a3716e5a302d
4cf75b487c9a7500bbbcb4317b366b38
166ed2daca1dbade4cfaf61ef49e0c4d
1fe791f7400ba85b89182eace3c5a9f9
2b7b1a10d7aa868548f4832510c259bf
f60ec9af67d683d93f5c6710af38b621
588fb33883f0395c8babd61dc240228d
9a14e454fdc7fcf30968948a95ea9e2d
0c63bab53f98791e55b1b34867277584

Fake Netflix apps
ccb142d80be793e421240cbf4ab07cea
afc32454565dba47fbc297f81fcb2e29
1b4a4c2e3210f01090b8c91e3bd5093d
359f91c0a4fdca0c4e2fe99fec2e586d
bb11fc617c9b531ba225897cfb2457c
66b99be9e13243585a736c2dcc7dc889
2e611c42b6a47f535bf832b054ada8d7
0c54db597886c0c27cfe10976162280e
eee5d59f8edb178c6d9ce643dc65bed8
bd8b142b5a23f7d3de2864b8dc564077
34cb1f4e8978ffd845d273d02f242c1b
54d28714d2b0b3bee51b4502dc80a263
047bc70544efa2e54f18d4d08684506b
e225d8588d906ca96f3858cb7a5f7050
b22aafb69326168754bfc45a64c82b44
38e6b5ead068b043aa79403bd25aa349
6d7e13236390b534ff8ac40a2054f6e0
058ee417df2ac5d8bef33aeafed3a211
96dd97eba0331d45a0aa9d4653ff65ff
519e90a27ab698248045db6a4a0aee98
d532728f31ce3d4007cbc3b3508157be
f5886519afbafd26b4e915ee9769ebf9
a714beb969a23aaaf4fc0fe2c3d575df
736f0e60313f0fe1dfa17162f26b6b28
aa777d159ddc97ad9044af591c287284
63a4275303dd8d3bd3a365758936676a
45004337635055eee5bfc4d01b7727e1
a1c6869a3a7990d4abf72faf334bb66a
0fd9b050c934ec4a09c6348e92d8c10b
9df1fe26ac5c907e50ee6ca4ae890f46
fceff334befad7e1dab384d3bce672ef
8051600de0c44a9982c2dc8a09f09e1d
e5f7ba0af844a44b5b67ce09ce876789
27297f9427af31197f6b05b906812004
722a4af04cd1e01dee4037384f31174f
8f8d1b2b1eafd666e4ba64a1bc5981c0
9c3b7da8b3dfeb9ef6d06eba9d75b0ed
7a95e3c3995565e5a3db8c81c28eb9f8
d6d9133059deb171b764d02dd96dc424
2ab8b7415ee9d27c66fe96054df1aab4
ae298377eb2cb5a4bf4fa78c0270876c
e8504cf11db57652a61f9d4ad02cd376
ff674a53c20321b1922918b7f70256f4
88c9166e410244dda2d708c887d53fe1
a6faf798af81e5b0df2cf4fce747d82b
3fbbc655db7509ba0b93b6a9850859f4
8e459486db1af4b884e9c09e27696b72
67700eaeb1ebd38380ec8e7b1d9b9851
b141d3aae08c81e2bb2610fa42ce90a3
729cf74df9e62a723f02ad58656f5336
eaa19a63b437c76d08b36bd5112da198
c819443b732a8b872f420ad741fcbd79
8582d52caa35f4d3f1408a4f7a1ce45f
9e563f9f0687bd8d632b86d56ef07ae5
8eb1b1bbd5cb46b124f9503376731f42
25679ae24604d810180e6955e5a69245
3ed5a8eb7cc625ff64b719bf4087ad83
d6f855f19aff36abd61043e62d2e3029
242d8511a112bd8d413388bf9c571e36
6541c3534267567c6c8119e17dfee4ab
de6b1f1c3733ed4feaf7ca6e1b1f323c
8cfff76dfeab767bedf4d56e27119bbc
a32a3666d827588eac02d4038da0e152
c68b6387880c5d484785660d10e6a3a6
86c597fe3a0b8817e1abad8e45740469
c8dfd65a28ce6252203769d1026db85f
447a3dcb6ec0a6fa3f2848279d0ec61f
60bc4bcc104779b3b0245fe48e9a1e6d
c5a78151058bcb10a7b80ecf9023c796
d7496d88c8f3e124c39e5395406beeff
9804f892bb34e5473def4945cfbb2833
ec649026f4d8e7325970af58c4b6a7dd
89406be6e16d81d21051e17a2c5cb2dc
b07ca0d715f2407883c6023662742c53
364cd9ab2f1dd01547ab9fcac75f7bca

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 AV Gartner 451 Research FORRESTER IDC GLOBAL

TECHNOLOGY ALLIANCES

Microsoft NUTANIX aws Pivotal Cloud Foundry CITRIX

Bitdefender

Founded 2001, Romania
Number of employees 1800+

Headquarters
Enterprise HQ – Santa Clara, CA, United States
Technology HQ – Bucharest, Romania

WORLDWIDE OFFICES
USA & Canada: Ft. Lauderdale, FL | Santa Clara, CA | San Antonio, TX | Toronto, CA
Europe: Copenhagen, DENMARK | Paris, FRANCE | München, GERMANY | Milan, ITALY | Bucharest, Iasi, Cluj, Timisoara, ROMANIA | Barcelona, SPAIN | Dubai, UAE | London, UK | Hague, NETHERLANDS
Australia: Sydney, Melbourne

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.

Bitdefender-THR-Whitepaper-Android-Apps-creat4408-en_EN
04/14/20 April 15, 2020 2:18 pm 04/15/20