

# Threat Actors Use Mockups of Popular Apps to Spread Teabot and Flubot Malware on Android

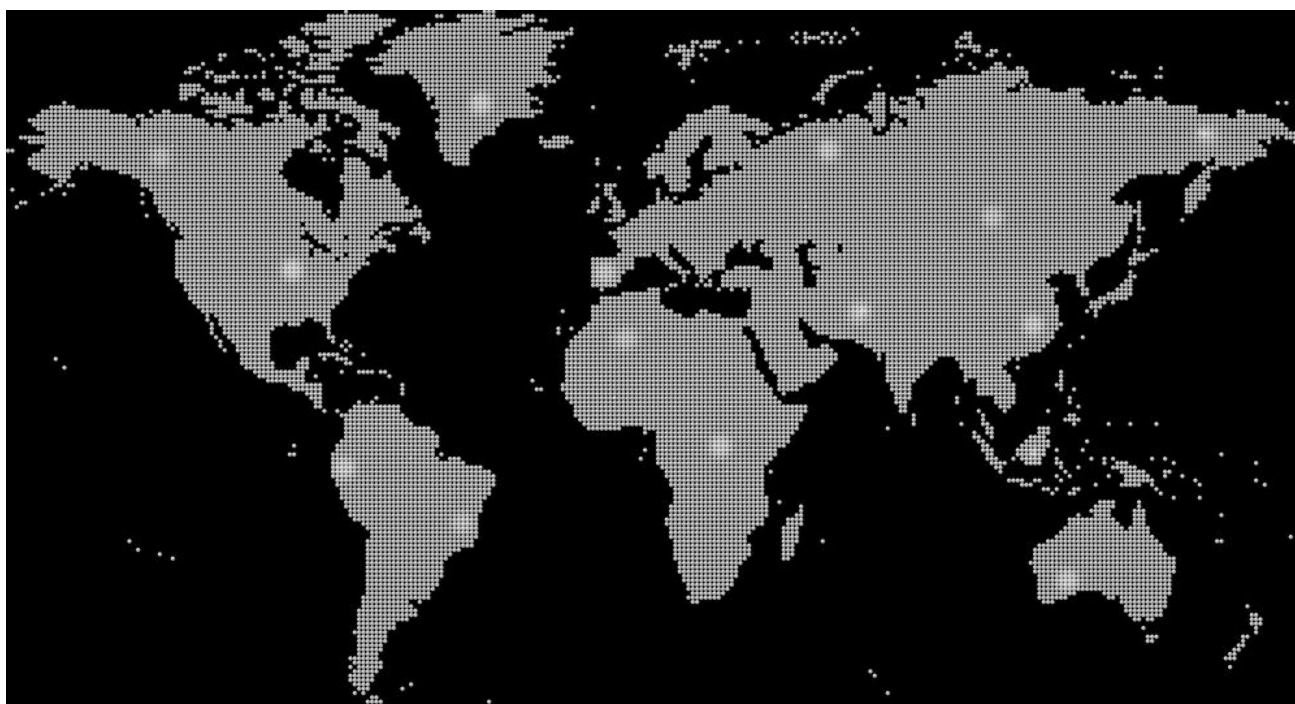
**B** [labs.bitdefender.com/2021/06/threat-actors-use-mockups-of-popular-apps-to-spread-teabot-and-flubot-malware-on-android/](https://labs.bitdefender.com/2021/06/threat-actors-use-mockups-of-popular-apps-to-spread-teabot-and-flubot-malware-on-android/)

## Anti-Malware Research

9 min read

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

[Free 90-day trial](#)



Spreading malware on Android devices is not easy, as the official store can usually (not always) prevent these types of apps from reaching users. But one of Android's greatest strengths, the ability to sideload apps from non-official sources, is also a weakness.

Using a combination of tricks to persuade users to install apps outside of the official store, criminals spread most of their malware through sideloading. If mobile devices have no security solution installed, malicious apps roam free.

The TeaBot and Flubot are the newest banker trojan families, as multiple security researchers identified them in the early months of 2021. Bitdefender researchers have discovered a batch of new malicious Android applications that impersonate real ones from popular brands but with a malware twist.

## **TeaBot Strikes Again**

---









TeaBot (also known as ‘Anatsa’) and its working mechanisms are known. According to an early analysis [report](#), the malware can carry out overlay attacks via Android Accessibility Services, intercept messages, perform various keylogging activities, steal Google Authentication codes, and even take full remote control of Android devices.

Criminals welcome the opportunity to spread malware directly from app stores, but that isn’t easy. Instead, they go for the next available method – imitating top-rated apps in the hopes of tricking at least some users into downloading and installing their malicious versions.





Bitdefender researchers have identified five new malicious Android applications that pack the Teabot banking trojan and impersonate real ones. Two of the apps are mentioned as banking malware on [Twitter](#), and we made the connection to the Anatsa malware.

The fake apps housing the Teabot payload are based on popular apps residing on Google Play, some with as many as 50M+ downloads. It’s no surprise that criminals try to take advantage and weaponize their popularity. The developers of the official apps have no fault in this matter.

The start of this fake malicious Android apps campaign dates to the beginning of December 2020, earlier than previously [identified](#). This was also indicated in a [tweet](#) when the original article was published.

<b>App label - infected version</b>	<b>App label – clean version</b>	<b>Clean app icon</b>	<b>Infected app icon</b>
Uplift: Health and Wellness App	Uplift: Health and Wellness App		
BookReader	Bookmate: Read Books & Listen to Audiobooks		
PlutoTV	Pluto TV - It's Free TV		
Госуслуги: Возврат НДС	Госуслуги		

---

Kaspersky: Free Antivirus	Kaspersky Antivirus: Security, Virus Cleaner		
VLC MediaPlayer	VLC for Android		

The campaign to distribute these apps in the wild remains active. Bitdefender has identified a strange distribution method with attackers using a fake **Ad Blocker** app that acts as a dropper for the malware. It's just one new distribution method. We suspect others are used, but they remain unknown for the time being.

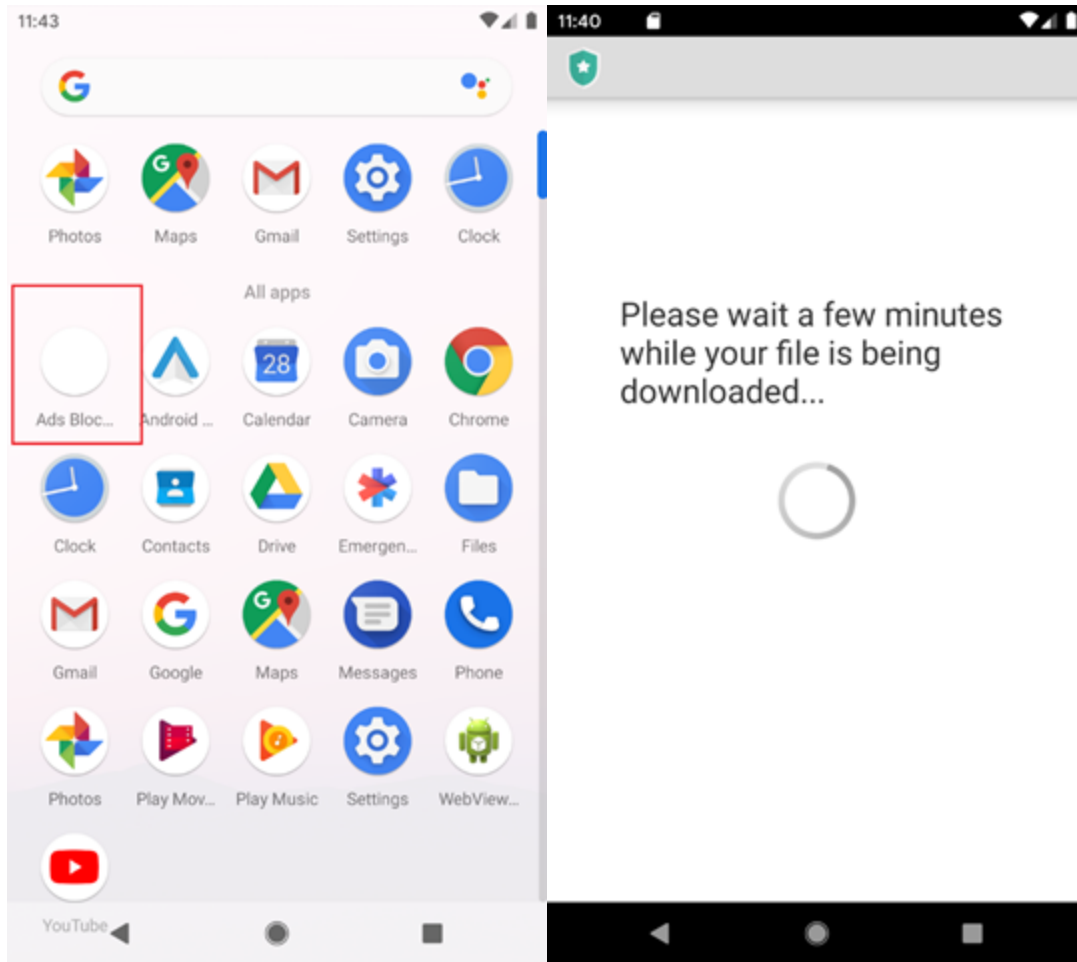
We put together a list of all banks targeted by the Teabot, but there's a caveat: Its operators can adapt it any given time, add more banks or remove support for some. The list is valid right now, but it's likely to change in the future.

App name	App package name
Bankia Wallet	com.bankia.wallet
BankinterMóvil	com.bankinter.launcher
BBVA Spain   Online banking	com.bbva.bbvacontigo
BBVA Net Cash   ES & PT	com.bbva.netcash
Kutxabank	com.kutxabank.android
Santander	es.bancosantander.apps
Bankia	es.cm.android
CaixaBankNow	es.lacaixa.mobile.android.newwapicon
Banca Digital Liberbank	es.liberbank.cajasturapp
Openbank – bancamóvil	es.openbank.mobile
UnicajaMovil	es.univia.unicajamovil
BBVA México (BancomerMóvil)	com.bancomer.mbanking
Banco Sabadell App. Your mobile bank	net.inverline.bancosabadell.officelocator.android

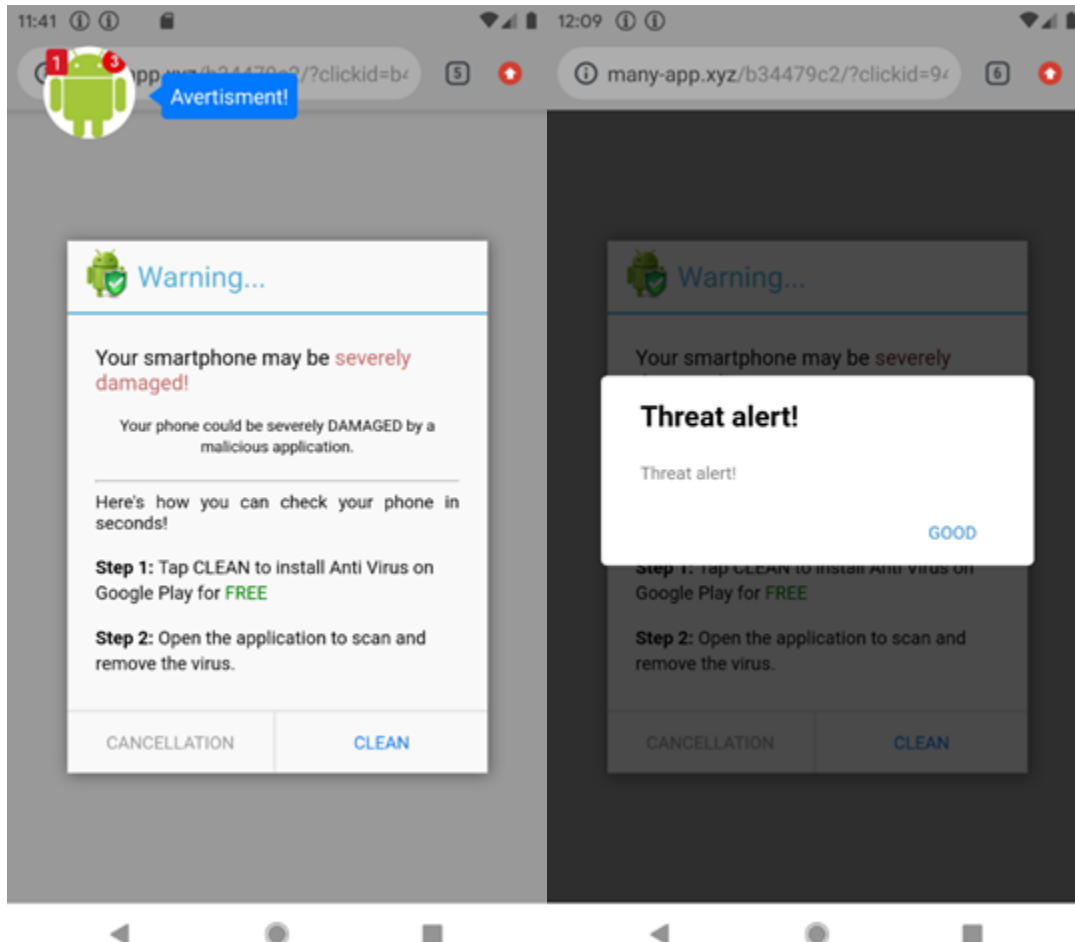
Commerzbank Banking – The app at your side	de.commerzbanking.mobil
comdirect mobile App	de.comdirect.android
Sparkasselhre mobile Filiale	com.starfinanz.smob.android.sfinanzstatus
Deutsche Bank Mobile	com.db.pwcc.dbmobile
Banco Sabadell App. Your mobile bank	net.inverline.bancosabadell.officelocator.android
VR Banking Classic	de.fiducia.smartphone.android.banking.vr
Cajasur	com.cajasur.android
GrupoCajamar	com.grupocajamar.wefferent
BW-Mobilbankingmit Smartphone und Tablet	com.starfinanz.smob.android.bwmobilbanking
Ibercaja	es.ibercaja.ibercajaapp
ING España. Banca Móvil	www.ingdirect.nativeframe

From Bitdefender’s telemetry, we were able to identify two new infection vectors, namely the applications with package names ‘com.intensive.sound’ and ‘com.anaconda.brave’, which downloads Teabot. These are malware dropper applications known for imitating legitimate applications (such as **Ad Blocker** in our case).

The fake Ad Blocker apps don’t have any of the functionality of the original version. They ask permission to display over other applications, show notifications, and install applications outside of Google Play, after which they hide the icon.



From time to time, the fake apps will show out-of-context ads and will eventually download and attempt to install Teabot, as instructed by the CnC.



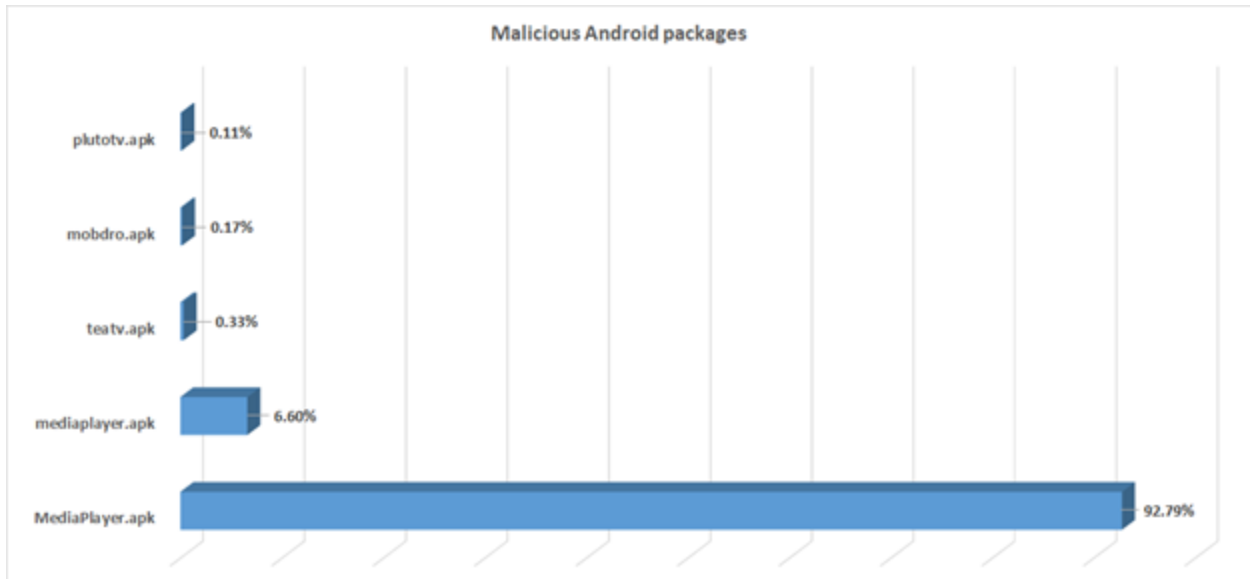
This is not a surprise; offering malware download as a service is a fairly common practice in the underground malware industry.

[/Android/data/com.intensive.sound/files/Download/MediaPlayer.apk](#)

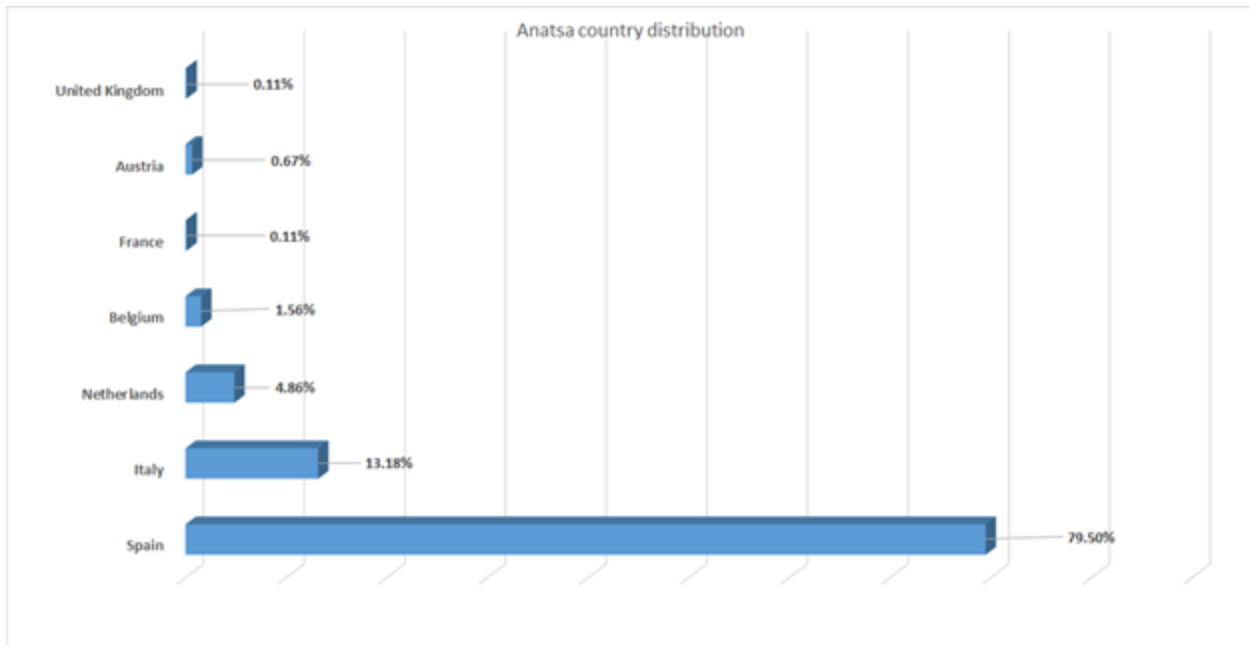
[/Android/data/com.anaconda.brave/files/Download/MediaPlayer.apk](#)

We detect these dropper applications with Bitdefender Mobile Security as Android.Trojan.HiddenApp.AID.

This is the current distribution, with an app simply named MediaPlayer ruling the landscape. But it's not the only one. As it turns out, the MediaPlayer.apk actually tries to impersonate one of the most famous multimedia players in the Google Play Store, named VLC. Security researchers from Cleafy were the first to identify the malware impersonating the VLC app.



The country distribution of Teabot is already known and rather interesting, with countries such as Spain, Italy and Netherland highly targeted.



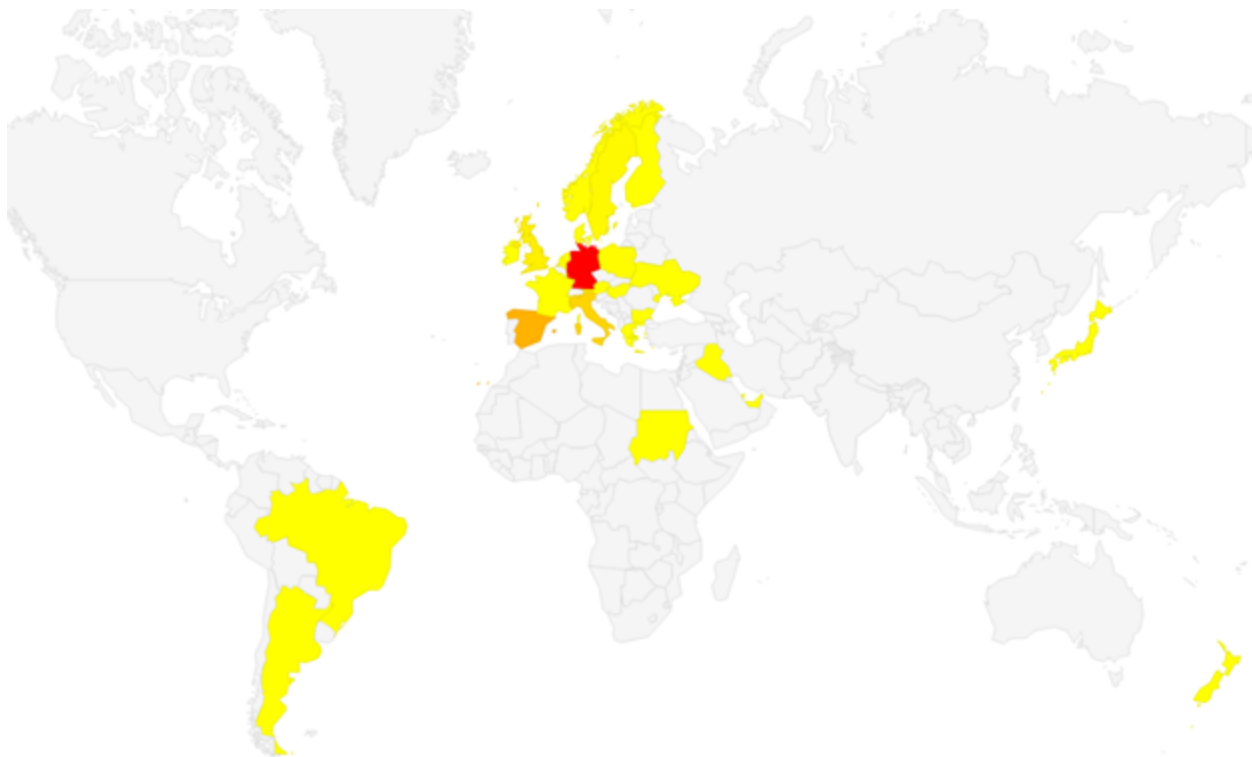
TeaBot heatmap distribution:



## FluBot is not far behind

---

Flubot (also known as Cabassous) is another banker family quickly gaining popularity. The heatmap shows that this family of banking trojans has been more successful in spreading internationally, predominantly in Germany, Spain, Italy and the UK.





Unlike Teabot, which is sometimes dropped by an app posing as an ad blocker, Flubot operators have a much more direct campaign, using spam SMS as a means of delivery.

While its malicious functionality is not as complex as Teabot's (which through accessibility logging enables threat actors to monitor the device in real-time), FluBot is still a banker trojan. It steals banking, contact, SMS and other types of private data from infected devices, and has an arsenal of other commands available, including the ability to send an SMS with content provided by the CnC.

Flubot uses that command to spread, through its SMS spamming and worm-like behavior. In our analysis, we have observed over 100 different domains used in the campaign to host the fake APK files. These domains belong to hacked/hijacked sites, where the threat actors injected their malware to spread further. In many cases, these are legitimate websites and domains that criminals have successfully attacked through existing vulnerabilities, allowing them to inject download links for malware.

Some examples of sent SMS:

Target victims	Samples of SMS sent to victims
Spanish speaking	Hola, Tiene (1) Paquete de Media Markt! Ref: UPS-20147 Ultima oportunidad para recogerlo>> <a href="http://wxz14[.]com/p/?o5l08o8nmt">http://wxz14[.]com/p/?o5l08o8nmt</a>
Spanish speaking	No hemos podido entregarte el paquete. Sigue el enlace para programar una nueva fecha de entrega: <a href="http://dukessailsoptin[.]com/info/?l7m4lnkvgp">http://dukessailsoptin[.]com/info/?l7m4lnkvgp</a>
Spanish speaking	FedEx: Tu envío está por llegar, rastrealo aquí: <a href="https://nsoft[.]fr/fedex/?apc9senmy3">https://nsoft[.]fr/fedex/?apc9senmy3</a>
Polish speaking	Dostawianowe przesyłki: <a href="http://thejoblessemperor[.]in/pkg/?6bh4l5qy">http://thejoblessemperor[.]in/pkg/?6bh4l5qy</a>

By looking at hundreds of SMS, we noticed that attackers use templates that only modify the recipient's name and download link. The malware steals real contact names and phone numbers from the victim's phone and sends them to servers hosted by the threat actors. The server composes the SMS message, using that real information and sends it back to the malware on infected phones. Flubot then sends SMS messages directly from the victim's device.

An observed example of such a template:

Hola<CONTACT\_NAME>, confirmes tus credenciales para la entrega de hoy, de lo contrario, el paquete será devuelto al remitente: <MALWARE\_DOWNLOAD\_LINK>

Example of Flubot SMS messages:

Hola**Ruben**, confirmesuscredenciales para la entrega de hoy, de lo contrario, supaquete sera devuelto al remitente: [https://defencelover\[.\]in/out/?iaw1g6md2w](https://defencelover[.]in/out/?iaw1g6md2w)

---




Hola**Marci**, confirmesuscredenciales para la entrega de hoy, de lo contrario, supaquete sera devuelto al remitente: [http://www.zyzlk\[.\]com/pack/?qq3s32hc4q](http://www.zyzlk[.]com/pack/?qq3s32hc4q)

---

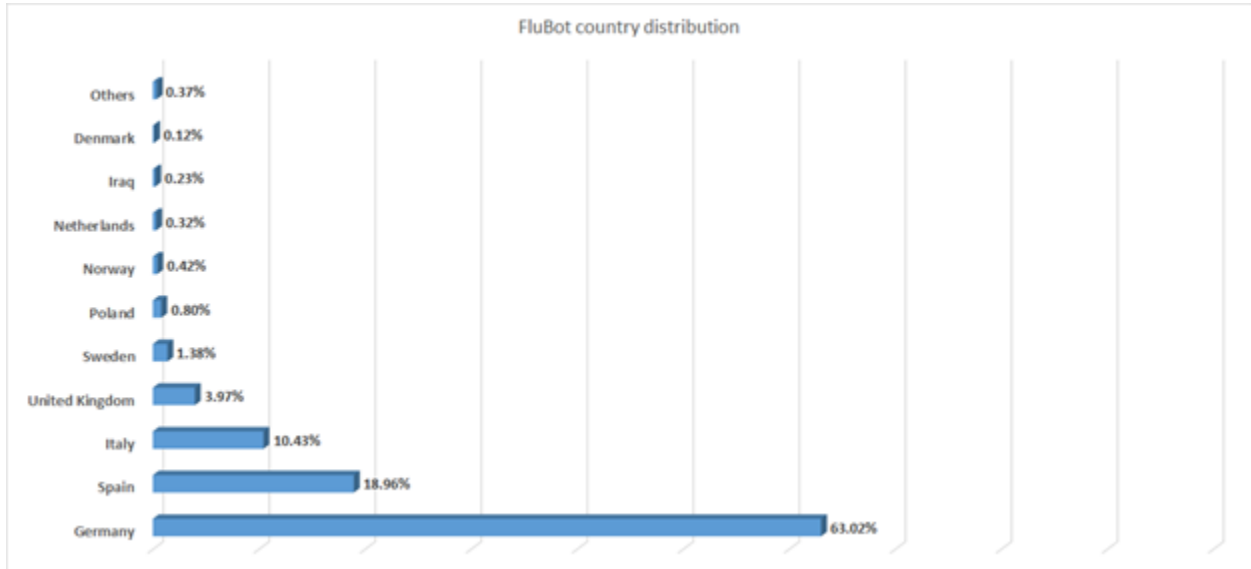
Hola**Ramiro**, confirmesuscredenciales para la entrega de hoy, de lo contrario, supaquete sera devuelto al remitente: [http://patchbuy\[.\]com/url/?rfzw0d1p8o](http://patchbuy[.]com/url/?rfzw0d1p8o)

Like in the case of Teabot, the FluBot operators go after banks and their apps, but the list of targeted apps can change at any time, as commanded by the attackers.

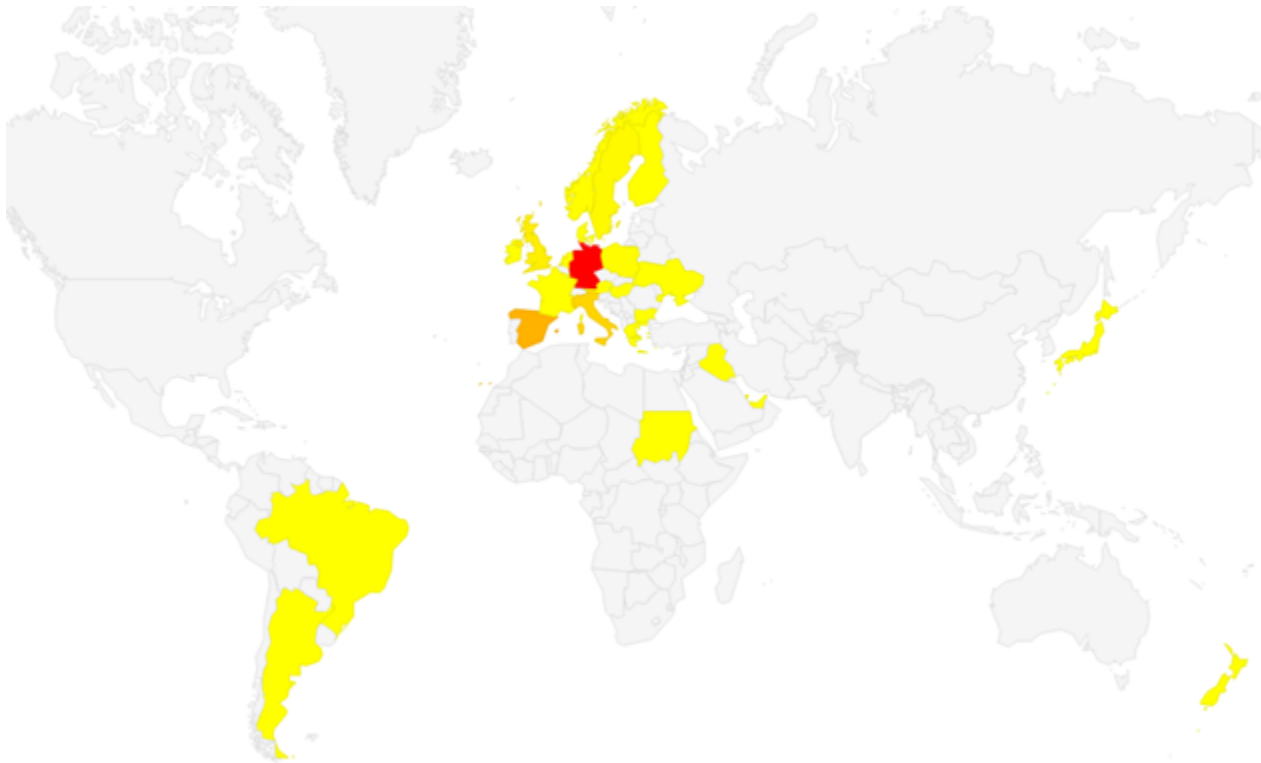
FluBot imitates the following apps, among others:

App label	App icon	Google Play Installs
DHL Express Mobile		1,000,000+
FedEx Mobile		5,000,000+
Correos		500,000+

This is a top 10 list of the countries where Bitdefender's telemetry identified the largest number of samples, but FluBot's reach extends to many others including Hungary, Japan, Ireland, Greece, Argentina, Austria, France and others.

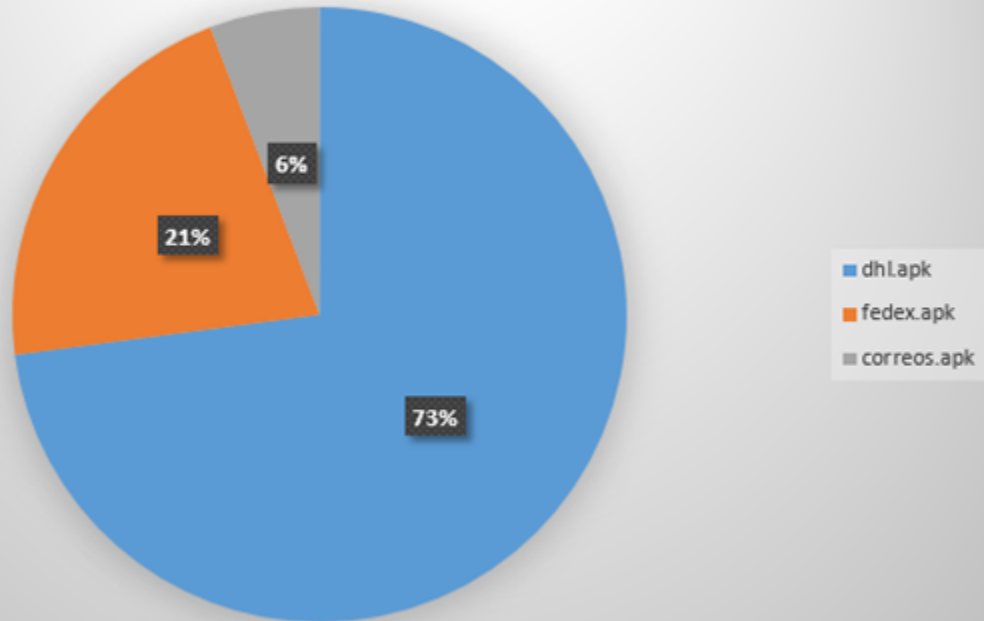


## Flubot heatmap



The file name distribution of Flubot is seen in this chart.

## Threat file name distribution ITW



### Indicators of compromise

MD5	Package name
4642c7a56039a82d8268282802c2fee9	trust.royal.vibrant
30ce352e03a873122ec9f701145893a7	double.slide.clip
a5ec451a40194e55765c77457b6060b1	where.reunion.subway
3cdc0c143454a50b8603a1b6c6d6d3e9	convince.achieve.syrup
730f22b9031a7987b4bed8e3a7487b6d	stereo.march.wire
43f8bd0078741b4fdc894b27ecd60a88	rebel.tragic.hazard
c20c6cd13bd8b5ccaca9e212635f7057	question.cancel.cradle

### CnCDomain – already mentioned

Pokymase[.]xyz

185[.]215[.]113[.]31

### CnCDomains – new

Jamelal[.]xyz

---

Foreannul[.]top

---

Forunkulosko2122[.]top

---

Peskoleonido9201[.]top

---

185[.]215[.]113[.]39

---

Biomakein202best[.]top

---

Losh190sup29asp[.]top

### Applications impersonated by Anatsa/TeaBot

---

App package name	App name	Google Play installs
org.videolan.vlc	VLC for Android	100,000,000+
tv.pluto.android	Pluto TV – It's Free TV	50,000,000+
com.kms.free	Kaspersky Antivirus: Security, Virus Cleaner	50,000,000+
ru.rostel	Госуслуги	10,000,000+
com.bookmate	Bookmate: Read Books & Listen to Audiobooks	1,000,000+
com.upliftwork.android	Uplift: Health and Wellness App	1,000+

### FluBot/Cabassous

---

The research on FluBot is extensive and approximately 1600 MD5 hashes have been identified by various teams. Here are three for some of the more widely circulated app tainted with the FluBot malware. Unfortunately, there are hundreds of compromised websites and domains, many of which are legitimate. Some of them are now offline, some have fixed the intrusions and deleted the malware, so listing them separately is not a viable solution.

#### MD5

#### Package name

---

fdcaa6e277c5ea7627b8fcfcc523f25b com.taobao.taobao

---

ff1575ee37bba19d2f0a8a0e6b2f6267 com.tencent.mm

---

fa40188a4db5620fc8fa72f83ffdc320 com.tencent.mm

### FluBotDroppers

---

**Package name**

---

com.intensive.sound

---

com.anaconda.brave

The best way to avoid infection with either of these two threats is never to install apps outside the official store. Also, never tap on links in messages and always be mindful of your Android apps' permissions. Finally, having a security solution such as Bitdefender Mobile Security installed on Android devices is recommended.

**TAGS**

---

[anti-malware research](#)

---

**AUTHOR**

---

**Silviu STAHIE**

---

Silviu is a seasoned writer who followed the technology world for almost two decades, covering topics ranging from software to hardware and everything in between.

[View all posts](#)

**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](#)



do a