CapraTube | Transparent Tribe's CapraRAT Mimics YouTube to Hijack Android Phones

sentinelone.com/labs/capratube-transparent-tribes-caprarat-mimics-youtube-to-hijack-android-phones/

Alex Delamotte

Executive Summary

- SentinelLabs identified three Android application packages (APK) linked to Transparent Tribe's CapraRAT mobile remote access trojan (RAT).
- These apps mimic the appearance of YouTube, though they are less fully featured than the legitimate native Android YouTube application.
- CapraRAT is a highly invasive tool that gives the attacker control over much of the data on the Android devices that it infects.

Background

Transparent Tribe is a suspected Pakistani actor known for targeting military and diplomatic personnel in both India and Pakistan, with a more recent expansion to the Indian Education sector. Since 2018, reports have detailed the group's use of what is now called CapraRAT, an Android framework that hides RAT features inside of another application. The toolset has been used for surveillance against spear-phishing targets privy to affairs involving the disputed region of Kashmir, as well as human rights activists working on matters related to Pakistan.

Transparent Tribe distributes Android apps outside of the Google Play Store, relying on self-run websites and social engineering to entice users to install a weaponized application. Earlier in 2023, the group distributed CapraRAT Android apps disguised as a dating service that conducted spyware activity.

One of the newly identified APKs reaches out to a YouTube channel belonging to Piya Sharma, which has several short clips of a woman in various locales. This APK also borrows the individual's name and likeness. This theme suggests that the actor continues to use romance-based social engineering techniques to convince targets to install the applications, and that Piya Sharma is a related persona.

CapraRAT is a comprehensive RAT that provides the actors with the ability to harvest data on demand and exfiltrate it. Notable features include:

- Recording with the microphone, front & rear cameras
- Collecting SMS and multimedia message contents, call logs
- Sending SMS messages, blocking incoming SMS

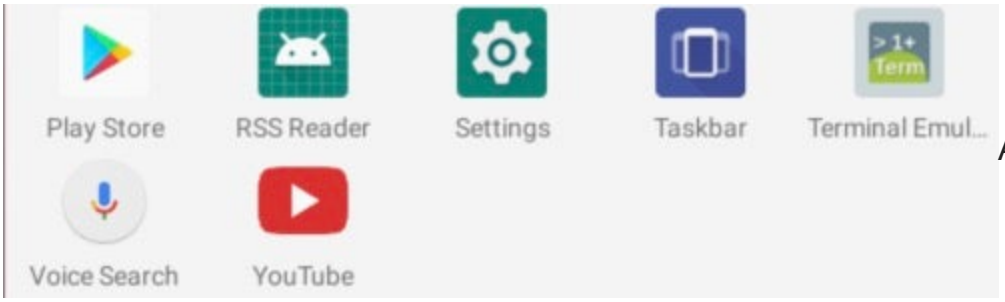
- Initiating phone calls
- Taking screen captures
- Overriding system settings such as GPS & Network
- Modifying files on the phone's filesystem

App Analysis

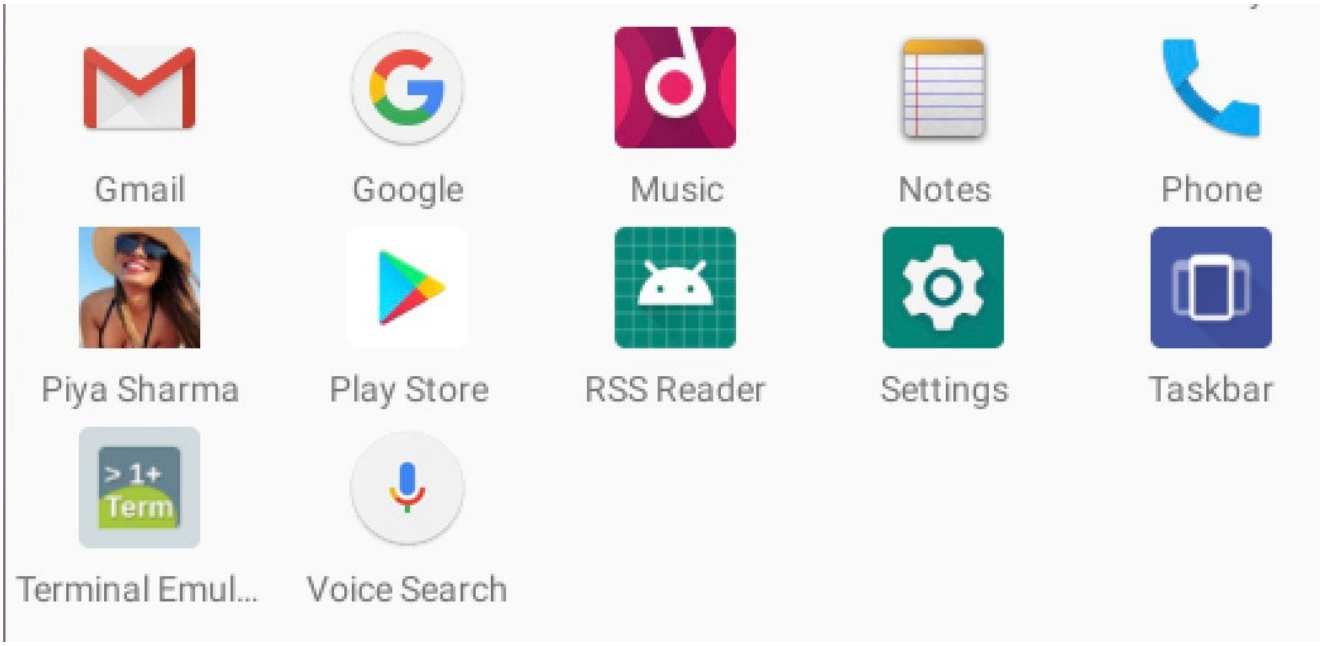
CapraRAT is distributed as an Android APK. When the tool was initially named by Trend Micro, their research team noted that CapraRAT may be loosely based on the AndroRAT source code.

We performed static analysis on two YouTube-themed CapraRAT APKs: `8beab9e454b5283e892aeca6bca9afb608fa8718` – yt.apk, uploaded to VirusTotal in July 2023. `83412f9d757937f2719ebd7e5f509956ab43c3ce` – YouTube_052647.apk, uploaded to VirusTotal in August 2023. We also identified a third APK called Piya Sharma, the YouTube channel persona described earlier: `14110facecceb016c694f04814b5e504dc6cde61` – Piya Sharma.apk, uploaded to VirusTotal in April 2023

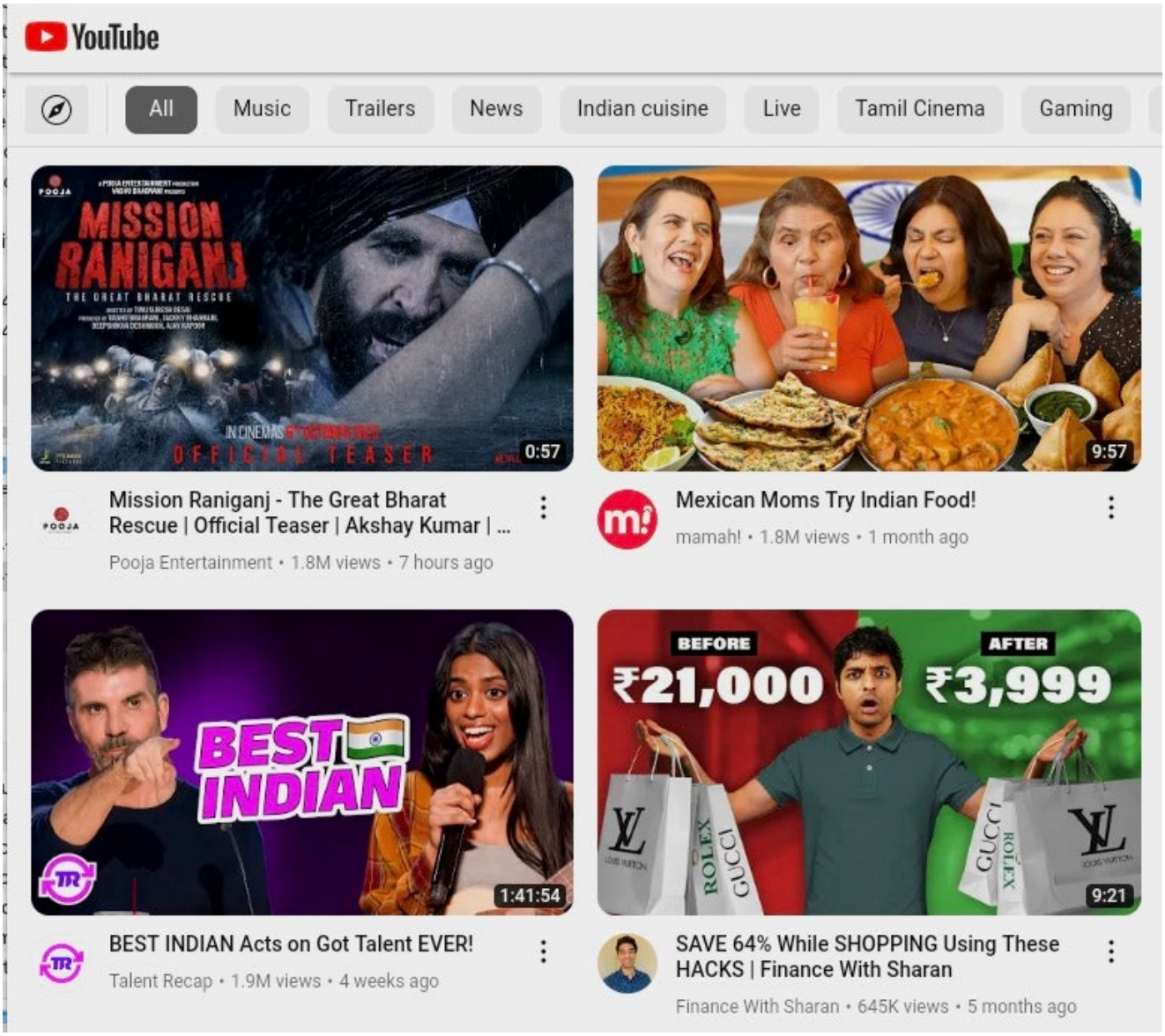
The yt and YouTube APKs apps are disguised as YouTube, borrowing the YouTube icon.



Applications icons on an Android device, including YouTube_052647.apk

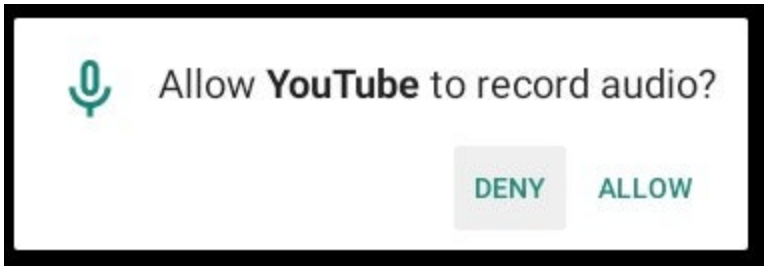


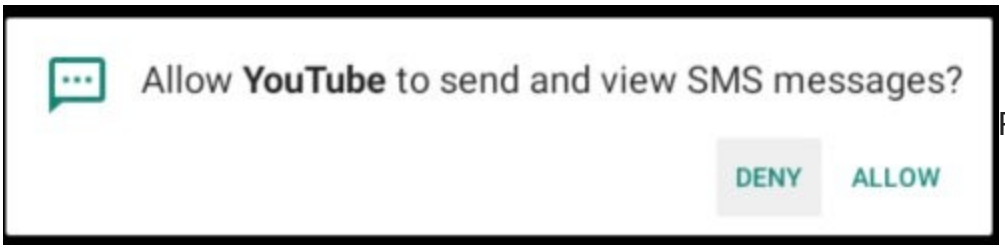
Application icons, including the Piya Sharma app



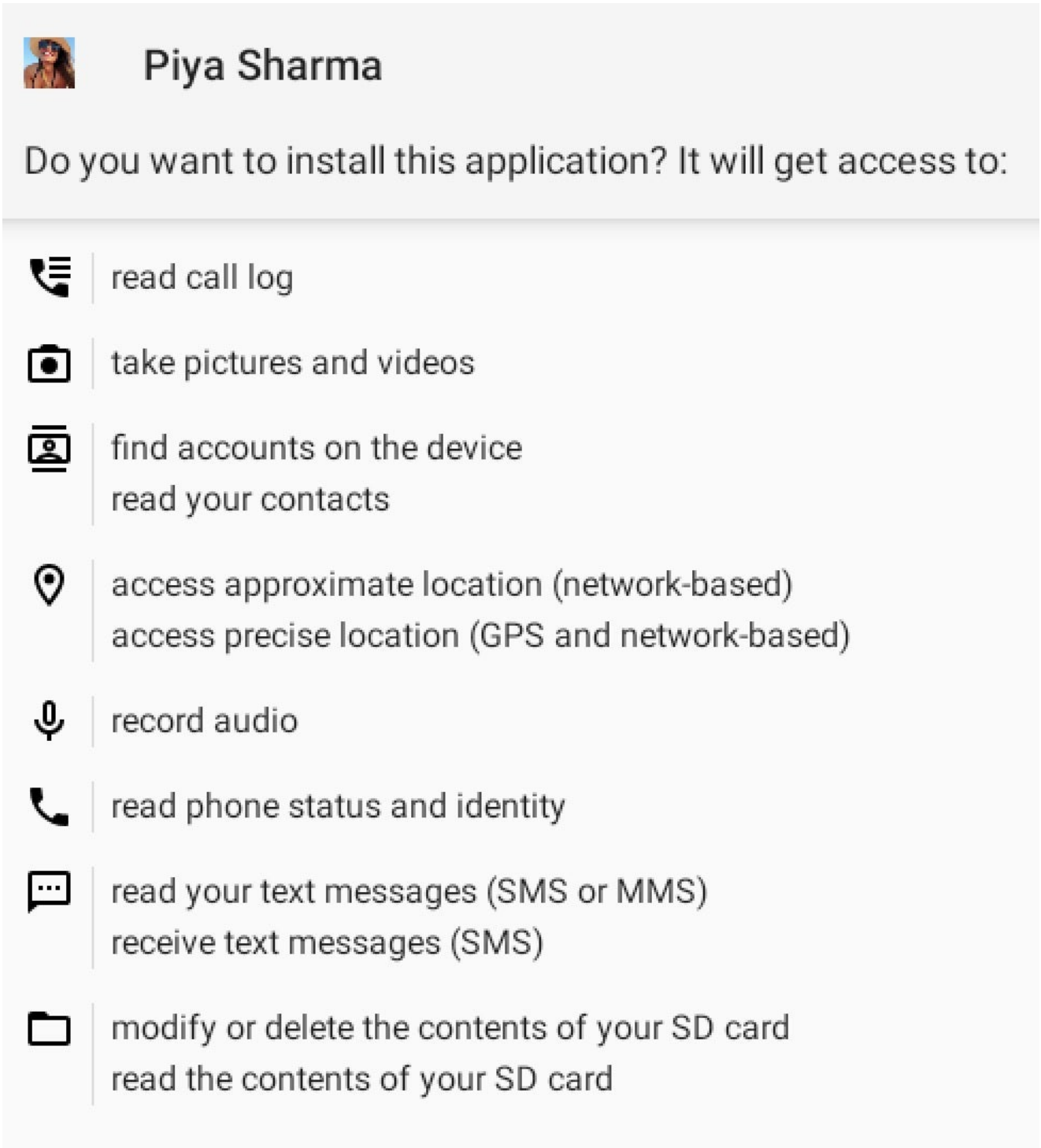
YouTube_052647.apk displays the YouTube website when launched

The app requests several permissions. YouTube is an interesting choice for masquerading the app: some permissions, like microphone access, make sense for recording or search features. Other permissions–like the ability to send and view SMS–are less relevant to the expected app behaviors.





Permissions prompts during install of the weaponized YouTube app



Installation permissions requested by the Piya Sharma APK

When the app is launched, `MainActivity`'s `load_web` method launches a WebView object to load YouTube's website. Because this loads within the trojanized CapraRAT app's window, the user experience is different from the native YouTube app for Android and akin to viewing the YouTube page in a mobile web browser.

```
.method private load_web()V
    .line 93
    :goto_0
    iget-object v0, p0, Lcom/Base/media/service/MainActivity;->webView:Landroid/webkit/WebView;

    const-string v1, "https://www.youtube.com/"

    invoke-virtual {v0, v1}, Landroid/webkit/WebView;->loadUrl(Ljava/lang/String;)V

    .line 95
    iget-object v0, p0, Lcom/Base/media/service/MainActivity;->webView:Landroid/webkit/WebView;

    invoke-virtual {v0}, Landroid/webkit/WebView;->getSettings()Landroid/webkit/WebSettings;

    move-result-object v0

    const/4 v1, 0x1

    invoke-virtual {v0, v1}, Landroid/webkit/WebSettings;->setJavaScriptEnabled(Z)V
```

Smali snippet of the *load_web* method in *MainActivity*

Key Components

Because CapraRAT is a framework inserted into a variety of Android applications, the files housing malicious activity are often named and arranged differently depending on the app. The CapraRAT APKs we analyzed contain the following files:

Name	yt.apk
Configuration	com/media/gallery/service/settings
Version	MSK-2023
Main	com/media/gallery/service/MainActivity
Malicious Activity	com/media/gallery/service/TPSClient

Name	YouTube_052647.apk
Configuration	com/Base/media/service/setting
Version	A.F.U.3
Main	com/Base/media/service/MainActivity

Malicious Activity	com/Base/media/service/TCHPClient

Name	Piya Sharma.apk
Configuration	com/videos/watchs/share/setting
Version	V.U.H.3
Main	com/videos/watchs/share/MainActivity
Malicious Activity	com/videos/watchs/share/TCPClient

CapraRAT's configuration file, which is named interchangeably `setting` or `settings`, holds the default configuration information, as well as metadata like versioning. The CapraRAT version syntax seen in YouTube_052647.apk and Piya Sharma.apk–`A.F.U.3` and `V.U.H.3`, respectively–matches the convention used to track Transparent Tribe's Windows tool, CrimsonRAT. However, there is no tangible relationship between these version numbers and the C2 domains as we saw in CrimsonRAT.

Thanks to creative spelling and naming conventions, the RAT's configuration provides consistent static detection opportunities, with each of the following present in the samples from earlier in 2023 as well:

```
is_phical
isCancl
isRealNotif
SERVERIP
smsMoniter
smsWhere
verion
```

`MainActivity` is responsible for driving the application's key features. This activity sets persistence through the `onCreate` method which uses Autostarter, an open-source project with code that lets developers automatically launch an Android application. The `TPSClient` class is initialized as an object called `mTCPService`; then, this method calls the `serviceRefresh` method, which creates an alarm at the interval specified in the settings file's `timeForAlarm` variable. In this example, the value **0xea60** is equal to 60,000 milliseconds, meaning the alarm and persistence launcher run once per minute.

The RAT's core functionality is in an activity similar to the `Extra_Class` activity from the March 2023 samples reported by ESET. Henceforth, we call this activity `TPSClient` for simplicity. These files are rather large, decompiling to over 10,000 lines of Smali code. By comparison, the March versions' equivalents have only about 8,000 lines.

`TPSClient` contains CapraRAT's commands, which are invoked through the `run` method via a series of switch statements that map the string command to a related method.

```
.method public run()V

    :sswitch_3d
    const-string v11, "smsmons"

    invoke-virtual {v9, v11}, Ljava/lang/String;->equals(Ljava/lang/Object;)Z

    move-result v9
    :try_end_0
    .catch Ljava/lang/Exception; {:try_start_0 .. :try_end_0} :catch_0

    if-eqz v9, :cond_6

    const/16 v9, 0x3a

    goto :goto_2

    :goto_1
    const/4 v9, -0x1

    :goto_2
    const-string v10, "/"

    const/4 v11, 0x0

    packed-switch v9, :pswitch_data_0

    goto/16 :goto_3
```

The *smsmons* command logic inside the *run* method of TPSClient

Many of these commands have been documented in previous research, though there are several changes in these new versions. The `hideApp` method now checks if the system is running Android version 9 or earlier and if the `mehiden` variable in the `setting(s)` config file was set to False; if applicable, the app will be hidden from the user's view. While similarities between CapraRAT and AndroRAT are seemingly minimal at this point in CapraRAT's development, the AndroRAT source code documentation notes that the tool becomes unstable after Android version 9, so there are likely underlying changes to the OS that make this method behave differently depending on the OS version.

`TPSClient` has a method `check_permissions()` that is not in `Extra_Class`. This method checks the following series of Android permissions and generates a string with a True or False result for each:

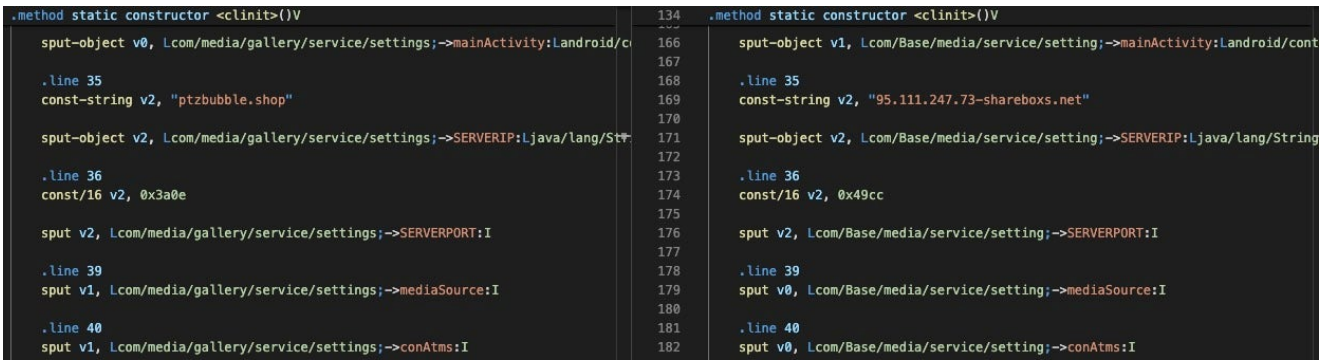
- READ_EXTERNAL_STORAGE
- READ_CALL_LOG
- CAMERA
- READ_CONTACTS
- ACCESS_FINE_LOCATION

- RECORD_AUDIO
- READ_PHONE_STATE

Interestingly, some other older versions contain this method, suggesting that the samples may be tailored for targets or are potentially developed from different branches.

C2 & Infrastructure

In CapraRAT's configuration file, the `SERVERIP` variable contains the command-and-control (C2) server address, which can be a domain, IP address, or both. The C2 port is in hexadecimal Big Endian format; the human readable port can be obtained by converting into decimal, resulting in port 14862 for yt.apk, port 18892 for YouTube_052647.apk, and port 10284 for Piya Sharma.apk.



```
.method static constructor <clinit>()V
    sput-object v0, Lcom/media/gallery/service/settings;->mainActivity:Landroid/c

    .line 35
    const-string v2, "ptzbubble.shop"

    sput-object v2, Lcom/media/gallery/service/settings;->SERVERIP:Ljava/lang/St

    .line 36
    const/16 v2, 0x3a0e

    sput v2, Lcom/media/gallery/service/settings;->SERVERPORT:I

    .line 39
    sput v1, Lcom/media/gallery/service/settings;->mediaSource:I

    .line 40
    sput v1, Lcom/media/gallery/service/settings;->conAtms:I
```

```
134 .method static constructor <clinit>()V
166     sput-object v1, Lcom/Base/media/service/setting;->mainActivity:Landroid/cont
167
168     .line 35
169     const-string v2, "95.111.247.73-shareboxs.net"
170
171     sput-object v2, Lcom/Base/media/service/setting;->SERVERIP:Ljava/lang/String
172
173     .line 36
174     const/16 v2, 0x49cc
175
176     sput v2, Lcom/Base/media/service/setting;->SERVERPORT:I
177
178     .line 39
179     sput v0, Lcom/Base/media/service/setting;->mediaSource:I
180
181     .line 40
182     sput v0, Lcom/Base/media/service/setting;->conAtms:I
```

C2 configuration from yt.apk (left) and YouTube_052647.apk (right)

The `shareboxs[.]net` domain used by YouTube_052647.apk has been associated with Transparent Tribe since at least 2019. Interestingly, the `ptzbubble[.]shop` domain was registered the same week of ESET's report outlining the group's Android apps that leveraged other C2 domains.

The IP addresses associated with C2 from the two YouTube samples have Remote Desktop Protocol port 3389 open with the service identified as Windows Remote Desktop, indicating the group uses Windows Server infrastructure to host the CapraRAT C2 application. The Piya Sharma app's C2 IP, `209[.]127.19.241`, has a certificate with common name value `WIN-P9NRMH5G6M8`, a longstanding indicator associated with Transparent Tribe's CrimsonRAT C2 servers.

`84[.]46.251.145`–the IP address hosting `ptzbubble[.]shop` domain–shows historical resolutions associated with Decoy Dog Pupy RAT DNS tunneling lookups. Any connection between these campaigns is unclear; it is plausible that a service hosted on this IP was infected by that campaign. Based on the query dates, the `claudfront[.]net` lookup was during the time the CapraRAT actor was using this IP address to host `ptzbubble[.]shop`, while a lookup to `allowlisted[.]net` was in December 2022, which was potentially before this actor started using the IP.

Resolve	First	Last
ptzbubble.shop	2023-05-13	2023-09-10
vmi1232940.contaboserver.net	2023-06-18	2023-09-07
326eeg.easypanel.host	2023-03-09	2023-07-25
zzokjni9.ahxx5vaminzfi4rrh64owtd6b5ba9999.hx5xtilnrusmj1kapg5epiy9.claudfront.net	2023-07-02	2023-07-02
*.326eeg.easypanel.host	2023-05-21	2023-05-21
test.ispdashboard.com	2023-02-24	2023-02-24
vmi1175215.contaboserver.net	2023-02-24	2023-02-24
145.251.46.84.mobile.mezon.lt	2016-11-14	2023-01-06
jy6qypq9.eyhzglvqrhypc6fpq4vwalu1rkia9999.gkdpp3fh25tqatj46yo2z5q9.allowlisted.net	2022-12-27	2022-12-27

Resolution history for IP hosting *ptzbubble[.]shop*, 84[.]46.251.145

Conclusion

Transparent Tribe is a perennial actor with reliable habits. The relatively low operational security bar enables swift identification of their tools.

The group's decision to make a YouTube-like app is a new addition to a known trend of the group weaponizing Android applications with spyware and distributing them to targets through social media.

Individuals and organizations connected to diplomatic, military, or activist matters in the India and Pakistan regions should evaluate defense against this actor and threat.

Defensive and preventative measures should include:

- Do not install Android applications outside of the Google Play store.
- Be wary of new social media applications advertised within social media communities.
- Evaluate the permissions requested by an application, particularly an application you are not particularly familiar with. Do these permissions expose you to more risk than the potential benefit of the app?
- Do not install a third-party version of an application already on your device.

CapraRAT malware is fully detected by SentinelOne's Singularity Mobile solution.

Indicators of Compromise (IOC)

Files Hashes – SHA1

14110facecceb016c694f04814b5e504dc6cde61 – Piya Sharma APK
83412f9d757937f2719ebd7e5f509956ab43c3ce – CapraRAT, YouTube_052647.apk
8beab9e454b5283e892aeca6bca9afb608fa8718 – CapraRAT, yt.apk

C2 Network Communications

newsbizshow.net
ptzbubble.shop
shareboxs.net

95[.]111.247.73
209[.]127.19.241