Love scam or espionage? Transparent Tribe lures Indian and Pakistani officials

welivesecurity.com/2023/03/07/love-scam-espionage-transparent-tribe-lures-indian-pakistani-officials/

March 7, 2023

ESET researchers analyze a cyberespionage campaign that distributes CapraRAT backdoors through trojanized and supposedly secure Android messaging apps – but also exfiltrates sensitive information

Lukas Stefanko
7 Mar 2023 - 11:30AM

ESET researchers analyze a cyberespionage campaign that distributes CapraRAT backdoors through trojanized and supposedly secure Android messaging apps – but also exfiltrates sensitive information

ESET researchers have identified an active Transparent Tribe campaign, targeting mostly Indian and Pakistani Android users – presumably with a military or political orientation. Victims were probably targeted through a honey-trap romance scam, where they were initially contacted on another platform and then convinced to use supposedly "more secure" apps, which they were then lured into installing. Most likely active since July 2022, the campaign has distributed CapraRAT backdoors through at least two similar websites, while representing them as untainted versions of those secure messaging apps.

Key points of the blogpost:

- **This Transparent Tribe campaign mainly targets Indian and Pakistani citizens, possibly those with a military or political background.**
- **It distributed the Android CapraRAT backdoor via trojanized secure messaging and calling apps branded as MeetsApp and MeetUp; the backdoor can exfiltrate any sensitive information from its victims' devices.**
- **These trojanized apps were available to download from websites posing as official distribution centers. We believe a romance scam was used to lure targets to these websites.**
- **Poor operational security around these apps exposed user PII, allowing us to geolocate 150 victims.**
- **CapraRAT was hosted on a domain that resolved to an IP address previously used by Transparent Tribe.**

Campaign overview

Besides the inherent working chat functionality of the original legitimate app, the trojanized versions include malicious code that we have identified as that of the CapraRAT backdoor. Transparent Tribe, also known as APT36, is a cyberespionage group known to use CapraRAT; we have also seen similar baits deployed against its targets in the past. The backdoor is capable of taking screenshots and photos, recording phone calls and surrounding audio, and exfiltrating any other sensitive information. The backdoor can also receive commands to download files, make calls, and send SMS messages. The campaign is narrowly targeted, and nothing suggests these apps were ever available on Google Play.

We identified this campaign when analyzing a sample posted on Twitter that was of interest due to matching Snort rules for both CrimsonRAT and AndroRAT. Snort rules identify and alert on malicious network traffic and can be written to detect a specific type of attack or malware.

CrimsonRAT is Windows malware, known to be used only by Transparent Tribe. In 2021, the group started to target the Android platform, using a modified version of an open-source RAT named AndroRAT. It bears similarities to CrimsonRAT, and has been named CapraRAT by Trend Micro in its research.

MeetsApp

Based on the Android Package Kit (APK) name, the first malicious application is branded MeetsApp and claims to provide secure chat communications. We were able to find a website from which this sample could have been downloaded (meetsapp[.]org); see Figure 1.

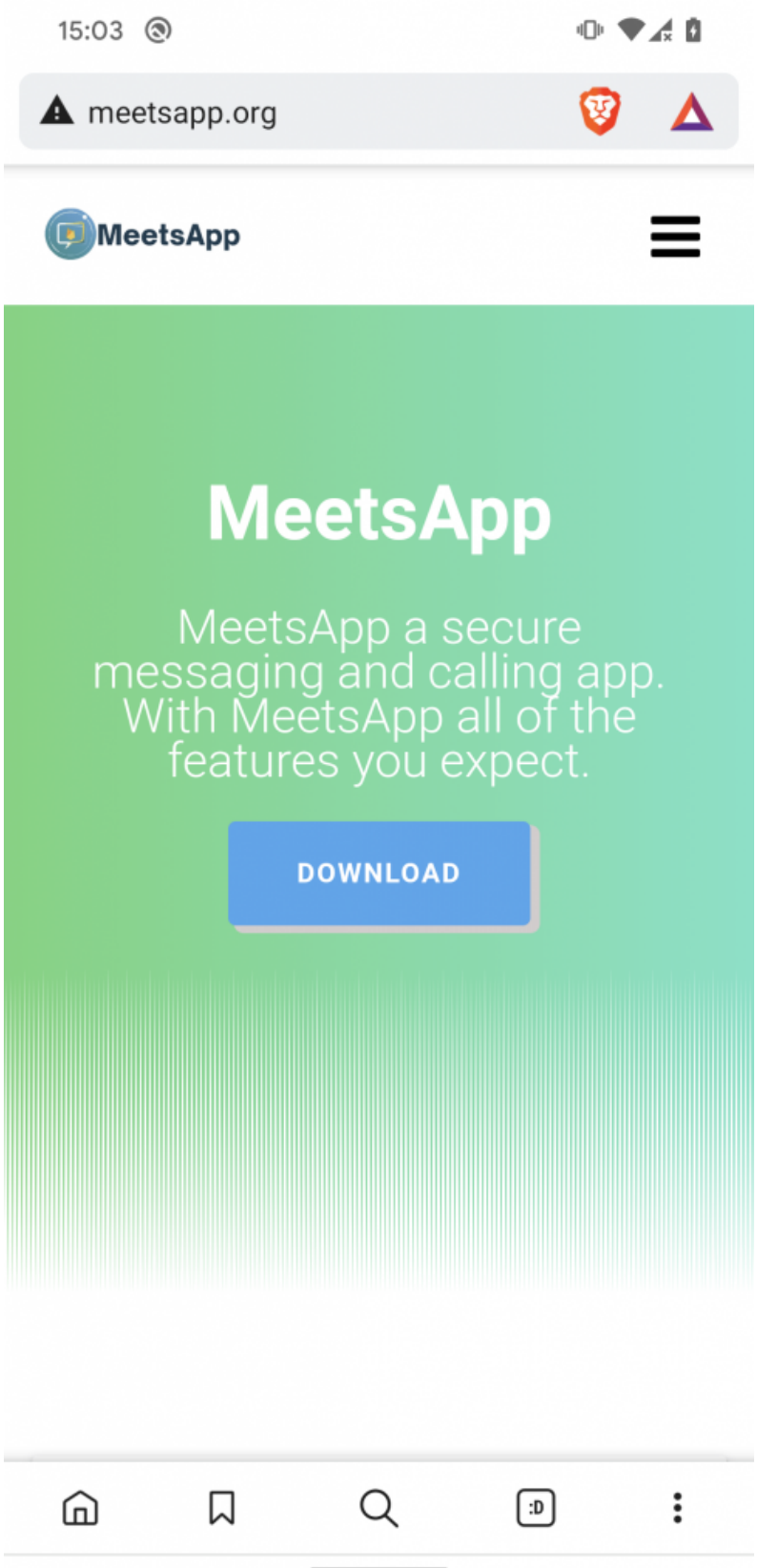

Figure 1. Distribution website of CapraRAT posing as MeetsApp

That page's download button leads to an Android app with the same name; unfortunately, the download link is not alive anymore (https://phone-drive[.]online/download.php?file=MeetsApp.apk). At the time of this research, phone-drive[.]online resolved to 198.37.123[.]126, which is the same IP address as phone-drive.online.geo-news[.]tv, which was used in the past by Transparent Tribe to host its spyware.

MeetUp

Analysis of the MeetsApp distribution website showed that some of its resources were hosted on another server with a similar domain name – meetup-chat[.]com – using a similar service name. That site also provided an Android messaging app, MeetUp, to download with the same package name (com.meetup.app) as for MeetsApp, and having the same website logo, as can be seen in Figure 2.

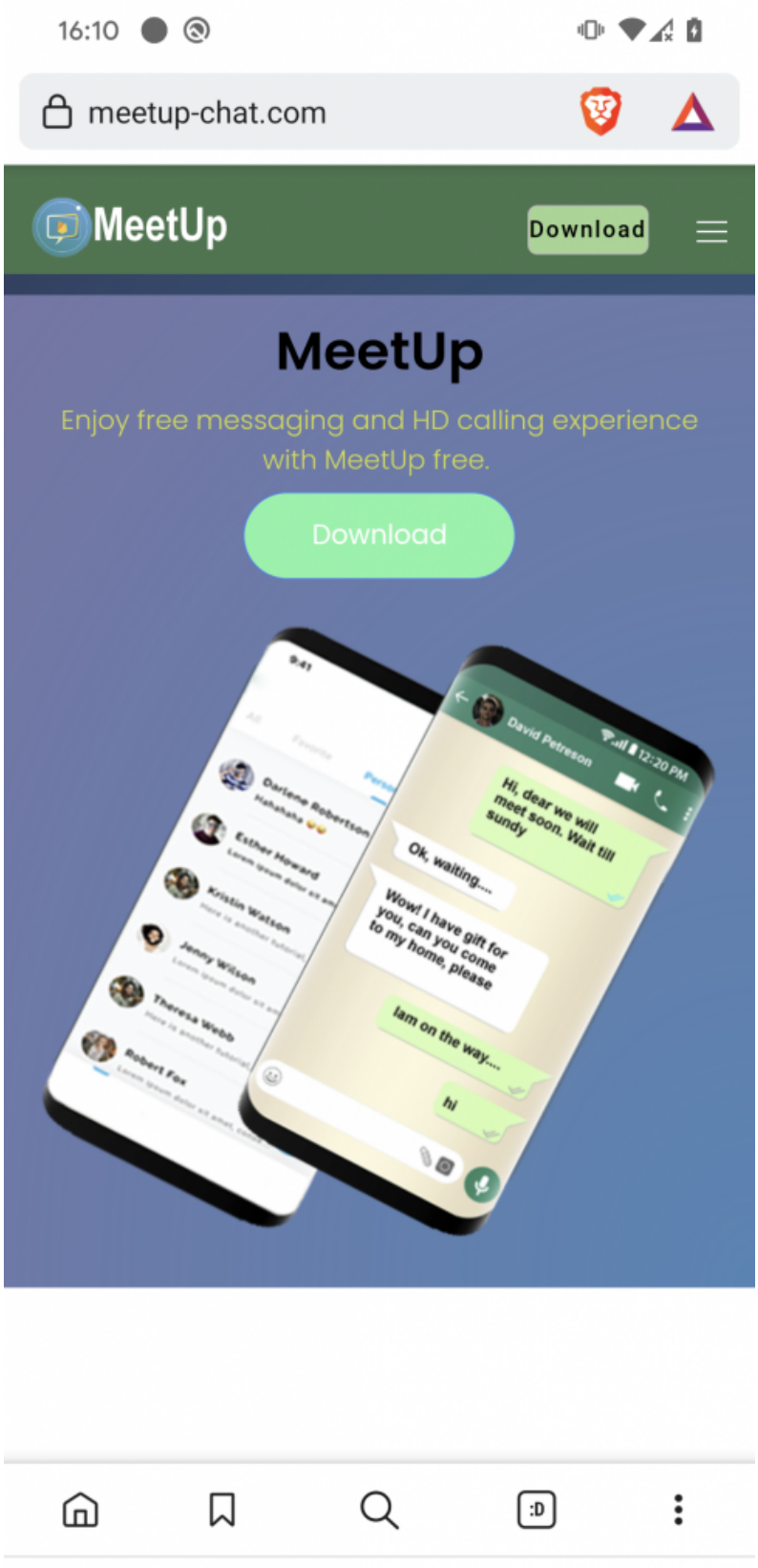

Figure 2. Distribution website of CapraRAT posing as MeetUp

Attribution to Transparent Tribe

Both apps – from the tweet and from the sample downloaded from meetup-chat[.]com – include the same CapraRAT code, communicate with the same C&C server (66.235.175[.]91:4098), and their APK files are signed using the same developer certificate.

Hence, we strongly believe that both websites were created by the same threat actor; both domains were registered around the same time – July 9th and July 25th, 2022.

Both apps are based on the same legitimate code trojanized with CapraRAT backdoor code. Messaging functionality seems either to be developed by the threat actor or found (maybe purchased) online, since we couldn't identify its origin. Before using the app, victims need to create accounts that are linked to their phone numbers and require SMS verification. Once this account is created, the app requests further permissions that allow the backdoor's full functionality to work, such as accessing contacts, call logs, SMS messages, external storage, and recording audio.

The domain phone-drive[.]online on which the malicious MeetsApp APK was placed started to resolve to the same IP address around the same time as the domain phone-drive.online.geo-news[.]tv that was used in the past campaign controlled by Transparent Tribe, as reported by Cisco. Besides that, the malicious code of the analyzed samples was seen in the previous campaign reported by Trend Micro where CapraRAT was used. In Figure 3 you can see a comparison of malicious class names from CapraRAT available from 2022-01 on left side, and its more recent variant having the same class names and functionality.

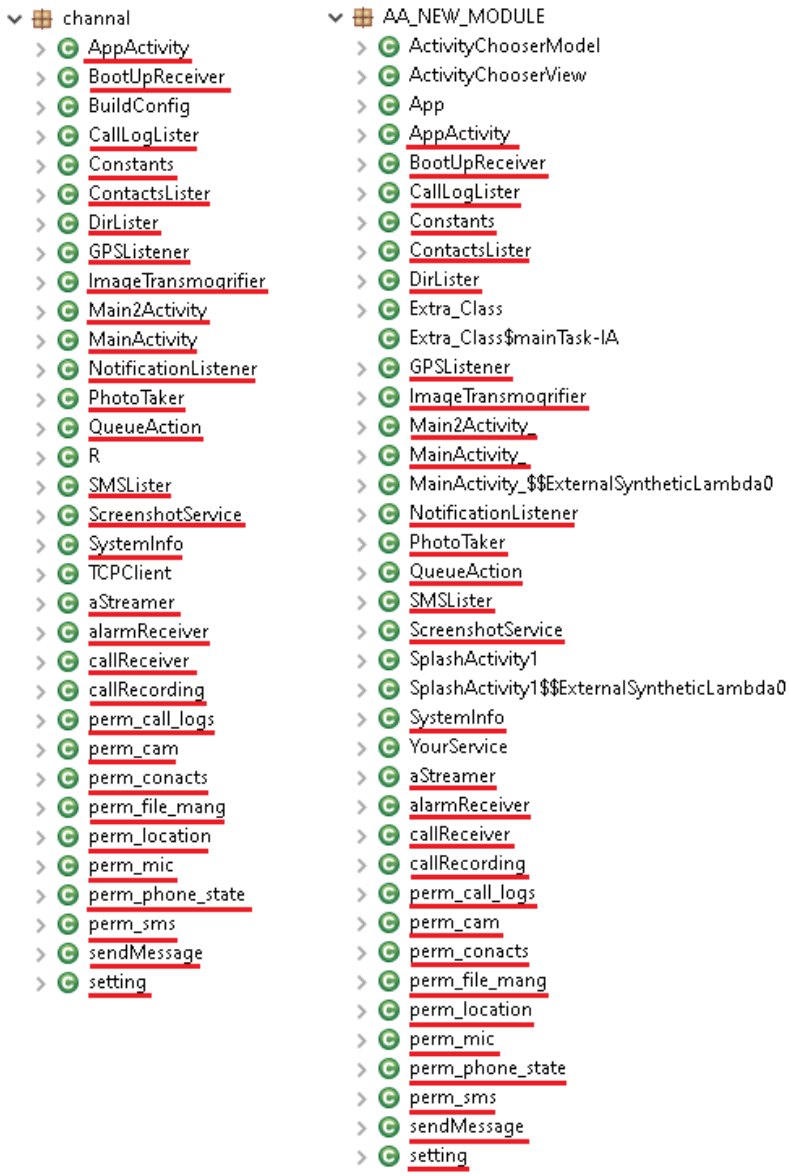

Figure 3. Malicious class name comparison of older CapraRAT (left) and more recent version (right)

Victimology

During our investigation, weak operational security resulted in the exposure of some victim data. This information allowed us to geolocate over 150 victims in India, Pakistan, Russia, Oman, and Egypt, as seen in Figure 4.

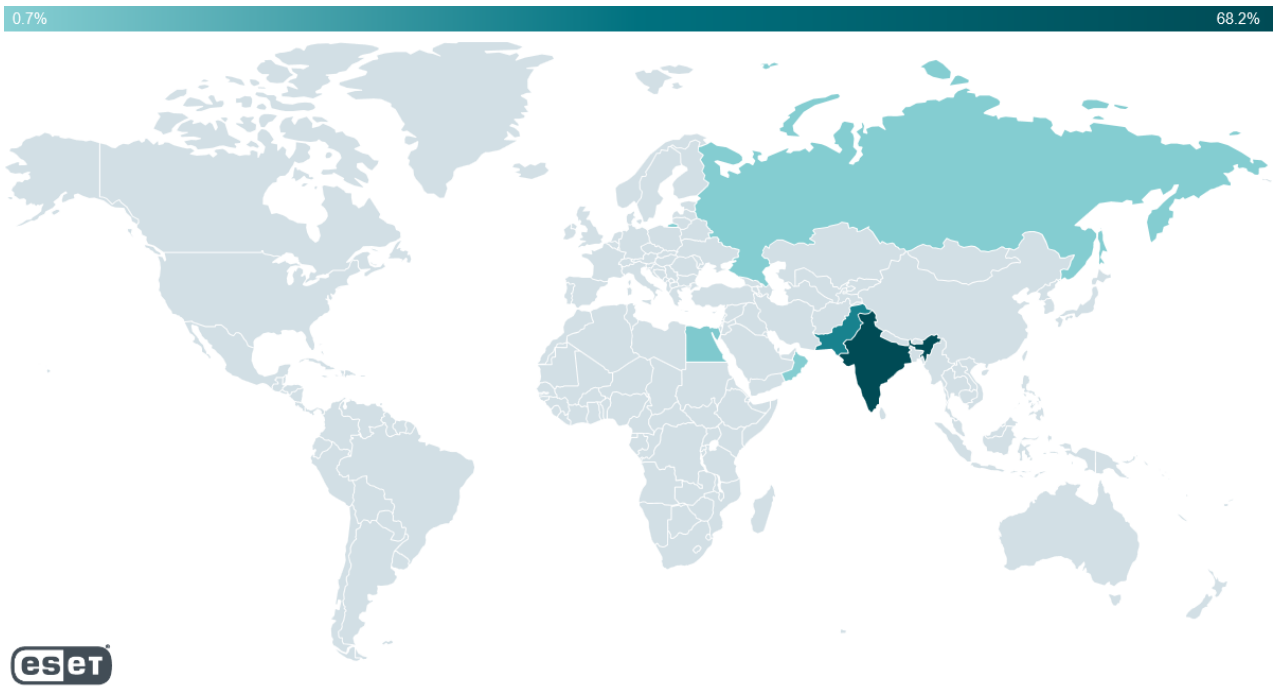

Figure 4. Victim distribution

Based on our research, potential victims were lured to install the app by a honey-trap romance scam operation, where most likely they were first contacted on a different platform and then persuaded to use the "more secure" MeetsApp or MeetUp app. We have previously seen such baits being used by Transparent Tribe operators against their targets. Finding a mobile number or an email address they can use to make first contact is usually not difficult.

Technical analysis

Initial access

As described above, the malicious MeetUp app has been available at meetup-chat[.]com, and we believe with high confidence that the malicious MeetsApp was available at meetsapp[.]org. Neither app would be automatically installed from these locations; the victims had to choose to download and install the apps manually. Considering that only a handful individuals were compromised, we believe that potential victims were highly targeted and lured using romance schemes, with Transparent Tribe operators most likely establishing first contact via another messaging platform. After gaining the victims' trust, they suggested moving to another – allegedly more secure – chat app that was available on one of the malicious distribution websites.

There was no subterfuge suggesting the app was available in Google Play.

Toolset

After the victim signs into the app, CapraRAT then starts to interact with its C&C server by sending basic device info and waits to receive commands to execute. Based on these commands, CapraRAT is capable of exfiltrating:

- **call logs,**
- **the contacts list,**
- **SMS messages,**
- **recorded phone calls,**
- **recorded surrounding audio,**

- **CapraRAT-taken screenshots,**
- **CapraRAT-taken photos,**
- **a list of files on the device,**
- **any particular file from the device,**
- **device location,**
- **a list of running apps, and**
- **text of all notifications from other apps.**

It can also receive commands to download a file, launch any installed app, kill any running app, make a call, send SMS messages, intercept received SMS messages, and download an update and request the victim to install it.

Conclusion

The mobile campaign operated by Transparent Tribe is still active, representing itself as two messaging applications, used as a cover to distribute its Android CapraRAT backdoor. Both apps are distributed through two similar websites that, based on their descriptions, provide secure messaging and calling services.

Transparent Tribe probably uses romance scam baits to lure victims into installing the app and continues to communicate with them using the malicious app to keep them on the platform and make their devices accessible to the attacker. CapraRAT is remotely controlled and based on the commands from the C&C server, it can exfiltrate any sensitive information from its victims' devices.

Operators of these apps had poor operational security, resulting in victim PII being exposed to our researchers, across the open internet. Because of that, it was possible to obtain some information about the victims.

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	Package name	ESET detection name	Description
4C6741660AFED4A0E68EF622AA1598D903C10A01	com.meetup.chat	Android/Spy.CapraRAT.A	CapraRAT backdoor.
542A2BC469E617252F60925AE1F3D3AB0C1F53B6	com.meetup.chat	Android/Spy.CapraRAT.A	CapraRAT backdoor.

Network

IP	Provider	First seen	Details
66.235.175[.]91	N/A	2022-09-23	C&C.
34.102.136[.]180	GoDaddy	2022-07-27	meetsapp[.]org – distribution website.
194.233.70[.]54	123-Reg Limited	2022-07-19	meetup-chat[.]com – distribution website.
198.37.123[.]126	Go Daddy	2022-01-20	phone-drive[.]online – APK file hosted website.

IP	Provider	First seen	Details
194.233.70[.]54	Mesh Digital Limited	2022-09-23	share-lienk[.]info – APK file hosting website.

MITRE ATT&CK techniques

This table was built using version 12 of the MITRE ATT&CK framework.

Tactic	ID	Name	Description
Persistence	T1398	Boot or Logon Initialization Scripts	CapraRAT receives the BOOT_COMPLETED broadcast intent to activate at device startup.
T1624.001	Event Triggered Execution: Broadcast Receivers	CapraRAT functionality is triggered if one of these events occurs: PHONE_STATE, NEW_OUTGOING_CALL, BATTERY_CHANGED, or CONNECTIVITY_CHANGE.	
Discovery	T1420	File and Directory Discovery	CapraRAT can list available files on external storage.
T1424	Process Discovery	CapraRAT can obtain a list of running applications.	
T1422	System Network Configuration Discovery	CapraRAT can extract IMEI, IMSI, IP address, phone number, and country.	
T1426	System Information Discovery	CapraRAT can extract information about the device including SIM serial number, device ID, and common system information.	
Collection	T1533	Data from Local System	CapraRAT can exfiltrate files from a device.
T1517	Access Notifications	CapraRAT can collect notification messages from other apps.	
T1512	Video Capture	CapraRAT can take photos and exfiltrate them.	
T1430	Location Tracking	CapraRAT tracks device location.	
T1429	Audio Capture	CapraRAT can record phone calls and surrounding audio.	
T1513	Screen Capture	CapraRAT can record the device's screen using the MediaProjectionManager API.	
T1636.002	Protected User Data: Call Logs	CapraRAT can extract call logs.	
T1636.003	Protected User Data: Contact List	CapraRAT can extract the device's contact list.	

Tactic	ID	Name	Description
T1636.004	Protected User Data: SMS Messages	CapraRAT can extract SMS messages.	
Command and Control	T1616	Call Control	CapraRAT can make phone calls.
T1509	Non-Standard Port	CapraRAT communicates with its C&C over TCP port 4098.	
Impact	T1582	SMS Control	CapraRAT can send SMS messages.

7 Mar 2023 - 11:30AM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion