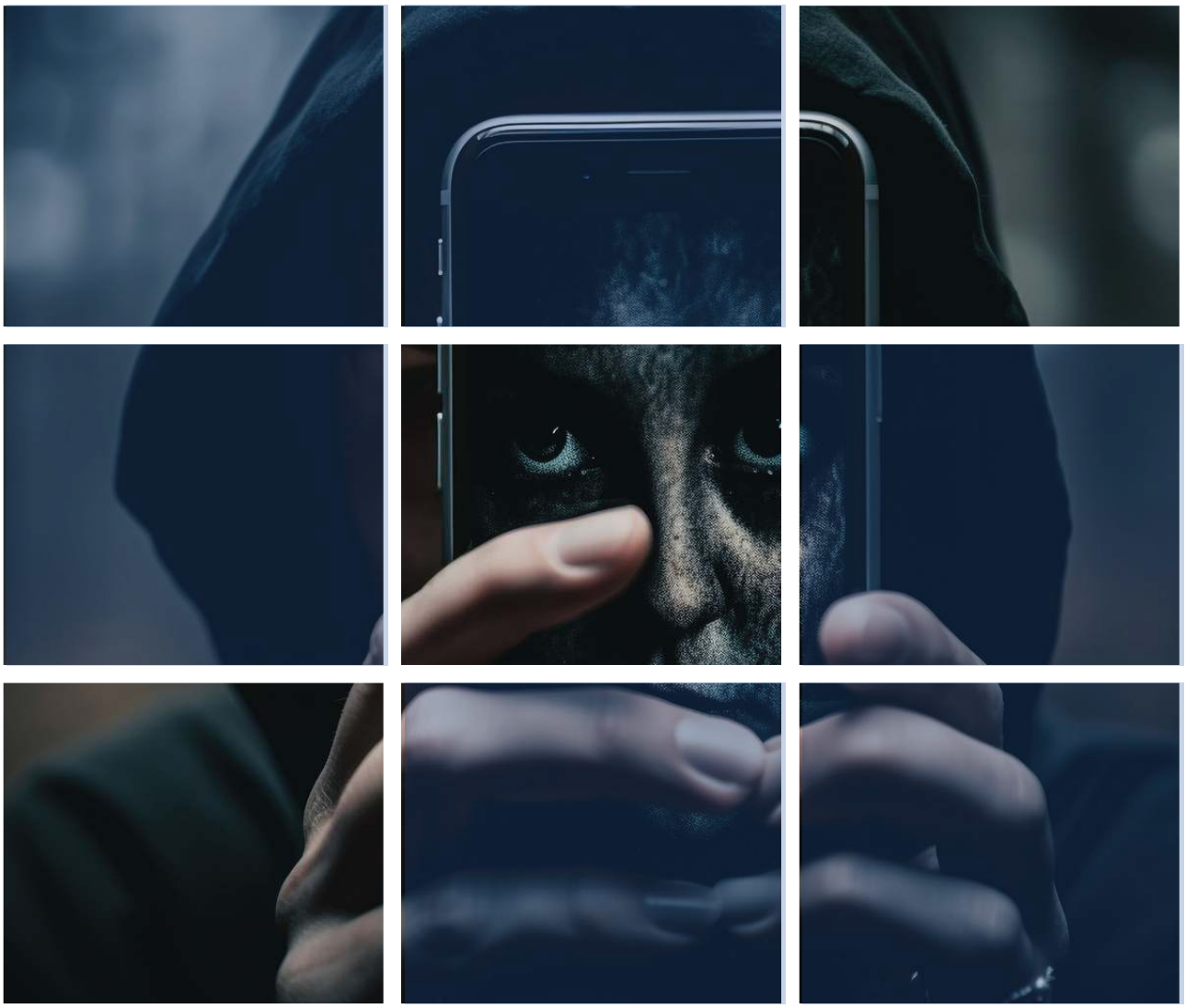
ATHENIAN TECH



TRANSPARENT TRIBE'S CAPRA TUBE

CAPRARAT MIMICS YOUTUBE TO HIJACK ANDROID PHONES

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In a hyper-connected world, the threat landscape, especially in cyberspace is evolving at an alarming pace. A rate that the human mind will find it hard to fathom. While the pace of evolution, in cyber space, has given mankind a host of conveniences but on the flipside, it has also exposed the human race to a new breed of threats, behind which are typically specialized threat actors (the driving force behind these threats). In recent years, a persistent and highly sophisticated threat actor group known as Transparent Tribe has been making headlines, targeting the disputed region of Kashmir and human rights activists working on Pakistan-related matters. This group's weapon of choice is CapraRAT, a malicious Android framework that hides within an innocent-looking application, primarily using YouTube-themed apps as a disguise.

Transparent Tribe, also known as APT36, is believed to have its origins in Pakistan and has a history of targeting military and diplomatic personnel, based in Kashmir. Over time, their focus has expanded to include the Indian education sector, making them a cause of concern for a broader range of individuals and institutions. They have been active largely since 2013.

One of the most intriguing aspects of Transparent Tribe's modus operandi is their use of romance-based social engineering. They create fake YouTube applications with the likeness of a fictitious individual for example like "Piya Sharma." This implies that Piya Sharma is in some way connected to the threat actor and that he continues to Piya Sharma to lure targets to install his application. By mimicking legitimate/popular applications and using familiar themes, the threat actors convince users to install their malicious applications. Once installed, these applications request extensive permissions, allowing CapraRAT to snoop on sensitive data, including text messages, call logs and even the ability to initiate phone calls from the victim phone.

CapraRAT isn't your average malware. It has a sophisticated array of features that can take control of your Android device, effectively giving the attacker a full view of your digital life. It can record audio, capture photos and even manipulate files on the infected device's filesystem. These capabilities make it a formidable tool in the hands of malicious actors. This report provides an in-depth analysis of the strategies and consequences of recent activities of Transparent Tribe, between April and September 2024. The topics covered, in this report, include:

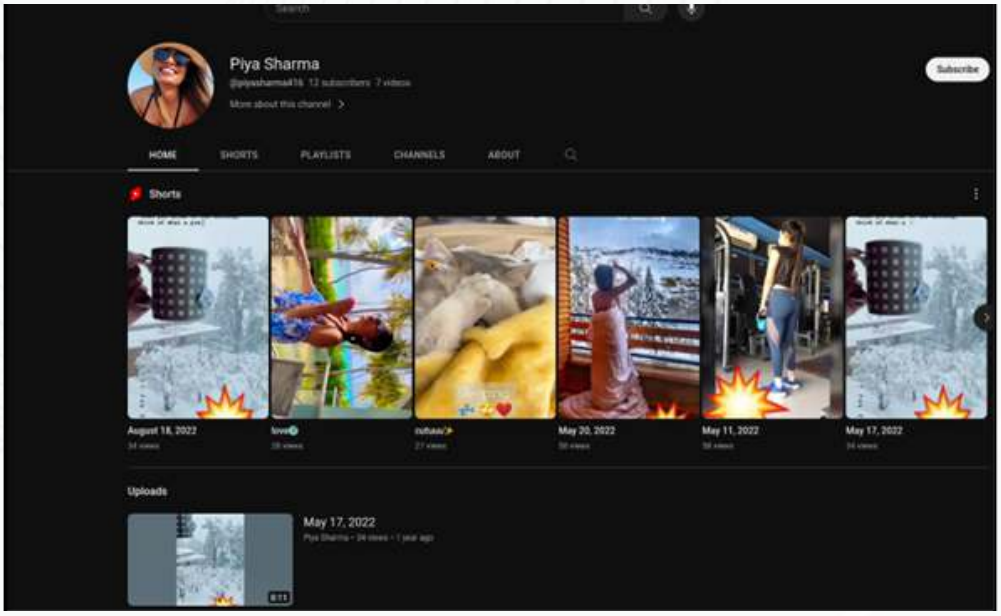
- An exploration of the command and control techniques employed by Transparent Tribe.
- Functionalities and capabilities of the CapraRAT.
- The recognition of CapraRAT as a highly dangerous malware by VirusTotal.
- Compilation of relevant hashes and indicators of compromise (IOCs) associated with this malware.

INTRODUCTION

In the ever-evolving landscape of cybersecurity threats, one actor has consistently emerged as a major concern threatening our national security – “Transparent Tribe” which is a Pakistani threat actor group that is known to target the online security of the Indian Army, Diplomats based in Kashmir. More recently the group has been targeting the country’s educational sector. This report delves into the strategies and impact of the recent activities (April-September 2024) of “Transparent Tribe.” Since 2018, reports have described the threat actor usage of the Android framework CapraRAT, that conceals RAT(Remote Access Trojan) functionality inside another application. This android based tool is used for surveillance on human rights activists who are involved in issues concerning Pakistan as well as in spear phishing targets who are involved in the disputed region of Kashmir.

Transparent Tribe spreads this android apk outside of the Google Play Store, employing hosted by them and through social engineering techniques to lure users into installing the malicious applications (yt.apk, YouTube_052647.apk and Piya Sharma.apk). In early 2024, this threat actor group distributed CapraRAT application camouflaged as a dating service, which was an actual medium for secret spyware operation.

It was recently discovered that of the three APKs mentioned above, one of the APKs was linked to Piya Sharma's YouTube channel, which featured a number of brief videos showing a woman in various settings. Additionally, the person's name and likeness were used in this APK. This implies that Piya Sharma is a connected person and that the actor continues to use romance-based social engineering techniques to convince targets to install the applications.



Youtube Channel - Piya Sharma’s

Source: https://www.youtube.com/channel/UC3q06Ws0fhFftO9Ioor_m-w/videos?app=desktop

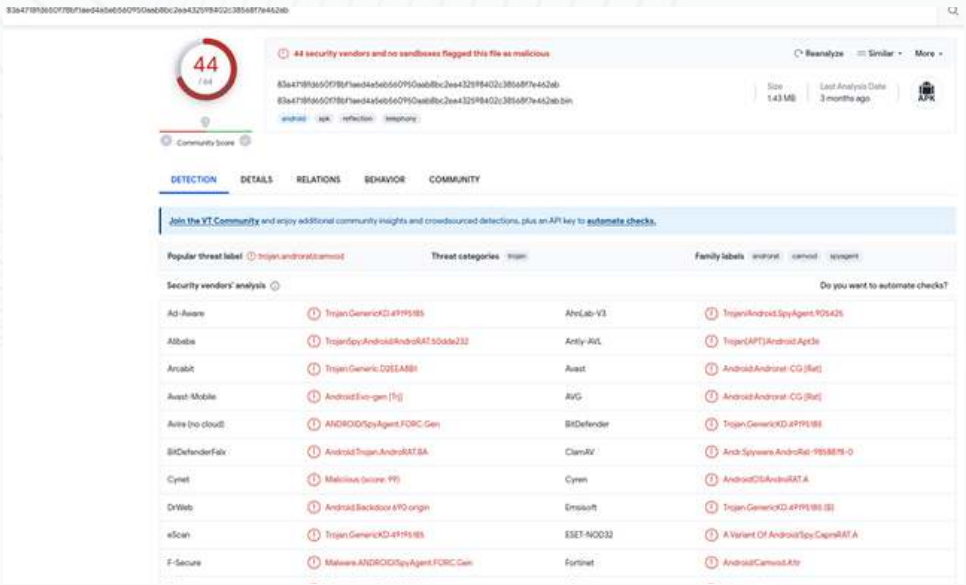
CapraRAT is a complete RAT that gives actors the ability to exfiltrate and capture data as needed. Key characteristics of CapraRAT include:

- Records with the microphone, front & rear cameras
- Collects SMS and multimedia message contents, call logs
- Send SMS messages, blocking incoming SMS
- Initiate phone calls on your behalf
- Take screen captures
- Override system settings such as GPS & Network
- Modify files on the phone's filesystem

CAPRARAT (REMOTE ACCESS TROJAN)

CapraRAT is the name of an Android malware also known as Remote Access Trojan (RAT). Hackers make use this software to compromise Android devices. This trojan is a modified version of another RAT(remote access trojan) called AndroRAT. CapraRAT malware is used by a sophisticated and well-known group "APT36."

APT 36 is a cyberespionage threat actor group primarily focused on South Asian targets. They are believed to be based in Pakistan and have been linked to cyber-spying operations against several targets, especially India. Spear-phishing attacks, use of Android-based malware like CapraRAT and performing cyber-espionage operations with emphasis on political, military and diplomatic targets are part of their modus operandi. The intelligence-gathering activities of APT36 have been connected to the disputed Kashmir region as well as other geopolitical challenges in the South Asian region.



Virustotal identified CapraRAT apk (as a malware)

Source: Virustotal

CapraRAT can access the phone number, microphone (and record audio), location data, call logs and contact information. It can also open the camera and launch installation packages for other programmes. Additionally, MP4 or APK files from the asset directory can be dropped using it.

CapraRAT also has a unique mechanism that allows the malware to run continuously in the background and consistently check the code's status, restarting it whenever it stops.

CapraRAT malware is mainly focused on harvesting & transferring unauthorized information data from systems to its handler. This malware can, not only retrieve contact information (on the phone), call history and other information that mentioned above but can also send messages (to others on your behalf), take screenshots and access SMS data.

Threat Summary

Name	CapraRAT remote access trojan
Threat Type	Android malware, malicious application, unwanted application.
Detection Names	Avast-Mobile (Android:Evo-gen [Trj]), Combo Cleaner (Trojan.GenericKD.49195185), ESET-NOD32 (A Variant Of Android/Spy.AndroRAT.AE), Kaspersky (HEUR:Trojan-Spy.AndroidOS.Camvod.a)
Symptoms	The device is running slow, system settings are modified without user's permission, questionable applications appear, data and battery usage is increased significantly, browsers redirect to questionable websites, intrusive advertisements are delivered.
Distribution methods	Infected email attachments, malicious online advertisements, social engineering, deceptive applications, scam websites.
Damage	Stolen personal information (private messages, logins/passwords, etc.), decreased device performance, battery is drained quickly, decreased Internet speed, huge data losses, monetary losses, stolen identity (malicious apps might abuse communication apps).

Source: https://www.pcrisk.com/removal-guides/24915-caprarat-malware-android

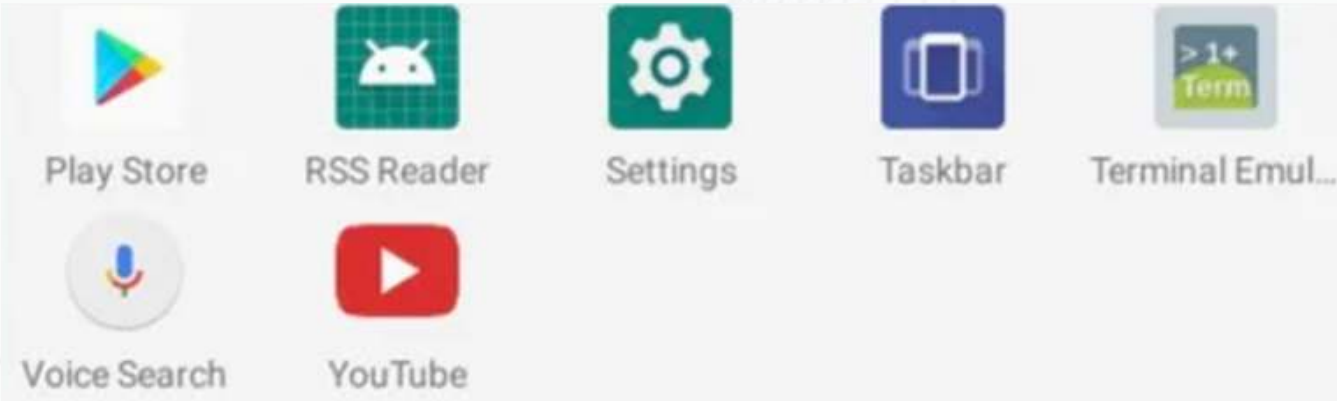
APP ANALYSIS

Android APKs are used to deliver CapraRAT. Trend Micro's research team discovered that CapraRAT may be loosely based on the AndroRAT source code when the programme was first named.

Sentinelone performed static analysis on two YouTube-themed CapraRAT APKs: 8beab9e454b5283e892aeca6bca9afb608fa8718 – yt.apk, uploaded to VirusTotal in July 2024.

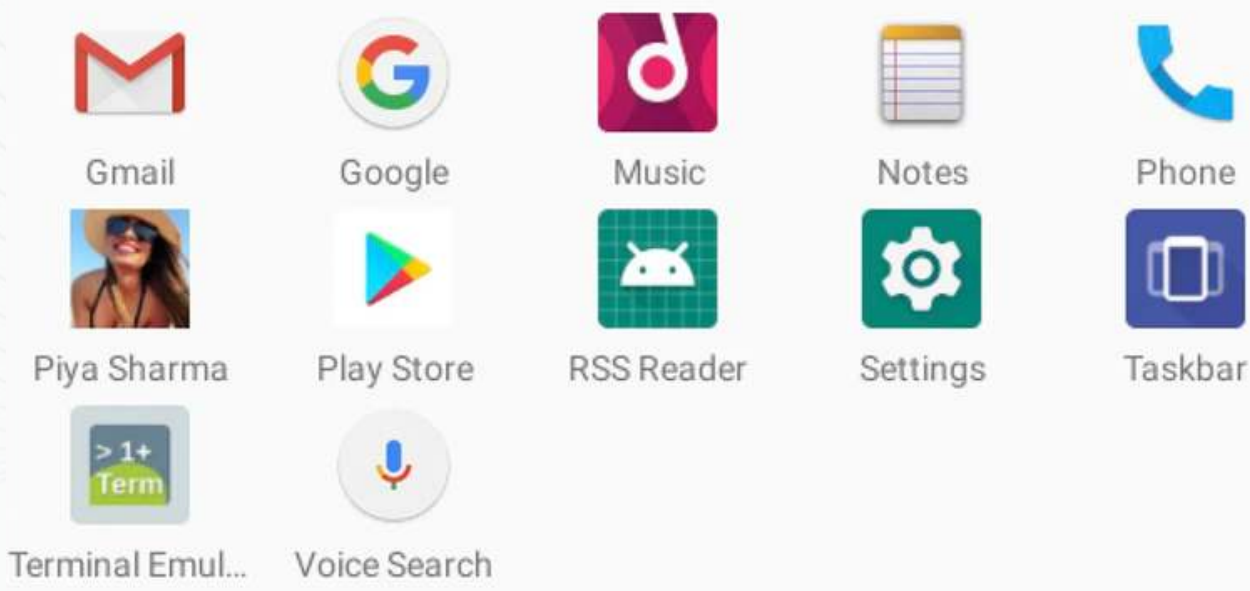
83412f9d757937f2719ebd7e5f509956ab43c3ce – YouTube_052647.apk, uploaded to VirusTotal in August 2024.

They also identified a third APK called Piya Sharma, the YouTube channel persona described earlier: 14110facecceb016c694f04814b5e504dc6cde61 – Piya Sharma.apk, uploaded to VirusTotal in April 2024.



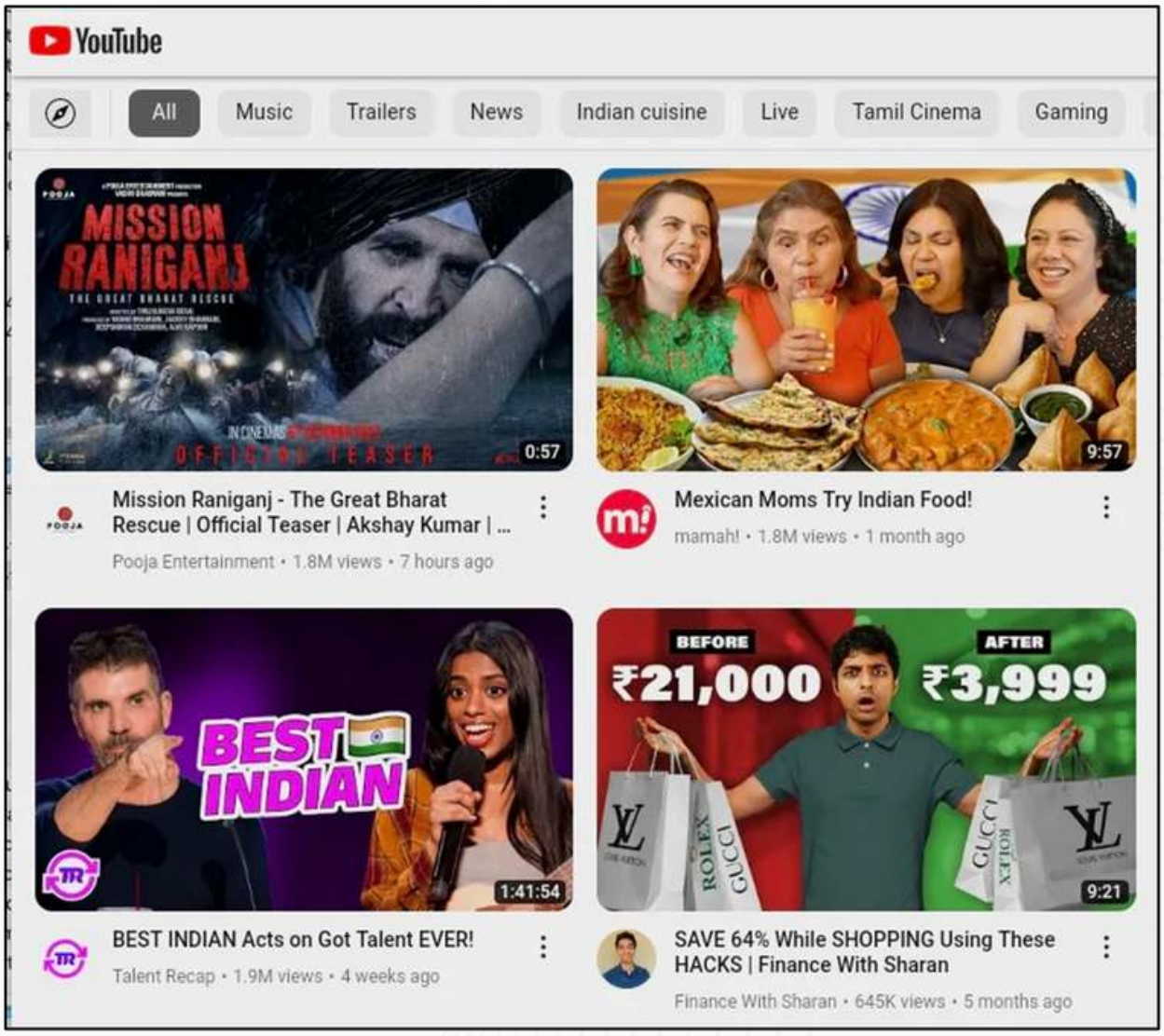
Applications icons on an Android device, including YouTube_052647.apk

Source: https://www.sentinelone.com/labs/capratube-transparent-tribes-caprarat-mimics-youtube-to-hijack-android-phones/ (Sentinelone)



Application icons, including the Piya Sharma app

Source: https:www.sentinelone.com/labs/capratube-transparent-tribes-caprarat-mimics-youtube-to-hijack-android-phones/ (Sentinelone)

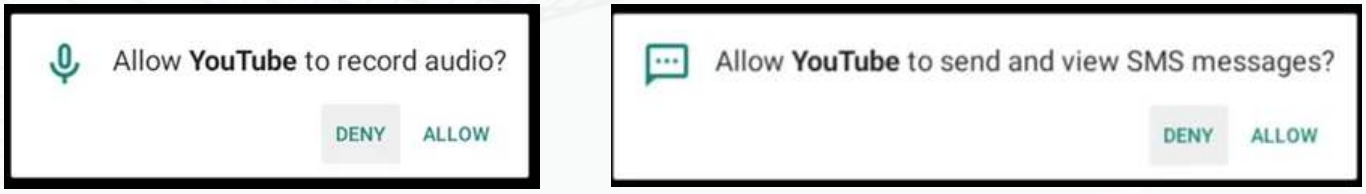


YouTube_052647.apk displays the YouTube website

Source: https://www.sentinelone.com/labs/capratube-transparent-tribes-caprarat-mimics-youtube-to-hijack-android-phones/ (Sentinelone)

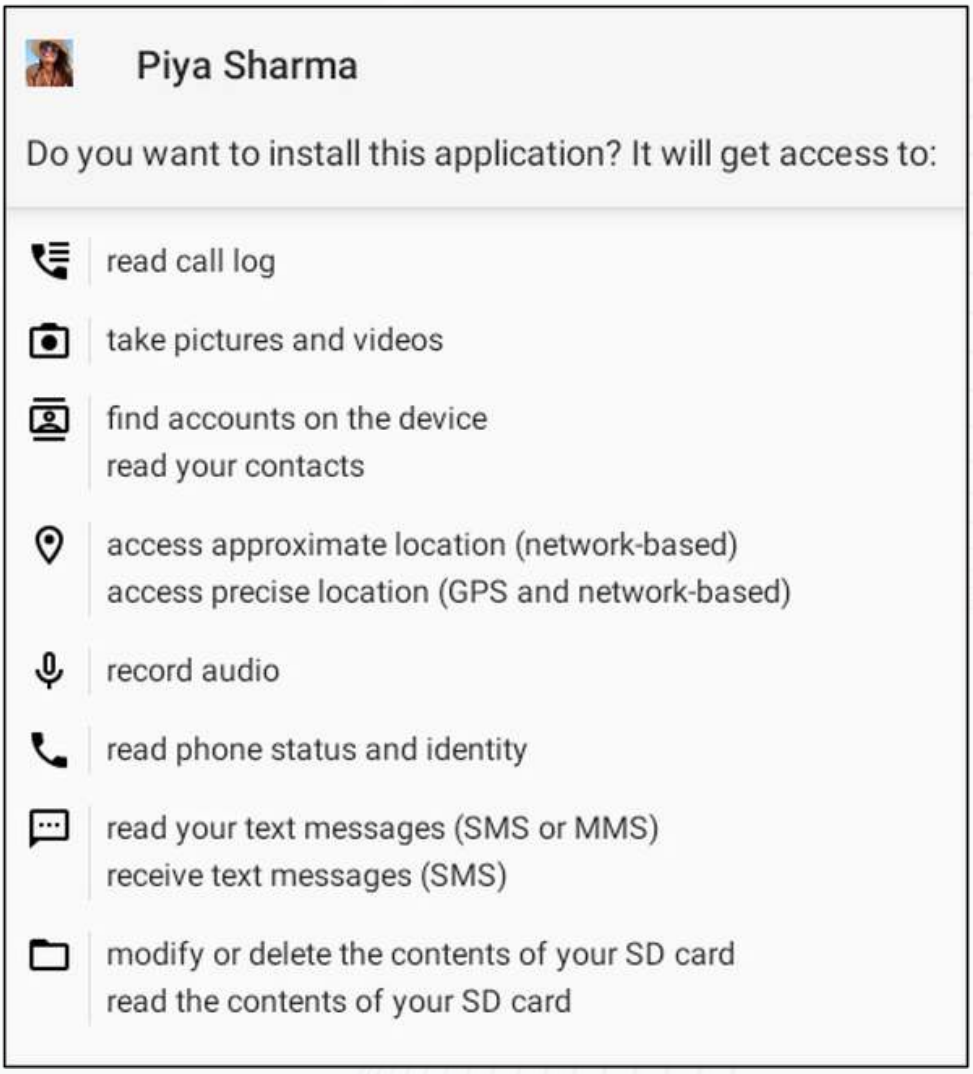
Several Permissions (Youtube Application)

The application requests multiple permissions such as microphone access, aligning with legitimate functions like recording or search capabilities. However, other permissions, such as the ability to send and view SMS messages, are less relevant to the expected application behaviour.



Permissions prompts during install of the weaponized YouTube app

Source: www.sentinelone.com/labs/capratube-transparent-tribes-caprarat-mimics-youtube-to-hijack-android-phones/(Sentinelone)



Installation permissions requested by the Piya Sharma APK

Source: https://www.sentinelone.com/labs/capratube-transparent-tribes-caprarat-mimics-youtube-to-hijack-android-phones/ (Sentinelone)

KEY COMPONENTS

The CapraRAT APKs we analyzed contain the following files:

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

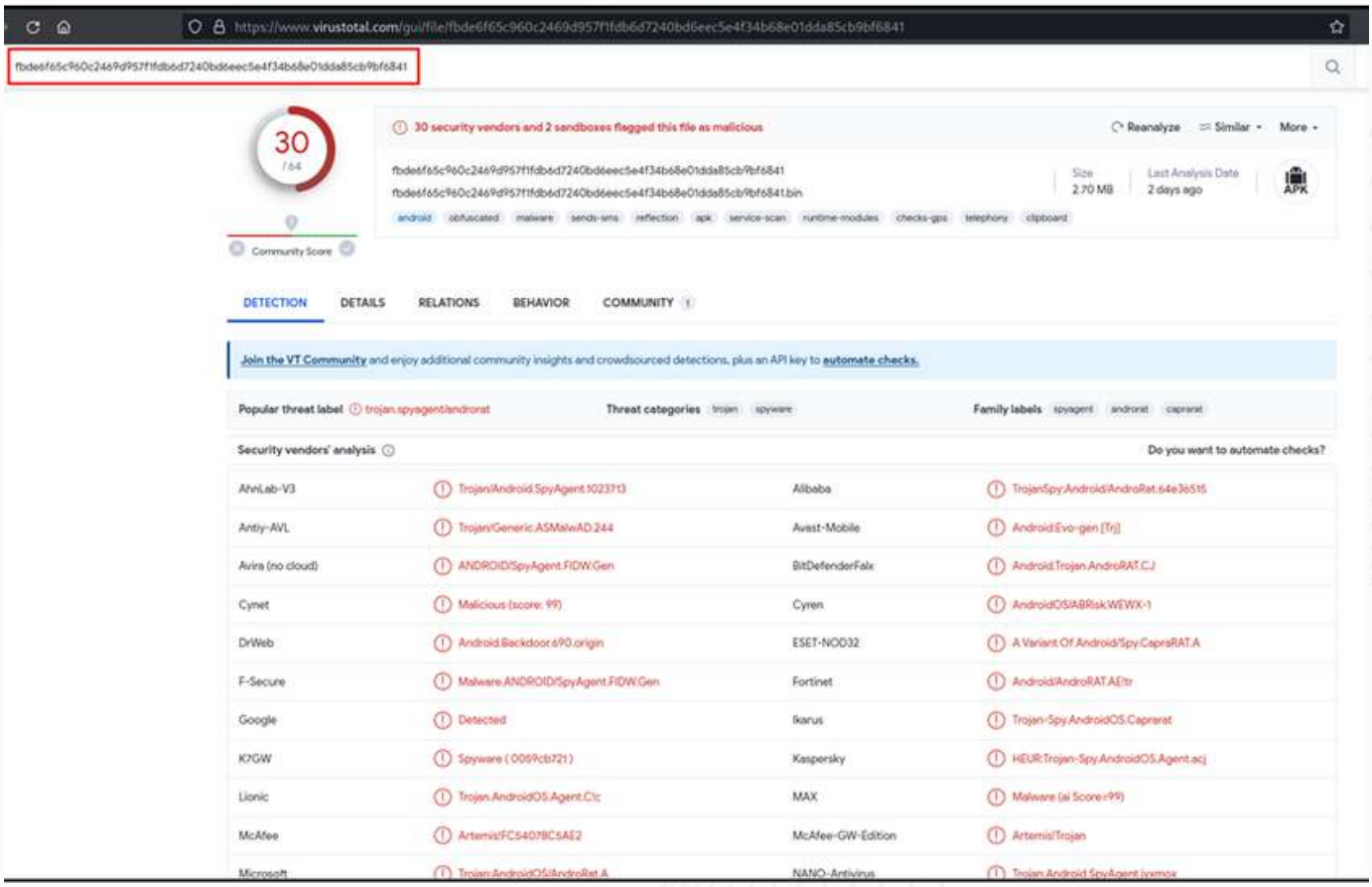
Name	Piya Sharma.apkrvice/TCHPClient
Configuration	com/videos/watchs/share/setting
Version	V.U.H.3
Main	com/videos/watchs/share/MainActivity
Malicious Activity	com/videos/watchs/share/TCPClient

Name	yt.apk
Configuration	com/media/gallery/service/settings
Version	MSK-2024
Main	com/media/gallery/service/MainActivity
Malicious Activity	com/media/gallery/service/TPSClient

Virustotal Identifies as a RAT (Remote Access Trojan)

Yt.apk (Youtube Application)

Name	• fbde6f65c960c2469d957f1fdb6d7240bd6eec5e4f34b68e01dda85cb9bf6841.bin • yt.apk
MD5	fc54078c5ae26d856109d306c37909ae
SHA-1	8beab9e454b5283e892aeca6bca9afb608fa8718
Vhash	fbde6f65c960c2469d957f1fdb6d7240bd6eec5e4f34b68e01dda85cb9bf6841
SSDEEP	49152:1+GXVzVoug3HVnBkzUpz1p59ze+WuGnnlUxA2Uf+Vv9exf7N74bLWSSHV5jgdXOC:TXnoug3ZBt3/3W9nIUfc0fh4/wzeth
TLSH	T1E0D50143EB88D822D4F7E632D2B2826655124C595753E3834E507B7C6DBBBC09B4AFC8
Permhash	df982878b5985c41f7616241f9685 21c779aa88a634132792918b8380dee2015
Filetype	Android
Magic	Zip archive data, at least v2.0 to extract, compression method=deflate
TrLD	Android Package (48.1%) Java Archive (20%) Sweet Home 3D design (generic) (15.5%) Google Earth saved working session (8.8%) ZIP compressed archive (5.9%)
File Size	2.70 MB (2828813 bytes)

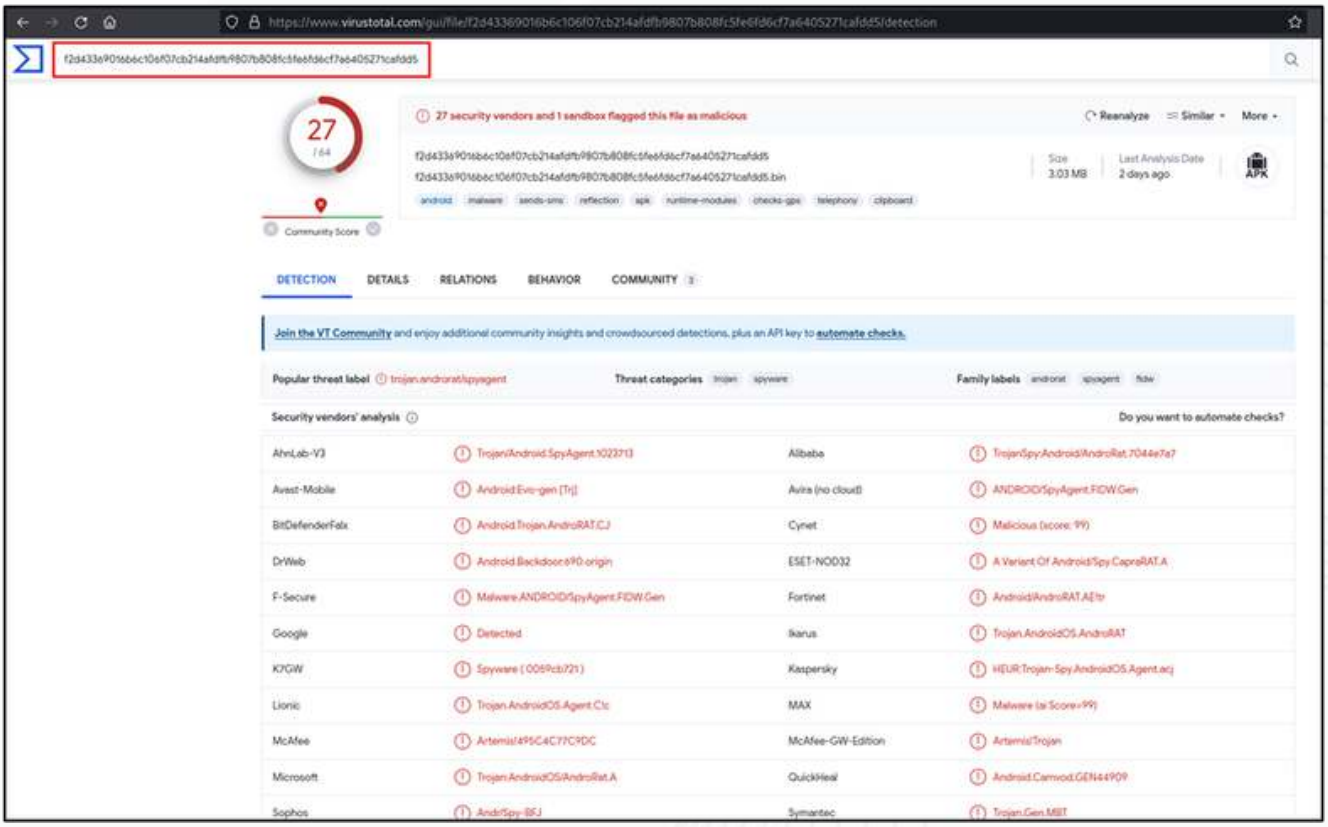


Yt.apk identified as RAT

Source: Virustotal

YouTube_052647.apk

Name	• f2d43369016b6c106f07cb214afdfb9807b808fc5fe6fd6cf7a6405271cafdd5.bin • YouTube_052647.apk
MD5	495c4c77c9dceda458930c33b8391f27
SHA-1	83412f9d757937f2719ebd7e5f509956ab43c3ce
SHA-256	f2d43369016b6c106f07cb214afdfb9807b808fc5fe6fd6cf7a6405271cafdd5
Vhash	95d416bb8c299182f58dea6c253726ac
SSDEEP	49152:Z7Ach7rvJmtg7QZwQgnLtd4w96h6W85/ZPG9+9P/l80D5PDmZggvwFmB2fP0qcQk:997bB7KRE47h1cZOQXFDfFmB2fEb
TLSH	T1DBE50181FB04D82BC4B754334BB2467611564E8E8992D7039AECB25C5D7BAC09FDAFC8
Permhash	ca07e621bd8ac3997b29f79319da3d4e788ca29dd52f7808716f6c0a3c260d71
Filetype	Android
Magic	Zip archive data, at least v2.0 to extract, compression method=deflate
TrLD	Android Package (52.8%) Java Archive (21.9%) Sweet Home 3D design (generic) (17%) ZIP compressed archive (6.5%) PrintFox/Pagefox bitmap (640x800) (1.6%)
File Size	3.03 MB (3181635 bytes)



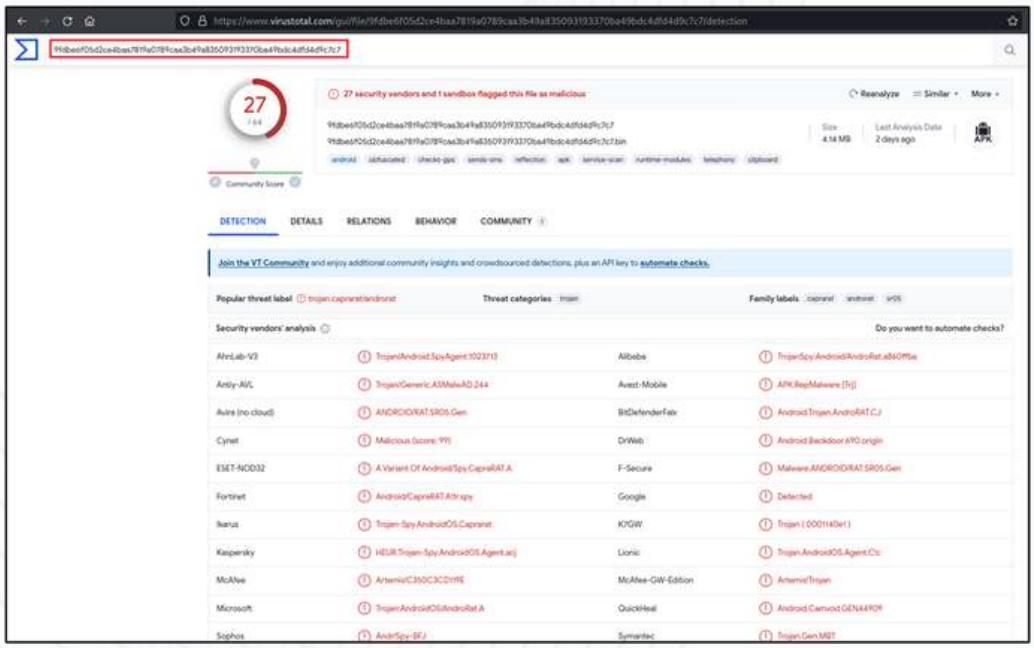
yt.apk identified as RAT

Source: Virustotal

Piya Sharma APK

Name	• 9fdbe6f05d2ce4baa7819a0789caa3b49a835093193370ba49bdc4dfd4d9c7c7.bin • c350c3cd119e517477b35e6830947531.virus
MD5	c350c3cd119e517477b35e6830947531
SHA-1	14110facecceb016c694f04814b5e504dc6cde61
SHA-256	9fdbe6f05d2ce4baa7819a0789caa3b49a835093193370ba49bdc4dfd4d9c7c7
Vhash	ac8af3bc7b1463a592f054ed4a32583a
SSDEEP	98304:2cH7nInQnnnnYRbMn9RjO413qnsSr+Xg7t77Ksry5YLZHbhmc5LkWy:2I7nInQnnnnBnC0y7754+Nxkx
TLSH	T1DD160141FB54E42FC4B790330AE6463615525E8E8A42E34759DCB3AC6CB7AD48FC6BC8

Permhash	100ba8f26850b08bb1640a5172d6b15ca59594ca5401b3ff7b47a189971b704b
Filetype	Android
Magic	Zip archive data, at least v2.0 to extract, compression method=deflate
TrLD	Android Package (52.8%) Java Archive (21.9%) Sweet Home 3D design (generic) (17%) ZIP compressed archive (6.5%) PrintFox/Pagefox bitmap (640x800) (1.6%)
File Size	4.14 MB (4336874 bytes)



Piya_Sharma.apk identified as RAT

Source: Virustotal

C2 & INFRASTRUCTURE

In the Configuration file of the CapraRAT application, SERVERIP variable contains the command-and-control(C2) server address; it might be a domain, IP address, or both. The C2 port is in the form of hexadecimal Big Endian format. Human readable port is obtained after converting into decimal format, resulting in port 14862 for yt.apk, port 18892 for YouTube_05264.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
```

```
.method static constructor <clinit>()V
    sput-object v1, Lcom/Base/media/service/setting;->mainActivity:Landroid

    .line 35
    const-string v2, "95.111.247.73-shareboxs.net"

    sput-object v2, Lcom/Base/media/service/setting;->SERVERIP:Ljava/lang/S

    .line 36
    const/16 v2, 0x49cc

    sput v2, Lcom/Base/media/service/setting;->SERVERPORT:I

    .line 39
    sput v0, Lcom/Base/media/service/setting;->mediaSource:I

    .line 40
    sput v0, Lcom/Base/media/service/setting;->conAtms:I
```

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

Source: Sentinelone

During analysis of YouTube_052647.apk, by xxxxxx this apk uses the shareboxs.net domain that has been associated with the “Transparent Tribe” since at least 2019.

In the two youtube applications, IP addresses that are associated with C2 servers have RDP(Remote Desktop Protocol) port 3389 open & the service identified as Windows Remote Desktop; that indicates the threat actor group uses windows server infrastructure to host the CapraRAT C2 application.

Piya Sharma application C2 IP, 209.127.19.241 has a certificate with common name value WIN-P9NRMH5G6M8, that indicates a longstanding connection with “Transparent Tribe’s” CrimsonRAT C2 servers.

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

Source: Sentinelone

During analysis of YouTube_052647.apk, by xxxxxx this apk uses the shareboxs.net domain that has been associated with the “Transparent Tribe” since at least 2019.

In the two youtube applications, IP addresses that are associated with C2 servers have RDP(Remote Desktop Protocol) port 3389 open & the service identified as Windows Remote Desktop; that indicates the threat actor group uses windows server infrastructure to host the CapraRAT C2 application.

Piya Sharma application C2 IP, 209.127.19.241 has a certificate with common name value WIN-P9NRMH5G6M8, that indicates a longstanding connection with “Transparent Tribe’s” CrimsonRAT C2 servers.

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

CONCLUSION

In conclusion, Transparent Tribe's use of CapraRAT (Remote Access Trojan), an android apk, malware poses a significant threat, targeting India's defence establishment, diplomats and the education sector. The threat actor employs deception and social engineering techniques, to disguise their malicious applications as seemingly harmless services. The threat actor group's choice to create a YouTube-like app is the latest twist in a well-established pattern in which the group equips Android applications with spyware and distributes them to targets via social media.

The persistence of their activities highlights the importance of ongoing vigilance in the face of evolving cybersecurity threats, particularly in the South Asian region. Proper cybersecurity measures and awareness are essential to mitigate/counter these threats and protect sensitive information.

Defensive and preventative measures should include:

- careful of opening links or files in suspicious emails (e.g., irrelevant emails sent from unknown addresses).
- Download applications only from trusted sources (official pages and stores).
- Use trustworthy mobile security solutions to protect devices against these threats.
- Be wary of new social media applications advertised within social media communities.
- Assess the permissions requested by an application, particularly an application you are not particularly familiar with.
- Do not install any third-party version of an application already on your device.

ATHENIAN TECH

Contact Us

www.atheniantech.com