

CapraTube Remix | Transparent Tribe’s Android Spyware Targeting Gamers, Weapons Enthusiasts

By Alex Delamotte

Published: 2024-07-01 · Archived: 2026-04-05 17:31:25 UTC

Executive Summary

- SentinelLABS has identified four new CapraRAT APKs associated with suspected Pakistan state-aligned actor Transparent Tribe.
- These APKs continue the group’s trend of embedding spyware into curated video browsing applications, with a new expansion targeting mobile gamers, weapons enthusiasts, and TikTok fans.
- The overall functionality remains the same, with the underlying code updated to better suit modern Android devices.

Overview

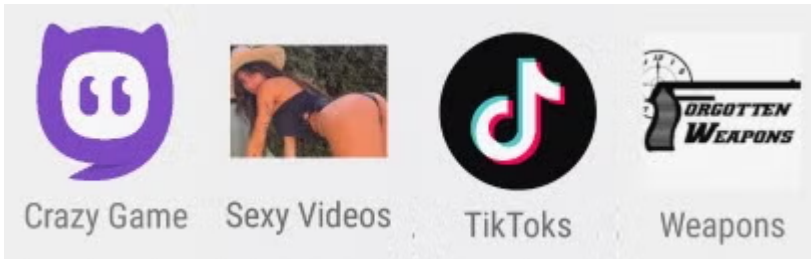
Transparent Tribe (*aka* APT 36, Operation C-Major) has been active since at least [2016](#) with attacks against Indian government and military personnel. The group relies heavily on social engineering attacks to deliver a variety of Windows and Android spyware, including spear-phishing and watering hole attacks.

In September 2023, SentinelLABS outlined the [CapraTube](#) campaign, which used weaponized Android applications (APK) designed to mimic YouTube, often in a suspected dating context due to the nature of the videos served. The activity highlighted in this report shows the continuation of this technique with updates to the social engineering pretexts as well as efforts to maximize the spyware’s compatibility with older versions of the Android operating system while expanding the attack surface to include modern versions of Android.

New CapraRAT APKs

SHA-1	c307f523a1d1aa928fe3db2c6c3ede6902f1084b
App Name	Crazy Game signed.apk
Package Name	com.maeps.crygms.tktols
SHA-1	dba9f88ba548cebfa389972cddf2bec55b71168b
App Name	Sexy Videos signed.apk
Package Name	com.nobra.crygms.tktols
SHA-1	28bc3b3d8878be4267ee08f20b7816a6ba23623e

App Name	TikTok signed.apk
Package Name	com.maeps.vdosa.tktols
SHA-1	fff24e9f11651e0bdbbee7c5cd1034269f40fc424
App Name	Weapons signed.apk
Package Name	com.maeps.vdosa.tktols



New CapraRAT app logos

The new versions of CapraRAT each use WebView to launch a URL to either YouTube or a mobile gaming site, CrazyGames[.]com . There is no indication that an app with the same name, [Crazy Games](#), is weaponized as it does not require several key CapraRAT permissions, such as sending SMS, making calls, accessing contacts, or recording audio and video. The URL query in the CapraRAT code is obfuscated as `ht tUUpTs://www.youUtube.com/resulUUts?seUUarch_quUUery=TiUUk+ToUUks` , which is cleaned to remove occurrences of UU, resulting in `https[:]//www.youtube[.]com/results?search_query=Tik+Toks` .

```
.method private load_web()V
    .registers 5
    00000000 const         v0, 0x7F0B001D          # layout:activity_webview
    00000006 invoke-virtual MainActivity->setContentView(I)V, p0, v0 # actual call site: Landroid/sup
    0000000C const         v0, 0x7F0800C7          # id:webView1
    00000012 invoke-virtual MainActivity->findViewById(I)View, p0, v0 # actual call site: Landroid/s
    00000018 move-result-object v0
    0000001A check-cast     v0, WebView
    0000001E iput-object    v0, p0, MainActivity->webView:WebView
    :try_22
    00000022 invoke-virtual MainActivity->getSupportActionBar()ActionBar, p0 # actual call site: Lanc
    00000028 move-result-object v0
    0000002A invoke-virtual ActionBar->hide()V, v0
    .catch NullPointerException {:try_22 .. :tryend_30} :catch_32
    :tryend_30
    00000030 goto             :34
    :catch_32 # used for: Ljava/lang/NullPointerException;
    00000032 move-exception v0
    :34
    00000034 iget-object    v0, p0, MainActivity->webView:WebView
    00000038 const-string   v1, "htUUpTs://www.youUtube.com/resulUUts?seUUarch_quUUery=TiUUk+ToUUks"
    0000003C const-string   v2, "UU"
    00000040 const-string   v3, ""
    00000044 invoke-virtual String->replace(CharSequence, CharSequence)String, v1, v2, v3
    0000004A move-result-object v1
    0000004C invoke-virtual WebView->loadUrl(String)V, v0, v1
    00000052 iget-object    v0, p0, MainActivity->webView:WebView
    00000056 invoke-virtual WebView->getSettings()WebSettings, v0
    0000005C move-result-object v0
    0000005E const/4       v1, 1
    00000060 invoke-virtual WebSettings->setJavaScriptEnabled(Z)V, v0, v1
    00000066 iget-object    v0, p0, MainActivity->webView:WebView
    0000006A new-instance   v1, MainActivity$1
    0000006E invoke-direct MainActivity$1-<<init>(MainActivity)V, v1, p0
    00000074 invoke-virtual WebView->setWebViewClient(WebClient)V, v0, v1
    0000007A iget-object    v0, p0, MainActivity->webView:WebView
    0000007E new-instance   v1, MainActivity$MyChrome
    00000082 invoke-direct MainActivity$MyChrome-<<init>(MainActivity)V, v1, p0
    00000088 invoke-virtual WebView->setWebChromeClient(WebChromeClient)V, v0, v1
    0000008E return-void
.end method
```

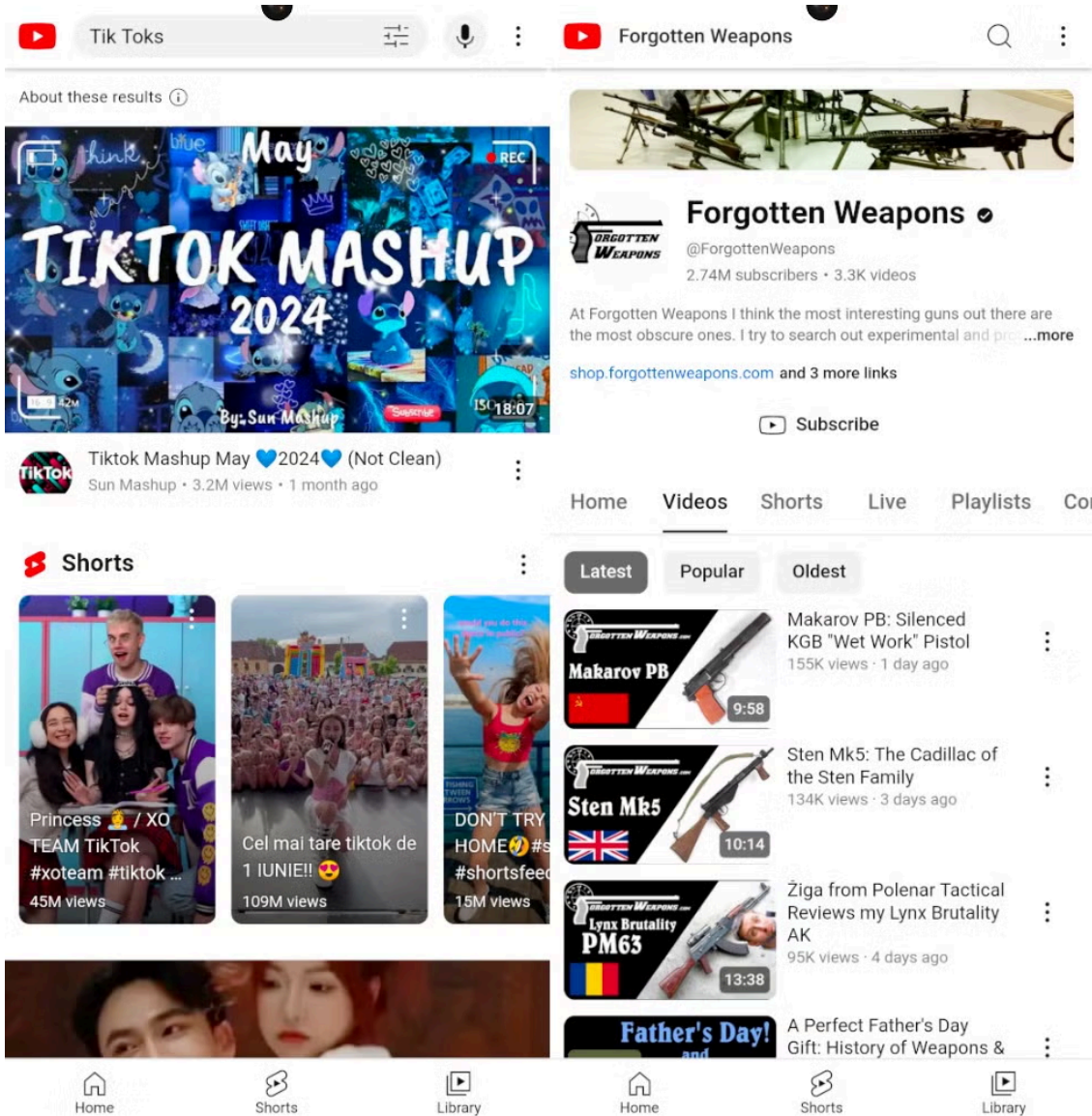
URL deobfuscation and loading performed by CapraRAT's *load_web* method

```
private void load_web() {
    this.setContentView(0x7F0B001D); // layout:activity_webview
    this.webView = (WebView)this.findViewById(0x7F0800C7); // id:webview1
    try {
        this.getSupportActionBar().hide();
    }
    catch(NullPointerException unused_ex) {
    }

    this.webView.loadUrl("https://www.youtube.com/results?search_query=Tik+Toks");
    this.webView.getSettings().setJavaScriptEnabled(true);
    this.webView.setWebViewClient(new WebViewClient() {
        @Override // android.webkit.WebViewClient
        public boolean shouldOverrideUrlLoading(WebView view, String url) {
            view.loadUrl(url);
            return true;
        }
    });
    this.webView.setWebChromeClient(new MyChrome(this));
}
```

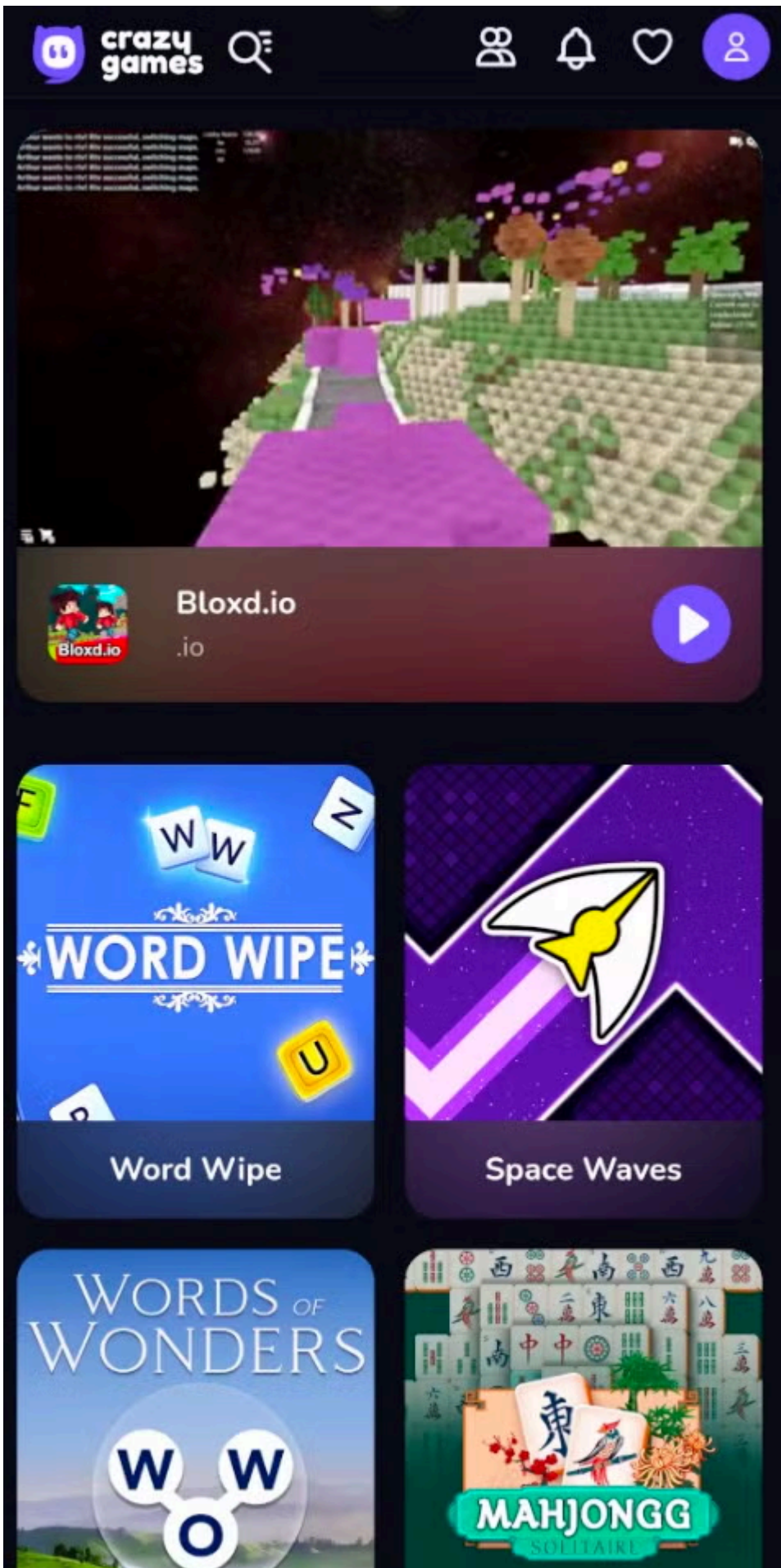
Decompiled view of *load_web* method

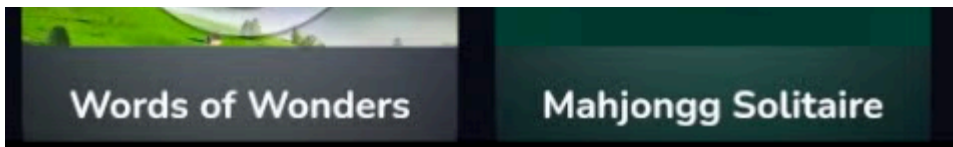
The [previous CapraTube campaign](#) had one APK called Piya Sharma that was likely used in a romance-themed social engineering pretext. The new campaign continues that trend with the Sexy Videos app. While two of the previously reported apps launched only YouTube with no query, the YouTube apps from this campaign are each preloaded with a query related to the application's theme. The TikTok app launches YouTube with the query "Tik Toks," and the Weapons app launches the Forgotten Weapons YouTube channel, which reviews a variety of classic arms and has 2.7 Million subscribers.



TikTok and Weapons-themed CapraRAT YouTube WebView

The Crazy Games app launches WebView to load `CrazyGames[.]com`, a site containing in-browser mini games. This particularly resource-intensive site did not work well on older versions of Android during our testing.





Crazy Games CapraRAT WebView

When the app first launches, the user is prompted to grant several risky permissions, including:

- Access GPS location
- Manage network state
- Read and send SMS
- Read contacts
- Record audio and screen, take screenshots
- Storage read and write access
- Use camera
- View call history and make calls

In contrast with the previous CapraRAT campaign, the following Android permissions are no longer requested or used:

- READ_INSTALL_SESSIONS
- GET_ACCOUNTS
- AUTHENTICATE_ACCOUNTS
- REQUEST_INSTALL_PACKAGES

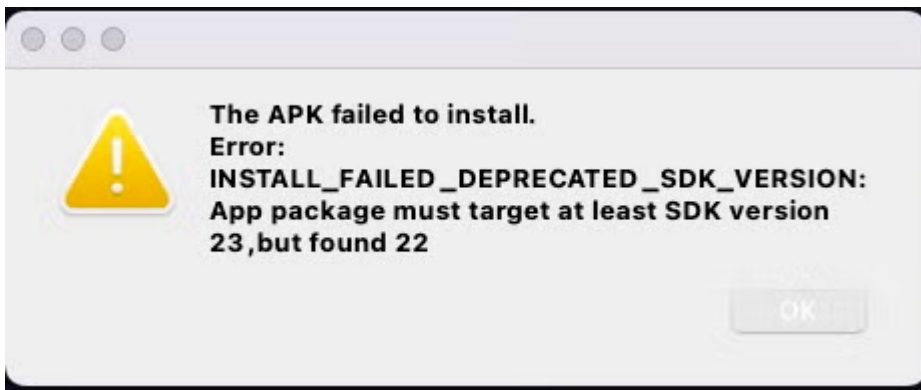
The reduction in permissions suggests the app developers are focused on making CapraRAT a surveillance tool more than a fully featured backdoor.

App Compatibility

The most significant changes between this campaign and the September 2023 campaign are to app compatibility. The newest CapraRAT APKs we identified now contain references to Android's Oreo version (Android 8.0), which was released in 2017. Previous versions relied on the device running Lollipop (Android 5.1), which was released in 2015 and less likely to be compatible with modern Android devices.

We tested the APKs from this campaign and the September 2023 campaign on an Android device running Android Tiramisu *aka* Android 13 (2022) and Android 14 (2023). The new campaign's apps ran smoothly on this modern version of Android. The September 2023 campaign apps prompted a compatibility warning dialog, which could raise suspicion among victims that the app is abnormal. When running on the newest released version of Android 14, the September 2023 campaign's Piya Sharma app fails to install. Each of the newer versions ran successfully.

In all cases, the app still requests gratuitous permissions from the user that hint to the tool's capabilities. Even if the user declines permissions, the app still runs, meaning the group has not overcome this hurdle to successfully implementing their spyware.



Piya Sharma app install failure dialog on Android 14

The new CapraRAT packages also contain a very minimal new class called `WebView`, which is responsible for maintaining compatibility with older versions of Android via the Android Support Library, which developers can choose to include in a project to enhance compatibility.

Spyware Activities and C2

The app's `MainActivity` initiates requests for permissions. The app still runs even if permissions are not granted.

`MainActivity` calls the `TCHPClient` class, which contains the malicious capabilities leveraged by CapraRAT. This class drives several spyware classes and methods, including:

- `audioStreamer` (`aStreamer`)
- `CallLogLister`
- `CallReceiver`
- `ContactsLister`
- `DirLister` (file browsing)
- `downloadFile`
- `killFile` (file deletion)
- `killProcess`
- `PhotoTaker`
- `SMSLister`
- `SMSReceiver`

These give the spyware fine-grained control over what the user does on the device.

The `sendData` method is responsible for constructing the data collected by other methods and classes and sending it to the C2. The `mRun` method constructs the socket and sends the data to the C2 server using the variables specified in the `Settings` class. Each of the current campaign's APKs use the same C2 server hostname, IP address and TCP port number 18582. The `Settings` class also shows the same CapraRAT version identifier for each APK, `A.D.0.2`.

```
static {
    setting.is_load_app = true;
    setting.is_hide_app = false;
    setting.is_phical = false;
    setting.verion = "A.D.0.2";
    setting.timerDelay = 5000;
    setting.timerStart = 50000;
    setting.mainActivity = null;
    setting.SERVERIP = "173.249.50.243-shareboxs.net";
    setting.SERVERPORT = 0x4896;
    setting.mediaSource = 0;
    setting.conAtms = 0;
    setting.mehiden = false;
    setting.errors = false;
    setting.imi = "";
    setting.os = "";
    setting.ip = "";
    setting.userID = "0";
    setting.timeForAlarm = 60000;
    setting.MINIMUM_DISTANCE_CHANGE_FOR_UPDATES = 10L;
    setting.MINIMUM_TIME_BETWEEN_UPDATES = 10000L;
    setting.folder_path = Environment.getExternalStorageDirectory().getAbsolutePath() + "/._DRAGDS/";
    setting.setPath = Environment.getExternalStorageDirectory().getAbsolutePath() + "/._DEDSET_";
    setting.capPath = Environment.getExternalStorageDirectory().getAbsolutePath() + "/._DETCAP_";
    setting.logPath = Environment.getExternalStorageDirectory().getAbsolutePath() + "/._DETLOG_";
    setting.notiPath = Environment.getExternalStorageDirectory().getAbsolutePath() + "/._DENIFI_";
    setting.recPath = Environment.getExternalStorageDirectory().getAbsolutePath() + "/._AATECS_";
    setting.phoneNumber = "";
    setting.commandType = 0;
    setting.mGPS = false;
    setting.isMAct = false;
    setting.recMic = false;
    setting.recCall = false;
    setting.remUser = false;
    setting.appRun = false;
    setting.capQuality = 100;
    setting.enbScren = false;
    setting.activityresCode = 0;
    setting.activityData = null;
    setting.singleScren = false;
    setting.screnSize = 50;
    setting.isCancl = false;
    setting.smsMoniter = false;
    setting.smsWhere = "";
    setting.callWhere = "";
    setting.isGPSEnabled = false;
    setting.isNetworkEnabled = false;
    setting.isRealNotif = false;
    setting.pInterv = 0;
    setting.iMemorySize = "";
    setting.eMemorySize = "";
    setting.aMemorySize = "";
    setting.notiMap = new HashMap();
}
```

mRun performs a connectivity check to decide whether to connect to the C2 using the hostname shareboxs[.]net or the hardcoded IP address 173[.]249[.]50[.]243 . This IP address has been tied to Transparent Tribe’s CrimsonRAT and AhMyth Android RAT C2 activity since at least 2022. As of this writing, shareboxs[.]net resolves to 173[.]212[.]206[.]227 .

Conclusion

The updates to the CapraRAT code between the September 2023 campaign and the current campaign are minimal, but suggest the developers are focused on making the tool more reliable and stable. The decision to move to newer versions of the Android OS are logical, and likely align with the group’s sustained targeting of individuals in the Indian government or military space, who are unlikely to use devices running older versions of Android, such as Lollipop which was released 8 years ago.

The APK theme updates show the group continues to lean into its social engineering prowess to gain a wider audience of targets who would be interested in the new app lures, such as mobile gamers or weapons enthusiasts.

To help prevent compromise by CapraRAT and similar malware, users should always evaluate the permissions requested by an app to determine if they are necessary. For example, an app that only displays TikTok videos does not need the ability to send SMS messages, make calls, or record the screen. In incident response scenarios, treat the related network indicators of compromise as suspect, including the use of port 18582, and search suspect apps for the presence of strings using the unique method names outlined in the Spyware Activities & C2 section of this report.

Indicators of Compromise

Files

SHA1	Name
28bc3b3d8878be4267ee08f20b7816a6ba23623e	TikTok signed.apk
c307f523a1d1aa928fe3db2c6c3ede6902f1084b	Crazy Game signed.apk
dba9f88ba548cebfa389972cddf2bec55b71168b	Sexy Videos signed.apk
fff24e9f11651e0bdbbee7c5cd1034269f40fc424	Weapons signed.apk

Network Indicators

Domain/IP	Description
shareboxs[.]net	C2 domain
173[.]212[.]206[.]227	Resolved C2 IP address, hosts shareboxs.net
173[.]249[.]50[.]243	Hardcoded failover C2 IP address

Source: <https://www.sentinelone.com/labs/capratube-remix-transparent-tribes-android-spyware-targeting-gamers-weapons-enthusiasts/>