

Android app breaking bad: From legitimate screen recording to file exfiltration within a year

[welivesecurity.com/2023/05/23/android-app-breaking-bad-legitimate-screen-recording-file-exfiltration/](https://www.welivesecurity.com/2023/05/23/android-app-breaking-bad-legitimate-screen-recording-file-exfiltration/)

May 23, 2023

ESET researchers discover AhRat – a new Android RAT based on AhMyth – that exfiltrates files and records audio



Lukas Stefanko

23 May 2023 - 11:30AM

ESET researchers discover AhRat – a new Android RAT based on AhMyth – that exfiltrates files and records audio

ESET researchers have discovered a trojanized Android app that had been available on the Google Play store with over 50,000 installs. The app, named iRecorder – Screen Recorder, was initially uploaded to the store without malicious functionality on September 19th, 2021. However, it appears that malicious functionality was later implemented, most likely in version 1.3.8, which was made available in August 2022.

Key points of the blogpost:

- As a Google App Defense Alliance partner, we detected a trojanized app available on the Google Play Store; we named the AhMyth-based malware it contained AhRat.
- Initially, the iRecorder app did not have any harmful features. What is quite uncommon is that the application received an update containing malicious code quite a few months after its launch.
- The application's specific malicious behavior, which involves extracting microphone recordings and stealing files with specific extensions, potentially indicates its involvement in an espionage campaign.
- The malicious app with over 50,000 downloads was removed from Google Play after our alert; we have not detected AhRat anywhere else in the wild.

It is rare for a developer to upload a legitimate app, wait almost a year, and then update it with malicious code. The malicious code that was added to the clean version of iRecorder is based on the open-source AhMyth Android RAT (remote access trojan) and has been customized into what we named AhRat.

Besides this one case, we have not detected AhRat anywhere else in the wild. However, this is not the first time that AhMyth-based Android malware has been available on Google Play; we previously [published our research](#) on such a trojanized app in 2019. Back then, the spyware, built on the foundations of AhMyth, circumvented Google's app-vetting process twice, as a malicious app providing radio streaming.

Overview of the app

Aside from providing legitimate screen recording functionality, the malicious iRecorder can record surrounding audio from the device's microphone and upload it to the attacker's command and control (C&C) server. It can also exfiltrate files with extensions representing saved web pages, images, audio, video, and document files, and file formats used for compressing multiple files, from the device. The app's specific malicious behavior – exfiltrating microphone recordings and stealing files with specific extensions – tends to suggest that it is part of an espionage campaign. However, we were not able to attribute the app to any particular malicious group.


As a Google App Defense Alliance partner, ESET identified the most recent version of the application as malicious and promptly shared its findings with Google. Following our alert, the app was removed from the store.

Distribution

The iRecorder application was initially released on the Google Play Store on September 19th, 2021, offering screen recording functionality; at that time, it contained no malicious features. However, around August 2022 we detected that the app's developer included malicious functionality in version 1.3.8. As illustrated in Figure 1, by March 2023 the app had amassed over 50,000 installations.

09:58 4G

← Google Play

 **iRecorder - Screen Recorder**
Coffeeholic Dev

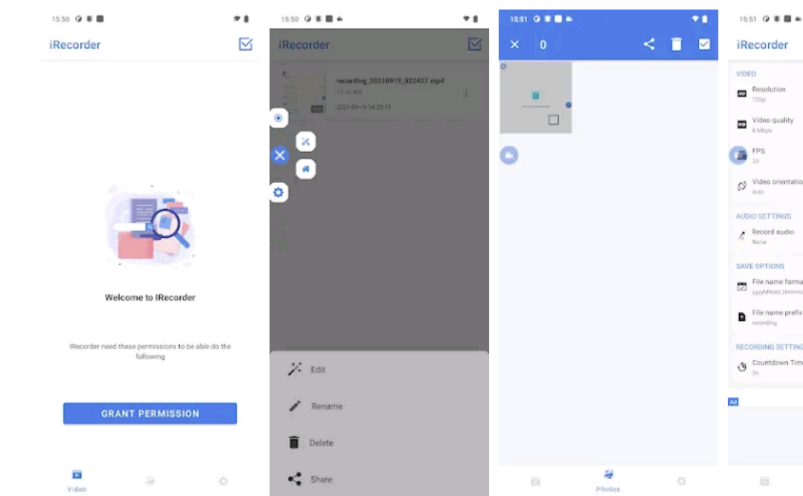
INSTALL

Contains ads

4.2 ★
259 reviews

50K+
Downloads

3
PEGI 3 ⓘ



Capture Screen - Simple Edit Crop Photo & Video - Add Music

[READ MORE](#)

Ratings and reviews ⓘ



Figure 1. The trojanized iRecorder app

However, Android users who had installed an earlier version of iRecorder (prior to version 1.3.8), which lacked any malicious features, would have unknowingly exposed their devices to AhRat, if they subsequently updated the app either manually or automatically, even without granting any further app permission approval.

Following our notification regarding iRecorder's malicious behavior, the Google Play security team removed it from the store. However, it is important to note that the app can also be found on alternative and unofficial Android markets. The iRecorder developer also provides other applications on Google Play, but they don't contain malicious code.

Attribution

Previously, the open-source AhMyth was employed by [Transparent Tribe](#), also known as APT36, a cyberespionage group known for its [extensive use of social engineering techniques](#) and targeting government and military organizations in South Asia. Nevertheless, we cannot ascribe the current samples to any specific group, and there are no indications that they were produced by a known advanced persistent threat (APT) group.

Analysis

During our analysis, we identified two versions of malicious code based on AhMyth RAT. The first malicious version of iRecorder contained parts of AhMyth RAT's malicious code, copied without any modifications. The second malicious version, which we named AhRat, was also available on Google Play, and its AhMyth code was customized, including the code and communication between the C&C server and the backdoor. By the time of this publication, we have not observed AhRat in any other Google Play app or elsewhere in the wild, iRecorder being the only app that has contained this customized code.

AhMyth RAT is a potent tool, capable of various malicious functions, including exfiltrating call logs, contacts, and text messages, obtaining a list of files on the device, tracking the device location, sending SMS messages, recording audio, and taking pictures. However, we observed only a limited set of malicious features derived from the original AhMyth RAT in both versions analyzed here. These functionalities appeared to fit within the already defined app permissions model, which grants access to files on the device and permits recording of audio. Notably, the malicious app provided video recording functionality, so it was expected to ask for permission to record audio and store it on the device, as shown in Figure 2. Upon installation of the malicious app, it behaved as a standard app without any special extra permission requests that might have revealed its malicious intentions.



Allow iRecorder to record audio?

Allow

Deny

iRecorder need these permissions to be able do the following

GRANT PERMISSION



Video



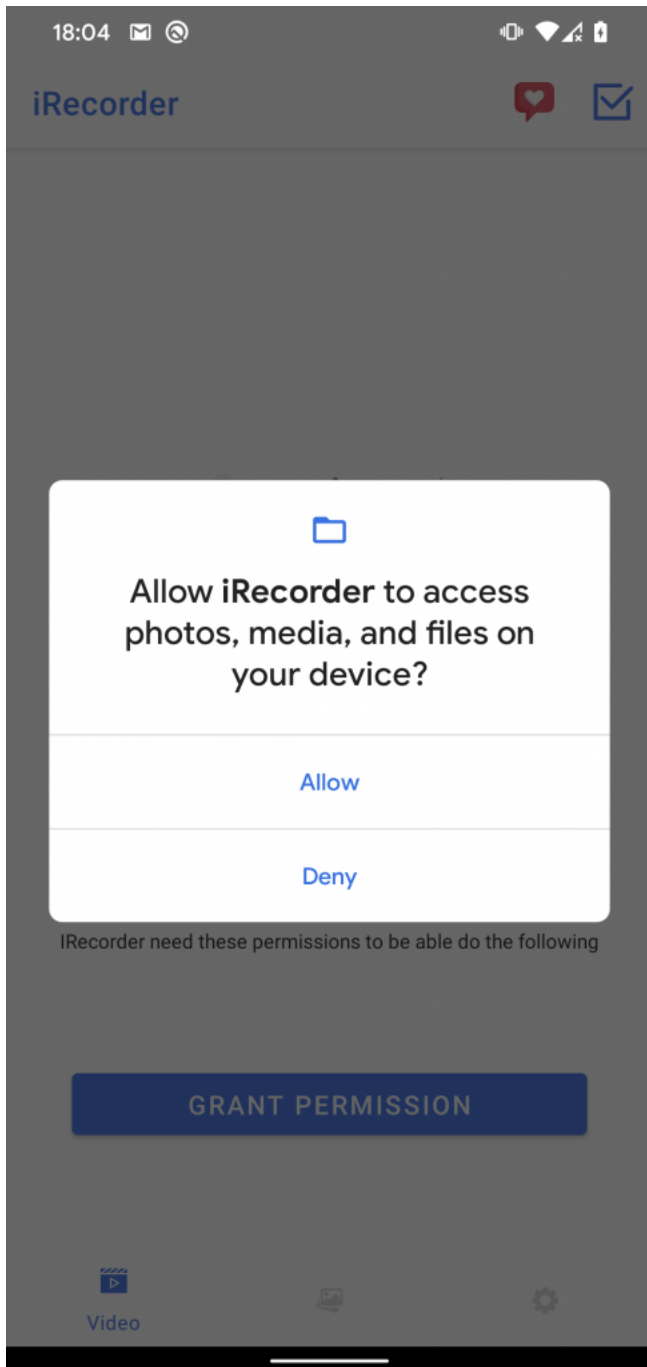


Figure 2. Permissions requested by the iRecorder app

After installation, AhRat starts communicating with the C&C server by sending basic device information and receiving encryption keys and an encrypted configuration file, as seen in Figure 3. These keys are used to encrypt and decrypt the configuration file and some of the exfiltrated data, such as the list of files on the device.

1051	https://order.80876dd5.shop	POST	/agent/init	✓	200	2434	JSON
1052	https://order.80876dd5.shop	POST	/agent/init	✓	200	2430	JSON
1053	https://order.80876dd5.shop	GET	/agent/config?clientId=9dc5f8b4d6341756	✓	200	5172	JSON
1054	https://order.80876dd5.shop	POST	/agent/data/encrypt	✓	200	391	JSON
1055	https://order.80876dd5.shop	POST	/agent/upload-file	✓	200	614	JSON
1056	https://order.80876dd5.shop	POST	/agent/upload-file	✓	200	611	JSON
1057	https://order.80876dd5.shop	POST	/agent/upload-file	✓	200	647	JSON
1058	https://order.80876dd5.shop	POST	/agent/upload-file	✓	200	902	JSON

Figure 3. AhRat's initial C&C communication

After the initial communication, AhRat pings the C&C server every 15 minutes, requesting a new configuration file. This file contains a range of commands and configuration information to be executed and set on the targeted device, including the file system location from which to extract user data, the file types with particular extensions to extract, a file size limit, the duration of microphone recordings (as set by the C&C server; during analysis it was set to 60 seconds), and the interval of time to wait between recordings – 15 minutes – which is also when the new configuration file is received from the C&C server.

Interestingly, the decrypted configuration file contains more commands than AhRat is capable of executing, as certain malicious functionality has not been implemented. This may indicate that AhRat is a lightweight version similar to the initial version that contained only unmodified malicious code from the AhMyth RAT. Despite this, AhRat is still capable of exfiltrating files from the device and recording audio using the device's microphone.

Based on the commands received in the configuration from the C&C server, AhRat should be capable of executing 18 commands. However, the RAT can execute only the six commands from the list below marked in bold and with an asterisk:

- **RECORD_MIC***
- CAPTURE_SCREEN
- LOCATION
- CALL_LOG
- KEYLOG
- NOTIFICATION
- SMS
- OTT
- WIFI
- APP_LIST
- PERMISSION
- CONTACT
- **FILE_LIST***
- **UPLOAD_FILE_AFTER_DATE***
- **LIMIT_UPLOAD_FILE_SIZE***
- **UPLOAD_FILE_TYPE***
- **UPLOAD_FILE_FOLDER***
- SCHEDULE_INTERVAL

The implementation for most of these commands is not included in the app's code, but most of their names are self-explanatory, as shown also in Figure 4.

The remotely controlled AhRat is a customization of the open-source AhMyth RAT, which means that the authors of the malicious app invested significant effort into understanding the code of both the app and the back end, ultimately adapting it to suit their own needs.

AhRat's malicious behavior, which includes recording audio using the device's microphone and stealing files with specific extensions, might indicate that it was part of an espionage campaign. However, we have yet to find any concrete evidence that would enable us to attribute this activity to a particular campaign or APT group.

IoCS

Files

SHA-1	Package name	ESET detection name	Description
C73AFFAF6A9372C12D995843CC98E2ABC219F162	com.tsoft.app.iscreenrecorder	Android/Spy.AhRat.A	AhRat backdoor.
E97C7AC722D30CCE5B6CC64885B1FFB43DE5F2DA	com.tsoft.app.iscreenrecorder	Android/Spy.AhRat.A	AhRat backdoor.
C0EBCC9A10459497F5E74AC5097C8BD364D93430	com.tsoft.app.iscreenrecorder	Android/Spy.Android.CKN	AhMyth-based backdoor.
0E7F5E043043A57AC07F2E6BA9C5AEE1399AAD30	com.tsoft.app.iscreenrecorder	Android/Spy.Android.CKN	AhMyth-based backdoor.

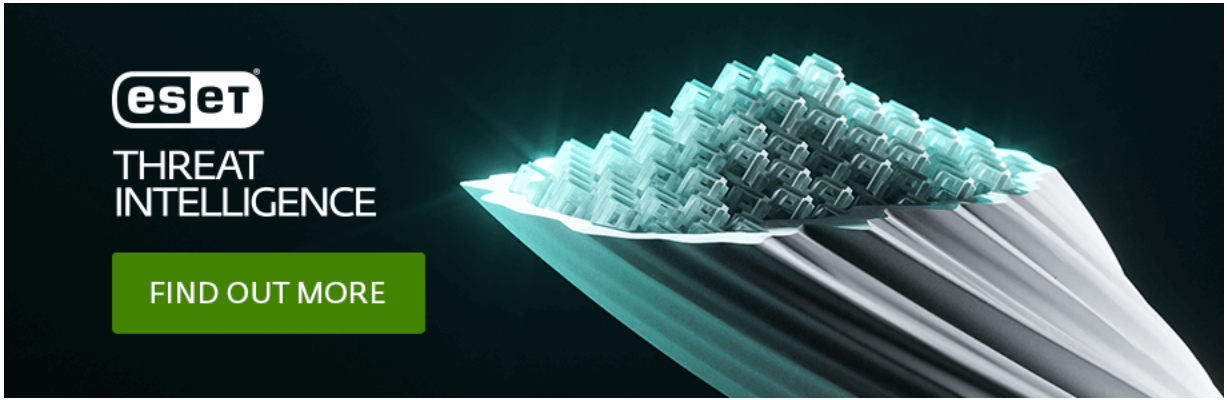
Network

IP	Provider	First seen	Details
34.87.78[.]222	Namecheap	2022-12-10	order.80876dd5[.]shop C&C server.
13.228.247[.]118	Namecheap	2021-10-05	80876dd5[.]shop:22222 C&C server.

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	AhRat receives the <code>BOOT_COMPLETED</code> broadcast intent to activate at device startup.
	T1624.001	Event Triggered Execution: Broadcast Receivers	AhRat functionality is triggered if one of these events occurs: <code>CONNECTIVITY_CHANGE</code> , or <code>WIFI_STATE_CHANGED</code> .
Discovery	T1420	File and Directory Discovery	AhRat can list available files on external storage.
	T1426	System Information Discovery	AhRat can extract information about the device, including device ID, country, device manufacturer and mode, and common system information.
Collection	T1533	Data from Local System	AhRat can exfiltrate files with particular extensions from a device.
	T1429	Audio Capture	AhRat can record surrounding audio.
Command and Control	T1437.001	Application Layer Protocol: Web Protocols	AhRat uses HTTPS to communicate with its C&C server.
Exfiltration	T1646	Exfiltration Over C2 Channel	AhRat exfiltrates stolen data over its C&C channel.



23 May 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
