# FastViewer Variant Merged with FastSpy and disguised as a Legitimate Mobile Application

S2W ⋮⋮ 10/30/2023

**Author**: Youngjae Shin, Sebin Lee | BLKSMTH

*: Oct 30, 2023*

Photo by on

## Executive Summary

- The S2W Threat Analysis team recently hunted and analyzed a new FastViewer sample from the Kimsuky APT group behind North Korea, and found that the group seems to be using a variant of FastViewer.

— Past FastViewer and FastSpy analysis reports: (2022–10–24) Unveil the evolution of Kimsuky targeting Android devices with newly discovered mobile malware

- The variant has been in production since at least July 2023 and, like the initial version, is found to induce installation by distributing repackaged APKs that include malicious code in legitimate apps.

— The package name, app name, icon, and some features are identical to the legitimate app.

- The exact distribution route of the malicious app has not been identified, but it is believed to be the same as last year, disguised as a legitimate app through spearphishing emails or smishing to trick targets into running it.

— As noted in a security advisory published by Korea's National Cyber Security Center last year, it is possible to exploit the Google Play Sync feature to force installation.

- In the past, FastViewer was responsible for downloading and loading the FastSpy, which is the actual remote control module, but the newly identified variant integrates some of the functionality of FastViewer with FastSpy and does not download additional malware.

— FastSpy is based on AndroSpy, an Android open-source written in Xamarin.

- The variant has all the same features as the old FastViewer, including string obfuscation, the name of the class, generated value to identify the victim, and the use of the Turkish language.
- The Kimsuky group continues to utilize mobile malware that disguises a major portal and popular apps in South Korea.

## Introduction

In October 2022, we identified malware disguised as a "Hancom Office Viewer" and linked it to the North Korean-based threat group Kimsuky. The malware was named FastViewer by S2W, and the additional mobile RAT downloaded was named FastSpy.

In the past, the FastViewer malware only executed malicious behavior when a specially created document created by the attacker was loaded. If the first 4 bytes of the file have the value "EDC%", the malicious code is executed, downloads the FastSpy malware from the C&C server, and dynamically loads it.

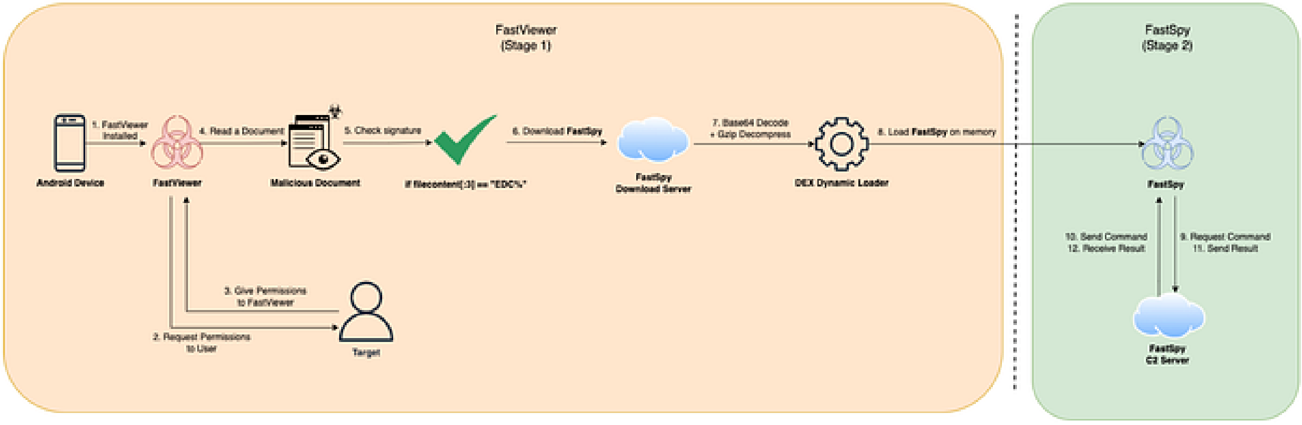


Figure 1. Overall attack flow in 2022

At the time, we traced and analyzed the C&C server used by the FastViewer and FastSpy malware, and confirmed the link between the malware and the Kimsuky group. Recently, through our threat hunting, we further identified a variant of FastViewer with some changes in functionality, and we would like to describe our analysis.

## Detailed Analysis

FastViewer impersonated a Korean Hangul Word Processor (HWP) file viewer program called Hancom Office last year, but the latest iteration of FastViewer disguises itself as a legitimate app unrelated to file viewers. Below is a list of the apps that FastViewer has impersonated so far. In addition to this, we have also seen FastViewer trying to disguise itself as a Google Authenticator, anti-virus, or payment service app.

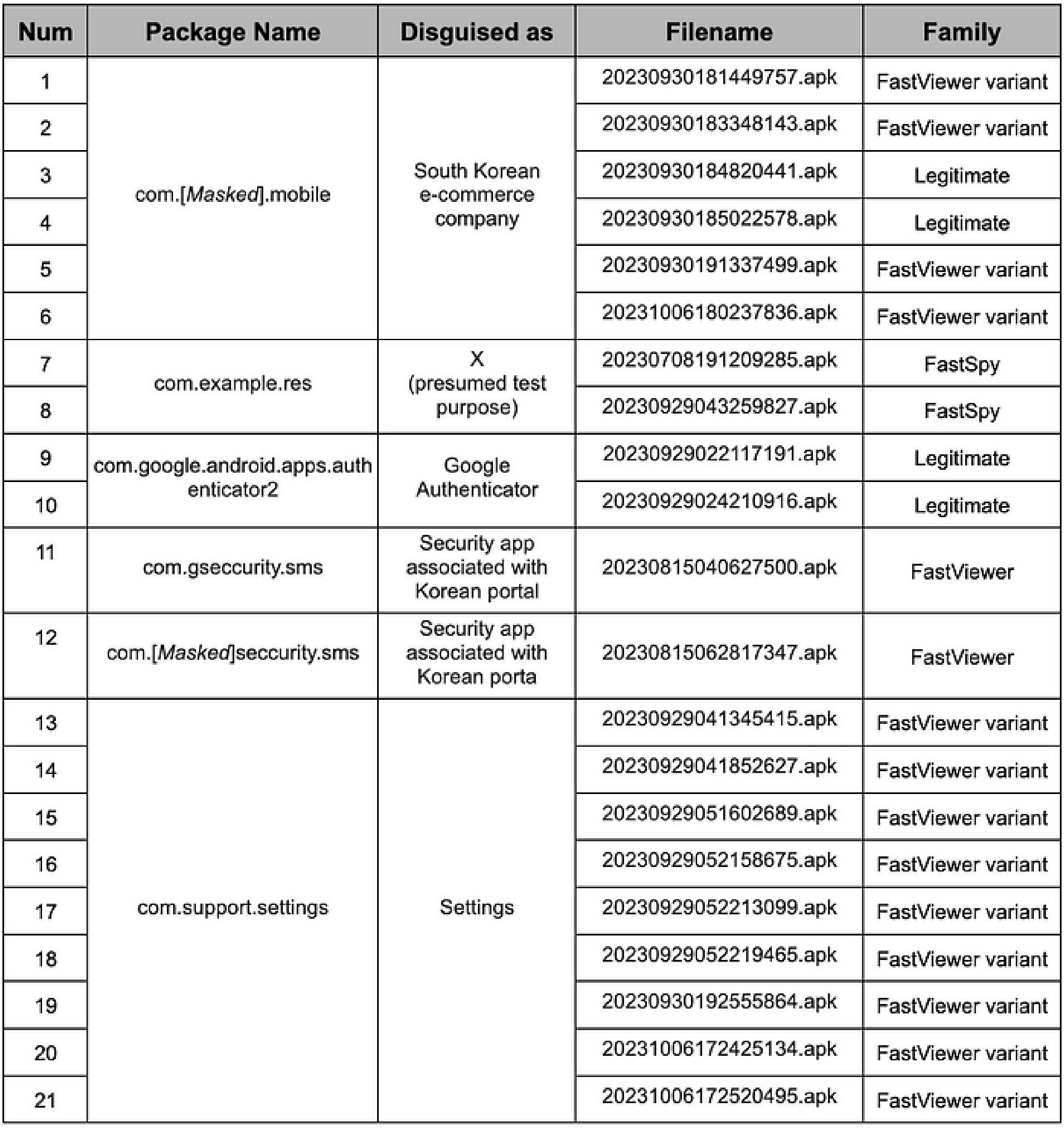
- Security app associated with a major Korean portal (which doesn't actually exist)
- South Korean e-commerce company
- Settings, etc.

The FastViewer we analyzed last year downloaded an additional malicious app based on the open-source project AndroSpy called FastSpy to execute commands, and in the case of the FastViewer we identified this time, some of the features of FastSpy were merged.

In addition, previously, the FastViewer disguised as a viewer file was configured to execute the malicious behavior only when the first 4 bytes of the file (EDC%) were loaded, but the latest version does not seem to have adopted the above feature in that this feature is not called. Also, since they are no longer using FastSpy and have integrated some of its features into FastViewer, it is assumed that they have removed the document triggering process since they are using a common app theme.

## Server Analysis

From the servers identified as being operated by the Kimsuky group, we secured 21 APK files that appear to have been created by the attackers. After categorizing the files, a total of 6 package names were used and 5 themes were identified. Based on the saved filenames, it appears that they have been preparing for this campaign since at least July 8, 2023.



| Num | Package Name | Disguised as | Filename | Family |
|---|---|---|---|---|
| 1 | com.[*Masked*].mobile | South Korean e-commerce company | 20230930181449757.apk | FastViewer variant |
| 2 | | | 20230930183348143.apk | FastViewer variant |
| 3 | | | 20230930184820441.apk | Legitimate |
| 4 | | | 20230930185022578.apk | Legitimate |
| 5 | | | 20230930191337499.apk | FastViewer variant |
| 6 | | | 20231006180237836.apk | FastViewer variant |
| 7 | com.example.res | X (presumed test purpose) | 20230708191209285.apk | FastSpy |
| 8 | | | 20230929043259827.apk | FastSpy |
| 9 | com.google.android.apps.authenticator2 | Google Authenticator | 20230929022117191.apk | Legitimate |
| 10 | | | 20230929024210916.apk | Legitimate |
| 11 | com.gseccurity.sms | Security app associated with Korean portal | 20230815040627500.apk | FastViewer |
| 12 | com.[*Masked*]seccurity.sms | Security app associated with Korean porta | 20230815062817347.apk | FastViewer |
| 13 | com.support.settings | Settings | 20230929041345415.apk | FastViewer variant |
| 14 | | | 20230929041852627.apk | FastViewer variant |
| 15 | | | 20230929051602689.apk | FastViewer variant |
| 16 | | | 20230929052158675.apk | FastViewer variant |
| 17 | | | 20230929052213099.apk | FastViewer variant |
| 18 | | | 20230929052219465.apk | FastViewer variant |
| 19 | | | 20230930192555864.apk | FastViewer variant |
| 20 | | | 20231006172425134.apk | FastViewer variant |
| 21 | | | 20231006172520495.apk | FastViewer variant |

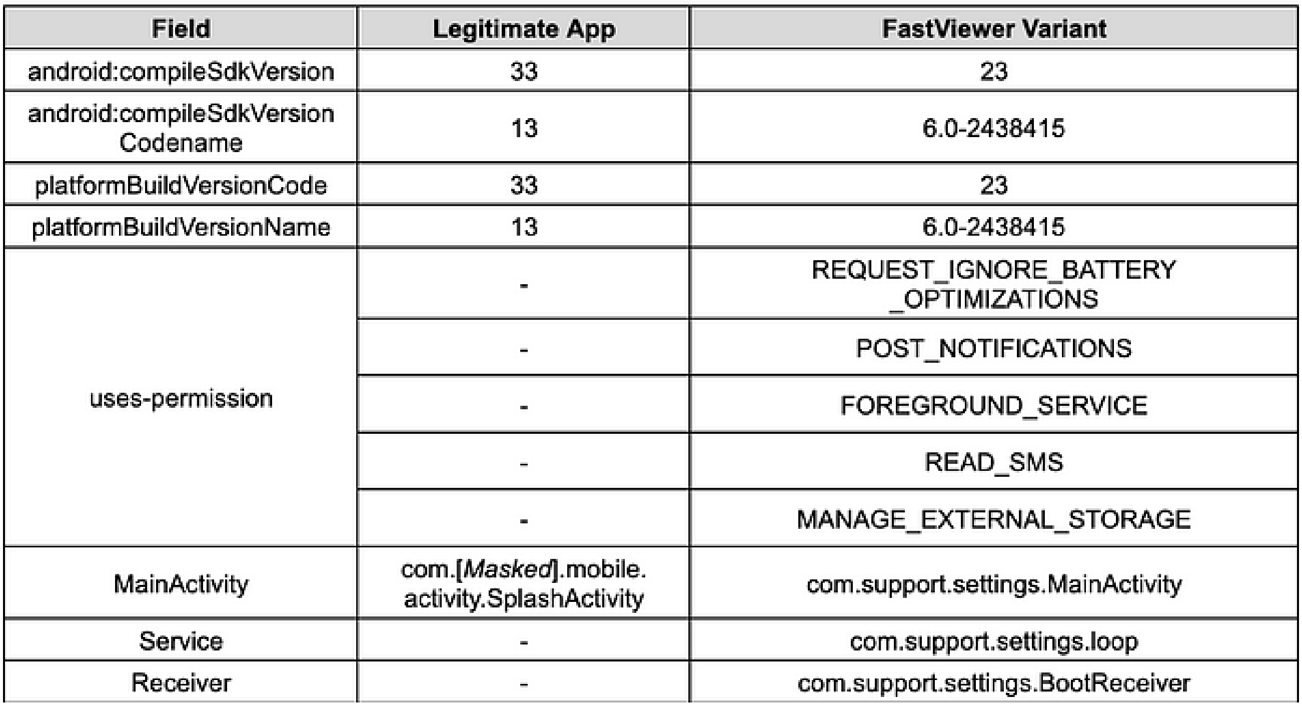
Table 1. Acquired APK classification

The 144.76.109[.]61 server operated by the attacker at the time was directory listed, allowing us to see all of the files uploaded to it, which further confirmed that the AsyncRAT malware was uploaded on the server.

## Analysis of FastViewer Variant

After analyzing the malicious apps, we found that the latest version of FastViewer used the same package name, app name, and app icon as the legitimate app. In the past, the package name and app icon were partially different from the legitimate app, but this time it was implemented the same as the legitimate app, making it difficult to distinguish the malicious app from the app.

In addition, fields such as Target SDK and main activity information in the AndroidManifest.xml were tampered with, and permissions, broadcast receivers, and services were added for malicious behavior.



| Field | Legitimate App | FastViewer Variant |
|---|---|---|
| android:compileSdkVersion | 33 | 23 |
| android:compileSdkVersion Codename | 13 | 6.0-2438415 |
| platformBuildVersionCode | 33 | 23 |
| platformBuildVersionName | 13 | 6.0-2438415 |
| uses-permission | - | REQUEST_IGNORE_BATTERY _OPTIMIZATIONS |
|  | - | POST_NOTIFICATIONS |
|  | - | FOREGROUND_SERVICE |
|  | - | READ_SMS |
|  | - | MANAGE_EXTERNAL_STORAGE |
| MainActivity | com.[*Masked*].mobile. activity.SplashActivity | com.support.settings.MainActivity |
| Service | - | com.support.settings.loop |
| Receiver | - | com.support.settings.BootReceiver |

Table 2. Modified and added fields (AndroidManifest.xml)

1.

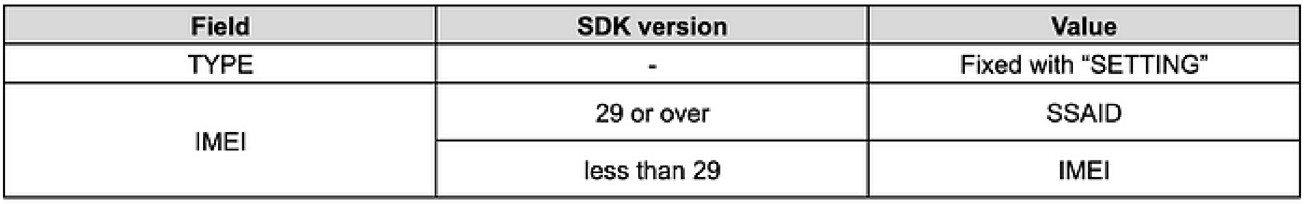
FastViewer variant calls a service if a specific permission is granted, or executed by a receiver at boot time. When the malware is launched, the added or tampered main activity checks if the **battery optimization permission** is granted to the app and if not, it requests permission from the user. If the battery optimization permission is granted, the malicious behavior is performed by calling the malicious service.

In addition, when the device reboots or a boot-related event occurs after the app is installed, the broadcast receiver added during the repackaging executes the malicious service. When the malware is invoked by receiving a boot event, it does not check for battery optimization permissions, unlike the main activity case. If the app has additional permissions to read SMS and access all files, it will execute normal update-related activities.

**2. Information theft**

The main purpose of the FastViewer variant is to steal information from the infected device. Once the malicious service is triggered by the aforementioned conditions, the malicious code implemented inside is executed repeatedly at a set cycle. (Default value is 5 minutes) It then sends the infected device's information in plain text, prefixed with the string "Kur-" to identify the infected device. This format of string is recognized by the same characteristics as FastViewer, FastSpy, and AndroSpy in the past. After transmission, it receives commands from the C&C server and performs malicious actions corresponding to those commands.

- C&C server: http[:]//144.76.109[.]61/dash/index.php?ati=



| Field | SDK version | Value |
|---|---|---|
| TYPE | - | Fixed with "SETTING" |
| IMEI | 29 or over | SSAID |
|  | less than 29 | IMEI |

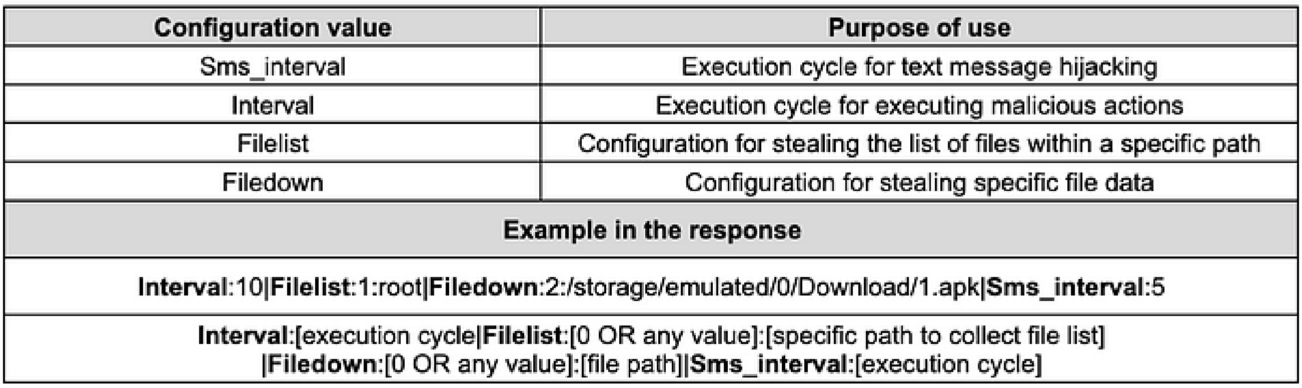
Table 3. List of collected information

### 3. Command and Control

The FastViewer variant communicates with the C&C server repeatedly for the time specified in the Interval value of the setting value as described above. At this time, it reads the setting.txt file stored for each infected device from the C&C server, which contains a list of configuration values.

For command and control, it refers to the above data to determine whether to perform malicious behavior. Depending on the value of the received command, it is determined whether to perform SMS stealing, resetting the malicious behavior execution cycle, file list stealing, and file data stealing.

In the case of file list/data stealing commands, the value for the command must be set to 0 to be executed, but the default settings are set to 1 and 2, respectively, so it works only by updating the configuration value.

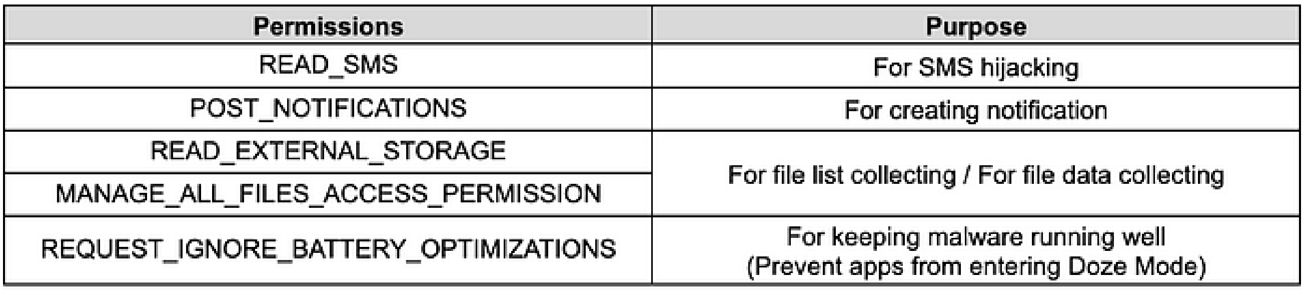


| Configuration value | Purpose of use |
|---|---|
| Sms_interval | Execution cycle for text message hijacking |
| Interval | Execution cycle for executing malicious actions |
| Filelist | Configuration for stealing the list of files within a specific path |
| Filedown | Configuration for stealing specific file data |
| **Example in the response** | |
| **Interval**:10\|**Filelist**:1:root\|**Filedown**:2:/storage/emulated/0/Download/1.apk\|**Sms_interval**:5 | |
| **Interval**:[execution cycle\|**Filelist**:[0 OR any value]:[specific path to collect file list]<br>\|**Filedown**:[0 OR any value]:[file path]\|**Sms_interval**:[execution cycle] | |

Table 4. Configurations for each malicious behavior received from the server

### 4. Permissions

The permissions required by FastViewer variants to perform malicious behaviors are as follows. The permissions requested from the user include “READ_SMS” to steal text messages, “POST_NOTIFICATIONS” to generate notifications, access to external storage/all files to steal files or file data after communication, and battery optimization mode to prevent the app from entering Doze Mode.



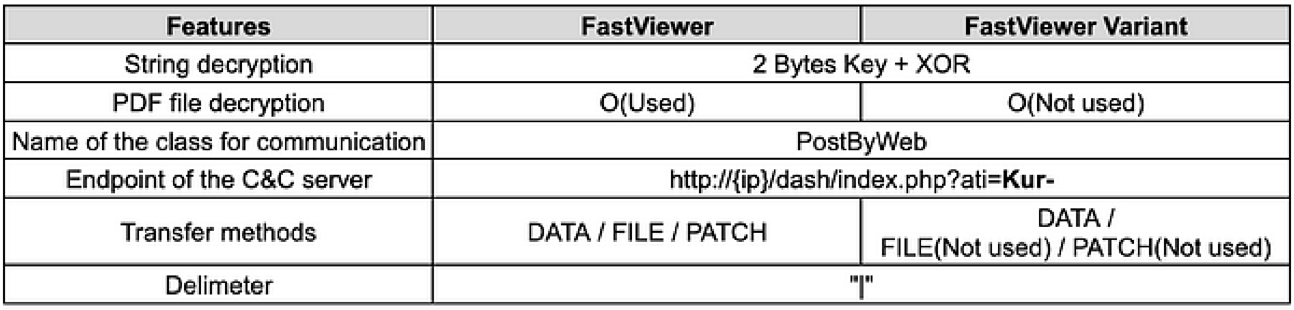
| Permissions | Purpose |
|---|---|
| READ_SMS | For SMS hijacking |
| POST_NOTIFICATIONS | For creating notification |
| READ_EXTERNAL_STORAGE | For file list collecting / For file data collecting |
| MANAGE_ALL_FILES_ACCESS_PERMISSION | |
| REQUEST_IGNORE_BATTERY_OPTIMIZATIONS | For keeping malware running well<br>(Prevent apps from entering Doze Mode) |

Table 5. List of requested permissions

### 5. Association with Old FastViewer

The past FastViewer and FastSpy feature an XOR operation with a decryption key of 2 bytes in size to decrypt the encrypted string. The variant of FastViewer also uses this feature, which is the biggest similarity to the old one, except for the Turkish language variable due to AndroSpy.

Furthermore, the PDF decryption method, the name of the class that performs the C&C communication, the endpoint when communicating with the C&C, the commands received from the C&C, and the command separators received are also the same as the old FastViewer.



| Features | FastViewer | FastViewer Variant |
|---|---|---|
| String decryption | 2 Bytes Key + XOR | |
| PDF file decryption | O(Used) | O(Not used) |
| Name of the class for communication | PostByWeb | |
| Endpoint of the C&C server | http://{ip}/dash/index.php?ati=**Kur-** | |
| Transfer methods | DATA / FILE / PATCH | DATA /<br>FILE(Not used) / PATCH(Not used) |
| Delimeter | "\|" | |

Table 6. Comparison of past and current versions of FastViewer

## Conclusion

- Unlike in the past, the newly identified FastViewer malware receives commands directly from the server without downloading additional malware (FastSpy).
- It uses the same package name as the legitimate app, so it can replace the original app if a variant of FastViewer with the same package name is installed on a device that already has the legitimate app installed.
- There are no known cases of this variant being distributed in the wild, but based on the Kimsuky group's past malware distribution methods, it is possible that it could be distributed in the future through spearphishing or smishing to exploit the Google Sync feature.

## IoCs

- f1570d3c0974968d3c7acaa268d36497 (FastSpy)
- 0a3fe48c8ff1f7c50c22accfc5185d42 (FastSpy)
- d1af9d1d4580e4a578f10b9515963545 (FastViewer)
- f334167b35ae5b6e1166819f98e77c90 (FastViewer)
- dec2ca08aa5abbc4d0e20ab67aa26e5d (FastViewer variant)
- d66aeb492dec0c88d447711017458182 (FastViewer variant)
- 7ced6bf0f2e26716a0ed64238425e29f (FastViewer variant)
- a810fafd4b6ac524ce032896c295f37b (FastViewer variant)
- 02dd6e7a49138d4fe7c4a8cd920afb21 (FastViewer variant)
- 536e736ea4009376f60f77f044461bee (FastViewer variant)
- a7412db9b5bcf564d66b2babdc26aa39 (FastViewer variant)
- 72587b3da56546285496198af6c67809 (FastViewer variant)
- 1315ac032903371e6e1be2f06875c117 (FastViewer variant)
- 144.76.109[.]61 (C&C Server)

## MITRE ATT&CK

### Persistence

- (T1624.001) Broadcast Receivers

### Discovery

- (T1420) File and Directory Discovery

### Collection

- (T1636.004) SMS Messages
- (T1533) Data from Local System

**Command and Control**

- (T1437.001) Web Protocols

**Exfiltration**

- (T1646) Exfiltration Over C2 Channel