Unveil the evolution of Kimsuky targeting Android devices with newly discovered mobile malware

medium.com/s2wblog/unveil-the-evolution-of-kimsuky-targeting-android-devices-with-newly-discovered-mobile-malware-280dae5a650f

S2W

November 24, 2022


18
4
13
10

S2W

Oct 24

.

14 min read

Author: Sebin, Lee & Yeongjae, Shin | S2W TALON

> *: Oct 24, 2022*

Photo by on

Executive Summary

- S2W's threat research and intelligence center, Talon, recently identified three new types of malware that target Android devices.
- We named the malicious APKs , , and by adding 'Fast' included in the package name and the characteristics of each.
- As a result of analyzing the APKs, we figured out that there is a significant association with the past campaigns attributed to Kimsuky group.
- The malware is disguised as a Google security plugin, and the malware disguises itself as "Hancom Office Viewer", is a remote access tool based on AndroSpy.
- All three APKs were recently confirmed to have been developed by the Kimsuky group and were actually used to attack South Koreans.
- Since Kimsuky group's mobile targeting strategy is getting more advanced, it is necessary to be careful about sophisticated attacks targeting Android devices.
- An understanding of the Kimsuky group's new strategy for targeting mobile devices that we have described will help to prevent infection proactively.

— Be careful not to open phishing pages on mobile

— Be careful not to download a viewer program and document files from third parties and anyone.

Introduction

North Korean hacking groupKimsuky (aka Thallium, Black Banshee) first became active in 2012 and has carried out attacks on targets engaged in Media, Research, Politics, and Diplomacy, etc around the world. The group mainly attempts to collect by distributing malware and taking over accounts through spear-phishing attacks. Attacks have mainly targeted Windows, though instances of attacks on Android devices have likewise been discovered.

In November 2020, we found the mobile version of the AppleSeed family used by Kimsuky group. In that sample, the group even called themselves Thallium, a name given by Microsoft. We published our analysis on VB2021 localhost.

In April 2021, a malicious APK disguised as a mobile security program of KISA (Korea Internet & Security Agency) to which KrCERT/CC belongs was distributed. The APK was also a mobile version of the *AppleSeed* family. When infected with a malicious APK, it communicates with the C&C server using the HTTP/S protocol, receives commands, and performs malicious behaviors such as stealing information from the infected device.

S2W's threat research and intelligence center, Talon, recently identified three new types of malware that target Android devices in the process of tracking the Kimsuky group. We named the three malicious APKs **FastFire**, **FastViewer**, and **FastSpy** by adding 'Fast' included in the package name of each malicious APK and the characteristics of each.

1. is a malicious APK currently being developed by the Kimsuky group, disguised as a Google security plug-in. It receives commands from Firebase, an app development platform backed by Google, rather than receiving commands from the C&C through HTTP/S communication as in the traditional method.
2. malware disguises itself as "Hancom Viewer", a mobile viewer program that can read the Hangul documents (.hwp) used in Korea, and downloads additional malware after stealing information from an infected device.
3. The FastViewer malware downloads , and receives commands from the attacker's server through TCP/IP protocol. FastSpy is developed based on the source code of AndroSpy, a remote control tool for Android devices that was released as an .

FastFire malware disguised as Google Security Plugin

Analyzing the IP of the C&C server domain used by the Kimsuky group in the past, we found a suspected malicious APK that the Kimsuky group is developing to target mobile devices. It is named "**FastFire**" as its package name contains "**fast**secure" and uses the "**Fire**base" for C&C communication.

> All antivirus vendors in VirusTotal have not classified the APK as malicious so far. (detection result 0/64, as of 2022.10.18)

The malicious APK has a package name *com.viewer.fastsecure* and disguises Google Security Plugin. After installation, it hides its launcher icon so that the victim does not know that it is installed.

> APK File Certificate Information ()

Detailed analysis of FastFire

FastFire contains five malicious classes. After installation, only three classes are actually executed, and two classes are not. FastFire transmits a device token to the C&C server, and then the C&C server sends a command to the infected device through Firebase Cloud Messaging (FCM).

1. Request a permission

When FastFire is executed, MainActivity class is executed first, and "*You must grant permission to the Google Security Plugin in order to be safely downloaded.*" message is displayed, and the MANAGE_OVERLAY_PERMISSION permission is requested. If permission is granted, the message "*Downloaded safely*" is displayed.

2. C&C Communication in Services

In the manifest file in FastFire, two classes are specified to be executed as services. Of these, only the *MyFirebaseMessagingService* class is actually executed.

StartModuleService

The *StartModuleService* class is specified on the manifest, but it is not actually executed when FastFire is running. This class performs the function of reading a specific HTML page through the Android VIEW indent.

startmodule

startmodule class is not in the manifest nor is it called by another class, but a malicious code is implemented. Kimsuky group conducts phishing attacks disguised as the site to hijack the accounts of large Korean portal sites such as Naver and Daum, FastFire malware also targets the two portal sites. If the string "naver", "daum" or "facebook" exists in the value received as an argument when calling the startmodule class, it connects to the C&C server and gets an HTML page. As that class is not actually called, it is likely still in development.

- hxxp[:]//mc.pzs[.]kr/themes/mobile/images/about/temp/android/naver.html
- hxxp[:]//mc.pzs[.]kr/themes/mobile/images/about/temp/android/daum.html
- hxxp[:]//mc.pzs[.]kr/themes/mobile/images/about/temp/android/facebook.html

MyFirebaseMessagingService

Firebase is a mobile development platform that provides various necessary functions such as DB, authentication, and messaging. Using this, message payloads can include a notification property that the Firebase SDKs intercept and attempt to display a visible notification to users.

MyFirebaseMessagingService class performs malicious behaviors by receiving commands through Firebase Cloud Messaging (FCM). FastFire generates a device token to use FCM, and the token value is transmitted to the C&C server. After obtaining the token, the attacker makes a request to Firebase to send a message payload containing the attacker's command to the infected device. In response to the request, Firebase sends a message to the device.

> hxxp[:]//navernnail[.]com/fkwneovjubske4gv/report_token/report_token.php?token=[Device token]

When the command is received, the onMessageRecived method is executed to perform an action. If the data of *my_custom_key* exists in the message, FastFire reads an HTML file from the C&C server and connects the deep link that takes the user to a specific page in an app. The HTML file according to whether the value is "naver", "daum", or "facebook".

- hxxp[:]//navernnail[.]com/fkwneovjubske4gv/android/naver.html
- hxxp[:]//navernnail[.]com/fkwneovjubske4gv/android/daum.html
- hxxp[:]//navernnail[.]com/fkwneovjubske4gv/android/facebook.html

3. Additional C&C Server and Malicious Pages

After further analysis of FastFire's infrastructure, an additional domain assigned to the Resolved IP of FastFire's C&C server was discovered. Since the domain has specific HTML files in the same directory path as FastFire's, it is also identified as another C&C server used by Kimsuky.

- FastFire's C&C Server: navernnail[.]com ()
- Additional C&C server: goooglesecurity[.]com ()

The HTML file obtained from the additional C&C server performs the function of calling a specific application through a deep link on an Android device. FastFire takes the user to a specific page in an app using the deep link according to the command, but the values in the secured HTML were all unidentified. The attacker is expected to fill in that value with a test APK name "*[Target]_host"* or a random string for the test.

Generally, the notification sent from Firebase is handled with the *onMessageReceived* method. However, the feature is not performed as the method is not implemented. Also, in a separate function for testing notifications, related messages *Facebook* and *Google* are included in Turkish.

In addition, a file "fcm.html" was secured, and it calls the *fcm_host* through the deep link and downloads additional malicious code.

> hxxp[:]//goooglesecurity[.]com/fkwneovjubske4gv/android/fcm.html

As such, FastFire is believed to be a new mobile malware currently being developed by the Kimsuky group in that the deep link calling function is not yet properly implemented and there are classes that are not actually executed.

FastViewer & FastSpy disguised as Hancom Office Viewer

In addition to FastFire, we discovered mobile RAT that impersonates the “Hancom Office Viewer”. “Hancom Office Viewer” is a mobile document viewer application used to view Microsoft Word, PDF, or ‘Hangul (.hwp)’ documents and the number of downloads on the Google Play store is over 10 million.

FastViewer normally performs a document viewer, but when **reading a document file specially created by an attacker**, it performs malicious behaviors. The first 4 bytes of the file are checked to determine whether the document was created by the attacker, and if the conditions are met, device information is transmitted to the C&C server. After that, FastViewer additionally downloads **FastSpy** malware and executes it in memory to perform additional malicious actions.

FastViewer is a repackaged APK by adding arbitrary malicious code inserted by an attacker to the normal Hancom Office Viewer app, and the package name, app name, and icon are very similar to the normal app.

- 8420236c32f0991feaa7869549abdb97 (Hancom Office Viewer
- 3458daa0dffdc3fbb5c931f25d7a1ec0 (FastViewer)

FastViewer is signed with *jks* certificate (Java-based certificate format). The certificate information is as follows. (Link)

FastViewer

Detailed analysis of FastViewer & FastSpy

1. String decryption algorithm

The string used in FastViewer is decrypted by the custom algorithm. The encrypted string is used as the first argument, and the index of the key table is used as the second argument. After obtaining a key pair using the value of the XOR key table corresponding to the index, XOR is performed alternately from the back of the encrypted string.

2. Request permissions

FastViewer requests additional permissions from users for malicious actions such as receiving commands, persistence, and spying. FastViewer abuses accessibility, so it is checked whether accessibility is enabled before performing malicious behaviors.

The class name that requests the permissions is “HiPermission”, which is an open-source that has been released in the past. It is believed that Kimsuky group partially modified the source code and applied it to FastViewer.

3. Check the header of document files

Malicious behavior operates when a special document file created by an attacker is read, by checking whether the first 4 bytes of the file are “EDC%”. It then changes “EDC%” to the original 4 bytes, converting it to a normal document and displaying it to the user, executing malicious behavior in the background.

According to the calling condition, malicious behavior is performed that meets the condition according to the variable “StrOpt”.

4. C&C Communication

FastViewer collects the information of the device and sends it to the C&C server as an *ati* parameter. If the app acquires permissions on the device and successfully gets the Device’s IMEI value, the ati parameter is assigned “Kur-{Device IMEI}_{Device IMEI}”. If IMEI value cannot be acquired due to permission failure or other problems, *ati* is assigned “Kur-null_error_imei”.

- (Success) hxxp://23.106.122[.]16/dash/index.php?&ati=
- (Fail) hxxp://23.106.122[.]16/dash/index.php?&ati=

After that, the data that FastViewer receives from the C&C server is as follows, and it determines whether to download additional modules by comparing the version variable defined in the FastViewer with the version value received from the server. If the response value is “ok”, only simple information stealing is performed, and an additional module is not downloaded.

> (Response)
> version:0|rat:on|ip:23.106.122[.]16|port:4545|package:com.example.res|interval:120

As above, when information about the additional module is successfully received, the request for downloading the module is sent to the C&C server. The version value is the value received from the server.

> (Download request) hxxp://23.106.122[.]16/dash/patch.php?name=Image.bin&ati=

5. Download an additional module — FastSpy

The downloaded module is a compressed DEX file, and the original data is extracted through base64 decoding and GZIP decompression in memory. The extracted file is **FastSpy** which performs remote control.

After data extraction, the malicious class in the DEX in memory is dynamically called by calling the LoadClass API that matches the SDK version of the device. If the class is successfully called, the decrypted DEX is saved as *image{version}.bin* in the app install path.

- Install Path: {App install path}/image{version}.bin
- Filename: image0.bin (version: 0)
- Package Name: com.example.res
- MD5 hash (Compressed): aefa23b91cc667be041cad40abbfa043
- MD5 hash (Extracted): 89f97e1d68e274b03bc40f6e06e2ba9a

When FastSpy is executed, the internally stored C&C server information is compared with the information previously received from the C&C server. If the two values are different, the information is updated in memory with the information received from the server.

Internally stored C&C server information
FastSpy could abuse the accessibility API obtained from FastViewer to get additional privileges without the user's consent. If FastSpy requests specific permission for malicious behaviors, a pop-up window requesting permission is displayed. In this case, FastSpy automates the function of clicking the "Agree" button in the window, so that FastSpy acquires the permission itself without interaction with users. However, it isn't actually called in FastSpy we secured.

The above method is similar to the method used by the previous Malibot malware to bypass Google MFA authentication.

sendAutoAction
FastSpy can take control of infected devices, hijack phone and SMS information, or identify the device's location and whether it is used via camera, microphone, speaker, GPS, or KeyStroke in real-time.

In addition, the attacker can access files on the infected device and send them to the C&C server. To exfiltrate, the file is compressed with the gzip algorithm and base64 encoding as used in FastSpy.

Correlation between FastSpy and AndroSpy

FastSpy and AndroSpy have similar characteristics in the method name, message format, functions, and code. AndroSpy is an open-source RAT malware that was released in 2018 and has the characteristic that methods and key variables are in Turkish.

Attribution

As a result of analyzing the association between the FastFire, FastViewer, and FastSpy malware and Kimsuky group, it was found that the FastFire's C&C server domain also used in the "다양한 주제의 보도자료를 사칭한 Kimsuky 공격시도" performed by Kimsuky group in the past.

Comparing the C&C URL released at the time and FastFire's C&C URL, the same domain was used for both campaigns, and the path under the *temp* directory was used. In addition, the group mainly impersonates Korean large portal sites (Naver and Daum) in order to steal information from the target.

The domains (navernnail[.]com, goooglesecurity[.]com) used by the FastFire malware have a history of pivoting to 23[.]106.122.16 in the past, and this IP was also used as a distribution site and C&C server for FastViewer and FastSpy.

In that, the signature date of FastViewer and that of FastFire are included within the period in which the navernnail[.]com domain which was bound to 23[.]106.122.16 (Singapore), all three malware and infrastructure are used by Kimsuky at the same time.

In addition, the fact that goooglesecurity[.]com, an additionally verified C&C server of FastFire, also supports this point.

Overlapped time
Figure 26. Overall infrastructure
During the analysis, there was a directory listing vulnerability in navernnail[.]com, so we were able to collect files existing on the server. Among them, the *key_ps.txt* file has a code similar to the keylogging script used by the Kimsuky group in the past, and the same mutex name is also used.

- Filename: key_ps.txt
- MD5 : 5D56371944DEC9DA57DB95D0199DD920
- Mutex name: Global\AlreadyRunning191122
- Reference:

Directory Listing
Figure 28. Kimsuky's keylogger script (key_ps.txt)
In addition, the *info_sc.txt* file was also confirmed to have similarities with Kimsuky group. February 18, 2022, the malicious document disguised as the customer center of Klip, a virtual asset wallet service in Korea, downloaded a very similar script.

Reference:

Left: 2022–02–18 1589989024.xml / Right: info_sc.txt

Conclusion

Kimsuky group has continuously performed attacks to steal the target's information targeting mobile devices. Firebase, a normal service used as the C&C server in **FastFire**, is their advanced tactic. In addition, various attempts are being made to bypass detection by customizing Androspy, an open-source RAT. In the future, caution is required as the Kimsuky group may distribute malicious codes with similar functions and variants to Android devices.

Like **FastViewer**, sophisticated attack vectors are used to attack only specific targets, and existing open sources are actively used to create high-performance variants such as **FastSpy**. Since Kimsuky group's mobile targeting strategy is getting more advanced, it is necessary to be careful about sophisticated attacks targeting Android devices.

Appendix A. IoC

IoC:

FastFire

- FDD0E18E841D3EC4E501DD8BF0DA68201779FD90237C1C67078D1D915CD13045
- C038B20F104BE66550D8DD3366BF4474398BEEA330BD25DAC2BB2FD4B5377332
- 1510780646E92CBEFC5FB4F4D7D2997A549058712A81553F90E197E907434672
- 38D1D8C3C4EC5EA17C3719AF285247CB1D8879C7CF967E1BE1197E60D42C01C5
- 884FF7E3A3CEA5CE6371851F205D703E77ABC7D1427D21800A04A205A124B649

FastViewer

031BDE16D3B75083B0ADDA754AA982D4F6BD91E6B9D0531D5486DC139A90CE5A

FastSpy

- AE7436C00E2380CDABBDCCCACF134B95DDBAF2A40483FA289535DD6207CC58CE
- 539231DEA156E29BD6F7ED8430BD08A4E07BA330A9FAD799FEA45D9E9EED070C

key_ps.txt

9722107FFF4F3B2255556E0CF4D367CCB73305C34B1746BAED31B16899EEFC4B

info_sc.txt

59CB6BB54A6A222C863258BAF9EE2500A539B55411B468A3E672FE7B26166B98

FastFire

- hxxp[:]//mc.pzs[.]kr/themes/mobile/images/about/temp/android/naver.html
- hxxp[:]//mc.pzs[.]kr/themes/mobile/images/about/temp/android/daum.html

- hxxp[:]//mc.pzs[.]kr/themes/mobile/images/about/temp/android/facebook.html
- hxxp[:]//navernnail[.]com/fkwneovjubske4gv/report_token/report_token.php?token=[Token]
- hxxp[:]//navernnail[.]com/fkwneovjubske4gv/android/naver.html
- hxxp[:]//navernnail[.]com/fkwneovjubske4gv/android/daum.html
- hxxp[:]//navernnail[.]com/fkwneovjubske4gv/android/facebook.html

FastViewer/FastSpy

- 23.106.122[.]16
- hxxp[:]//23.106.122.16/dash/index[.]php
- hxxp[:]//23.106.122.16/dash/patch[.]php

Appendix B. Mobile MITRE ATT&CK

Mobile MITRE ATT&CK:

Appendix C. Decryption key & Decrypted strings (FastViewer, FastSpy)

Decryption key table

Decrypted strings

Reference