

Lookout Discovers North Korean APT37 Mobile Spyware

lookout.com/threat-intelligence/article/lookout-discovers-new-spyware-by-north-korean-apt37



- KoSpy is a new Android spyware attributed to the North Korean group APT37. It masquerades as utility apps and targets Korean and English speaking users.
- The spyware was first observed in March 2022 and remains active with new samples still publicly hosted. It uses a two-stage C2 infrastructure that retrieves initial configurations from a Firebase cloud database.
- KoSpy can collect extensive data, such as SMS messages, call logs, location, files, audio, and screenshots via dynamically loaded plugins.
- The spyware has Korean language support with samples distributed across Google Play and third-party app stores such as Apkpure.
- There is evidence of infrastructure being shared with APT43, which is another notorious North Korean state-sponsored group also known as Kimsuky.

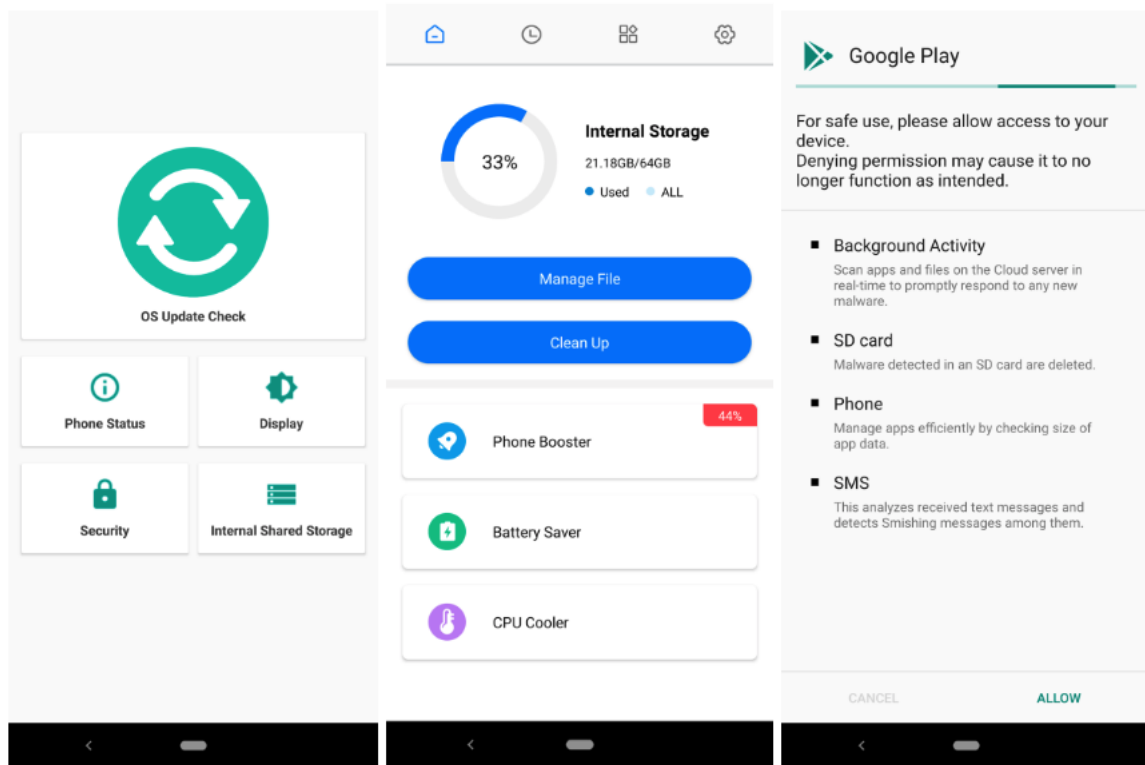
Lookout Threat Lab researchers have discovered a novel Android surveillance tool, dubbed KoSpy, which appears to target Korean and English-speaking users. The spyware, attributed with medium confidence to the North Korean APT group ScarCruft (also known as APT37), is a relatively new family with early samples going back to March 2022. The most recent samples were acquired in March 2024.

KoSpy has been observed using fake utility application lures, such as "File Manager", "Software Update Utility" and "Kakao Security," to infect devices. The spyware leveraged the Google Play Store and Firebase Firestore to distribute the app and receive configuration data. All the apps mentioned in the report have been removed from Google Play, and the associated Firebase projects have been deactivated by Google.

ScarCruft is a North Korean state-sponsored cyber espionage group active since 2012. While primarily targeting South Korea, it has also conducted operations in countries including Japan, Vietnam, Russia, Nepal, China, India, Romania, Kuwait, and several Middle Eastern nations.

KoSpy

KoSpy samples in Lookout's corpus masquerade as five different apps: 휴대폰 관리자 (Phone Manager), File Manager, 스마트 관리자 (Smart Manager), 카카오 보안 (Kakao Security) and Software Update Utility. The samples with utility application lures have basic interfaces which open up the related internal phone settings view. For instance, the Software Update Utility opens up the Software Update screen under the System settings. The File Manager app functions as a simple file browser with some additional features. Kakao Security app on the other hand, doesn't have any useful functionality and displays a fake system window and requests multiple permissions.



Most KoSpy samples offer some basic functionality except the Kakao Security app which gets stuck at a fake permission request screen.

Behind the basic interface, KoSpy starts the spyware functionality by first getting a simple configuration from Firebase Firestore. This encrypted configuration contains two parameters: an “on”/“off” switch and the Command and Control (C2) server address. This two-staged C2 management approach provides the threat actor with flexibility and resiliency. They can enable or disable the spyware and change C2 addresses at any time in the case of a C2 being detected or blocked.

After retrieving the C2 address, KoSpy ensures the device is not an emulator and that the current date is past the hardcoded activation date. This activation date check ensures that the spyware does not reveal its malicious intent prematurely.

C2 Communication and Infrastructure

KoSpy sends two different types of requests to the C2 address. One downloads plugins while the other retrieves configurations for the surveillance functions. The plugin request is supposed to receive an encrypted, compressed binary; however, this could not be confirmed since no C2 was active during the analysis. The configuration request is set to receive a JSON document which configures the following settings: C2 ping frequency, messages to show the user in Korean and English, URL to download a plugin and the class name to dynamically load.

| Request | Response |
|---|---|
| <pre> 1 POST /index.php HTTP/1.1 2 Content-Type: application/json 3 Accept-Encoding: gzip, deflate, br 4 User-Agent: Dalvik/2.1.0 (Linux; U; Android [redacted]) 5 Host: joinupvts.org 6 Connection: close 7 Content-Length: [redacted] 8 9 { "vtr": "[redacted]", "type": "[redacted]", "pref": "[redacted]" }</pre> | <pre> 1 HTTP/1.0 404 Not Found 2 Date: [redacted] 3 Server: Apache/2.4.41 (Ubuntu) 4 Content-Length: 0 5 Connection: close 6 Content-Type: text/html; charset=UTF-8 7 8</pre> |

Some KoSpy C2 domains are still online however they don't respond to client requests.

An example of a “conf” request can be seen in the image above. The request is an HTTP POST request and the payload is in JSON format. Values in the JSON are encrypted and Base64 encoded while the field names are clear text. The “vtr” field contains the unique victim ID generated from the hardware fingerprint and Android ID. The “type” field can be one of “conf” or “code” which determines the type of C2 request. The “pref” field is a composite field and contains information such as package name, app version, device language, hardware details and a list of enabled permissions.

KoSpy can collect an extensive amount of sensitive information on the victim devices with the help of the dynamically loaded plugins. These capabilities include:

- Collecting SMS messages
- Collecting call logs
- Retrieving device location
- Accessing files and folders on the local storage
- Recording audio and taking photos with the cameras
- Capturing screenshots or recording the screen while in use
- Recording key strokes by abusing accessibility services
- Collecting wifi network details
- Compiling a list of installed applications

The collected data is sent to the C2 servers after getting encrypted with a hardcoded AES key. Lookout researchers observed five different Firebase projects and five different C2 servers during the analysis of the available KoSpy samples which can be seen in the indicators of compromise section.

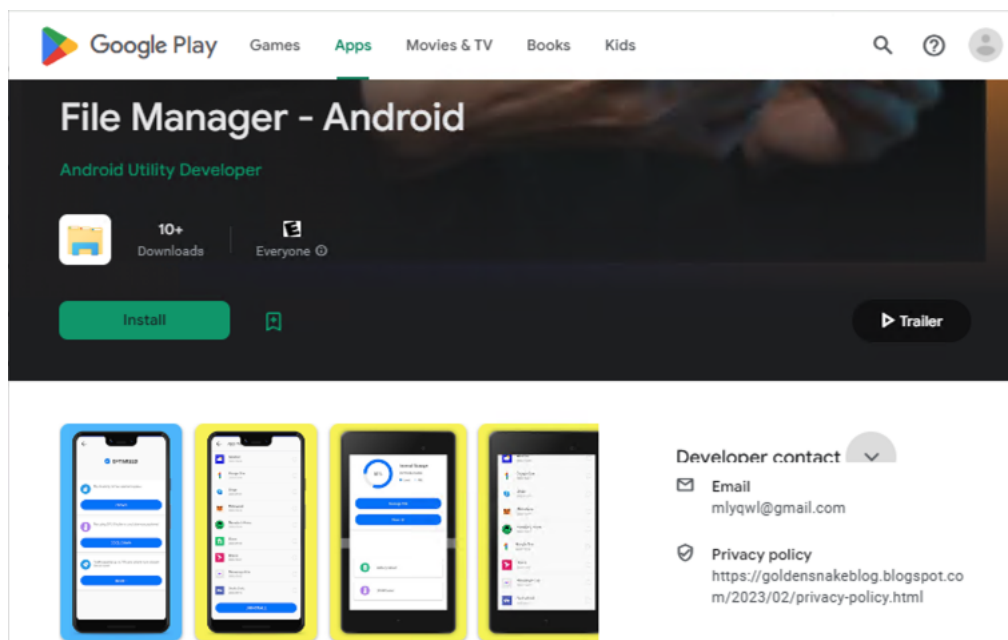
Targeting and Distribution

Lookout researchers assess that this KoSpy campaign was targeted at Korean and English speaking users. More than half of the apps have Korean language titles and the UI supports two languages: English and Korean. The messages and text fields in the app are shown in Korean if the device language is set to Korean and in English otherwise.

```
enc_constant.install = "install";
enc_constant.activity = "activity";
enc_constant.arr_Google_Play = new String[]{"Google Play", "Google Play"};
enc_constant.arr_Google_Protect = new String[]{"Google Protect", "Google 프로텍트"};
enc_constant.arr_checking_update_msg = new String[]{"Checking for updates. Please Wait."};
enc_constant.arr_device_missing_security_msg = new String[]{"Your device is missing impor"};
enc_constant.arr_do_you_want_to_update_msg = new String[]{"Do you want to update %s?\nTh"};
enc_constant.arr_device_missing_updates_msg = new String[]{"Your device is missing impor"};
enc_constant.arr_permission_asking_msg = new String[]{"For updates in your country, you i"};
enc_constant.arr_update = new String[]{"Update", "업데이트"};
enc_constant.arr_install = new String[]{"INSTALL", "설치"};
enc_constant.arr_UPDATE = new String[]{"UPDATE", "업데이트"};
enc_constant.arr_Allow = new String[]{"Allow", "허용"};
enc_constant.arr_OK = new String[]{"OK", "확인"};
enc_constant.arr_NEXT = new String[]{"NEXT", "설정"};
enc_constant.arr_CANCEL = new String[]{"CANCEL", "취소"};
```

KoSpy has language support for Korean language,

Some of the samples of KoSpy were available for download from the Google Play Store alongside the third party app store Apkpure. However, no app is currently publicly available on Google Play Store. A cached snapshot of the Play Store listing page¹ for the File Manager app (com.file.exploer) shows that the app was publicly available for a while and was downloaded more than ten times. The snapshot also reveals that the developer account was named “Android Utility Developer” and the developer contact email address was mlyqwl@gmail[.]com. The related privacy policy page was set to [https://goldensnakeblog.blogspot\[.\]com/2023/02/privacy-policy.html](https://goldensnakeblog.blogspot[.]com/2023/02/privacy-policy.html). The listing also contained an embedded Youtube video to promote the app. The video was uploaded to the @filemanager-android channel² and the channel also contained a Youtube Shorts video.




Attribution

Lookout researchers observed that this KoSpy activity has connections to previous malicious activities attributed to two North Korean threat groups: APT43 and APT37. One of the C2 domains of KoSpy, st0746[.]net, resolves³ to the IP address 27.255.79[.]225 located in South Korea. This IP address was associated with many potentially malicious Korea-related domain names in the past:

27.255.79.225 (27.255.79.0/24)

AS 45382 (EHOSTICT)

KR



Passive DNS Replication (18)

| Date resolved | Detections | Resolver | Domain |
|---------------|------------|------------|---------------------------------|
| 2022-03-28 | 10 / 91 | VirusTotal | ftp.account-google.info |
| 2022-03-27 | 0 / 91 | VirusTotal | naverfiles.com |
| 2022-03-24 | 0 / 91 | VirusTotal | account-google.info |
| 2022-03-23 | 1 / 91 | VirusTotal | upbit-kr.com |
| 2022-03-21 | 0 / 91 | VirusTotal | siren24.info |
| 2022-02-26 | 0 / 91 | VirusTotal | st0746.net |
| 2021-08-20 | 0 / 91 | VirusTotal | kr01.allvpn.kr |
| 2021-03-09 | 0 / 91 | VirusTotal | kr06.allvpn.kr |
| 2020-07-13 | 0 / 91 | VirusTotal | l49588d9.justinstalledpanel.com |
| 2020-03-24 | 0 / 91 | VirusTotal | maeilbox.com |
| 2020-03-24 | 0 / 91 | VirusTotal | ladeec69.justinstalledpanel.com |
| 2019-09-12 | 0 / 91 | VirusTotal | daum.net.in |

KoSpy C2 domains are tied to suspicious domains by shared infrastructure.

The domain names naverfiles[.]com and mailcorp[.]center have been reported⁴ to be involved in attacks targeting Korean users using the Konni desktop malware. Konni⁵ is a Windows RAT family linked to the APT37⁶ threat actor.

Another domain tied to the same IP address, nidlogon[.]com, was reported⁷ to be part of the command and control infrastructure of Thallium (a.k.a. Kimsuky, APT43) by Microsoft.

In addition to its ties to APT37, this KoSpy campaign also has ties to infrastructure used by APT43 - another North Korean hacking group. North Korean threat actors are known to have overlapping infrastructure, targeting and TTPs which makes attribution to a specific actor more difficult. Based on the aforementioned shared infrastructure, common targeting and connection recency, Lookout researchers attribute this KoSpy activity to APT37 with medium confidence.

Indicators of Compromise

Files

911d9f05e1c57a745cb0c669f3e1b67ac4a08601
cd62a9ab320b4f6be49be11c9b1d2d5519cc4860
2d1537e92878a3a14b5b3f55b32c91b099513ae0
f08f036a0c79a53f6b0c9ad84fb6eac1ac79c168
df39ab90c89aa77a92295721688b18e7f1fdb38d
ea6d12e4a465a7a44cbad12659ade8a4999d64d1
1cc97e490b5f8a582b6b03bdba58cb5f1a389e78
1a167b65be75fd0651bbda072c856628973a3c1e
985fd1f74eb617b1fea17095f9e991dcaceec170
744e5181e76c68b8b23a19b939942de9e1db1daa
062a869caac496d0182decfad57a23057caa4ab
b84604cad2f3a80fb50415aa069cce7af381e249
3278324744e14ddf4f4312d375f82b31026f51b5
5639fa1fa389ed32f8a8d1ebada8bbbe03ac5171

C2 Domains

joinupvts[.]org
resolveissue[.]org
crowdon[.]info
st0746[.]net

Firebase Projects

mydb-a1554
project-27ef0
project-75f80
smart-743cf
version-25b53

Citations

¹ <https://play.google.com/store/apps/details?id=com.file.exploer>

² <https://www.youtube.com/@filemanager-android>

³ <https://www.virustotal.com/gui/ip-address/27.255.79.225/relations>

⁴ <https://www.kisia.or.kr/bucket/uploads/2022/12/09/%EC%82%AC%EC%9D%B4%EB%B2%84%EB%B3%B4%EC%95%88%20%EB%8C%80%E>

⁵ <https://malpedia.caad.fkie.fraunhofer.de/details/win.konni>

⁶ <https://malpedia.caad.fkie.fraunhofer.de/actor/apt37>

⁷ <https://noticeofpleadings.com/thallium/files/Ghaffari%20Declaration%20in%20Support%20of%20Motion%20for%20TRO%20and%20Preliminary%20Injunction>

Authors



Alemdar Islamoglu

Staff Security Intelligence Researcher

Alemdar Islamoglu is a security intelligence engineer at Lookout who focuses on mobile threats and related threat actors. He has prior experience in reverse engineering, pentesting, and security software development. He also enjoys organizing and participating in capture the flag competitions when he can find the time.

Entry Type

In-Depth Analysis

Platform(s) Affected

Android

Threat Type

Spyware

Platform(s) Affected

In-Depth Analysis

Android

Spyware