Reaper Group's Updated Mobile Arsenal

By Ruchna Nigam

Published: 2018-04-05 · Archived: 2026-04-06 00:27:40 UTC

Summary
A recent post from EST Security revealed the use of Android spyware in spear phishing email attachments linked to the North Korean Reaper group (also known as APT37, Scarcruft, Group 123 or Red Eyes), highlighting a new mobile vector added to the threat group's toolkit.
Unit 42 has looked further into EST's findings and found a more advanced variant of the Trojan mentioned in their original article. Talos has written on this variant and named it KevDroid.
This post provides our analysis of KevDroid., as well as details on the discovery of previously unknown trojanized versions of a Bitcoin Ticker Widget and a PyeongChang Winter Games application, that are downloaders for the spyware variants.

Background

The post by EST Security detailed an Android spyware disguising itself as an Anti-Virus app from Naver (the largest search and web portal service provider in South Korea). While hunting for similar samples, I came across two more versions of the same variant. One of those called home to cgalim[.]com, a domain that Palo Alto Networks had already observed being used by the Reaper group in non-mobile attacks (IOCs in Appendix).

Table 1: Additional samples found for the original Android spyware variant linked to the Reaper group

Pivoting on artefacts from the original variant led to the discovery of a more advanced variant of the same spyware, which is described in detail further below. In addition, I also stumbled upon two Android applications that serve as downloaders for each of the two variants. They are discussed next.

Downloaders

While investigating the Reaper group's Android spyware variants, I found two applications that have the ability to download and install an application from hxxp://cgalim.com/admin/hr/1[.]apk. I also observed the same URL serving the advanced variant of the Android spyware, confirming that these two applications served as downloaders for the Reaper group's Android spyware. The two applications are trojanized versions of popular applications available on the Google Play Store. The two trojanized versions were not posted on Google Play.
While both downloaders contacted the same URL to download their payloads, looking further into their code I found that they were each written to respectively download and drop one specific variant of Reaper's Android spyware.

App Name	Icon	SHA256	DROPPED PAYLOAD
PyeongChang Winter Games		28c69801929f0472cef346880a295cdf4956023cd3d72a1b6e72238f5b033aca	New variant

Bitcoin Ticker Widget		679d6ad1dd6d1078300e24cf5dbd17efea1141b0a619ff08b6cc8ff94cfbb27e	Original variant

Table 2: Android downloaders used to drop spyware variants linked to the Reaper group

Both applications are signed with the same certificate thereby confirming their origins from the same author(s)

1	Owner: CN=Jhon Phalccon, OU=Google Chrome, O=Google Chrome, L=Washington, ST=US, C=US
2	Issuer: CN=Jhon Phalccon, OU=Google Chrome, O=Google Chrome, L=Washington, ST=US, C=US
3	Serial number: 7b320fab
4	Valid from: Wed Jan 24 10:22:50 GMT 2018 until: Sun Jun 11 10:22:50 GMT 2045

Once these downloaders are installed, they display a message prompting the user to update the application. If the user follows the prompts, the downloader retrieves the payload and saves it to the external device memory as *AppName.apk*. The payload is then loaded prompting the user again to confirm its installation before it is finally installed on the device. The next section provides an analysis of the newer, more advanced variant of these payloads.

Advanced Variant Analysis

The following sample was used for this analysis

App Name	Icon	SHA256
PU	(Blank)	990d278761f87274a427b348f09475f5da4f924aa80023bf8d2320d981fb3209

Table 3: New Android spyware variant discovered, linked to the Reaper group

This sample has the following abilities:

- Record video (default duration is 10 mins)
- Record audio (default duration is 5 mins, saved as *48_d[TS].amr*)
- Capture screenshots (saved as *96_d[TS].jpg*)
- Grab the phone's file listing (saved as *128_d[TS].txt*)
- Fetch specific files
- Download a list of commands
- Get device info - 64-bit Android ID, Phone number, System Properties etc (saved as *208_d[TS].json*)
- Rooting the device, using a binary called *'poc'* in the package assets

Additionally, this advanced variant is capable of exfiltrating:

- Voice recordings from incoming and outgoing calls (saved as *_p[Ph]_in_[D].amr* or *_p[Ph]_out_[D].amr*)

- Call logs (saved as *16_d[TS].json)*
- SMS history (saved as *32_d[TS].json)*
- Contact lists (saved as *144_d[TS].json)*
- Information on registered accounts on the phone (saved as *160_d[TS].json),*

In each of these cases, *[TS]* is the current timestamp in the format yyyyMMddkkmmss, *[Ph]* is the source or destination phone number for a call, and *[D]* is the call duration.
While these exfiltration capabilities are shared in common with the original variant, this new variant writes its own call recording library as opposed to using the open source library that was used by its predecessor.
All exfiltrated information is written to the directory /sdcard/_pu on the phone and sent to hxxp://hakproperty.com/new/plat/pu[.]php?do=upload.
Before transmission, the files are AES-encrypted using the key "08D03B0B6BE7FBCD". This encryption scheme and key is consistent across the two variants.
Post-encryption the files are renamed with the addition of a suffix *'x'*. All created files are deleted after they are sent to the upload server.
When commanded to fetch a list of commands, the list is fetched from

1	hxxp://hakproperty.com/new/plat/pu[.]php?do=download_rc&aid=" + [64-bit android_id]

Conclusion
The emergence of a new attack vector, followed by the appearance of new variants disguising themselves as currently relevant applications like the Winter Olympics, indicates expanding operations of the Reaper group that are actively in development.
Palo Alto Networks customers benefit from the following protections against these attacks:

1. AutoFocus customers can track the group's activity using the Reaper tag.
2. WildFire detects all related samples with malicious verdicts.
3. Traps blocks all malicious files associated with this group.

IOCs

Reaper Downloader APK samples
28c69801929f0472cef346880a295cdf4956023cd3d72a1b6e72238f5b033aca
679d6ad1dd6d1078300e24cf5dbd17efea1141b0a619ff08b6cc8ff94cfbb27e
Advanced Variant sample
990d278761f87274a427b348f09475f5da4f924aa80023bf8d2320d981fb3209
Non-APK Reaper-related samples making use of cgalim[.]com
0de087ffb95c88a65e83bd99631d73d0176220e8b740785de78d2d79294f2303

6b1f2dfe805fa0e27139c5a4840042599262dbbf4511a118d3fba3d4ec35f2d7
86887ce368d9a3e7fdf9aa62418cd68daeea62269d17afb059ab64201047e378
d29895aa3f515ec9e345b05882ee02033f75745b15348030803f82372e83277a
d5de09cc5d395919d2d2000f79326a6997f4ec079879b11b05c4d1a1a847ed00
