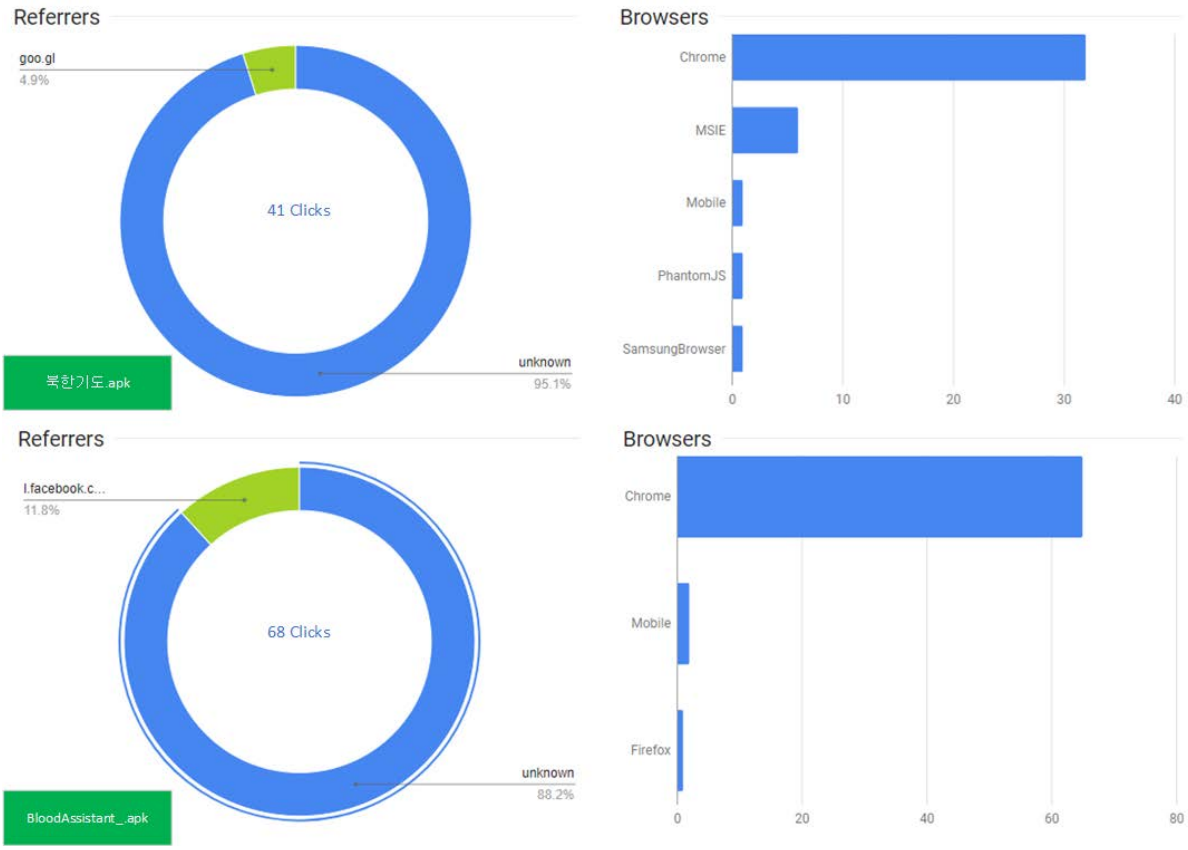
EMBARGOED UNTIL THURSDAY, JANUARY 11, 5:00 AM ET

North Korean Defectors and Journalists Targeted Using Social Networks and KakaoTalk

By Jaewon Min, McAfee Mobile Research Team

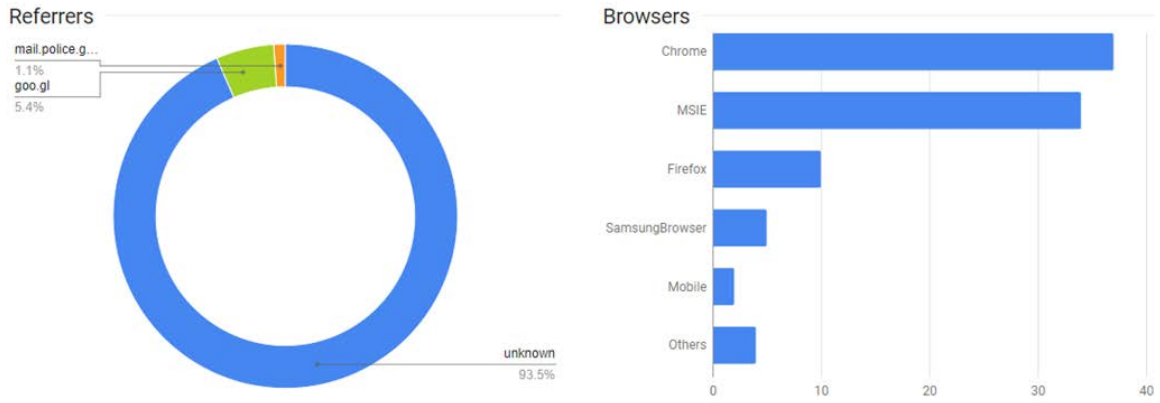
Recently, South Korean media wrote about North Korean refugees and journalists being targeted by unknown actors using KakaoTalk (a popular chat app in South Korea) and other social network services (such as Facebook) to send links to install malware on victims' devices. This method shows that attackers are always looking for different ways to deliver malware.

The McAfee Mobile Research Team has acquired malicious APK files that were used in the targeted attacks. According to the articles, Google-shortened URLs were used to spread malware. We analyzed those statistics.



There are two versions of the dropper malware: "북한기도" (Pray for North Korea) and "BloodAssistant" (a health care app). In both cases, most clicks originated in South Korea and the most common browser and operating system combination was Chrome and Windows. (Android was the second most common.) The referrers diagram of BloodAssistant shows Facebook was used in 12% of cases to send the link to its targets.

In the case of the journalist who was targeted, the attacker sent a shortened link showing a thumbnail of another story written by the journalist, according to the news article. The link directs to ihoodtec[.]com/upload/newslist[.]php (now offline), which seems to be used for redirecting to links in other domains. This shortened URL was clicked by someone with an account at mail[.]police[.]go[.]kr, suggesting the shortened URL was also sent via email to the police address.



The number of clicks might not be meaningful because it can include access from malware researchers, but what is meaningful is that malware-download links were spread using different platforms: Facebook, KakaoTalk, email, etc.

Analysis

Dropper

All the malicious APK files (including additional variants) dropped the Trojan on the victim's device. Although the apps look different, the dropper mechanism is identical. The following screens show the execution of the dropper files.

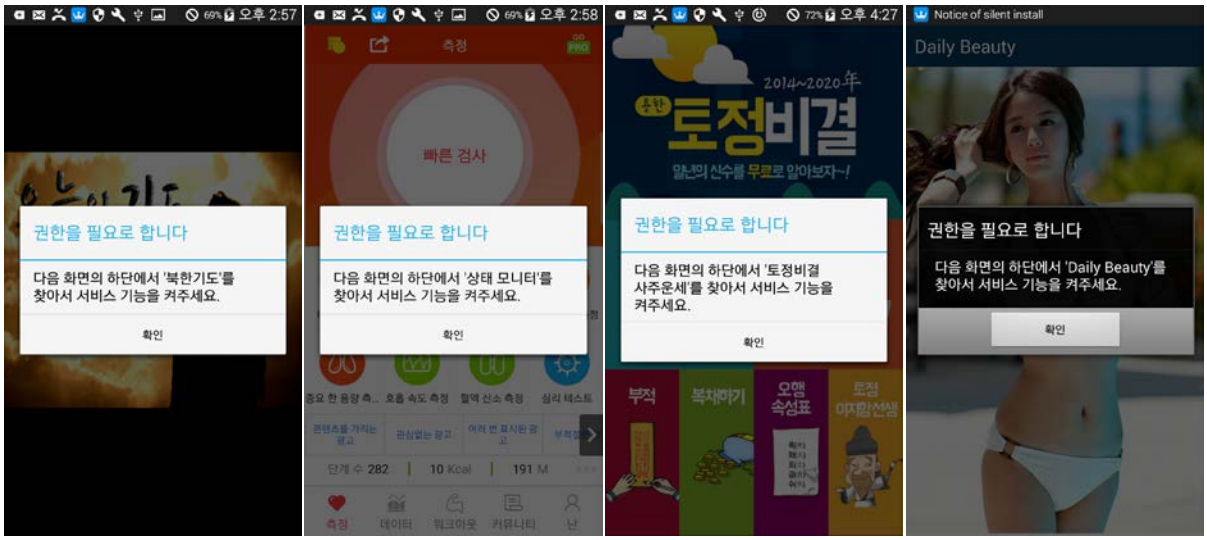


Figure 1: Screenshots of droppers.

When the dropper APK executes, it first checks whether the device is already infected. If not infected, it phishes the victim to turn on the accessibility permission. If the victim clicks the pop-up window, the view changes to the accessibility settings menu so the app can acquire the permission.

When the accessibility service starts, it overlays the window (by playing a video, for example) to hide the process of turning on required settings and dropping and installing the Trojan. The overlay is removed after the Trojan is installed. The following diagram explains the flow after executing the dropper malware.

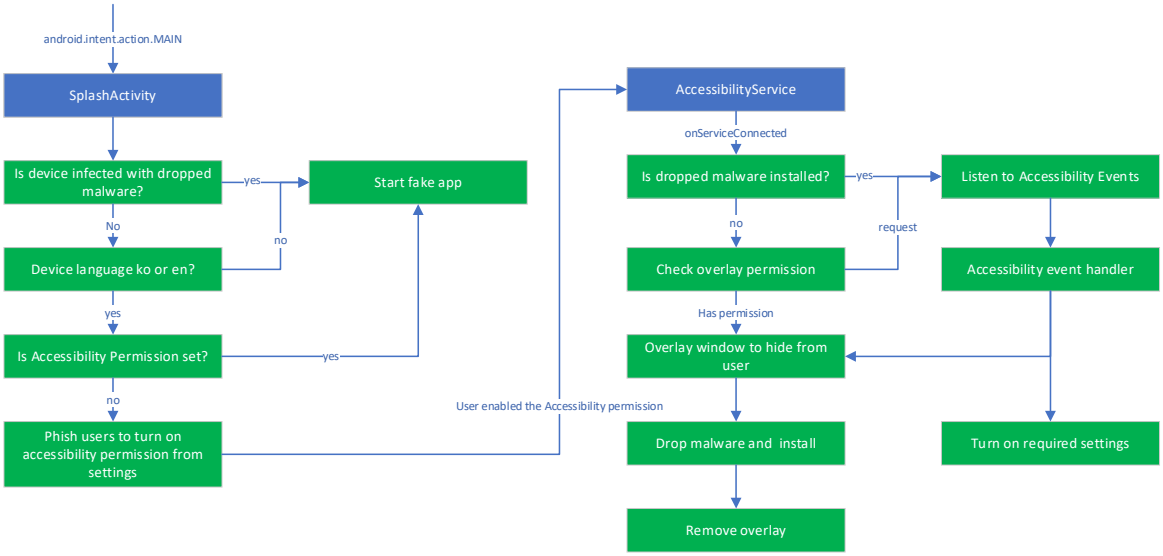


Figure 2: Execution flow of the dropper.

Trojan

The dropped Trojan uses popular cloud services Dropbox and Yandex as a control server to upload data and receive commands. The following diagram explains the execution flow of the Trojan. The names of broadcast receivers and services (with some misspellings) may vary between samples but the execution is the same.

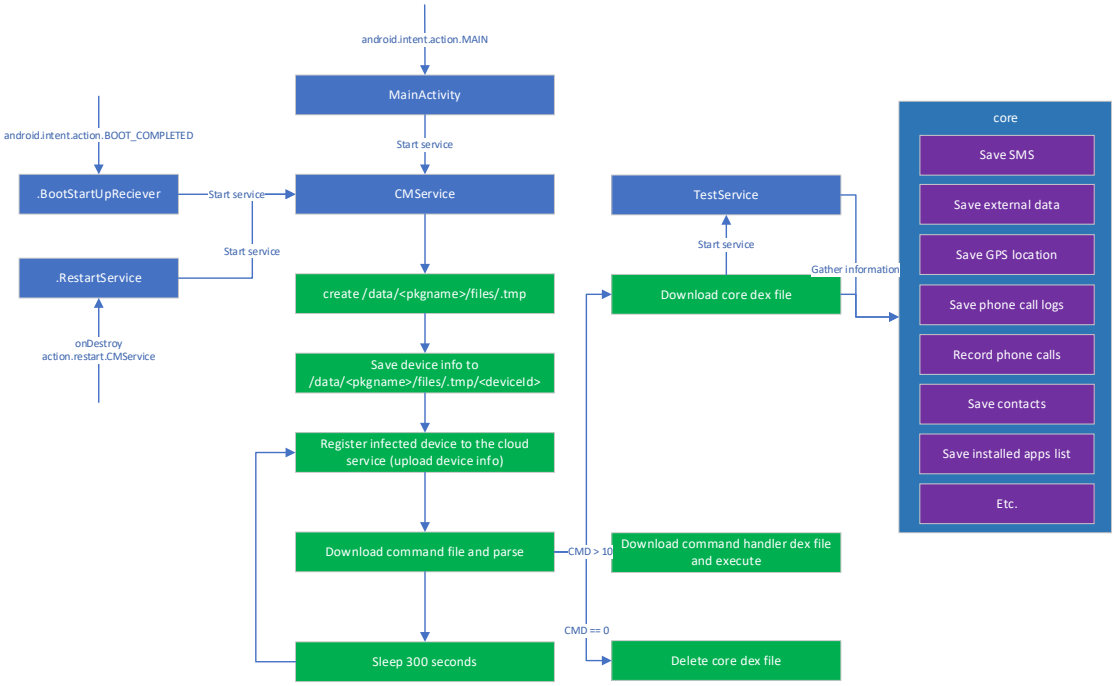


Figure 3: Execution flow of the Trojan.

When the dropped Trojan is installed, it saves device information in a temporary folder and uploads it to the cloud. It then downloads a file containing commands and other data to control the infected device. (We'll explain the format of the downloaded file in the next section.) Most of the malicious behaviors—such as saving SMS, contact information, etc.—are implemented inside a separate dex file "core," which is downloaded from the control server. This dex file is referenced in many places in the malware. The malicious functionality can be extended, as we'll explain in the following section.

Command file structure

The command file has its own format. The following diagram explains the types of values. Offset designators are used to retrieve each value when parsing the file. The next table explains each value.

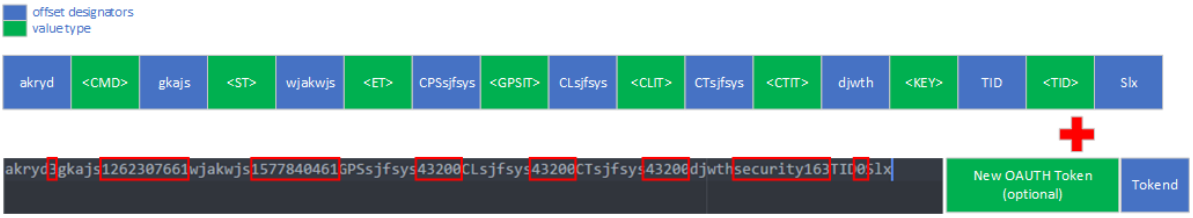


Figure 4: Command file format.

Type	Value
CMD	Command code
ST	Unknown
ET	Unknown
GPSIT	Time interval for sending GPS data
CLIT	Time interval for sending call logs
CTIT	Time interval for sending contacts
KEY	Unknown
TID	Device ID

Figure 5: Command file values.

The handler for command code received from the cloud (CMD value) is implemented as a separate dex file and is downloaded either before or after the malware parses the command file. This mechanism allows the attacker to easily extend its malicious functionality without needing to update the whole malware.

Our analysis shows that only some of the commands are implemented now and uploaded to the cloud control server. Note Command 12 captures KakaoTalk chat logs.

CMD	Behavior
11	Call System.exit(0)
12	Extract KakaoTalk chat logs
100	Set related shared preference key values to 0
101	Set related shared preference key value to download handler for CMD 100
102	Delete /storage/emulated/0/Download/blackstring.apk

Figure 6: Implemented commands.

Variants

We have found variants of the APKs that news articles initially reported on Google Drive. (The APKs on Google Drive are marked as malware and cannot be downloaded.) Some variants use different cloud services as their control servers while others drop the separate call-recording app "com.toh.callrecord" (assets/bbb). The following graph shows the relationships among variants and dropped files.

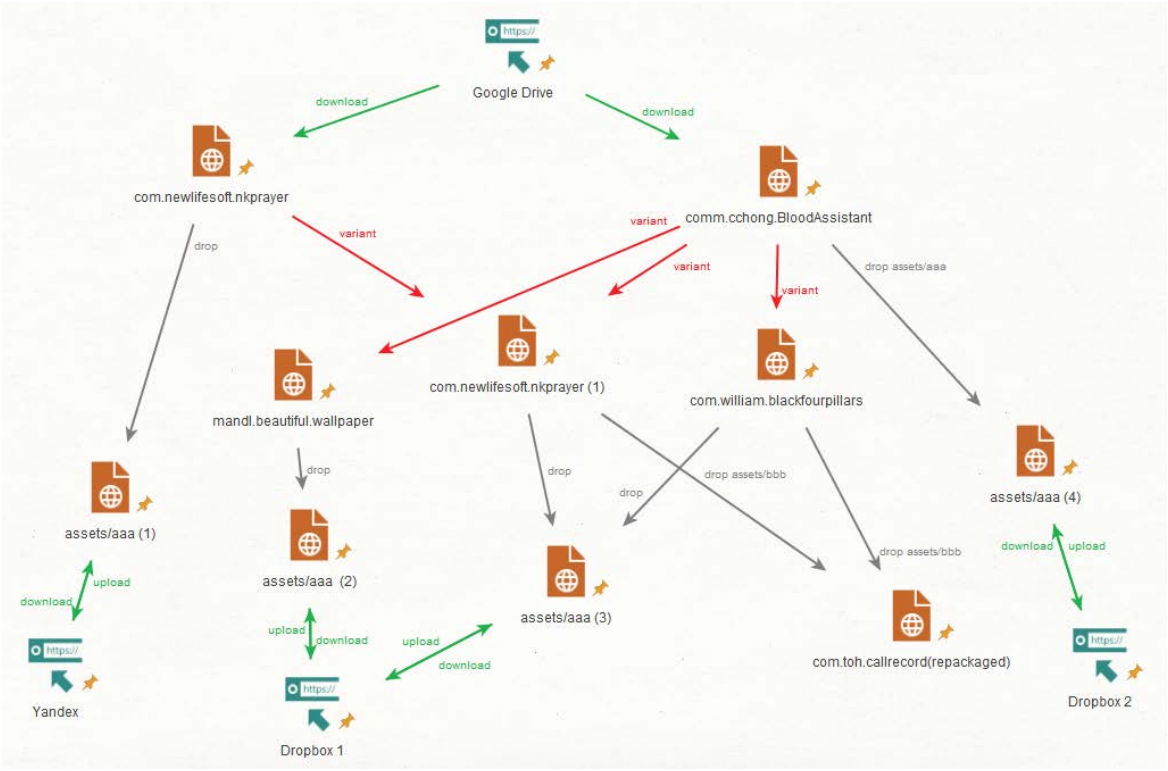


Figure 7: Relationships among variants.

The Actors

Initial malicious APKs we found were uploaded to Google Drive by the same account, and we found a connected social network account. By following activities of this account, we conclude with high confidence that this account was used to send shortened URLs to victims to get them to download malicious APK files.

The group behind this campaign is certainly familiar with South Korean culture, TV shows, drama, and the language because the account names associated with the cloud services are from Korean drama and TV shows, including the following:

Account	Info
yusijin, sijin yu	Korean drama character name
kang moyon	Korean drama character name
junyong ju	Korean competition series participant
jack black	Appeared in Korean reality show

Figure 8: Cloud service accounts.

We found the use of an interesting word, “피형” (“blood type”), which is not used in South Korea but is used in North Korea. (“혈액형” is the word for blood type in South Korea.) We also found a North Korean IP address in test log files of some Android devices that are connected to accounts used to spread the malware. However, Wi-Fi was on so we cannot exclude the possibility that the IP address is private.

By looking at the list of deleted folders in the cloud, we found one with the name “sun Team Folder,” possibly the name of the actors. This group has been active since 2016, according to the cloud storage creation date.


```
{ "entries": [ { ".tag": "deleted", "name": "sun Team Folder", "path_lower":
"/sun team folder", "path_display": "/sun Team Folder" },
```


Figure 9: Deleted folder in the cloud.

Conclusion

This malware campaign is highly targeted, using social network services and KakaoTalk to directly approach targets and implant spyware. We cannot confirm who is behind this campaign, and the possible actor Sun Team is not related to any previously known cybercrime groups. The actors are familiar with South Korea and appear to want to spy on North Korean defectors, and on groups and individuals who help defectors.

McAfee Mobile Security detects this malware as Android/HiddenApp.BP. Always keep your mobile security application updated to the latest version, and never install applications from unverified sources. We recommend installing KakaoTalk only from Google Play. These habits will reduce the risk of infection by malware.