

# ***Dragon Messenger***

## ■ Background of “Dragon Messenger” APT Operation

ESRC (ESTsecurity Security Response Center) has recently discovered the stealthy mobile APT attack carried out by Geumseong121 APT hacking group.

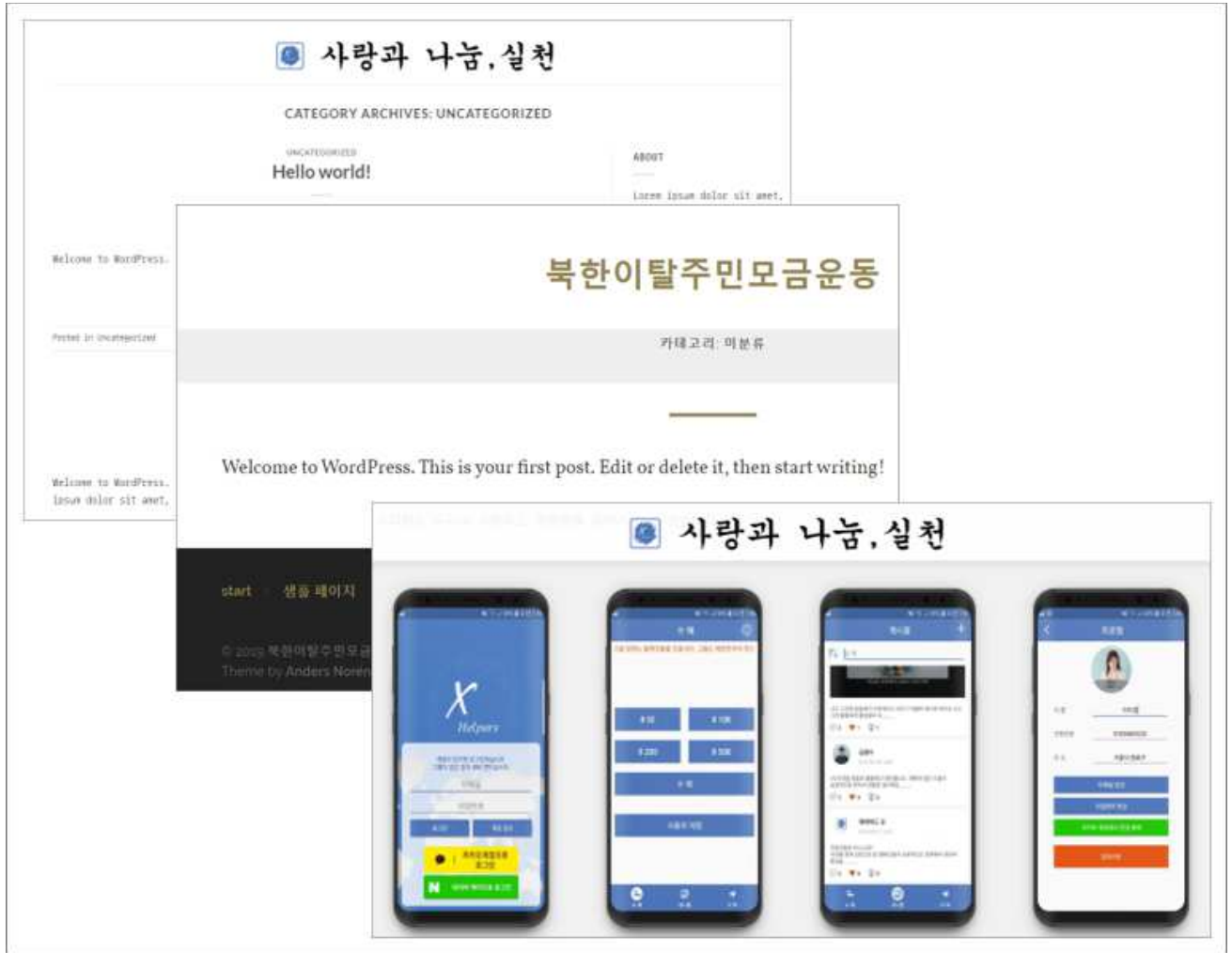
The hacker group also distributed a malicious app (APK) via the site disguised as a fundraising service for supporting North Korean defectors.

The website is built on WordPress platform, and the domain was created on August 23, 2019, and updated on October 22.

The snapshots displayed from September 11 to October on the timeline indicates that it is the charity site supporting North Korean defectors, and the Android app installation link (Google Play) was added in October.

The site disguised as a charity website tricks North Korean defectors and North Korea- related organizations into installing the apps using the promotion strategies in many different forms.

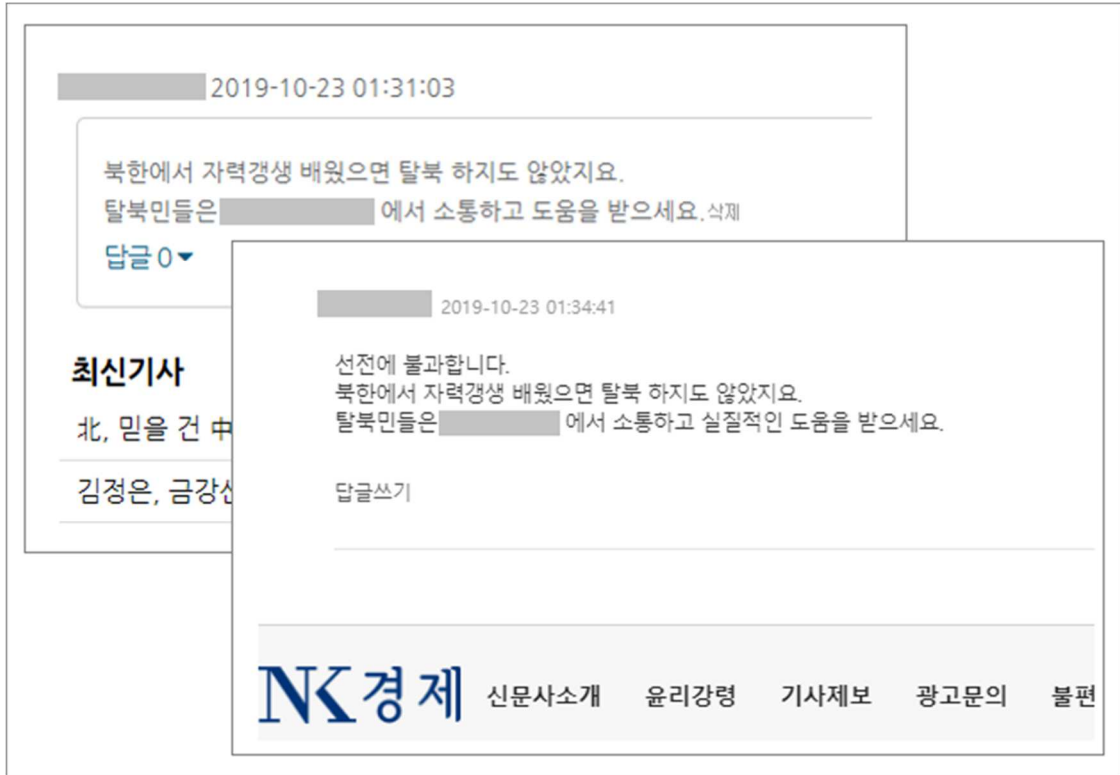
ESRC has named the operation "Dragon Messenger" based on the several interesting factors found in the campaign, such as the malicious application that collects the data via the 'DragonTask' path and the attack performed by disguised as a secure messenger.



[ Figure 1] The sites disguised as fundraising organizations supporting North Korean defectors

Since the above fundraising sites for supporting North Korean defectors were made, they have been spread via various channels (email, SNS) along with guidelines of the related apps, mainly targeting those who work in the North Korea- related field.

Besides, it became known to the public with the promotion using the comments written by the ID 'David Kim' who introduces himself as the administrator of the website that is related to the North Korea- related field.

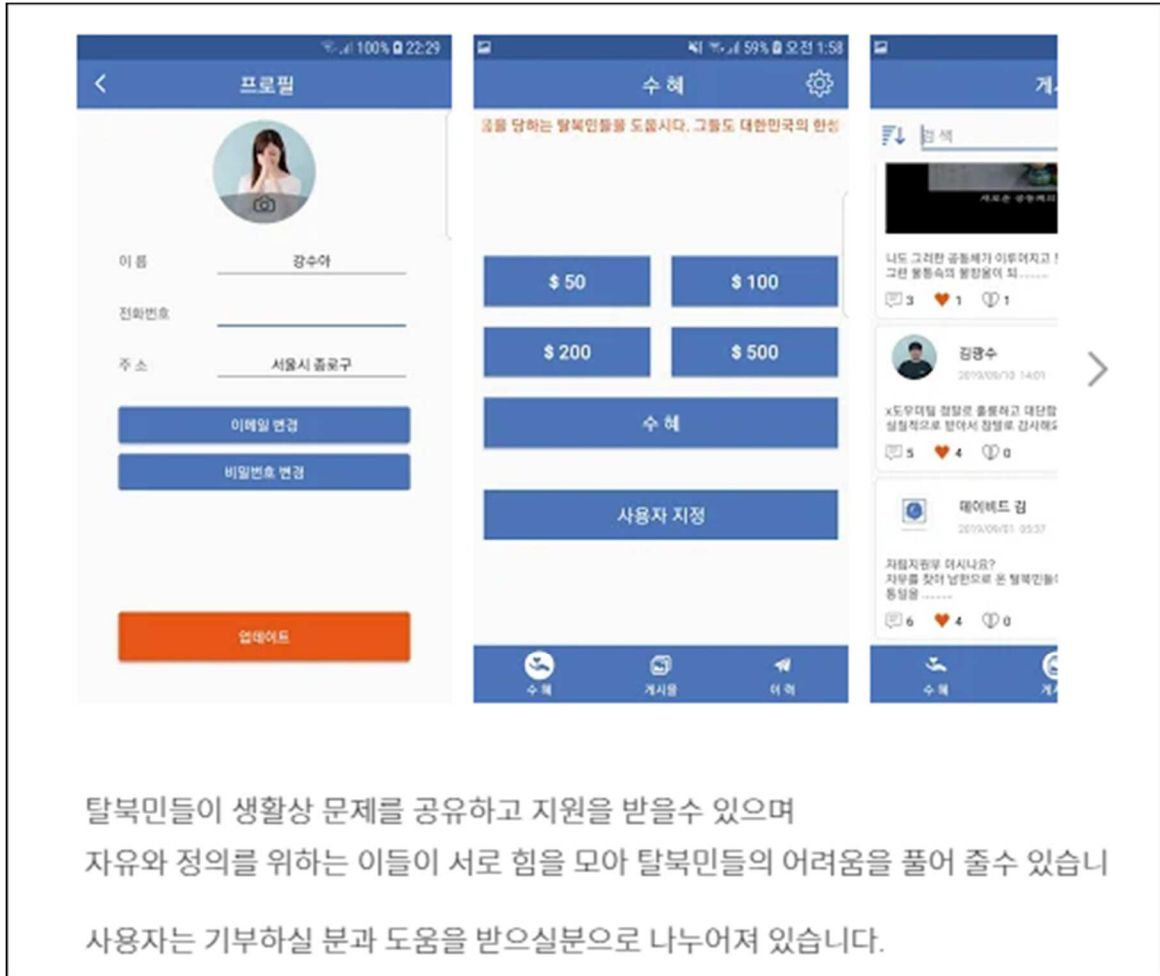


[ Figure 2] Comments posted on media site covering North Korea- related issues

Many words and expressions written in North Korean were found during the website investigation process. It is highly likely that such expressions exist in reality because it is a North Korean defector- related site.

ESRC has conducted a thorough investigation on the YouTube site run by the same administrators as those of the Android apps that were distributed on the site when two apps were registered on the official Google Play Store, all of which have currently been removed by Google.

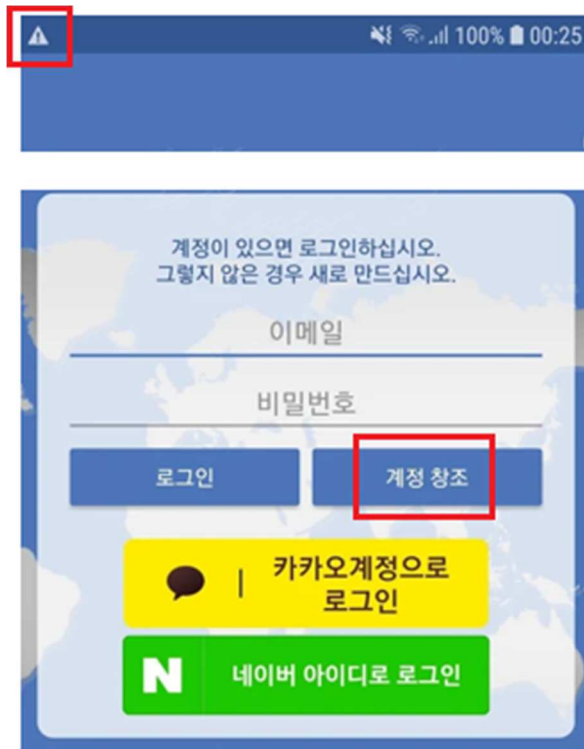
The application informs that North Korean defectors can share their life- related issues, get the support they need, and specify donation services.



[ Figure 3] Application registered on Google Play

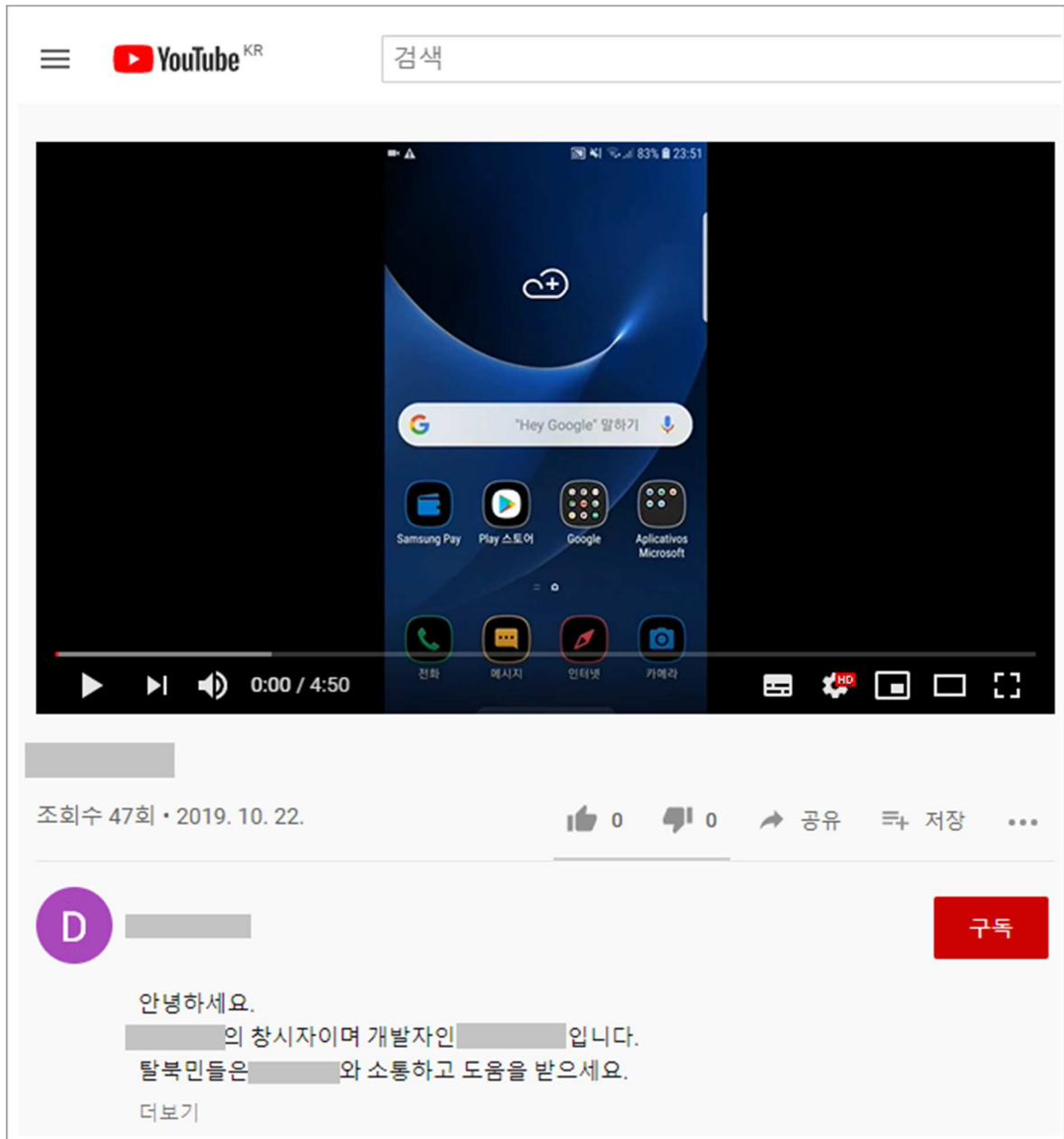
In the application image displayed in the official Google Play Market, there is '계정 창조 (North Korean expression, which means creating an account)' button. For reference, this is usually referred to as "계정 생성 (South Korean expression, which means creating an account)" in South Korea. That is, both '창조' and '생성' mean 'creation' in English.

Also, the only Wi- Fi connection was likely used for performing a screenshot capture, which seems to be because the SIM card was not inserted on the smartphone.



[ Figure 4] Some of the images registered on Google Play

Cosmosfarm- based board for posting social comments had been included on the site until October 23, but the bulletin board was removed around October 28. The deleted board had YouTube links and comments saying that the writers prefer the site.



[ Figure 5] Use of the app registered on YouTube

YouTube videos to show how to use the Korean smartphone provides information on the installation of the application and the guidance on how to use the installed application. The attacker performs malicious activities on Facebook with the same account as YouTube, with about 330 friends registered.

This suggests that attackers have prepared the attack in advance using Facebook, and the registered friends can be exposed to a potential threat.



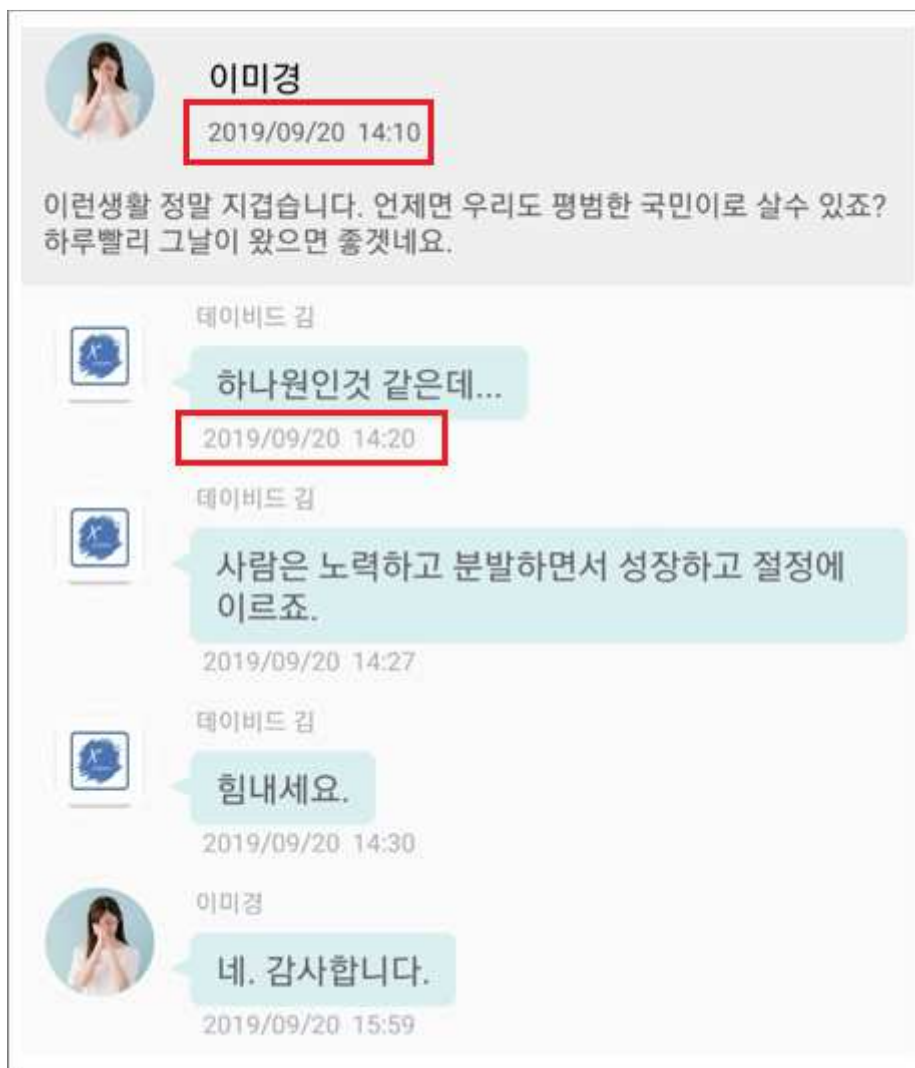
[ Figure 6 ] Registered on Facebook

The YouTube video shows a demo of installing an application on the smartphone. Taking a closer look at scenes from the video reveals that the hacker logged in with the name 'Lee Mi- Kyung' and the account 'borisanatoly' when creating the video.

'Lee Mi- Kyung' is the first person who wrote a post in an app service on September 20, 2019, at 14:10.

The 'David Kim' account, possibly the administrator of the website, posted several comments on September 20 at 14:20. It seems that the attacker posted the comments that appeared as the conversation between two persons using the two different accounts every 10 minutes.

Also, the name 'Lee Mi Kyung' left on the information on the official Google Play app indicates that two accounts were closely related from the beginning and that one person managed both accounts.



[ Figure 7 ] Conversation between the two different accounts in the app service

The APT hacker planned a highly strategic tactic scenario to gather the attack targets by developing the community-based charity app for North Korean defectors.

Gathering North Korean defectors in the specific cyberspace enabled the hackers secretly spy on the defectors' conversation as well as create monetary profit by collecting donations and promoting the site with advertisements.

ESRC believes that such malicious activities of the Geumseong121 hacker group will be the signal 'a new mobile threat' in the future.

■ Smart threat disguised as a charity site for supporting North Korean defectors

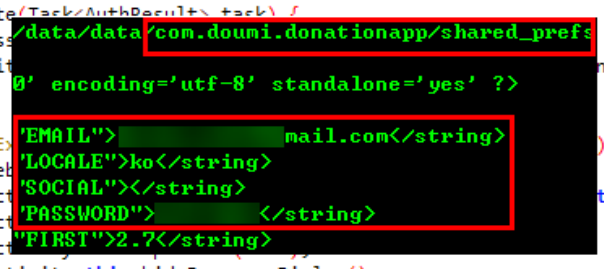


The hacker group behind the attack created and distributed the multiple malicious apps, and disguised them as the messengers mainly used for secret chats.

One of the apps disguised as sponsoring North Korean defectors was officially registered in the official Google Play market. When joining the membership of the site using the email account except for Kakao or Naver, the username and password entered by the user using the 'createUserWithEmailAndPassword' method will be used to create the account 'Firebase' and log in to the site.

In addition, the account information is stored in plain text in the 'config.xml' file in the 'shared\_prefs' path of the app, exposing users to the potential security threats.

```
private void createAccount(String str, String str2) {
    if (!validateForm()) {
        this.preference.putUserEmail(str);
        this.preference.putUserPassword(str2);
        showProgressDialog(R.string.text_creating);
        this mAuth.createUserWithEmailAndPassword(str, str2).addOnCompleteListener((Activity)
        public void onComplete(Task<AuthResult> task) {
            if (task.isSuccessful) {
                SigningActivity.this.startActivityForResult(Intent.makeMainActivity(), 1);
            } else {
                try {
                    throw ((Exception) new Exception("Failed to create account"));
                } catch (Exception e) {
                    SigningActivity.this.startActivityForResult(Intent.makeMainActivity(), 1);
                }
            }
            SigningActivity.this.hideProgressDialog();
        }
    }
}
```



The image shows a code snippet from an Android application. The code defines a method `createAccount` that takes two strings, `str` and `str2`, and attempts to create a user account. It uses `AuthResult` and `AuthResult.Task` objects. A red box highlights the file path `/data/data/com.doumi.donationapp/shared_prefs/config.xml` where the account information is stored. Another red box highlights the XML content of the file, which includes fields for `EMAIL`, `LOCALE`, `SOCIAL`, `PASSWORD`, and `FIRSI`.

[ Figure 8] Login credentials stored in plain text

ESRC focused on collecting the additional threat evidences in addition to the possibility of account disclosure threats upon initial SignUp, regarding the latest version registered on Google Play's official market, and found other similar codes in the analyzing process.

We also found a connection between the recently found campaign and the previous mobile infringement by Geumseong 121 APT hacker group during the analyzing process of the additional codes.

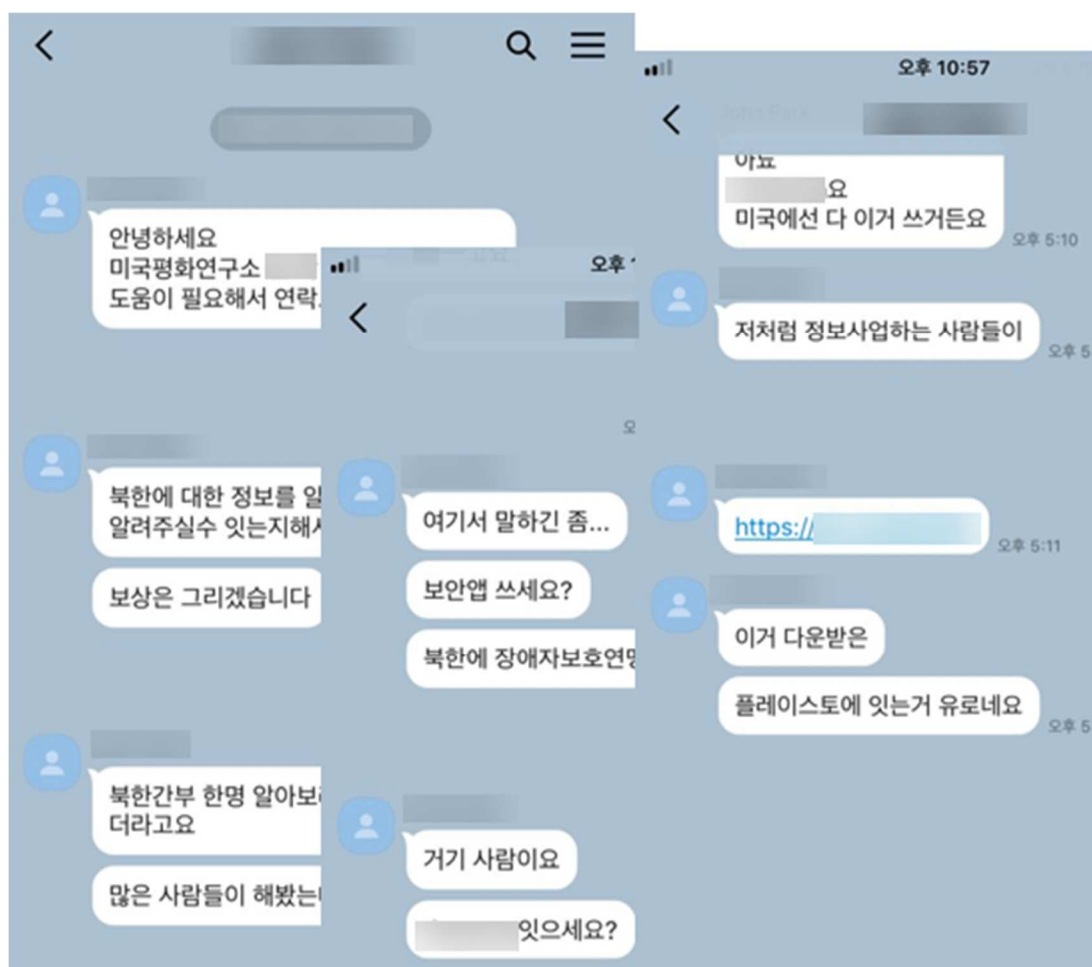
#### ■ Targeted attack using KakaoTalk message

Many malicious apps that attempts an installation have been detected from June 2019 until recently.

The attackers steal the names and profile images of certain people who live in the United States, create their KakaoTalk accounts, and attempt to access to South Koreans who are working in the North Korea- related field.

KakaoTalk users can add friends only with their phone numbers, which could help the attackers to abuse the list of phone numbers to select attack targets.

The attacker attempts to impersonate a vice president and an advisory board of The Korean American Association, or a researcher at the Institute of Peace.



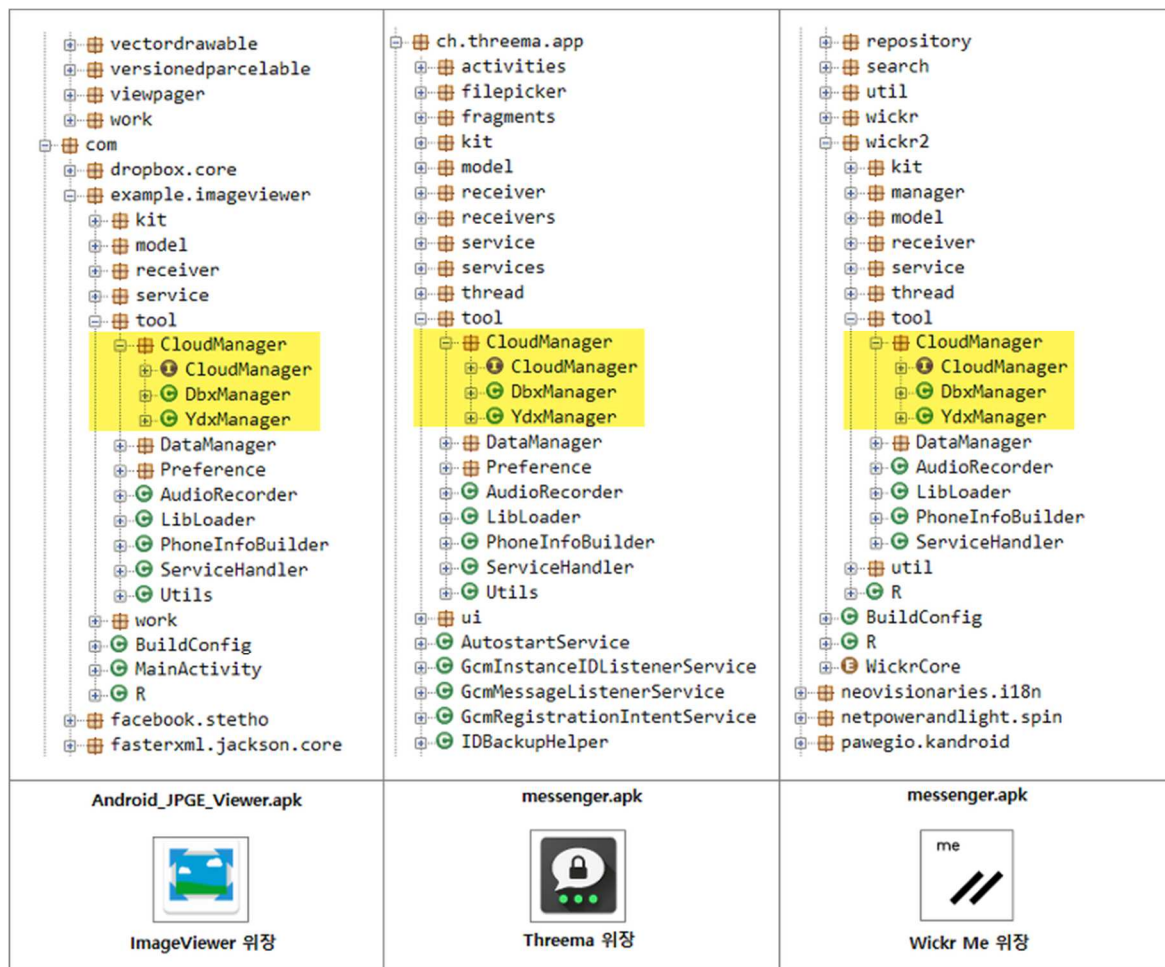
[ Figure 9] Distribution of malicious apps using KakaoTalk Messenger

The attacker pretends to be the researcher at the Institute of Peace in the US in KakaoTalk dialogue, tricks victims into believing that he has been collecting the North Korea- related information, and suggests the conversation with a secure messenger app while encouraging users to click the specific URL link to install a malicious app disguised as messenger app.

The attacker has disguised himself as secured messengers, such as the ‘Threema’ developed in Swiss and ‘Wickr ‘ made in the US.

The malicious apps provide most of the functions that a normal secure messenger has, to avoid users’ suspicion and all of these apps perform similar functions.

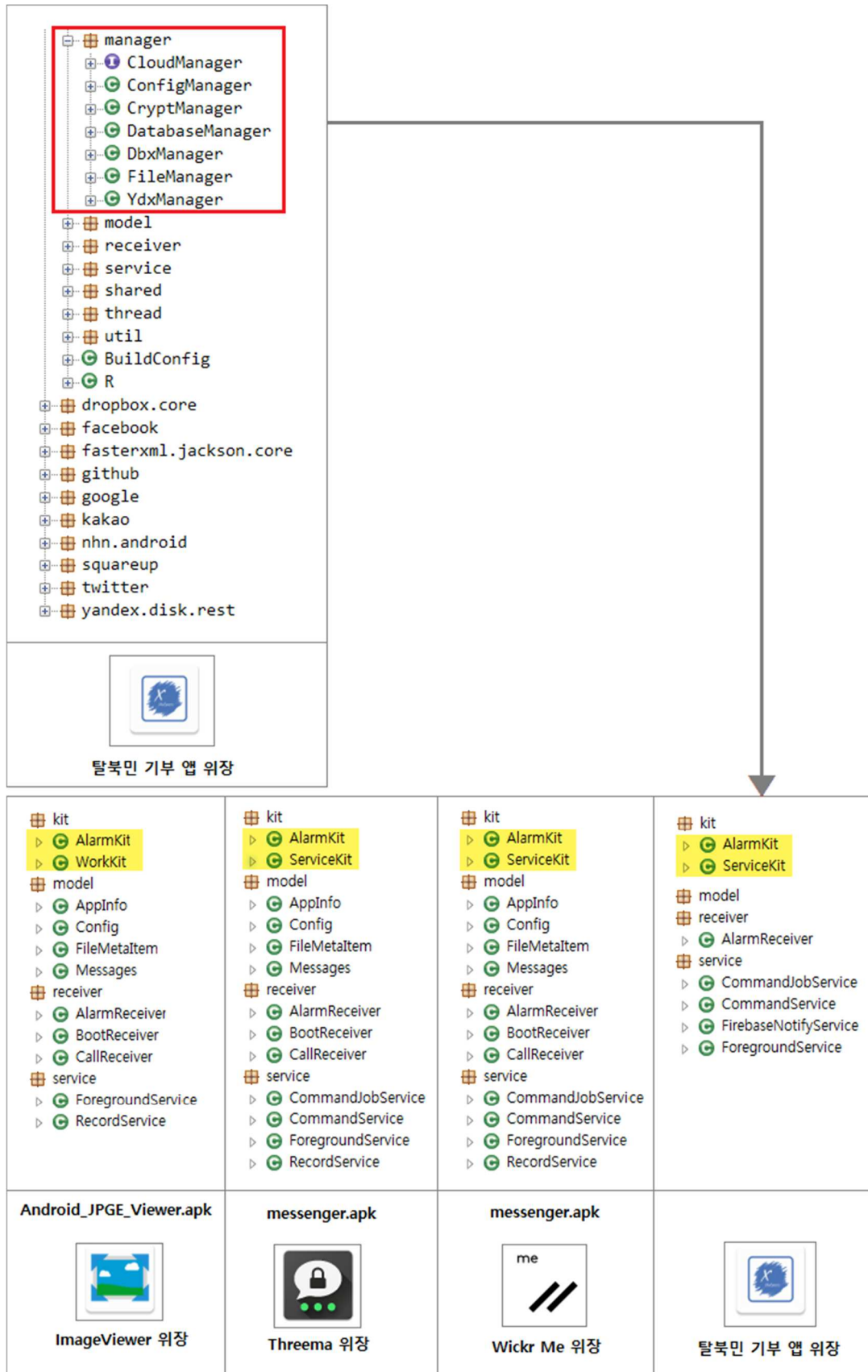
The apps are highly similar to the Android malicious apps found in the ‘Geumsoeng121 APT hacker group performing the attack targeting smartphones using the steganography technique’ released on August 5.



[ Figure 10] Comparison of internal codes by malicious app type

The investigation reveals that the victims of malicious apps disguised as overseas secure messengers were also exposed to the attack disguised as the charity site supporting North Korean defectors.

The same functions were found in an earlier version of a malicious app, but not in the final version found in the official Google Play market.



[ Figure 11] Comparison of the malwares disguised as a secure messenger and the charity site for NK defectors

It seems that the attackers made an effort to avoid the suspicion that the North Korean fundraising apps are originated from the previously discovered malicious apps.

However, the initial version of those malicious apps includes the functionality that attempts to communicate with Dropbox and Yandex.

We also found that some variable declarations used by malicious apps are almost identical to the previously found malicious apps.

 <p>탈북민 기부 앱 위장</p>	<pre> Config.TAG = "NCSCLog"; Config.PERIODIC_WORKER_TAG = "LoadAppPeriodic"; Config.ONETIME_WORKER_TAG = "LoadAppOneTime"; Config.REQUEST_ALARM_CODE = 101; Config.REQUEST_RESTART_CODE = 102; Config.JOB_SERVICE_ID = 333; Config.FOREGROUND_ID = 444; Config.NOTIFICATION_ID = "NCSC_NotificationID"; Config.FOREGROUND_KEY = "LoadAppForeground"; Config.EXTRA_KEY = "CMD_KEY"; Config.P_NUMBER_KEY = "P_NUMBER"; Config.S_DATE_KEY = "S_DATE"; Config.E_DATE_KEY = "E_DATE"; Config.TYPE_KEY = "TYPE"; Config.R_STATE_KEY = "R_STATE"; Config.S_TIME_KEY = "S_TIME"; storeConfig(); </pre>
<p>messenger.apk</p>  <p>Threema 위장</p>	<pre> Config.TAG = "NCSCLog"; Config.PERIODIC_WORKER_TAG = "LoadAppPeriodic"; Config.ONETIME_WORKER_TAG = "LoadAppOneTime"; Config.REQUEST_ALARM_CODE = 101; Config.REQUEST_RESTART_CODE = 102; Config.JOB_SERVICE_ID = 333; Config.FOREGROUND_ID = 444; Config.NOTIFICATION_ID = "NCSC_NotificationID"; Config.FOREGROUND_KEY = "LoadAppForeground"; Config.EXTRA_KEY = "CMD_KEY"; Config.P_NUMBER_KEY = "P_NUMBER"; Config.S_DATE_KEY = "S_DATE"; Config.E_DATE_KEY = "E_DATE"; Config.TYPE_KEY = "TYPE"; Config.R_STATE_KEY = "R_STATE"; Config.S_TIME_KEY = "S_TIME"; storeConfig(); </pre>
<p>messenger.apk</p>  <p>Wickr Me 위장</p>	<pre> Config.TAG = "NCSCLog"; Config.PERIODIC_WORKER_TAG = "LoadAppPeriodic"; Config.ONETIME_WORKER_TAG = "LoadAppOneTime"; Config.REQUEST_ALARM_CODE = 101; Config.REQUEST_RESTART_CODE = 102; Config.JOB_SERVICE_ID = MjolinirRecyclerAdapter.TYPE_ITEM; Config.FOREGROUND_ID = 444; Config.NOTIFICATION_ID = "NCSC_NotificationID"; Config.FOREGROUND_KEY = "LoadAppForeground"; Config.EXTRA_KEY = "CMD_KEY"; Config.P_NUMBER_KEY = "P_NUMBER"; Config.S_DATE_KEY = "S_DATE"; Config.E_DATE_KEY = "E_DATE"; Config.TYPE_KEY = "TYPE"; Config.R_STATE_KEY = "R_STATE"; Config.S_TIME_KEY = "S_TIME"; storeConfig(); </pre>

[ Figure 12] Comparison of Configuration Variables of the apps disguised as a secure messenger and the charity site for NK defectors

In addition, we have gained many artifacts to show that the two malwares have high similarity in the path that the attackers used for performing malicious commands, the data they stolen, and the additionally downloaded data.

## ■ Eavesdropping attacks using Android smartphone

ESRC is paying attention to investigate the threat activities of the state-sponsored APT hacking group 'Geumseong121' targeting Android smartphone users.

The 'zombied' smartphones, which are exploited in cyber operations, has emerged as an important threat that should not be overlooked.

Several attempts to steal SMS and phone address books, eavesdrop on a phone conversation and leak the KakaoTalk messages appearing in the notification window have been discovered until recently.

It is also worth noting that the quite popular celebrities have been exposed to the 'Dragon Messenger' APT attack.

When an Android smartphone is exposed to mobile threat, not only personal privacy, but also the contents of institutional and corporate meetings and photos in the gallery will be leaked in real time.

ESRC has found that many smartphone users in a wide range of fields have been 'zombied' in the tracking and analyzing process of the mobile APT attack. It was quite surprising that most of the victims are unaware of the infection and the infected smartphones have been monitored by attackers for a long period.

## ■ Indicator of Compromise

1594679f51bdebe4701d062f3c8f0dc3  
dfb8e001b3ecfc63200dd4c5c21f53d5  
02d5e68bef32871765b7e6e71f50499d  
c36de50fe488e5015a58a241eb9b2411  
1e32cd693a0dd137959b87ca359b2831



ESRC will provide additional Indicators of Compromise (IoC) of the threat via 'Threat Inside' threat intelligence report.