THE SOUTH KOREAN FAKE BANKING APP SCAM

The Yanbian Gang Sets Sights on South Koreans

Simon Huang
Mobile Threat Research Team
INTRODUCTION

In 2014, we took a close look at the Chinese underground market and found that it continued to thrive. But what we did not see was that even cybercriminals in remote parts of the country—Yanjian—were successfully profiting from the Android™ mobile banking customers in a neighboring country—South Korea.

What we have dubbed the “Yanbian Gang” has successfully been siphoning millions from their victims’ accounts since 2013. The hackers used fake banking and other popular apps to victimize more than 4,000 South Korean Android mobile banking customers throughout 2013 and 2014. They also used effective social engineering lures like “The Interview” to bait victims into installing their fake apps.

This research paper provides in-depth information on the Yanbian Gang’s structure, operations, and prowess.
THE YANBIAN GANG

Where Did the Gang Get Its Name?

The gang featured in this paper operate from the Yanbian Prefecture in Jilin, China, located north of the North Korean border, hence the name “Yanbian Gang.” [1] Although the prefecture’s economy primarily relies on agriculture, attacks recently instigated by a gang of hackers hailing from it put Yanbian on the security industry’s radar. [2] Much like the rest of the cybercriminals in China, members of the Yanbian Gang may have learned from so-called masters or baishis who passed on their blackhat skills and know-how to their apprentices or shoutus. [3]

Who Are the Gang’s Members?

Cybercriminal gangs typically have several members who play certain roles to instigate impactful attacks. The Yanbian Gang, in particular, comprises four major players or groups—the organizer, translators, cowboys, and malware creators.

THE ORGANIZER

The organizer can be considered the founding father of a hacker gang. He scouts for and recruits its members. Although he is not expected to be a technical expert, he should be very familiar with the cybercrime business. [4] He should know what kind of people he needs to hire for the attacks he has planned.

The members of a hacker gang do not necessarily need to know one another. They do not need to directly communicate with their peers. But they all communicate with the organizer, which makes the latter an indispensable gang member.

TRANSLATORS

Translators localize threats, depending on what countries they wish to target. In the case of the threat featured in this paper, the translators used Korean for their
specially crafted text messages and even the malicious file’s user interface (UI). A hacker gang can have more than one translator, especially if it wishes to target potential victims that speak more than one language.

**COWBOYS**

Cowboys reside in the same countries as their attacks’ intended victims. They are responsible for collecting the proceeds from successful attacks and giving them to the organizer. In the featured threat’s case, the cowboys were from South Korea.

Cowboys use so-called black or fridge cards to evade law enforcement. Black or fridge cards are bank cards that cannot be traced back to the cowboys or anyone they know. That way, even if the cards were found suspicious, they cannot be used to identify their users.

Chinese hackers trade black or fridge cards via QQ Chat groups. Interested buyers can purchase such cards for around US$725 or KRW800,000* each.

**MALWARE CREATORS**

Malware creators, the malicious app developers in this case, are probably the most important members of the gang, as the success of an attack largely depends on how effective their malicious creations are.

Mobile malware should continuously evolve to infect as many user devices as possible while evading detection by security solutions. It is the malware creators’ responsibility to stay abreast of security developments in order to create effective malware, which determine the success of an attack.

A hacker gang can have more than one malware creator. Most malware, in fact, were created by several people, each with his own field of expertise. Hackers can be seen publicly recruiting malware cocreators in bulletin board systems (BBSs) or chat groups.

**How Does the Gang Operate?**

The Yanbian Gang’s operator previously worked as an apprentice in another hacker gang where he learned about the cybercrime business. He probably met most of his new gang’s members through his former master who was most likely his former

*Exchange rate used (2 February 2015): US$1 = KRW1,103
gang’s organizer. He recruited others and communicated with all of the gang’s members via underground QQ Chat groups.

As far as research revealed, the Yanbian Gang only had one translator. But he could be working with several gangs at the same time. He does all of his transactions with the organizer via QQ Chat as well. Unlike most of the other members of the gang, however, he gets a fixed salary instead of a share of the profits.

The Yanbian Gang also had just one cowboy who lives in South Korea. Like the translator, he most likely communicated with the organizer via QQ Chat and phone calls. Though it was not clear how the cowboy sent the attack proceeds to the organizer, he most likely bought black or fridge cards from other hackers. As far as gangs go, cowboys or those who directly handle cash get a pretty huge share of the profit—40–95%. They are, after all, take the greatest amount of risk because they could be tracked if law enforcers decide to follow the money trail.

The gang also had just one malware creator who communicated with and submitted his creations to the organizer also via QQ Chat. Like the translator, he did not directly get a share of the profit, instead he gets a monthly salary as agreed upon when he was hired.

Cowboys collect money made from victimizing users via black or fridge cards. They then transfer the proceeds to the organizer’s bank account. Investigation results revealed that tens of thousands are transferred from the cowboys’ to the operator’s accounts each day.

What Types of Android Malware Did the Gang Use?

Note that all of the Android malware that the Yanbian Gang used in their attacks were not available for download on Google Play™ or any third-party app site. They were only distributed through malicious text messages or downloaded by other malware.

* Exchange rate used (2 February 2015): US$1 = RMB6
Fake banking apps sport the same icons and UIs as the official ones they spoof. These add to their feigned legitimacy. But for good measure, they also come with the ability to uninstall and take the place of the real apps they are spoofing. This allows them to run undetected while obtaining what they are after—victims’ personal account credentials that translate to financial gain for the fake apps’ operators.

Fake app execution is usually triggered by actions like booting devices, receiving text messages, and changes in user presence and network configuration. Once triggered, fake apps’ background services continuously and silently run in the background, leaking confidential user information to the malware operators. Victims’ bank account numbers, user names, passwords, and other data end up in hackers’ hands.

The malware used in one of the attacks we saw victimized customers of five South Korean banks—KB Kookmin Bank, NH Bank, Hana Bank, Shinhan Bank, and Woori Bank. Though they used different icons and UIs, it is clear that they were developed using the same malicious source code.
The fake apps exhibited the following behaviors:

- Designed and implemented a novel software-based AIS transmitter called “AISTX”

- Uploaded stolen user information, including mobile phone numbers; account names and numbers; and login credentials, to designated command-and-control (C&C) servers

- Wait for certain text messages that contain hacker commands to execute

- Block incoming text messages with control commands that do not come from the gang or whose content and sender numbers match certain rules the hackers set on their C&C servers

  Sender number rules block messages like verification codes sent by target banks. This allows the hackers to get the codes they will need to steal victims’ money while keeping the theft secret from the victims.

- Steal and upload stolen text messages to designated C&C servers

The C&C servers the Android malware accessed revealed close relationships among the malicious files. Our experiment revealed a total of 38 C&C servers located in different countries. Among these, 26 were accessed by two or more
malware. Clearly, the members of the Yanbian Gang are exerting a lot of effort to target certain South Korean banks’ customers. Evidence shows that they are well-organized, constantly improve their malware, and ensure that their C&C servers are always active.

APPS THAT HIJACK MOBILE BANKING SESSIONS

Android apps that hijack mobile banking sessions are designed to target several banks at once. They mimic their targets’ icons to dupe bank customers into thinking they are the real thing. Faking Android apps almost guarantees downloads and
installations due to the vast majority of the platform’s users. [5]

Android malware have BroadcastReceiver that could trigger various actions. [6] This class starts several background services, one of which monitors all currently running apps. It triggers certain malicious actions in the fake apps’ case every time an app of one of the banks it monitors is used. It allows a fake app to replace a legitimate one. The fake app’s UI then logs all of the affected user’s inputs—account number, user name, password, and other personally identifiable information (PII)—and uploads the stolen data to a C&C server.

One of the samples we analyzed for this paper targeted 17 South Korean banks based on its code. They also had all of the target banks’ UIs to add to their credibility. They intercepted text messages coming from and sent to the target banks, which were then uploaded to the hackers’ C&C servers.

FAKE VERSIONS OF POPULAR APPS

Apart from directly spoofing banking apps, cybercriminals also fake other apps that are downloaded by many Android users. Examples of these are the Google Play and Search and the Adobe® Flash® Player as well as porn apps. To better evade detection, some of them delete their icons but make sure that when the icons of their legitimate counterparts are clicked, the fake UIs are opened. Like the fake banking apps, these also silently run malicious behaviors in the background. Some download and install other malicious apps, delete files and folders, record text messages, take photos, steal files, and others, depending on what their creators want them to do.
Fake Google Apps

Google apps were most commonly spoofed to target South Korean bank customers. We took a look at a total of 1,007 fake Google app versions, 994 of which were fake versions of the Google Play app while the remaining 13 were fake versions of other Google apps. Cybercriminals most likely spoofed Google apps because they normally came preinstalled in every Android mobile device. The fake apps sported the Google apps' icons, which were deleted after installation.

Fake Porn Apps

Fake banking apps also came in the guise of popular porn apps with lewd icons and names and eye-catching descriptions like "sexy women photos" and "porn movies." They hardly ever deliver on their promise though when run. All they do, in fact, is steal and upload victims' mobile banking credentials to C&C servers.

Other Fake Apps

Cybercriminals also use fake versions of other popular apps, including utilities, chat, portal, and security apps to infect South Korean victims' devices and steal their mobile banking credentials.
HOW DID THE GANG INFECT VICTIMS’ DEVICES?

SMS Phishing

Fake banking apps are usually distributed via SMS phishing messages. To run successful SMS phishing campaigns though, cybercriminals need special hardware to send out large numbers of text spam to get as many victims as possible. They would need a GSM modem, for instance, to send thousands of text messages per hour. [7] These messages use convincing lures so victims would click a link that downloads malware, usually in the form of fake apps, onto their devices.

Via Other Malware

INTERNET POLICE SCARE TACTIC

The Yanbian Gang used fake Internet Police apps to victimize South Korean mobile banking customers. Potential victims received SMS phishing messages that scared them with supposed investigations if they did not click a given link. When clicked, however, the link installed a malicious app in their devices that communicated with designated C&C servers to listen for commands. We first spotted these malware in September 2013 and continued to see them till April 2014, proving the steadfast nature of the threats.
Cybercriminals are also known for using hot Hollywood topics or much-talked-about movies as lure to trick potential victims into downloading malware. One of the 2014 movies they spoofed to distribute malware that stole South Korean victims' mobile banking credentials was “The Interview.” This particular app had a very simple UI with two buttons that, when clicked, downloaded malware onto the users' devices.

How Do the Gang's C&C Servers Work?

The malware featured in this paper were primarily remote access tools (RATs). Each had a control panel that allowed the gang members to remotely go through and take control of victims' devices.
MOBILE BANKING MALWARE TRENDS

We observed an exponential increase starting January 2014 in the number of Android banking malware detected from May 2013 to December 2014. This could be due to the apparent malware source code sharing among cybercriminals particularly in Yanbian. In response, Trend Micro created heuristic detection patterns, which resulted in a decrease in the number of mobile banking malware after April 2014. Only the more highly skilled cybercriminals were able to push through with their attacks.

Relationships between Android malware and C&C servers were then determined. Each point in the following figure refers to a malware variant that accesses specific C&C servers marked by IP addresses. Seven significant C&C servers that hosted huge numbers of Android malware were found. These pointed to two different active hacker gangs.

A total of 174 mobile malware variants accessed 1.234.38.88. These also accessed 74 other servers. An additional 583 variants accessed 75 C&C servers, 11 of which hosted more than 10 variants each.

The C&C servers the mobile malware accessed at certain times were then plotted out. As shown, cybercriminals used several C&C servers to host and distribute malware. Before December 2013, several Android malware simultaneously accessed different C&C servers to receive updates, store stolen user information, and remotely control infected devices. After that, however, they only accessed a single server. Finally, the cybercriminals have been keeping all of the servers active since August 2013.

The C&C servers the Android malware accessed were widely distributed worldwide, so were their Internet service providers (ISPs). This showed just how much effort their operators exerted to evade detection by both security solutions and law enforcement.
Two Android malware variants targeting the customers of South Korean banks from one family were chosen for a comparison. The first was detected in October 2013 while the other was seen in February 2014. The second sample had six more classes than the first, clearly indicating improvements. The newly added class, `BankScardActivity`, allowed the Android malware to compress and upload mobile banking information to the hackers’ C&C servers.
This paper featured a still-active hacker gang from Yanbian that targeted customers of chosen South Korean banks. During the course of research, we found that what we have dubbed the “Yanbian Gang” was well-structured. The gang was brought and held together by an operator. This operator sought out the gang’s members—translators, cowboys, and malware creators—in BBSs and chat groups. Together, the gang’s members have been targeting the mobile banking customers of at least five banks in South Korea since 2013, earning them millions in profit.

As with other threats, awareness is the first step in protecting oneself from cybercrime. Potential business and individual targets should stay abreast of emerging trends and keep track of underground market developments to stay protected from all kinds of threats. [8–10] Learning lessons from victims of successful attacks can also help others protect themselves if they are ever in the same boat.
REFERENCES


