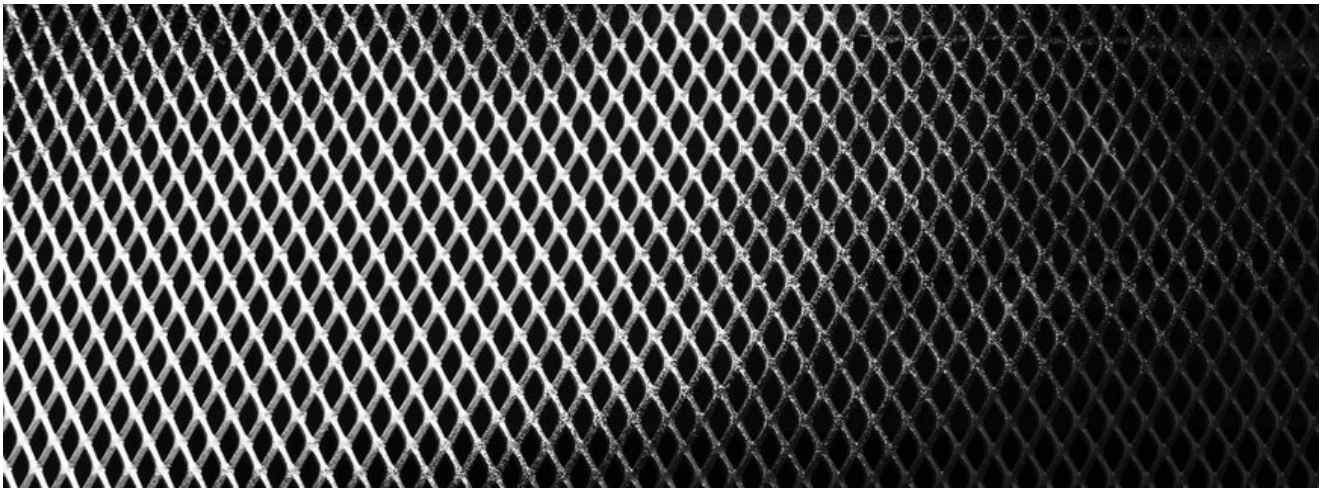
Yanbian Gang Malware Continues with Wide-Scale Distribution and C2

riskiq.com/blog/external-threat-management/yanbian-gang-malware-distribution/

April 7, 2021



Fake banking apps laced with malware continue to be an effective tool for threat actors. For the Yanbian Gang, a criminal group centered in Yanbian, China, that targets organizations across Asia, it's a craft they've been improving on for over a decade.

The Yanbian Gang has targeted South Korean Android mobile banking customers since 2013 with malicious Android apps purporting to be from major banks, namely Shinhan Savings Bank, Saemaul Geumgo, Shinhan Finance, KB Kookmin Bank, and NH Savings Bank. RiskIQ's threat research team examined some of the threat group's more recent activity in this vector to analyze their malware of choice and the large-scale hosting infrastructure they use to distribute and control it.

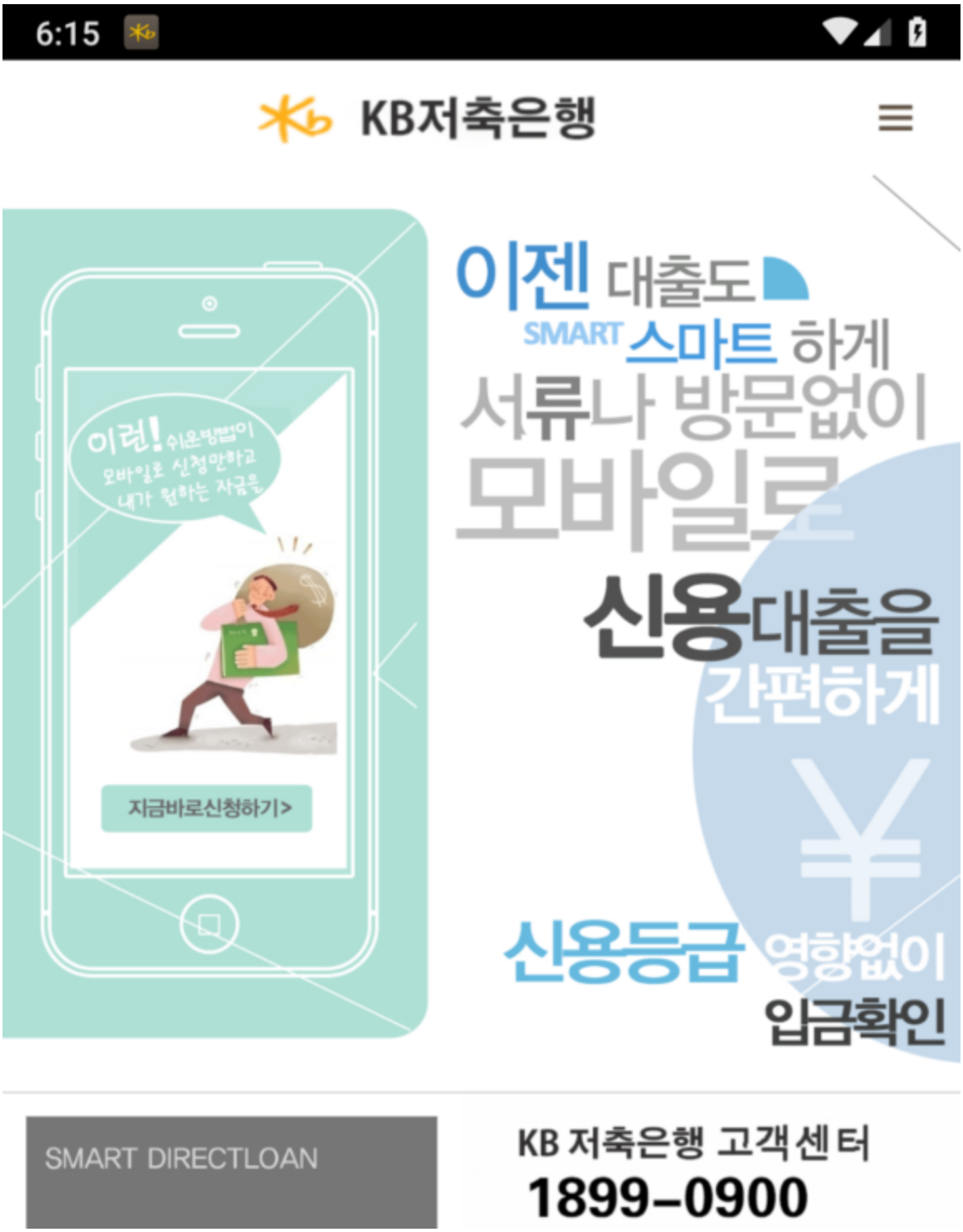
During their analysis of Yanbian Android apps, our researchers discovered hundreds of Korean language-specific apps across an extensive list of IP addresses. These apps were purpose-built to steal information from infected victims, including loan application details, contacts, SMS messages, phone call details, call logs, and applications currently installed on the device.

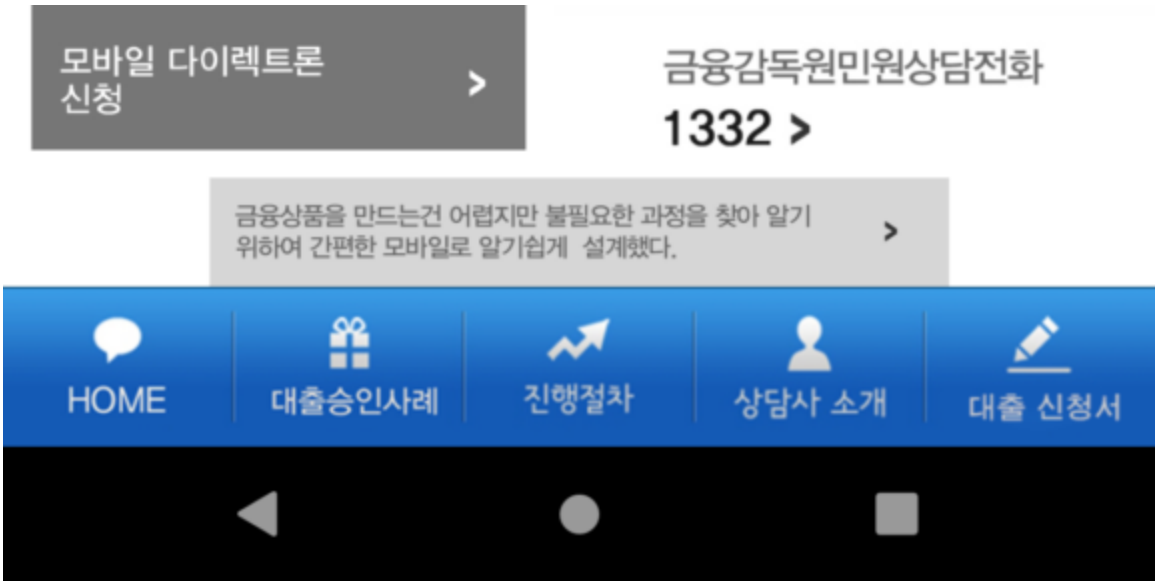
From a list of C2 servers used by the group gathered by OSINT and our own analysis, we identified pivot points and connections to more C2 servers used by other samples of malicious Android applications distributed by the Yanbian Gang. With RiskIQ data, we could catalog pages distributing the Yanbian Gang applications and paint a clear picture of the group's recent activity, infrastructure, and hosting services.

Yanbian Apps Reach Deep into Victim Pockets

Overall, RiskIQ's analysis identified 377 individual samples of malicious Android apps developed and distributed by the Yanbian Gang since December 2020. Many of these apps have multiple variants and set up services to run in the background of victim phones—both of which fit the known modus operandi of the Yanbian Gang.

While simple in nature, these apps perform several malicious activities unbeknownst to the victim. Yanbian Gang actors get details of the victim themself, but also their contacts, installed applications, and even messages sent from the infected device. These apps also have dozens of permissions they can potentially abuse for malicious purposes.





Example of Yanbian Gang app analyzed by riskIQ

A sample analyzed by RiskIQ was bundled with several packages, including for the application itself, its services, and how stolen data is encrypted and forwarded to the eventual C2 server. However, the reuse of an AES key and initialization vector (IV) we found in the apps' decompiled code helped us decrypt messages revealing interesting mechanisms that make the apps work.

One of these revelations was references to different URL paths that reached out to a direct IP address over HTTP. These paths, referred to by the Yanbian Gang as "methods," act as Command and Control (C2), allowing the app to initiate device registration, assess device capabilities, steal information, and receive instructions from specified C2 servers.

The 'Methods' to Yanbian Gang's Madness

RiskIQ researchers observed one of the samples communicating via only *some* of these "methods," likely because of the limited amount of data stored in our testing device and its lack of features. The app sent these communications via encrypted HTTP POST and GET requests to the C2 server. We used the Yanbian AES key and IV mentioned above to decrypt these messages and better understand the malware and the "method" URLs.

In-app view of customer data fields sent out to Yanbian C2s

We found that, for example, 'method 4' actively sends SMS messages to the C2 server that includes the recipient's contact name and number. Afterward, a POST request sends a list of all installed applications on the victim's phone to 'method 7." Then, after more interaction by

the victim in the faux Kookmin Bank App, another POST request sends name, contact, date of birth, address, name of work, annual salary, and other loan application details.

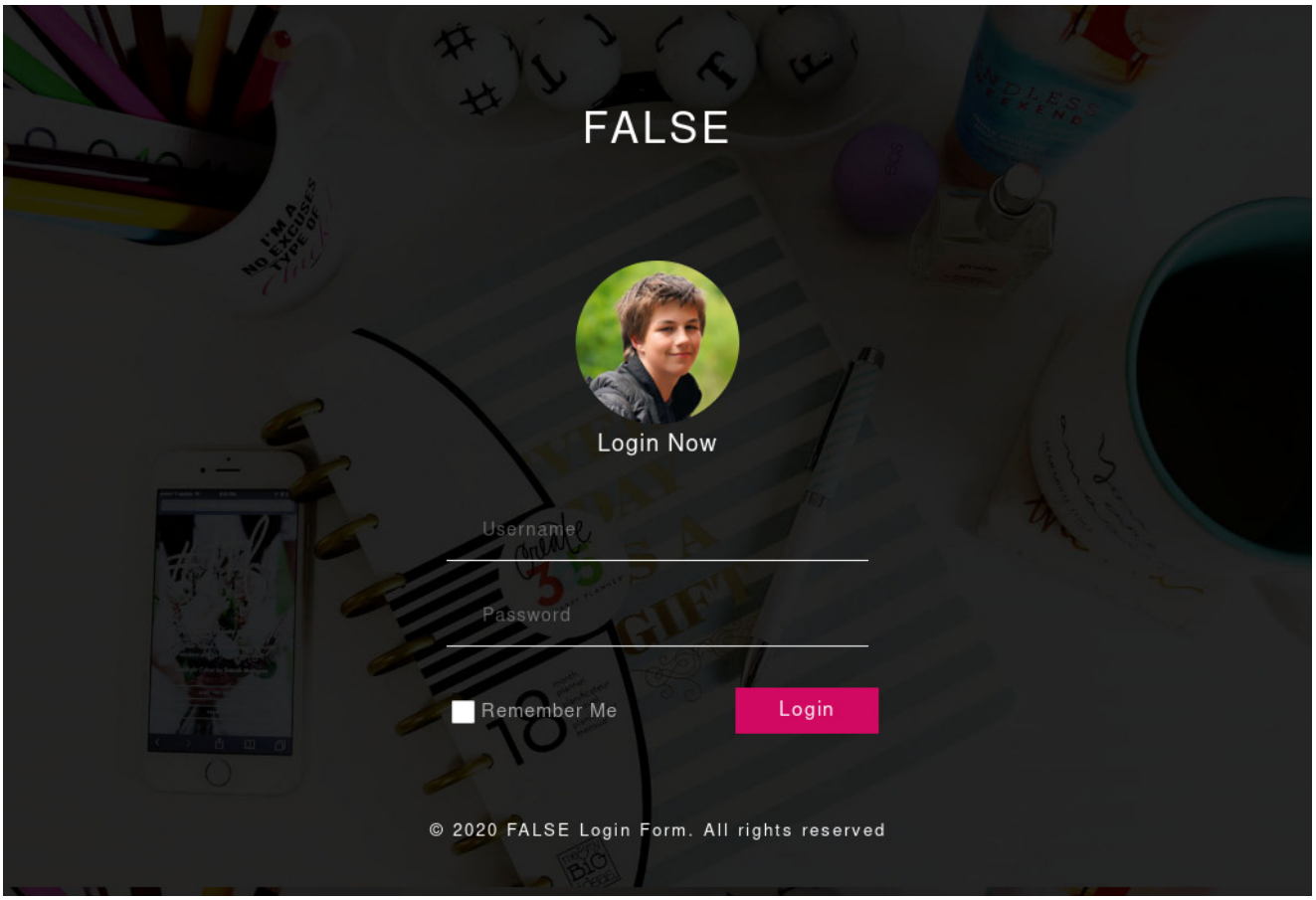
Yanbian Infrastructure Knows Its Role

The Yanbian gang uses large sets of servers for distribution and C2. However, our analysis shows operators keep distribution wholly separate from C2 activity with designated servers filling three sole functions:

- Hosting call-to-action pages and delivering malicious apps. Distribution occurs via Yanbian Gang-controlled hosts, not through app stores
- C2
- Running the Real-Time Messaging Protocol, which receives call information.

We have so far identified 377 individual samples of malicious Android apps, each containing strings pointing to C2 servers. During our breakdown of a malware sample, we identified one such C2 server at an IP address. A RiskIQ crawl showed that this and other Yanbian C2 servers were all loading fake banking pages from the same host.

We can pivot on one of these fake banking pages by its Mark of the Web source via our Trackers dataset in PassiveTotal. We found five hosts and 745 IP addresses all connected to the same page:



Yanbian Gang fake banking login page

RiskIQ has directly observed 86 of these IP addresses in the code of malicious Yanbian Gang Android applications ingested into our mobile app index. Further analysis of fake login pages allowed us to identify a total of 177 IP addresses used by the Yanbian Gang for C2.

The Yanbian Gang uses many servers for both distribution and C2, though we observed far more distributing the malware than acting as C2. The distribution pages from which these apps were downloaded were hosted on 266 IP addresses. Not surprisingly, the distribution pages all mimic the websites of banking institutions.

All told, with RiskIQ's unique data sets, we could identify 177 IP addresses acting as C2 servers and 266 IP addresses acting as distribution servers.

Yanbian Hosting: Divide and Conquer

The Yanbian Gang uses different hosting providers for their C2 servers versus their distribution servers, which appears to be a new group evolution. The Gang operates a huge number of servers for both distribution and C2. However, we have observed many more servers distributing the malware than acting as C2.

The group's 177 C2 servers are primarily hosted in Hong Kong by SunnyVision Limited, Forewin Telecom Group Limited, and Sun Network (Hong Kong) Limited. A few servers are also hosted in Singapore by BGPNET Global.

Yanbian's 266 distribution servers, in contrast, are located in China and Taiwan. The largest share of the servers are hosted by Taiwanese company HINET, with a few more hosted in Taiwan by Asia Pacific On-line Service Inc. Fifty of the distribution servers are hosted by CHINANET-BACKBONE.

The set of hosting providers used for C2 is more diverse than distribution, centered mainly on HINET infrastructure. The group appears to reuse C2 infrastructure, with multiple malicious apps communicating with the same servers, thus leading to fewer servers needed for that purpose.

Conclusion

The Yanbian Gang continues to target South Korean users with malware, tactics, and targeting similar to that previously reported in 2015. However, the group has evolved to separate infrastructure based on its function and change hosting providers. RiskIQ observed that Yanbian Gang actively leverages web servers hosting their call-to-action and malicious application delivery, C2 servers, and servers running the Real-Time Messaging Protocol that receive call information.

Extending security and IT protection outside the firewall requires mapping these billions of relationships between the internet components belonging to every organization, business, *and* threat actor on Earth. RiskIQ's Internet Intelligence Graph enables us to take a broader view of campaigns, such as those by the Yanbian Gang targeting South Korean mobile banking customers. By graphing the deep relationships between infrastructure in the global attack surface, we can discover significant trends and fingerprint different sets of indicators to identify large-scale malicious infrastructure efficiently.

Visit our Threat Intelligence Portal for the complete technical analysis of the Yanbian Gang, including a full list of IOCs surfaced in our investigation.