Introduction

A unique difference with the past cases was discovered during the analysis of the Kimsuky group's spear phishing URLs. Until now, the group used Fully Qualified Domain Names (FQDN) disguised as famous Korean web portals. An analysis of the URLs collected during the past two months revealed multiple new FQDNs including keywords related to certain Korean banks, instead of the past FQDNs disguised as web portals.

Kimsuky Group

1) About the Threat Actor

Kimsuky is a threat group thought to be supported by North Korea, and it has been active since 2013. At first, they attacked North Korea-related research institutes in South Korea before attacking a Korean energy corporation in 2014. Since 2017, their attacks have been targeting countries other than South Korea as well. Other names of Kimsuky are as follows.

APT-Q-2, Baby Coin, Black Banshe, Black Banshee, Mystery Baby, Operation Stolen Pencil, RGB-D5, Smoke Screen, Stolen Pencil, Thallium, Velvet Chollima

(1) Trends

The Kimsuky group seems to be sending phishing emails not to unspecified masses but only to targets deemed to be North Korean defectors or North Korea-related figures. Relevant details were covered in an ASEC blog post.

- Web Page Disguised as a Naver Login Page // Feb. 13, 2023
- Web Page Disguised as a Kakao Login Page // Jan. 10, 2023

Such phishing emails sent to specific targets are called spear phishing emails. The following is a chart showing the number of the Kimsuky group's spear phishing URLs collected during the past two months. In addition, it must be noted that this figure includes duplicate collections as spear phishing typically does not yield a high number of cases and the same URL can be sent multiple times to a particular target.

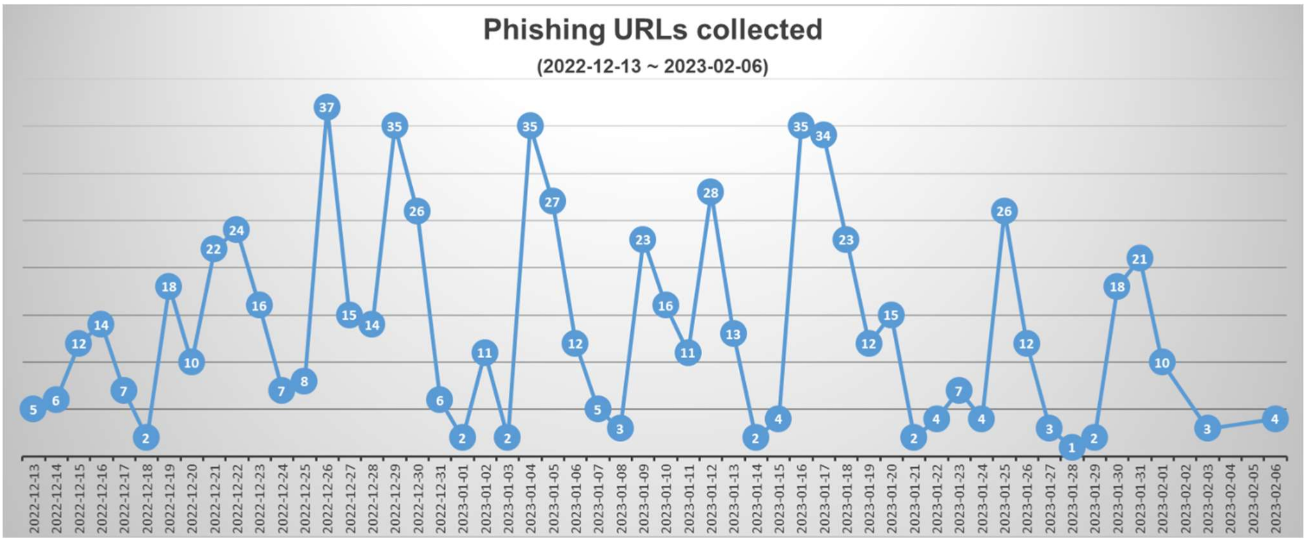

Figure 1. Kimsuky spear phishing URLs collected in the last two months

Cases up to this point disguised the URLs and the spear phishing web pages as those of famous Korean web portals (Naver, Kakao, Daum) to induce relevant targets to change the password to their email services, blog, and cloud services provided by the portals.

(2) Unique Characteristics

A unique characteristic was found during the analysis of recently collected spear phishing URLs of the Kimsuky group. A keyword analysis of the URL FQDNs collected during the above period revealed that there were more cases with keywords related to "Nonghyup (Korean National Agricultural Cooperative Federation)" than keywords that impersonate well-known Korean web portals. This is a very interesting point as keywords related to other Korean banks and credit card companies were not found in the collected URLs. The following is a chart summarizing 700 FQDNs collected during the above period that shows the ratio of the brands impersonated.

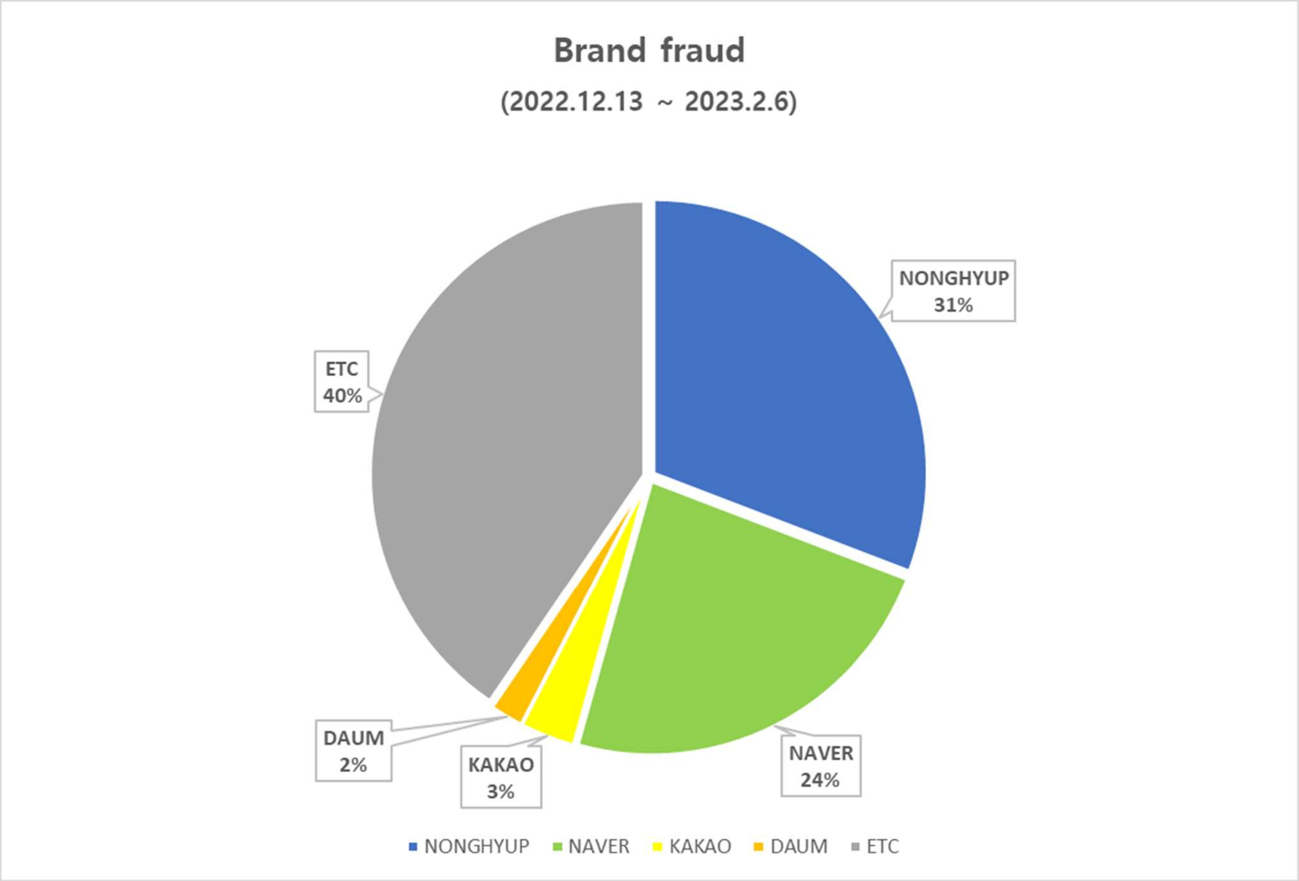

Figure 2. Ratio of brands impersonated in keywords of the FQDNs

The following is the list of the top 10 FQDNs where the keyword "Nonghyup" was most frequently used.

No	Domain
1	nid.nhcard.nemo.de-one.click
2	nid.nong.hyup.view.file.nh2023.click
3	nld.nhcard.svchost.click
4	nid.nhcard.nemo.trade.de-one.click
5	uid.nong.card.view.mpevalr.success.de-one.click
6	nood.nong.card.nemo.mpevalr.success.de-one.click
7	nld.nhcard.com-wine.click
8	nood.nong.hyup.view.nh2023.click
9	mld.nhcard.blog.mpevalr.vultr.com-wine.click
10	nid.nhcard.svchost.click

Table 1. List of the top 10 FQDNs most frequently used

These domains were all registered by a Japanese domain registrar. The following shows the Whois information of the most frequently used domain.

Whois Lookup	Data
Create date	2023-01-13
Domain name	de-one.click
Domain registrar id	49
Domain registrar url	http://www.onamae.com
Expiry date	2024-01-13

Table 2. Whois information of the most frequently used domain

(3) Conclusion

As in most spear phishing cases, this URL is not available for access, and it could be determined whether only the FQDN was disguised as a bank or if the content of the web page was also forged.

However, seeing from the fact that 40% of the FQDNs (ETC category) collected during the concerned period are meaninglessly created domains that have no connection to Nonghyup or famous Korean web portals, it is deemed that the content of the websites was not forged. This may be also because it is costly and time-consuming for threat actors to create website content for meaninglessly made FQDNs.

It is assumed that only the general keywords and formats of the URLs (web portal names, service names, keywords such as Blog, Mybox, and Cloud) are maintained to create a sense of familiarity as many users do not pay close attention to security before clicking URLs; thus only the login page content of web portals is forged to steal the target's email passwords.