Kimsuky Group's Phishing Attacks Targetting North Korea-Related Personnel - ASEC

By ATCP

Published: 2023-05-15 · Archived: 2026-04-05 18:13:57 UTC

AhnLab Security Emergency response Center (ASEC) has recently discovered that the Kimsuky group had created a webmail website that looks identical to certain national policy research institutes. Earlier this year, ASEC had covered similar issues in the posts 'Web Page Disguised as a Kakao[1]/Naver[2] Login Page'. The previous attacker set the fake login page with autocompleted IDs of trade, media, and North Korea-related individuals and organizations. In addition to that, the recently discovered web page **used a similar tactic of having the ID of the target organization's leader autocompleted in the recently created website.** When the user attempts to login, the threat actor comes into possession of the internal webmail website account credentials. This data is deemed as useful as procuring the account information of the target user's portal website account credentials.

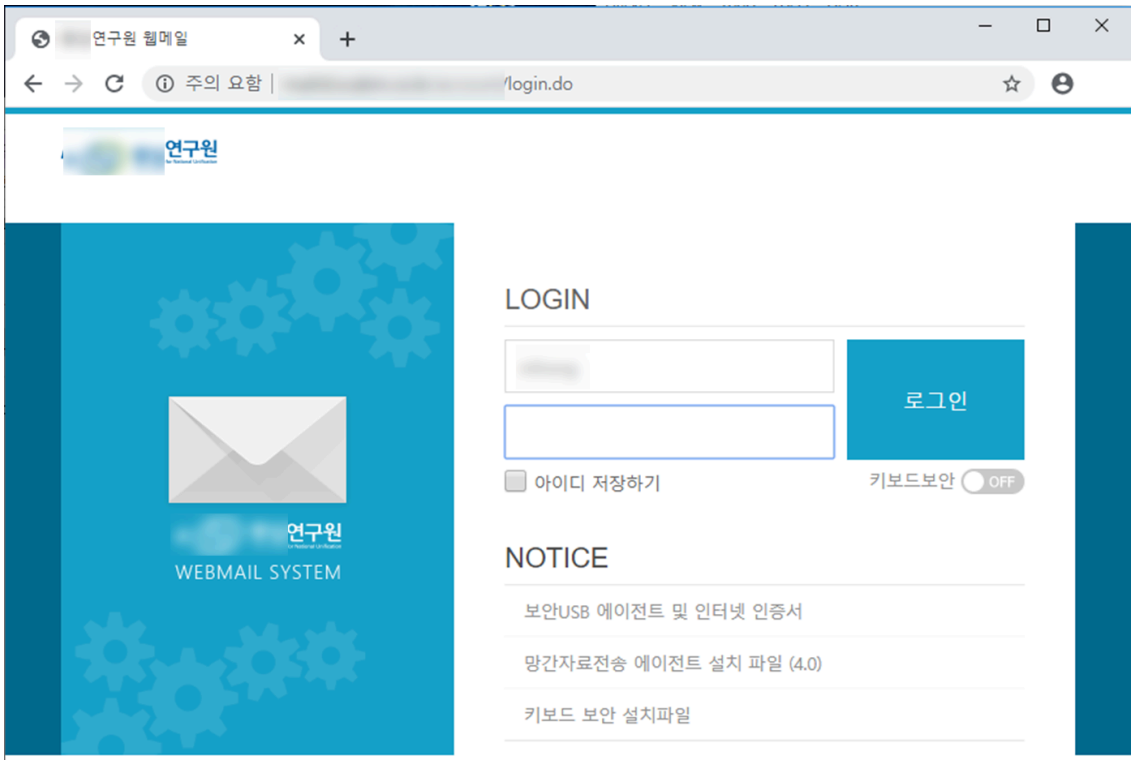

Figure 1. Webmail login page created to target North Korea-related business managers

Judging from the reverse DNS data-related IP/domain addresses and relevant files collected by ASEC up to this point, **it is assumed that the Kimsuky group is behind this act.** As just explained, cases that directly use web sources of widely well-known websites are increasing, and websites that impersonate portal websites and organizations' webmail infrastructures by manipulating multiple domains are constantly being found. When users need to log in to web pages that require a separate login process including webmail systems, users must re-check

the validity and authenticity of the visited URL and its certificates, and must refrain from accessing unknown URLs sent from a separate external source.

URL

http[:]//mailid[.]scabm[.]co[.]kr/account/login[.]do

Additional IOCs are available on AhnLab TIP.

Gain access to related IOCs and detailed analysis by subscribing to **AhnLab TIP**. For subscription details, click the banner below.

Source: https://asec.ahnlab.com/en/52970/