Kimsuky’s latest campaign involves using social engineering tactics to trick victims into logging into fake websites and providing sensitive information. The group sends phishing emails with malicious documents containing ReconShark reconnaissance malware. The fake login sites are hosted on a website impersonating NK News, and the C2 server for ReconShark communication is hosted on a domain associated with Kimsuky.

The social engineering tactic is designed to look like a legitimate NK News login site hosted at `https://www.nknews.pro/ip/register/login.php`. On closer inspection, the displayed URL points to a Google document, delving into the topic of North Korea, to build perceived legitimacy. The URL's destination is manipulated through the spoong technique of setting a `loc` HTML property.

The displayed URL to a Google document points to an actual article hosted on Google Docs, which can be accessed directly by entering the full URL. This is a common tactic used by malicious actors to enhance the perceived legitimacy of their sites.

Kimsuky's objective is to gather strategic intelligence by gathering email credentials, stealing subscription credentials from NK News, and deploying ReconShark reconnaissance malware. The group's activities are probably part of a broader campaign to gather intelligence about their targets.

The group's tactics include using spoofed URLs, websites imitating legitimate websites, and employing social engineering techniques to trick victims into providing sensitive information. These actions are probably part of their broader objective to gather strategic intelligence, contributing to their subsequent malicious activities.

Kimsuky remains active in monitoring the threats posed by this persistent threat actor. Implementing effective security measures is imperative to mitigate the risks posed by this campaign.