# North Korean Kimsuky Hackers Use Russian Email Addresses for Credential Theft Attacks

By The Hacker News

Published: 2024-12-03 · Archived: 2026-04-05 15:59:04 UTC

The North Korea-aligned threat actor known as **Kimsuky** has been linked to a series of phishing attacks that involve sending email messages that originate from Russian sender addresses to ultimately conduct credential theft.

"Phishing emails were sent mainly through email services in Japan and Korea until early September," South Korean cybersecurity company Genians said. "Then, from mid-September, some phishing emails disguised as if they were sent from Russia were observed."

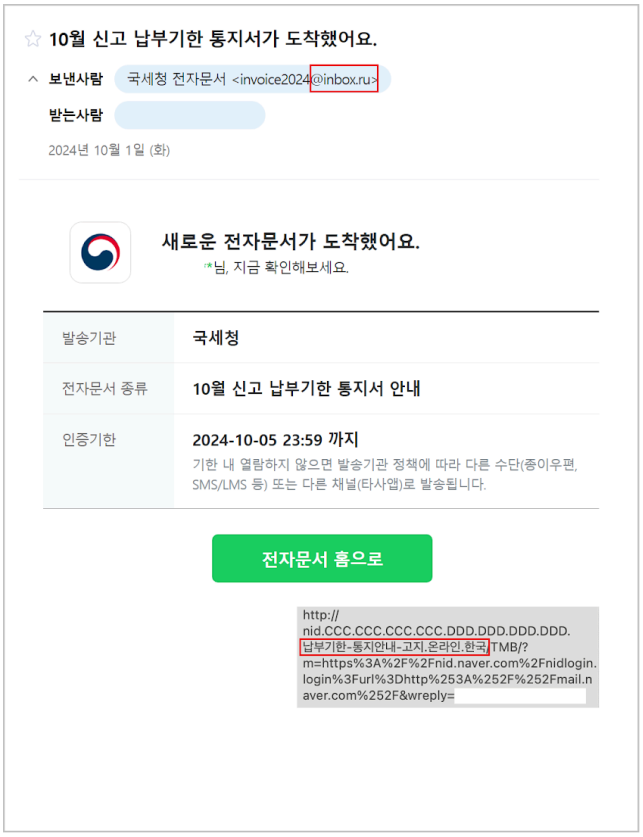
This entails the abuse of VK's Mail.ru email service, which supports five different alias domains, including mail.ru, internet.ru, bk.ru, inbox.ru, and list.ru.

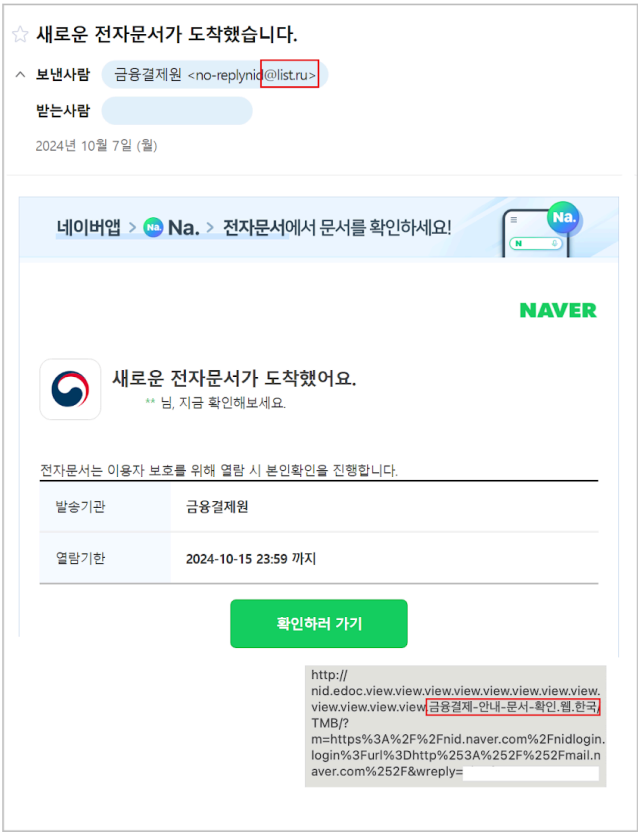
Genians said it has observed the Kimsuky actors leveraging all the aforementioned sender domains for phishing campaigns that masquerade as financial institutions and internet portals like Naver.

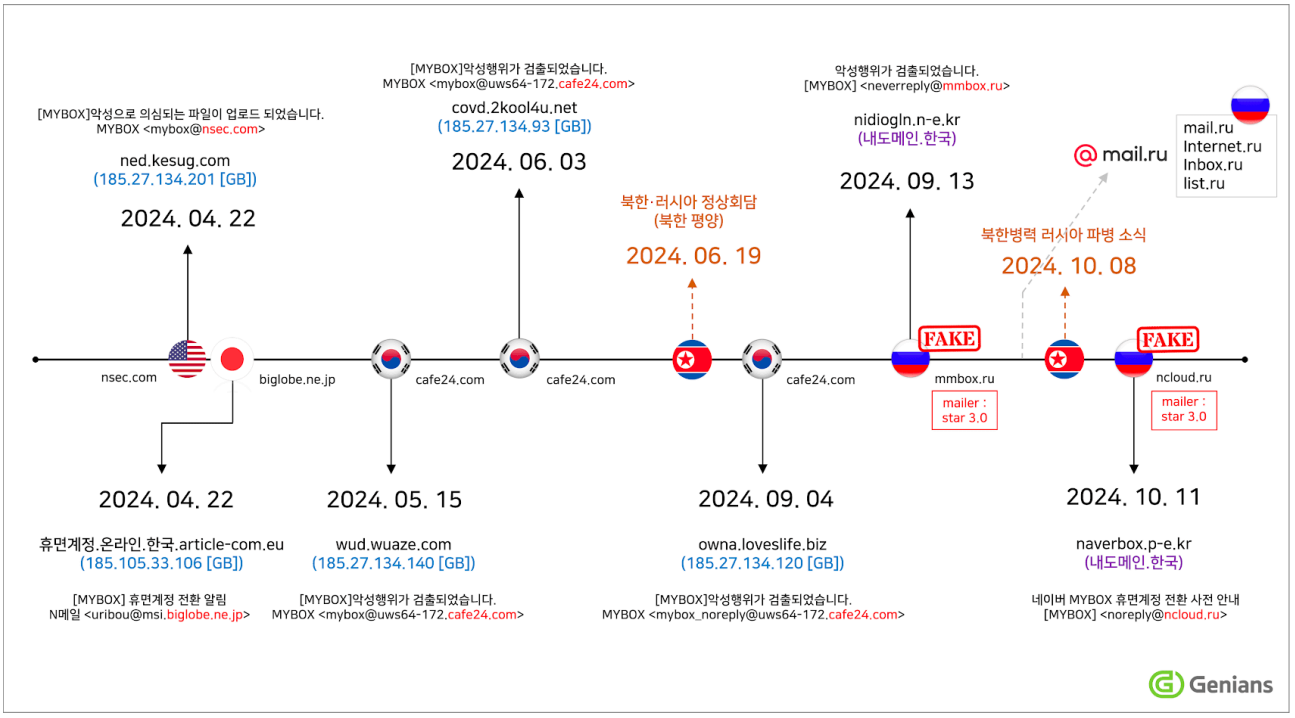


Other phishing attacks have entailed sending messages that mimic Naver's MYBOX cloud storage service and aim to trick users into clicking on links by inducing a false sense of urgency that malicious files had been detected in their accounts and that they need to delete them.

Variants of MYBOX-themed phishing emails have been recorded since late April 2024, with the early waves employing Japanese, South Korea, and U.S. domains for sender addresses.



While these messages were ostensibly sent from domains such as "mmbox[.]ru" and "ncloud[.]ru," further analysis has revealed that the threat actor leveraged a compromised email server belonging to Evangelia University (evangelia[.]edu) to send the messages using a PHP-based mailer service called Star.

It's worth noting that Kimsuky's use of legitimate email tools like PHPMailer and Star was previously documented by enterprise security firm Proofpoint in November 2021.

The end goal of these attacks, per Genians, is to carry out credential theft, which could then be used to hijack victim accounts and use them to launch follow-on attacks against other employees or acquaintances.



Over the years, Kimsuky has proven to be adept at conducting email-oriented social engineering campaigns, employing techniques to spoof email senders to appear as if they are from trusted parties, thus evading security checks.

Earlier this year, the U.S. government called out the cyber actor for exploiting "improperly configured DNS Domain-based Message Authentication, Reporting and Conformance (DMARC) record policies to conceal social engineering attempts."

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.

---

Source: https://thehackernews.com/2024/12/north-korean-kimsuky-hackers-use.html