Analyst's Note — Kimsuky

2025-01-20
By Alec Dhuse

The threat actor known as Kimsuky, also referred to as Emerald Sleet, has been observed targeting a United States-based think tank. The target received an invitation to a meeting with the Embassy of Japan in Washington, D.C., which was sent to their personal email. The threat actor created a free Proton email account, using it to impersonate an employee of the Japanese Embassy.

The email included the impersonated embassy staff member's benign Curriculum Vitae (CV) and encouraged the target to communicate with the attackers via WhatsApp. The target of this attack did not respond to the message or further the communication chain, so the next steps are unknown.

While the steps of this specific attack are unknown, this tactic is likely designed to initiate credential phishing or to deliver a malicious file that could start a malware infection. Due to the encrypted nature of WhatsApp and its frequent use on personal devices, standard security tools may struggle to intercept malicious links and files sent via this service.

Recommendations:

1. Train staff to recognize that emails from free email providers such as Gmail, Outlook, Yahoo, and Proton Mail can easily be used for impersonation. Emphasize that personal emails are also likely targets due to fewer security measures.

2. Educate staff on the risks of switching to encrypted messaging platforms like WhatsApp, as the app's encryption makes it difficult for security tools to intercept or inspect malicious content.

3. Use a secure DNS service on mobile devices with block lists for new and suspicious domains to prevent connections to phishing and malware-hosting sites.

Indicators of Compromise (IoCs):

Sender Email: a.keiichi0922@proton[.]me

WhatsApp Number: +19402886399

Benign CV File Hash:
b68c90763a11b10027a10f5c17bd731eb4d2c50770dbcf5456ea0102efbaad3a

Tags

- **Cybersecurity**
- **Threat Intelligence**