Severity

High

Analysis Summary

Konni’s APT Group continues to attack malicious documents written in Russian. Konni’s APT Group conducts attacks with Russian-North Korean trade and economic investment documents.

The vector used for the attack is probably the Spear Phishing method and has been reported in Korea.

The malicious file suspected of being used as an attachment has the name congratulation.zip.

On December 20th messages made to contaminate the Russian consulate situated in Indonesia have been distinguished; these messages involved the New Year Eve 2022 merriment as imitation topic. In spite of its past activities, the North Korean APT gathering this time didn’t involve vindictive records as connections; all things being equal, they joined a .compress record type named “congratulation.zip”, which implies “praise” in Russian, containing an installed executable addressing the primary phase of the disease. The messages were spoofed utilizing a *@mid.ru account as a source to imagine that it was sent from the Russian Embassy in Serbia.

Impact

- Information Theft and Espionage

Indicators of Compromise

MD5

- 4c904f67a1328ed1aaa306dfd562afc2

SHA-256

- f1131f164ab07608f6f04a600d616cc1c768cc234a1714f8120636a8e6446315

SHA-1

- 81bd8dbbdd66f7b9826b157d5c675bb2324d3fc9

Remediation

- Block all threat indicators at your respective controls.
- Search for IOCs in your environment.
- Always be suspicious about emails sent by unknown senders.
- Never click on the link/attachments sent by unknown senders.