New North-Korean based backdoor packs a punch

cyberarmor.tech/new-north-korean-based-backdoor-packs-a-punch/

Nguyen Nguyen

In recent months, North Korean based threat actors have been ramping up attack campaigns in order to achieve a myriad of their objectives, whether it be financial gain or with espionage purposes in mind. The North Korean cluster of attack groups is peculiar seeing there is quite some overlap with one another, and it is not always straightforward to attribute a specific campaign to a specific threat actor.

In this research paper we analyse a new threat campaign, discovered in late May, and which features multiple layers and ultimately delivers a seemingly new and previously undocumented backdoor.

The threat campaign is specifically focused on Aerospace and Defense companies: sectors appealing to multiple threat actors, but of particular interest to North Korean threat groups in other recent campaigns. We have named this threat campaign "Niki" as it refers to the potential malware developer(s).

Click to Download