Andariel, Silent Chollima, PLUTONIUM, Onyx Sleet, Group G0138

Archived: 2026-04-02 10:55:01 UTC

Andariel is a North Korean state-sponsored threat group that has been active since at least 2009. Andariel has primarily focused its operations--which have included destructive attacks--against South Korean government agencies, military organizations, and a variety of domestic companies; they have also conducted cyber financial operations against ATMs, banks, and cryptocurrency exchanges. Andariel's notable activity includes Operation Black Mine, Operation GoldenAxe, and Campaign Rifle.[1][2][3][4][5]

Andariel is considered a sub-set of Lazarus Group, and has been attributed to North Korea's Reconnaissance General Bureau.[6]

North Korean group definitions are known to have significant overlap, and some security researchers report all North Korean state-sponsored cyber activity under the name Lazarus Group instead of tracking clusters or subgroups.

Source: https://attack.mitre.org/groups/G0138/