Konni (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-06 02:13:03 UTC

Konni is a remote administration tool, observed in the wild since early 2014. The Konni malware family is potentially linked to APT37, a North-Korean cyber espionage group active since 2012. The group primary victims are South-Korean political organizations, as well as Japan, Vietnam, Russia, Nepal, China, India, Romania, Kuwait, and other parts of the Middle East.

▶ [TLP:WHITE] win_konni_auto (20251219 | Detects win.konni.)
