Kimsuky: North Korea takes its AI offline

A North Korean state hacking group has installed AI software on its own servers so it can run offline. No provider to log what it asks, and nobody to switch it off. The capability is early; the barrier it steps around is not.

INCIDENT DETAILS · 5WH

Who Kimsuky, also tracked as APT43 and Velvet Chollima - reported to operate under North Korea's Reconnaissance General Bureau, US Treasury-sanctioned in 2023. Disclosed by Genians.
What Software for running large language models found installed, configured and executed on the group's own machines, plus a tested method for pointing a model at a private document collection.
Where On infrastructure attributed to the group. Targeting directed at South Korean diplomatic, military, security, policy, academic and financial organisations.
When Published Monday 10 Aug 2026, after months of infrastructure tracking.
Why Running it in-house removes the provider - no account to suspend, no third-party logs, no refusal.
How Forensic traces show the software was run, not merely downloaded. No victim of the AI capability has been identified.

IMPACT

- Immediate: none demonstrated. No victim identified and no incident attributed to it. This is a finding about preparation.
- Detection: better lures defeat the advice most organisations give - look for poor English and odd formatting is exactly what this removes.
- Policy: efforts to police AI misuse assume it can be caught where the technology is served. An actor on its own hardware is outside all of it.
- Context: DPRK-linked actors are reported to have stolen over two billion dollars in digital assets in 2025.

SEQUENCE OF EVENTS

A Running a model locally means no provider sees the requests
B Kimsuky previously used a commercial chatbot for phishing - and was seen
C GitHub used to carry attacker instructions, documented since April

1 Operation GitPower: a shortcut file installs remote-access software
2 Instructions taken from public code repositories, not a suspect server
3 Decoy documents show signs of AI generation and read naturally
4 Three local AI environments found installed and executed
5 No self-trained models, no victim shown, findings unverified by Reuters

ASSESSMENT, LESSONS, AND RECOMMENDATIONS

- The headline overstates what was found; the finding is still important, and does not need inflating.
- Provider-side controls cannot reach an actor who does not use a provider.
- The advice most organisations give on phishing is now the advice most likely to fail.
- It is highly likely that locally hosted AI becomes routine in state and criminal operations.