Microsoft Attributes ConnectWise Cloud Backup Compromise to China-Aligned Storm-0940



Microsoft says China state-aligned actor Storm-0940 was behind the supply chain compromise of ConnectWise Cloud Backup, using the agentic AI framework ARTEX to speed up its activity.

- Microsoft disclosed the attribution on a Wednesday, naming Storm-0940 as the actor.
- The target was the ConnectWise Cloud Backup application, compromised through the supply chain.
- The actor used ARTEX, a Go-based agentic AI penetration testing framework, to accelerate scanning and related activity.
- ARTEX was reportedly made closed-source after earlier abuse against South Korean financial institutions.
- The source excerpt gives no technical indicators, CVEs or victim counts.

What was reported

Microsoft has disclosed that Storm-0940, an actor it describes as China state-aligned, was responsible for the recent supply chain compromise of the ConnectWise Cloud Backup application. According to the report, the group used **ARTEX**, a Go-based agentic AI penetration testing framework, to speed up scanning and related activity during the incident.

The framework was reportedly made closed-source after it was abused against South Korean financial institutions. The source excerpt is brief and does not provide indicators of compromise, affected versions, CVE identifiers or the number of victims.

Why it matters

This case combines two concerns for regulated institutions: reliance on third-party backup and management tooling, and attackers using AI agents to move faster through reconnaissance. Financial institutions have already been named as targets of earlier ARTEX abuse, which makes the report relevant to the Saudi financial sector.

What to do next

Institutions that use ConnectWise Cloud Backup should treat this as a prompt for a calm, structured review rather than an emergency. Watch for fuller technical details from Microsoft and ConnectWise, and confirm your exposure through your vendor management channels. Until more is published, avoid assumptions about scope or impact.

What to do now

1. Check whether ConnectWise Cloud Backup is used anywhere in your environment, including by managed service providers acting for you.
2. Contact ConnectWise and your service providers for confirmation of exposure and any guidance they have issued.
3. Review the access and credentials held by backup tooling and rotate them if the vendor advises it.
4. Monitor Microsoft and ConnectWise publications for indicators of compromise and add them to detection once available.
5. Record the review in your third-party risk register and brief the CISO and relevant committee.