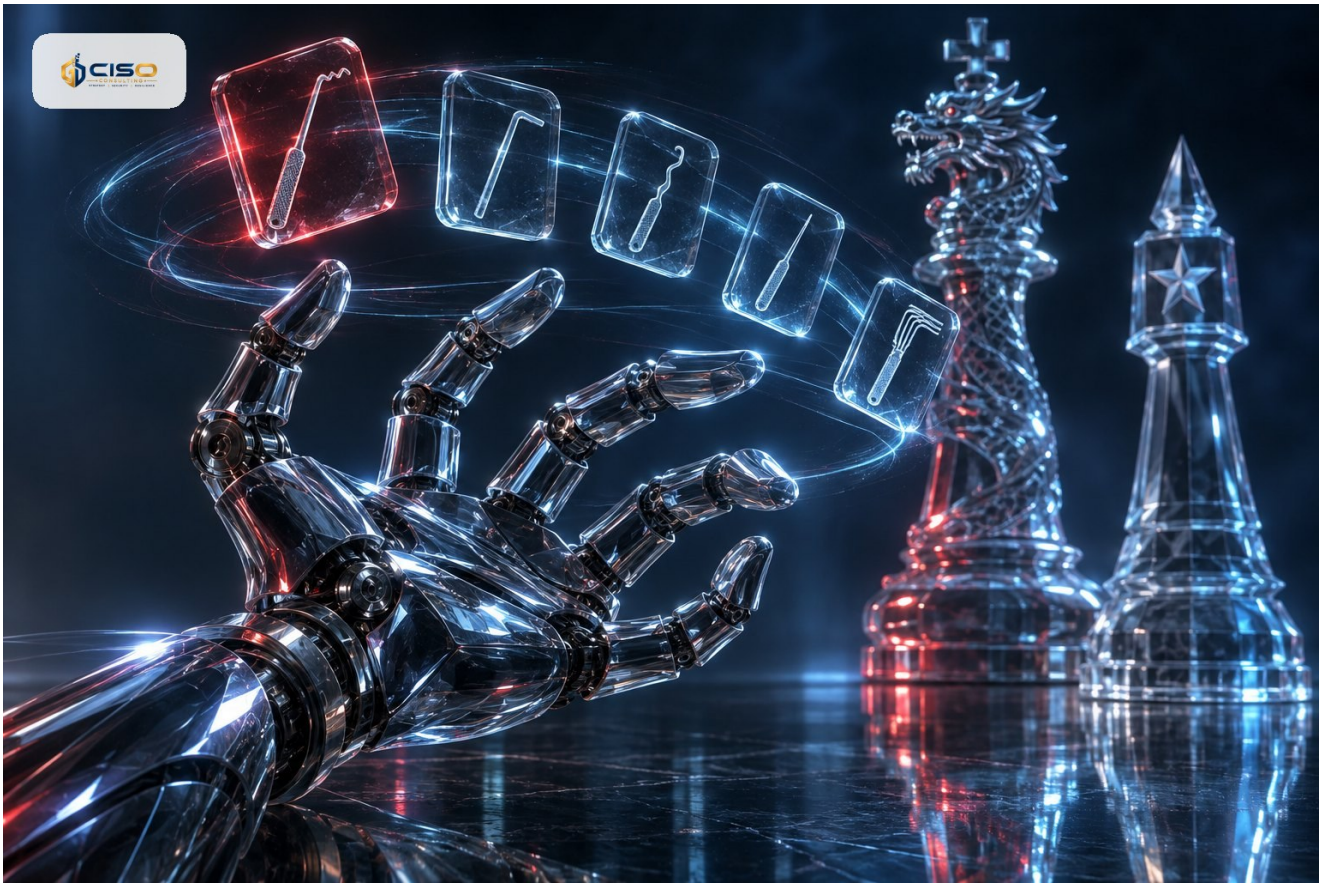
Microsoft: State-backed groups are using the AI tool Artex to speed up intrusions



Microsoft reports that Chinese and North Korean state-backed groups, including Salt Typhoon, use the AI platform Artex to automate intrusion stages. Its most reliable signal is behavioural, so detection should not rely on static indicators.

- Microsoft says Artex is an AI-powered platform that automates several phases of an intrusion at machine speed.
- Chinese groups Crystal Typhoon and Salt Typhoon use it for network reconnaissance, credential attacks and web application exploitation.
- Artex adds no new techniques; it uses existing penetration testing tools, and attackers vary IP addresses and user agent strings to evade signature-based blocking.
- The most durable signal is behavioural: many varied requests in a short time, repeated retries and

rapid movement to next-stage actions.

- The FBI issued its own advisory two weeks earlier, and copies of the tool remain available after the original source code was removed from GitHub.

Microsoft has published a report saying state-backed and financially motivated threat actors are using Artex, an AI-powered platform that automates multiple phases of a cyber intrusion at machine speed. It names the Chinese groups Crystal Typhoon and Salt Typhoon, which it says use the tool for network reconnaissance, credential attacks and web application exploitation. North Korean groups are also reported to use it.

What the tool does

Artex lets an operator set specific goals and then directs AI agents against a target. Microsoft says it can move from reconnaissance to persistent, privileged access in a matter of minutes. Recent campaigns abused it to search public repositories for exposed secrets, enable supply chain compromise and scan internet-facing systems for exploitation.

Microsoft stresses that Artex introduces no new attack techniques. It relies on common penetration testing tools. By default it makes no effort to hide its activity.

Detection implications

Attackers using Artex can change source IP addresses and user agent strings, so static or simple signature-based blocking may miss them. Microsoft describes behaviour as the most reliable signal: a wide variety of requests in a brief time, retries of variations on the same technique, and quick moves to next-stage actions. A large volume of anomalous traffic from a single source in a short period is a typical sign.

The original developer removed the source code from GitHub, but copies exist and at least one Chinese company offers commercial access to a version. The FBI has also issued its own advisory on the tool. The source does not give details of any activity in Saudi Arabia.

What to do now

1. Add behavioural detections for bursts of varied requests, repeated retries and rapid progression from one source, rather than relying only on IP or user agent blocklists.
2. Review internet-facing systems and web applications for exposure and patch priorities, since Artex is used to scan and exploit them.
3. Search public code repositories for exposed secrets and rotate any credentials found.
4. Strengthen credential protections such as multi-factor authentication and monitoring for credential attacks.
5. Review supplier and IT management software access, given the reported supply chain use.

6. Update incident response playbooks for intrusions that move from reconnaissance to privileged access within minutes.