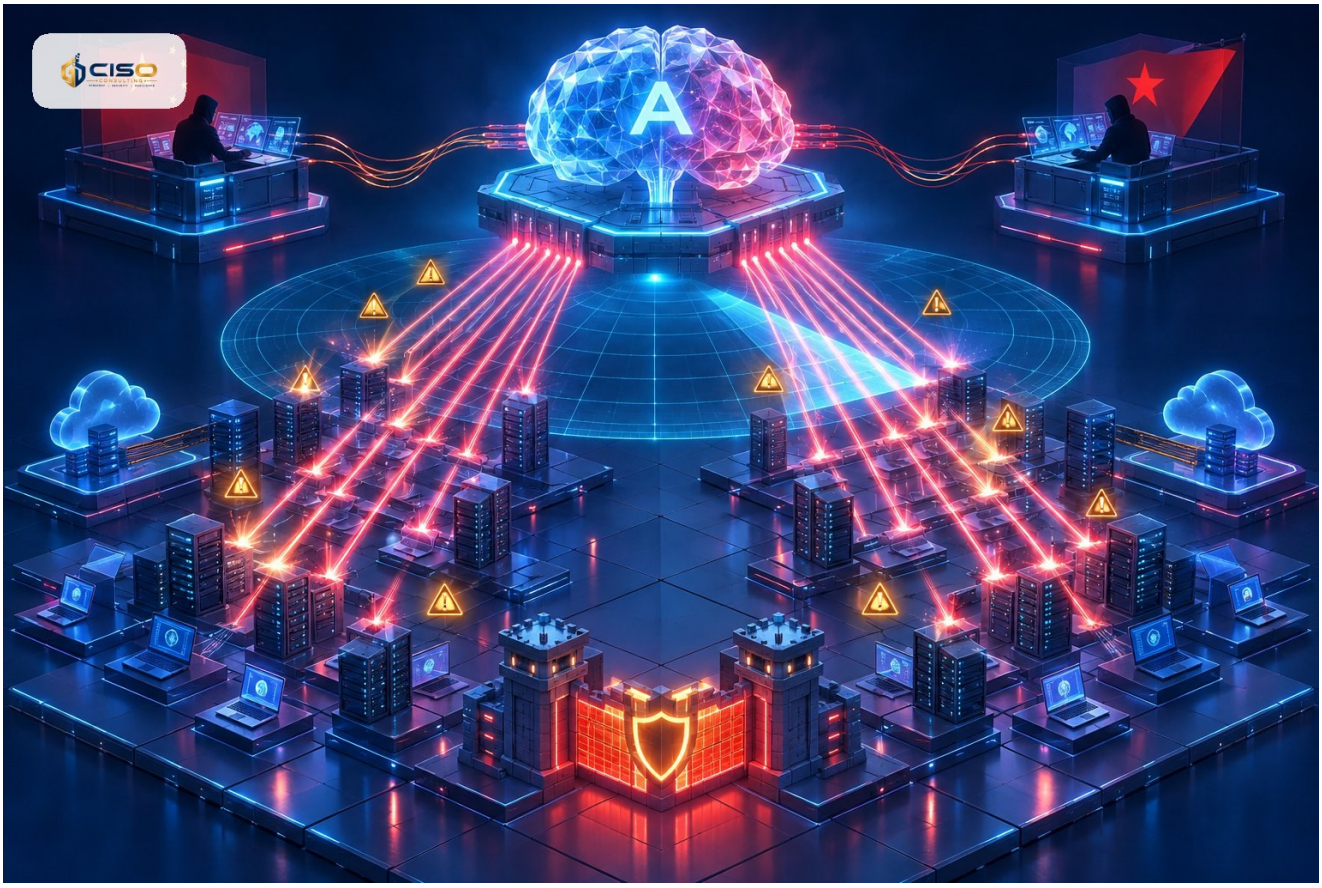
State-linked hackers adopt ARTEX AI pentest framework, Microsoft warns



Microsoft Threat Intelligence reports that China- and North Korea-linked groups now use ARTEX, an open-source LLM-driven pentest framework, to automate attacks. Its machine-speed behaviour is noisy and detectable.

- ARTEX is an open-source, LLM-driven pentest framework published on GitHub in July 2026; AI agents plan and execute steps toward an operator's goal.
- As of November 2026 Microsoft has seen state-sponsored and financially motivated actors, including Storm-0940, Onyx Sleet, Pearl Sleet, Crystal Typhoon and Salt Typhoon, integrating it.
- Observed campaigns searched public repositories for exposed secrets, enabled supply chain compromise and scanned internet-facing systems.
- One Storm-0940 password spraying run against Microsoft 365 logged over 151,000 failed sign-ins

> and reached privileged access in under three hours.
>
> - ARTEX adds no new techniques and is noisy by default, but operators can vary IP addresses and user agents to evade simple signatures.

Microsoft Threat Intelligence has warned that state-sponsored groups tied to China and North Korea have begun using ARTEX in attacks. ARTEX is an open-source penetration testing framework driven by large language models. The operator sets a goal, and AI agents plan and carry out the steps needed to reach it with little further input.

What Microsoft observed

As of November 2026, Microsoft has seen both state-sponsored and financially motivated actors integrating ARTEX, including Storm-0940, Storm-3358, Onyx Sleet, Pearl Sleet, Crystal Typhoon and Salt Typhoon. Reported campaigns searched public repositories for exposed secrets, enabled supply chain compromise and scanned internet-facing systems.

In one password spraying run against Microsoft 365, Storm-0940 logged more than 151,000 failed sign-ins, peaking at 2,900 per minute, and reached privileged access in under three hours. In another case, an AI agent went from searching GitHub for client secrets to taking data from Azure Key Vault in five minutes.

Detection still works

Microsoft stresses that ARTEX introduces no new techniques; it relies on common penetration testing tools. Attackers can change source IPs and user agent strings to defeat static or signature-based blocking, so indicator lists alone are weak. Behaviour is harder to hide: bursts of varied requests, rapid retries and machine-speed movement between stages stand out in logs. The UK National Cyber Security Centre reached a similar view on agentic frameworks in general, while cautioning that future tools may be built with stealth in mind.

The practical lesson is that attack speed is rising, so exposed secrets and weak authentication matter more, and detection should focus on behaviour.

What to do now

1. Scan your public and internal code repositories for exposed secrets and client credentials, and rotate any found.
2. Enforce MFA and conditional access on Microsoft 365 and Azure, and alert on high-volume failed sign-ins and password spraying patterns.
3. Restrict access to Azure Key Vault and review app credentials and permissions granted to third-party applications.
4. Tune detection to behaviour such as request bursts, rapid retries and fast stage-to-stage movement,

rather than relying only on IP or user agent indicators.

5. Review exposure of internet-facing systems and patch them promptly, and assess supply chain suppliers' access to your environment.