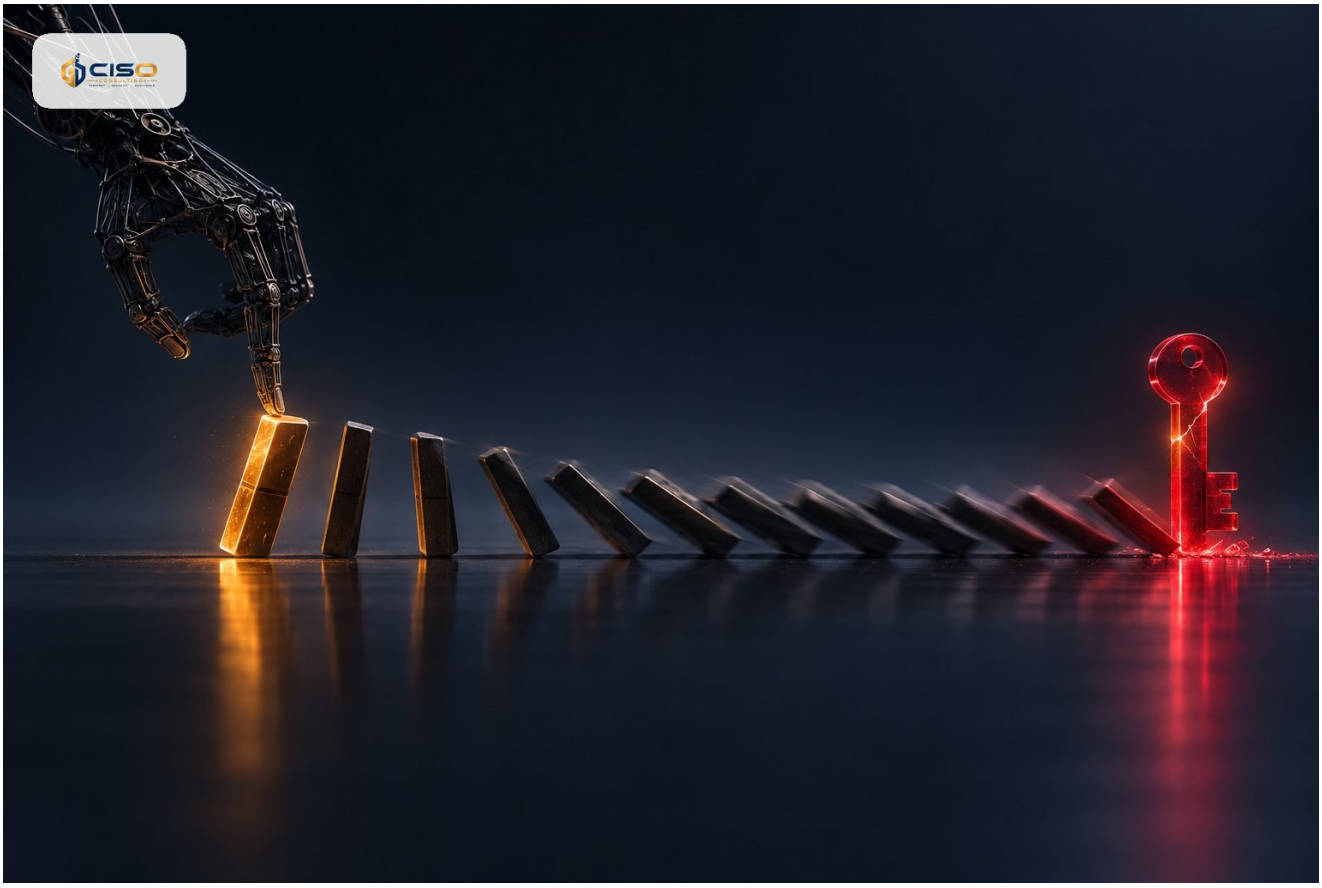
FBI warns that the ARTEX AI framework is automating attacks worldwide



The FBI says several threat actors have used the AI-driven ARTEX framework since August 2026 to speed up intrusions, in some cases reaching privileged access in under three hours. It has published indicators of compromise and defensive guidance.

- The FBI FLASH advisory says ARTEX has been used since at least August 2026 against financial, government, technology, defense and healthcare organizations, among others.
- ARTEX is an open-source framework written in Go that connects to external LLMs and directs AI agents to perform reconnaissance, exploitation, privilege escalation and data theft.
- Some intrusions reached privileged access in under three hours, and the tool is especially effective against overlooked systems such as partner portals, legacy services and third-party integrations.
- Reported cases include the ConnectWise Cloud Backup supply-chain attack on Microsoft 365

tenants, attacks on South Korean banks, and a campaign by Vapor Panda.

- The original repository was removed in October, but forks, archived copies and a commercial edition called ARTEX PRO remain available.

The FBI has issued a FLASH advisory warning that multiple threat actors are using ARTEX, an AI-powered penetration testing framework, to automate attacks against organizations in many sectors. The agency says abuse has been observed since at least August 2026.

What ARTEX does

ARTEX is an open-source framework written in Go. It does not ship its own AI model; it connects to external large language models, including Anthropic Claude, OpenAI GPT, DeepSeek, GLM, Grok and Kimi. Operators describe their goals, and specialized AI agents turn them into commands for reconnaissance, vulnerability discovery, exploitation, privilege escalation and data theft, with little human involvement.

The FBI notes that some intrusions moved from initial targeting to privileged access in under three hours, and that the tool lets less skilled actors run complex operations against several targets at once. It is particularly good at finding weaknesses in overlooked assets such as partner portals, employee applications, legacy services and third-party integrations.

Reported incidents and availability

The advisory references the October ConnectWise Cloud Backup supply-chain attack, in which compromised application identities were used to authenticate to Microsoft 365 customer tenants. Microsoft attributed the campaign to Storm-0940, which used ARTEX for reconnaissance, password spraying and abuse of cloud application permissions. It also cites attacks on South Korean banks that exposed data on about 67,000 people, and a CrowdStrike report on Vapor Panda targeting more than 200 organizations in 14 countries.

The developer removed the original GitHub repository on October 8, yet forks, archived copies, localized versions and a commercial edition, ARTEX PRO, remain available. Researchers had found more than 1,600 exposed ARTEX consoles by early November.

Defensive resources

The 13-page advisory lists indicators of compromise, though the FBI cautions that IP addresses may have changed. Researcher MalwareMustDie has released an open-source detection pack and a playbook that grades indicators by confidence.

What to do now

1. Inventory internet-facing applications, partner portals, legacy services and third-party integrations, and close or restrict any that are not needed.

2. Restrict access to cloud administration interfaces and review application permissions and grants in Microsoft 365 and other cloud tenants, especially for backup and other third-party apps.
3. Review authentication logs for password spraying, unexpected credential or privilege changes and unusual application sign-ins.
4. Apply rate limits to sensitive APIs and alert on bursts of automated requests and large data transfers.
5. Load the FBI indicators and the MalwareMustDie detection rules into monitoring tools, treating IP-based indicators as time-limited and checking for false positives.
6. Add AI-accelerated intrusion scenarios to incident response plans, given that defenders may have only hours to react.