

AI penetration testing tools exploited in South Korean banking attacks



A threat actor used ARTEX AI and Claude agents to breach multiple South Korean banks, exposing customer data and causing outages, prompting the developer to close-source the tool.

- Chinese-speaking attacker targeted Shinhan Bank, KB Kookmin Bank, and Hana Bank using ARTEX AI penetration testing suite and Claude agents
- Breaches exposed client personal data and credit card information, causing system outages at some institutions
- CrowdStrike traced the attack through open directories containing Claude session histories and ARTEX configuration files
- ARTEX developer made the project closed-source after confirming its use in real attacks, though derivatives remain available

- Attacker had no monetization plan and used AI tools to identify Telegram data-sales channels

Attack profile and impact

A threat actor launched coordinated attacks against multiple South Korean financial institutions earlier this month, exploiting **AI-powered penetration testing tools** to breach defenses. The campaign targeted Shinhan Bank, KB Kookmin Bank, and Hana Bank, resulting in the exposure of client personal data and credit card information. Some institutions experienced system outages during the incident. The South Korean government convened an emergency meeting and issued calls for immediate security measures across critical IT infrastructure.

Technical attribution and tooling

CrowdStrike confirmed the attacker used ARTEX AI, a formerly open-source agentic penetration testing suite developed in China, alongside Claude agents. Researchers discovered open directories containing Claude Code session histories, ARTEX configuration files, and Claude memory files that revealed the attack infrastructure. The ARTEX instance relied on DeepSeek v4.1-flash as its primary large language model backend, supplemented by GLM-5.3 and Grok 4.6 for additional Claude Code sessions. Evidence suggests the attacker accessed DeepSeek through an LLM API proxy or reseller.

The investigation uncovered that the attacker used the same AI tools to create a résumé, inadvertently exposing identification details, contact information, and a Telegram account. CrowdStrike assessed the threat actor may be a 26-year-old Chinese national who studied at the South China University of Technology and resides in Maoming, Guangdong. However, inconsistencies in the personal details—including an initial birth date listed as 2007—mean the identity cannot be reliably confirmed.

Tool availability and monetization intent

The records indicate the attacker had no predetermined plan to monetize the stolen banking data and consulted Claude to identify Telegram data-sales groups focused on Korea. Following confirmation that ARTEX had been weaponized in real-world attacks, the developer discontinued public updates and made the project closed-source. Nevertheless, English- and Korean-language derivatives of the current codebase remain available, sustaining the tool's accessibility to other threat actors.

What to do now

1. Review and strengthen credential management policies to prevent unauthorized access using valid credentials, which remain a primary attack vector
2. Assess exposure to AI-powered penetration testing tools by monitoring for unusual automated scanning or enumeration activity across critical systems
3. Implement enhanced monitoring for API access patterns, particularly connections to LLM proxies or

resellers that may indicate AI-assisted reconnaissance

4. Verify that security controls remain effective after initial access, as prevention rates drop significantly once attackers obtain valid credentials
5. Coordinate with threat intelligence providers to identify indicators of compromise associated with ARTEX derivatives and similar AI-assisted attack frameworks
6. Conduct tabletop exercises simulating AI-augmented attacks against banking infrastructure to test detection and response capabilities