GBBC **JUST THE FACTS**

Prepared November 17, 2026 · gbbc.io

GBBC is a non-profit focused on education, partnerships and standards for the blockchain and digital-assets community. GBBC does not lobby.

Autonomous AI-Powered Cyberattacks: ARTEX

AI is accelerating how attackers find and exploit existing security weaknesses

WHAT IS ARTEX?

An LLM-powered autonomous penetration-testing framework. Originally intended for security testing, it is being weaponized to automate reconnaissance, vulnerability exploitation, and other stages of cyberattacks

HOW ARE ATTACKERS USING EXISTING TOOLS?

CERT-In has identified ARTEX, PentAGI, Cairn and CyberStrikeAI in attacks targeting financial institutions

FIND	Exposed systems, APIs and credentials
EXPLOIT	Weaknesses in apps and cloud environments
DIVERT	Abuse legitimate payment APIs to transfer funds
SCALE	Automate attacks, including during holidays

HOW SHOULD BUSINESSES DEFEND?



PREVENT

Patch vulnerabilities, enforce MFA and least privilege, isolate testing from production



PROTECT FUNDS

Validate API transactions server-side; require dual approval and transaction limits



DETECT

Monitor cloud/API activity 24/7; flag suspicious small payments followed by large transfers

WHAT IF AN ATTACK SUCCEEDS?

CONTAIN

Isolate affected systems and suspend suspicious accounts

→

INVESTIGATE

Preserve logs, revoke credentials, and identify the source

→

RECOVER

Patch weaknesses, verify eradication, and restore services

WHAT SHOULD GOVERNMENTS DO?

Strengthen critical-infrastructure standards, coordinate threat-intelligence sharing, enforce incident reporting, and conduct cross-sector response exercises

KEY MESSAGE

Strong access controls, payment safeguards, and rapid incident response remain essential

Sources:

- FBI Overview: https://www.ic3.gov/CSA/2026/261113.pdf?
- CERT-In (CIAD-2026-0058): https://cert-in.org.in/s2cMainServlet?VLCODE=CIAD-2026-0058&pageid=PUBVLNOTES02&