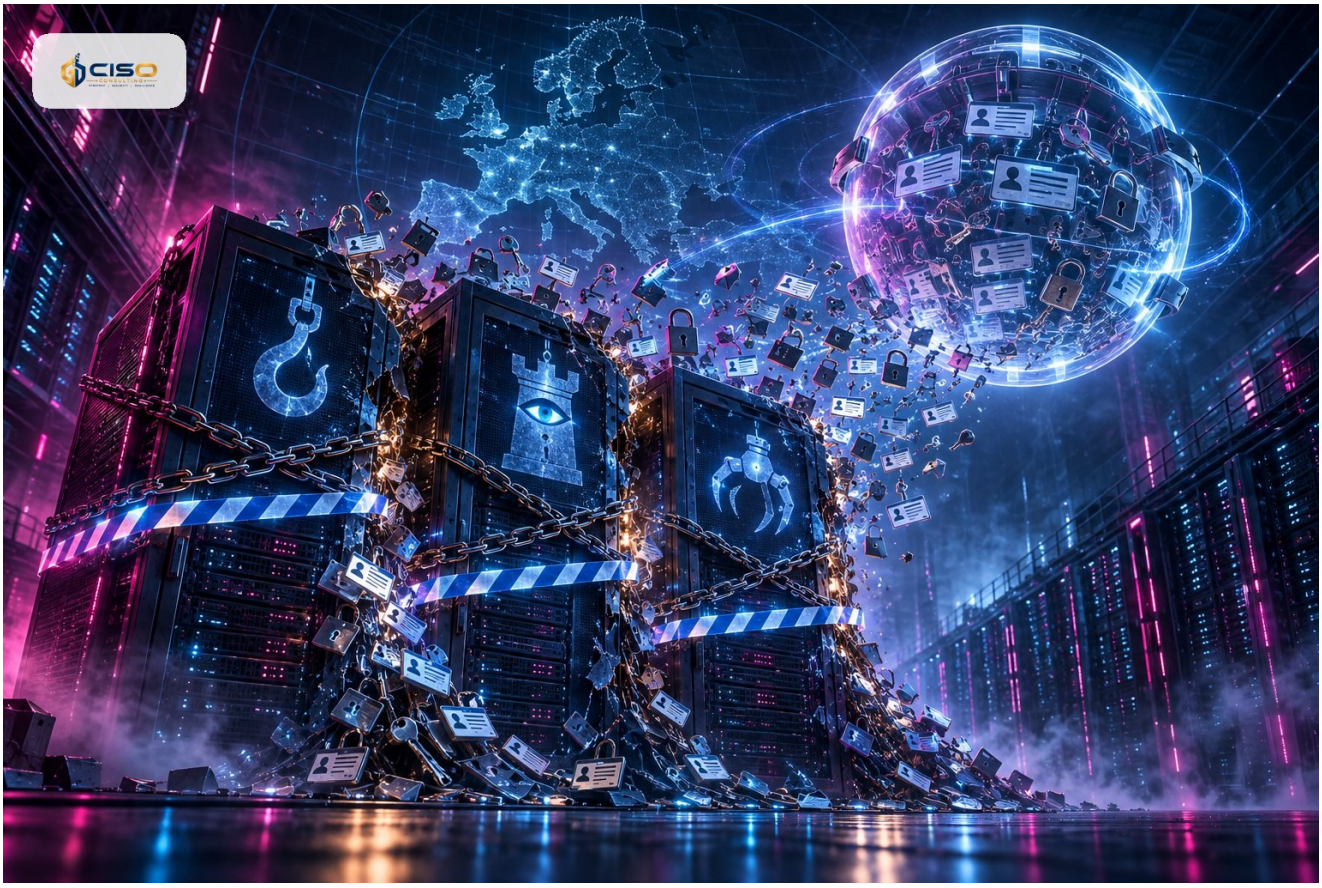
Operation Endgame Disrupts Gootloader, CastleRAT and StealC Servers



An international police operation took down servers behind three malware tools used for access, password theft and ransomware. Germany's BKA says about 6.4 million stolen logins from over 40,000 victims were seized.

- Servers behind Gootloader, CastleRAT and StealC were taken down in an international police operation.
- The tools were used to gain access to computers, steal passwords and launch ransomware attacks.
- About 6.4 million stolen logins were seized, belonging to more than 40,000 victims, per the BKA.
- Seized credentials may still be valid for affected accounts until they are reset.

An international police operation, reported this week under the name Operation Endgame, took down servers

behind three malware tools: Gootloader, CastleRAT and StealC. According to the report, criminals used these tools to gain access to computers, steal passwords and launch ransomware attacks.

What was seized

Germany's Federal Criminal Police Office (BKA) says police seized about 6.4 million stolen logins belonging to more than 40,000 victims. The source excerpt describes Gootloader as a loader but does not go further on the technical details of each tool, and it does not name affected organisations or countries.

What it means for institutions

A takedown disrupts the infrastructure behind these tools, but it does not by itself remove infections already present on endpoints, and it does not make previously stolen credentials safe. Where employee or customer logins were captured, the accounts remain exposed until passwords are changed and sessions are revoked.

Regulated institutions should treat this as a prompt to check for infostealer and loader activity, review credential hygiene, and confirm that incident response plans cover credential theft that precedes ransomware.

What to do now

1. Hunt on endpoints and in EDR/proxy logs for signs of Gootloader, CastleRAT and StealC activity.
2. Force password resets and revoke active sessions and tokens for accounts with suspected exposure.
3. Enforce multi-factor authentication on remote access, email and privileged accounts.
4. Check whether corporate credentials appear in available breach or stealer-log intelligence.
5. Confirm the incident response plan covers credential theft leading to ransomware, including escalation to NCA where required.