SpyCloud

2026 Cybercrime at-a-glance

A timeline of activity, research, and takedowns from the criminal underground this year

Takedowns and arrests | Breaches and extortion | New attacker tools

JAN

Malicious AI agent skills delivered Atomic Stealer, and stolen card data surfaced on Threads

FEB

Operation Red Card 2.0 made 651 arrests, and an exposed IDMerit database held about 875 million names

MAR

Tycoon 2FA and LeakBase fell, LeakBase's owner was arrested in Russia, and TeamPCP hit Cisco and the European Commission

APR

ShinyHunters took data from cloud accounts at Udemy and Vimeo, and SpyCloud parsed 6.38 billion unique Chinese PII records

MAY

ShinyHunters pushed ransom pop-ups to Canvas users during finals, and Kali365 faked its own shutdown

JUN

The Klue breach exposed Salesforce tokens, Operation Endgame hit StealC, and FortiBleed leaked 73,932 firewall logins

JUL

A fake ransomware group fooled security vendors, LeakBase returned, the Jalisco kit beat device code expiry, and Latin American breaches ran 2.9x the usual rate

AUG

Five forum accounts coordinated 15 leaks from one French SaaS platform

SEP

BlueKit introduced browser-in-the-middle phishing, EvilTokens fell, and ShinyHunters hijacked Cl0p's site as two of its members were arrested

AHEAD

2027 OUTLOOK