Daily Threat Intelligence Briefing

Today's threat briefing contains live links that connect you to the original source articles. You can see the real URL by hovering your mouse over the links and checking that they match the source articles. These links were taken straight from the website of the source article. Tyler Technologies has not checked these sites or links for security.

News from Wednesday January 28, 2026 (Reported on Thursday January 29, 2026)

Government

AI Use by CISA Chief Alarms Cyber Officials
Read more at GovInfoSecurity

States Put 'Unprecedented' Attention on AI's Role in Schools
Read more at Edweek.org

Financial Institutions

Social Engineering Hackers Target Okta Single Sign On
Read more at BankInfoSecurity

CFPB To Use Full Rulemaking Process For Section 1033 Rewrite
Read more at CUtoday

Memcyco Gets $37M to Fight AI-Powered Impersonation Attacks
Fraudtoday.io

Healthcare

'AI-Powered' Services Firm Says Hack Affects 3.1M
Read more at HealthcareInfoSecurity

Comstar to Pay State AGs $515,000 to Settle Alleged HIPAA Violations
Read more at TheHIPAAJournal

Other

eScan confirms update server breached to push malicious update
Read more at Bleeping Computer

New sandbox escape flaw exposes n8n instances to RCE attacks
Read more at Bleeping Computer

SolarWinds warns of critical Web Help Desk RCE, auth bypass flaws
Read more at Bleeping Computer

News from Wednesday January 28, 2026
(Reported on Thursday January 29, 2026)

Viral Moltbot AI assistant raises concerns over data security
Read more at Bleeping Computer

FBI seizes RAMP cybercrime forum used by ransomware gangs
Read more at Bleeping Computer

Empire cybercrime market owner pleads guilty to drug conspiracy
Read more at Bleeping Computer

AI Is Rewriting Compliance Controls and CISOs Must Take Notice
Read more at Bleeping Computer