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 July 22, 2026
(Reported on Thursday July 23, 2026)

Local Government

CISA orders urgent action on actively exploited Langflow RCE flaw | Vulnerability | Bleeping Computer

CISA directed federal agencies to immediately remediate an actively exploited remote code execution vulnerability affecting Langflow under its Known Exploited Vulnerabilities catalog.

Financial Institutions

EU Financial Institutions Leak Data Through Cookie Trackers | Data Breach | Dark Reading

Banking institutions in Europe and America unintentionally exposed customer information to advertising networks through website tracking technologies.

When Identity Verification Fails: Lessons from a Real-World SIM Swap and Near Account Takeover | Social Engineering | Security Week

Analysis of SIM swap attack exploiting weak identity verification processes highlights need for continuous authentication monitoring.

Healthcare

TriWest Healthcare Alliance Announced Breach Affecting Almost 12,000 Tricare Beneficiaries | Data Breach | HIPAA Journal

Healthcare contractor TriWest Healthcare Alliance disclosed unauthorized access compromising personal data of nearly 12,000 military health beneficiaries.

Clover Health Assessing Impact of Social Engineering Incident | Social Engineering | HIPAA Journal

Medicare Advantage insurer Clover Health reported a social engineering attack to SEC and is evaluating data exposure scope.

Other

Microsoft to stop Exchange 2016 / 2019 security updates in October | Vulnerability | Bleeping Computer

Extended security support ending for on-premises Exchange Server versions, requiring organizations to upgrade or migrate.

Flaws in Passkey Implementation Show Old Attacks Still Work | Vulnerability | Dark Reading

Security researchers discovered implementation weaknesses in Microsoft's passkey authentication that enable user impersonation attacks.

Chick-fil-A discloses data breach after credential stuffing attacks | Data Breach | Bleeping Computer

Chick-fil-A disclosed a data breach after attackers used credential stuffing attacks to access customer accounts using previously compromised usernames and passwords.

Attackers Are Learning to Live Off the AI Toolchain | Malware | Dark Reading

New malware variant exploits legitimate AI development tools to hide malicious operations within normal workflows.
