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 Tuesday September 01, 2026
(Reported on Wednesday September 02, 2026)

Local Government

FBI Probes Service Selling 153M+ Drivers Licenses | Data Breach | Krebs on Security

Dark web vendor is selling scans of over 153 million US and Canadian driver's licenses apparently stolen from an identity verification firm, prompting an FBI probe.

Financial Institutions

Financial Stability Board Sounds the Alarm Over Frontier AI Risks | Risk Advisory/Regulatory Warning | Infosecurity Magazine

Global financial regulator body warned G20 banking officials that advanced AI systems could introduce new cyberattack and financial stability risks.

Healthcare

Aesto Health says data breach affects over 9.5 million patients | Data Breach | Bleeping Computer

Aesto Health disclosed a data breach exposing sensitive information of more than 9.5 million patients.

Novocure data breach affects more than 1,400 cancer patients | Data Breach | Bleeping Computer

Cancer treatment company Novocure disclosed a cyberattack exposing personal data of over 1,400 patients and employees.

Other

Frontier AI used to help exploit flaws in key industrial devices | AI-Assisted Exploitation/ICS Vulnerability | Cybersecurity Dive

Research finds Anthropic's Claude AI model can assist attackers in crafting exploitation strategies against industrial PLCs used in water and other critical utilities.

Critical Langflow flaw exploited to steal OpenAI and AWS keys | Vulnerability/Remote Code Execution | Bleeping Computer

Attackers actively exploit an unauthenticated RCE flaw in the open-source Langflow AI framework to steal OpenAI, AWS, and other credentials.

Attackers Exploit Critical JFrog Artifactory Flaw to Mint Admin Tokens Days After Disclosure | Vulnerability/Authentication Bypass | The Hacker News

Hackers began exploiting a critical JFrog Artifactory authentication bypass flaw to create rogue admin tokens just days after its public disclosure.

Nearly 22,000 Microsoft Exchange servers vulnerable to hijack attacks | Vulnerability | Bleeping Computer

Roughly 22,000 internet-exposed Microsoft Exchange servers remain unpatched against a high-severity flaw enabling attackers to hijack all mailboxes.