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 August 18, 2026
(Reported on Wednesday August 19, 2026)

Local Government

CISA Weighs Outsourcing Its Cyber Software Buying | Federal Cybersecurity Procurement | BankInfoSecurity

CISA is exploring whether a contractor could manage more than 500 cybersecurity software procurements a year for civilian federal agencies, potentially totaling $6 billion over a decade.

Financial Institutions

One Attacker Has Scraped Both Salesforce and ServiceNow Portals Since 2025 | SaaS / Cloud Data Exposure | The Hacker News

Researchers linked a year-long campaign to a single server that has systematically scraped records from Salesforce and ServiceNow customer portals, including targets in banking, financial services, telecom, technology, and the public sector.

Healthcare

American Addiction Centers & Oculus Pathology Disclose Hacking Incidents | Data Breach / Unauthorized Access | HIPAA Journal

American Addiction Centers reported data theft from its Salesforce environment, while Oculus Pathology disclosed unauthorized access to employee email accounts that exposed personal, financial, and protected health information.

Other

Malicious SIM Cards Threaten IoT Cellular Modems | IoT / Cellular Security | GovInfoSecurity

Researchers found that malicious or compromised SIM cards can abuse modem AT-command interfaces to trigger code execution, denial-of-service, file access, and cellular downgrade attacks, with IoT modems appearing particularly exposed.

Perplexity Builds Guardrails to Rein in Rogue AI Agents | Agentic AI Security | BankInfoSecurity

Perplexity released Numbat, an open-source security tool that evaluates AI-agent actions against enterprise policies before execution and provides monitoring and forensic reconstruction capabilities.

Microsoft tests faster Windows File Explorer, new context menu | Windows / Product Update | BleepingComputer

Microsoft is testing File Explorer performance and reliability improvements alongside a redesigned Windows 11 context menu intended to reduce clutter and give users more customization options.

Microsoft starts removing WMIC tool used by cybercriminals | Windows Security / LOLBin Removal | BleepingComputer

Microsoft is removing the legacy WMIC command-line utility from newer Windows 11 installations and beta builds, eliminating a tool frequently abused by ransomware and malware to disable recovery and security protections.
