# 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 Thursday August 06, 2026**
**(Reported on Friday August 07, 2026)**

---

## Local Government

**Despite federal warnings, thousands of U.S. industrial controllers used in water systems remain exposed online** | Vulnerability | CyberScoop

*Security researchers found roughly 4,400 internet-exposed industrial controllers in US water systems, including 22 in previously attacked cities.*

**Hackers grow more willing to destroy, not just disrupt OT systems** | Vulnerability | Cybersecurity Dive

*Security researchers warn attackers increasingly aim to physically destroy industrial control systems rather than merely disrupt them.*

**The water sector just got it's wake-up call. Again.** | Vulnerability/Unpatched Systems | CyberScoop

*Op-ed analysis argues recent cyberattacks on water utilities across seven US states were avoidable due to unused existing security guidance.*

## Financial Institutions

**Hedge fund cyberattacks tied to BlackFile-linked UNC6671 extortion group** | Data Breach | Bleeping Computer

*Extortion group UNC6671, linked to BlackFile actors, is blamed for a wave of cyberattacks against hedge funds and private-equity firms.*

## Healthcare

**Unlimited Technology Systems Data Breach Affects 3.8 Million Patients** | Data Breach | HIPAA Journal

*Ohio-based revenue cycle management vendor Unlimited Technology Systems disclosed a breach exposing data of 3.8 million patients.*

**Possible cyber incident eyed as JPS Health Network in Texas remains in multiday downtime** | Unknown/Suspected Cyberattack | DysruptionHub

*JPS Health Network in Fort Worth faces multiday IT outage possibly tied to a cyberattack, disrupting operations and records access.*

## Other

**New TONTOU CPU attack bypasses Spectre v2 fixes, leaks Linux password hashes** | Vulnerability | Bleeping Computer

*Researchers unveil TONTOU, a new CPU side-channel attack that bypasses Spectre v2 mitigations to steal Linux password hashes and sensitive kernel data.*

**Cisco Patches 12 SD-WAN and IOS XE Flaws, Including Three 9.9 CVSS Score Bugs** | Vulnerability | The Hacker News

*Cisco released patches for a dozen Catalyst SD-WAN and IOS XE vulnerabilities, including three critical flaws rated 9.9 severity.*

**Zero-Click AI Browser Hacking: Claude and ChatGPT Atlas Hijacked via Emails, X Posts** | Vulnerability / Prompt Injection | Security Week

*Researchers found unpatched prompt-injection flaws letting emails and X posts hijack Anthropic's Claude and OpenAI's ChatGPT Atlas AI browsers without user clicks.*

**Ransom Cartel Creator Gets 16 Years in Prison for Operating Ransomware-as-a-Service** | Ransomware | The Hacker News

*A federal court sentenced the operator of the Ransom Cartel ransomware-as-a-service scheme to 16 years for attacks on at least 18 companies worldwide.*

---