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 November 19, 2025 (Reported on Thursday November 20, 2025)

Government

CISA Releases Guide to Mitigate Risks from Bulletproof Hosting Providers
Read more at Cisa.gov

US, Allies Sanction Russian Bulletproof Ransomware Host
Read more at GovInfoSecurity

CISA Adds One Known Exploited Vulnerability to Catalog
Read more at Cisa.gov

Financial Institutions

Misconfigured AI Agents Let Attacks Slip Past Controls
Read more at BankInfoSecurity

New Study: Nearly One-Third Of Fraud Victims Took No Protective Steps—Highlighting Member-Education Gaps
Read more at CUtoday.info

Healthcare

Feds, AHA Warn Health Sector of Evolving Akira Threat, Again
Read more at HealthInfoSecurity

Vendor Breaches Announced by Illinois and Virginia Healthcare Providers
Read more at TheHIPAAJournal

Other

W3 Total Cache WordPress plugin vulnerable to PHP command injection
Read more at Bleeping Computer

Sneaky2FA PhaaS kit now uses redteamers' Browser-in-the-Browser attack
Read more at Bleeping Computer

New WrtHug campaign hijacks thousands of end-of-life ASUS routers
Read more at Bleeping Computer

News from Wednesday November 19, 2025
(Reported on Thursday November 20, 2025)

The hidden risks in your DevOps stack data—and how to address them
Read more at Bleeping Computer

CISA gives govt agencies 7 days to patch new Fortinet flaw
Read more at Bleeping Computer

Meet ShinySp1d3r: New Ransomware-as-a-Service created by ShinyHunters
Read more at Bleeping Computer