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, June 10, 2026
(Reported on Thursday, June 11, 2026)

Government

China-linked JDY botnet expands targeting of U.S. military networks
Read more at Bleeping Computer

CISA tells agencies to patch smarter, not harder — foreshadowing broader industry practice
Read more at CSO Online

Financial Institutions

Credit Unions Back FCC Crackdown On Phone Number Resellers To Fight Fraud, Spoofing
Read more at CU Today

Healthcare

Cybersecurity Incidents Reported by Multiple Dental Practices
Read more at HIPAA Journal

Data Breaches Announced by Two Digestive Health Companies
Read more at HIPAA Journal

Other

Autonomous AI agents duped into leaking sensitive data in phishing test
Read more at CSO Online

Critical HVAC and UPS Vulnerabilities Could Let Hackers Disrupt Data Centers
Read more at Security Week

GitHub announces npm security changes to tackle supply-chain attacks
Read more at Bleeping Computer

Ivanti, Fortinet, and SAP Release Patches for Multiple Critical Vulnerabilities
Read more at The Hacker News

Microsoft patches Exchange Server zero-day exploited in attacks
Read more at Bleeping Computer

News from Wednesday, June 10, 2026
(Reported on Thursday, June 11, 2026)

Nightmare-Eclipse Drops Yet Another Microsoft Exploit, RoguePlanet
Read more at Dark Reading

Russian APTs Still Exploiting Patched WinRAR Flaw CVE-2025-8088
Read more at Security Affairs

Who Runs the Ransomware Group 'The Gentlemen?'
Read more at Krebs on Security