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 Monday, July 13, 2026 (Reported on Tuesday, July 14, 2026)

Government

The US government warns that Russia state hackers are coming after your router
Read more at Arstechnica

CISA warns of actively exploited RCE flaws in Joomla extensions
Read more at Bleeping Computer

St. Paul, Minn., Notifies People Affected by 2025 Cyber Attack
Read more at Govtech

Financial Institutions

Tokenomics: To Spend or Not to Spend
Read more at Bank Info Security

Healthcare

Marlboro-Chesterfield Pathology Agrees to Settle Lawsuit Over 2025 Ransomware Attack
Read more at HIPAA Journal

Bipartisan House Bill Pushes AI for Pediatric Cancer Care
Read more at Health Care Info Security

Other

New CrashStealer malware poses as Apple crash reporting tool
Read more at Bleeping Computer

Turning the Tables on Email Scammers With 'ScamBuster'
Read more at Dark Reading

Misconfigured Server Reveals Three Evilginx Phishing Operations Targeting Microsoft 365
Read more at The Hacker News

Japan's largest taxi operator shuts systems after cyberattack
Read more at Bleeping Computer

Forg365 PhaaS Targets Microsoft 365 with Device Code and AitM Session Theft

News from Monday, July 13, 2026
(Reported on Tuesday, July 14, 2026)

Read more at The Hacker News

Hackers blackmail Bosh as secret engineering files surface on the dark web
Read more at Cybernews

Lidl discloses online shop breach after service provider hack
Read more at Bleeping Computer

Attacker Uses Suspected AI-Generated PowerShell Script to Map Active Directory
Read more at The Hacker News

Progress warns ShareFile Users: shut down on-premises servers immediately
Read more at Cybernews

RabbitMQ flaws expose OAuth secrets, risk complete takeover of the broker
Read more at CSO Online