# 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, July 15, 2026 (Reported on Thursday, July 16, 2026)

### Government

**U.S. CISA adds SonicWall and Microsoft flaws to its Known Exploited Vulnerabilities catalog**
Read more at Security Affairs

**US charges alleged operators of Russian bulletproof hosting service**
Read more at Bleeping Computer

### Financial Institutions

**OkoBot Malware Framework Injects Seed Phrase Phishing Into Ledger and Trezor Apps**
Read more at The Hacker News

**IMF Warns Tokenized Finance Could Reshape Global Financial System**
Read more at CUtoday.info

### Healthcare

**Community Health Center of Buffalo & Greenbaum Rowe Smith & Davis Confirm Data Breaches**
Read more at HIPAA Journal

### Other

**AsyncAPI npm packages infected with credential-stealing malware**
Read more at Bleeping Computer

**Windows 0-day drops the same day Microsoft releases record number of patches**
Read more at Arstechnica

**Google Gemini CLI abused as a hacking agent, malware botnet operator**
Read more at Bleeping Computer

**Firefox, Chrome, Adobe, and VMware Updates Fix Multiple Critical Security Flaws**
Read more at The Hacker News

**Zoom warns of critical account takeover vulnerability**
Read more at Bleeping Computer

## News from Wednesday, July 15, 2026
## (Reported on Thursday, July 16, 2026)

**Threat actor impersonated hundreds of brands on GitHub to push infostealer malware**
Read more at Help Net Security

**Claude Flaw Automatically Sends Malicious Prompts to AI Agents**
Read more at Dark Reading

**ClickFix is changing the economics of social engineering**
Read more at Help Net Security

**New Windows Bind Link techniques let attackers evade EDR, security controls**
Read more at CSO Online