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 Friday May 16, 2025, through Sunday May 18, 2025
(Reported on Monday May 19, 2025)

Government

Former U.S. Govt Employees Targeted by Chinese Intelligence
Read more at GovInfoSecurity

No Fairy Tale Ending: PowerSchool's Hacker Targets Customers
Read more at Fraudtoday.info

Financial Institutions

Can Insurance Fraud Teams Handle Regulatory Scrutiny of AI?
Read more at BankInfoSecurity

Cryptohack Roundup: Celsius CEO's 12-Year Prison Sentence
Read more at CUtoday.info

US charges 12 more suspects linked to $230 million crypto theft
Read more at Bleeping Computer

Healthcare

Agentic AI Tech Firm Says Health Data Leak Affects 483,000
Read more at HealthcareInfoSecurity

Tri-City Cardiology Consultants & Northeast Georgia Health System Announce 21K+ Record Data Breaches
Read more at TheHIPAAJournal

Other

New 'Defendnot' tool tricks Windows into disabling Microsoft Defender
Read more at Bleeping Computer

Microsoft confirms May Windows 10 updates trigger BitLocker recovery
Read more at Bleeping Computer

Hackers exploit VMware ESXi, Microsoft SharePoint zero-days at Pwn2Own
Read more at Bleeping Computer

News from Friday May 16, 2025, through Sunday May 18, 2025
(Reported on Monday May 19, 2025)

Printer maker Procolored offered malware-laced drivers for months
Read more at [Bleeping Computer](#)

CISA tags recently patched Chrome bug as actively exploited
Read more at [Bleeping Computer](#)

Ransomware gangs increasingly use Skitnet post-exploitation malware
Read more at [Bleeping Computer](#)