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 April 21, 2025
(Reported on Tuesday April 22, 2025)

Government

Seeking Post-Mitre Management: What's Next for CVE Program?
Read more at GovInfoSecurity

Financial Institutions

Reborn: Cybercrime Marketplace Cracked Appears to Be Back
Read more at BankInfoSecurity

Debit Card Fraud Leads Financial Losses In 2024
Read more at CUtoday.info

Healthcare

Minnesota Dental Clinic Notifying 135,000 of 2024 Hack
Read more at HealthcareInfoSecurity

OCH Regional Medical Center Notifies 51,000 Patients About September 2023 Data Breach
Read more at TheHIPAAJournal

Other

In depth with Windows 11 Recall—and what Microsoft has (and hasn’t) fixed
Read more at Arstechnica

Microsoft Entra account lockouts caused by user token logging mishap
Read more at Bleeping Computer

It's 2025... so why are obviously malicious advertising URLs still going strong?, (Mon, Apr 21st)
Read more at SANS

White House plagued by Signal controversy as Pentagon in “full-blown meltdown”
Read more at Arstechnica

Healthcare Organizations Struggling to Shift from Reactive to Proactive Cybersecurity
Read more at HIPAAJournal

News from Monday April 21, 2025 (Reported on Tuesday April 22, 2025)

Kimsuky Exploits BlueKeep RDP Vulnerability to Breach Systems in South Korea and Japan
Read more at TheHackerNews