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 Cybersecurity has not checked these sites or links for security.

News from Wednesday, June 05, 2024
(Reported on Thursday, June 06, 2024)

Government

FBI recovers 7,000 LockBit keys, urges ransomware victims to reach out
Read more at Bleeping Computer

FBI Warns of Rise in Work-From-Home Scams
Read more at Information Security Magazine

Financial Institutions

SecurityScorecard Accuses Vendor of Stealing Trade Secrets
Read more at BankInfoSecurity

Healthcare

Rebranded Knight Ransomware Targeting Healthcare and Businesses Worldwide
Read more at TheHackerNews

Other

Advance Auto Parts stolen data for sale after Snowflake attack
Read more at Bleeping Computer

RansomHub Actors Exploit ZeroLogon Vuln in Recent Ransomware Attacks
Read more at DarkReading

Linux version of TargetCompany ransomware focuses on VMware ESXi
Read more at Bleeping Computer

83% of organizations faced at least one account takeover the past year
Read more at Security Magazine

Check-in terminals used by thousands of hotels leak guest info
Read more at Bleeping Computer

#Infosec2024: Organizations Urged to Adopt Safeguards Before AI Adoption
Read more at Information Security Magazine

Club Penguin fans breached Disney Confluence server, stole 2.5GB of data
Read more at Bleeping Computer

News from Wednesday, June 05, 2024
(Reported on Thursday, June 06, 2024)

Zyxel Releases Patches for Firmware Vulnerabilities in EoL NAS Models
Read more at TheHackerNews

Celebrity TikTok Accounts Compromised Using Zero-Click Attack via DMs
Read more at TheHackerNews