

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 April 3, 2026 through Sunday April 5, 2026
(Reported on Monday April 6, 2026)**

Government

White House sets \$75.7B topline IT budget for fiscal 2027

Read more at [FedScoop](#)

Financial Institutions

One-Time Passcodes Are Gateway for Financial Fraud Attacks

Read more at [BankInfoSecurity](#)

Healthcare

Telehealth Giant Him & Hers Announces Data Breach

Read more at [HIPAAJournal](#)

Other

\$285 Million Drift Hack Traced to Six-Month DPRK Social Engineering Operation

Read more at [TheHackerNews](#)

CBP facility codes sure seem to have leaked via online flashcards

Read more at [Arstechnica](#)

Hackers exploit React2Shell in automated credential theft campaign

Read more at [Bleeping Computer](#)

Germany Doxes "UNKN," Head of RU Ransomware Gangs REvil, GandCrab

Read more at [KrebsOnSecurity](#)

Fortinet Patches Actively Exploited CVE-2026-35616 in FortiClient EMS

Read more at [TheHackerNews](#)

Why Third-Party Risk Is the Biggest Gap in Your Clients' Security Posture

Read more at [TheHackerNews](#)

Critical ShareFile Flaws Lead to Unauthenticated RCE

Read more at [SecurityWeek](#)



**News from Friday April 3, 2026 through Sunday April 5, 2026
(Reported on Monday April 6, 2026)**

Inconsistent Privacy Labels Don't Tell Users What They Are Getting

Read more at [DarkReading](#)

TeamPCP Supply Chain Campaign: Update 006 - CERT-EU Confirms European Commission Cloud Breach, Sportradar Details Emerge, and Mandiant Quantifies Campaign at 1,000+ SaaS Environments

Read more at [SANS](#)

New Phishing Platform Used in Credential Theft Campaigns Against C-Suite Execs

Read more at [InfoSecurityMagazine](#)

LinkedIn Hidden Code Secretly Searches Your Browser for Installed Extensions

Read more at [CyberSecurityNews](#)

