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 March 30, 2026
(Reported on Tuesday March 31, 2026)

Government

Permitting Scammers Target Residents in Plainfield, Conn.
Read more at Govtech

Financial Institutions

Lloyds exposed nearly half a million customers' data in banking app glitch
Read more at Cybernews

Healthcare

Cloud-Based EHR Vendor Notifies SEC About Hacking Incident
Read more at HealthCareInfoSecurity

Woodfords Family Services Notifies Patients Affected by April 2024 Ransomware Attack
Read more at HIPAAJournal

Other

Apple adds macOS Terminal warning to block ClickFix attacks
Read more at Bleeping Computer

Critical Fortinet FortiClient EMS bug under active attack (CVE-2026-21643)
Read more at HelpNetSecurity

Hackers exploiting critical F5 BIG-IP flaw in attacks, patch now
Read more at Bleeping Computer

AI-Powered 'DeepLoad' Malware Steals Credentials, Evades Detection
Read more at DarkReading

New RoadK1ll WebSocket implant used to pivot on breached networks
Read more at Bleeping Computer

Zero-click vulnerability afflicts Telegram, allows full device takeover through animated stickers
Read more at Cybernews

News from Monday March 30, 2026
(Reported on Tuesday March 31, 2026)

OpenAI Patches ChatGPT Data Exfiltration Flaw and Codex GitHub Token Vulnerability
Read more at TheHackerNews

Researchers warn that macOS users face browser credential-stealing attack
Read more at Cybernews

European Commission confirms data breach after Europa.eu hack
Read more at Bleeping Computer