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 Thursday July 16, 2026
(Reported on Friday July 17, 2026)

Local Government

CISA urges immediate action on actively exploited Fortinet flaws | Vulnerability | BleepingComputer

Federal cybersecurity agency mandates emergency patching of two security flaws in Fortinet sandbox products under active attack.

CISA orders feds to patch actively exploited Oracle flaw by Saturday | Vulnerability | BleepingComputer

Federal agencies given weekend deadline to remediate critical Oracle E-Business Suite flaw under active exploitation.

Financial Institutions

Inside the Search for "Clean" Residential Proxies for Carding | Fraud/Carding | BleepingComputer

Cybercriminals evolve carding tactics by combining clean residential proxies with browser fingerprints to bypass fraud detection systems.

New OkoBot framework deploys 20 payloads to steal data, crypto | Malware | BleepingComputer

Malicious framework distributes multiple payloads targeting cryptocurrency wallets and credential theft across organizations.

Healthcare

23andMe to pay $18 million in new genetics data breach settlement | Data Breach | BleepingComputer

Genetic testing firm settles with state attorneys general for $18M following failure to adequately safeguard sensitive customer DNA information.

All About Women's Care Data Breach Affects Up to 12,000 Patients | Data Breach | HIPAA Journal

Colorado women's healthcare provider compromised patient information belonging to approximately 12,000 individuals.

Other

New Windows LegacyHive zero-day gives hackers admin privileges | Zero-Day | BleepingComputer

Publicly disclosed Windows privilege escalation flaw enables attackers to gain admin rights on fully patched systems.

Fresh SharePoint Vulnerability Exploited Soon After Disclosure | Vulnerability | Security Week

Attackers actively exploiting critical SharePoint server flaw enabling remote code execution shortly after public disclosure.

Windows Server 2022 reach end of mainstream support in 90 days | Vulnerability | BleepingComputer

Microsoft's Server 2022 platform transitions to extended support phase in October, requiring organizations to plan upgrade paths.

The Gentlemen Overtakes Qilin as Most Prolific Ransomware Threat | Ransomware | Infosecurity Magazine

New ransomware group called The Gentlemen has surpassed Qilin to become the most active threat actor targeting organizations.