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 Wednesday November 18, 2026
(Reported on Thursday November 19, 2026)

Financial Institutions

Coinbase blocks $4.7 million in transfers to Elon Musk deepfake scam | Social Engineering / Deepfake Scam | Bleeping Computer

Coinbase intercepted $4.7 million in crypto transfers after scammers used an AI deepfake of Elon Musk during a fake Tesla livestream giveaway.

Other

AI unearths 'internet breaker' flaws in Nginx web server | Vulnerability | CSO Online

Security researchers used AI agents to uncover critical unauthenticated remote-code-execution flaws in Nginx that had persisted undetected for over a decade.

Microsoft's Agent Framework PyPI package compromised to steal credentials | Supply Chain | Bleeping Computer

Attackers published malicious versions of Microsoft's Agent Framework PyPI package to harvest developers' cloud credentials and sensitive data.

Russian COLD RELIC Hackers Use Stolen Google Workspace Data to Breach Second U.S. Organization | Cloud Account Compromise / Supply Chain | The Hacker News

Russian state-linked group Cold Relic (formerly COLDRIVER) pivoted from a stolen Google Workspace cloud compromise to breach a second U.S. organization in a chained espionage campaign.

Apache warns of Roller RCE vulnerability exploited in attacks | Vulnerability | Bleeping Computer

Apache patched a critical remote code execution flaw in its Roller blogging software after attackers were found exploiting it in active attacks.

F5 Warns 6 Critical BIG-IP Flaws Can Crash Traffic in Specific Setups, May Allow RCE | Vulnerability | The Hacker News

F5 disclosed six critical BIG-IP vulnerabilities letting unauthenticated attackers crash core traffic processing and potentially execute remote code in specific configurations.

Russian Espionage Actor Star Blizzard Focuses on Cloud Identities for Mass Data Theft | Social Engineering / Cloud Account Compromise | Infosecurity Magazine

Google reports Russian state-linked group Star Blizzard shifting tactics to compromise cloud accounts for espionage and mass data theft.

New Attack Bypasses TPM Lockout to Crack Windows Hello and BitLocker PINs in Days, Not Years | Vulnerability | The Hacker News

Researchers found a hardware flash-chip attack that resets TPM lockout on some AMD and Intel PCs, enabling brute-force cracking of Windows Hello and BitLocker PINs.

The forced audit: how AuditTeam's OpsAgent framework masks ransomware as consulting | Ransomware | Securelist

Researchers detail a ransomware group that disguises its Rust-based OpsAgent malware and extortion scheme as a legitimate corporate audit service.

UAT-12643: Suspected North Korea-aligned actor blends blockchain resilience with targeted infostealing | Malware | Cisco Talos Blog

Cisco Talos identifies a financially motivated, suspected North Korea-linked group using blockchain-resilient infrastructure to deploy targeted infostealing malware.

Suspected Chinese APT Rebuilds EggStreme Malware After Exposure | Malware | Infosecurity Magazine

Chinese state-linked hacking group redeveloped the EggStreme malware toolkit and infrastructure after researchers exposed earlier versions.
