Daily Intelligence Update | 29 October 2025

Researchers reported that TransparentTribe, also tracked as APT36, conducted a cyber espionage campaign targeting Indian government and military organizations, specifically those operating on the Bharat Operating System Solutions (BOSS) Linux distribution. The operation, believed to advance Pakistan's strategic intelligence objectives, followed a multi-stage attack sequence beginning with phishing emails that delivered malicious ZIP archives containing deceptive ".desktop" files. These executed Bash one-liners to deploy DeskRAT, a Golang-based remote access trojan designed to establish persistence and exfiltrate targeted file types. In a parallel campaign, the APT group SideWinder was observed conducting multi-wave espionage operations against diplomatic and government institutions across South Asia, including India, Sri Lanka, Pakistan, and Bangladesh. This campaign used tailored geopolitical lures and phishing emails with weaponized PDF documents that prompted execution of a malicious ClickOnce application, ultimately delivering custom malware strains ModuleInstaller and StealerBot to enable surveillance and data theft.

Outside of state-sponsored espionage activity, multiple organizations disclosed significant data breaches. Toys "R" Us Canada reported that on July 30, 2025 it discovered an unauthorized third party had copied customer records from its database, after the information appeared on what the company referred to as the "unindexed internet." The exposed data included customer names, addresses, email addresses, and phone numbers, though no financial details or passwords were involved. Separately, Sotheby's confirmed that a cybersecurity incident first detected on July 24, 2025 led to unauthorized access to internal systems, exposing sensitive employee data. According to a filing with the Maine Attorney General's Office, the breach compromised financial account information, Social Security Numbers, and full names of staff, though client data remained unaffected. The company emphasized that law enforcement and external specialists were engaged to contain the incident and investigate the scope of compromise.
