TOP ATTACKS AND BREACHES

- A data breach has exposed 500GB of Indian biometric data, affecting Indian police, military personnel, and other public workers during elections in India. The leak stemmed from unsecured databases managed by ThoughtGreen Technologies and Timing Technologies, comprising sensitive information like fingerprints and facial scans. The leaked data was particularly sensitive as it can allegedly be used to manipulate the biometric systems used during Indian elections.
- Western Sydney University suffered a data breach leading to unauthorized access to personal details of students, including names, addresses, and contact numbers. The breach was detected during routine security checks, prompting security enhancements and notification to the affected individuals.
- New York's Albany County officials are investigating a possible cybersecurity breach detected just before the Memorial Day weekend. The county's Executive, Daniel McCoy, mentioned that there has been no evidence of data exfiltration. The incident has prompted collaboration with the state's Division of Homeland Security and Emergency Services Cyber Incident Response Team.
- $22 million in cryptocurrency was stolen from Gala Games due to unauthorized access that enabled the minting and selling of 600 million GALA coins. The breach was swiftly identified, and security measures were reinforced to prevent future incidents.
- PC Tattletale, a spyware application, suffered a security breach resulting in its website being defaced and its source code and database leaked. The attackers managed to alter the content of the website, showcasing their capabilities and potentially compromising user data stored by the spyware app.
- OmniVision Technologies have disclosed a data breach following a ransomware attack by the Cactus Ransomware group in 2023. The breach involved unauthorized access to various types of sensitive data, which according to the Cactus group include passport scans, contracts, and confidential documents. OmniVision has warned that the incident could have exposed sensitive information.
- An Indian citizen admitted guilt in a wire fraud conspiracy involving over $37 million stolen through a spoofed Coinbase Pro website. This scheme tricked victims into entering credentials on a fake site, enabling unauthorized access to real accounts and subsequent cryptocurrency theft.
- Cencora, a prominent provider in the pharmaceutical sector, recently confirmed a significant data breach. This incident led to the unauthorized access of sensitive patient information from 11 major drug companies, exposing personal data across multiple states.

VULNERABILITIES AND PATCHES

- Google has patched a Chrome zero-day vulnerability, CVE-2024-5274, a high-severity type confusion flaw in Chrome's V8 JavaScript engine. Discovered by Google's internal team, this vulnerability had been exploited in the wild, prompting an urgent security update to mitigate potential arbitrary code execution risks.
- Recent updates in GitLab have addressed multiple critical vulnerabilities that could lead to unauthorized account takeovers. The most severe issue, CVE-2024-4024, involved an OAuth authentication flaw with Bitbucket, allowing attackers to potentially hijack GitLab accounts. The flaws, also including CVE-2024-2434 and CVE-2024-2829, were patched in updated versions.
- Veeam disclosed a critical vulnerability, CVE-2024-29849, which allows unauthenticated threat actors to log into Veeam Backup Enterprise Manager as any user. This authentication bypass poses a significant risk, with a CVSS score of 9.8.

THREAT INTELLIGENCE REPORTS

- Check Point Research has uncovered an ongoing cyber espionage campaign focusing on targeting governmental organizations in Africa and the Caribbean. Attributed to Chinese threat actor Sharp Dragon, the campaign adopts Cobalt Strike Beacon as the payload, enabling backdoor functionalities like C2 communication and command execution while minimizing the exposure of their custom tools. This refined approach suggests a deeper understanding of their targets.
- Check Point Research has revealed the activities of Void Manticore, an Iranian threat actor affiliated with the Ministry of Intelligence and Security (MOIS). This threat actor has garnered attention for its involvement in destructive wiping attacks, often coupled with influence operations. Notably, Void Manticore has adopted various online personas to carry out its operations, with the most prominent ones being “Homeland Justice” for attacks in Albania and “Karma” for operations targeting Israel. The actor works in close cooperation with espionage focused Iranian threat actor Scarred Manticore.
- Researchers report on the emergence of Embargo ransomware, developed in Rust, which employs double extortion tactics and has so far listed 4 victims. The ransomware's technical analysis reveals its use of ChaCha20 and Curve25519 encryption, along with targeted termination of processes and services. Embargo's evolution signifies a shift towards more sophisticated and cross-platform ransomware.
- Security researchers have identified a new threat actor, dubbed Unfading Sea Haze, targeting entities in the South China Sea. This group focuses on geopolitical intelligence gathering, aligned with Chinese interests. Their methods include spear-phishing and exploiting vulnerabilities in network infrastructure to establish long-term presence with known malware like Gh0st RAT.