CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The University of Nottingham, a UK research university, has suffered a data breach after ShinyHunters accessed its student records system. The incident affected about 454,600 current and former students and exposed contact details, passport numbers, enrollment information, and fee payment records later appeared online. According to analysts, this breach is part of a larger wave of attacks targeting more than 100 organizations by ShinyHunters, exploiting CVE-2026-35273, a critical zero-day vulnerability in Oracle PeopleSoft that allows remote code execution.

  Check Point IPS provides protection against this threat *(Oracle PeopleSoft Enterprise PeopleTools Server-Side Request Forgery (CVE-2026-35273))*

- Mackay Sugar, Australia's second-largest sugar producer, has been hit by a cyberattack that disrupted operations and shut down its Farleigh and Racecourse mills in Queensland. The company instructed growers to stop harvesting and suspended cane haulage while temporary measures were deployed to maintain essential operations.

- Danish pharmaceutical giant Novo Nordisk has disclosed a breach after attackers accessed internal IT systems and copied pseudonymized clinical trial data from research systems. The exposed information included patient IDs, trial participation details, limited health data, and some healthcare professionals' contact information.

AI THREATS

- Check Point Research has demonstrated exploitable flaws in LangGraph, an open-source framework for stateful AI agents. Researchers chained SQL injection and unsafe deserialization issues to achieve remote code execution, with patches issued for SQLite, core, and Redis checkpointer components in affected deployments.

  Check Point IPS provides protection against this threat *(LangChain LangGraph SQL Injection (CVE-2026-27022))*

- Researchers highlighted a China-based phishing-as-a-service network, Outsider, that allegedly used Gemini to generate fake websites and support SMS phishing campaigns. Google filed a lawsuit after linking the operation to thousands of phishing sites, more than 1.5 million URLs, and large-scale victim targeting.

- Researchers warned that prompt-injection attacks against Anthropic's Claude Code GitHub Action could leak CI/CD workflow secrets. Malicious issue or pull request text can instruct the agent to read environment variables and expose API keys, enabling workflow abuse and impersonation inside software repositories.

VULNERABILITIES AND PATCHES

- Check Point Research has identified active exploitation of CVE-2026-50751, a critical authentication bypass vulnerability affecting Check Point Remote Access VPN and Mobile Access deployments configured to use the deprecated IKEv1 key exchange protocol. Attacks began in May and increased in early June, affecting a limited number of organizations, with one case tied to Qilin ransomware activity.

  Check Point IPS provides protection against this threat *(IKEv1 Remote Access Authentication Bypass PoC Exploit (CVE-2026-50751))*

- Microsoft released its largest Patch Tuesday update to date, addressing more than 200 Windows and Defender vulnerabilities amid an AI-driven surge in vulnerability discovery. The fixes include CVE-2026-45657, a critical Windows flaw with a CVSS score of 9.8 that could enable network-based propagation, CVE-2026-41091, which has been actively exploited to gain full system control, and CVE-2026-50507, a BitLocker bypass vulnerability.

- Veeam has released security updates to fix a critical flaw affecting Backup & Replication. The vulnerability allows an authenticated domain user to execute code remotely on a domain-joined backup server, exposing sensitive backup infrastructure and recovery systems.

THREAT INTELLIGENCE REPORTS

- Check Point Research's May 2026 attack trends report found that organizations experienced an average of 2,055 weekly attacks, down 7% month over month, while ransomware incidents increased 48% year over year. The report also highlights continued GenAI exposure across enterprise environments, including risks linked to business-related prompts.

- Researchers detected a supply-chain compromise in the Arch User Repository, where attackers seized hundreds of packages and modified build scripts to install credential-stealing malware. The campaign deployed malicious dependencies, a Rust stealer, and, with administrative privileges, an eBPF rootkit on Linux systems.

- Researchers analyzed a Brazilian phishing campaign abusing the legitimate NinjaOne remote management agent to gain access to company computers. The campaign uses fake Portuguese business portals and phone-based social engineering to install a signed agent connected to attacker-controlled infrastructure on victim endpoints

- Researchers described ongoing exploitation of WinRAR flaw CVE-2025-8088 by Russia-linked groups targeting Ukrainian military and government organizations. Spear-phishing archives plant hidden files that run at login and deploy stealers for browser passwords, cookies, VPN configurations, and other credentials across affected Windows systems.