CHECK POINT RESEARCH

# WEEKLY INTELLIGENCE REPORT

## TOP ATTACKS AND BREACHES

- Thomson Reuters, a global information and technology company, has disclosed a breach of its C-Track court case-management platform affecting courts across 11 US states and Canada. An unauthorized party obtained C-Track files containing court records, including names and other personal information.
- Hit, a major Slovenian gambling and tourism operator, has sustained a cyberattack that forced six casinos to close for about three days. Operations have resumed, but some table games, bingo, loyalty services, cash registers, and hotel systems remained unavailable during restoration, while some employees were temporarily furloughed.
- Baylor Genetics, a US clinical diagnostic laboratory, has disclosed a data breach affecting 2.8M patients and employees after unauthorized access to part of its IT environment in June. Stolen data included names, birth dates, medical testing and laboratory results, health insurance information, and some Social Security numbers.
- Global cloud storage provider Dropbox has disclosed unauthorized access to about 5,000 accounts after attackers exploited Lenovo's email verification process. Fraudulent Lenovo IDs created with victims' email addresses enabled access without Dropbox passwords, while files were viewed or downloaded from affected accounts.

## AI THREATS

- Researchers have detailed an AI-assisted ransomware intrusion that compromised an enterprise network in under 10 hours. Autonomous agents mapped internal systems, mined code repositories, obtained root credentials from a secrets manager, and abused build pipelines and cloud resources, compressing activity that normally requires substantially more human effort.
- Security researchers have disclosed GitSpawn, a vulnerability class affecting AI coding agents including Claude Code, Codex, Cursor, Goose, Qwen Code, Grok Build, and Hermes. Malicious repository Git configurations can trigger arbitrary code execution as the developer when agents automatically gather project context, in some cases before trust prompts.
- Researchers have showcased how an AI coding assistant can be used to port a known PLC exploit to a different controller model, producing working payloads after guided analysis. While the process still required significant manual effort, it demonstrated how AI can accelerate exploit development for industrial systems.

## VULNERABILITIES AND PATCHES

- SonicWall has addressed CVE-2026-83548 and CVE-2026-83549, critical vulnerabilities affecting SMA 1000 remote access gateways. CVE-2026-83548 is a pre-authentication SSRF flaw rated CVSS 10.0, while CVE-2026-83549 enables post-authentication remote code execution. Both were exploited as zero-days and affect SMA 6210, 7210, and 8200v appliances.

- JFrog has addressed CVE-2026-82329, a critical CVSS 9.8 authentication bypass affecting self-hosted Artifactory deployments. The flaw allows unauthenticated attackers to obtain administrator access tokens and take control of repositories. Exploitation was observed shortly after disclosure against internet-exposed systems, while JFrog Cloud environments were patched by the vendor.

  *Check Point IPS provides protection against this threat* *(JFrog Artifactory Authentication Bypass (CVE-2026-82329))*

- Security researcher have unveiled FalconFlank, a zero-day privilege escalation technique affecting CrowdStrike Falcon on Windows 11 25H2 and Windows Server 2025. The proof-of-concept abuses Falcon's Microsoft Office macro-removal remediation behavior, allowing a low-privileged local user to obtain elevated access on affected systems.

## THREAT INTELLIGENCE REPORTS

- Check Point Research has uncovered a Chinese-speaking cybercrime cluster, dubbed Gambling Goblin, that compromises Brazilian government and education websites. The group installs malicious Apache modules to proxy visitors to gambling and phishing pages while manipulating search rankings. Its infrastructure spans multiple languages and shows links to Earth Berberoka.

  *Check Point Threat Emulation and Harmony Endpoint provide protection against this threat*

- Check Point Research has analyzed JSCeal, a cryptocurrency-focused information stealer compiled into V8 bytecode and executed through a bundled Node.js runtime. Researchers developed a static deobfuscation pipeline that recovered readable code, revealing keylogging, browser credential theft, HTTPS interception, additional encryption, and newer variants targeting macOS systems.

  *Check Point Threat Emulation and Harmony Endpoint provide protection against this threat*

- Researchers have mapped a campaign by Iran-linked Mirage Kitten that uses fake LinkedIn coding tests to deliver NodeRabbit and PollCat malware. The malicious tests are distributed through cloud links and install cross-platform implants. Targets include fintech and aviation organizations in Egypt, Ethiopia, and Afghanistan.

- Researchers have analyzed new macOS delivery activity linked to North Korea's Contagious Interview campaign. Attackers use fake job interviews and trojanized disk images or installer packages impersonating legitimate Mac applications. The samples connect to infrastructure previously associated with malicious Git hooks and VS Code task files.