

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Carnival Corporation, a global cruise line operator, has [confirmed](#) a data breach affecting nearly 6 million people after attackers used social engineering to compromise an employee account. Exposed information may include names, contact details, dates of birth, and government identification numbers.
- Charter Communications, a US telecommunications provider operating under the Spectrum brand, has [suffered](#) a data breach by ShinyHunters group. Analysts report that 4.9 million email addresses were exposed, with names, phone numbers, physical addresses, and a subset of employee directory records.
- Lithuania's Centre of Registers, the state agency responsible for property and legal entity records, has [disclosed](#) a data breach affecting more than 600,000 records. Attackers reportedly misused institutional login credentials to access names, dates of birth, national identification numbers, and property-related data.
- Station Casinos, a major Las Vegas casino operator owned by Red Rock Resorts, has [disclosed](#) a breach after an unauthorized third party accessed a single employee account and associated files. The company began notifying affected individuals on May 21 and said business operations were not affected.

AI THREATS

- Researchers [profiled](#) GREYVIBE, a Russia-aligned group using ChatGPT and Google Gemini to accelerate phishing, malware development, and post-compromise activity against Ukrainian targets. The campaign uses spear-phishing, fake CAPTCHA pages, and decoy websites to deliver PhantomRelay on Windows and FallSpy on Android.
- Researchers [unveiled](#) an AI-driven influence and fraud campaign run by a Russian-speaking actor behind a MAGA-themed Telegram channel with 17,000 subscribers. The operator bypassed Gemini safeguards to automate propaganda and credential theft, used stolen API keys, cracked WordPress accounts, and drained a crypto wallet.
- Researchers [identified](#) an AI-generated malicious npm package, mouse5212-super-formatter, that steals developers' files by scanning a local directory and uploading data to a GitHub repository using a hardcoded private token. The package recorded at least seven exfiltration events and 676 downloads.

VULNERABILITIES AND PATCHES

- Check Point [announced](#) a Jumbo Security Release based on large-scale AI-driven code scanning across the products. The release addresses vulnerabilities in Check Point security gateways, including CVE-2026-48131 and CVE-2026-48132. The vulnerabilities were not exploited in the wild.

Check Point IPS provides protection against these threats (IKE Unsigned Underflow (CVE-2026-48131) IKE Improper Length Validation (CVE-2026-48132))

- CVE-2026-0257, a PAN-OS GlobalProtect authentication bypass which was fixed earlier this month, is now being [exploited](#) against unpatched Palo Alto Networks devices. Attackers are using forged authentication override cookies to create unauthorized VPN sessions, potentially giving them access to internal networks. CISA added the flaw to its Known Exploited Vulnerabilities catalog on May 29.
- A critical remote code execution flaw has been [disclosed](#) in Gogs, a popular open-source self-hosted Git service, with a CVSS score of 9.4 and no patch available. An authenticated user can abuse rebase merging to execute commands, risking repository access and cross-tenant data exposure. The vulnerability remains unpatched by the developer for more than two months.

Check Point IPS provides protection against this threat (Gogs Remote Code Execution)

- Ghost CMS vulnerability CVE-2026-26980 is actively being [exploited](#) in attacks that use SQL injection to steal Admin API keys and alter website pages. At least two groups have targeted more than 700 sites using fake Cloudflare checks to deliver data-stealing malware.

Check Point IPS provides protection against this threat (Ghost SQL Injection (CVE-2026-26980))

THREAT INTELLIGENCE REPORTS

- Researchers [attributed](#) a destructive campaign against LA Metro to an Iran-linked intelligence operation using the Ababil of Minab persona. LA Metro confirmed an intrusion involving wiped servers, and analysts linked additional transit and technology attacks to Black Shadow infrastructure.
- Researchers [observed](#) renewed Grandoreiro banking malware campaigns targeting Portuguese banks and organizations across Spain, Mexico, and Latin America. The attacks begin with phishing and using DLL side-loading or malicious scripts, then abuse cloud services to hide traffic while stealing credentials and displaying fake banking overlays.
- Researchers [uncovered](#) GHOST STADIUM, a fraud network cloning FIFA-related websites across more than 300 active domains ahead of the 2026 World Cup. The operation steals login credentials and payment data, locks fans out of accounts, and is promoted through Facebook ads.
- Researchers [exposed](#) JINX-0164, a financially motivated group targeting cryptocurrency organizations through recruiter-themed social engineering and macOS malware, including AUDIOFIX and MINIRAT. The campaigns moved from compromised developer laptops into code repositories and build systems, creating supply chain compromise risk.