CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- RansomHub ransomware group has claimed responsibility for a cyber-attack on Luxshare, an electronics manufacturer of Apple, Nvidia, LG, Tesla, and others. The threat actors claimed access to 3D CAD models, circuit board designs, and engineering documentation. The company has not yet confirmed the breach.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat
  (Ransomware.Wins.Ransomhub.ta.; Ransomware.Win.RansomHub)*

- Dark-web threat actor has leaked an alleged database belonging to Under Armour, a US sportswear company, affecting 72 million customer records following a November ransomware attack. The claimed exposed data includes names, email addresses, genders, dates of birth, and addresses.

- Raaga, an India-based music streaming platform, has experienced a data breach involving 10.2 million user records, reportedly exfiltrated in December and later advertised on criminal forums. Exposed details include names, emails, demographics, locations, and passwords stored with unsalted MD5 hashes, raising credential stuffing and phishing risks.

- Germany's Dresden State Art Collections (SKD), one of Europe's oldest museum networks, has confirmed a cyberattack that resulted in widespread disruption to its digital infrastructure and communications. The incident disabled online ticket sales, visitor services, and the museum shop, forced on-site payments to cash-only, and limited digital and phone services, with no indication of data theft or exposure reported.

AI THREATS

- Researchers discovered an indirect prompt-injection flaw in Gemini's Google Calendar assistant that bypassed Calendar privacy controls via a malicious invite description. Gemini used Calendar.create to place summaries of the victim's meetings into a new event readable by the attacker.

- Researchers uncovered a web attack technique where hidden prompts in benign pages call LLM API to generate polymorphic malicious JavaScript at runtime. This enables phishing and credential theft while evading signature-based detection and network filtering by leveraging AI service domains.

- Advanced language models such as GPT-5.2 and Opus 4.5 were observed generating working exploits for a previously unknown zero-day vulnerability in QuickJS, a JavaScript interpreter, including in hardened environments where automated systems can produce functional attack code with little to no human intervention. Across six different configurations, the systems produced over 40 distinct exploits.

VULNERABILITIES AND PATCHES

- Three high severity vulnerabilities (CVE-2025-68143, CVE-2025-68144, CVE-2025-68145) were disclosed in mcp-server-git, Anthropic's Git MCP server, enabling path traversal and argument injection exploitable via prompt injection to read or delete files and achieve remote code execution. Fixes available in versions 2025.9.25 and 2025.12.18.
- Zoom has fixed CVE-2026-22844, a critical command injection flaw in Zoom Node Multimedia Routers, used in Meeting Connector and Meetings Hybrid deployments. It enables participant remote code execution in versions before 5.2.1716.0, with no confirmed in-the-wild exploitation.
- Fortinet has confirmed active exploitation of a FortiCloud SSO auth bypass on fully patched FortiGate firewalls, tied to CVE-2025-59718 and CVE-2025-59719. Attackers are logging in via crafted SAML messages, creating persistent accounts, enabling VPN access, and extracting firewall configurations.

THREAT INTELLIGENCE REPORTS

- Check Point Research revealed that VoidLink, a recently exposed cloud-native Linux malware framework, is authored almost entirely by AI, likely under the direction of a single individual. The malware was produced predominantly through AI-driven development, reaching the first functional implant in under a week. From a methodology perspective, the actor used the model beyond coding, adopting an approach called Spec Driven Development (SDD).
- Check Point Research identified an ongoing phishing campaign associated with KONNI, a North Korean–linked threat actor active since at least 2014. The campaign targets software developers and engineering teams across the Asia-Pacific region, including Japan, Australia, and India, using blockchain-themed lures to prompt interaction and deliver malicious content. In observed activity, the threat actor deploys AI-generated PowerShell backdoors that establish persistence, steal credentials, and enable infiltration of development environments
- Check Point researchers describe a Microsoft Teams phishing campaign abusing guest invitations and finance-themed team names to mimic billing notices. More than 12K emails were observed hitting 6,135 users via invite emails with obfuscated text. The campaign targeted US-based organizations across manufacturing, technology, and education.
- Researchers revealed a new ransomware family, Osiris, that blends legitimate Windows tools with custom malware to infiltrate networks and deploy encryption. The operators use a custom malicious driver, Poortry, masquerading as Malwarebytes to disable security software, and exfiltrated data with Rclone to Wasabi buckets before encryption.
- Researchers identified a North Korean spear-phishing campaign targeting South Korea that abuses Microsoft Visual Studio Code tunnels for remote access. JSE files masquerading as Hangul documents start the infection chain and grant attackers terminal and file access using living-off-the-land techniques.