CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Colombia's Ministry of Justice has experienced a ransomware attack that affected part of its technology infrastructure and disrupted public services related to illicit-drug monitoring and legal processes. Officials confirmed that some files were encrypted but stated that no data theft was detected during the incident.
- MyDr, Poland's primary healthcare platform for appointments, medical records, and prescriptions, has suffered a data breach potentially affecting nearly 19 million citizens. Attackers claimed to hold 2.5TB of information and shared a senior politician's identification details, phone numbers, and prescriptions as evidence of the compromise.
- Levi Strauss & Co., the global American apparel company, has reported a cyberattack after attackers used social engineering to compromise three employee devices and steal corporate information. According to the firm, preliminary findings indicate no consumer data was accessed or copied. The company notified affected individuals and relevant regulators.
- IEH Corporation, a US defense and aerospace component manufacturer, has confirmed a phishing compromise of an employee's Microsoft 365 mailbox. Attackers used a fraudulent document-sharing link to steal credentials, potentially exposing customer communications, purchase orders, engineering documents, and export-controlled technical information.

AI THREATS

- Researchers detailed a suspected China-linked campaign that used autonomous AI agents against Taiwanese government systems. The operation reportedly mapped 21 systems, compromised 85 accounts, and obtained 2,500 personnel records before expanding toward a nuclear safety organization and seven companies in the energy sector.
- Researchers outlined how North Korea-linked Kimsuky is building an offline AI environment to support phishing, intelligence analysis, and malware development. The setup combines locally hosted language models with document retrieval, code resources, and transcription capabilities, potentially allowing operators to automate additional stages of cyberespionage activity.
- Researchers found that encrypted reasoning blocks used by OpenAI, Anthropic, and Google APIs could be replayed across sessions. Analysis of more than 315,000 blocks recovered hundreds of sensitive artifacts from published agent logs, including API keys, passwords, authentication tokens, and private cryptographic keys.

VULNERABILITIES AND PATCHES

- Microsoft has released its August Patch Tuesday security updates, addressing 421 vulnerabilities across Windows, Office, SharePoint, Exchange Server, Azure and other products. The fixes include 42 critical flaws and CVE-2026-68820, an actively exploited Windows Ancillary Function Driver for WinSock vulnerability that allows local attackers to gain SYSTEM privileges.
- Apple released patches for CVE-2026-65400, a critical macOS Screen Sharing authentication vulnerability with a CVSS score of 9.8. The flaw allows network attackers to authenticate without valid credentials. Active exploitation against internet-exposed systems has resulted in root access and deployment of Monero cryptocurrency miners.
- Adobe released a fix for CVE-2026-71362, a critical authentication vulnerability affecting Adobe Commerce and Magento Open Source. Attackers began exploiting the flaw shortly after public disclosure. Successful exploitation enables unauthorized session switching, potentially allowing account takeover and access to information associated with affected accounts.
- Zoom addressed three critical vulnerabilities in Zoom Workplace, including CVE-2026-53413, that could enable remote code execution during a meeting. The flaws affected annotation functionality and required no interaction from the targeted participant. Fixed releases include versions 7.0.6 and 7.1.5 for fast-track users.

THREAT INTELLIGENCE REPORTS

- Check Point Research has exposed a new wave of the Lazarus-linked Operation Dream Job targeting defense organizations in Europe, India and Brazil. Attackers used fraudulent job opportunities and trojanized PDF software to deploy malware, while exploiting Windows zero-day CVE-2026-68820 to obtain SYSTEM privileges and disable security visibility.
- Check Point Research has assessed ransomware activity during Q2 2026, identifying 2,139 publicly reported victims, up 33% year over year. The ransomware ecosystem expanded to 93 active groups, while leaked communications showed The Gentlemen using AI coding assistants to accelerate development of operational tooling.
- Check Point Research have reported that organizations experienced an average of 2,336 weekly cyberattacks during July 2026, representing a 16% year-over-year increase. Ransomware activity also accelerated, while generative AI usage continued exposing corporate information through high-risk prompts submitted to external AI services.
- Researchers revealed a China-linked Jewelbug campaign using XG-Web to conduct espionage against government and military organizations while supporting cryptocurrency fraud. The operation collected approximately 580,000 browser cookies, thousands of credentials, and 2,300 emails through compromised web infrastructure and malicious cryptocurrency services.