CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Ernst & Young, a global accounting and professional services company, has disclosed a data breach involving a compromised third-party IT support platform. The exposed support tickets may have contained client documents, tax information, employee details, and other sensitive information submitted while requesting technical assistance.
- Jscrambler, a JavaScript code-protection package with more than 15,000 weekly downloads, has experienced a supply chain compromise after stolen npm publishing credentials distributed malicious releases. The packages deployed malware targeting developers', cloud, browser, cryptocurrency, and messaging credentials. Jscrambler removed the affected versions.
- Coca-Cola's US dairy subsidiary Fairlife has confirmed a ransomware attack that temporarily halted production across the United States. Attackers accessed systems supporting manufacturing operations, prompting the company to activate incident response and business continuity procedures. Coca-Cola has not confirmed whether data was exfiltrated in the attack.
- Nihon Kotsu, Japan's largest taxi operator, has suffered a malware attack following unauthorized access to its internal network. The company shut down affected systems, disrupting taxi dispatches, telephone services, bookings, reservations, and car rentals from July 11. No theft of customer or corporate information has been confirmed.

AI THREATS

- Researchers identified a China-linked campaign that used Claude Code and DeepSeek to automate attacks against government and financial organizations. The tools generated scripts, adapted failed exploits, created credential-harvesting pages, and executed commands. Confirmed compromises affected government systems in Thailand and Afghanistan and organizations in Taiwan.
- Researchers found that xAI's Grok Build coding assistant could upload entire Git repositories while processing debugging requests. Transferred information included unopened files and complete commit histories, potentially exposing API keys, credentials, and proprietary source code. Initial privacy controls did not prevent uploads until a server-side restriction was introduced.
- Researchers verified a weakness in Anthropic's Claude for Chrome extension that allowed malicious browser extensions to impersonate Claude and act through authenticated user sessions. Successful exploitation could expose Gmail, Google Drive, or GitHub information through Claude's permissions. Anthropic released fixes, although researchers reported that a bypass remained possible.

VULNERABILITIES AND PATCHES

- Microsoft released patches for 622 vulnerabilities in July's Patch Tuesday, the largest monthly release recorded by the company. Two vulnerabilities were under active exploitation, including CVE-2026-56164 in SharePoint Server and CVE-2026-56155 in Active Directory Federation Services. Both vulnerabilities could allow attackers to elevate privileges.

  Check Point IPS provides protection against these threats *(Microsoft SharePoint Authentication Bypass (CVE-2026-56164))*

- WordPress has issued emergency updates for CVE-2026-63030 and CVE-2026-60137, collectively called wp2shell. The critical WordPress Core vulnerabilities allow unauthenticated remote code execution and website takeover. Affected releases include versions 6.9.0 through 6.9.4 and 7.0.0 through 7.0.1. Fixed versions include 6.9.5 and 7.0.2.

  Check Point IPS provides protection against these threats *(WordPress Authentication Bypass (CVE-2026-63030)), WordPress SQL Injection (CVE-2026-60137))*

- SonicWall has released a hotfix for CVE-2026-15409 and CVE-2026-15410, two critical vulnerabilities affecting SMA 1000 Series gateways. The flaws allow unauthenticated attackers to execute system commands on vulnerable appliances. Active exploitation has been associated with Inc ransomware.

  Check Point IPS provides protection against these threats *(SonicWall SMA1000 Series Server-Side Request Forgery (CVE-2026-15409) & SonicWall SMA1000 Series Path Traversal (CVE-2026-15410))*

THREAT INTELLIGENCE REPORTS

- Check Point Research has released the 2026 AI Security 2026, finding that AI has evolved from an attack aid into an active operator across live intrusions and malware development. The report also highlights indirect prompt injection, synthetic identity abuse, and enterprise data exposure, with high-risk GenAI prompts doubling to 4%.

- Researchers analyzed ShinyHunters-linked campaigns that abused OAuth application approvals to access Salesforce environments. Attackers used voice phishing to authorize lookalike applications, then accessed CRM information through approved APIs. Compromised integrations and misconfigured guest access provided additional entry points and persistence.

- Researchers analyzed CylindricalCanine, a subgroup of the Chinese cybercrime collective GoldenEyeDog, and linked it to DigiCert's April 2026 support portal compromise. The actor stole code-signing certificates, leading to 60 revocations, including at least 27 associated with malware. The group also targets Asia-Pacific finance teams using Golden Gh0st RAT.

- Researchers documented Spirals, a Rust-based ransomware family used against a South Asian information technology services company. The attackers moved from initial access to network encryption in less than 24 hours. They used an IIS web shell, WMI, and PsExec to spread, disable security services, disrupt backups, and encrypt systems.