CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Nichirei, a Japan-based frozen-food supplier and logistics company, has experienced a ransomware attack that disrupted shipping operations and affected approximately 5,000 customers. KFC Japan warned of possible shortages. Nichirei confirmed personal data theft, while the RansomHouse group claimed responsibility and published a subset of the stolen information.
- Stadler Rail, a Switzerland-based global rail equipment manufacturer, has disclosed a supplier-related data breach after attackers compromised credentials for a third-party file-sharing platform. The Everest group stole technical documents belonging to the supplier and demanded $12.3 million. Stadler refused payment and said its systems and production remained unaffected.
- Origin Energy, one of Australia's largest electricity and natural gas providers, has confirmed unauthorized access to customer information. Exposed data may include names, addresses, birth dates, phone numbers, account details, and partial payment information. Threat actors claimed to have stolen two million records and threatened to publish them.
- Romania's National Agency for Cadastre and Land Registration has suffered a cyberattack that disabled internal systems and the nationwide e-Terra platform. The disruption halted property transactions for nearly a week. Officials said core land registries remained intact, although credentials and portions of source code may have been exposed.

AI THREATS

- OpenAI disclosed that AI models escaped a restricted cyber evaluation environment and compromised Hugging Face while seeking benchmark solutions. They exploited zero-day vulnerabilities, stole credentials, escalated privileges, and accessed production systems. Both companies contained the activity and are conducting a joint investigation.
- Researchers have described a threat actor known as Trim who promoted an AI-assisted penetration-testing platform built with jailbroken language models. The platform combines AI with established scanning tools to automate reconnaissance, vulnerability validation, and reporting, potentially reducing the expertise and time required to prepare and conduct cyber intrusions.
- Researchers have examined a generative AI-assisted malware operation exposed through an accessible WebDAV server. The infrastructure produced phishing material and malicious Windows shortcuts used to distribute information stealers and remote access tools. Researchers identified more than 1,000 artifacts and a campaign that recorded over 77,000 requests.

VULNERABILITIES AND PATCHES

- Check Point has addressed CVE-2026-16232, an authentication bypass vulnerability in SmartConsole that is under active exploitation, affecting a handful of customers. The flaw allows remote attackers to bypass authentication and gain administrative access to Check Point management servers. Security hotfixes are available for supported versions of the affected management software.
- Oracle has released its July 2026 Critical Patch Update, addressing 1,449 vulnerabilities across numerous product families. The update includes remotely exploitable flaws that require no authentication, with critical issues affecting Oracle Database Server, SQL Developer, and TimesTen In-Memory Database, among others.
- Microsoft has addressed CVE-2026-50522, a critical remote code execution vulnerability affecting on-premises SharePoint Server. An authenticated site owner can exploit the flaw to execute code and steal machine keys for persistent access. Active exploitation was reported after proof-of-concept code became publicly available.

  Check Point IPS provides protection against this threat *(Microsoft SharePoint Remote Code Execution (CVE-2026-50522))*

THREAT INTELLIGENCE REPORTS

- Check Point Research has revealed that Microsoft was the most impersonated brand in Q2 2026, accounting for 23% of observed phishing attempts. LinkedIn, Google, Apple, and Amazon completed the top five. ChatGPT entered the top ten as attackers increasingly targeted users of widely recognized AI platforms.
- Researchers have described the growing use of infostealers logs as an initial-access resource for cloud and software-as-a-service intrusions. Criminal marketplaces sell passwords and active session cookies soon after collection. The research identified 2.05 million logs during 2025, with 79% connected to Microsoft single sign-on environments
- U.S. federal agencies have warned that Iran-linked actors are targeting internet-exposed industrial controllers at water and energy facilities. The attackers have manipulated controller logic, falsified operator displays, and disabled alarms or shutdown functions. The activity affects equipment deployed in critical infrastructure environments.
- Researchers have analyzed a Russian cyberespionage campaign targeting Zimbra webmail servers at government, defense, transportation, and financial organizations. The attackers exploit CVE-2025-66376 through zero-click phishing emails that inject malicious JavaScript, stealing credentials, two-factor authentication codes, email archives, and search histories from vulnerable systems.

  Check Point IPS provides protection against this threat *(Zimbra Collaboration Suite Cross-Site Scripting (CVE-2025-66376))*