cp<r>
CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- United States-based medical technology company Stryker has suffered a cyberattack that caused a global disruption to its environment. The company said its surgical robotics, clinical communications platform, and life support monitors are safe to use. Media reports said employee devices were factory reset across multiple locations worldwide. Iranian group Handala Hack has claimed responsibility for the attack and said it had exfiltrated large amounts of data as part of the attack.
- Telus Digital, a subsidiary of Canadian telecom firm Telus, has confirmed a breach involving unauthorized access to a limited number of systems. Hacker group ShinyHunters claims to have stolen nearly one petabyte of customer and call data and demanded $65 million in ransom, although the company said it has not verified those claims and reported no disruption.
- Encrypted messaging service Signal has experienced targeted phishing campaigns leading to account takeovers of high-profile users, including journalists and government officials. Signal said its infrastructure and encryption remain intact, and attackers tricked victims into sharing SMS verification codes and Signal PINs to provision new devices and impersonate them.
- Loblaw Companies Limited, Canada's largest food and pharmacy retailer, has suffered a data breach after hackers accessed part of its IT network. The company said names, phone numbers, and email addresses were exposed, prompting a forced logout for customer accounts, while payment, health, and password data do not appear affected.

AI THREATS

- Researchers evaluated autonomous AI agents on widely used models and found they initiated offensive actions without malicious prompts, hacking their own operating environments. In tests, agents posted passwords, bypassed antivirus, forged credentials, and escalated privileges to access sensitive data, showing how autonomy can amplify security risk.
- Researchers unearthed a campaign using an AI-powered bot, hackerbot-claw, to exploit misconfigured GitHub Actions in open-source repositories, including Aqua Security. The bot stole a token to seize Aqua's Trivy repository and publish a malicious extension that ran AI tools to harvest secrets and push results to the victim's GitHub.
- Researchers investigated malvertising campaigns that impersonate popular AI agents, including Claude Code, OpenClaw, and Doubao, to push infostealing malware through Google Search ads. The fake documentation pages instruct users to run commands that install AMOS on macOS and Amatera on Windows, enabling theft of credentials and corporate files.

VULNERABILITIES AND PATCHES

- SolarWinds Web Help Desk, an IT ticketing platform, is affected by CVE-2025-26399, a high-severity deserialization flaw that attackers are exploiting to run commands on servers. Successful exploitation can enable takeover and data theft, and patches are available after the vulnerability was added to CISA's exploited flaws catalog.

  Check Point IPS provides protection against this threat *(SolarWinds Web Help Desk Insecure Deserialization (CVE-2024-28986, CVE-2024-28988, CVE-2025-40553, CVE-2025-26399))*

- Google has released an out-of-band Chrome update addressing two high-severity zero-days, CVE-2026-3909 in Skia memory handling and CVE-2026-3910 in V8. Both can be triggered by visiting a malicious site and may enable code execution in the browser.

- The n8n workflow automation platform has fixed CVE-2025-68613, a CVSS 10 remote code execution flaw that is under active exploitation. The issue allows authenticated users to run code and compromise servers, and patches were released in versions 1.120.4, 1.121.1, and 1.122.0.

  Check Point IPS provides protection against this threat *(n8n Remote Code Execution (CVE-2025-68613))*

THREAT INTELLIGENCE REPORTS

- Check Point Research has analyzed the Iranian threat group Handala Hack, a hacktivist persona run by the Void Manticore APT group, which is affiliated with the Iranian Ministry of Intelligence. The group targets IT and VPN infrastructure to gain initial access to victim organizations, before using tools such as NetBird for lateral movement. The group then aims to exfiltrate and wipe victim organizations' data.

  Check Point Harmony Endpoint and Threat Emulation provide protection against these threats

- Check Point Research has examined Iranian Ministry of Intelligence-linked groups use of criminal tools and services, including Handala Hack deploying Rhadamanthys infostealer alongside wipers against Israeli targets. The report also noted overlaps between MuddyWater activity, Tsundere and DinDoor botnet infrastructure, and CastleLoader certificates.

  Check Point Harmony Endpoint and Threat Emulation provide protection against these threats

- Check Point Research analyzed February 2026 cyber-attacks, as organizations averaged 2,086 weekly attacks, up 9.6% year over year, with education most targeted and Latin America recording the highest volumes. Ransomware totaled 629 incidents, while enterprise GenAI use continued to pose data-leak risk in 1 of every 31 prompts.

- Check Point Research have analyzed China-nexus espionage campaigns targeting Qatar. A Camaro Dragon campaign attempted to deploy PlugX, while a second operation delivered Cobalt Strike via war-themed lures abusing trusted software targeting government and energy-related entities.

  Check Point Harmony Endpoint and Threat Emulation provide protection against these threats