CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- U.S. auto insurer AssuranceAmerica has disclosed a data breach affecting approximately 7 million people. Attackers targeted an employee and used compromised credentials to access company systems, stealing names, contact information, driver's license numbers, insurance policy and account data, vehicle information, and claims details.
- Latvia's state-owned forestry company Latvijas Valsts Meži has suffered a ransomware attack that disrupted mapping, hunting, contractor, and customer systems. Attackers exploited a system that had remained unpatched for two years and leaked approximately 44GB of internal documents, credentials, cryptographic keys, source code, and email correspondence.
- Injective Labs, a developer of blockchain and cryptocurrency software, has experienced a supply chain compromise after attackers accessed its SDK project and published malicious npm packages. The affected releases exfiltrated cryptocurrency wallet private keys and seed phrases when developers used legitimate key-generation functions embedded in the compromised software.
- Moody Bible Institute, a U.S. faith-based educational institution, has disclosed a data breach affecting more than 2.3 million donors, students, alumni, and supporters. The ShinyHunters extortion group published allegedly stolen information, including names, dates of birth, residential addresses, email addresses, and phone numbers.

AI THREATS

- Researchers profiled JadePuffer, an autonomous ransomware operation that used a large language model to conduct an intrusion without direct human control. The operation exploited CVE-2025-3248 in an exposed Langflow instance, accessed a production MySQL server, exfiltrated selected information, deleted the database, and issued an extortion demand.
- Researchers showed that malicious instructions hidden inside open-source project files could achieve remote code execution through Anthropic Claude Code and OpenAI Codex. When operating with automated permissions, the coding agents processed the instructions and executed attacker-controlled scripts, demonstrating a risk that may affect other autonomous development tools.
- Researchers disclosed Rogue Agent, a vulnerability in Google Dialogflow CX that allowed users with limited agent-editing permission to insert persistent malicious code. The injected code could capture and exfiltrate chatbot conversations. Google addressed the issue, and no known customer environments were compromised through the vulnerability.

VULNERABILITIES AND PATCHES

- Multiple Tenda router models are affected by CVE-2026-11405, an undocumented authentication backdoor that provides administrative access through a hidden password. The flaw affects several FH1201, W15E, AC10, AC5, and AC6 firmware versions and allows attackers to bypass configured credentials and modify device and network settings.
- Linux maintainers have patched CVE-2026-53359, a critical vulnerability in the Kernel-based Virtual Machine hypervisor. A malicious guest virtual machine could corrupt host kernel memory and potentially escape into the host environment. The flaw affects Intel and AMD x86 systems and is particularly relevant to shared cloud infrastructure.
- U-Boot has addressed six vulnerabilities affecting signature verification of Flattened Image Tree files used during secure boot. Two flaws could enable arbitrary code execution while a device loads a supposedly verified image, and four could cause crashes. The affected bootloader is widely used in routers, cameras, and embedded controllers.
- Opera has addressed a critical vulnerability in the Opera GX browser that allowed malicious websites to install browser modifications without user confirmation. An attacker-controlled modification could inject styles across open tabs, leak information such as Gmail addresses, and crash the browser. Opera corrected the issue.

THREAT INTELLIGENCE REPORTS

- Check Point Research has profiled Cavern Manticore, an Iran-linked threat actor targeting Israeli government and information technology organizations. The group uses a modular .NET command-and-control framework and has abused remote management software and a compromised software update mechanism to deploy file-management, database, scanning, and tunneling capabilities.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat
- Check Point Research have analyzed global cyberattack activity during June 2026, recording an average of 2,270 weekly attacks per organization. Ransomware incidents increased by 33% from June 2025, while The Gentlemen overtook Qilin as the most active group during the month.
- Check Point researchers have investigated a student employment phishing campaign that abused compromised school email accounts and Google Forms. More than 3,200 messages passed email authentication checks and attempted to collect banking information, residential addresses, and other details associated with money mule recruitment and account compromise.
- Researchers analyzed UAT-7810, a China-linked threat actor that compromises internet-facing networking devices to expand operational relay box infrastructure. The group developed new malware components and exploited unpatched Ruckus and ASUS devices to create proxy nodes for associated threat actors.