CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Instructure, the US education technology company behind the Canvas learning platform, has confirmed a major data breach affecting its cloud-hosted environment. Exposed data reportedly includes student and staff records and private messages, while ShinyHunters escalated the attack by defacing hundreds of school login portals with ransom messages.
- Zara, the flagship brand of Spanish fashion group Inditex, has experienced a data breach tied to a third-party technology provider. Inditex confirmed unauthorized access, and experts verified that 197,400 unique email addresses, order IDs, purchase history, and customer support tickets were exposed.
- Hungarian media company Mediaworks, which operates dozens of newspapers and online outlets, was hit by a data-theft extortion attack. The company confirmed an intrusion after World Leaks posted 8.5TB of internal files online, reportedly including payroll records, contracts, financial documents, and internal communications.
- Czech automaker Škoda has fallen victim to a security incident affecting its online shop after attackers exploited a software flaw to gain unauthorized access. Exposed customer data may include names, contact details, order history, and logins, but according to the company passwords payment card data was not affected.

AI THREATS

- Researchers have uncovered a critical WebSocket hijacking vulnerability in Cline's local Kanban server, impacting the widely used open-source AI coding agent. Rated CVSS 9.7 and patched in version 0.1.66, the flaw allowed any website a developer visited to exfiltrate workspace data and inject arbitrary commands into the AI agent.
- Security researchers found a flaw in Anthropic's Claude in Chrome extension that allowed other browser extensions to hijack the AI agent. The issue enabled malicious prompts to trigger unauthorized actions and access sensitive browser-connected data, showing how AI assistants can extend browser attack surfaces.
- Researchers detailed an InstallFix campaign using fake Claude AI installer pages promoted through Google Ads to infect Windows and macOS users. Victims were tricked into running commands that launched multi-stage malware, stole browser data, disabled protections, and established persistence through scheduled tasks.

VULNERABILITIES AND PATCHES

- Progress alerted customers to CVE-2026-4670, a critical authentication bypass in MOVEit Automation managed file transfer software that allows unauthorized access, and CVE-2026-5174, a privilege escalation flaw. Fixes are available in versions 2025.1.5, 2025.0.9, and 2024.1.8.
- Ivanti has fixed CVE-2026-6973, a high-severity Endpoint Manager Mobile vulnerability which is exploited as a zero-day. The flaw affects EPMM 12.8.0.0 and earlier and allows attackers with administrator permissions to run remote code, while hundreds of appliances reportedly remain exposed online.
- Palo Alto Networks PAN-OS Authentication Portal is affected by CVE-2026-0300, a critical buffer overflow flaw allowing unauthenticated attackers to run code with root privileges on affected firewalls. Palo Alto Networks observed active exploitation against exposed portals, with no fix available at this time.
- Dirty Frag, an unpatched Linux kernel flaw, enables local privilege escalation across Ubuntu, RHEL, Fedora, AlmaLinux, and CentOS Stream. By chaining bugs in IPsec and RxRPC, a local user can gain root access with high reliability, and public proof-of-concept code is available.

THREAT INTELLIGENCE REPORTS

- Researchers linked Iran's MuddyWater to using the Chaos ransomware as cover for espionage and data theft. In a recent case, attackers used Microsoft Teams social engineering to harvest credentials and deploy remote tools, then extorted the victim without encrypting files before leaking data.
- Researchers detailed a Silver Fox campaign targeting organizations in India and Russia with tax-themed phishing emails. The activity delivered the previously undocumented ABCDoor backdoor, ValleyRAT, and related malware, affecting industrial, consulting, retail, and transportation sectors through more than 1,600 socially engineered messages.
- Researchers unmasked a multi-stage phishing campaign using fake code-of-conduct emails and adversary-in-the-middle tactics to hijack sign-in sessions and bypass multi-factor authentication. Active between April 14 to 16, it targeted more than 35,000 users at 13,000 organizations across 26 countries.
- Researchers profiled UAT-8302, a China-linked espionage group conducting long-term intrusions against government agencies in South America and southeastern Europe. The actors combine custom backdoors, including NetDraft and CloudSorcerer, with OneDrive and GitHub command channels and open-source tools for reconnaissance and lateral movement.
- Researchers revealed a software supply chain campaign on NuGet in which five packages impersonating Chinese .NET UI libraries install an infostealer. The packages have recorded nearly 65,000 downloads, putting developer workstations and systems at risk by stealing passwords, SSH keys, and cryptocurrency wallet data.