CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- MicroWorld Technologies, maker of eScan antivirus, has suffered a supply-chain compromise. Malicious updates were pushed via the legitimate eScan updater, delivering multi-stage malware that establishes persistence, enables remote access, and blocks automatic updates. In response, eScan shut down its global update service for more than eight hours.
- Crunchbase, a private company intelligence platform, has confirmed a data breach of over 2 million records claimed by ShinyHunters threat group after a ransom demand was refused. The published files were stolen from its corporate network and include customer names, contact details, partner contracts and other internal documents. Crunchbase said that their operations were not disrupted.
- Qilin ransomware group has leaked an alleged database belonging to Tulsa International Airport in Oklahoma. The database include financial records, internal emails, and employee identification data. The airport authority has not yet confirmed compromise, and operations reportedly continue.

  Check Point Threat Emulation provides protection against this threat *(Ransomware.Wins.Qilin.ta.*; Ransomware.Wins.Qilin)*
- WorldLeaks extortion group has claimed responsibility for a data breach on the sportswear giant Nike. The threat group allegedly exposed samples totaling 1.4 terabytes of internal data including documents and archives related to the company's supply chain and manufacturing operations.

AI THREATS

- Clawdbot, an open source AI agent gateway, has more than 900 publicly exposed and often unauthenticated instances due to localhost auto approval behind reverse proxies. It enables credential theft, access to chat histories, and remote code execution.
- Researchers uncovered RedKitten, a 2026 campaign with LLM-assisted development indicators targeting Iranian activists and NGOs. The campaign uses password-protected Excel lures to deliver SloppyMIO, a C# implant that uses Telegram for C2 and GitHub/Google Drive for payloads, with steganographic configuration, AppDomain Manager injection, and scheduled task persistence.
- Researchers identified 16 malicious Chrome extensions for ChatGPT that exfiltrate authorization details and session tokens. The extensions inject scripts into the ChatGPT web application to monitor outbound requests, allowing attackers to hijack sessions and access chat histories.
- Researchers analyzed publicly accessible open-source LLM deployments via Ollama and revealed many with disabled guardrails and exposed system prompts, enabling spam, phishing, disinformation, and other abuse.

© 2026 Check Point Software Technologies Ltd. All Rights Reserved

VULNERABILITIES AND PATCHES

- A critical path traversal vulnerability (CVE-2025-8088) in WinRAR is actively exploited by government backed threat actors linked to Russia and China as well as financially motivated threat actors. Weaponized phishing forces WinRAR to write malware into the Windows Startup folder, enabling automatic execution for ransomware and credential theft. A patch is available on WinRAR 7.13.

  Check Point IPS provides protection against this threat *(RARLAB WinRAR Directory Traversal (CVE-2025-8088))*

- SmarterTools addressed two critical SmarterMail flaws, including CVE-2026-24423 enabling remote code execution and CVE-2026-23760 allowing unauthenticated admin account takeover. The second flaw is actively exploited, and over 6,000 exposed SmarterMail servers are reportedly vulnerable.

  Check Point IPS provides protection against this threat *(SmarterTools SmarterMail Remote Code Execution (CVE-2026-24423); SmarterTools SmarterMail Authentication Bypass (CVE-2026-23760))*

- Fortinet has fixed CVE-2026-24858, an authentication bypass in FortiCloud single sign on which allowed unauthorized access and admin creation on downstream devices. The flaw carries CVSS 9.4 and is actively exploited via FortiCloud SSO.

THREAT INTELLIGENCE REPORTS

- Check Point Research has published the 2026 Cyber Security Report, highlighting AI as a force multiplier across attacks, fragmentation in ransomware with data only extortion, and multi-channel social engineering attacks. It maps threat activity to geopolitics and identity driven paths, quantifies risky AI usage, and provides sector and regional breakouts.

- Polish CERT detailed coordinated destructive attacks on Polish energy and manufacturing sectors, attributed to Static Tundra, using FortiGate SSL VPN access. The attackers conducted reconnaissance, firmware damage, lateral movement, and deployed DynoWiper and LazyWiper that corrupt files.

- Researchers have uncovered renewed Matanbuchus downloader campaigns using Microsoft Installer files disguised as legitimate installers, with frequent component changes to evade antivirus and machine learning detection. In many cases, the loader is used for further ransomware deployment.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(Trojan-Downloader.Wins.Matanbuchus.ta.*; Trojan-Downloader.Wins.Matanbuchus; Trojan-Downloader.Win.Matanbuchus)*

- Researchers have identified PyRAT, a Python based cross platform RAT for Windows and Linux, using unencrypted HTTP POST C2, fingerprinting victims, and file and screenshot exfiltration. Persistence uses a deceptive autostart on Linux and a user Run key on Windows, with semi persistent identifiers.

- Researchers have found an Android campaign distributing a RAT via fake security alerts installing TrustBastion, which retrieves a second-stage payload from Hugging Face. The malware abuses Accessibility Services, deploys credential-stealing overlays, and uses server-side polymorphism to regenerate payloads every 15 minutes.

© 2026 Check Point Software Technologies Ltd. All Rights Reserved