CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Romania's national oil pipeline operator, Conpet, has suffered a cyberattack that disrupted its IT systems and took its website offline. The company said operational technology, including pipeline control and telecommunications systems, remained fully functional and oil transport continued without interruption. The attack was claimed by the Qilin ransomware group.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (Ransomware.Wins.Qilin.ta.; Ransomware.Wins.Qilin)*

- La Sapienza University in Rome, one of Europe's largest universities, has confirmed a cyberattack that prompted it to take down computer systems for three days, with email and workstations partially limited. The website remains offline as the school restores services.

- The City of New Britain, a municipal government in Connecticut, was hit by a ransomware attack that disrupted internet and phone services for over 48 hours. While emergency services remained operational, it is unclear whether personal data was compromised.

- Onze-Lieve-Vrouw Instituut (OLV) Pulhof, a secondary school in Berchem, Belgium, has experienced a ransomware attack that escalated into extortion of parents. Attackers reduced demand from €100,000 to €15,000 and threatened to leak student and staff data or charge parents €50 per child, while the school refused payment and is investigating potential exposure.

AI THREATS

- Threat actors leveraged exposed credentials from public AWS S3 buckets to launch an AI-assisted intrusion, escalating cloud privileges from ReadOnlyAccess to admin within eight to ten minutes via Lambda code injection and IAM role assumptions. The attack further abused Amazon Bedrock models for LLMjacking and provisioned GPU-based EC2 instances using JupyterLab to exploit resources, pivoting rapidly across 19 AWS principals.

- Ask Gordon, Docker's AI assistant, was affected by the critical "DockerDash" vulnerability, allowing Meta Context Injection via Model Context Protocol that treats malicious Docker image LABEL metadata as executable instructions. This enabled remote code execution and data exfiltration in cloud, CLI, and Docker Desktop environments, with mitigations released in Docker Desktop 4.50.0.

- Bondu, an AI plush toy maker, exposed a web console that allowed anyone with a Google account to access 50,000 chat transcripts with children - revealing names, birth dates, family details, and intimate conversations. Researchers reported the issue, after which Bondu disabled the console and added authentication.

VULNERABILITIES AND PATCHES

- Ivanti addressed two zero-days in Endpoint Manager Mobile, CVE-2026-1281 and CVE-2026-1340 (CVSS 9.8), exploited for unauthenticated code injection and remote code execution. The flaws affect in-house app distribution and Android file-transfer features, with emergency fixes issued January 29 for on-premises EPMM deployments.

  Check Point IPS provides protection against this threat *(Ivanti Endpoint Manager Mobile Command Injection (CVE-2026-1281, CVE-2026-1340))*

- Active exploitation of CVE-2025-11953, an OS command injection flaw, was detected in the React Native Community CLI and the Metro development server used by major mobile app projects. This flaw can enable unauthenticated remote code execution, including full shell access on Windows.

  Check Point IPS provides protection against this threat *(React Native Community CLI Command Injection (CVE-2025-11953))*

- n8n maintainers have released patches for a critical issue allowing authenticated users to run system commands through crafted workflows, risking full server compromise and credential theft. The flaw extends a prior expression-engine bug and fixes available in versions v1.123.17 and v2.5.2.

THREAT INTELLIGENCE REPORTS

- Check Point Research observed Amaranth-Dragon, a Chinese-aligned group linked to APT41, conducting espionage against government and law enforcement across Southeast Asia. The threat actor weaponized WinRAR flaw CVE-2025-8088 within 10 days after its disclosure, geo-fenced servers to targets, and introduced TGAmaranth, a Telegram-based remote access tool.

  Check Point IPS, Threat Emulation and Harmony Endpoint provide protection against this threat *(RARLAB WinRAR Directory Traversal (CVE-2025-8088); Trojan.Win.Amaranth; Trojan.Wins.Amaranth.ta.*; APT.Win.APT41; APT.Wins.APT41.ta.*; Trojan.Wins.APT41.ta.*)*

- Check Point researchers assessed three most significant financial-sector trends in 2025. DDoS attacks surged 105%, data breaches and leaks rose 73%, and ransomware incidents reached 451 cases with aggressive multi-extortion tactics. Hacktivists drove DDoS attacks, and ransomware groups like Qilin, Akira, and Cl0p scaled operations via shared tooling and third-party access.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat *(Ransomware.Wins.Qilin.ta.*; Ransomware.Wins.Qilin; Ransomware.Wins.Akira.ta.*; Ransomware.Wins.Clop; Ransomware.Wins.CLOP.ta.*; Ransomware.Win.Clop)*

- Check Point researchers described a phishing campaign that abused legitimate SaaS notifications from Microsoft, Zoom, Amazon, PayPal, YouTube, and Malwarebytes to drive phone-based scams. The operation sent 133,260 emails to 20,049 organizations, intensifying in recent months as attackers leveraged trusted messages to bypass link-focused defenses and steer targets to attacker-controlled phone numbers.