CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- DentaQuest, a U.S. dental benefits administrator owned by Sun Life, has suffered a data breach after threat group ShinyHunters leaked exfiltrated data. Analysts assessed that 2.6 million accounts were exposed, including names, emails, government IDs, and health insurance details.
- Password manager Dashlane has disclosed an attack in which threat actors brute-forced two-factor codes to register unauthorized devices and download encrypted password vaults for less than 20 users. The campaign began May 31 and was contained after lockouts.
- The United Nations World Food Programme has disclosed unauthorized access to its Gaza self-registration application, exposing names, identification numbers, mobile numbers, and location data. The breach affected about 600,000 Palestinian households across Gaza, and WFP suspended the platform while responding to the incident.
- Russia's Federal Security Service claims that foreign intelligence agencies hacked mobile devices belonging to senior Russian officials. The alleged spyware operation enabled access to correspondence, calls, geolocation data, contact lists, and covert audio and video surveillance.
- Hola, whose Windows browser serves millions of users, has confirmed a supply chain compromise that pushed an unauthorized executable to some users. The file operated as a cryptominer, installed as a Windows service, and excluded itself from Defender. An independent review found impact limited to about 0.1% of users.

AI THREATS

- Check Point highlighted an AI security risk after reports that attackers used Meta's AI support chatbot to seize Instagram accounts. Granting AI agents account recovery authority to change emails or approve requests without identity checks can enable unauthorized access, showing that permissions and verification shape the risk.
- Researchers demonstrated a notification-based prompt injection technique called Fake Context Alignment that manipulated Google's Gemini voice assistant through incoming messages. The attack hid authorization prompts and enabled device control, auto-joining Zoom video calls, and cross-device memory poisoning. Google deployed classifier updates after disclosure.
- Researchers described an AI-enabled EDR evasion lab where a threat actor automates malware development and testing against Sophos, CrowdStrike, and Microsoft Defender. LLM-driven agents and an automated Active Directory panel coordinate iterative trials, supporting stealthy post-exploitation tied to ransomware deployment and data theft.

VULNERABILITIES AND PATCHES

- Google has released its June Android security patch for 124 vulnerabilities, including CVE-2025-48595, a high-severity Android Framework flaw under exploitation. Local attackers can use the vulnerability to gain code execution and escalate privileges on devices running Android 14 or later.
- Cisco has released patches for CVE-2026-20230, a critical Unified Communications Manager and Session Management Edition flaw that allows unauthenticated network attackers to write files and escalate to root. A public proof-of-concept was already published. The bug requires WebDialer enabled, and fixes include 14SU6 and an interim 15.x COP.
- SolarWinds Serv-U CVE-2026-28318 has been exploited in attacks against file transfer servers. The unauthenticated flaw lets crafted HTTP POST requests using a deflate header crash the service and disrupt operations. SolarWinds fixed the vulnerability in Serv-U 15.5.4 HF1.
- CVE-2026-41089 in Microsoft Windows Netlogon is being exploited in attacks against Windows Server domain controllers. The critical stack-based buffer overflow flaw can allow remote code execution through crafted network requests. Successful exploitation may give attackers SYSTEM-level control of domain controllers in vulnerable Active Directory environments.

  Check Point IPS provides protection against this threat *(Microsoft Windows Netlogon Remote Code Execution (CVE-2026-41089))*

THREAT INTELLIGENCE REPORTS

- Check Point Research has investigated a large-scale impersonation and click-hijacking scheme that reroutes downloads from fake open-source sites through a gated traffic distribution system. Impersonating tools like Ghidra and dnSpy, it led to infection by RemusStealer, AnimateClipper, and a new loader called SessionGate.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat
- Check Point Research linked a Dutch seizure of about 800 servers at hosting provider WorkTitans B.V. to Iranian cyber espionage operations. MuddyWater, Agrius, and Nimbus Manticore used this infrastructure for attacks that enabled remote access, credential theft, and scanning.
- Check Point researchers have surveyed the 2026 U.S. midterm threat landscape, finding that operations focus on phishing, brand impersonation, and domain abuse rather than ballot tampering. Russian-linked Doppelganger networks cloned major media sites, vote-related domains increased, and exposed ActBlue and WinRed credentials surfaced.
- Researchers identified a months-long espionage campaign that covertly siphoned a senior executive's Microsoft Outlook mailbox at a major global stock exchange. Attackers used legitimate cloud storage services and disguised update tasks to persist and move data in small batches, enabling five months of undetected access.