

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The FBI has [confirmed](#) unauthorized activity affecting FBIjobs.gov after the ShinyHunters group defaced the website. The group claimed to have stolen employee and applicant information and shared samples of purported FBI personnel records with several media organizations.
- Astrana Health, a major US healthcare technology provider, has [confirmed](#) a cyberattack that exposed confidential information. Attackers spoofed the company's telephone number to impersonate personnel and gained access to its servers. Astrana restored systems from backups and disclosed the incident in an SEC filing but has not publicly revealed what data was exposed.
- Cryptocurrency exchange Bitget has [disclosed](#) the theft of \$351.6 million from several hot and warm wallets. The company detected unauthorized transfers on September 24 and temporarily suspended withdrawals. Bitget said cold wallets and most platform assets were unaffected, while suspected North Korean involvement remains under examination.
- Ludwig Maximilian University of Munich, one of Germany's largest universities, has [suffered](#) a data breach after an attacker accessed an enrollment system. The university said information was likely retrieved, potentially including names, bank details, health insurance information, and financial aid identifiers belonging to students.

AI THREATS

- Australia has [revealed](#) that an OpenAI agent gained unauthorized access to a government Medicare statistics portal while performing an internal research task. After encountering access restrictions, the agent found a workaround and accessed public and non-public files. Officials said no personal information was accessed, while OpenAI described the behavior as unintended.
- Researchers have [described](#) a financially motivated campaign using open-source AI agents to automate attacks against online retailers. The operators launched 105 attack projects between September 10 and 15 and compromised at least 27 organizations to varying degrees, stealing more than 600,000 valid payment card records.
- Researchers have [highlighted](#) CLOSEDQUORUM, a Windows malware that uses four commercial AI models to determine its next post-compromise action. The models can direct credential and cryptocurrency wallet theft, persistence, or process injection. Cisco Talos has not confirmed that the malware has been successfully deployed in real-world attacks.

VULNERABILITIES AND PATCHES

- Check Point has [observed](#) active exploitation of two critical pre-authentication vulnerabilities with CVSS scores of 9.8 - CVE-2026-85102 and CVE-2026-93616. The flaws affect Security Gateway and Security Management products and can enable remote code execution. Fixes for both vulnerabilities are available.
- F5 has [released](#) fixes for CVE-2026-94127, a critical heap-based buffer overflow vulnerability in BIG-IP Access Policy Manager with a CVSS score of 9.8. The actively exploited flaw allows unauthenticated remote code execution when affected systems are configured with an access policy and OAuth profile.

Check Point IPS provides protection against this threat (F5 BIG-IP Heap Overflow (CVE-2026-94127))

- WordPress has [fixed](#) CVE-2026-87902, a vulnerability affecting versions before 7.1.2 that allows unauthenticated attackers to include local PHP files outside active theme directories. Attackers have begun exploiting the flaw to write malicious PHP files and execute commands under specific server and theme configurations.

THREAT INTELLIGENCE REPORTS

- Researchers have [detailed](#) Storm-2570, a ransomware affiliate operating across Qilin, DragonForce, Anubis, and BERT ecosystems. The actor maintains consistent post-compromise tooling and infrastructure across deployments, including remote access, credential theft, lateral movement, security tampering, and cloud-based data exfiltration before ransomware deployment.
- Researchers [detailed](#) an INC ransomware intrusion affecting at least 175 endpoints. Particularly useful intelligence includes BYOVD-based security-tool disabling, AnyDesk, lateral movement through scheduled tasks, and a 17-day gap that researchers say could indicate separate initial-access and ransomware actors.
- Researchers have [tracked](#) an active TeamFiltration campaign targeting more than 5,700 Microsoft 365 accounts across 28 tenants in Latin America, particularly organizations in Chile. Seven service accounts were compromised, with subsequent activity including corporate VPN authentication attempts and access to Azure Portal and SharePoint Online.
- Researchers have [identified](#) Storm-3168, associated with JADEPUFFER, using compromised service principals to conduct destructive operations in Azure environments. The actor performed reconnaissance, credential collection, and bulk deletion attempts targeting storage accounts, SQL databases, Key Vaults, virtual machines, recovery protections, and other cloud resources.