CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The US Energy Department, including its National Nuclear Security Administration (NNSA), was reportedly breached as part of a Microsoft SharePoint vulnerability exploit. The breach was linked to a broader espionage campaign, that targeted government agencies via the CVE-2025-53770 flaw. The extent of the intrusion and data compromise at NNSA is unclear.
- American tech company Dell has confirmed a cyber attack that resulted in unauthorized access to its Customer Solution Centers product demonstration platform, with the threat actor exfiltrating 1.3 TB of primarily synthetic, publicly available, or Dell system data. The attack was carried out by the World Leaks extortion group, recently rebranded from Hunters International.
- Insurance company Allianz Life has suffered a data breach that resulted in the exposure of personally identifiable information belonging to the majority of its 1.4 million customers, financial professionals, and select employees through a compromised cloud-based CRM system. The breach, attributed to the ShinyHunters group, involved the use of social engineering to access sensitive data.
- Indian crypto company CoinDCX has confirmed a cyber attack that resulted in the theft of over $44 million worth of cryptocurrency from one of its internal operational accounts. The incident did not affect customer wallets or user data, as only the company's internal reserves in USDC and USDT stablecoins were stolen, traced to wallets holding $27.6 million and $16.2 million. No threat actor has claimed responsibility yet.
- A cyber attack targeting the AMEOS hospital network in Germany affected several hospital locations. While AMEOS has not confirmed whether sensitive medical data was exfiltrated, authorities, including data protection regulators, are currently investigating the scope of the breach.
- Radiology Associates of Richmond confirmed it has suffered a data breach that resulted in unauthorized access to sensitive information. The attack compromised the personal and medical data, including protected health information and Social Security Numbers, of approximately 1.4 million individuals. No threat actor has claimed responsibility yet.
- French national employment agency, France Travail, reported a data breach affecting around 340,000 job seekers after an attacker accessed its Kairos training platform via a compromised partner account. Exposed data includes names, contact details, and France Travail IDs.
- French defense firm Naval Group is investigating claims by a hacker who says they stole sensitive data on submarines and frigates, including source code. The threat actor allegedly leaked 30 GB and claims to hold up to 1 TB. Naval Group denies any system breach or ransom demand and is working with authorities to verify the claims.

VULNERABILITIES AND PATCHES

- Check Point Research updated on the wide exploitation wave using a critical zero-day remote code execution vulnerability (CVE-2025-53770), affecting on-premises Microsoft SharePoint servers. deserialization. On July 24, Check Point Research found wide exploitation of the CVE, with more than 4600 compromise attempts on over 300 organizations, worldwide. While the initial exploitation wave was focused and targeted mostly government, software and telecommunications sectors, now it also targets financial services, business services and consumer goods sectors.

  Check Point IPS provides protection against this threat *((Microsoft SharePoint Server Insecure Deserialization (CVE-2025-49704, CVE-2025-49704), Microsoft SharePoint Server Authentication Bypass (CVE-2025-49706, CVE-2025-53771))*

- Cisco has released a patch for a critical remote code execution vulnerability (CVE-2025-20281, CVE-2025-20282, CVE-2025-20337) in its Identity Services Engine (ISE). The flaw allows unauthenticated attackers to execute arbitrary code remotely via crafted messages. Cisco urges immediate updates, noting there are no workarounds and that the flaw could pose a severe risk if left unpatched.

- Sophos released a patch for 5 vulnerabilities ranging from severities of medium to critical (CVE-2025-6704, CVE-2025-7624, CVE-2025-7382, CVE-2024-13974, CVE-2024-13973). The flaws include arbitrary file writing vulnerability in the Secure PDF eXchange, SQL injection vulnerability in the legacy SMTP proxy, command injection and SQL injection vulnerabilities in WebAdmin that can lead to code execution, and a business logic vulnerability in the Up2Date component that can lead to remote code execution.

THREAT INTELLIGENCE REPORTS

- Check Point Research has unveiled that phishing attackers in Q2 2025 predominantly impersonated the technology sector, with Microsoft accounting for 25% of brand impersonation attempts, followed by Google (11%), Apple (9%), and Spotify (6%), the latter reentering the top 10 for the first time since 2019. The report details a major Spotify credential-harvesting campaign that replicated the platform's login page and a surge of over 700 Booking themed fake domains using personalized data to increase authenticity.

- Researchers have analyzed the resurgence of Lumma Stealer, an information-stealing malware that rapidly re-emerged with stealthier evasion tactics following its infrastructure takedown in May 2025. They detail how operators shifted from widespread Cloudflare abuse to alternative hosting providers, particularly Russian ones, and diversified their delivery methods to include fake cracked software, GitHub repositories with AI-generated content, compromised websites deploying fake CAPTCHA (ClickFix campaigns), and social media distribution.

- Researchers uncovered a new Iranian spyware dubbed "DCHsy" used in targeted attacks against Android users, primarily in the Middle East. The spyware can harvest sensitive data, including location, call logs, and microphone recordings.