cp<r>
CHECK POINT RESEARCH

# WEEKLY INTELLIGENCE REPORT

## TOP ATTACKS AND BREACHES

- Stellantis, Automotive maker giant which owns Citroën, FIAT, Jeep, Chrysler, and Peugeot, has suffered a data breach that resulted in exposure of North American customer contact information after attackers accessed a third-party platform tied to its Salesforce environment. ShinyHunters threat actor claims responsibility, stating they stole over 18 million Salesforce records.
- Volvo Group North America has confirmed a data breach that resulted in exposure of employee personal data after a ransomware attack on its third-party HR software provider Miljödata. Exposed information includes names and Social Security numbers. DataCarry ransomware group claimed responsibility and leaked the stolen data.
- Union County, Ohio was hit by a ransomware attack that resulted in theft of sensitive personal data including names, Social Security numbers, driver's license and passport numbers, financial account details, medical information, and fingerprint data. The breach impacted 45,487 individuals after attackers accessed the county network between May 6 and May 18, 2025.
- Las Vegas-based casino giant Boyd Gaming has been a victim of a cyberattack that resulted in the theft of employee information and data belonging to a limited number of other individuals from its internal IT system. The incident did not impact business operations or customer-facing systems, but sensitive employee data was compromised, with no specific details regarding the type or volume.
- South Korea's fifth-largest card issuer Lotte Card has experienced a data breach that resulted in the exposure of personal information belonging to around 3 million customers, including identification numbers, contact details, and sensitive financial data such as card numbers and verification codes. The breach affected approximately 2,700 files, of which only 56% were encrypted, and was linked to an unpatched flaw on a payment's server.
- Convenience store chain Circle K in Hong Kong was hit by a cyberattack that disrupted networks at nearly 400 stores, paralyzing e-payments, email, and loyalty systems. Customers couldn't use most services however it remains unclear if any personal data has been compromised.
- Kido, a UK nursery chain with 18 sites in London and abroad, was hacked by the Radiant group, which threatened to leak sensitive child and staff records. The attackers claimed to have stolen data on around 8,000 children and employees, including names, photos, addresses, contact details, and safeguarding notes. As proof, Radiant published profiles of 10 children online while demanding ransom. The Metropolitan Police and UK data regulators are investigating, with no arrests made and further leaks still possible.

## VULNERABILITIES AND PATCHES

- A patch was released for CVE-2025-26399, a critical unauthenticated remote code execution vulnerability affecting SolarWinds Web Help Desk up to version 12.8.7, caused by unsafe deserialization in the AjaxProxy component. It's the third fix after CVE-2024-28986/28988, which attackers had already exploited to run commands by bypassing earlier patches.
- Cisco patched two actively exploited zero-days in ASA and FTD software. CVE-2025-20333 allows authenticated remote code execution, and CVE-2025-20362, enables unauthenticated access to restricted endpoints. Both flaws have been targeted in the wild. A related critical issue, CVE-2025-20363, also enables unauthenticated RCE, and broad campaigns are hitting exposed devices.
- A newly disclosed flaw, CVE-2025-10184, in OnePlus OxygenOS allows any installed app to read SMS/MMS data and metadata without READ_SMS or user interaction via a Telephony provider permission bypass. The flaw is due to improperly exposed providers with unrestricted R/W access, including a blind SQL injection in ServiceNumberProvider's update method. Successful exploitation enables silent message exfiltration and effective bypass of SMS-based MFA.

## THREAT INTELLIGENCE REPORTS

- Check Point Research has uncovered a campaign by Iranian threat actor Nimbus Manticore targeting European defense and telecom sectors. Using spear-phishing and fake HR portals, the group deploys a DLL side-loading chain and obfuscated malware like MiniJunk and MiniBrowse. The tools employ valid signatures and advanced evasion, indicating nation-state capabilities.

  *Check Point Harmony Email & Collaboration, Harmony Endpoint and Threat Emulation provide protection against this threat*

- Check Point reveals over 4,300 domains registered ahead of FIFA World Cup 2026, mimicking FIFA, host cities, and event branding - peaking in August and September 2025. These domains, concentrated on registrars like GoDaddy and Namecheap, use synchronized DNS setups and templates for scams involving fake tickets, streams, and merchandise.
- Researchers report ongoing BRICKSTORM malware attacks on US legal, tech, and SaaS sectors, aimed at espionage and zero-day development. Tactics include Go-based proxy backdoors, credential theft (BRICKSTEAL) and VMware compromise.

  *Check Point Threat Emulation, Harmony Endpoint, IPS and AB blades provide protection against this threat*

- Researchers analyzed LockBit 5.0 ransomware variants for Windows, Linux, and ESXi, which use obfuscation, DLL reflection, and flexible command-line options. All versions avoid Russian systems, randomize file extensions, clear event logs, and target both physical and virtual environments. The ESXi variant specifically encrypts VMware, showing LockBit's cross-platform evolution.

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