CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Russia's largest airline Aeroflot has been attacked by pro-Ukrainian hacktivist groups, resulting in severe flight delays and major technical disruptions. The attackers claim to have exfiltrated databases containing flight history, workstation data, phone call recordings, and personnel monitoring information, allegedly wiping 7,000 servers totaling over 22TB of data.
- French telecommunications giant Orange has experienced a cyber attack that resulted in operational disruptions, primarily affecting French customers and certain business and consumer services. No evidence of exfiltration of customer or company data has been found, and the extent of compromised data remains unclear at this stage.
- The City of Saint Paul in Minnesota, US, has experienced a cyber attack that resulted in widespread disruptions to its digital services and critical municipal systems, including the unavailability of online payments and temporary outages in libraries and recreation centers. While emergency services were not affected, 311,000 residents experienced delays or interruptions in accessing city resources.
- Pi-hole, a popular network-level ad-blocker, has suffered a data breach that resulted in the exposure of donor names and email addresses due to security vulnerability in the GiveWP WordPress donation plugin. The incident impacted nearly 30,000 donors.
- Seychelles Commercial Bank has suffered a data breach that resulted in the exposure of 2.2GB of sensitive customer information, including personal data such as names, dates of birth, phone numbers, account types, balances, and records linked to government officials. The attack impacted both individual and business accounts, along with staff data.
- Russian pharmacy chains Stolichki and Neofarm have confirmed a cyberattack that resulted in hundreds of branch closures and disruption of payment systems, drug reservations, and customer loyalty programs, affecting access of thousands of patients to medication across Russia.
- Dating safety application Tea has experienced a data breach that resulted in the exposure of over 59 GB of sensitive user data, including approximately 72,000 images such as selfies, government IDs, and photos posted in the application, as well as a separate database containing 1.1 million private messages exchanged between members.
- The French National Museum of Natural History has confirmed a cyberattack that resulted in a significant disruption of its internal and collaborative research systems. The attack affected access to scientific databases and ongoing research, particularly impacting international projects and collaborations.

VULNERABILITIES AND PATCHES

- Researchers discovered a critical vulnerability in the AI-powered development platform Base44 that allowed unauthenticated access to private applications by abusing exposed endpoints. The flaw stemmed from improperly secured API which accepted arbitrary app_id values without requiring credentials or SSO verification. Successful exploitation could grant attackers unauthorized access to sensitive enterprise tools handling HR data, internal systems, or PII.

- Researchers have released a technical analysis of three critical vulnerabilities in SonicWall SMA100 series devices: CVE-2025-40596, CVE-2025-40597, and CVE-2025-40598. The flaws include a stack buffer overflow, a heap overflow, and an arbitrary memory write, all triggerable via unauthenticated HTTP POST requests to a CGI endpoint. Successful exploitation may lead to remote code execution with root privileges.

  Check point IPS provides protection against these threats *(SonicWall SMA100 Stack Overflow)*

- Enable Security identified a critical vulnerability (CVE-2025-53399) in the ngcp-rtpengine software that allows unauthenticated remote code execution via crafted WebSocket messages. The issue stems from a type confusion in processing control protocol messages, enabling attackers to overwrite function pointers and hijack execution flow. Exploitation results in full control over the rtpengine process, with a public proof-of-concept available.

THREAT INTELLIGENCE REPORTS

- Check Point Research released a comprehensive analysis of Q2 2025 ransomware trends, highlighting ecosystem fragmentation after several Ransomware-as-a-Service groups disruption, the operational use of AI as part of ransomware operations, and the emergence of cartel models such as DragonForce. Qilin ransomware was the leader in Q2 with new extortion tools and legal services, while groups like Global Group offered AI-powered negotiation as a RaaS feature. Payment rates dropped globally due to increased distrust in attackers and policy pressure, but ransom groups now focus more on data extortion and innovative reputation attacks.

- Check Point Research conducted a focused analysis of Storm-2603, one of the threat actors associated with recent ToolShell exploitations, which likely targeted organizations in Latin America throughout the first half of 2025, in parallel to attacking organizations in APAC. Storm-2603 utilizes a custom malware Command and Control framework dubbed internally by the attacker as “ak47c2” which includes HTTP-based and DNS-based clients.

- Check Point Research have uncovered a new malicious campaign dubbed "JSCEAL", targeting crypto applications users by leveraging malicious advertisements. The campaign uses fake applications impersonating popular cryptocurrency trading apps, with over 35,000 malicious ads served in the first half of 2025, generating millions of impressions in the EU alone. JSCEAL malware, which is delivered through sophisticated multi-layered infection flows, steals cryptocurrency-related data like credentials and wallets, making it a significant threat to crypto applications users.