May 5 – 11, 2025

CHECK POINT RESEARCH

# WEEKLY INTELLIGENCE REPORT

## TOP ATTACKS AND BREACHES

- The UK's Legal Aid Agency has suffered a cyberattack. The agency, which operates under the Ministry of Justice to provide billions in legal aid funding, has stated that financial information relating to legal aid providers may have been accessed by a third party.

- UK based Education giant Pearson disclosed it had suffered a cyberattack in January 2025. The breach exposed legacy data but did not impact employee information. Reportedly, the attack was enabled due to an exposed GitLab Personal Access Token found in a public configuration file, allowing threat actors access to its developer environment.

- Medical device manufacturer Masimo was hit a cyberattack in April, impacting its ability to process, manufacture and ship customer orders from certain manufacturing facilities. Company officials say the company has initiated an ongoing investigation and notified law enforcement.

- South African Airways experienced a cyberattack that disrupted its website, mobile app, and some internal systems. The incident was quickly contained, and core operations were unaffected. An investigation is underway to assess any data breaches.

- Coweta County's school district in Georgia, United States reported that it had suffered a cyberattack. According to the school district, some functionalities were disrupted by the attack. The school district has not confirmed whether personal data was exfiltrated in the attack.

- Framlingham College in Suffolk confirmed it was targeted by a significant cyberattack just days after similar incidents hit major UK retailers like Marks and Spencer, Co-op, and Harrods. The school swiftly isolated the issue and remains fully operational, working with cybersecurity experts to secure its systems. The National Cyber Security Centre is involved and has urged organizations to review IT help desk password reset processes to prevent further attacks.

- Several Indian defense websites, including those of Armoured Vehicles Nigam Limited (AVNL), Military Engineering Services (MES), and the Manohar Parrikar Institute for Defence Studies and Analyses (MP-IDSA), were reportedly hacked and defaced, possibly exposing sensitive data and personal information of defense personnel. The hacker group "Pakistan Cyber Force" claimed responsibility for the attacks, boasting of defacing AVNL's website and accessing confidential information.

- Pakistan-based Karachi Port Trust (KPT) claimed their account had been hacked, after having posted on X (formerly Twitter) that the port had suffered damage from an Indian Navy strike. While the port asserted that the port was safe and secure, this incident occurred amid escalating tensions between India and Pakistan, with both sides engaging in military actions and cyber-related activities.

## VULNERABILITIES AND PATCHES

- Google has published Android's May 2025 security bulletin. Among 47 vulnerabilities fixed, the patch addresses CVE-2025-27363, a local code execution that did not require execution privileges or any user interaction. According to Google, the critical flaw was actively exploited in the wild.
- Elastic has released a security advisory addressing a critical vulnerability in Kibana. The flaw, CVE-2025-25014, is a Prototype pollution vulnerability which allows attackers to gain arbitrary code execution via crafted HTTP requests to machine learning and reporting endpoints.
- WordFence disclosed an active exploitation of a critical vulnerability in OttoKit (SureTriggers) plugin for WordPress. The vulnerability, CVE-2025-27007, allows unauthenticated privilege escalation and received a 9.8 CVSS score. According to WordFence, vulnerability has been actively exploited during the last week.
- Researchers warn of active exploitation of Samsung MagicINFO 9 Server vulnerability CVE-2024-7399, following the publication of a PoC last week. MagicINFO 9 Server is a CMS used to manage digital signage displays, and the high-severity flaw allows arbitrary file writing.

## THREAT INTELLIGENCE REPORTS

- Check Point Research published its April 2025 Most Wanted Malware report. FakeUpdates (aka SocGholish) remained the most prevalent malware, impacting 6% of organizations worldwide. This downloader malware is associated with the Russian hacking group Evil Corp and is used to deliver various secondary payloads after the initial infection.
- Check Point Research highlights the DragonForce ransomware group, which has recently taken responsibility of the attacks on major UK retailers, M&S, Harrods and the Co-op. Formerly a hacktivist group, the cybercrime gang now operates a Ransomware-as-a-service model which allows affiliates to create their own ransomware 'brands'.

  *Check Point Harmony Endpoint and Threat Emulation provide protection against this threat*

- Check Point Researchers have uncovered a sophisticated phishing campaign that abuses Discord and targets crypto users, deploying the Inferno Drainer, a cryptocurrency stealer script. The threat actors use phishing and social engineering techniques to persuade victims to sign malicious smart contracts. In the past 6 months, more than 30,000 wallets were victimized by Inferno Draine,

  *Quantum Gateway and Harmony Browse provide protection against this threat*
  *(Trojan.UNKNOWN.InfernoDrainer.A)*

- CISA has issued a warning against recent low-level, unsophisticated attacks targeting ICS/SCADA systems in the United States critical infrastructure, specifically the Energy and Transportation sectors. Despite using only basic techniques, the attacks can cause operational disruptions in poorly configured environments.