cp<r>
CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Orange Group has confirmed a cyberattack on its Romanian branch, in which a hacker linked to the HellCat ransomware group stole 6.5GB of data over a month. The breach exposed 380,000 email addresses, internal documents, source code, invoices, contracts, and partial payment card details. While some data appears outdated, Orange assures that customer operations remain unaffected and is investigating the incident.

- The Medusa ransomware group has allegedly exfiltrated approximately 50TB of data from British healthcare provider HCRG Care Group's network, claiming full control over the healthcare provider's systems. Initially, Medusa reported stealing 2.275TB of data but later they revealed the breach was significantly larger, encompassing two HCRG subdomains. In response to HCRG's public statements minimizing the attack's impact, Medusa labeled the company as "liars" and provided evidence of the extensive data theft, including NTDS logs of the corporate network.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Ransomware.Wins.MedusaLocker.ta.; Ransomware.Wins.MedusaLocker.*; Trojan.WIN32.Medusalocker.*)*

- The Qilin ransomware group has claimed responsibility for a cyberattack on Lee Enterprises, a major US media company, disrupting operations and exfiltrating 350GB of data. The stolen data, which includes government ID scans, financial documents, contracts, and non-disclosure agreements, has been partially leaked, with the group threatening to release the full trove by March 5 if ransom demands are not met. Lee Enterprises reported the attack to the US SEC, detailing operational disruptions, including loss of access to internal systems, cloud storage, and corporate VPNs.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Ransomware_Linux_Qilin_A; Ransomware.Win.Agenda; Ransomware.Wins.Qilin)

- Texas-based DM Clinical Research fell victim to a cyber-attack which resulted in the exposure of over 1.6 million sensitive records, including personal and clinical data. The incident is attributed to a misconfigured, non-password-protected database that was publicly accessible.

- The Philippine Army has confirmed a cyberattack, following claims by hacking group Exodus Security that it breached army systems and accessed sensitive military and personal records of 10,000 service members. While the army stated that the intrusion was contained with no confirmed data theft, Exodus Security alleges it obtained names, addresses, medical records, and financial details.

- Cleveland Municipal Court has experienced a cyber incident that forced the shutdown of its internal systems and software platforms, leading to its closure since February 23. Officials have not disclosed the nature or scope of the attack but are working to secure and restore services.

VULNERABILITIES AND PATCHES

- A critical remote code execution vulnerability (CVE-2025-27364) was discovered in MITRE Caldera. This flaw resides in the dynamic agent compilation functionality of the server, specifically affecting the Manx and Sandcat agents. Exploitation allows remote attackers to execute arbitrary code on the server hosting Caldera by sending crafted web requests to the server's API used for compiling and downloading these agents. The vulnerability is particularly concerning because it can be triggered without authentication, and the necessary dependencies (Go, Python, and GCC) are typically present in default configurations.

  Check Point IPS provides protection against this threat *(MITRE Caldera Remote Code Execution (CVE-2025-27364))*

- Researchers have uncovered a critical SQL injection flaw (CVE-2025-26794) in Exim version 4.98 with SQLite hints database functionality. Attackers can insert malicious SQL code via specially crafted email transactions, leading to potential unauthorized access, data extraction, or full system compromise.

- A patch was released for a critical vulnerability (CVE-2025-1128) in the Everest Forms plugin (versions up to 3.0.9.4) that allows unauthenticated file upload, read, and deletion. Successful exploitation could lead to remote code execution, site takeover, and arbitrary file manipulation. The issue was resolved in version 3.0.9.5.

THREAT INTELLIGENCE REPORTS

- Check Point Research has uncovered a large-scale campaign exploiting over 2,500 variants of the vulnerable Truesight.sys driver (version 2.0.2), known as the RogueKiller Antirootkit Driver. Attackers leveraged a Windows policy loophole to load this legacy driver on the latest OS versions, bypassing security measures like the Microsoft Vulnerable Driver Blocklist. They distributed the driver through phishing methods, disguising malicious samples as legitimate applications, primarily targeting victims in China and other parts of Asia. The campaign's sophistication underscores the need for vigilant security practices and timely updates to security policies.
  Check *Point Threat Emulation and Harmony Endpoint provide coverage against this threat.*
  (Backdoor.Wins.Truesight.A, Gen.Rep.sys, Behavioral.Sideloading.p)

- Check Point Research has analyzed the evolution of hacktivist groups, which have shifted from minor website defacements and DDoS attacks to sophisticated operations resembling state-sponsored activities. To improve attribution, researchers are now employing language-based machine-learning models and linguistic analysis. By examining thousands of public messages from various hacktivist groups, this modern approach integrates traditional cyber threat intelligence with advanced technologies to uncover key topics, motivations, and potential connections, enhancing the accuracy of hacktivist group attribution.