CHECK POINT RESEARCH

# WEEKLY INTELLIGENCE REPORT

## TOP ATTACKS AND BREACHES

- The BlackSuit ransomware group has hit South Africa's National Health Laboratory Service (NHLS), disrupting lab result dissemination amid a Mpox outbreak. The actors have deleted system sections, including backups, forcing manual result communication. Despite the attack, labs continue processing samples, but system restoration timing is unknown.

  *Check Point Harmony Endpoint and Threat Emulation provide protection against this threat* *(Ransomware.Wins.BlackSuite, Ransomware.Wins.BlackSuit, Ransomware_Linux_BlackSuit)*

- Luxury fashion retailer Neiman Marcus reported a data breach impacting nearly 65,000 individuals, with the stolen data being sold on an underground forum by a hacker known as 'Sp1d3r'. The breached data includes names, contact details, birth dates, and gift card numbers. The incident is part of broader Snowflake-related cyber-attacks affecting various organizations.

- A data breach initially claimed to involve the US Federal Reserve, has been revealed to be to Evolve Bank & Trust. LockBit ransomware group threatened to release 30 TB of sensitive banking information unless a ransom was paid. The leaked data reportedly includes account numbers, balances, and personal information of various fintech customers.

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

- Brain Cipher ransomware has attacked Indonesia's National Data Center, encrypting government servers and disrupting services like immigration and passport control. The attackers demanded $8 million, which the government will not pay. Brain Cipher uses a modified version of the LockBit 3.0 encryptor and has launched a data leak site for double extortion.

- TeamViewer has confirmed a hack by the state-sponsored group APT29 (Cozy Bear), linked to Russian intelligence. The breach involved unauthorized access to TeamViewer’s systems, yet it is believed that the attackers did not reach the company's product environment or customer data.

- Ukrainian military intelligence and affiliated hacker groups have targeted Russian-operated internet providers in Crimea with DDoS attacks, causing significant service disruptions. These DDoS attacks primarily affected the local provider Miranda Media, leading to intermittent internet availability and impacting crucial communication channels in the region.

- Dordt University has been hit by a data breach conducted by the BianLian group, resulting in the exfiltration of 3TB of sensitive documents. The attack compromised a vast amount of personal and institutional data, posing significant risks to affected individuals and the university’s operations.

  *Check Point Threat Emulation provides protection against this threat* *(Ransomware.Wins.BianLian)*

## VULNERABILITIES AND PATCHES

- Two critical vulnerabilities in MOVEit Transfer and MOVEit Gateway have been disclosed, affecting the MOVEit Transfer SFTP service and the SFTP feature of MOVEit Gateway. The vulnerabilities (CVE-2024-5805 and CVE-2024-5806) could allow unauthorized access and potential credential theft. Vendor-provided patches for both are available and urgently recommended, with an exploit (PoC) available for CVE-2024-5806.

  *Check Point IPS provides protection against this threat* *(Progress MOVEit Transfer Authentication Bypass (CVE-2024-5806))*

- GitLab has issued patches for 14 security vulnerabilities, including a critical flaw (CVE-2024-5655) that could allow malicious actors to execute CI/CD pipelines under another user's identity. This flaw, with a CVSS score of 9.6, affects various versions of GitLab Community and Enterprise Editions.

- Researchers have identified a severe Remote Code Execution vulnerability (CVE-2024-37032) in the Ollama AI infrastructure project. This vulnerability, due to improper input validation, could allow arbitrary file writes and remote code execution.

- Researchers have discovered flaws in a $100K Emerson Rosemount 370XA gas chromatograph, commonly used in industrial environments. These could allow manipulations of the device remotely without physical access, potentially leading to inaccurate readings and operational disruptions.

## THREAT INTELLIGENCE REPORTS

- Researchers have analyzed Chamelgang, a suspected Chinese APT group, targeting critical infrastructure globally using CatB ransomware for financial gain and disruption. Their campaigns affected sectors like healthcare and aviation, with notable incidents involving AIIMS in India and the Presidency of Brazil. Additionally, Chamelgang leveraged off-the-shelf tools like BestCrypt and BitLocker, impacting various industries, primarily in the US manufacturing sector.

  *Check Point Harmony Endpoint and Threat Emulation provide protection against this threat* *(APT.Wins.ChamelGang, Ransomware.Wins.Catb.ta, Ransomware.Win.CatB)*

- Researchers have identified threat actors exploiting publicly available Cobalt Strike Malleable C2 profiles to conduct cyber-attacks. These profiles, hosted on public code repositories, allow attackers to evade detection by customizing Cobalt Strike's communication methods. The analysis revealed multiple Cobalt Strike samples utilizing modified profiles.

- Researchers detail the utilization of Craxs Rat malware in various phishing schemes targeting Singapore from April 2023 by a suspected Chinese speaking threat actors. The RAT was observed exploiting fake Android apps to compromise banking credentials and control devices. Derived from Spymax and evolved into Craxs Rat by the threat actor "EVLF," the malware was distributed via counterfeit apps mimicking legitimate brands. This RAT facilitates complete remote access, with capabilities expanded in its versions sold through EVLF's Telegram channel.