cp<r>
CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Mizuno USA, giant sports equipment manufacturer, has confirmed a cyber-attack that resulted in the theft of personal information from its network between August and October 2024. The data breach included names, Social Security numbers, financial account information, driver's license details, and passport numbers. The BianLian ransomware gang claimed responsibility for the attack.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Ransomware.Wins.BianLian.ta.; Ransomware.Wins.BianLian; Backdoor.Wins.BianLian; HackTool.Wins.BianLian)*

- El Cruce hospital in Buenos Aires, Argentina, suffered a ransomware attack by the Medusa ransomware group. The group launched a significant attack on the hospital's IT networks and now threatens to disclose 760GB of data - including patient information - unless it is paid $200K in BTC.

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

- New York Blood Center Enterprises was hit by a ransomware attack on January 26th, which affected their IT systems. The blood center has taken its network offline and stated that there is no specific timetable for system restoration, and blood donations are delayed.

- Indian tech giant Tata Technologies has experienced a ransomware attack that resulted in temporary suspension of some IT services while core client delivery systems remained unaffected. No threat actor has claimed responsibility for the attack, and it remains unclear if any data was stolen.

- Japanese tablet manufacturer Wacom suffered a cyber-attack likely resulting in customer payment card theft from its online checkout between November 28, 2024, and January 8, 2025. The attack used malicious code to steal payment card information during transactions on Wacom's website.

- US healthcare services provider Community Health Center (CHC) has been a victim of a data breach that exposed the sensitive personal and health information of over one million individuals. The breach, which occurred on January 2, 2025, involved unauthorized access to CHC's systems, compromising personal details, Social Security numbers, medical information, and financial data.

- The Iranian hacktivistic group Handala exploited the emergency systems of various Israeli kindergartens and educational institutions to broadcast alarm sirens and various terrorism supportive songs. The group claimed to have targeted Maagar-Tec, an Israeli electronics firm that operates panic button systems in schools.

- UK-based engineering giant Smiths Group disclosed a cyber-attack involving unauthorized access to its systems. The company has not disclosed when the attack occurred or if any data was exfiltrated. No threat actor has claimed responsibility yet.

© 2025 Check Point Software Technologies Ltd. All Rights Reserved

VULNERABILITIES AND PATCHES

- A publicly accessible ClickHouse database belonging to the new Chinese AI engine DeepSeek was found, exposing over a million lines of log streams. The data included highly sensitive information, such as chat history, API secrets, and backend details. This exposure granted full control over database operations and potential privilege escalation within DeepSeek's environment due to the absence of authentication or defense mechanisms. The issue was fixed following its disclosure.

- A critical-severity vulnerability (CVE-2024-55591) in Fortinet's FortiOS was reported as actively exploited in the wild. The flaw, an Authentication Bypass Using an Alternate Path or Channel vulnerability, allows a remote attacker to gain super-admin privileges via crafted requests to Node.js websocket module.

  Check Point IPS provides protection against this threat *(Fortinet Multiple Products Authentication Bypass (CVE-2024-55591))*

- Critical vulnerabilities in Node.js versions (v18.x, v20.x, v22.x, v23.x) could result in data theft, DoS, and system compromise. Notable vulnerabilities include CVE-2025-23087 through CVE-2025-23089, affecting various versions with issues such as worker permission bypasses, path traversal, and memory leaks. These allow remote attackers to potentially gain unauthorized access, execute arbitrary code, and compromise systems.

THREAT INTELLIGENCE REPORTS

- Xloader malware, a successor to Formbook known for stealing information from web browsers, email clients, and FTP applications, employs enhanced obfuscation and encryption techniques like runtime code encryption and NTDLL hook evasion. It establishes persistence by copying itself to specific directories, modifying Windows registry entries, and using process injection.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat
  (Trojan.Win.Xloader; Trojan.Win.Xloader.ja; Trojan.Wins.Xloader.tayc; Trojan.Wins.Xloader.ta.)*

- A recently discovered ransomware called Windows Locker, first observed on GitHub in December 2024, targets victims by encrypting files and modifying registry keys for persistence. It prevents standard recovery methods and uses AES encryption techniques to encrypt data. Additionally, Windows Locker deletes shadow copies, leaving users unable to retrieve manipulated files.

- A technical analysis of Arcus Media ransomware shows it elevates privileges using the ShellExecuteExW API without administrative access and maintains registry-based persistence. It halts critical processes like SQL servers and email clients via the CreateToolhelp32Snapshot API, encrypts files with the ChaCha20 cipher adding "[Encrypted].Arcus" to filenames, and hinders recovery by deleting shadow backups, disabling system recovery, and clearing event logs.

© 2025 Check Point Software Technologies Ltd. All Rights Reserved