CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The second-largest bar association in the US, The State Bar of Texas, has experienced a ransomware attack that resulted in unauthorized access to its network, exposing sensitive member information including full names and legal case documents. The INC ransomware gang claimed responsibility for the attack and has already leaked samples of stolen files.

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

- Port of Seattle has disclosed a ransomware attack from 2024 that resulted in a data breach exposing personal information of approximately 90,000 individuals, including names, dates of birth, Social Security numbers, driver's license numbers, and some medical information. The breach affected data from employees, contractors, and parking records, with about 71,000 affected individuals residing in Washington state. The attack was attributed to the Rhysida ransomware operation.

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

- Minnesota native tribe, The Lower Sioux Indian Community, has been a victim of a ransomware attack that resulted in widespread disruptions to its healthcare, government, and casino systems. The incident caused outages in communications, digital gaming, and hotel booking services. The attack was claimed by the RansomHub gang.

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

- Britain's Royal Mail was allegedly hit by a data breach that resulted in the exposure of 293 folders and 16,549 files containing personal data such as names, physical addresses, phone numbers, and package details. The breach occurred through Spectos, a compromised German logistics management supplier, with a reported 144GB of data offered for sale by the GHNA hacking group.

- American dental service provider Chord Specialty Dental Partners has suffered a cyber-attack that resulted in unauthorized access to several employee email accounts between August 19 and September 25, 2024. The attackers accessed sensitive information, including names, birth dates, addresses, bank account data, driver’s license numbers, Social Security Numbers, health insurance information, and medical records.

- Giant car-rental company Europcar Mobility Group confirmed a cyber-attack that allegedly breached its GitLab repositories, leading to the theft of source code for its Android and iOS applications and SQL backups. Dark web forum user claimed to have exposed over 9,000 SQL files and 269 .ENV files containing personal data such as names and email addresses, affecting between 50k to 200K clients.

VULNERABILITIES AND PATCHES

- Two vulnerabilities (CVE-2024-20439 and CVE-2024-20440) in Cisco Smart Licensing Utility are currently being exploited in the wild. CVE-2024-20439, an undocumented static administrative credential, enables unauthenticated attackers to gain full administrative privileges via the CSLU API, while CVE-2024-20440, caused by excessive debug log verbosity, exposes API credentials through crafted HTTP requests. Both flaws, rated 9.8, can lead to complete system compromise.

  Check Point IPS provides protection against this threat *(Cisco Smart Licensing Utility Use of Hard-coded Credentials (CVE-2024-20439))*

- Researchers found active exploitation of CVE-2025-22457, a buffer overflow flaw in Ivanti Connect Secure VPN appliances version 22.7R2.5 and earlier, by the suspected China-nexus espionage actor UNC5221. Successful exploitation allows remote code execution, leading to the deployment of malware families TRAILBLAZE and BRUSHFIRE, as well as the previously reported SPAWN ecosystem.

  Check Point IPS provides protection against this threat *(Ivanti Buffer Overflow (CVE-2025-22457))*

- Apple patched three zero-day vulnerabilities (CVE-2025-24085, CVE-2025-24200 and CVE-2025-24201) affecting older iOS and macOS devices. CVE-2025-24085, a use-after-free bug in Core Media (CVSS 7.3), enables privilege escalation; CVE-2025-24200, an Accessibility authorization flaw (CVSS 4.6), disables USB Restricted Mode; and CVE-2025-24201, an out-of-bounds write in WebKit (CVSS 8.8), permits escape from the Web Content sandbox.

THREAT INTELLIGENCE REPORTS

- Check Point Research found that PDFs, used in 22% of malicious email attachments, are increasingly weaponized to conceal malicious payloads. Threat actors exploit the PDF format's complexity—leveraging obfuscation techniques such as benign redirect services, QR codes, and static analysis evasion—to embed hidden links and code, bypassing conventional detection mechanisms.

- Researchers warn of a fileless cryptominer campaign targeting misconfigured and publicly exposed PostgreSQL servers. The threat actor, dubbed Jinx-0126, exploits weak, guessable credentials to deploy XMRig-C3 cryptominers filelessly and assigns a unique mining worker to each victim.

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

- Researchers report on a malicious zoom installer leading to a BlackSuit ransomware infection. The attackers used loaders and malware (d3f@ckloader, IDAT loader, SectopRAT, Cobalt Strike, Brute Ratel, QDoor) for lateral movement, exfiltrating data and deploying ransomware over nine days.

- Researchers have uncovered a malicious Python package, named 'disgrasya', on PyPI that automates carding attacks targeting WooCommerce stores via CyberSource payment gateways. The package, introduced in version 7.36.9 and downloaded over 34,000 times, simulates legitimate checkout flows to test stolen credit cards and facilitate automated fraud.