January 20 - 26, 2025

CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Stark Aerospace, a US-based manufacturer specializing in missile systems and UAVs, contractor of the US Military and the Department of Defense (DoD), has been targeted by the INC ransomware group. The attackers claim to have exfiltrated 4TB of data, including design documentation, source codes, firmware for various UAVs, contracts with the DoD, supply chain information, and personal data of company instructors.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat (Ransomware.Wins.INC.A)

- TalkTalk, a UK telecommunications company, has suffered a data breach that resulted in the exposure of customer information, including names, email addresses, IP addresses, and phone numbers. A threat actor named "b0nd" claimed on a hacking forum to have stolen data affecting approximately 18.8 million current and former customers.
- ICICI Bank, an Indian multinational bank, has allegedly been a victim of a cyber-attack claimed by the BASHE ransomware group (also known as APT73 or Eraleig). The group has claimed to breach the bank's database, and set an initial ransom deadline of January 24, 2025, threatening to expose sensitive data. ICICI Bank has not confirmed the breach, and legitimacy of the claims is being questioned with the deadline pushed to January 31, with no files leaked.
- Singapore-based cryptocurrency platform Phemex has experienced a cyberattack resulting in the theft of over $69 million in digital assets, including ETH, Bitcoin, and Binance Coin. The company has paused certain operations and is manually reviewing withdrawal requests while working on a compensation plan for affected users.
- Conduent, a major American business services provider and government contractor, has confirmed that a recent service outage was due to a cybersecurity incident. The disruption affected clients across multiple US states, including the Wisconsin Department of Children and Families.
- Rostelecom, a major Russian telecommunications provider, is investigating a suspected cyberattack on one of its contractors after the hacker group Silent Crow claimed to have leaked company's data. The leaked information reportedly includes thousands of customer emails and phone numbers. The contractor is responsible for maintaining Rostelecom's corporate website and procurement portal, which were targeted in the attack. Initial findings suggest no leak of highly sensitive personal data.
- West Virginia's Harrison County school district has disclosed that it had suffered a cyber-attack. According to the district, it had shut down its network upon discovering the attack. The district has not provided information on whether any data was exfiltrated.

VULNERABILITIES AND PATCHES

- CISA and FBI have identified exploitation of four vulnerabilities in Ivanti Cloud Service Appliances (CSA): an administrative bypass vulnerability (CVE-2024-8963), an SQL injection vulnerability (CVE-2024-9379); and remote code execution vulnerabilities (CVE-2024-8190 and CVE-2024-9380). Threat actors leveraged two distinct exploit chains to gain initial access, execute remote code, exfiltrate credentials, and implant webshells on victim networks. Affected versions include Ivanti CSA 4.6 (end-of-life) and earlier 5.0.1 versions. The vulnerabilities were actively exploited as zero days and were added to CISA's Known Exploited Vulnerabilities Catalog.

  Check Point IPS provides protection against this threat *(Ivanti Cloud Services Appliance Path Traversal (CVE-2024-8963), Ivanti Cloud Services Appliance SQL Injection (CVE-2024-9379), Ivanti Cloud Services Appliance Command Injection (CVE-2024-8190), Ivanti Cloud Services Appliance Command Injection (CVE-2024-9380))*

- SonicWall has disclosed a critical deserialization vulnerability (CVE-2025-23006) in SMA1000 Appliance Management Console (AMC) and Central Management Console (CMC). The flaw allows remote unauthenticated attackers to execute arbitrary OS commands. It has reportedly been exploited as a zero-day in attacks, targeting firmware versions up to 12.4.3-02804.

- Oracle's January 2025 Critical Patch Update addresses 520 vulnerabilities across various products. Among these, 55 vulnerabilities have a CVSS v3 score of 9.8 and 14 are exploitable remotely without authentication. Affected products include Oracle Database Server, Oracle Communications, and Oracle Fusion Middleware.

THREAT INTELLIGENCE REPORTS

- Check Point has released its Brand Phishing Report for Q4 2024, highlighting that Microsoft continues to be the most impersonated brand in phishing attacks, accounting for a significant percentage of attempts. Notably, LinkedIn has reentered the top ten list, indicating a resurgence in phishing campaigns targeting social media platforms. The technology sector remains the most imitated industry, followed by social networks and banking.

- FBI has issued a warning about North Korean IT workers exploiting remote work opportunities to steal source code and extort employers. These state-sponsored individuals deceive companies by posing as independent contractors and using their access to extract information. The FBI identifies these actions as part of a larger effort to generate revenue for the North Korean government.

- Researchers have identified ransomware affiliates Hellcat and Morpheus deploying identical malicious payloads despite operating under different branding. Both groups employ sophisticated techniques for data encryption and exfiltration, targeting organizations across multiple industries. The findings suggest a shared codebase or toolkit used by these affiliates.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat *(RAT.Win.Morpheus.A, RAT.Win.Morpheus.B)*