Check Point Research
WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- In a joint statement with Germany and NATO, the Czech Republic uncovered a cyber espionage campaign by Russian state affiliated actor APT28. These cyber-attacks targeted Czech institutions using a new vulnerability in Microsoft Outlook. APT28, linked to Russian military intelligence, is involved in a long-term espionage campaign across Europe, compromising political and state institutions.
- Dropbox Sign eSignature platform suffered a breach where hackers accessed customer emails, usernames, phone numbers, hashed passwords, API keys, OAuth tokens, and MFA keys. The breach did not affect customer documents or other Dropbox services.
- American healthcare provider Kaiser Permanente disclosed a data security incident affecting about 13.4 million people due to third-party trackers on its websites and mobile applications. These trackers, now removed from the organization's platforms, may have transmitted personal information of patients to vendors like Google, Microsoft Bing and X (formerly Twitter).
- A cyberattack targeted Kansas City's Scout System, disabling real-time weather and traffic information services. This system, managed by the Departments of Transportation of both Missouri and Kansas, experienced system-wide outages affecting traffic cameras and digital message boards, impacting critical communications during severe weather conditions.
- London Drugs, a Canadian retail pharmacy chain, experienced a significant cybersecurity incident that forced the temporary closure of several stores. The attack, which involved unauthorized access to their systems, prompted an immediate response prevent further unauthorized access.
- Panda Restaurant Group, the largest Asian-American restaurant chain in the United States, suffered a data breach, affecting the personal information of associates. The breach, detected on March 10th, 2024, involved unauthorized access to corporate systems between March 7-11, compromising details like driver's license numbers.
- The Hôpital de Cannes (CHC-SV) in France was targeted by the Lockbit ransomware gang in an attack that caused severe disruptions to its operations. The attack forced a shutdown of hospital's systems and rescheduling of non-emergency procedures and appointments. Following a refusal to pay a ransom demand, the ransomware group published confidential data stolen from the hospital.

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

VULNERABILITIES AND PATCHES

- Four critical vulnerabilities were discovered and patched in HPE Aruba devices, which could enable remote code execution. These vulnerabilities (CVE-2024-26304, CVE-2024-26305, CVE-2024-33511, CVE-2024-33512), found in ArubaOS, impact various networking devices managed by Aruba Central.
- Team82 researchers have uncovered a deserialization vulnerability (CVE-2022-23450, CVSS v3 score of 9.8) in Siemens SIMATIC Energy Manager, a critical infrastructure component. The vulnerability allows remote code execution that could enable attackers to gain control over affected systems. A proof of concept is available, with relevant patches in place.
- CISA reported multiple severe vulnerabilities in CyberPower's PowerPanel software. These vulnerabilities, exploitable remotely with low complexity, could lead to authentication bypass, administrator privilege acquisition, JWT token forgery, arbitrary file writing and code execution, SQL injection, and more. Affected versions are PowerPanel 4.9.0 and earlier.
- Researchers have identified a critical vulnerability, CVE-2024-27322, in the R programming language that allows arbitrary code execution through deserializing untrusted RDS or RDX files. This flaw affects the readRDS function, posing a significant supply chain attacks risk, potentially compromising systems by executing malicious code during data serialization processes.

THREAT INTELLIGENCE REPORTS

- Check Point reports an increase in phishing attacks where scammers impersonate Shein to steal user credentials. Over 1,000 such fraudulent emails were identified, featuring misleading subject lines and links to credential harvesting sites, exploiting Shein's popularity and customer excitement.
- Researchers have identified a malware campaign named Mal.Metrica that exploits vulnerabilities in popular WordPress plugins to redirect users to scam sites. The malware injects fake verification prompts on compromised websites, tricking users into initiating redirects. This campaign has compromised over 17K websites by targeting vulnerabilities in plugins like tagDiv Composer and Popup Builder.
- Researchers have uncovered the activities of the Muddling Meerkat APT, seemingly a China affiliated nation state actor. Findings show that this group manipulates China's Great Firewall for its espionage operations, focusing on surveillance and data exfiltration without detection. Their tactics include the use of malware and network intrusion to gather intelligence and monitor communications.
- A new report highlights multiple campaigns by Iran-linked group APT42 in the past year. The threat actor used phishing emails from spoofed “trusted” accounts, such as journalists, legitimate services, and businesses to gain access to cloud credentials. The threat actors also used two separate backdoors, dubbed NETCURL and TAMECAT, as part of their campaigns.