TOP ATTACKS AND BREACHES

- The BlackSuit ransomware group has disrupted operations at CDK Global, a significant provider of IT and digital marketing solutions to the automotive industry, targeting their SaaS platforms across the United States and Canada. This incident led to significant operational disruptions, impacting vehicle sales and dealer services. The BlackSuit ransomware, introduced in May 2023, is reportedly a continuation or new version of what was previously known as the Royal ransomware operation.

- Maxicare, a major Philippines-based health maintenance organization, has reported a significant data breach to the National Privacy Commission (NPC), revealing unauthorized access to sensitive customer data. The breach potentially exposes personal details of numerous insured members, raising serious privacy and security concerns.

- Major manufacturer Crown Equipment is handling a cyber-attack that led to a shutdown of its operations, impacting forklifts functionality and manufacturing globally. The specifics of the shutdown, such as the attack methods, data impacted and the involved threat actor responsible for this incident, have not been disclosed.

- The Association of Texas Professional Educators (ATPE) has disclosed a data breach that resulted in the exposure of personal information of more than 400K members of the organization, employees, and their dependents. The compromised data includes Social Security numbers, dates of birth and addresses. For employees of ATPE only, the data breach also included passport numbers, driver's license numbers, financial information, and medical records. No threat actors have claimed responsibility yet.

- ANSSI has reported that Nobelium, linked to Russia's SVR, has targeted French diplomatic interests through phishing and attempts to install Cobalt Strike. These efforts include compromises of French public organizations and embassies, though significant breaches were prevented by vigilant staff.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(APT.Win.APT29; APT.Wins.Nobelium)*

- UK based Total Fitness has suffered a data breach that resulted in the exposure of close to 500,000 individuals' photos, with no password requirement for access. The incident involved an open and insecure Amazon S3 bucket. The fitness company acknowledged the incident and secured the data, but the full extent of the breach's impact remains unclear.

VULNERABILITIES AND PATCHES

- A critical SQL injection vulnerability in the pkfacebook module for PrestaShop (CVE-2024-36680) has been actively exploited to deploy card skimmers on e-commerce sites. This flaw allows attackers to manipulate database queries and steal credit card information from unsuspecting users.
- Researchers have identified several critical vulnerabilities in VMware vCenter Server, including heap-overflow and local privilege escalation issues (CVE-2024-37079, CVE-2024-37080, and CVE-2024-37081). These flaws can allow attackers to execute remote code or escalate privileges to root, impacting versions 7.0 and 8.0 of the software.
- D-Link has published an advisory addressing a high severity vulnerability (CVE-2024-6045) affecting many of its wireless router products. The routers contain an undisclosed factory testing backdoor, which allows adjacent network attackers to gain admin credentials or force Telnet access to a specified URL.

THREAT INTELLIGENCE REPORTS

- Check Point Research has analyzed Rafel RAT, an open-source remote administration tool that enables espionage and ransomware attacks against Android devices. This malware has been employed in various campaigns, notably targeting high-profile organizations, including in the military sector. Most of the targeted victims were from the United States, China, and Indonesia. The tool's capabilities include data exfiltration, surveillance, and full device control, leading to significant privacy and security breaches.

  Check Point's Harmony Mobile provides protection against this threat.

- Researchers have uncovered a long-running espionage campaign targeting telecom operators in Asia using tools linked to Chinese espionage groups. The campaign involved deploying backdoors like Coolclient, Quickheal, and Rainyday for credential theft and surveillance, affecting telecom operators and related sectors since at least 2021.
- Researchers have shared a deep dive into UNC3886, a suspected China-nexus cyber espionage actor, revealed the use of multiple zero-day vulnerabilities and advanced malware to target global strategic organizations. Their techniques included exploiting flaws in VMware and Fortinet products, deploying rootkits like REPTILE and MEDUSA for persistence, and using public platforms for C&C.
- Researchers have analyzed a campaign by the Void Arachne threat group, targeting Chinese-speaking users with malware-infused MSI files. These files, posing as legitimate software, include malicious Winos payloads capable of system compromise. The campaign leverages SEO poisoning and social media to spread, exploiting increased interest in VPN technologies in China.