TOP ATTACKS AND BREACHES

- Australian electronic prescriptions provider MediSecure suffered a significant ransomware attack, leading to widespread disruptions and data breaches. The impact of the attack has been profound, broadly affecting healthcare data broadly in the country.
- WebTPA, an American healthcare management and administrative services provider, disclosed a data breach affecting nearly 2.5 million individuals. The breach, detected on December 28, 2023, involved unauthorized access to personal information between April 18 and April 23, 2023. While sensitive data like Social Security numbers was compromised, financial and medical information remained unaffected.
- Russia affiliated hacktivist group has defaced hundreds local and regional British newspaper websites of the American-owned and the second-largest publisher of regional and local newspapers in the United Kingdom, Newsquest Media Group. The group has used the platforms to publish the message "PERVOKLASSNIY RUSSIAN HACKERS ATTACK".
- Rockford public school district in Michigan was forced to shut down its computers, internet services and phones following a ransomware attack. Ransomware group INC Ransom has claimed responsibility in a ransom note left on printers.
- MLS Chicago Fire Football Club has reported that it had suffered a security breach. According to the club, a cyberattack late last year has led to the disclosure of personal information. The information included Social Security numbers, driver's licenses and passports, as well as medical and financial information.
- The city of Helsinki, Finland, has disclosed that a breach of its Education Division has resulted in the leak of personal information of all city personnel, as well as students and their guardians. According to the city's statement, the exfiltrated data includes tens of millions of files.
- Japanese auto maker Nissan has said that personal information of more than 53K of its current or former American employees has been leaked in the breach that took place late last year. According to the company, the information includes the employees' Social Security numbers.
- The FBI and DOJ have successfully seized the website and telegram channel in services of BreachForums, a known cybercrime forum used to trade and sell hacked or stolen data. This operation disrupted a major cybercrime hub that facilitated various illegal activities, including the exchange of sensitive information and illicit services among hackers.

VULNERABILITIES AND PATCHES

- Microsoft and Adobe released their May 2024 Patch Tuesday, with Microsoft addressing 67 vulnerabilities and Adobe addressing 37 vulnerabilities. Microsoft's release included patches for three zero-day vulnerabilities, confirmed to be exploited in the wild (CVE-2024-30051, CVE-2024-30040 and CVE-2024-30046). In Adobe's release, 26 of the vulnerabilities were given critical severity ratings, and can possibly lead to arbitrary code execution.

- A critical remote code execution vulnerability (CVE-2024-25641) has been disclosed in popular network monitoring tool Cacti. The vulnerability allows an attacker to use the Packet Import feature to execute arbitrary PHP code on the web server.

  Check Point IPS provides protection against this threat *(Cacti Arbitrary File Upload (CVE-2024-25641))*

- Google has shared a security update addressing a high severity Chrome vulnerability (CVE-2024-4761), which could allow a remote attacker to perform an out-of-bounds memory write. Google acknowledges that an exploit for the vulnerability exists in the wild.

- Broadcom has published a security update addressing 4 vulnerabilities in VMware Workstation and Fusion. The most severe vulnerability (CVE-2024-22267) is a critical use-after-free vulnerability which could lead to remote code execution.

THREAT INTELLIGENCE REPORTS

- Check Point Research reports on malware campaigns using malicious PDFs, involving exploitation of Foxit PDF Reader. The exploitation takes advantage of the flawed design of Warning messages in Foxit Reader which provide as default options that are the most harmful. Once a user proceeds twice with the default option, the exploit triggers, downloading and executing a payload from a remote server.

  Check Point Threat Emulation, Harmony Endpoint, and Harmony Mobile Protect provide protection against this threat *(Exploit.Wins.FoxitExploit.ta.A)*

- Check Point has shared data showing the escalating threat of malicious PDF attachments in emails, which in the last month comprise approximately 75% of all malicious files, with healthcare as the most targeted sector. Hackers exploit PDFs by embedding URLs and scripts to bypass traditional security measures, posing a significant challenge for cybersecurity analysts.

- Researchers have identified an espionage campaign by the Turla APT group targeting unnamed European Ministry of Foreign Affairs. The campaign involved two custom backdoors, LunarWeb and LunarMail, utilizing sophisticated techniques like steganography and Lua scripting, first observed in 2020 and linked to Russian state interests.