# TOP ATTACKS AND BREACHES

- Colorado State University (CSU) has been affected by ransomware gang Cl0p's MOVEit Managed File Transfer attack. The threat actors compromised the University's service vendors, which resulted in an unauthorized access to personal information of students and employees dating back to at least 2021. The exposed data includes names, date of birth, student or employee identification numbers, social security number, and other demographic information.

  *Check Point IPS blade, Harmony Endpoint and Threat Emulation provide protection against this threat ((Progress MOVEit Transfer Multiple Vulnerabilities); Webshell.Win.Moveit, Ransomware.Win.Clop, Ransomware_Linux_Clop; Exploit.Wins.MOVEit)*

- The American-Singaporean gaming hardware giant Razar has confirmed a data breach that affected its Razer Gold payment system. The breach was claimed by dark web forum user that allegedly stole the source code, database, encryption keys, and backend access logins for the company's main website. The threat actor demanded more than $130K in cryptocurrency for the data.

- The American hospital operator HCA Healthcare has disclosed a data breach that possibly affected data of 11M patients. The breach includes patients' personal information such as names, home addresses, dates of birth, appointments details and more. HCA confirms that the breach didn't include clinical or payment information. This breach is considered to be one of the largest breaches of health data in 2023.

- Ventia, a major essential infrastructure services provider based in Australia and New Zealand, shared that it has taken some of its systems offline due to a cyberattack. The company didn't share details on the attack, but its decision to shut down its systems is a characteristic response to ransomware attacks.

- The Chinese affiliated group Storm-0558 has breached the email systems of approximately 25 organizations including government agencies as well as accounts of individuals likely associated with those agencies. Microsoft shares further details on the espionage campaign, including analysis of the threat actor's techniques, tools, and infrastructure.

- The City of Hayward, California, has suffered a ransomware attack and as a precaution turned off access to the city's public website and other services. The City says that it has no evidence of a breach of personal information. No ransomware group has claimed responsibility for the attack yet.

- The Republic of Trinidad and Tobago, the southernmost island country in the Caribbean with more than 1.4M population, has been a victim of a cyber-attack that impacted the country's Office of the Attorney General and Ministry of Legal Affairs (AGLA).

# VULNERABILITIES AND PATCHES

- Check Point Research in collaboration with Claroty Team82 have uncovered a few major security vulnerabilities in the QuickBlox platform architecture that, if exploited, could allow threat actors to access tens of thousands of applications' user databases and put millions of user records at risk.

- Microsoft's Patch Tuesday fixes 132 flaws, the largest count since April 2022, including nine critical-severity vulnerabilities as well as six zero-day vulnerabilities. Among those is the remote code execution flaw (CVE-2023-36884) in Microsoft Office and Windows that can be exploited using specially-crafted Microsoft Office documents. Successful exploitation could result in the execution of remote code on the victim's machine.

  *Check Point Threat Emulation provides protection against this threat* *(Technique.Win.OleEmbed.Ia.A)*

- Apple has released emergency security updates that address an actively exploited flaw (CVE-2023-37450) in the WebKit engine shared by iOS and macOS devices. Successful exploitation could result in the execution of remote code on the victim's machine.

# THREAT INTELLIGENCE REPORTS

- Check Point Research has released an analysis of Google's generative AI platform Bard, presenting several scenarios where the platform permits to generate malicious content. Threat actors could utilize Bard to generate phishing emails, malware keylogger and a basic ransomware code.

- Check Point Research detects 8% surge in global weekly cyberattacks during Q2 2023, with organizations facing an average of 1258 attacks per week. Ransomware attacks have hit 1 out of every 44 organizations worldwide every week, mostly focused in APAC and Europe. Furthermore, the Government/Military sector has experienced a 9% increase from the parallel period last year, following the Education/Research sector that was found to be the most targeted one.

- Researchers have uncovered a sophisticated and staged campaign utilizing the Blackmoon Trojan (KRBanker) in a campaign that began in November 2022. The campaign targets businesses in the US and Canada, employing evasion and persistence techniques to deploy multiple unwanted programs and maintain a presence in the victims' environment for an extended duration. Unlike typical credential theft, the focus of this campaign is on persistent presence rather than stealing credentials.

  *Check Point Harmony Endpoint and Threat Emulation provide protection against this threat*
  *(Banker.Win.BlackMoon; Banker.Wins.BlackMoon)*

- Researchers have identified multiple versions of RedDriver, a driver-based browser hijacker, which uses the Windows Filtering Platform (WFP) to intercept browser traffic. RedDriver has been active since at least 2021, and is designed to target native Chinese speaking users.