TOP ATTACKS AND BREACHES

- The American resort, casino and hotel chain MGM has suffered a cyber-attack that resulted in widespread disruption across the company's hotels and casinos, and has shut down its internal networks as a precaution. The cyber-attack paralyzed the company's ATMs, slot machines, room digital key cards and electronic payment systems. ALPHV ransomware affiliate, has claimed responsibility for the attack. Check Point Research is sharing its analysis insights on the activity of the ALPHV group during the last 12 month.

- The European aerospace giant Airbus has disclosed a data breach that potentially resulted in the exposure of 3,200 sensitive Airbus vendors' contact information, including names, addresses, phone numbers and email addresses. The breach was claimed by the notorious ransomware group called Ransomed that have targeted many companies with ransomware attacks during September 2023.

- Sri Lanka's government has been a victim of a ransomware attack that affected its cloud system, Lanka Government Cloud (LGC). The government has lost 3 months of data after restoring a backup of the cloud environment as a response to the breach. The data was erased from nearly 5K email addresses, including ones belonging to top government officials. No ransomware gang has claimed responsibility for the attack yet.

- BianLian ransomware gang has claimed responsibility for a cyber-attack on the world's leading non-profit organization Save the Children International. The threat actors claim to have stolen almost 7TB of data, including 800GB of the charity's financial data, human resources data, and personal information such as health and medical data, as well as email correspondence.

- Giant software bug-tracking company Rollbar, which is used by more than 400 million end users of applications and numerous global companies, has confirmed a data breach. The threat actors have infiltrated the company's systems and gained access to sensitive clients' information, including usernames, email addresses, account names and project details.

- The International Joint Commission (IJC) has been a victim of a cyber-attack that affected the water levels and flows across US-Canada border. The NoEscape ransomware gang has claimed responsibility for the attack, claiming to have stolen 80GB of data, including contracts, geological files, conflict of interest forms and more.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Ransomware_Linux_NoEscape; Ransomware.Win.NoEscape)

VULNERABILITIES AND PATCHES

- Adobe's Patch Tuesday update for September 2023 has been released, providing a fix for the critical zero-day vulnerability in Adobe Acrobat and Reader (CVE-2023-26369). Successful exploitation of this bug could lead to code execution by opening a specially crafted PDF document.

  Check Point IPS provides protection against this threat *(Adobe Acrobat and Reader Out-of-bounds Write (APSB23-34: CVE-2023-26369))*

- Microsoft has released fixes for 59 bugs, including two zero-day flaws in Microsoft Word (CVE-2023-36761) and Microsoft Streaming Service Proxy (CVE-2023-36802).

  Check Point IPS provides protection against this threat *(Microsoft Streaming Service Proxy Elevation of Privilege (CVE-2023-36802))*

- A new vulnerability in GitHub was discovered, exploiting a race condition within GitHub's repository creation and username renaming operations. Successful exploitation of this vulnerability could allow an attacker to perform a Repojacking attack (hijacking popular repositories to distribute malicious code).

- Google has patched a critical zero-day heap buffer overflow vulnerability in WebP (tracked as CVE-2023-4863). The vulnerability is suspected to be related to the recently discovered Pegasus zero-day vulnerabilities in Apple products.

THREAT INTELLIGENCE REPORTS

- Check Point Research have encountered a new large-scale phishing campaign that targeted more than 40 prominent companies across multiple industries in Colombia. The attackers' objective was to discreetly install the sophisticated Remcos malware on victims' computers, which grants full control over the infected machine and can be used in a variety of attacks.

  Check Point Threat Emulation provides protection against this threat *(Technique.Win.Unhooking; Technique.Win.WrongFileExt; Technique.Win.UnhookingNtdll)*

- Check Point Research has released August 2023's Most Wanted Malware report, highlighting a new ChromeLoader campaign named "Shampoo" which targets Chrome browser users with malware-loaded fake ads. In addition, Qbot (aka Qakbot), which was the most prevalent malware last month with an impact of 5% worldwide organizations, has been shut down by the FBI.

- Microsoft warns of a new phishing campaign conducted by Storm-0324 (aka DEV-0324, TA543 and Sagrid), an initial access broker group using email-based initial infection vectors, and usually sells accesses to ransomware operations including FIN7 (aka Sangria Tempest, ELBRUS, Carbon Spider). The latest campaign is using Teams messages as lures to infiltrate corporate networks.