TOP ATTACKS AND BREACHES

- The City of Dallas, Texas has suffered a ransomware attack conducted by Royal ransomware gang. The attack caused a network outage of its Information and Technology Services (ITS), including Dallas police department, Dallas fire-rescue, Dallas municipal court, payment systems and more.

  Check Point Harmony Endpoint provides protection against this threat *(Ransomware.Win.Royal)*

- ALPHV (aka Blackcat) ransomware gang claims to have attacked the Australian commercial law firm HWL Ebsworth. The threat actors claimed to have access to 4TB worth of HWL Ebsworth data, including employee CVs, IDs, financial reports, accounting data, client documentations, credit card information, and a complete network map.

  Check Point Harmony Endpoint and Check Point Threat Emulation provide protection against this threat
  (Ransomware.Wins.BlackCat; Ransomware_Linux_BlackCat)

- AvosLocker ransomware gang has claimed responsibility for a ransomware attack affecting the IT systems of the Virginia-based Bluefield University. The threat actors compromised the university's RamAlert emergency broadcast system, to inform students and university staff about the attack. According to the gang's alerts, the stolen data consists of 1.2TB of files, including thousands of students' admissions data, which will be leaked on dark web forums unless they pay the ransom.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Ransomware.Win.AvosLocker; Ransomware_Linux_AvosLocker; Ransomware.Wins.Avoslocker; Trojan.Wins.Avos)

- After launching a devastating attack on the city of Oakland on April, the Play ransomware gang has taken responsibility for another attacks in the United States on Massachusetts city of Lowell. The gang claims to have stolen an undisclosed amount of data that includes passports, government IDs, financial documents and more.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(Ransomware.Win.Play)*

- T-Mobile has revealed its second data breach that occurred in 2023, which caused the leakage of hundreds of the company clients' data. The leaked data could cause a potential fraud and identity theft, as it includes sensitive personal information such as contacts information, accounts number and associated phone numbers, T-Mobile accounts PIN, social security numbers, government IDs and more.

VULNERABILITIES AND PATCHES

- Apple has issued the first-ever security updates for its AirPods and Beats headphones products that fixes an authentication vulnerability (CVE-2023-27964) in which attackers could gain access to users' headphones through a Bluetooth connection.

  Check Point IPS provides protection against this threat *(Microsoft Message Queuing Remote Code Execution (CVE-2023-21554))*

- Researchers have disclosed a vulnerability in TikTok social media platform that could allow attackers to monitor users' activity on both mobile and desktop devices. They found that the window message event handler doesn't properly validate the origin of incoming messages, providing attackers access to sensitive user information. The vulnerability has been already patched.

- Security researcher has discovered a cross-site scripting vulnerability (CVE-2023-30777) at the Advanced Custom Fields and Advanced Custom Fields Pro WordPress plugins, which have over 2 million active installations. This vulnerability could cause the theft of sensitive information, as well as privilege escalation on WordPress site. The vulnerability was fixed in version 6.1.6 and later.

THREAT INTELLIGENCE REPORTS

- Check Point Research has analyzed a cluster of activity that deploys ROKRAT, a malware previously attributed to a North Korean threat actor commonly referred to as APT37, Inky Squid, RedEyes, Reaper or ScarCruft. New tools affiliated with the same actor were deployed in various multi-stage infection chains, including another custom backdoor, GOLDBACKDOOR, and the commodity malware Amadey.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Technique.Win.EmbedExeLnk; Trojan.Wins.SusLNK; Injector.Win.RemoteThread; Technique.Win.MalOfficeVBA; Exploit.Win.MalChildren)

- Check Point Research revealed new Android malware called FluHorse. The malware mimics legitimate applications, most of which have more than 1,000,000 installations. The malware steals victims' credentials and Two-Factor Authentication (2FA) codes. FluHorse targets different sectors of Eastern Asian markets and is distributed via emails.

  Check Point Harmony Mobile provides protection against this threat *(FLU_HORSE_STR)*

- Check Point Research has noticed a surge in cyberattacks leveraging websites associated with the ChatGPT brand. These attacks involve the distribution of malware and phishing attempts through websites that appear to be related to ChatGPT, to lure users into downloading malicious files or disclose sensitive information.