TOP ATTACKS AND BREACHES

- Hawaii's largest university, the University of Hawai'i, has disclosed that one of its campuses had suffered a ransomware attack. The impact of the attack had not been made public by the university, but ransomware gang NoEscape, which has assumed responsibility for the attack, claimed to have exfiltrated 65 GB of sensitive data from the university's network.

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

- After Manchester University has revealed on June 9th that it had suffered a data breach that resulted from an unauthorized party access to some of its systems, now the threat actors started using triple extortion tactic. Students and the stuff of the university received emails threatening to sell or expose their personal data, in order to put pressure on the university to pay the ransom.

- Ransomware group BlackCat (ALPHV) has breached American plastic surgery clinic Beverly Hills Plastic Surgery, and claims to have exfiltrated patient information in the attack. The group threatens to leak patients' pre and post operation photos, alongside other sensitive personal information, if the ransom demand is not met. The gang has previously leaked patients' photos and medical records following an attack against American healthcare provider LVHN in February of this year.

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

- The two largest public pension fund systems in the United States, CalPERS and CalSTRS, have posted notices that they had been affected by ransomware gang Cl0p's MOVEit Transfer attack. The California-based pension funds join a growing list of over 100 organizations impacted by the attack, including the United States Department of Energy, the BBC, British Airways, and others. Some victims in the United States have opted to sue Progress Software in a class action lawsuit as a result of the attack.

  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)*

- Two of the largest airlines in the world, American Airlines and Southwest Airlines, have stated they are handling data breaches due to an incident involving a hack of Pilot Credentials, a third-party vendor. The breach, which occurred at the end of April, has included the illicit obtainment of documents related to almost 9,000 applicants in the pilot and cadet hiring process to both airlines. Despite that, there has not been an impact on the airlines' own networks or systems.

VULNERABILITIES AND PATCHES

- Apple has released a security patch addressing three zero-day vulnerabilities (CVE-2023-32434, CVE-2023-32435 and CVE-2023-32439). The vulnerabilities have been exploited in the wild in a wide iPhone campaign affecting Russian citizens that was dubbed Operation Triangulation.
- Zyxel Networks has published an advisory regarding CVE-2023-27992, a critical severity pre-authentication command injection vulnerability in Zyxel NAS devices. An attacker could potentially execute commands remotely without requiring authentication on unpatched devices.
- The ISC has patched three vulnerabilities affecting multiple versions of the BIND 9 DNS software toolset. The vulnerabilities, which were assigned High severity, allow a remote attacker to cause denial of service.
- VMware has addressed five memory corruption vulnerabilities affecting its vCenter Server and Cloud Foundation products. Some of the vulnerabilities could be exploited by a malicious actor with network access to execute arbitrary code on the affected products.

THREAT INTELLIGENCE REPORTS

- Check Point researchers have discovered a sophisticated malware affecting a European medical institution. The attack is attributed to Camaro Dragon (Mustang Panda), a Chinese state-sponsored APT group. The threat actors employ malicious USB drives as an initial access vector in order to target restricted networks, and their payload includes a module that further infects any additional USB drive that is plugged into an infected host. It is believed that the malware thus propagated beyond the attackers' initial intent, likely inadvertently infecting dozens of organizations worldwide.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (APT.Wins.MustangPanda; APT.Wins.MustangPanda.ta)

- The Ukrainian have encountered a spyware campaign affecting prominent government entities, as well as a military aircraft maintenance organization. The campaign was attributed to APT28 (Fancy Bear), affiliated with the Russian GRU. The attackers sent emails containing 3 exploits to gain access to Roundcube mail servers and extract information from the victims.
- An analysis of macOS malware Jokerspy has been published. The threat actors employ both open-source and custom made tools to eventually establish full backdoor access to victims' macOS platforms. Among the targets of this campaign was a prominent Japanese cryptocurrency exchange.
- Researchers have analyzed the activities of known North Korean state-sponsored APT groups to determine the country's offensive cyber strategy. The major focus of the groups was espionage and financial theft, with the main targets being South Korea and the United States.