TOP ATTACKS AND BREACHES

- LockBit ransomware gang has claimed responsibility for an alleged attack on the multibillion-dollar IT products and services reseller CDW. The gang has demanded $80M ransom and threatened to release stolen data, said to include employee badges, audits, commission payout data and more. The company has isolated the affected servers, which are claimed to be non-customer-facing.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Ransomware.Win.Lockbit; Gen.Win.Crypter.Lockbit; Ransomware.Wins.LockBit.ta; Ransomware_Linux_Lockbit)

- IT systems of Kwik Trip, American chain of over 800 convenience stores and gas stations, have been disrupted by a possible ransomware attack that resulted in numerous outages reported by the company's clients. The attack has affected the Kwik Rewards platform, the orders and payments system, as well as the company's offices' email and phone systems.

- Air Europa, Spain's third-largest airline, has suffered a data breach that exposed sensitive information of an undisclosed amount of the company's clients. The threat actors have hacked its web portal to steal credit card information, including card numbers, expiration dates, and CVV security code used to authorize online payments.

- The American major manufacturing company Simpson Manufacturing has disclosed a cyber-attack that resulted in a disruption of its IT infrastructure. Once malicious activity was detected, the company has shut down the compromised systems as a precaution. No threat actors have claimed responsibility yet.

- Valve, the US company behind the Steam video game platform, has confirmed that attackers modified some of its games to distribute malware. Most likely it was done by taking over Steam developer accounts using malware that steals session cookies from browsers of infected PCs. As a new precaution security update Valve has enforced SMS-based two-factor authentication for developers accounts that want to update their build on Steam's default branch.

- Multiple hacktivists groups are targeting Israeli websites and organizations as part of the war against Israel. While most of the claims of the groups weren't confirmed, the successes included few billboards in Israel that were hacked and displayed pro Hamas messages, and Ono Academic College that was breached. About 250,000 records of employees, students, former students, and more were published in Telegram. The college subsequently had to take its systems offline.

VULNERABILITIES AND PATCHES

- Security flaws have been uncovered in Curl, a highly-trusted command line tool used to transfer data to and from a server. The more severe flaw of the two, CVE-2023-38545, a SOCKS5 heap-based buffer overflow vulnerability, impacts both the cURL tool and libcurl library. Patches have been released.

  Check Point IPS and Harmony End Point provide protection against this threat *(cURL libcurl Heap Buffer Overflow (CVE-2023-38545) cURL libcurl Heap Buffer Overflow (CVE-2023-38545); Exploit_Linux_CVE-2023-38545)*

- Microsoft and Adobe have released their Patch Tuesday reports for October 2023. Microsoft has addressed three zero-day vulnerabilities, including an elevation-of–privilege flaw in Skype for Business (CVE-2023-41763), an information disclosure bug in WordPad (CVE-2023-36563) and "HTTP/2 Rapid Reset" – a zero-day DDoS attack method (CVE-2023-44487). Adobe has released three security advisories to address 13 vulnerabilities in Adobe Bridge, Adobe Commerce, and Adobe Photoshop.

  Check Point IPS provides protection against this threat *(HTTP/2 Denial of Service (CVE-2023-44487))*

THREAT INTELLIGENCE REPORTS

- Check Point Research uncovers "Stayin' Alive", an ongoing campaign that has been active since at least 2021. The campaign operates in Asia and primarily targets the Telecom industry, as well as governmental organizations. The campaign leverages spear-phishing emails to deliver archive files utilizing DLL side-loading schemes.

  Check Point Harmony Endpoint, Threat Emulation and Anti-Bot provide protection against this threat *(Loader.Win.ToddyCat, Trojan.Wins.ToddyCat.ta, APT.Wins.ToddyCat.Q, Trojan.WIN32.ToddyCat.A)*

- Check Point Research introduces R2R stomping - a new method for running hidden implanted code in ReadyToRun (R2R) compiled .NET binaries that is not yet known in the wild. CPR explains the implementation of R2R stomping, which could affect the work of the reverse engineers and security researchers, and details techniques to reverse engineer R2R stomped Assemblies.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat.

- The FBI and CISA have released a joint Cybersecurity Advisory under their #StopRansomware campaign, warning of and diving into AvosLocker ransomware, which operates under a ransomware-as-a-service (RaaS) model. They focus on technical details and the group's TTPs to assist mitigation and defense.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat *(Ransomware.Wins.Avoslocker.ta.A, Gen.Win.Crypter.AvosLocker.B, Ransomware.Win.AvosLocker.B, Ransomware_Linux_AvosLocker)*