Check Point Research
WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The German hospital network Katholische Hospitalvereinigung Ostwestfalen (KHO) has been a victim of cyber-attack that disrupted the systems of hospitals in Bielefeld, Rheda-Wiedenbrück, and Herford. Lockbit ransomware group claimed responsibility for the attack.

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

- The Iran-affiliated group Homeland Justice has claimed responsibility for cyber-attacks against several Albanian high profile organizations - the Albanian parliament, two local telecom companies and Albania's flag carrier. The attacks are possibly related to the country's shelter support for the Iranian opposition group Mujahedeen-e-Khalq. Albanian officials confirmed that they are assisting to One Albania company and to the parliament in mitigating the attack.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Wiper.Win.GenericWiper.F; Trojan.Wins.HomeLandJusticeWiper.)*

- Europe's largest parking app operator EasyPark Group, which operates in over 20 countries, has acknowledged a data breach that affected the personal information of an unverified amount of EasyPark users in Europe. The data includes names, phone numbers, home addresses, email addresses and parts of IBAN or credit card numbers.

- The in-flight entertainment system supplier Panasonic Avionics Corporation has confirmed a data breach that impacted certain systems in the corporate's network environment. The threat actors gained access to personal and health information belongs to an unverified amount of employee and clients.

- The American entertainment giant National Amusements (parent company of Paramount and CBS) has disclosed a data breach that affected the personal and financial information of more than 82K people. The leaked data includes names, financial account numbers, credit and debit card numbers as well as PIN codes.

- Ohio lottery systems has suffered a cyber-attack on Christmas Eve, that has taken down the company's website and prevented clients from cashing in prizes above $599. DragonForce ransomware group claimed responsibility for the attack, which allegedly resulted in the leakage of about 600GB of data, and consists of over 3M entries of employees and players personal information, including Social Security numbers (SSN) and dates of birth (DOB).

VULNERABILITIES AND PATCHES

- Chinese threat actor dubbed UNC4841 has exploited a zero-day arbitrary code execution vulnerability (CVE-2023-7102) in Barracuda Email Security Gateway Appliance (ESG). The threat actor has utilized the flaw within a third party library, Spreadsheet::ParseExcel, to deploy a specially crafted Excel email attachment to target a limited number of ESG devices. Spreadsheet::ParseExcel is an open source library used by the Amavis virus scanner within the ESG appliance.

  Check Point IPS provides protection against this threat *(Barracuda Email Security Gateway Remote Code Execution (CVE-2023-7102))*

- Google Cloud has resolved two vulnerabilities (GCP-2023-047) in its Kubernetes Engine (GKE). The flaws could potentially be exploited by threat actors who already have access to a Kubernetes cluster, allowing them to increase their privileges. This access could allow them to carry out data theft, deploy malicious pods, and disrupt operations.

- Apache has released a patch for critical (9.8 CVSS score) Apache OFBiz pre-authentication remote code execution vulnerability (CVE-2023-51467). The vulnerability allows attackers to bypass authentication to achieve a simple Server-Side Request Forgery (SSRF). Apache OFBiz is an open-source Enterprise Resource Planning system, that is used in the codebase of many products (such as JIRA).

THREAT INTELLIGENCE REPORTS

- Researchers highlight one of the attack segments of the North Korean Kimsuky group. The group's recent modus operandi involved the persistent use of shortcut-type backdoor malware dubbed AppleSeed. The backdoor can be used to control the infected system, install additional malware, keylogging and taking screenshots, as well as stealing information from the users' systems.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Trojan.Wins.Appleseed.ta.; APT.Wins.APT37_Kimsuky; APT.Win.Kimsuky)*

- A new version (2.2) of the Meduza infostealer has been released on the Dark Web. This updated version of the infostealer has garnered attention for its enhanced features, including broader software client support, an improved credit card grabber, and advanced mechanisms for storing dumped passwords on various platforms.

  Check Point Threat Emulation provides protection against this threat *(InfoStealer.Wins.Meduza)*

- Financially motivated threat groups; including Storm-0569, Storm-1113, Sangria Tempest, and Storm-1674 have been observed abusing the ms-appinstaller protocol handler (MSIX files) to deliver malicious signed software to users, usually via malvertising.