October 21 - 27, 2024

CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Grupo Aeroportuario del Centro Norte (OMA), operator of 13 airports across Mexico, was hacked by the RansomHub ransomware gang, who threatened to leak 3TB of stolen data unless a ransom is paid. The attack disrupted terminal information screens and forced OMA to activate backup systems, with no reported material adverse effects on operations or finances yet.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Ransomware.Win.RansomHub; Ransomware.Wins.RansomHub.ta.)*

- Landmark Admin, a third-party administrator for major insurance carriers, has suffered a data breach that impacted over 800K individuals, resulting from unauthorized network access and data encryption between May to June this year. The breach exposed sensitive personal and financial information, including names, Social Security numbers, passport numbers, and medical information.

- Healthcare giant Henry Schein confirmed a ransomware attack that occurred at 2023 and resulted in the theft of sensitive data, affecting operations across manufacturing, distribution, and its ecommerce platform. The BlackCat ransomware group has claimed responsibility for the attack.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Ransomware.Win.BlackCat; Ransomware.Wins.BlackCat.ta.; Ransomware.Wins.Blackcat)*

- The FBI and CISA are investigating the breaches of multiple US telecommunications companies including AT&T, Verizon, and Lumen Technologies by the Chinese government-affiliated group Salt Typhoon. The attacks targeted systems used for wiretaps and targeted devices of former President Trump, Vice President Harris, and several prominent politicians.

- UnitedHealth's subsidiary Change Healthcare admitted that during a ransomware attack by the Russian-speaking BlackCat ransomware gang, personal and healthcare data of 100 million individuals was compromised. Sensitive information such as health insurance details, medical records, and Social Security numbers were exposed. The breach led to a $22 million ransom payment and estimated ongoing losses of $2.45 billion, marking it as the largest-ever US healthcare data breach.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Ransomware.Win.BlackCat; Ransomware.Wins.BlackCat.ta.; Ransomware.Wins.Blackcat)*

- Berufsbildungszentrum (BBZ), a vocational school in Switzerland, has been a victim of a ransomware attack that blocked access to several IT systems by exploiting a security gap in the firewall. Investigators are currently assessing whether personal data was compromised. This attack is part of a broader wave of cyberattacks targeting German-speaking educational institutions across Europe.

VULNERABILITIES AND PATCHES

- CISA has issued urgent advisories for CVE-2024-20481, a critical denial-of-service vulnerability in Cisco ASA and FTD, and CVE-2024-37383, a cross-site scripting vulnerability in RoundCube Webmail. The first flaw, rated at 9.8, enables system crashes through crafted HTTP requests, while the second, rated at 6.5, allows malicious script injections that can lead to data theft and session hijacking.

  Check Point IPS provides protection against this threat (RoundCube Webmail Stored Cross-Site Scripting (CVE-2024-37383))

- The Lazarus Group exploited a zero-day vulnerability (CVE-2024-4947) in Google Chrome via a fake DeFi game website to target cryptocurrency users. This flaw in Chrome's V8 engine allowed them to control victims' browsers and access sensitive data such as authentication tokens and passwords.

  Check Point IPS provides protection against this threat (Google Chrome Type Confusion (CVE-2024-4947))

- Fortinet has patched a critical vulnerability (CVE-2024-47575) in FortiManager, used to manage FortiGate firewalls. Dubbed FortiJump, it was exploited in zero-day attacks, allowing unauthorized access to servers and the exfiltration of sensitive data such as configuration files and credentials.

- VMware has fixed two critical-severity vulnerabilities (CVE-2024-38812 and CVE-2024-38813) in its vCenter Server and VMware Cloud Foundation products. These vulnerabilities could enable attackers to execute remote code and gain elevated privileges.

THREAT INTELLIGENCE REPORTS

- Amazon has identified internet domains abused by Russian APT29 group as part of a phishing campaign that deploys rogue Remote Desktop Protocol (RDP) files aimed at stealing Windows credentials and data from government and military organizations. These malicious RDP connections enabled attackers to access and potentially steal data from victims' shared resources.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (APT.Win.APT29; APT.Wins.APT29.ta.; APT.Wins.CozyBear; APT.Wins.Nobelium)*

- Researchers have discovered a new variant of the Qilin (aka Agenda) ransomware, dubbed Qilin.B, which exhibits advanced encryption techniques and enhanced defense evasion capabilities, targeting both Windows and Linux systems for double extortion schemes.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (Ransomware.Wins.Qilin; Ransomware.Win.Agenda)

- Researchers have analyzed Grandoreiro, a Brazilian banking trojan categorized under the Tetrade group. Threat actors are utilizing the trojan to conduct fraudulent banking operations through the victims' computers globally, bypassing banking institutions' security measures.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (Banker.Win.Grandoreiro; Banker.Wins.Grandoreiro)