CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Nonprofit healthcare organization Axis Health System has been hit by a ransomware attack by the Rhysida gang, leading to the theft of sensitive data, including mental health and substance abuse records. Rhysida is demanding $1.5 million and has threatened to publish the data in six days if unpaid. The gang has also begun leaking 102GB of data from Golden Age Nursing Home, including over 35K files, which allegedly contain medical records and discharge reports.

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

- Danish toy manufacturer LEGO was hit by a cyberattack that compromised its website, where hackers promoted the purchase of a fake "LEGO Coin" cryptocurrency. The attack had a limited success, with only a few hundred dollars' worth of the fake tokens purchased by victims.

- American Water, the largest water utility in the US, has confirmed a cyberattack that disrupted its internal systems, specifically affecting customer billing. The breach led to the shutdown of certain systems, though water and wastewater services remain unaffected.

- The Internet Archive's "The Wayback Machine" has experienced a cyberattack, resulting in the theft of 31 million user records, including email addresses, screen names, and bcrypt-hashed passwords. The attack also involved site defacement and a Distributed Denial of Service (DDoS) attack.

- Japanese tech giant Casio has disclosed a cyber-attack that caused a system failure, resulting in service disruptions. The attack led to the leak of more than 91K customer records in Japan and 35K records from other countries, including names, email addresses, and payment method information.

- Russian state media company VGTRK has been a victim of a cyberattack that resulted in the disruption of several television channels, including Russia 1 and Russia 24, for nearly an hour. The attack reportedly led to the erasure of data from the company’s servers, including backups. The pro-Ukrainian hacktivist group Sudo rm-RF is believed to be responsible for the breach.

- Fidelity Investments has suffered a data breach that resulted in the exposure and compromise of personal information for over 77K customers between August 17 and August 19. The breach involved unauthorized access to customer information through two recently established accounts, though no Fidelity accounts or funds were directly accessed. No threat actor has claimed responsibility yet.

- American security company ADT has confirmed a cyberattack that resulted in the exfiltration of encrypted internal company data related to employee user accounts, using compromised credentials obtained from a third party. The breach caused disruptions to some of ADT’s information systems, though no customer data or security systems were compromised.

VULNERABILITIES AND PATCHES

- Microsoft's October 2024 Patch Tuesday fixes 117 security vulnerabilities, including four zero-day flaws, two actively exploited (CVE-2024-43572, CVE-2024-43573). Key patches address critical Remote Code Execution vulnerabilities in Microsoft Configuration Manager (CVE-2024-43468) and Remote Desktop Protocol Server (CVE-2024-43582).

  Check Point IPS blade provides protections against these threats *((Microsoft Management Console Remote Code Execution (CVE-2024-43572), Microsoft Windows MSHTML Platform Spoofing (CVE-2024-43573))*

- Google's October 2024 Android security update addresses critical vulnerabilities, including a denial-of-service flaw in the Android Framework (CVE-2024-40675), local privilege escalation issues, and a remote code execution vulnerability (CVE-2024-40673). It also patches issues in MediaTek and Qualcomm components, covering WLAN, display, and modem functions.

- Adobe's October 2024 security update patches multiple vulnerabilities across its product family, including Adobe Substance 3D Painter, Adobe Commerce, and Adobe Animate. The update addresses memory leaks, privilege escalation, code execution, and security bypasses.

THREAT INTELLIGENCE REPORTS

- Check Point Research has released September 2024's Most Wanted Malware report which emphasizes the shift towards AI-driven malware tactics in the current cyber landscape, alongside the ongoing dominance of ransomware threats. Threat actors likely used AI to develop a script that delivers AsyncRAT malware, which is now ranked 10th on the most prevalent malware list. Joker remains the top mobile malware, while RansomHub leads among ransomware groups.

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

- Check Point Research has analyzed 'Operation MiddleFloor' disinformation campaign targeting Moldova's government and education sectors before the October 2024 elections. The Russian-aligned group, Lying Pigeon, uses spoofed emails to spread false information about EU membership and the pro-European leadership while gathering data for potential malware attacks.

- Researchers have discovered a campaign by the GoldenJackal APT group targeting air-gapped systems in government and diplomatic entities across Europe, the Middle East, and South Asia. The group used custom toolsets, including GoldenHowl and GoldenRobo, to breach isolated networks, steal sensitive information, and exfiltrate data through USB devices and modular backdoors.

  Check Point Harmony Endpoint provides protection against this threat *(APT.Win.GoldenJackal)*

- Researchers have uncovered a new phishing-as-a-service (PhaaS) platform called Mamba 2FA, designed for adversary-in-the-middle (AiTM) phishing attacks. It mimics Microsoft 365 login pages, and bypasses multi-factor authentication methods like one-time codes and app notifications, stealing credentials and cookies, which are then sent to attackers via a Telegram bot.