CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- American Bassett Furniture Industries has been a victim of a ransomware attack that resulted in the encryption of data files and the shutdown of its manufacturing facilities. The attack has significantly disrupted the company's operations, impacting its ability to fulfill orders despite keeping retail stores and its e-commerce platform open. No ransomware group has claimed responsibility yet.

- International location safety app Life360 and project management tool Trello have been victims of data breaches caused by a flaw in their respective APIs. Life360's breach resulted in the exposure of personal information for 442,519 customers, including email addresses, names, and phone numbers, while Trello's breach exposed 21.1GB of data, including full names, email addresses, and board memberships for millions of users. Both breaches were conducted by the threat actor known as 'emo', who released the stolen data on a dark web forum.

- Humanitarian organizations CARE International, the Norwegian Refugee Council, and the Saudi Arabian King Salman Humanitarian Aid and Relief Centre have been victims of a cyber-attack that resulted in the deployment of Android spyware designed to harvest sensitive information. The attack, attributed to the pro-Houthi threat group known as OilAlpha, involved malicious apps masquerading as legitimate entities to steal victim data and credentials.

  Check Point Harmony Endpoint provides protection against this threat *(RAT.Win.OilAlpha)*

- American boat retailer MarineMax has experienced a ransomware attack that resulted in a data breach affecting over 123K individuals. The Rhysida ransomware group claimed responsibility, stealing files that included financial documents and personal information.

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

- Indian crypto company WazirX has confirmed a data breach that resulted in the loss of $230M, nearly half of its reserves. The breach compromised a multisig wallet and led to the theft of over 200 different cryptocurrencies, including significant amounts of SHIB, Ethereum, Matic, Pepe, USDT, and Gala tokens. The attackers are reportedly affiliated with North Korea.

- Ukrainian defense enterprises were attacked by the UAC-0180 threat group. The attacks involve emails with ZIP file attachments containing a malicious PDF link. In the end of the infection chain, a bootloader facilitates the download and execution of the ATERA remote control program.

- Australian healthcare firm MediSecure has suffered a ransomware attack that resulted in the theft of 6.5TB of data belongs to approximately 12.9M Australians. The data includes names, contact information, and healthcare details. No ransomware group has claimed responsibility yet.

VULNERABILITIES AND PATCHES

- A recently disclosed critical remote code execution vulnerability, CVE-2024-27348, impacts Apache HugeGraph-Server and is actively exploited in the wild. This flaw, present in the Gremlin graph traversal language API, affects all versions before 1.3.0 and allows attackers to bypass sandbox restrictions, gaining complete control over the server.

  Check Point IPS provides protection against this threat *(Apache HugeGraph Server Remote Code Execution (CVE-2024-27348))*

- SolarWinds has released security updates for Access Rights Manager (ARM) software to address 13 vulnerabilities. Eight flaws rated as critical, including CVE-2024-23472, CVE-2024-28074, and CVE-2024-23469, could allow attackers to read, delete files, and execute code with elevated privileges.

- Cisco's SSM On-Prem and SSM Satellite products are affected by a critical vulnerability, CVE-2024-20419, which allows attackers to change any user or admin password. Rated 10 on the CVSS scale, this flaw demands no user interaction or privileges. Successful exploitation involves sending crafted HTTP requests to access the web UI or API with the compromised user's privileges.

THREAT INTELLIGENCE REPORTS

- Check Point Research reports on recent activity of the Iranian APT group MuddyWater. The group has significantly increased its activity against Israel since October 7th, while in parallel it targets victims in Saudi Arabia, Turkey, Azerbaijan, India and Portugal. The group is using a new custom backdoor dubbed BugSleep.

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

- Check Point Research has released its 2024 Q2 cyber-attack trends report. The report indicates a 30% year-over-year increase in global cyber-attacks for Q2 2024, reaching an average of 1,636 attacks per organization per week. The Education/Research sector experienced the highest rise, with 3,341 weekly attacks, marking a 53% increase. Africa reported the highest average of 2,960 attacks per week, while Latin America saw a 53% increase in attack volume compared to the previous year.

- Researchers have analyzed the increase in cyber threats targeting the Paris 2024 Olympics, revealing a significant rise in darknet activity related to French organizations, with a notable 80% to 90% increase in threats since the second half of 2023. Key concerns include phishing schemes, fraudulent ticket sales, and the use of infostealers like Raccoon, which accounts for 59% of detections in France.

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

- Researchers have uncovered Konfety, a large ad fraud operation using over 250 decoy apps on the Google Play Store paired with malicious "evil twin" apps. This scheme involves spoofing app IDs to perform ad fraud and sideload malware, generating up to 10 billion ad requests daily.