CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Memorial Hospital and Manor in Bainbridge, Georgia, has been a victim of a ransomware attack that resulted in the loss of access to its electronic health record system. The Embargo ransomware gang has claimed responsibility, threatening to leak 1.15 terabytes of purportedly stolen data by November 8.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Ransomware.Wins.Embargo., Ransomware.Win.Embargo.*)*

- Serco, a company operating prisoner escort services for the Ministry of Justice in the United Kingdom, has disclosed a cyberattack that resulted in the disabling of tracking systems and panic alarms on their prison transport vans. The incident, which also affected other companies like DHL, was due to a cyberattack on Microlise, a provider of tracking software.

- SelectBlinds, a U.S. windows blinds and shades seller, has acknowledged a data breach that resulted in the theft of credit card information and personal data of more than 200,000 customers. Hackers reportedly embedded malware on the company's website, enabling data scraping on the checkout page for nine months. Compromised information includes usernames, passwords, names, emails, shipping and billing addresses, phone numbers, and payment card details.

- The Washington state court system has suffered a cyberattack resulting in the shutdown of judicial information systems, websites, and related services. The Administrative Office of the Courts (AOC) detected unauthorized activity and proactively took systems offline to secure them.

- French multinational company Schneider Electric confirmed unauthorized access to its internal project tracking platform (Atlassian Jira system), by HellCat Ransomware. This is said to have resulted in the theft of 40GB of data, including 400,000 rows of user information with 75,000 unique email addresses and full names of employees and customers.

- Nokia has confirmed that a third-party vendor experienced a security breach, leading to the leak of a customized software application's source code on a hacker forum. The company stated that their own systems and data remain unaffected by this incident.

- Newpark Resources, a Texas-based oilfield supplier, experienced a ransomware attack discovered at the end of October, leading to disruptions and limited access to certain internal information systems and business applications.

- South East Technological University (SETU) in Ireland is handling a cyberattack that led to the postponement of classes at its Waterford campuses. The university stated that there is currently no evidence of data compromise, but their WiFi and phones are out of action.

VULNERABILITIES AND PATCHES

- Cisco has disclosed a critical vulnerability (CVE-2024-20418) in its Unified Industrial Wireless Software for Ultra-Reliable Wireless Backhaul (URWB) Access Points. The flaw has a CVSS score of 10.0. Unauthenticated, remote attacker to perform command injection attacks with root privileges. The flaw stems from improper validation of input to the web-based management interface.

- Hewlett Packard Enterprise (HPE) has released updates for Instant AOS-8 and AOS-10 software to address two critical vulnerabilities (CVE-2024-42509 and CVE-2024-47460) in Aruba Networking Access Points. These flaws allow remote attackers to perform unauthenticated command injection by sending specially crafted packets to Aruba's Access Point management protocol (PAPI) over UDP port 8211.

- The November 2024 Android security update addresses, among others, two actively exploited zero-day vulnerabilities (CVE-2024-43093 and CVE-2024-43047). The vulnerabilities could allow elevation of privilege, remote code execution and unauthorized access to Android devices if exploited. The update mitigates risks posed by these critical flaws to enhance device security.

THREAT INTELLIGENCE REPORTS

- Check Point Research has revealed a phishing campaign, dubbed "CopyRh(ight)adamantys," that deploys the latest Rhadamanthys stealer (0.7) using copyright infringement themes. This campaign impersonates various companies, mainly in the Entertainment/Media and Technology/Software sectors, adapting content and language per target across regions like the United States, Europe, East Asia, and South America. Though the stealer's new version claims AI-powered text recognition, analysis reveals it uses classic machine learning typical of OCR rather than modern AI engines.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (InfoStealer.Wins.Rhadamanthys.ta.V, InfoStealer.Wins.Rhadamanthys.)*

- Check Point Research has uncovered the ongoing evolution of ElizaRAT, a sophisticated Remote Access Tool (RAT) used by the Pakistan-affiliated threat group APT36 (Transparent Tribe) in targeted attacks against India. This campaign leverages cloud platforms like Google Drive, Telegram, and Slack for command and control, enhancing evasion by blending with legitimate network traffic. Key additions to ElizaRAT include new evasion techniques, second-stage payloads, and the ApoloStealer component.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (APT.Win.ElizaRAT.B/C/D, RAT.Wins.Eliza.ta.A/B/C/D)

- Researchers have analyzed the crimeware bundle dubbed SteelFox Trojan, which masquerades as activators for popular software like Foxit PDF Editor and AutoCAD. Once executed, it delivers a bundle containing both stealer and cryptocurrency miner malware. The Trojan employs sophisticated techniques, including shellcoding and exploitation of vulnerable drivers, to evade detection and escalate privileges.