CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- The State of Rhode Island has issued a notification that RIBridges, the state's portal for social services, has suffered a cyber attack and data leak. According to the reports, the breach was likely caused by a ransomware attack, including compromise of personal information of hundreds of thousands of the state's residents.

- US identity and access management solutions company, Beyond Trust, has suffered a breach affecting its Remote Support product for some its customers. The attackers gained access to a Remote Support API key, which allowed them access to local application accounts.

- Namibia's state telecom company, Telecom Namibia, has suffered a ransomware attack. According to reports, the company was breached by the ransomware group Hunters International, which has stolen more than 600GB of data.

- Healthcare software company Phreesia disclosed a breach of its subsidiary, ConnectOnCall, impacting 914,138 patients' personal and health data. The breach occurred between February and May 2024, allowing unauthorized access to personal identifiable information and medical records. The compromised data involved communications between patients and healthcare providers.

- Ukrainian Justice Ministry suffered a cyber attack by Russia-linked actors that shutdown various online services. The threat actors prepared the cyberattack through several months, while the Ukrainian security service's cyber department attribute the attack to the Russian military intelligence (GRU).

- The Texas Tech University Health Sciences Center has disclosed a ransomware attack that occurred in September and caused disruption of some systems and applications. The attack resulted in extraction of the combined data of 1,465,000 people that include personal identifiable information, financial details and medical data. Interlock ransomware claimed credit for the attack.

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

- Ascension Health ransomware attack resulted in exposure of 5.6 million people’s data. Black Basta ransomware targeted Ascension in May, disrupting operations for weeks. Recently Ascension confirmed that the attackers extracted medical records, financial data and personal identifiable information.

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

VULNERABILITIES AND PATCHES

- Google has released a security update for Google Chrome, addressing five security vulnerabilities. One of the vulnerabilities, CVE-2024-12692, is a high severity type confusion vulnerability. This vulnerability was reported to Google on December 5th and could lead to heap corruption via a crafted HTML page.

- Researchers have identified vulnerabilities in Azure Data Factory's Apache Airflow integration that could allow attackers to gain unauthorized access. The flaws include misconfigured Kubernetes RBAC, weak authentication in Azure's internal Geneva service, and secret handling issues. Exploitation of these issues could lead to access, data exfiltration, and malware deployment.

- Severe security vulnerability was discovered in FortiWLM Wireless Manager. This vulnerability (CVE-2023-34990) enables remote code execution through unauthorized access to log files and critical system files enabled by relative path traversal.

  Check Point IPS blade provides protection against this threat *(Web Servers Malicious URL Directory Traversal)*

- The Australian Cyber Security Center (ACSC) has alerted organizations to a critical vulnerability in Apache Struts2 before version 6.4.0, which largely affects Java-based applications. The file upload flaw (CVE-2024-53677) can lead to extensive security breaches, including remote code execution, by exploiting path traversal flaws and manipulating file upload parameters.

  Check Point IPS blade provides protection against this threat *(Java Server Pages Backdoor)*

THREAT INTELLIGENCE REPORTS

- Check Point researchers discovered a phishing campaign abusing Google Calendar and Google Drawings to bypass email security. Attackers manipulate email headers to impersonate Google Calendar notifications, tricking users into visiting malicious pages that steal sensitive data for financial scams.

- Researchers have identified a campaign of malicious extensions targeting integrated development environment (IDE) software VSCode. Initially targeting crypto community, the latest malicious extensions all impersonate Zoom application. The campaign was also expanded to NPM package manager, introducing malicious JavaScript packages.

- Researchers found that threat actors abused a legitimate tool for leads generation to harvest Microsoft Azure credentials. The threat actors targeted automotive, chemical and manufacturing industries with fake forms created through HubSpot Free Form Builder service that consequently redirected to attacker-controlled phishing domains, impersonating Outlook Web Application.

- Researchers report on evolution of tools, techniques and procedures (TTPs) of North Korean hacking group Lazarus. In their latest attacks targeting the nuclear sector, the group introduced CookiePlus, a novel framework malware capable of downloading DLL and shellcode.