September 30 – October 6, 2024

CHECK POINT RESEARCH

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Chinese state-sponsored hackers, dubbed "Salt Typhoon", infiltrated US telecom companies such as Verizon, AT&T, and Lumen Technologies. The attackers gained access to systems used for court-authorized wiretaps, potentially remaining undetected for months while collecting sensitive information.

- French press agency AFP has disclosed a cyber-attack on its IT systems. According to the agency's statement, its delivery service has been impacted, and it has contacted the French National Agency for IT Systems Security (ANSSI), as well as French authorities. The company's website experienced intermittent outages during the incident.

- Wayne County, Michigan, is dealing with a cyberattack, suspected as ransomware attack, that disrupted government websites and limited several county office operations. Officials have confirmed the attack targeted internal systems, affecting online services such as tax payments and real estate records.

- Dutch police have identified a "state-sponsored threat actor" as the likely perpetrator of a large-scale data breach discovered last week. The attackers reportedly stole data containing names, emails, phone numbers, and private information of around 65,000 officers.

- Canadian game developer Red Barrels announced delays in their Outlast game series following a cyberattack on their internal IT systems. While player data was unaffected, production timelines have been significantly impacted.

- The University Medical Center Health System in Lubbock, Texas, has been forced to divert ambulances due to a ransomware attack that disrupted many of its systems. The incident caused IT outages, affecting radiology systems and patient record access across several clinics. No ransomware group has claimed responsibility for the attack yet.

- Highline Public Schools in Washington State confirmed a ransomware attack led to the shutdown of its schools in early September. The incident involved unauthorized access to the school district's network, affecting over 17,500 students. The school district is working to restore affected systems and is providing free credit and identity monitoring services to its employees as a precaution.

- The Barbados Revenue Authority (BRA) experienced a data breach, with a hacker named "Pryx" claiming access to the administrative portal. Sensitive data, including vehicle registration records, driver's licenses, passport numbers, and contact details, are reportedly for sale on a Russian-language cybercrime forum. "Pryx" has made a ransom demand, though there has been no response from the government.

VULNERABILITIES AND PATCHES

- A critical remote code execution (RCE) vulnerability has been discovered in Aurba 501, a popular web application framework. This vulnerability allows attackers to execute arbitrary code on targeted systems, potentially compromising sensitive data and services. The flaw exists in the file upload mechanism, and exploitation could lead to full server control.

  Check Point IPS provides protection against this threat *(Aruba 501 Command Injection)*

- A critical remote code execution vulnerability (CVE-2024-45519) in Zimbra's postjournal service is being actively exploited in the wild. The vulnerability allows unsanitized input to be passed to the popen function, enabling attackers to inject arbitrary commands. Despite patched versions being available, more than 50,000 web-exposed Zimbra servers remain vulnerable.

- Apple has released updates for iOS and iPadOS to address two security vulnerabilities. One flaw (CVE-2024-44204) could allow the VoiceOver feature to read out a user's saved passwords. The issue was caused by a logic problem in the Passwords app affecting a range of iPhones and iPads. Another patched flaw (CVE-2024-44207) involved audio capture in iPhone 16 models before the microphone indicator activation.

- CISA has added the critical vulnerability in Ivanti Endpoint Manager (CVE-2024-29824), with a CVSS score of 9.6, to its Known Exploited Vulnerabilities catalog, due to its active exploitation in the wild. This flaw allows unauthenticated attackers on the same network to execute arbitrary code via an SQL injection in the PatchBiz.dll.

  Check Point IPS provides protection against this threat *(Ivanti Endpoint Manager SQL Injection (CVE-2024-29824))*

THREAT INTELLIGENCE REPORTS

- Check Point Research has uncovered a growing trend of vulnerable Windows drivers being exploited by attackers to gain kernel privileges. The study identifies common characteristics of these drivers and highlights the risks associated with their abuse. Through mass hunting methods, the research reveals thousands of potentially at-risk drivers, including vulnerabilities that can be exploited for privilege escalation and bypassing security mechanisms.

- In preparation for Prime Day, Check Point Research has identified over 1,000 new Amazon-related domains registered in the last 30 days, 88% of which are malicious or suspicious. More than 100 unique Amazon Prime-themed scam emails targeting consumers and organizations were detected.

- Researchers have observed a mid-September campaign impersonating Royal Mail to deliver Prince ransomware, a ransomware variant freely available on GitHub. The campaign targeted individuals in the UK and the U.S., distributing ransomware via contact forms and emails. The attack appears mostly destructive since there are no decryption options or data exfiltration capabilities. This suggests that the actors have no intention of decrypting files, even if a ransom is paid.