CHECK POINT RESEARCH

July 1 – 7, 2024

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- FIA, the governing body for Formula 1, disclosed a data breach stemming from a phishing attack on their email accounts. The attack led to unauthorized access to personal data, and the incident has been reported to relevant data protection regulators. FIA is taking steps to bolster security and has initiated protective measures for affected individuals.

- Mercku, a Canadian router manufacturer, has suffered a breach in their support portal, resulting in automatic phishing responses to customer support tickets. Customers seeking assistance received emails directing them to update their MetaMask accounts, a tactic aimed at compromising cryptocurrency wallets.

- HealthEquity, a healthcare fintech firm, suffered a data breach when a partner's account was compromised, leading to unauthorized access and exfiltration of sensitive healthcare data. The stolen information includes personally identifiable information considered protected health information for certain members. HealthEquity has initiated notifications to impacted individuals and is offering credit monitoring and identity restoration services.

- Croatia's largest hospital, KBC Zagreb, experienced a significant ransomware attack perpetrated by the LockBit ransomware group. The attack disrupted the hospital's IT systems, including business software, storage systems, and patient admission information systems.

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

- A threat actor exploited Ethereum's mailing list provider, managing to send phishing emails to 35,000 users. These emails lured recipients to a malicious site offering a fake investment opportunity with a 6.8% APY on staked Ethereum, leading to a crypto drainer attack.

- The Alabama Department of Education faced a ransomware attack, leading to unauthorized access and theft of data despite the attack being partially blocked. The incident involved potential theft of personal information of both students and employees.

- Researchers have analyzed internet traffic and DDoS attacks during the UK 2024 election, observing significant traffic dips and spikes around polling times with notable attacks on political parties' post-election. The data highlights targeted DDoS incidents potentially influencing political processes.

- A large password compilation leak titled "RockYou2024" has been posted to a cybercrime forum, reportedly containing nearly 10 billion unique plaintext passwords originating from multiple data breaches. The data poses significant risks for credential stuffing and brute-force attacks, potentially affecting various online accounts and services.

VULNERABILITIES AND PATCHES

- An unauthenticated Remote Code Execution vulnerability (CVE-2024-6387) has been discovered in OpenSSH servers (sshd) operating in glibc-based Linux environments. The high severity vulnerability, caused by a regression that reintroduced old vulnerability (CVE-2006-5051), impacts versions from 8.5p1 to 9.8p1 and those earlier than 4.4p1 without specific patches.

  Check Point IPS provides protection against this threat *(Multiple SSH Initial Connection Requests)*

- Microsoft researchers disclosed two important vulnerabilities (CVE-2023-2071 and CVE-2023-29464) in Rockwell Automation's PanelView Plus devices that could allow unauthenticated remote code execution and denial-of-service attacks. The vulnerabilities, a critical severity RCE and a high severity DoS via out-of-bounds read, pose a high risk due to the potential for attackers to execute malicious code or disrupt operations in industrial settings.

- Researchers shared info on critical vulnerabilities (CVE-2024-38368, CVE-2024-38366, CVE-2024-38367) in CocoaPods, an open-source dependency manager for iOS and macOS applications. These vulnerabilities allow malicious actors to claim ownership of unclaimed packages and insert malicious code, potentially affecting thousands of applications.

  Check Point IPS provides protection against this threat *(Trunk Cocoapods Command Injection (CVE-2024-38366))*

- Two critical remote code execution vulnerabilities (CVE-2024-36401 and CVE-2024-36404) have been found in GeoServer and GeoTools. These vulnerabilities allow unauthenticated attackers to execute arbitrary code by exploiting XPath expression injection.

THREAT INTELLIGENCE REPORTS

- Ahead of Amazon Prime Day 2024, Check Point Research marks an increase in newly registered, malicious domains targeting Amazon customers. Notably, over 1,230 new domains were registered, with 85% flagged as suspicious, incorporating deceptive tactics such as phishing to steal login credentials and financial information. The report highlights phishing sites designed to mimic legitimate Amazon platforms to capture user data.

- Check Point Research has analyzed various modern cryptographic attacks, categorizing them into classic cryptanalysis, statistical bias attacks, and side-channel attacks. The article discusses techniques like meet-in-the-middle attacks, birthday attacks, and specific attacks on RSA encryption. These attacks exploit weaknesses in cryptographic algorithms and implementations, providing insights into their mechanisms and potential impact.

- Researchers have examined Eldorado ransomware, a sophisticated Ransomware-as-a-Service that emerged in March 2024 and has been increasing operations during June. Led by a Russian-speaking group and with a presence on cybercrime forums, Eldorado enables affiliates to create customized ransomware samples targeting both Windows and Linux systems. Notably, the RaaS uses advanced encryption techniques like Chacha20 and RSA-OAEP.