Check Point Research
WEEKLY INTELLIGENCE REPORT
February 19 - 25, 2024

TOP ATTACKS AND BREACHES

- The American Prince George's County Public Schools (PGCPS) has experienced a ransomware attack that compromised the personal data of nearly 100K individuals. The attack exposed individuals' full names, financial account information, and Social Security Numbers. The Rhysida ransomware gang is reportedly responsible for the attack.

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

- The American health insurance giant United Health Group (UHG) has confirmed that its subsidiary OptumChange Solutions, which operates Change Healthcare platform, has suffered a cyber-attack which forced it to shut down systems. The attack has disrupted healthcare services in pharmacies throughout the United States. The firm claims that a suspected nation-state threat actor is behind the attack.

- The Israeli airline El Al has suffered a cyber-attack that affected the communication network of a plane flying from Thailand to Israel. The attackers have attempted to conduct a takeover over an area where the Iran-backed Houthis are active, however the plane reached its destination safely.

- Threat actor IntelBroker has claimed responsibility for a data breach on Los Angeles International Airport (LAX). IntelBroker leaked an alleged database consists of 2.5M records of confidential user data belonging to private plane owners, extracted from the airport's network. The database includes full names, CPA numbers, email addresses, company names, plane model numbers and tail numbers.

- Truck and trailer rental company U-Haul has been a victim of a data breach affecting approximately 67K customers across the US and Canada. Threat actors have gained an unauthorized access using legitimate credentials to a reservation system. The breach exposed driver's license numbers among other identification details but did not compromise the payment system.

- Popular Ukrainian media outlets, including Ukrainska Pravda, one of the largest Ukrainian online newspapers, were hacked to spread the same piece of fake news of Russia destroying a unit of Ukrainian special forces. Ukraine's state cybersecurity agency (SSSCIP) attributed the attack to a Russian threat actor but didn't specify which group was behind the incident.

- The German control systems provider PSI Software SE has been a victim of a ransomware attack forced it to shut down external connections, and several IT systems including email systems, to prevent data exfiltration. No customer data has been compromised.

VULNERABILITIES AND PATCHES

- ConnectWise has announced two vulnerabilities in ScreenConnect product that affecting (on-premises) versions 23.9.7 and earlier. The first flaw is a critical-severity Authentication Bypass issue (CVE-2024-1708) and the second is a high-severity Path Traversal issue (CVE-2024-1709). Researchers have observed widespread exploitation of the vulnerabilities to deliver various malware payloads, including a LockBit ransomware variant named "buhtiRansom".

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Ransomware.Wins.LockBit.ta; Ransomware.Win.Lockbit; Gen.Win.Crypter.Lockbit.AI, Ransomware_Linux_Lockbit)*

- Mozilla has released February's security patches for Firefox, Firefox ESR, and Thunderbird vulnerabilities. These advisories address issues ranging from critical vulnerabilities that could allow attacker code execution to minor vulnerabilities like Denial-of-Service attacks.

- Five vulnerabilities were discovered in Joomla, potentially allowing arbitrary code execution. The most critical (CVE-2024-21725) involves XSS vulnerabilities due to inadequate mail address escaping. Other XSS issue (CVE-2024-21726) poses a moderate risk but could enable remote code execution if an administrator clicks a malicious link. Versions 5.0.3 and 4.4.3 include fixes.

THREAT INTELLIGENCE REPORTS

- Check Point Research has published 2024 Cyber Security Report, revealing a surge in ransomware attacks, with 1 in 10 organizations globally targeted in 2023. Researchers also noticed an evolution in tactics such as zero-day vulnerability exploitation for ransomware attacks, increase in targeting of Edge devices and cloud environments, as well as open-source repositories that pose software supply chain risks. The report also highlights AI as a crucial defense tool and calls for collaborative efforts and proactive measures to navigate the cyber threat landscape.

- Check Point Research has shared insights about how Deepfake technology threatens the 2024 U.S. elections. It highlights the widespread availability of deepfake technology and voice cloning technology, while the efforts to legislate against these technologies are still underway.

- An international law enforcement operation, dubbed 'Operation Cronos', including the UK's National Crime Agency, the FBI, and Europol, took down the LockBit ransomware group, known for its widespread attacks since late 2019. The operation resulted in the compromise of LockBit's primary platform and other critical infrastructure that enabled their criminal enterprise. Decryption keys have been released, as well as intelligence about LockBit operators.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Ransomware.Wins.LockBit.ta; Ransomware.Win.Lockbit; Gen.Win.Crypter.Lockbit.AI, Ransomware_Linux_Lockbit)*