December 18 - 24, 2023

Check Point Research

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Australia's largest non-profit healthcare provider, St. Vincent's Health Australia, experienced a cyberattack resulting in data theft from its networks. St. Vincent's operates public and private hospitals, as well as elderly care facilities across New South Wales, Victoria, and Queensland, employing over 20,000 staff.
- Xfinity, a major American cable TV and internet service provider, announced a data breach impacting nearly 36M people due to a Citrix vulnerability known as "Citrix Bleed" (CVE-2023-4966). The breach has occurred in mid-October.

  Check Point IPS provides protection against this threat (Citrix NetScaler Information Disclosure (CVE-2023-4966))
- A cyberattack has purportedly disabled the majority of gas stations across Iran, taking out of use about 70% of gas stations nationwide. Hacktivist group Predatory Sparrow, Gonjeshke Darande in Persian, has claimed responsibility for the wide attack.
- First American, a prominent title insurance company with reported revenues of $7.6 billion in 2022, has recently encountered a cyberattack, resulting in operational disruptions after shutting down systems. This development has led to a 2.6% decline in First American's stock price.
- ESO solutions, a US company which provides software for healthcare organizations, has disclosed that a ransomware attack had affected its network. According to the company, data of 2.7 million patients from 15 healthcare facilities across the United States has been exfiltrated by the attackers.
- Indian IT giant HCLTech reported that it was hit by a ransomware attack. According to the company's report, the attack was an isolated event in a specific project's cloud environment, and it did not affect HCL's network. The tech giant has over 225K employees and operated across 52 countries.
- The U.S. based mortgage company, Mr. Cooper, disclosed that nearly 14.7 million individuals had their information exposed during a cyberattack in October. The breach involved unauthorized access to systems, potentially compromising personal details like names, addresses, phone numbers, Social Security numbers, dates of birth, and bank account numbers.
- VF Corporation, a major global apparel company known for brands like North Face and Vans, reported a substantial cyberattack that included unauthorized activity on its IT systems, which resulted in disruptions due to encrypted systems and data theft, including personal information.

VULNERABILITIES AND PATCHES

- Google has released a security patch for Google Chrome, addressing the vulnerability CVE-2023-7024. The vulnerability is a heap overflow vulnerability affecting WebRTC, a real time communication browser feature. Google claims to be aware of active exploitation of this vulnerability in the wild.
- Mozilla has published Firefox version 121, which includes fixes for multiple security vulnerabilities. One of the vulnerabilities, CVE-2023-6856, allowed remote code execution and sandbox escape when used on systems with the Mesa VM driver.
- Ivanti has shared a security patch addressing 13 critical vulnerabilities affecting the company's Avalanche MDM (mobile device management) product. The vulnerabilities were caused by buffer overflows, and could allow remote code execution.

THREAT INTELLIGENCE REPORTS

- Check Point Research has revealed an alarming increase in advanced phishing schemes targeting a variety of Blockchain networks, employing wallet-draining techniques. Unique in their approach, these threats are targeting a wide range of Blockchain networks, from Ethereum and Binance Smart Chain to Polygon, Avalanche, and almost 20 other networks by using a crypto wallet-draining technique.
- The FBI, CISA, and ASD's ACSC have jointly released a #StopRansomware Cybersecurity Advisory for Play Ransomware, providing insights into the TTPs of the Play ransomware group, along with indicators of compromise identified through FBI investigations as of October 2023. The Play ransomware employs a double-extortion model impacting businesses and critical infrastructure organizations across North America, South America, Europe, and Australia.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat
  (Ransomware.Win.Play.B, Ransomware.Wins.PLAY.A)

- Researchers have identified the Iranian cyber-espionage group APT33 employing a new backdoor malware called FalseFont to target defense contractors globally. FalseFont has been observed in early November, facilitating remote access, file execution, and transfer to command-and-control servers.
- A coordinated international law enforcement effort, led by the FBI and involving agencies from the United Kingdom, Denmark, Germany, Spain, and Australia, successfully seized the dark web leak site of the notorious ALPHV (BlackCat) ransomware gang. This followed the sharing of a decryption tool, and a countering announcement on AlphV's site, claiming it had been "unseized”.

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