Check Point Research
WEEKLY INTELLIGENCE REPORT
February 5-11, 2024

TOP ATTACKS AND BREACHES

- One of the largest unions in California, Service Employees International Union (SEIU) Local 1000, has confirmed a ransomware attack that led to network disruption. The LockBit ransomware gang has assumed responsibility, claiming to have stolen 308GB of data including sensitive employee information such as Social Security numbers, salary information, financial documents and more.

  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)

- Hyundai Motor Company's European division has suffered a cyber-attack in which an unauthorized third party has accessed a limited part of its network. Black Basta ransomware gang had claimed to have breached Hyundai Motor Europe in early January, and to have stolen 3TB of corporate data.

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

- Two American insurance firms, Washington National Insurance and Bankers Life, subsidiaries of CNO Financial Group, disclosed a SIM swap attack that compromised the personal information of approximately 66,000 individuals. The attackers gained access through multi-factor authentication by targeting a senior officer's phone.

- Two French health insurance companies, Viamedis and Elmer’s, have confirmed a cyber-attack that compromised data of over 33 million people, almost half of France's population. The breached data includes sensitive personal information yet excludes medical histories.

- Dutch intelligence agencies revealed a cyber espionage operation by Chinese state-backed hackers against the Dutch Defense Ministry. Using a Fortinet vulnerability (CVE-2022-42475) the attacker aimed at accessing unclassified military research network. This incident marks the Netherlands' first public attribution of a cyber-attack to China.

- A DDoS attack hit Pennsylvania’s court system, causing significant disruptions to its online services, including filing systems and bail payment platforms. The FBI and CISA are involved in recovery efforts. There is no indication of data compromise, and the courts remain open.

- The Philippines have announced that an attempt to break into the country's president's and government's email systems has been thwarted. According to the communications ministry official's statement, the attacker's IP geolocates them in China.

VULNERABILITIES AND PATCHES

- Fortinet has released fixes for a zero-day critical vulnerability (CVE-2024-21762) in FortiOS that may have been exploited in the wild. The vulnerability is an out-of-bounds write issue that can be exploited by a remote, unauthenticated attacker for arbitrary code execution using specially crafted HTTP requests.
- Ivanti has alerted of another high-severity security flaw (CVE-2024-22024), with a CVSS score of 8.3, in its Connect Secure, Policy Secure, and ZTA gateway devices. The flaw could allow attackers to bypass authentication. Patches for the flaw are available and there is no current evidence of active exploitation.

  Check Point IPS blade provides protection against this threat (Ivanti XML External Entity Injection (CVE-2024-22024))
- A critical remote code execution vulnerability (CVE-2023-40547) in Linux shim, a small piece of code that used during secure boot process, allows attackers to take complete control of affected systems. All Linux distributions that support Secure Boot, including Red Hat, Ubuntu, Debian, and SUSE are affected.

THREAT INTELLIGENCE REPORTS

- Check Point Research outlines the evolution of the Raspberry Robin worm, highlighting its use of two 1-day Local Privilege Escalation exploits before those were publicly disclosed. This malware acts as an initial access broker for other crime groups, including EvilCorp and TA505, shifts its delivery methods and continues to improve its stealthiness.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (Trojan.Wins.RaspberryRobin.)*
- Check Point Research discusses the threat of outdated Microsoft Word and Excel vulnerabilities (CVE-2017-11882, CVE-2017-0199, CVE-2018-0802). These are still seen exploited to deliver malware like Dridex, GuLoader, and Formbook/Xloader in attacks against the Finance/Banking, Governmental, and Healthcare sectors.

  Check Point Harmony Endpoint and Threat Emulation provide protection against this threat (Wins.Maldoc_CVE-2017-0199., Exploit.Wins.CVE-2017-11882.*)*
- Check Point Research has released its January 2024’s Most Wanted Malware report, which uncovered a large cyber threat distributor known as VexTrio, that serves as a major traffic broker for cybercriminals to distribute malicious content. LockBit3 topped the list of active ransomware groups and Education was the most impacted industry worldwide.

  Check Point Threat Emulation provides protection against this threat (Trojan.Wins.RaspberryRobin.ta, Trojan.Wins.RaspberryRobin)