Check Point Research
WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Check Point Research identified a campaign against entities in Armenia, using a new version of OxtaRAT - an AutoIt-based backdoor for remote access and desktop surveillance. The threat actors have been targeting human rights organizations, dissidents, and independent media in Azerbaijan for several years, amid rising tensions between Azerbaijan and Armenia over the Lachin corridor.

  Check Point Threat Emulation and Anti-Bot provides protection against this threat *(Trojan.Win.OxtaRAT.A; Trojan.WIN32.OxtaRAT)*

- Web hosting company GoDaddy has reported a security breach where attackers stole source code and planted malware on its servers. The company discovered the breach to its cPanel shared hosting environment in late 2022, yet the attackers apparently had access to the network for several years.

- Australian software company Atlassian experienced a data leak after threat actors used stolen employee credentials to access a third-party vendor's data; customer data remains secure, but employees data has allegedly been leaked. Hacking group SeigedSec has taken credit, sharing the stolen data on Telegram.

- Scandinavian Airlines has issued a warning to passengers about a cyberattack that caused an outage of its website and mobile app for several hours, and resulted in the exposure of customer data; including contact details, past and future flights, and the last four digits of credit card numbers.

- City of Oakland has announced a local state of emergency as they are dealing with a ransomware attack that forced the city to take its IT systems offline.

- Community Health Systems, one of the leading healthcare providers in the US, has confirmed that it was affected by the recent attacks targeting a zero-day vulnerability in Fortra's GoAnywhere MFT file transfer platform, revealing that the breach exposed personal information of almost 1 million patients.

  Check Point IPS provides protection against this threat *(GoAnywhere MFT Insecure Deserialization)*

- The massive ESXiArgs ransomware campaign continues to expand, and recently affected over 500 hosts with the majority located in France, Germany, the Netherlands, the U.K., and Ukraine.

- MortalKombat ransomware and Laplas Clipper were observed in a recent financially motivated campaign, with the ransomware extorting money from victims by offering a decryptor and Laplas used to steal cryptocurrency by hijacking crypto transactions.

  Check Point Threat Emulation and Harmony Endpoint provide protection against this threat *(Ransomware.Win.Xorist.*)*

VULNERABILITIES AND PATCHES

- Hyundai and KIA issued an emergency software update for several car models that have been vulnerable to an easy hack that enables theft. The US Department of Transportation has disclosed that over 8 million Hyundai and KIA cars have been impacted by this security flaw, and that the hacks have resulted in at least 14 car crashes and 8 fatalities.

- Microsoft has released security updates to a total of 77 flaws in the latest Patch Tuesday. Nine vulnerabilities have been classified as 'Critical' as they allow remote code execution on vulnerable devices, and three are actively exploited in attacks (CVE-2023-21823, CVE-2023-21715 and CVE-2023-23376).

  Check Point IPS provides protection against these threats *(Microsoft Windows Graphics Component Elevation of Privilege (CVE-2023-21823); Microsoft Office Security Feature Bypass (CVE-2023-21715); Microsoft Windows Common Log File System Driver Elevation of Privilege (CVE-2023-23376) etc.)*

- Fortinet has released security updates for its FortiNAC and FortiWeb products, which tackle two critical-severity vulnerabilities (tracked as CVE-2022-39952 and CVE-2021-42756) that could enable unauthorized attackers to execute arbitrary code or command execution without authentication.

- Apple shared emergency security updates for iOS, iPadOS, macOS, and Safari browser, to fix a zero-day vulnerability (tracked as CVE-2023-23529), which is claimed to be actively exploited in the wild.

THREAT INTELLIGENCE REPORTS

- Check Point CloudGuard Spectral detected malicious crypto-mining packages on NPM, the leading registry for JavaScript Open-Source packages. The packages enabled Cryptojacking, which involves using a machine to mine cryptocurrencies without the user's consent.

- Researchers have identified a new backdoor, WhiskerSpy, used in a campaign by an advanced threat actor named ‘Earth Kitsune’. The actor targets individuals with an interest in North Korea, selecting victims from visitors to a pro North Korea website through a watering hole attack.

- A new variant of the Mirai botnet (tracked as 'V3G4') has been discovered, used in DDoS attacks to target Linux-based servers and IoT devices by exploiting 13 different vulnerabilities. The malware was spotted in three separate campaigns between July and December of 2022.

  Check Point IPS provides protection against these threats *(Atlassian Confluence Remote Code Execution (CVE-2022-26134); Airspan AirSpot 5410 Command Injection (CVE-2022-36267); Draytek Vigor Command Injection (CVE-2020-8515); FreePBX callmenum Remote Code Execution, etc.)*

- A new malware called 'Frebniis' has been discovered, deployed on Microsoft's IIS web servers. The malware operates silently by executing commands that are sent via web requests.