October 16 – 22, 2023

Check Point Research

WEEKLY INTELLIGENCE REPORT

TOP ATTACKS AND BREACHES

- Attackers have gained access to parts of the network of the cloud identity authentication giant Okta. The hackers managed to gain access to the firm's support unit for at least two weeks and have attempted to use tokens copied from support tickets to access the firm's customers' networks. Reportedly, the firm only became aware of the incident when a customer reported that a support ticket token being abused. According to Okta, the incident affected only a "very small number" of customers.

- The FBI has revealed that thousands of North Koreans had used false identities and other impersonation methods in order to find remote employment in IT jobs across the United States. The workers would then transfer their wages to North Korea's ballistic missile weapons program. The Justice Department has announced that it had seized 17 domains and $1.5M as part of its investigation into the operation.

- The hackers who had allegedly leaked 1.3 million records of 23andMe customers have leaked additional 4.1 million records of customers of the company. The information allegedly includes personal identifying details, as well as genetic ancestry data. The hackers claim that 4 million of the affected people are from the United Kingdom.

- Taiwanese network hardware giant D-Link has confirmed a data breach, after a threat actor has offered an alleged 3 million line customer database of the company for sale on darkweb forums. However, the company claims that the impact is much smaller than the threat actor alleges, as according to its statement the threat actor had only gained access to 700 outdated records from an end-of-life server.

- The District of Columbia's Board of Elections has disclosed that a data breach of its website provider may have leaked the entire district's voter database, after it had previously claimed that less than 4,000 voters have been impacted.

- Japanese electronics firm CASIO has posted notice that more than 120,000 records of its customers from 149 countries was leaked, after hackers gained access to the company's ClassPad education platform.

- American security agencies warn of widespread exploitation by an unspecified nation-state actor of Atlassian Confluence vulnerability CVE-2023-22515, a critical vulnerability which allows creating unauthorized administrator accounts to access Confluence instances. The agencies warn that threat actors continue their active exploitation of the vulnerability even after the patch has been applied.

  Check Point IPS provides protection against this threat (Atlassian Confluence Authentication Bypass (CVE-2023-22515))

VULNERABILITIES AND PATCHES

- A campaign exploiting a zero-day vulnerability in Cisco IOS XE software's Web UI feature has been discovered. According to Cisco, the campaign has been ongoing for over a month, and has affected more than 34,000 Cisco devices worldwide. The vulnerability, CVE-2023-20198, allows administrator-level remote access to Cisco devices running IOS XE. Cisco has released a patch addressing the vulnerability.

  Check Point IPS provides protection against this threat *(Cisco IOS XE Web UI Privilege Escalation (CVE-2023-20198))*

- Security researchers warn of active exploitation of Citrix Netscaler ADC and Gateway information disclosure vulnerability CVE-2023-4966. The vulnerability was disclosed by Citrix this month, yet evidence has been shared of the it being exploited as a zero-day since August. Furthermore, threat actors who had gained access to devices may still maintain it even after the patch has been applied.

- SolarWinds has released an advisory addressing eight high severity vulnerabilities affecting its Access Rights Manager (ARM) program. The vulnerabilities, CVE-2023-35180-7, allowed a combination of privilege escalation, directory traversal and remote code execution on the ARM product.

- VMware has addressed two high severity vulnerabilities affecting its Aria Operations for Logs product. The vulnerabilities, CVE-2023-34051-2, could allow a remote unauthenticated threat actor to either inject files and gain remote code execution, or trigger data deserialization to bypass authentication.

THREAT INTELLIGENCE REPORTS

- Check Point Research has analyzed cyber activity related to the first ten days of the Israel-Hamas war. Multiple hacktivist groups, Middle Eastern, Islamic, and Russian-affiliated, have intensified their operations against Israel. Various attack vectors have been observed, including DDoS, defacement, and information leakage from some Israeli websites – most of those with very limited impact.

- Check Point Research latest Brand Phishing Report reveals that retail was the most impersonated industry last quarter. Walmart is topping the list and Home Depot made it into the top ten impersonated brands.

- Researchers have discovered a campaign by the Iranian nation-state group APT34 targeting a middle eastern state's government. According to the report, the threat actors had breached the government's exchange server, and have maintained access to email correspondence for a period of eight months.

- The Ukrainian CERT reports on a wide campaign by Russian threat actor group 'Sandworm' targeting 11 telecom providers in Ukraine for a period of five months. The threat actors have used their access to the providers to cause disruptions in service and potentially steal communication data.