Daily Cyber Headlines

Daily Cyber Headlines | TLP:WHITE | Alert ID : f6219039 | Oct 24, 2023, 07:00 AM

Today's Headlines:

Leading Story

- 1Password Discloses Security Incident Linked to Okta Breach

Data Breaches & Data Leaks

- City of Philadelphia Discloses Data Breach After Five Months
- D.C. Board of Elections: Hackers May Have Breached Entire Voter Roll

Cyber Crimes & Incidents

- DoNot Team's New Firebird Backdoor Hits Pakistan and Afghanistan
- US Energy Firm Shares How Akira Ransomware Hacked Its Systems
- Cyberattack on NY Hospitals Forces Ambulance Diversions

Vulnerabilities & Exploits

- Citrix Warns Admins to Patch NetScaler CVE-2023-4966 Bug Immediately

Trends & Reports

- Nothing to Report

Privacy, Legal & Regulatory

- Nothing to Report

Cybersecurity Awareness Month

- The Daily Cyber Headlines are being shared during the month of October at **TLP:WHITE** for Cybersecurity Awareness Month.

Upcoming Health-ISAC Events

- Health-ISAC Monthly Threat Brief – October 31, 2023, 12:00 PM Eastern

Additional Information

Leading Story

1Password Discloses Security Incident Linked to Okta Breach

Summary

- Due to the Okta compromise, more customers reported cyber threats.

Analysis & Action

1Password, a password management platform used by numerous businesses worldwide, fell victim to a cyber-attack after threat actors gained access to their Okta ID management tenant.

The incident comes after Okta reported that threat actors got access to its support case management systems using stolen credentials and were able to view files uploaded by some Okta customers that contained sensitive customer information. This has resulted in a campaign where the threat actor is using the breached sensitive information to hijack customer accounts.

According to the latest statement, Okta has claimed all customers who were affected by the incidents were notified, and that they are actively working with impacted customers on the investigation of incidents. The full statement can be accessed here. Members who use Okta in their operations are advised to closely monitor System Logs for suspicious activity.

Data Breaches & Data Leaks

City of Philadelphia Discloses Data Breach After Five Months

Summary

- Officials in Philidelphia disclosed a potential data breach of personal and protected health information that occurred in May.

Analysis & Action

According to the City of Philidelphia, threat actors have gained access to email accounts and could be in possession of personal and private health information (PHI). Officials are currently investigating the breach of information.

Previous investigations uncovered the possibility of threat actors gaining access to certain email accounts and sensitive information these accounts contained. The information exposed contains social security numbers, medical and demographic information, and limited financial information.

Current sources have not yet disclosed how the threat actors breached the email accounts. Members within the area of Philidelphia are encouraged to employ multi-factor authentication and create stronger passwords to ensure email security. Phishing attacks are likely to occur due to this breach. Members are also recommended to

refresh staff memory on identifying emails and downloads containing potentially malicious links.

D.C. Board of Elections: Hackers May Have Breached Entire Voter Roll

Summary

- The District of Columbia Board of Elections says that a threat actor from the October incident may have obtained access to the personal information of all registered voters.

Analysis&Action

The entire voter roll may have been exposed in the recent breach of DataNet Systems' database server. Personally identifiable information (PII), including driver's license numbers, dates of birth, partial social security numbers, and contact information, may have been exposed.

Current efforts are focused on assessing the full extent of the breach, identifying the vulnerabilities exploited during the attack, and implementing measures to safeguard voter data and systems. RansomedVC has claimed responsibility for the breach, and the latest information indicates the stolen data has not been sold yet.

The extent of the data breach is still being determined. Members are advised to utilize caution when using third-party vendors and pay special attention to vendor risk management to keep their networks segmented, decreasing the chances of a successful supply chain attack.

Members in the D.C. area are advised to monitor personal accounts and be wary of any potential identity fraud because of the data breach.

Cyber Crimes & Incidents

DoNot Team's New Firebird Backdoor Hits Pakistan and Afghanistan

Summary

- DoNot Team is associated with the use of a new .NET-based backdoor called Firebird targeting victims in Pakistan and Afghanistan.

Analysis & Action

Kaspersky's APT trends report Q3 2023 found that DoNot Team delivers a downloader called CSVtyrei which is believed to be linked to the first-stage payload and downloader strain, Vtyrei. DoNot Team, also known as APT-C-35, Origami Elephant, and SECTOR02, has been found using spear-phishing emails and rogue Android apps to propagate malware in the past.

The report found that while some of the code was non-functional, it hints at ongoing development by DoNot Team. The attacks gather information from Android users by using the stager payload and then conduct a second-stage attack using this information in the form of malware with more destructive features after they have downloaded a rogue app in the Google Play Store.

Members should avoid suspicious apps in their app stores, and only download applications from trustworthy and reputable sources. In Pakistan, Afghanistan, and the Asia-Pacific region, members should be made aware of these spear-phishing campaigns, and only open links sent by known senders.

US Energy Firm Shares How Akira Ransomware Hacked Its Systems

Summary

- BHI Energy's internal investigation released the specific data that was found to be stolen after the Akira ransomware group's breach of their network.

Analysis & Action

BHI Energy fell victim to a cyberattack by Akira ransomware and sent out notifications to all impacted people, which included detailed information regarding the breach methods and the information that was stolen. The threat actors used stolen Virtual Private Network (VPN) credentials of a third-party contractor to access their internal network.

The threat actors stole around 767,000 files containing more than 690 gigabytes of data, including their active directory database, weeks after the initial breach. In an act of transparency, BHI announced that an investigation revealed that PII (Personally Identifiable Information) such as names, dates of birth, Social Security Numbers, and health information was stolen. BHI has managed to recover data from a cloud backup and restored its systems without paying a ransom.

Members should ensure that measures like multi-factor authentication (MFA) and frequent global password resets are in place to increase protections and reduce the likelihood of an attack for their own organizations, but also for the safety of their business associates.

Cyberattack on NY Hospitals Forces Ambulance Diversions

Summary

- Two hospitals were impacted by a cyber-attack which caused temporary operational disruption, including diversion of ambulances.

Analysis & Action

Westchester Medical Center Health Network (WMCHealth) was forced to shut down its IT systems over the weekend because of the latest cyber-attack.

Two impacted New York-based hospitals, which are a part of WMCHealth, were forced to shut down their networks after discovering a cyber-attack on October 20. Due to these operational disruptions, the ambulance services were diverted to other hospitals. While most of the diversion stopped over the weekend, emergency stroke patients will still be diverted to other hospitals during this week.

Cyberattacks on care delivery institutions can have a significant impact on the organizations' operations, resulting in reduced capacity and worsened patient outcomes. Members who provide care services should follow strict Business Continuity Management (BCM) policies to guarantee that their operations are disrupted as little as possible in the event of a cyber-attack, to minimize the impact on patient outcomes.

Vulnerabilities & Exploits

Citrix Warns Admins to Patch NetScaler CVE-2023-4966 Bug Immediately

Summary

- Citrix advises customers to fix their NetScaler ADC and Gateway devices to avoid the exploitation of a major vulnerability CVE-2023-4966.

Analysis & Action

Citrix warned its customers to secure NetScaler ADC and Gateway appliances against ongoing exploitation of the critical sensitive information disclosure vulnerability tracked as CVE-2023-4966.

The vulnerability was originally disclosed on October 10. Although there was no known reported exploitation at the time, a week later, Mandiant revealed an ongoing exploitation campaign, which has allegedly been running since August 2023, and has allowed attackers to steal authentication sessions and hijack accounts. Mandiant also uncovered instances where CVE-2023-4966 was utilized to compromise the infrastructure of government agencies and technological firms.

Citrix has urged its customers to immediately apply released patches as the vulnerability is considered critical. Persistent vigilance, even after patching, is necessary.

Trends & Reports

Nothing to Report.

Privacy, Legal & Regulatory

Nothing to Report.

Health-ISAC Cyber Threat Level

On October 19, 2023, the Health-ISAC Threat Intelligence Committee (TIC) evaluated the current Cyber Threat Level and collectively decided to raise the Cyber Threat Level to Yellow (Elevated). The Threat Level of Yellow (Elevated) is due to threats from concerns regarding hacktivist activity related to the conflict in the Middle East, an uptick in LinkedIn profile impersonations, MFA Bypass, QR code phishing, and the actively exploited Cisco IOS XE bug.

For more information about the Health-ISAC Cyber Threat Level, including definitions and response guidelines for each of the alert levels, please review the Threat Advisory System.

You must have Cyware Access to reach the Threat Advisory System document.
Contact membership@h-isac.org for access to Cyware.

Reference | References

The Hacker News
Health IT & CIO Report
Health-ISAC
okta
Bleeping Computer
Bleeping Computer
Bleeping Computer
Bleeping Computer
Bleeping Computer

Tags

DoNot, 1Password, Citrix

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Share Threat Intel:

For guidance on sharing indicators with Health-ISAC via CSAP, please visit the Knowledge Base article CSAP Share Threat Intel Documentation at the link address provided here: https://health-isac.cyware.com/webapp/user/knowledge-base Additionally, this collaborative medium provides opportunities for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

Turn off Categories:

For guidance on disabling this alert category, please visit the Knowledge Base article CSAP "Alert Categories" Toggle Documentation at the link address provided here: https://health-isac.cyware.com/webapp/user/knowledge-base

Access the Health-ISAC Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

For Questions or Comments:

Please email us at toc@h-isac.org