Health-ISAC Daily Cyber Headlines

Daily Cyber Headlines **TLP:WHITE** **Alert Id: 2f124c20** **2022-10-25 12:21:09**

Today's Headlines:

Leading Story

- Pendragon Car Dealer Refuses 60 million LockBit Ransomware Demand

Data Breaches & Data Leaks

- Hive Claims Ransomware Attack on Tata Power, Begins Leaking Data

Cyber Crimes & Incidents

- Cuba Ransomware Affiliate Targets Ukrainian Government Agencies
- SideWinder APT Using New WarHawk Backdoor to Target Entities in Pakistan

Vulnerabilities & Exploits

- Apple Releases Patch for New Actively Exploited iOS and iPadOS Zero-Day Vulnerability
- Atlassian Vulnerabilities Highlight Criticality of Cloud Services

Trends & Reports

- Nothing to Report

Privacy, Legal & Regulatory

- Nothing to Report

Upcoming Health-ISAC Events

- Health-ISAC Monthly Threat Brief – October 25, 2022, 12:00 PM Eastern

Leading Story

Pendragon Car Dealer Refuses 60 million LockBit Ransomware Demand

Summary

- Pendragon Group was the victim of a data breach due to a cyberattack perpetrated by the LockBit Ransomware group which demanded $60 million as a ransom payment.

Analysis & Action

Pendragon Group owns CarStore, Evans Halshaw, and Stratstone luxury car retailer, and has more than 200 car dealerships in the United Kingdom.

However, the company was breached in a cyberattack from the LockBit ransomware group which demanded $60 million to decrypt the organization's files and not leak them. In a security announcement made by Pendragon, it was stated that the suspicious activity on its IT systems evidenced a security incident that took place in September 2022.

According to the data retrieved from forensic analysis Pendragon has attributed the attack to the LockBit ransomware group. After discovering the attack, Pendragon reported the incident to UK's law enforcement agencies and decided not to engage in negotiations nor pay for the $60 million ransom.

Data Breaches & Data Leaks

Hive Claims Ransomware Attack on Tata Power, Begins Leaking Data

Summary

- It was observed in the dark web that the Hive ransomware group has targeted Tata Power, a multi-billion company based in Mumbai, India.

Analysis & Action

Security researchers identified on the dark web that the Hive ransomware group has added Tata Power to its data leak site. Tata Power is a subsidiary of the multinational conglomerate Tata Group, and it currently is India's largest integrated power company based in Mumbai.

According to the information retrieved the threat actor was abler to compromise confidential data including Tata Power employees' personally identifiable information, national identification card numbers, tax account numbers, and salary information. The compromised data could expose the affected individuals to cybercrime-related activities such as phishing, extortion, and identity theft.

Additionally, it was observed that engineering drawings and financial and banking records were leaked. Tata Power stated that some of its IT systems were affected, however, steps have been taken to retrieve and restore all the systems.

Cyber Crimes & Incidents

Cuba Ransomware Affiliate Targets Ukrainian Government Agencies

Summary

- An alert has been issued by the Ukrainian CERT as malicious activity from the Cuba ransomware group was detected targeting Ukrainian governmental agencies.

Analysis & Action

The Computer Emergency Response Team of Ukraine (CERT-UA) has recently issued an alert regarding the potential of malicious activity perpetrated by the Cuba ransomware group.

According to CERT-UA, a new wave of phishing emails impersonating the Press Service of the General Staff of the Armed Forces of Ukraine was registered to target Ukrainian government employees. The phishing attack contains an embedded link that, if clicked, leads the user to a third-party web page for a fake update of its PDF reader software.

However, as the user clicks on the download button, an executable will be downloaded which contains a DLL file known as ROMCOM RAT, Cuba ransomware's signature. The malware could

allow the threat actor to perform file operations on the host, steal data, spawn spoofed processes, and start reverse shells.

SideWinder APT Using New WarHawk Backdoor to Target Entities in Pakistan

Summary

- Known threat actor SideWinder is using new backdoor malicious modules that deliver Cobalt Strike, incorporating new TTPs.

Analysis & Action

SideWinder, a prolific nation-state actor mainly known for targeting Pakistan military entities, compromised the official website of the National Electric Power Regulatory Authority (NEPRA) to deliver a tailored malware called WarHawk. The threat group, also called APT-C-17, Rattlesnake, and Razor Tiger, is suspected to be an Indian state-sponsored group.

Researchers have concluded that SideWinder is responsible for1,000 attacks since April 2020. WarHawk, masquerades as legitimate apps such as ASUS Update Setup and Realtek HD Audio Manager to lure unsuspecting victims into execution, resulting the exfiltration of system metadata to a hard-coded remote server, while also receiving additional payloads from the URL.

SideWinder APT Group is continuously evolving their tactics and adding new malware to their arsenal to carry out espionage attacks.

Vulnerabilities & Exploits

Apple Releases Patch for New Actively Exploited iOS and iPadOS Zero-Day Vulnerability

Summary

- Apple has released updates to fix a zero-day vulnerability found in iOS and iPadOS which was observed to be exploited in the wild.

Analysis & Action

A zero-day vulnerability affecting iOS and iPadOS has been fixed by Apple as the vulnerability has been actively exploited in the wild.

The vulnerability is an out-of-bounds write issue in the Kernel, that an attacker could leverage to execute arbitrary code with the highest privileges. The vulnerability is tracked as CVE-2022-42827 and its successful exploitation could result in memory corruption of data, a crash, or execution of unauthorized code affecting in this way the confidentiality, integrity, and availability of the data.

As the vulnerability was observed to be exploited in the wild, for security and user's safety, Apple retrained from sharing more specific information about the zero-day vulnerability.

Atlassian Vulnerabilities Highlight Criticality of Cloud Services

Summary

- Two new vulnerabilities have been found affecting Atlassian Jira Align that could allow users to access the service to become application administrators and perpetrate attacks.

Analysis & Action

Atlassian's Jira Align application is used to set agile-development goals, however, the new vulnerabilities could allow an attacker to gain control of a part of the company's cloud infrastructure.

The vulnerabilities were discovered by security researchers at Bishop Fox and are tracked as CVE-2022-36802 and CVE-2022-36803. The former is a server-side request forgery that could allow the retrieval of AWS credentials of the Atlassian service that provisions the Jira Align instance. The latter could allow users to elevate their role to Super Admin, allowing an attacker to have access to all settings in the Jira Align tenant that could allow the threat actor to reset and modify settings.

It was assessed with confidence by security researchers and consultants that the combination of both vulnerabilities could lead to a dangerous cyberattack.

Bishop Fox's full advisory on Atlassian Jira Align vulnerabilities can be accessed here.

Trends & Reports

Nothing to Report

Privacy, Legal & Regulatory

Nothing to Report

Health-ISAC Cyber Threat Level

On October 20, 2022, the Health-ISAC Threat Intelligence Committee (TIC) evaluated the current Cyber Threat Level and collectively decided to maintain the Cyber Threat Level at Blue (Guarded). The Threat Level of Blue (Guarded) was chosen in response to ongoing Qbot activity, fraudulent Help Desk activity, ongoing ransomware attacks, observed credential phishing, and foreign policy quandaries amid midterm elections.

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(s): Bleeping Computer, Bleeping Computer, Bleeping Computer, The Hacker News, The Hacker News, Dark Reading, Bishopfox

Tags: WarHawk Backdoor, SideWinter APT, Pendragon, Daily Cyber Headlines, Hive Ransomware, Cuba ransomware gang, DCH, Apple IOS, Penalties, Ransomware

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