Daily Cyber Headlines

Daily Cyber Headlines | TLP:WHITE | Alert ID : b72af20a | Oct 26, 2023, 06:33 AM

Today's Headlines:

Leading Story

- Mandiant Intelligence Chief Raises Alarm Over China's Volt Typhoon Hackers in US Critical Infrastructure

Data Breaches & Data Leaks

- Seiko Says Ransomware Attack Exposed Sensitive Customer Data
- Redcliffe Labs Exposes Over 12 Million Patient Records

Cyber Crimes & Incidents

- Espionage Group Uses Webmail Server Zero-Day to Target European Governments

Vulnerabilities & Exploits

- VMware Fixes Critical Code Execution Flaw in vCenter Server

Trends & Reports

- A Continuing Cyber-Storm with Increasing Ransomware Threats and a Surge in Healthcare and APAC Region

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

Mandiant Intelligence Chief Raises Alarm Over China's Volt Typhoon Hackers in US Critical Infrastructure

Summary

- John Hultquist, Chief Analyst at Mandiant, advises defenders working in critical infrastructure to keep an eye out for Volt Typhoon in their systems.

Analysis & Action

Mandiant Intelligence Chief Analyst John Hultquist has warned that defenders in critical infrastructure should urgently work on finding and removing traces of Volt Typhoon, a Chinese government-backed hacking team that has been involved in a series of attacks against targets in Guam and continental United States.

Hultquist said the Volt Typhoon campaign included very deliberate targeting of critical infrastructure organizations and shows that Chinese APTs are changing their TTPs. Volt Typhoon was first identified in Guam, which is an island considered of strategic importance in case of a military conflict between Taiwan and China. The actor was also subsequently identified in infrastructures of critical infrastructure organizations in the continental US, where they have used botnets and zero-days to evade detection.

Hultquist has warned US organizations to monitor for Volt Typhoon activity within their networks and to be aware of geopolitical developments, specifically in the Middle East, as they may trigger an increased activity from additional APTs, most notably Iran-backed actors.

Data Breaches & Data Leaks

Seiko Says Ransomware Attack Exposed Sensitive Customer Data

Summary

- Seiko confirmed BlackCat ransomware attack led to sensitive information being exposed.

Analysis & Action

Japanese watchmaker Seiko was the victim of a BlackCat ransomware attack in July of this year. After an investigation, they confirmed that more than 60,000 pieces of personal data held by three of its departments were leaked. Investigation after the breach suggested that BlackCat bought access to their network from an initial access broker (IAB).

Personally identifiable information (PII) that got leaked by BlackCat included customer names, addresses, phone numbers, and certain emails. Seiko is working with cybersecurity specialists to assess the specific causes of the breach and create new measures to prevent incidents like this one from happening in the future.

Due to the sensitivity of data being held by companies across sectors, it is of the utmost importance for them to have numerous protections in place to prevent data from being accessed and leaked. Multi-factor authentication, as well as encryption, are ways to store data in a protected way. Members are advised to carry out targeted security enhancements to stay ahead of the curve and prevent any future data breaches or cyberattacks.

Redcliffe Labs Exposes Over 12 million Patient Records

Summary

- One of India's largest diagnostic centers just suffered a breach that exposed millions of patient records.

Analysis & Action

Redcliffe Labs, an India-based diagnostics center, exposed over twelve million patient records because of a misconfigured and non-password-protected database.

Medical data that was exposed contains patients' names, doctors, testing locations (whether done at home or a medical facility), and various other personal health details, such as diagnostic scans, test results, and similar sensitive information. The exposed database contains 7TB of data and over 12 million records. It was unclear if any malicious actor took advantage of the exposed data.

The exposure of this kind of sensitive information could lead to ransomware attacks, fraud attempts, and similar. Because of the significant information in their hands, healthcare institutions must prioritize data security by implementing data encryption and stringent security policies for data handling.

Cyber Crimes & Incidents

Espionage Group Uses Webmail Server Zero-Day to Target European Governments

Summary

- The exploitation of a zero-day vulnerability found in the webmail servers of European governments threatens the private data of government officials.

Analysis & Action

An advanced persistent threat (APT) group under the name “Winter Vivern” has been spotted in leading cyberattacks against the governments of Poland, Ukraine, and India. Winter Vivern is reported to be a pro-Russia hacking group.

Winter Vivern exploits internet-facing applications with known vulnerabilities and has a consistent campaign of phishing. A vulnerability found in Roundcube, tracked as CVE-2023-5631, has been the prime target of threat actors because of the webmail software’s connection to government entities. Once the vulnerability has been exploited, threat actors can exfiltrate email messages sent to and from government officials.

This breach in Roundcube might affect healthcare organizations that use the affected webmail software. Members who use Roundcube are highly encouraged to update their software to patch up any vulnerabilities in the system to decrease the chances of threat actors exploiting them.

Vulnerabilities & Exploits

VMware Fixes Critical Code Execution Flaw in vCenter Server

Summary

- VMware disclosed and patched a critical vulnerability tracked as CVE-2023-34048.

Analysis & Action

VMware issued patches addressing critical vCenter Server vulnerabilities that could allow attackers to conduct remote code execution attacks on unpatched devices.

The critical vulnerability, tracked as CVE-2023-34048, is an out-of-bounds write weakness in vCenter's DCE/RPC protocol implementation, and has a 9.8 CVSS (Common Vulnerability Scoring System) score. There is currently no reported exploitation of the vulnerability.

Due to the criticality of the vulnerability, VMware additionally released patches for multiple end-of-life products that are no longer under active support. More detailed information on available patches can be accessed here.

Trends & Reports

A Continuing Cyber-Storm with Increasing Ransomware Threats and a Surge in Healthcare and APAC Region

Summary

- This year, the healthcare industry saw an 11% increase in average weekly cyber-attacks.

Analysis & Action

So far, 2023 has marked a 3% increase in average weekly global cyber-attacks in comparison to the last year. The healthcare industry was the third most affected, with an average of 1,613 attacks per week, indicating a substantial 11% year-over-year surge.

The attacks on healthcare are continuously increasing. Some of the reasons for the trend are valuable data they store, large IoT (Internet of things) networks that increase the attack surface of healthcare organizations, outdated legacy systems and overall poor endpoint security of medical devices, low tolerance for operational disruptions due to the urgency of continuous patient care which makes healthcare institutions more prone to paying ransom quickly. Each of these factors makes the healthcare industry an attractive target for malicious actors.

Members are advised to educate their employees on phishing operations, to apply patches timely, to use anti-ransomware solutions, and to apply overall rigorous security measures to ensure good security posture of their organizations and minimize the risk of cyber-attacks.

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 Record
VMware
techobserver
Bleeping Computer
Security Week
Bleeping Computer
Check Point Research

Tags

Ukraine Targeting, VMware, 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