Health-ISAC Daily Cyber Headlines

Daily Cyber Headlines **TLP:WHITE** **Alert Id: 2d6fca2c** **2022-10-28 12:54:31**

Today's Headlines:

Leading Story

- Slovak and Polish Parliaments Hit by Cyberattacks

Data Breaches & Data Leaks

- Medlab Pathology Breach Impacts 223,000 Australians

Cyber Crimes & Incidents

- New York Post Hacked with Offensive Headlines Targeting Politicians

Vulnerabilities & Exploits

- Windows Event Log Vulnerabilities Could Be Exploited to Blind Security Products
- Google Releases Emergency Chrome 107 Update to Patch Actively Exploited Zero-Day

Trends & Reports

- 86% of Cloud Attacks in the Healthcare Sector Result in Financial Losses

Privacy, Legal & Regulatory

- Nothing to Report

Upcoming Health-ISAC Events

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

Leading Story

Slovak and Polish Parliaments Hit by Cyberattacks

Summary

- Security researchers have observed that cyberattacks hit the Slovak and Polish parliaments on Thursday 27, 2022.

Analysis & Action

Various cyberattacks were registered against the Slovak and Polish parliaments that impacted the voting system in Slovakia's legislature. According to the authorities, the cyberattack was multidirectional and it was assessed by security researchers that the attack's origin included the

Russian Federation.

The impact of the cyberattack paralyzed the entire Slovak parliament computer network which interrupted the parliament's session. The Slovak parliament was in the voting process regarding various bills and as a consequence of the cyberattack parliament's members were not able to use their computers or phone lines which denied their capacity to vote.

Although no attribution of the cyberattack has been granted yet, it was stated by the Slovak parliament's speaker Boris Kollar that the government's technicians have started their activities to remediate the impact as soon as possible.

Data Breaches & Data Leaks

Medlab Pathology Breach Impacts 223,000 Australians

Summary

- Australian Clinical Labs have disclosed a data breach that has compromised the personal information of approximately 223,000 individuals.

Analysis & Action

It was assessed by Australian Clinical Labs, the parent company of Australian Medlab Pathology, that a data breach took place compromising the personal information of 223,000 Australians.

According to the organization, it was possible to determine that an attacker was able to access personal and financial information. It was assessed that individuals' diagnoses; payment cards and national insurance cards data was stolen. The compromised information could expose the affected individuals to cybercrime related activity such as extortion, phishing, and identity theft.

Australian cybersecurity authorities were able to determine that the ransomware as a service threat actor Quantum malware is behind the malicious activity as they took credit for the cyberattack on its leak site. Also, the security researchers observed that the stolen data was available for download on the dark web.

Cyber Crimes & Incidents

New York Post Hacked with Offensive Headlines Targeting Politicians

Summary

- The New York Post has recently confirmed that it was the victim of a cyberattack that compromised its website and Twitter account.

Analysis & Action

The New York Times has recently stated that due to a cyberattack, its website as well as its Twitter account were hacked.

The organization has stated that the threat actors involved published offensive headlines and tweets against various government members including the New York City Mayor, various governors, and the U.S. President. Although investigations have started to determine the tactics, techniques, and procedures that the threat actor employed to compromise The New York Times, no information regarding this incident has been disclosed yet.

This security incident comes in line with the cyberattack against the American business magazine Fast Company that took place one month ago. Various alerts have been released by US agencies regarding disinformation campaigns as well as threat actors aiming to alter US elections and the cyberattack against The New York Times follows this trend.

Vulnerabilities & Exploits

Windows Event Log Vulnerabilities Could Be Exploited to Blind Security Products

Summary

- Varonis has warned that two Even Log vulnerabilities found in Windows could allow threat actors to cause a denial-of-service condition.

Analysis & Action

According to security researchers at Varonis, remote attackers could exploit two Event Log vulnerabilities in Windows to crash the Event Log application. Therefore, as the Event Log application is crushed by the threat actors, this will cause a denial-of-service condition.

The researchers have determined that the vulnerabilities affect all Windows iterations up to Windows 10. The first exploit has been dubbed LogCrusher, which allows a domain user to crash the Event Log on any Windows machine on the domain, and the second vulnerability, tracked as CVE-2022-37981, could allow an attacker to fill the hard drive of a Windows machine log data causing in this was a denial-of-service condition.

Microsoft has already released patches for these vulnerabilities on October 2022 Patch Tuesday.

Google Releases Emergency Chrome 107 Update to Patch Actively Exploited Zero-Day

Summary

- Google has released an emergency update for a vulnerability affecting the V8 JavaScript Engine, active exploitation was observed.

Analysis & Action

It was observed by security researchers at Avast that a zero-day vulnerability affecting V8 JavaScript engine was actively exploited by threat actors.

According to the security researchers at Avast, the vulnerability is tracked as CVE-2022-3723, it has a high severity CVSS score, and it has been described as a type confusion vulnerability. After Avast informed Google about the zero-day vulnerability on October 25, 2022, Google released an emergency update for the Chrome 107 patch to deal with the reported vulnerability.

It was observed by researchers that the zero-day vulnerability reported by Avast is the seventh Chrome zero-day vulnerability that has been patched during 2022. To avoid becoming a victim of cybercrime it is recommended to ensure that CVE-2022-3723 has been properly addressed.

Trends & Reports

86% of Cloud Attacks in the Healthcare Sector Result in Financial Losses

Summary

- Netwrix has released its 2022 Cloud Security Report which offers valuable insights regarding findings on the healthcare sector.

Analysis & Action
The new 2022 Cloud Security Report developed by Netwrix has provided important information regarding the state of cloud security in the healthcare sector.

According to the report, 61% of respondents in the healthcare industry suffered a cyberattack on their cloud infrastructure within the last 12 months. Also, it was possible to determine that phishing was the most common type of attack.

Additionally, it was highlighted that cyberattacks on the healthcare sector implies financial consequences, as 32% of respondents from other industries reported that an attack had no impact on their business while only 14% of healthcare organizations established the same.

Netwrix's full report on Cloud Data Security with a specific focus on healthcare can be accessed here.

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): Security Week, Healthcareinfosecurity, Bleeping Computer, Security Week, Security Week, Dark Reading, netwrix

Tags: Netwrix, Google Zero Day, Windows Event Log, The New York Times, Slovak parliament, Daily Cyber Headlines, DCH

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