Health-ISAC Daily Cyber Headlines

Daily Cyber Headlines | TLP:WHITE | Alert ID : 0942a9b6 | Oct 07, 2021, 10:33 AM

Today's Headlines:

Leading Story

- Data Breach Volumes for 2021 Already Exceed 2020 Total

Data Breaches & Data Leaks

- Cyberattacks Reported by Schneck Medical Center
- Infosec Experts: Twitch Breach as Bad as it Gets

Cyber Crimes & Incidents

- Texan Imprisoned Over COVID-19 Hoax

Vulnerabilities & Exploits

- Unpatched Dahua Cams Vulnerable to Unauthenticated Remote Access

Trends & Reports

- America Urged to Prepare for Shift to Post-Quantum Cryptography

Privacy, Legal & Regulatory

- US Govt to Sue Contractors Who Hide Breach Incidents

Upcoming Health-ISAC Events

- Health-ISAC Monthly Threat Brief – October 28, 2021, 12:00 PM Eastern

Additional Info

Leading Story

Data Breach Volumes for 2021 Already Exceed 2020 Total

Summary

- The number of data breaches publicly reported so far this year has already exceeded the total for 2020, placing 2021 on track for a record year, according to new data from the Identity Theft Resource Center (ITRC).

Analysis & Action

The non-profit's figures for Q3 breach volumes came in at 446 incidents. Although this is lower than the 491 breaches reported in the second quarter, the total for the year-to-date is now 1291, versus 1108 in 2020.

The all-time high of 1529 breaches was set in 2017, but with phishing and ransomware leading the way in driving volumes up this year, it's predicted that 2021 could exceed that figure. The ITRC's figures comprise not only traditional breaches where malicious parties steal data from organizations but also cases of cloud misconfigurations that lead to data leaking into the public domain.

The full ITRC report can be accessed here.

Data Breaches & Data Leaks

Cyberattacks Reported by Schneck Medical Center

Summary

- Schneck Medical Center has announced that it was a victim of a cyberattack which has had a significant impact on organizational operations.

Analysis & Action

The attack was detected on September 29, 2021, and an announcement was made the same day. In response to the attack, all IT systems within its facilities were suspended out of an abundance of caution, and third-party cybersecurity experts have been engaged to assist with the investigation.

Schneck Medical Center said investigations into cyberattacks and the restoration of IT systems take time to fully resolve and are ongoing, but steps have been taken to minimize disruption to its systems.

At this stage, it is unclear if patient information has been compromised.

Infosec Experts: Twitch Breach as Bad as it Gets

Summary

- Content streaming giant Twitch has confirmed a data breach has taken place at the firm after reports claimed a hacktivist leaked its entire source code, creator info, and sensitive internal data.

Analysis & Action

The confirmation comes after a tech news organization reported that an anonymous 4Chan user posted a 125GB torrent link to the site containing the data dump. Sources told the site it could have been taken as recently as early this week.

Leaked data reportedly includes all of the firm's source code; mobile, desktop, and console clients; proprietary SDKs, and internal AWS services; among other properties. Also leaked were red teaming tools used by the firm's SecOps function and financial information on how much it paid its most popular streamers back in 2019, which reached millions of dollars for some.

Cybersecurity experts were quick to ask questions the internal security posture at one of the world's biggest gaming platforms. An internal investigation is ongoing.

Cyber Crimes & Incidents

Texan Imprisoned Over COVID-19 Hoax

Summary

- A man from Texas has been sentenced to 15 months in federal prison after publishing false information on social media.

Analysis & Action

Christopher Charles Perez posted two messages on Facebook in April 2020 in which he falsely claimed to have hired a person infected with COVID-19 to lick items on display at grocery stores. Perez said in the messages that goods for sale in several shops in the San Antonio area had been licked.

On April 5, 2020, a screenshot of the first message posted by Perez was sent to the Southwest Texas Fusion Center (SWTFC) via an online tip. SWTFC then contacted the FBI office in San Antonio, which investigated the matter and found the threats made by Perez to be false.

Following the FBI investigation into his social media posts, Perez was charged with two counts of 18 U.S.C. § 1038, which criminalizes false information and hoaxes related to biological weapons. A federal jury found him guilty of the charges, and on Monday Perez was handed a custodial sentence, sentenced to 15 months in federal prison, and ordered to pay a $1,000 fine.

Vulnerabilities & Exploits

Unpatched Dahua Cams Vulnerable to Unauthenticated Remote Access

Summary

- Unpatched Dahua cameras have been discovered to be vulnerable to two authentication bypass vulnerabilities, proof-of-concept exploit code has also been released to the public.

Analysis & Action

The authentication bypass flaws, tracked as CVE-2021-33044 and CVE-2021-33045, are both remotely exploitable during the login process by sending specially crafted data packets to the target device.

This news comes a month after Dahua's security advisory which urged owners of vulnerable models to upgrade their firmware, but considering how neglected these devices are following their initial installation and set-up, it's likely that many of them are still running an old and vulnerable version.

The list of the affected models is extensive and covers many Dahua cameras, as a recent Shodan search by researchers found over 1.2 million Dahua systems around the world. It is important to clarify that not all of these devices are vulnerable to exploitation, but the list of the affected models contains some widely deployed ones.

The full Dahua security advisory can be accessed here.

Trends & Reports

America Urged to Prepare for Shift to Post-Quantum Cryptography

Summary

- The US Department of Homeland Security (DHS) has teamed up with the Department of Commerce's National Institute of Standards and Technology (NIST) to release a guide on the best way for organizations to navigate the transition to post-quantum cryptography.

Analysis & Action

The guide provides relevant stakeholders with achievable steps they can take to reduce the risks related to the advancement of quantum computing technology. While quantum computing promises unprecedented speed and power in computing, it also poses new risks, said the guide.

The guide's release follows US Secretary of Homeland Security Alejandro Mayorkas' identification of the move to post-quantum encryption as a priority.

DHS's new guidance will help organizations prepare for the transition to post-quantum cryptography by identifying, prioritizing, and protecting potentially vulnerable data, algorithms, protocols, and systems, concluded the report, which can be accessed here.

Privacy, Legal & Regulatory

US Govt to Sue Contractors Who Hide Breach Incidents

Summary

- Under the newly announced Civil Cyber-Fraud Initiative, sponsored by the US Department of Justice (DoJ), government contractors are now held accountable in a civil court if they don't report a breach or fail to meet required cybersecurity standards.

Analysis & Action

The initiative gives the DoJ the necessary leverage to fight digital threats to sensitive information and critical systems stemming from collaborators of federal agencies. The Civil Cyber-Fraud Initiative aims to strengthen defenses and minimize the risk of intrusion on government networks due to poor cybersecurity practices from external partners. Led by the Civil Division's Commercial Litigation Branch, Fraud Section, the initiative will use the False Claims Act (FCA), which makes liable anyone who knowingly submits false claims to the government.

The initiative will hold accountable entities or individuals that put U.S. information or systems at risk by knowingly providing deficient cybersecurity products or services, knowingly misrepresenting their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cybersecurity incidents and breaches, said the DoJ.

Reference | References

idtheftcenter
Info Security Magazine
Bleeping Computer
Info Security Magazine
HIPAA Journal
Health-ISAC
Info Security Magazine
dahuasecurity
Info Security Magazine
DHS
Bleeping Computer
Health-ISAC

Tags

Daily Cyber Headlines, DCH