DAILY CYBER HEADLINES

Health-ISAC Daily Cyber Headlines

TLP:GREEN

Nov 23, 2021

Today's Headlines:

Leading Story

- Hackers Hit Iran's Mahan Airline, Claim Confidential Data Theft

Data Breaches & Data Leaks

- Over a Million WordPress Sited Breached
- University Hospital Newark Notifies More Than 19k Individuals about Historic Insider Theft

Cyber Crimes & Incidents

- UK Govt Warns Thousands of SMBs Their Online Stores Were Hacked

Vulnerabilities & Exploits

- New Windows Zero-Day with Public Exploit Lets You Become an Admin

Trends & Reports

- October 2021 Healthcare Data Breach Report
- 32% of Healthcare Organizations Have a Comprehensive Security Program

Privacy, Legal & Regulatory

- Nothing to Report.

Upcoming Health-ISAC Events

- Health-ISAC Monthly Threat Brief – November 23, 2021, 12:00 PM Eastern

Leading Story

Hackers Hit Iran’s Mahan Airline, Claim Confidential Data Theft

Summary

- One of Iran’s largest privately owned airlines, Mahan Air, has announced a cybersecurity incident that has resulted in its website going offline and potentially data loss.

Analysis & Action

The firm announced over Twitter that the flight schedules won’t be affected, although people cannot access Mahan’s website. The firm stated that cybersecurity issues are considered a normal occurrence and that the Mahan Cyber Security Team has always acted in a timely manner and thwarted previous attacks.

The actor who took responsibility for the attack is known as Hooshryarane Vatan, who claims to fight for the rights of the Ahwaz minority. The actor claims to have stolen confidential documents exposing how Mahan Air has worked with Iran’s Islamic Revolutionary Guard Corps (IRGC) and threatened to publish names, numbers, and proof of Mahan’s activities.

Mahan Air was added to the United States sanctions list in 2011 for supporting members of Iran’s Islamic Revolutionary Guard Corps, for transportation of operatives, weapons, equipment, and funds abroad in support of the IRGC’s regional operations.

Data Breaches & Data Leaks

Over a Million WordPress Sited Breached

Summary

- GoDaddy reports that data on 1.2 million of its WordPress customers have been exposed.
- GoDaddy is currently reissuing and installing new certificates for customers.

Analysis & Action

GoDaddy’s Chief information security officer reported a breach of 1.2 million active and inactive managed WordPress customers. Customers had both their email addresses and customer numbers exposed, putting them at greater risk of phishing attacks. In addition, the WordPress admin password created at installation has also been exposed, and the company urges customers to change it immediately.

Active customers also had their database usernames and passwords exposed, which has been reset by GoDaddy. In addition, some active customers had their secure-socket layer private key exposed, and GoDaddy is currently issuing and installing new certificates for these customers.

University Hospital Newark Notifies More Than 19k Individuals about Historic Insider Theft

Summary

- University Hospital Newark (NY) has discovered the protected health information (PHI) of thousands of patients has been acquired by a former employee, who accessed and disclosed the information to other third parties over the course of a year.

Analysis & Action

The unauthorized access occurred between January 1, 2016, and December 31, 2017, after a former employee had been provided with access to patient data to complete work duties but had exceeded the authorized use of that access and had viewed patient data not pertinent to job functions.

The types of information viewed include names, addresses, dates of birth, social security numbers, health insurance information, medical record numbers, and clinical information related to care for patients. University Hospital said the matter has been reported to law enforcement and a criminal investigation into the unauthorized access and disclosure is ongoing.

University Hospital has stated mailing notification letters to affected individuals and has reviewed internal policies and procedures on patient privacy.

Cyber Crimes & Incidents

UK Govt Warns Thousands of SMBs Their Online Stores Were Hacked

Summary

- The UK’s National Cyber Security Center (NCSC) Says it warned the owners of more than 4,000 online stores that their sites were compromised in Magecart attacks to steal customers’ payment information.

Analysis & Action

In Magecart attacks, also known as web skimming, digital skimming, or e-skimming, threat actors inject scripts known as credit card skimmers into compromised online stores to harvest and steal the payment and/or personal information submitted by customers at the checkout page.

The attackers will later use this data for various financial and identity theft fraud schemes or sell it to the highest bidder on hacking or carding forums. The NCSC identified 4,151 compromised online shops up to the end of September 2021 and alerted retailers to those security vulnerabilities.

Impacted online retailers are urged to keep Magento and other software up to date to block attackers’ attempts to breach their servers and compromise their online shops and customers' information during Black Friday and Cyber Monday.

Resources to stay safe online while shopping can be found here.

Vulnerabilities & Exploits

New Windows Zero-Day With Public Exploit Lets You Become an Admin

Summary

- A security researcher has publicly disclosed an exploit for a new Windows Zero-Day local privilege elevation vulnerability that gives admin privileges in Windows 10, Windows 11, and Windows Server.

Analysis & Action

Using this vulnerability, threat actors with limited access to a compromised device can easily elevate their privileges to help spread laterally within the network. The vulnerability affects all supported versions of Windows, including Windows 10, Windows 11, and Windows Server 2022.

As part of the November 2021 Patch Tuesday, Microsoft fixed a Windows Installer Elevation of Privilege Vulnerability tracked as CVE-2021-41379. This new vulnerability was discovered by a security researcher who found a bypass to the patch and a more powerful new zero-day privilege elevation vulnerability after examining Microsoft’s fix. As is typical with zero-days, Microsoft will fix the vulnerability in a future Patch Tuesday update and urges users to wait until the patch is released, as attempting to patch the binary themselves will likely break the installer.

More information can be found here.

Trends & Reports

October 2021 Healthcare Data Breach Report

Summary

- October 2021 saw 59 data breaches of 500 or more records reported to the US Department of Health and Human Services' Office for Civil Rights, a 25.5% increase from September.

Analysis & Action

From November 2020 to October 2021, there have been 655 reported breaches of 500 or more records, 546 of which have been reported in 2021. The protected health information (PHI) of 3,589,132 individuals was exposed, stolen, or impermissibly disclosed across the 59 reported data breaches, which is 186% more records than September.

There were 18 data breaches reported to the Health and Human Services' Office for Civil Rights in October that impacted 10,000 or more individuals. Phishing remains the leading attack vector in ransomware attacks, and the main cause of data breaches in October was hacking or IT incidents. In addition, 22 breaches were classified as unauthorized access/disclosure incidents and involved the PHI of 200,887 individuals, where the average breach size was 9,131 records.

The full report can be found at the link posted above.

[32% of Healthcare Organizations Have a Comprehensive Security Progam]

Summary

- Core components of a comprehensive security program include regular reporting of security deficiencies and having a designated CISO.

Analysis & Action

32% of surveyed acute and ambulatory care organizations had a comprehensive security program in 2021, according to the College of Healthcare Information Management Executives (CHIME) survey. CHIME found that only 26% of long-term/post-acute organizations were considered to have a comprehensive security program. CHIME has recently updated some of its standards for 2021 to reflect industry advances, raising the bar for surveyed organizations.

Under the new standard, a program must include employee security training and education, a dedicated cybersecurity committee, and annual risk assessments to identify compliance gaps and security vulnerabilities. They must also include annual cyber response tabletop exercises, regular reporting of security progress to the board, an annually updated inventory of all business associates, a documented risk management program, a designated security operations officer, and a designated chief information security officer.

The full report can be read here.

Privacy, Legal & Regulatory

There is nothing to report.

Health-ISAC Cyber Threat Level

On November 4, 2021, the H-ISAC Threat Intelligence Committee (TIC) evaluated the current Cyber Threat Level and collectively decided to maintain the current Cyber Threat Level at Blue (Guarded). The Threat Level is remaining Blue (Guarded) due to ongoing threats from Qakbot, Zloader, and Dridex campaign observances, observed threat actors initiating phishing email campaigns and observances of BazarLoader malware

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)	HIPAA Journal, Health-ISAC, Microsoft, Health IT Security, Bleeping Computer, Bleeping Computer, cisa, ZDNet, HIPAA Journal, Bleeping Computer, Health-ISAC, chimecentral

Alert ID 94c8b835

View Alert

Tags Daily Cyber Headlines, DCH

TLP:GREEN Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.

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

Download Health-ISAC's Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.