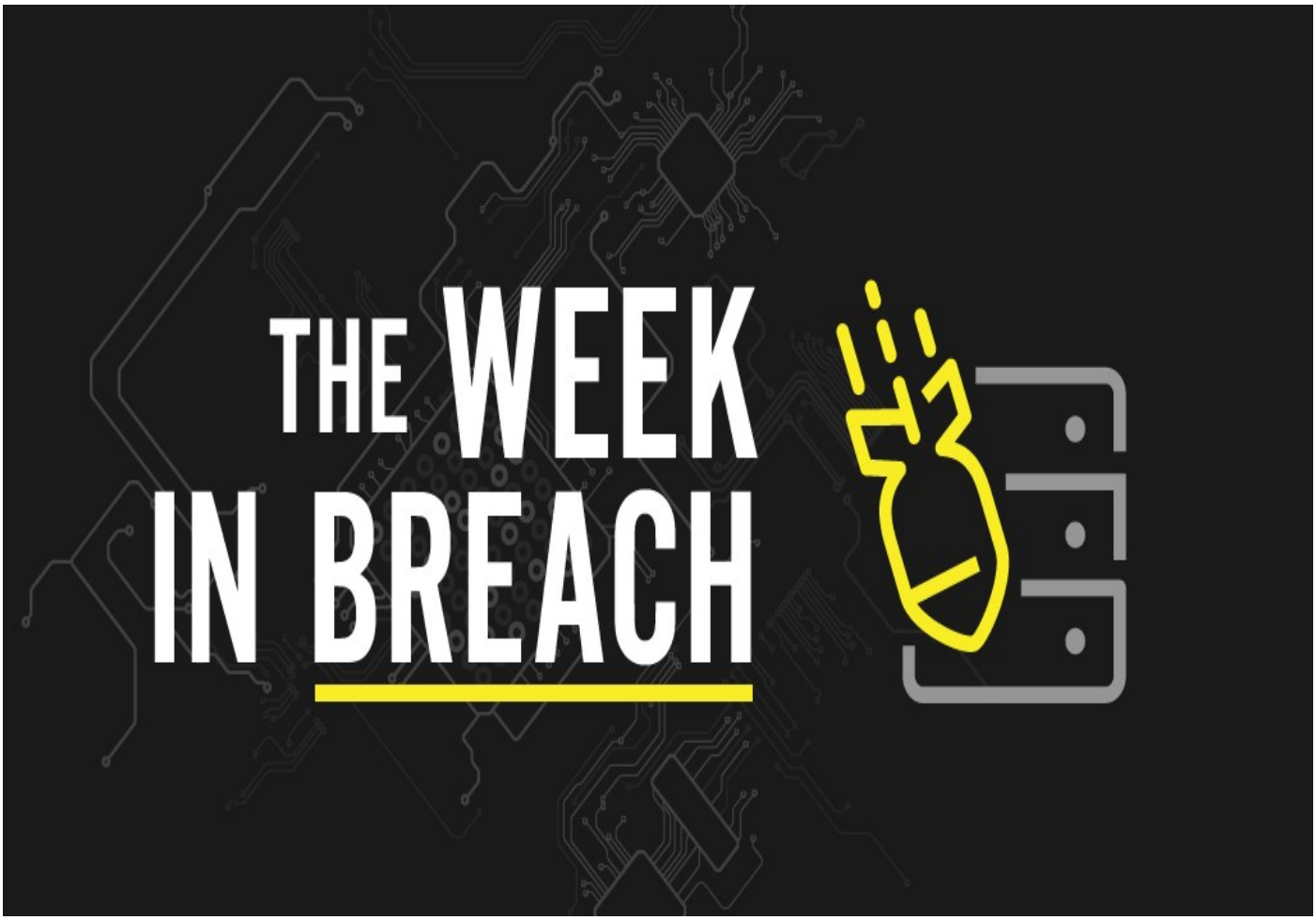
THE WEEK IN BREACH NEWS: 03/08/23 - 03/14/23

DenBe Computer Consulting
Connecting Business

March 15th 2023 by Dennis Jock



If your business isn't using our ***Dark Web Monitoring Services*** please call us for a free scan and to discuss setting up this cutting edge monitoring service for you!

Not ready to talk yet? Visit our website to get your ***FREE Dark Web Scan.*** You will get a free, no obligation scan sent to your inbox within 24hrs. ***Visit today: www.denbeconsulting.com***

U.S. Marshals Service
https://www.cbsnews.com/news/us-marshals-office-cyber-attack-compromised-sensitive-data/

Exploit: Ransomware

U.S. Marshals Service: Federal Agency

Risk to Business: 1.402 = Extreme

The U.S. Marshals Service announced that it is investigating a ransomware attack on its system. The attack has compromised some of its most sensitive information, including law enforcement materials, and the personal information of employees and potential targets of federal investigations. In the February 17 incident, cybercriminals were able to obtain access to sensitive administrative data including personal information of certain employees, and data about wanted fugitives, as well as information on unidentified third parties. The affected system also contained sensitive law enforcement information like ongoing legal procedures.

How It Could Affect Your Business: Highly sensitive data like this can do a lot of damage in the wrong hands

Pipefitters Local 537
https://www.securityweek.com/cyberattack-on-boston-union-results-in-6-4m-loss/

Exploit: Business Email Compromise

Pipefitters Local 537: Trade Union

Risk to Business: 1.702 = Severe

Pipefitters Local 537 in Boston is investigating a cyberattack that resulted in a loss of $6.4 million. Officials called the incident a social engineering attack, saying that their internal systems were not compromised or hacked. The evidence so far points to a business email compromise attack. The union was quick to assure members that it does not appear that the personal information of members was stolen or compromised and that this attack will have no impact on the members' health fund. The incident is under investigation by private and federal investigators.

How It Could Affect Your Business: Business email compromise is a dangerous and damaging nightmare that can strike any organization even charities and professional groups.

Animker.com
https://www.hackread.com/video-marketing-software-animker-data-leak/

Exploit: Misconfiguration

Animaker: Video Marketing Software Maker

Risk to Business: 1.808 = Severe

A misconfigured database owned by Animaker.com has exposed test and personal data belonging to over 700,000 people who are users of the websites getshow.io (an all-in-one video marketing platform) and animaker.com (a DIY video animation software). The database contains 5.3 GB of data, and new data is still being added daily. Exposed data includes full names, device type, postal codes, IP addresses, mobile numbers, email addresses, Animaker profile details and user country/city/state/location. The company doesn't think that user passwords were exposed.

How It Could Affect Your Customers' Business: Employee mistakes like misconfiguring a database are gateways to expensive problems like this.

Chick-fil-A
https://www.bleepingcomputer.com/news/security/chick-fil-a-confirms-accounts-hacked-in-months-long-automated-attack/

Exploit: Hacking

Chick-fil-A: Fast Food Restaurant Chain

Risk to Business: 2.779 = Moderate

Fast food giant Chick-fil-A has confirmed that over 71,000 customers' accounts were breached in a months-long credential stuffing attack. In this attack, threat actors were able to use customers' stored rewards balances and access those customers' personal information. In a security notice submitted to multiple Attorney General offices, the company specified that they suffered a credential stuffing attack between December 18, 2022, and February 12, 2023. This sustained attack allowed the threat actors to hack a total of 71,473 Chick-fil-A accounts. The cybercriminals had access to customers' personal information including their name, email address, Chick-fil-A One membership number and mobile pay number, QR code, masked credit/debit card number and the amount of Chick-fil-A credit (e.g., e-gift card balance) on your account (if any).

How It Could Affect Your Customers' Business: The incidence of credential stuffing attacks has been growing in the past two years.

Denver Public Schools (DPS)
https://www.9news.com/article/news/crime/denver-public-schools-cybersecurity-incident/73-5a79182e-4b9d-49b0-ab32-5dfe98b269ee

Exploit: Hacking

Denver Public Schools (DPS): Regional Education Authority

Risk to Business: 1.783 = Severe

Denver Public Schools (DPS has disclosed that the personal information of an estimated 15,000 system employees was recently exposed in a hacking incident. The district said that between Dec. 13, 2022, and Jan. 13, 2023, a hacker accessed, and potentially downloaded employee-related files stored on the district's computer servers. Data stolen in this incident includes the names and Social Security numbers of current and former participants in the DPS employee health plan, employee fingerprints, bank account numbers or pay card numbers, driver's license numbers, passport numbers and health plan enrollment information. No student information was involved.

How It Could Affect Your Customers' Business: School systems have been under fire from cybercrime gangs hoping for a quick payout.

Southeastern Louisiana University
https://www.govtech.com/education/higher-ed/southeastern-louisiana-university-likely-suffered-cyber-attack

Exploit: Hacking

Southeastern Louisiana University: Institution of Higher Learning

Risk to Business: 1.709 = Severe

Southeastern Louisiana University is experiencing a cyberattack that has left students and staff unable to access systems for at least five days. The university was left without a functional website, email system or system for submitting assignments after being forced to shut its network down as a response to an unnamed cyberattack. Students and faculty have been struggling with getting though daily business like completing coursework and conducting remote classes since late last week. Systems are slowly being restored.

How It Could Affect Your Customers' Business: The time-sensitive nature of online learning has made colleges bigger targets for cyberattacks.