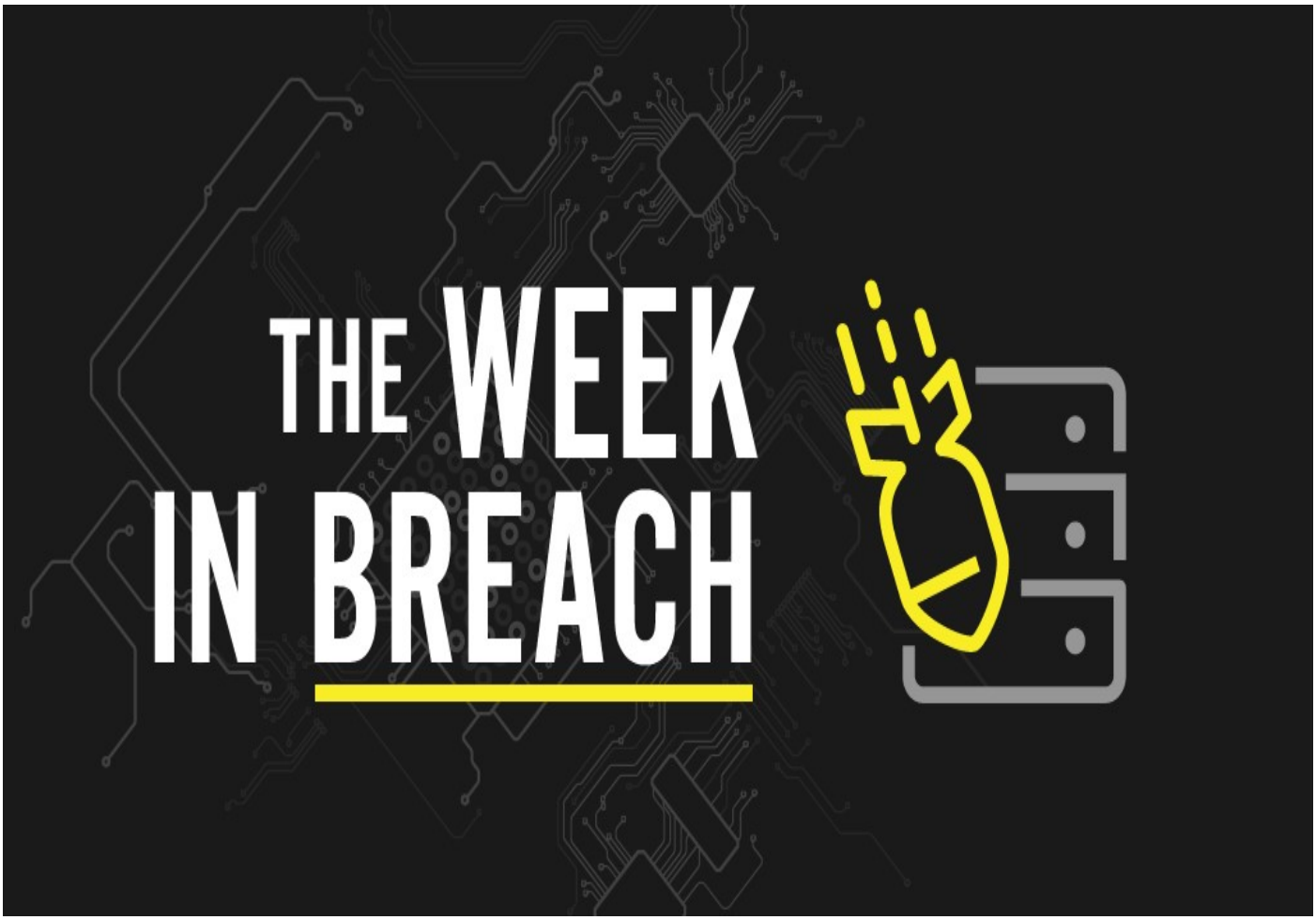
THE WEEK IN BREACH NEWS: 06/28/23 - 07/04/23

DenBe Computer Consulting
Connecting Business

July 5th 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***

Gen Digital

https://www.securityweek.com/norton-parent-says-employee-data-stolen-in-moveit-ransomware-attack/

Exploit: Ransomware

Gen Digital: Technology Company

Risk to Business: 1.886 = Severe

Gen Digital, the parent company of cybersecurity brands such as Avast, Avira, AVG, Norton, and LifeLock, has confirmed that employees' personal information was compromised in a ransomware attack tied to the MOVEit exploit. The company disclosed that some personal information of Gen employees and contractors was potentially exposed including a worker's name, company email address, employee ID number, and in some limited cases home address and date of birth. The company was quick to note that it does not believe that any customer data was stolen.

How It Could Affect Your Business: Zero-day attacks and similar exploits are an unfortunate reality that businesses have to handle now and moving forward.

Reddit

https://www.bleepingcomputer.com/news/security/reddit-hackers-threaten-to-leak-data-stolen-in-february-breach/

Exploit: Ransomware

Reddit: Online Forum

Risk to Business: 1.876 = Severe

BlackCat claims that it snatched 80GB of data from Redditt in a ransomware attack in February 2023 that is just coming to light. Reddit confirmed the attack, admitting that the bad actors made off with an array of internal documents, source code, employee data and limited data about the company's advertisers. User data was not impacted. In an interesting twist, BlackCat is threatening to leak Reddit's data if the company doesn't pay the ransom and backtrack on its plans on charging for API access. Reddit has been facing backlash over its plan to charge for API access at an expected price of $0.24 per 1,000 calls.

How It Could Affect Your Business: Using ransomware to punish companies for instituting unpopular policies is just one more use for that dangerous menace.

The California Public Employees' Retirement System (CalSTRS)

https://www.planadviser.com/calpers-calstrs-hit-third-party-cybersecurity-breach/

Exploit: Ransomware

The California Public Employees' Retirement System (CalSTRS): Benefits System

Risk to Business: 1.469 = Severe

The California Public Employees' Retirement System, the largest of its kind in the U.S., has announced that it has fallen victim to a cyberattack thanks to the MOVEit exploit that may impact 769,000 members. CalSTRS said that it became mixed up in this ongoing cyber incident through one of its service providers, PBI Research Services, on June 24. How much and what kind of data was stolen was not available at press time. CalSTRS says that retirees and beneficiaries with impacted personal information are being contacted by mail. The California State Teachers Retirement System, the public pension fund serving California teachers, has also disclosed that it is a victim of a similar attack.

How It Could Affect Your Business: Many exploits can be avoided by regularly patching and updating software and systems.

Zacks Investment Research

https://www.bleepingcomputer.com/news/security/have-i-been-pwned-warns-of-new-zacks-data-breach-impacting-8-million/

Exploit: Hacking

Zacks Investment Research: Data and Analysis Firm

Risk to Business: 2.149 = Severe

Airline pilot recruiting platform Pilot Credentials has disclosed that it has experienced a data breach. The Texas-based company said that bad actors obtained access to its network on April 30 and the impacted airlines, including Southwest Airlines and American Airlines, were notified of the attack on May 3. The files stolen contained a range of data about pilot applicants, including their names, Social Security numbers, passport numbers, driver's license numbers, dates of birth, Airman Certificate numbers, and other government-issued identification numbers. An estimated 8000 people had their data exposed.

How It Could Affect Your Business: This kind of very specialized data has many uses for bad actors, especially for spear phishing.