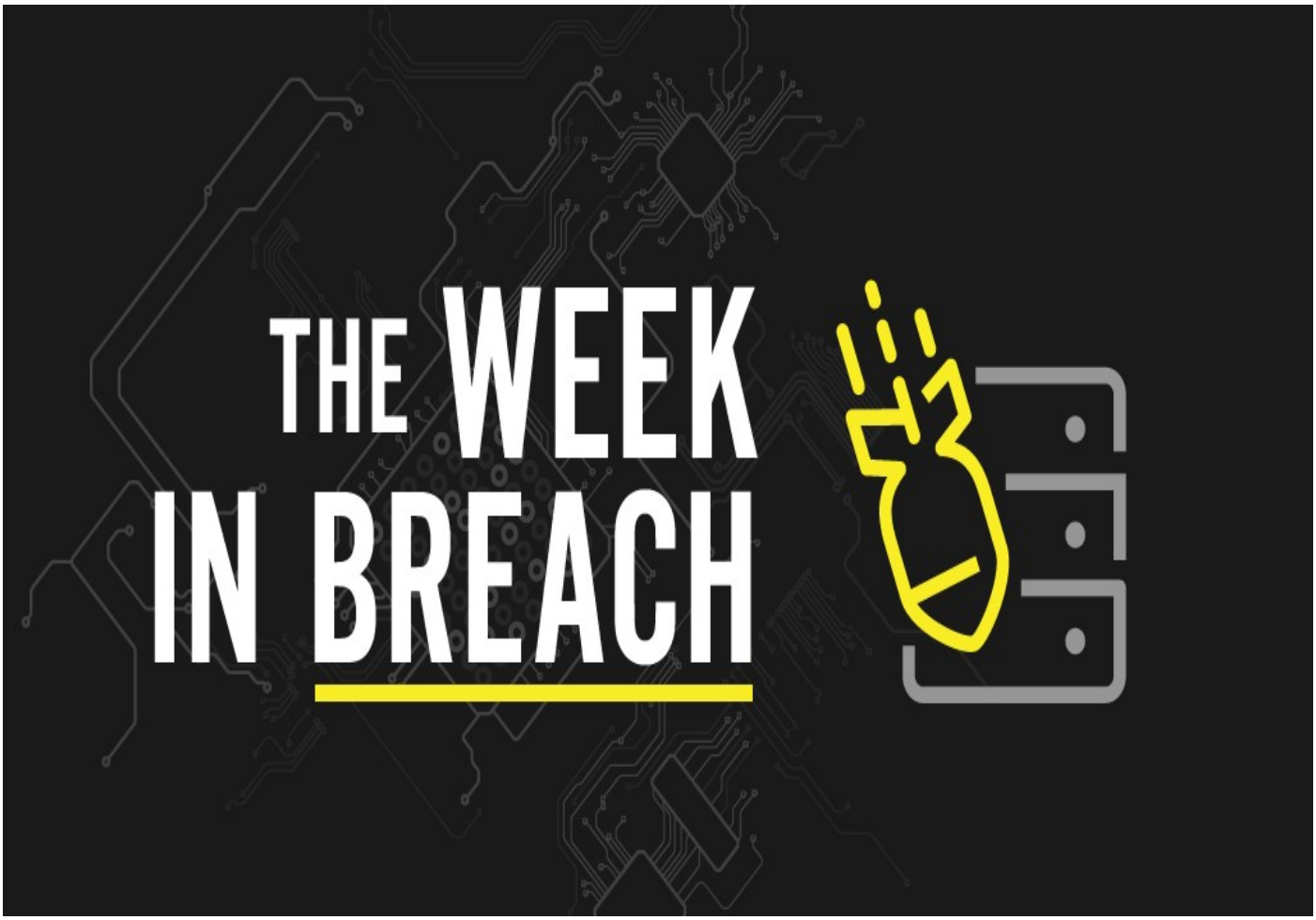
THE WEEK IN BREACH NEWS: 05/10/23 –05/16/23

DenBe Computer Consulting
Connecting Business

May 17th 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***

Murfreesboro Medical Clinic & SurgiCenter (MMC)
https://www.hipaajournal.com/ransomware-attack-results-shutdown-operations-tn-medical-clinic/

Exploit: Ransomware

Murfreesboro Medical Clinic & SurgiCenter (MMC): Healthcare Provider

Risk to Business: 1.622 = Extreme

The Murfreesboro Medical Clinic & SurgiCenter (MMC)in Tennessee has been forced to shut down operations for two weeks as the result of a devastating ransomware attack. The incident began on April 22, resulting in a complete shutdown of the facility's systems to limit the spread of the attack. Some individual offices within the system have reopened, but many major functions including a surgical center remain closed. MMC officials said that they have been working with cybersecurity experts and law enforcement to investigate the incident and determine the extent of the attack and restore full operations.

How It Could Affect Your Business: a virtually complete closure for two weeks is a disaster for this medical group and the community it serves.

AvidXchange
https://techcrunch.com/2023/05/03/avidxchange-second-ransomware-attack-2023/

Exploit: Ransomware

AvidXchange: Payment Processor

Risk to Business: 1.762 = Severe

North Carolina-based payments company AvidXchange has disclosed that it is suffering its second ransomware incident of 2023. The RansomHouse ransomware gang has claimed responsibility for the attack and released the stolen data on its leak site. That data includes non-disclosure agreements, employee payroll information and corporate bank account numbers. The data that was published by RansomHouse also includes many user accounts' login details, including usernames, passwords and, in some cases, answers to security questions for a variety of the company's systems, including cloud accounts and security software, through to smart door locks and surveillance cameras. The company said that it detected the intrusion in early April.

How It Could Affect Your Business: This type of financial data is extremely desirable on the dark web and valuable to bad actors, so it needs strong protection.

The City of Dallas, TX
https://www.securityweek.com/ransomware-attack-affects-dallas-police-court-websites/

Exploit: Ransomware

The City of Dallas, TX: Municipal Government

Risk to Business: 1.681 = Severe

A ransomware attack on the systems of the city government of Dallas, Texas impacted some systems last week. The attack shut down the Police Department and City Hall websites as well causing jury trials to be postponed in the Municipal Court. The computer-assisted dispatch system that is used to help firefighters respond to emergency calls was also knocked out, forcing first responders that utilize those systems to handle dispatch manually. The city said that the attack's impact was limited and it's working to restore affected systems. No word of any ransom demand and no one has claimed responsibility.

How It Could Affect Your Business: Governments and government agencies of every size have been prime targets for ransomware attacks in the past few years.

Edison Learning
https://thejournal.com/articles/2023/05/01/ransomware-gang-claims-edison-learning-data-theft.aspx

Exploit: Ransomware

Edison Learning: Education Management Organization

Risk to Business: 2.719 = Moderate

The Royal ransomware gang says that it is responsible for a ransomware attack on public school and distance learning management company Edison Learning. The group added Edison Learning to its dark web data leak site on April 26. It claims to have stolen 20GB of the company's data including personal information of employees and students. Edison Learning has confirmed the incident but refused to provide further details, saying that an investigation is ongoing.

How It Could Affect Your Customers' Business: Because of the time-sensitive nature of their operations, schools are prime targets for ransomware attacks.

Webster Bank
https://www.ctinsider.com/news/article/webster-bank-data-breach-ct-customers-17906370.php

Exploit: Supply Chain Attack

Webster Bank: Bank

Risk to Business: 1.663 = Severe

Hundreds of thousands of customers of Webster Bank have had their data exposed after a data breach at one of the bank's service providers. The bank notified regulators and customers after being informed of an intrusion between Nov. 27, 2022, and Jan. 22, 2023, at fraud detection services provider Guardian Analytics. In a filing with the Connecticut Attorney General's Office, Webster Bank disclosed that 153,754 Connecticut customers were affected — 117,278 of whom had their name and account number exposed, while 36,476 had their name, account number and Social Security numbers exposed.

How It Could Affect Your Customers' Business: Supply chain attacks have been escalating, bringing fresh danger to businesses in every sector.