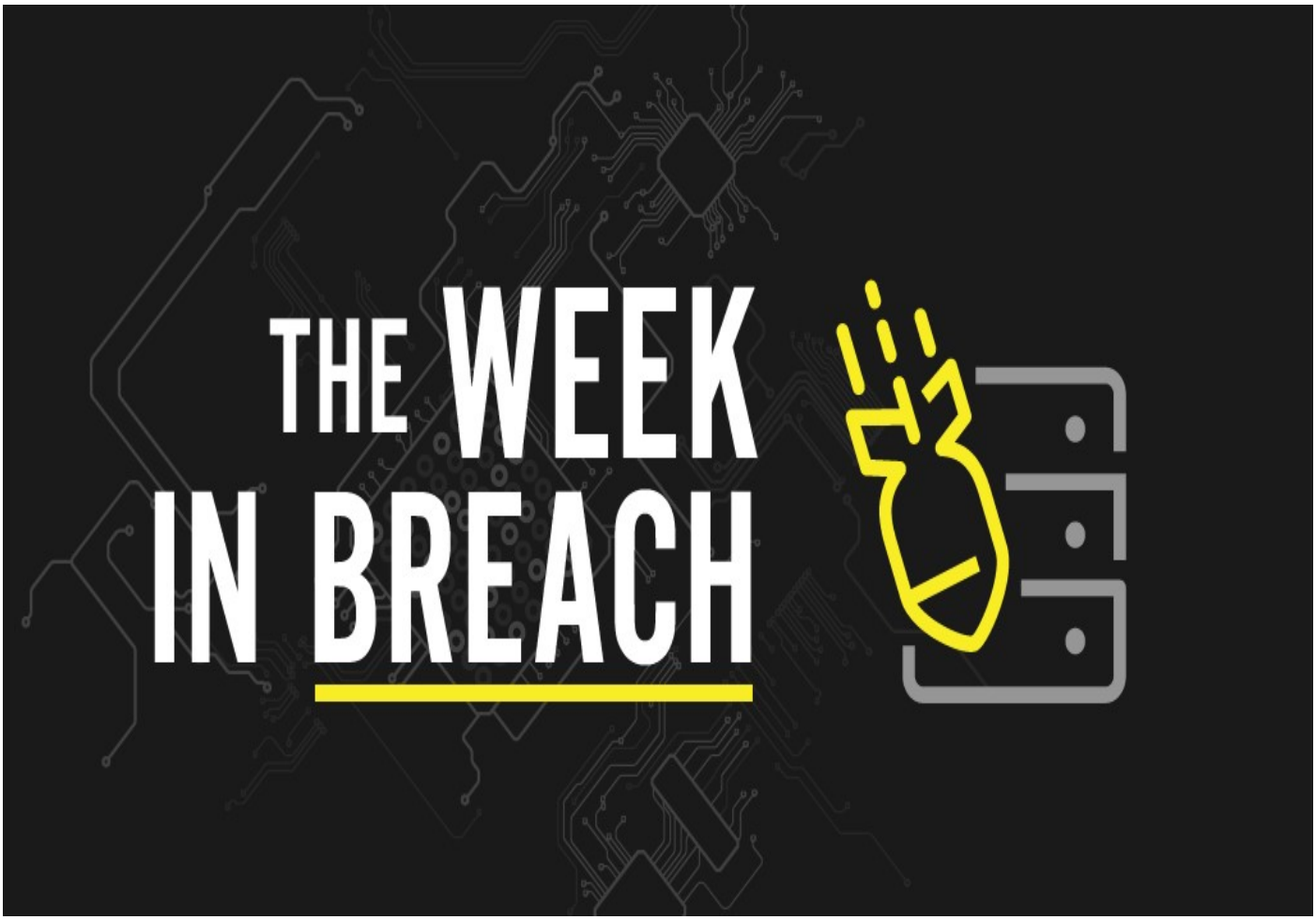
THE WEEK IN BREACH NEWS: 04/26/23 - 05/02/23

DenBe Computer Consulting
Connecting Business

May 3rd 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***

American Bar Association
https://www.bleepingcomputer.com/news/security/american-bar-association-data-breach-hits-14-million-members/

Exploit: Hacking

American Bar Association: Professional Group

Risk to Business: 1.673 = Severe

The American Bar Association (ABA) has experienced a data breach that has exposed information pertaining to 1,466,000 members. The ABA disclosed that a hacker was detected on its network on March 17th, 2023. An ABA statement noted that "An unauthorized third party acquired usernames and hashed and salted passwords that you may have used to access online accounts on the old ABA website prior to 2018 or the ABA Career Center since 2018."

How It Could Affect Your Business: Big batches of credentials like this are gold for cybercriminals and can be used to facilitate other cyberattacks.

Consumer Financial Protection Bureau (CFPB)

https://edition.cnn.com/2023/04/20/business/cfpb-confidential-data/index.html

Exploit: Malicious Insider

Consumer Financial Protection Bureau (CFPB): Federal Agency

Risk to Business: 1.213 = Extreme

The U.S. Consumer Financial Protection Bureau (CFPB) says that they've experienced a data breach caused by the actions of a potentially malicious employee. In the incident, a now former employee sent a total of 14 emails that included consumer personally identifiable information to their private email address. Along with that data, the employee sent two spreadsheets that listed names and transaction-specific account numbers related to about 256,000 consumer accounts at an unnamed institution. The CFPB also said that they identified data from another institution that included approximately 140 loan numbers, of which roughly 100 also included de-identified information related to the loan or borrower, such as income, credit score and demographic information. The CFPB said that The Office of Inspector General and Federal lawmakers and government agencies have been notified,

How It Could Affect Your Business: Malicious insiders can do a lot of damage quickly through actions like stealing sensitive data and selling it.

CommScope
https://techcrunch.com/2023/04/17/hackers-publish-sensitive-employee-data-stolen-during-commscope-ransomware-attack/

Exploit: Ransomware

CommScope: Infrastructure Provider

Risk to Business: 1.681 = Severe

The Vice Society ransomware gang has added CommScope to their dark web leak site. The data published included a variety of information including internal documents, invoices and technical drawings. The personal data of thousands of CommScope employees was also exposed, including full names, postal addresses, email addresses, personal numbers, Social Security numbers, bank account information, scans of employee passports and visa documentation. The company has disclosed that the attack happened on March 23.

How It Could Affect Your Customers' Business: Internal data including contracts and technical data is very valuable and profitable for bad actors.

Point32 Health
https://www.hipaajournal.com/major-massachusetts-health-insurer-suffers-ransomware-attack/

Exploit: Ransomware

Point32 Health: Health Insurer

Risk to Business: 1.681 = Severe

The Vice Society ransomware gang has added CommScope to their dark web leak site. The data published included a variety of information including internal documents, invoices and technical drawings. The personal data of thousands of CommScope employees was also exposed, including full names, postal addresses, email addresses, personal numbers, Social Security numbers, bank account information, scans of employee passports and visa documentation. The company has disclosed that the attack happened on March 23.

How It Could Affect Your Customers' Business: Internal data including contracts and technical data is very valuable and profitable for bad actors.

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.