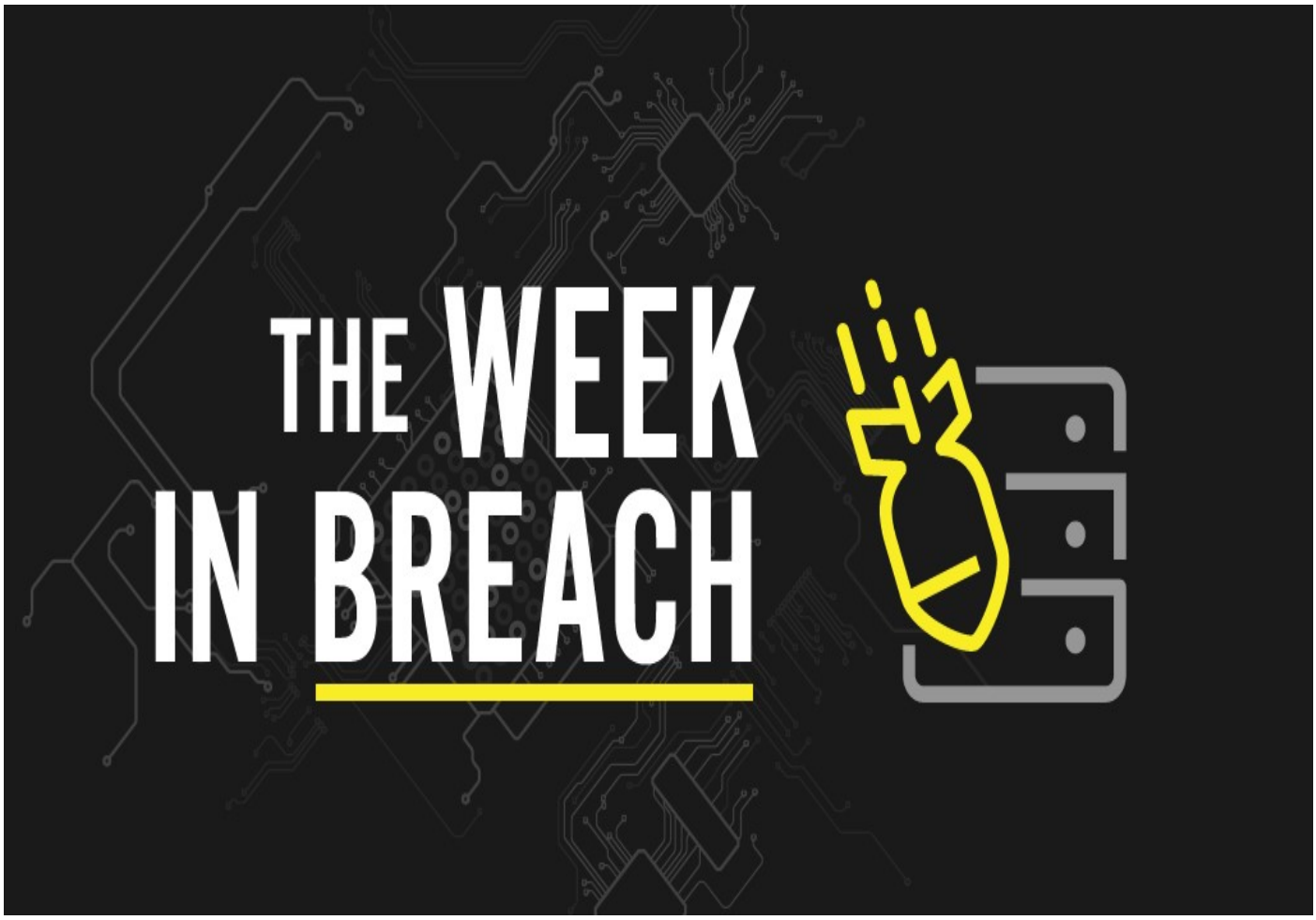
The Week in Breach News: 02/02/22 – 02/08/22

DenBe Computer Consulting
Connecting Business

February 09, 2022 by Dennis Jock



Cybercriminals take a bite out of a UK snack company, a massive ransomware attack hampers fuel operations at EU ports, more De Fi hacks and why you should be worried about cryptocurrency risk.

Morley Companies Inc.

https://www.safetydetectives.com/news/business-services-provider-morley-discloses-ransomware-attack/

Exploit: Ransomware

Morley Companies Inc.: Business Services

Risk to Business: 1.507= Severe

Morley Companies, a business service provider to several Fortune 500 companies, announced that it had been hit with a ransomware attack that may have exposed sensitive information for more than 500,000 people. In a statement, the company said that "a ransomware-type malware had prevented access to some data files on our system beginning August 1, 2021, and there was an unauthorized access to some files that contained personal information.", chalking up the delay in notifying possible victims of this exposure to the complexities of the incident investigation.

Individual Risk: 1.663= Severe

Morley Companies said the attack affected the information of "current employees, former employees and various clients." The potentially compromised information leaked includes names, addresses, Social Security numbers, dates of birth, client identification numbers, medical diagnostic and treatment information and health insurance information. The company is offering credit monitoring and identity theft protection for victims.

Customers Impacted: 500,000

How It Could Affect Your Business *Companies that store large quantities of personal or medical information are prime targets for the bad guys.*

Civicom, Inc.

https://abcnews.go.com/International/wireStory/official-puerto-ricos-senate-targeted-cyberattack-82495236

Exploit: Misconfiguration

Civicom Inc.: Business Services

Risk to Business: 2.017 =Severe

Civicom is in hot water after leaving 8 TB of data exposed in an unsecured AWS S3 bucket. The New York-based company specializes in virtual conferencing facilitation, transcription and research services. With offices in the United States, the Philippines and the United Kingdom. Ultimately, Civicom exposed records containing more than 100,000 files including thousands of hours of audio and video recordings containing private conversations as well as written transcripts of meetings and calls by the company's clients.

Individual Impact: No specifics about consumer/employee PII or financial data loss were available at press time.

Customers Impacted: Unknown

How It Could Affect Your Business *This is not an uncommon mistake, but it's always a problem and could be an expensive regulatory disaster in some industries*

Wormhole

https://indianexpress.com/article/technology/crypto/hackers-steal-nearly-320-million-worth-of-crypto-assets-from-wormhole-7758034/

Exploit: Hacking

Wormhole: De Fi Platform

Risk to Business: 1.227= Extreme

Hackers swooped in and snatched up more than $320 million from De Fi platform wormhole this week. The DeFi platform, a bridge between cryptocurrency Solana (SOL) and other blockchains, was exploited for approximately 120,000 wrapped Ethereum in what is thought to be the second-largest cryptocurrency hack to date. Wormhole's parent company Jump Crypto pledged to replace the 120,000 ether Wormhole lost. The company was quick to note that the crypto was stolen through exploiting a vulnerability in the

Individual Impact: No specifics about consumer/employee PII or financial data loss were available at press time.

Customers Impacted: Unknown

How It Could Affect Your Business *De Fi has been a hotbed of having activity as cybercriminals seek quick scores of cryptocurrency, and there's no end to the danger in sight.*

News Corp.

https://www.reuters.com/business/media-telecom/news-corp-says-one-its-network-systems-targeted-by-cyberattack-2022-02-04/

Exploit: Nation-State Cybercrime

News Corp.: Media & Publishing Company

Risk to Business: 2.071 = Severe

Major media company News Corp. has disclosed that it was the target of a cyberattack by suspected Chinese nation-state hackers. The attack came to light in late January and affected News Corp. business units, including The Wall Street Journal and its parent company Dow Jones, the New York Post, News U.K. and News Corp. Headquarters. The hack affected emails and documents of what it described as a limited number of employees, including journalists. The incident is under investigation.

Individual Impact: No specifics about consumer/employee PII or financial data loss were available at press time.

Customers Impacted: Unknown

How it Could Affect Your Customers' Business *Organizations should keep in mind the fact that the preferred weapon of nation-state cybercriminals is ransomware.*