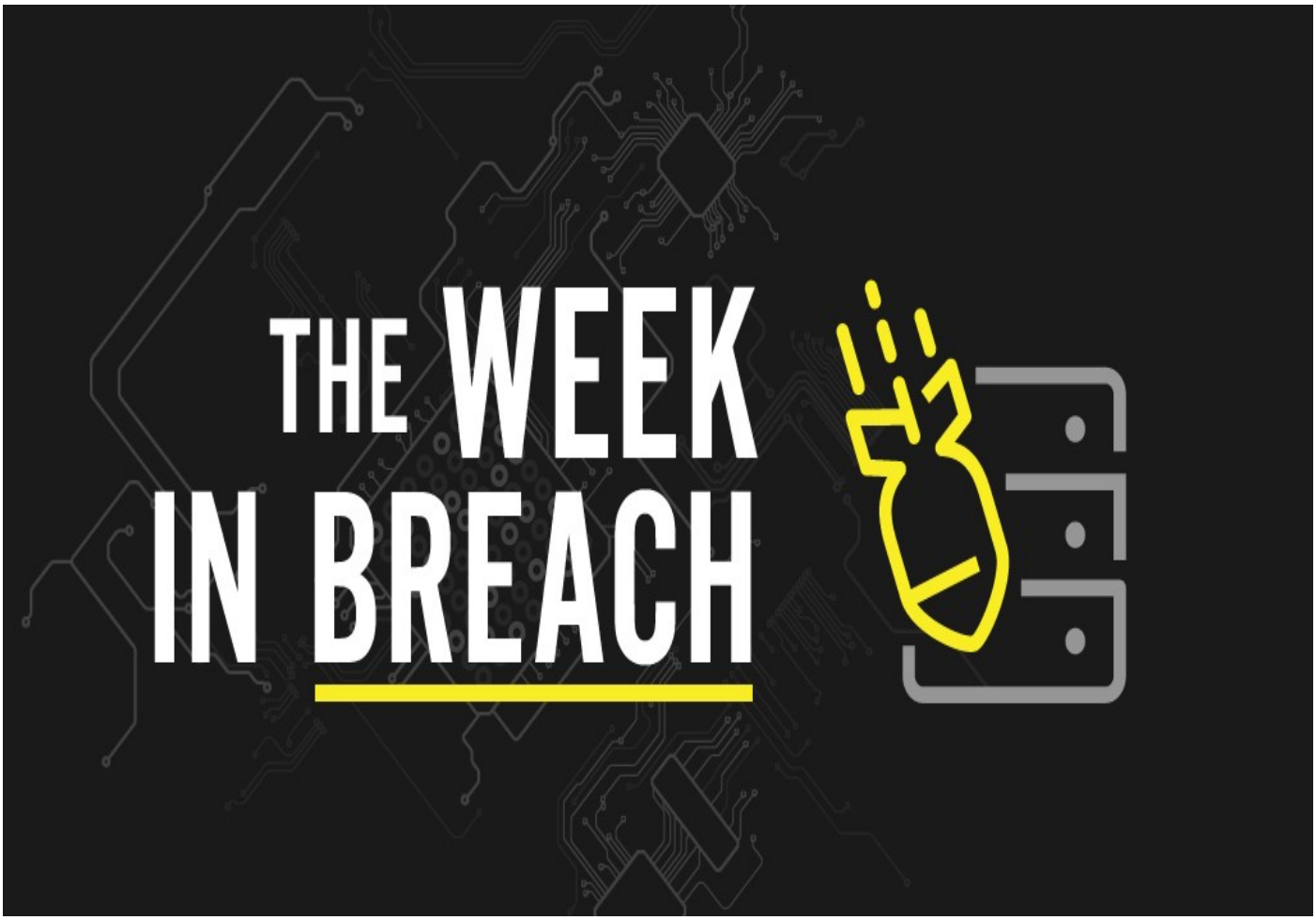
THE WEEK IN BREACH NEWS: 11/09/22 - 11/15/2022

DenBe Computer Consulting
Connecting Business

November 16th, 2022 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***

Dropbox
https://www.reuters.com/business/retail-consumer/bed-bath-beyond-reviewing-possible-data-breach-2022-10-28/?utm_campaign=fullarticle&utm_medium=referral&utm_source=inshorts

Exploit: Phishing

Dropbox: File Hosting Service

Risk to Business: **2.836 = Moderate**

Dropbox has revealed that they have experienced a data breach. The company noted unauthorized access to some of its repositories after a successful phishing attack. That attack resulted in someone copying 130 of its private GitHub code repositories and swiping some of its secret API credentials. Microsoft's GitHub detected suspicious behavior on Dropbox's corporate account on October 13 and informed the company. Dropbox ultimately determined the cause was a phishing attack in which bad actors impersonated the code integration and delivery platform CircleCI. Reports point out that three weeks before the attack, GitHub warned of phishing campaigns that involved the impersonation of CircleCI. Dropbox also said the intruder's access to the GitHub repo silo was revoked on October 14, and that all developer API credentials to which the intruder had access have been rotated.

How It Could Affect Your Business: Even the biggest, most tech-savvy companies can be taken down by phishing in a flash.

Kearney & Company
https://securityaffairs.co/wordpress/138136/cyber-crime/lockbit-ransomware-kearney-company.html

Exploit: Ransomware

Kearney & Company: Financial Services Firm

Risk to Business: 2.101 = Severe

The LockBit 3.0 ransomware group has added Kearney & Company, an accounting and financial services firm that does business with the U.S. government, to its published list of victims on November 05. That group is threatening to publish the firm's stolen data by November 26, 2022, if the company doesn't pay the $2 million demanded ransom. A sample of the stolen data including financial documents, contracts, audit reports and billing documents has been published on the group's dark website.

How It Could Affect Your Business: Financial services was the most hard-hit sector in terms of ransomware in 2021 and this year isn't looking much better.

Multi-Color Corporation (MCC)
https://www.securityweek.com/label-giant-multi-color-corporation-discloses-data-breach

Exploit: Ransomware

Multi-Color Corporation (MCC): Printer

Risk to Business: 2.764 = Moderate

Label printing company Multi-Color Corporation (MCC) has disclosed that on September 29, 2022, it discovered unauthorized access to its network. An investigation revealed that sensitive HR data might have been compromised, including personnel files and information on employees' enrollment in benefits programs. Both current and former MCC employees are impacted. Some reports are saying that this was a ransomware attack.

The company's breach announcement said that sensitive personal data of MCC employees and their spouses, partners, and/or dependents who are enrolled in the benefits programs may have been exposed. Exposed data may include a person's name, date of birth, email address, mailing address, telephone number, Social Security number, driver's license number, healthcare and health insurance-related data, and certain tax and financial data.

How it Could Affect Your Business: This is a goldmine of personal data that will enable cybercrime like phishing and identity theft for years to come.

Somnia Inc.
https://www.govinfosecurity.com/vendor-hack-tied-to-20-anesthesiology-practice-breaches-a-20414

Exploit: Hacking

Somnia Inc.: Medical Practice Management

Risk to Business: 1.382 = Extreme

Somnia Inc, a physician-owned firm that manages anesthesiology practices, has experienced a data breach that may impact an estimated 20 practices serving about 430,000 people. A company spokesperson confirmed that the firm is the management services organization behind the recent breaches affecting many anesthesiology practices. Somnia declined to disclose how many clients and individuals in total were affected. The company said that their forensic investigation into a security incident found that some information stored on the management company's systems may have been compromised.

Individual Risk: 1.361 = Extreme

Affected information includes individuals' name, Social Security number, and some combination of data including date of birth, driver's license number, financial account information, health insurance policy number, medical record number, Medicaid or Medicare ID and health information such as treatment and diagnosis.

How it Could Affect Your Business: This incident is still snowballing, but however it plays out this will cost Somnia a fortune in regulatory penalties on top of other damages.