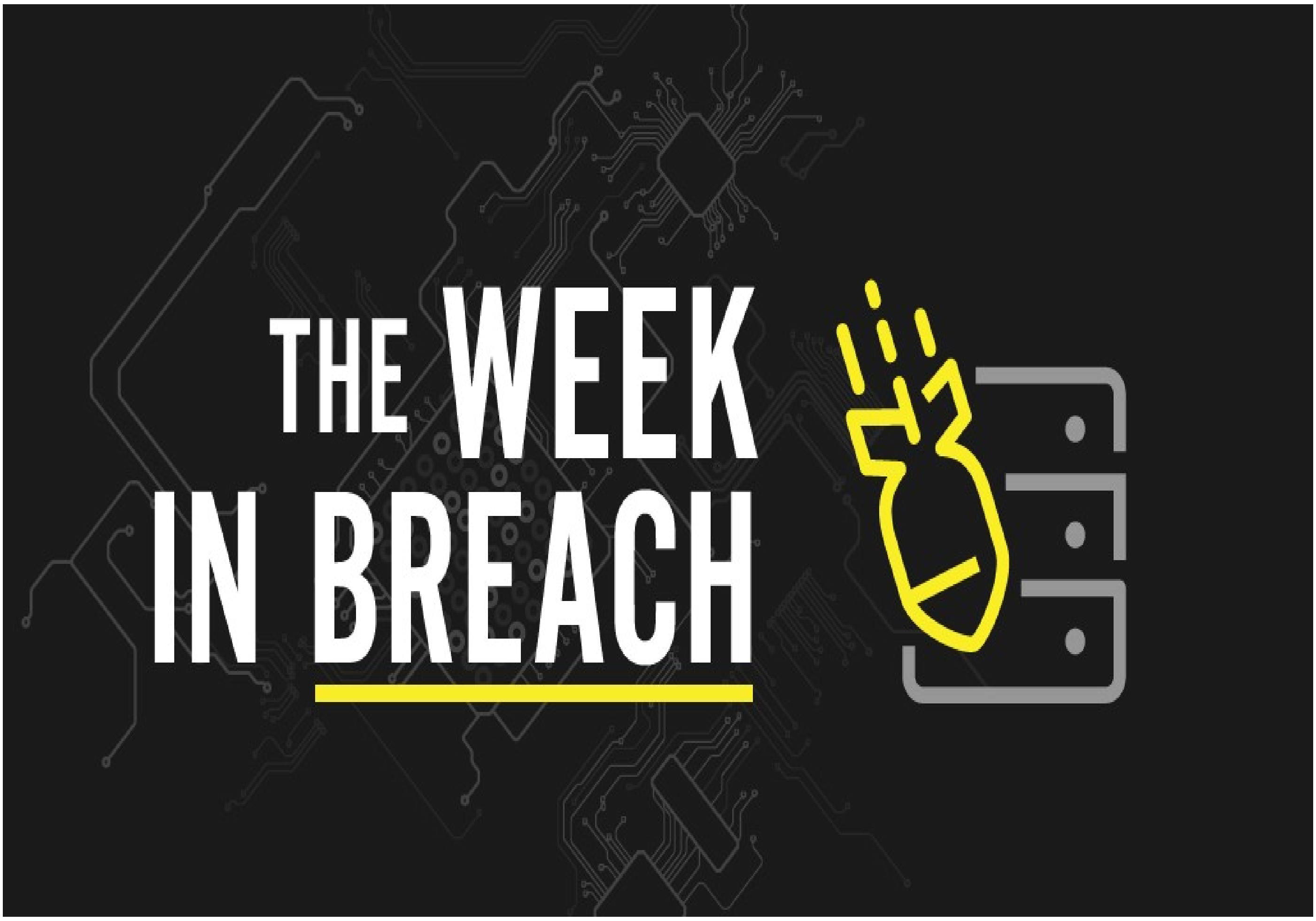
THE WEEK IN BREACH NEWS: 12/7/2022 - 12/13/2022

DenBe Computer Consulting
Connecting Business

December 14th, 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***

LastPass

https://blog.lastpass.com/2022/11/notice-of-recent-security-incident/

Exploit: Hacking

LastPass: Software Company

Risk to Business: 1.106 = Extreme

LastPass has experienced a second data breach. The company disclosed in its blog that hackers used information obtained in the August 2022 LastPass breach to access customer information in third-party cloud storage shared with its corporate partner GoTo. LastPass specified that customers' passwords it stores were unaffected and remain safely encrypted. It is unclear as whether or not clients of GoTo and LogMeIn were affected by this incident. All the brands involved said that the incident is under investigation and LastPass specified that it has engaged Mandiant as part of that effort. No specifics as to what information was exposed were available at press time.

How It Could Affect Your Business: Multiple breaches in one year can cause customers to lose faith in a company.

U.S. Immigration and Customs Enforcement (ICE)

https://www.businessinsider.com/more-than-6000-immigrants-affected-ice-data-leak-hours-2022-11

Exploit: Misconfiguration

U.S. Immigration and Customs Enforcement (ICE): Federal Government Agency

Risk to Business: **2.121 = Severe**

Personal information about more than 6,000 potential immigrants applying for refuge from possible torture or political persecution in the U.S. was exposed by ICE in a misconfiguration error. The data breach was first discovered by immigrant advocacy group Human Rights First. After the group reported the problem to ICE the leak was quickly corrected, but not before information about people seeking refuge from countries around the world including China, Iran and Russia was left unprotected and available to anyone for more than five hours. The agency determined that the data had been exposed accidentally as part of a website update. Unfortunately, the availability of the information may have exposed threatened people to danger.

Individual Risk: **2.207 = Severe**

In this incident, immigrants' names, case status, detention locations, and other information was published on a page where ICE regularly publishes detention statistics.

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.

Rackspace

https://www.bleepingcomputer.com/news/security/rackspace-confirms-outage-was-caused-by-ransomware-attack/

Exploit: Ransomware

Rackspace: Cloud Solutions Provider

Risk to Business: 1.652 = Severe

A ransomware attack forced Virginia-based cloud solutions provider Rackspace was forced to shut down its Hosted Exchange servers on December 2. The company disclosed that Rackspace's Hosted Exchange service began experiencing problems on December 2 and told customers that the shutdown was the result of a security incident on December 3 that was later identified as ransomware. The company told customers to shift to Microsoft 365 for email services and is offering them free access. Rackspace gave no estimated timeline for the restoration of its Exchange services but cautioned customers that the outage was expected to be extended. A company statement said that the attack was confined to its Hosted Exchange servers. The incident is under investigation but Rackspace said that it is too early to tell if any data was accessed by the threat actors.

How It Could Affect Your Business: IT service providers have been experiencing extraordinarily high levels of ransomware as bad actors perpetrate supply chain attacks.

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.