THE WEEK IN BREACH NEWS: 12/30/20 – 01/05/21

DenBe Computer Consulting
Connecting Business

January 6, 2021 by Dennis Jock

This Week in Breach News: It may be a new year, but cybercriminals are up to the same old tricks around the world. Old-fashioned hacking nails Kawasaki, T-Mobile and Promutuel.

Read more in our report.

The Week in Breach News: Top Threats This Week

- **Top Source Hits:** ID Theft Forum
- **Top Compromise Type:** Domain
- **Top Industry:** Education & Research
- **Top Employee Count:** 501+

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***

Whirpool

https://www.bleepingcomputer.com/news/security/home-appliance-giant-whirlpool-hit-in-nefilim-ransomware-attack/

Exploit: Ransomware

Company Type: Type

Risk to Business: 2.311 = Severe

The Nefilim ransomware gang struck at Whirlpool, stealing data but not impacting manufacturing operations. The gang claims that the files it published were obtained from Whirlpool during a ransomware attack in December 2020. The leaked data appeared to be proprietary and staff information including documents related to employee benefits, accommodation requests, medical information requests, background checks, and more.

Individual Risk:

No personal or consumer information was reported as impacted in this incident at this time but the incident is still under investigation.

Customers Impacted: Unknown

How it Could Affect Your Business: While using ransomware to disrupt manufacturing or operations has been in vogue recently, it’s still a favored tool for cybercriminals to use in a classic data grab.

GetSchooled

https://welpmagazine.com/bill-melinda-gates-foundations-charity-getschooled-breaches-900k-childrens-details/

Exploit: Unsecured Database

Company Type: Education Non-Profit

Risk to Business: 2.302 Severe

An unsecured database at education charity operation GetSchooled left personally identifiable information exposed for more than 900K students, ranging from 10-year-olds to college students. GetSchooled is an arm of the Bill and Melinda Gates Foundation that encourages educational achievement for students in need through gamification, personalized support, and content development. The database was left open and exposed for approximately one month.

Individual Risk: 2.271 Severe

The exposed information includes personally identifiable information of students including children, teenagers and young adults. Some of the information left exposed in this incident was very detailed including full addresses, schools, phone numbers and emails, graduation details, ages, genders.

Customers Impacted: 930,000

How it Could Affect Your Business: Failing to secure a database is a rookie mistake, and especially embarrassing (and dangerous) for a charity that primarily serves minors.

Aetna

https://medcitynews.com/2020/12/information-of-nearly-half-a-million-aetna-members-exposed-in-email-hack/

Exploit: Malicious Insider

Company Type: Insurance Company

Risk to Business: **1.928 Severe**

Aetna is in hot water after a debacle that involved a contractor BEC and phishing in an explosive insider incident. On Sept. 28, Aetna was informed that an EyeMed email account was accessed by an unauthorized individual and that phishing emails were sent to addresses contained in the mailbox. The email account contained information about individuals who previously or currently receive vision-related services through EyeMed, including Aetna customers.

Individual Risk: **2.122 Severe**

The information that may have been accessed included names, addresses, dates of birth and vision insurance accounts/identification numbers. In some cases, full or partial Social Security numbers, birth or marriage certificates, medical diagnoses and conditions, treatment information or financial information may have been accessed. Customers of Aetna that use EyeMed should be wary of potential spear phishing and identity theft.

Customers Impacted: 500,000

How it Could Affect Your Business: Insider threats are one of the most overlooked high-damage cybersecurity threats. No one wants to believe that their employees are out to get them, but even non-malicious insiders can do massive damage fast.

T-Mobile

https://www.bleepingcomputer.com/news/security/t-mobile-data-breach-exposed-phone-numbers-call-records/

Exploit: Hacking

Company Name: Telecom

Risk to Business: 2.383 = Severe

T-Mobile has found itself embroiled in a "malicious hacking incident" that has resulted in data exposure for an estimated 200,000 clients. The company said in a statement that Customer proprietary network information (CPNI) was accessed and may have included phone numbers, the number of lines on the account and call-related information.

Individual Risk: 2.212 = Severe

T-Mobile maintains that only a small fraction of its clients were impacted in the incident, and the company has sent text messages to the affected account holders.

Customers Impacted: 200,000

How it Could Affect Your Business: It's not all ransomware these days – good old-fashioned hacking is still a risk that every business faces. When information like this makes its way to the Dark Web, it makes hackers' jobs easier

Door Controls USA

https://cybernews.com/security/140gb-of-confidential-data-from-us-based-door-parts-distributor-leaked-on-hacker-forum/

Exploit: Ransomware

Company Type: Door Parts Distributor

Risk to Business: **2.083 = Severe**

Hackers have leaked more than 140 GB of confidential and proprietary information from Texas-based Door Controls USA after the company failed to pay a requested ransom. The information is sorted into two categories, with one containing assorted documents related to company financials and accounting information including credit card statements,

Individual Impact: No personal data was reported as exposed in the incident.

Customer's Impacted: Unknown

How it Could Affect Your Business: Information like this can live forever on the Dark Web. Manufacturing data like blueprints spec sheets, research and development files, schema, product plans and similar specific product information is a hot seller in Dark Web markets

Sonoma Valley Hospital

https://www.infosecurity-magazine.com/news/svh-notifies-67k-patients-of-data/

Exploit: Hacking (Nation State)

Sonoma Valley Hospital: Medical Center

Risk to Business: 1.809 = Severe

In their 3rd breach of the year, Spotify has announced that starting in April 2020, some user information was inadvertently exposed to third-party partners that shouldn't have been able to access it. The leak was discovered and closed in November 2020.

Individual Risk: 2.667 Moderate

It's unclear to what extent customer data was impacted, but it is possible that some personally identifying information and treatment data was accessed or copied by the intruders. The investigation is ongoing, but people who have been treated at this facility should be alert for spearphishing attempts.

Customers Impacted: 67,000

How it Could Affect Your Business: Ransomware is a huge threat to every organization right now, and it has been so widely deployed in the healthcare sector that CISA released guidance on risk avoidance.