THE WEEK IN BREACH NEWS: 11/11/20 – 11/17/20

DenBe Computer Consulting
Connecting Business

November 18, 2020 by Dennis Jock

This Week in Breach News: Hackers scale The North Face, ransomware rocks eCommerce, an in-depth look at the importance of cyber resilience, and how remote work increases ransomware danger.

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***

Delaware Division of Public Health

https://news.delaware.gov/2020/11/15/delaware-division-of-public-health-announces-data-breach-incident/

Exploit: Accidental Data Sharing

Delaware Division of Public Health: State Health Agency

Risk to Business: 2.311 = Severe

The Delaware Division of Public Health announced that in mid-September, a temp sent two emails containing COVID-19 test results for approximately 10,000 individuals to the wrong party. The August 13, 2020, email included test results for individuals tested between July 16, 2020, and August 10, 2020. The August 20, 2020, email included test results for individuals tested on August 15, 2020. Investigators have determined that these emails were sent by mistake, as the information was supposed to be sent to a member of the call center staff to assist individuals in obtaining their test results.

Individual Risk: 2.824 = Moderate

The information mistakenly released in this foul-up included the date of the test, test location, patient name, patient date of birth, phone number if provided, and test result.

Customers Impacted: 10,000

How it Could Affect Your Customers' Business: Human error remains the number one cause of a data breach. Security awareness training is the most effective way to prevent unfortunate employee errors.

Vertafore Inc.

https://siliconangle.com/2020/11/15/data-belonging-27-7m-texas-drivers-stolen-latest-case-unsecured-storage/

Exploit: Unsecured Database

Vertafore Inc.: Insurance Company

Risk to Business: 1.702 = Severe

Information about 27.7 million Texas drivers has been exposed online and stolen from an unsecured database belonging to insurance company Vertafore Inc. after someone put three major company files on an unsecured storage server.

Individual Risk: 2.662 = Moderate

The company says that no identification misuse has been determined, but they're also offering free credit monitoring and identity restoration services to all Texas driver's license holders potentially affected by the data breach.

Customers Impacted: 27.7 million

How it Could Affect Your Customers' Business: Bad data handling is a symptom of poor cybersecurity hygiene, and it can easily lead to bigger problems like ransomware and password compromise.

X-Cart

http://www.digitaljournal.com/tech-and-science/technology/x-cart-suffers-from-ransomware-attack/article/580881

Exploit: Third Party Software

X-Cart: eCommerce Platform Creator

Risk to Business: **2.003 = Severe**

X-cart discovered the danger of vetting errors when attackers exploited a vulnerability in a third-party software tool to gain access to X-Cart's store hosting systems. Some stores went down completely, while others reported issues with sending email alerts. The incident is under investigation and service has been restored for clients.

Individual Risk: No personal or consumer information was reported as impacted in this incident.

Customers Impacted: Unknown

How it Could Affect Your Customers' Business: Cyberattacks can come from unexpected quarters, like a vulnerability in third-party software that you rely on.

Wildworks (Animal Jam)

https://www.informationsecuritybuzz.com/expert-comments/animal-jam-kids-virtual-world-hit-by-data-breach-impacting-46m-accounts-expert-commentary/

Exploit: Third Party Data Breach

Wildworks: Video Game Developer

Risk to Business: 1.664 = Severe

Wildworks, the developer of the online kid's playground Animal Jam, announced a data breach involving a third-party vendor that exposed the information of millions of children on the Dark Web. The information appeared on the Dark Web as the booty of cybercrime gang ShinyHunters.

Individual Risk: 1.902 = Severe

Exposed information includes 46 million player usernames, which are human moderated to make sure they do not contain a child's proper name, 46 million SHA1 hashed passwords and approximately 7 million email addresses of parents whose children registered for Animal Jam.

Customers Impacted: 46 million

How it Could Affect Your Customers' Business: Third-party service providers may not have the same commitment to data security as you do. It pays to do your homework to avoid these problems whenever possible.

Pluto TV

https://www.bleepingcomputer.com/news/security/hacker-shares-32-million-pluto-tv-accounts-for-free-on-forum/

Exploit: Hacking

Pluto TV: Online Television Service

Risk to Business: 2.166 = Severe

Hackers from the cybercrime gang ShinyHunters have announced the acquisition of 3.2 million Pluto TV user records that were purportedly stolen during a data breach. The data appears to be somewhat out of date, and Pluto TV has not confirmed the breach.

Individual Risk: 2.611 = Moderate

Exposed information includes a member's display name, email address, bcrypt hashed password, birthday, device platform, and IP address. The data is estimated to be about two years old.

Customers Impacted: Unknown

How it Could Affect Your Customers' Business: Protecting your client records and other sensitive data from thieves has to be a top priority, no matter how old it is. Customers expect that you'll keep it safe with reasonable security precautions in place.

The North Face

https://chainstoreage.com/report-hackers-may-have-obtained-north-face-customer-data

Exploit: Credential Stuffing

The North Face: Outdoor Apparel Retailer

Risk to Business: 2.322 = Severe

Hackers mounted a successful attack against outdoor retailer The North Face, capturing an unknown amount of client data in the process. While retail operations were not disrupted, the company has released a caution to customers about the incident.

Individual Risk: 2.711 = Moderate

The company noted that the breach includes "products you have purchased on our website, products you have saved to your 'favorites,' your billing address, your shipping address(es), your VIPeak customer loyalty point total, your email preferences, your first and last name, your birthday (if you saved it to your account), and your telephone number (if you saved it to your account)". Payment information was stored separately and more securely and not impacted in this incident.

Customers Impacted: Unknown

How it Could Affect Your Customers' Business: Credential stuffing attacks have gained new fuel from a bountiful harvest of Dark Web data dumps adding fresh ammo for cybercrime.