THE WEEK IN BREACH NEWS: 01/06/21 – 01/12/21

DenBe Computer Consulting
Connecting Business

January 13, 2021 by Dennis Jock

This Week in Breach News: Multiple healthcare targets receive an unwelcome diagnosis of ransomware.

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***

Lake Regional Healthcare

https://www.beckershospitalreview.com/cybersecurity/minnesota-health-system-hit-by-ransomware-attack-4-details.html

Exploit: Ransomware

Company Name: Hospital System

Risk to Business: 1.919 = Severe

A ransomware attack at this Minnesota healthcare system on December 30 led to impacts in patient care as the hospital was forced to adopt downtime procedures. Most impacted systems have been restored and the incident is under investigation.

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: Ransomware is an increasingly popular option for cybercriminals looking to disrupt operations to score a quick payday from a much-needed service provider or manufacturer.

OmniTRAX

https://www.freightwaves.com/news/ransomware-attack-hits-short-line-rail-operator-omnitrax

Exploit: Ransomware

OmniTRAX: Short Line Railway

Risk to Business: 2.172 = Severe

Conti ransomware is to blame for a major information theft at OmniTRAX and parent company Broe Group. Although rail and freight operations were not disrupted, proprietary data was stolen. The 70 gigabytes of leaked files presented by the gang include internal OmniTRAX documents and clearly showed that data came from the contents of individual employee work computers. It was not clear if it included data pertaining to

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: Just one stolen or cracked password can wreak havoc on a company and its subsidiaries, leading to extensive (and expensive) recovery operations.

Apex Laboratory

https://hotforsecurity.bitdefender.com/blog/apex-laboratory-confirms-ransomware-gang-stole-patient-info-in-cyberattack-25002.html

Exploit: Ransomware

Apex Laboratories: Consumer Medical Testing

Risk to Business: 1.783 = Severe

Apex Laboratories definitely got a result that they weren't expecting when DoppelPaymer ransomware popped up on December 15, snatching a large quantity of data. The attack resulted in the exfiltration of thousands of documents containing both protected health information of patients and personally identifiable information of Apex employees.

Individual Risk: 2.166 = Severe

The data impacted is estimated to include patient names, dates of birth, test results, and some Social Security and phone numbers. The company is notifying affected patients. Apex employees and clients should be cautious about potential spear phishing email using this information.

Customers Impacted: Unknown

How it Could Affect Your Business: Ransomware has been an especially pernicious menace to healthcare targets throughout the pandemic, and that's not slowing down.

Dassault Falcon Jet

https://securityaffairs.co/wordpress/113216/data-breach/dassault-falcon-data-breach.html

Exploit: Ransomware

Dassault Falcon Jet: Aviation Manufacturing

Risk to Business: 2.127 = Severe

Dassault Falcon Jet, a division of French conglomerate Dassault Aviation, was hit by the Ragnar Locker ransomware gang, resulting in extensive data theft. Bad actors made off with employee information, but no proprietary data theft was reported in the incident.

Individual Risk: 1.702 = Severe

Extensive PII was exposed for current and former employees and their families including names, personal and company email address, personal mailing address, employee ID number, driver's license number, passport information, financial account number, Social Security number, date of birth, work location, compensation and benefit enrollment

Customers Impacted: Unknown

How it Could Affect Your Business: Ransomware is no joke, and it has been increasingly pointed at manufacturing targets to both steal data and impact production, especially dangerous when a company manufactures assets like planes.