THE WEEK IN BREACH NEWS: 12/23/20 – 12/29/20

DenBe Computer Consulting
Connecting Business

December 30, 2020 by Dennis Jock

This Week in Breach News: Ransomware was an unwelcome holiday gift for a plastic surgery group, a trucking company, and other organizations.

The Week in Breach News: Top Threats This Week

- **Top Source Hits:** Ransomware
- **Top Compromise Type:** Domain
- **Top Industry:** Medical
- **Top Employee Count:** 250+

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***

Forward Air

https://www.bleepingcomputer.com/news/security/trucking-giant-forward-air-hit-by-new-hades-ransomware-gang/

Exploit: Ransomware

Risk to Business: **2.113 = Severe**

Another trucking company gotbhit with ransomware this week, as attacks on shipping and logistcs targets continue to surge. Forward Air toook the hit this time from a ransomware gang that's just coming on the scene, Hades. Operations and we services were disrupted, and recovery is ongoing.

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 increasingly being used to disrupt business operations instead of just snatch business data, and that's equally bad news for every company.

TennCare

https://www.wkrn.com/news/tenncare-announces-privacy-breach-impacting-3300-members/

Exploit: Insider Accident (Accidental)

TennCare: Medicaid Services Agency

Risk to Business: **2.602 = Moderate**

A blunder at TennCare has led to the exposure of personally identifiable information for about 3,300 Medicaid patients in Tennesee. Employees at an information processing vendor mistakenly sent out misaddressed mailers that may have contained protected health information to the wrong recipients.

Individual Risk: **2.771 = Moderate**

The state has set up a hotline for members to find out if they're at risk by calling (833) 754-1793. The state will also be providing free credit monitoring for breach victims. TennCare users should be wary of potential spear phishing and financial scams using this information.

Customers Impacted: 3,300

How it Could Affect Your Business: To err is human…unfortunately. But increased security awareness training can help reduce a company's chance of experiencing a damaging security incident by up to 70%.

TaskRabbit

https://latesthackingnews.com/2020/12/26/taskrabbit-reset-passwords-after-credential-stuffing-attack/

Exploit: Credential Stuffing

TaskRabbit: Microlabor Marketplace

Risk to Business: **2.803 = Moderate**

Users of the Boston-based gig work platform TaskRabbit were surprised to get forced password reset notices when they logged in over the weekend. The company says it stopped a credential stuffing attack and did not suffer a breach or intrusion, but is having users reset their passwords “out of an abundance of caution”. The incident is still under investigation.

Individual Risk:

No personal or consumer information was reported as exposed in the incident at this time, but may change as the investigation progresses.

Customers Impacted: Unknown

How it Could Affect Your Business: Credential stuffing attacks can be devastating. In this case, TaskRabbit got lucky, but they may not be as fortunate next time.