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

DenBe Computer Consulting
Connecting Business

January 20, 2021 by Dennis Jock

This Week in Breach News: Capcom's breach hits 40K players in Japan gaming giant's breach. Healthcare was also hit hard again.

The Week in Breach News: Top Threats This Week

- **Top Source Hits:** ID Theft Forum
- **Top Compromise Type:** Domain
- **Top Industry:** Health & Medical 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***

Ubiquiti Networks

https://www.securitymagazine.com/articles/94336-ubiquiti-suffers-data-breach-and-alerts-customers-to-change-passwords

Exploit: Ransomware

Ubiquiti Networks: Communications Technology Firm

Risk to Business: 1.979 = Severe

Ubiquiti Networks announced that an intruder made its way into that company's servers. The hacker was able to access stored data on UI.com users, such as names, email addresses, and salted and hashed passwords. It is currently unclear how many users have been affected. The company says there is no indication that there has been unauthorized activity with respect to any user's account, and the incident is still under investigation.

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

Customers Impacted: Unknown

How it Could Affect Your Business: Hacking can come from many directions, but one common source is credential compromise. By adding strong access point protection, companies can add extra security against hackers like this.

Parler

https://cybernews.com/news/70tb-of-parler-users-messages-videos-and-posts-leaked-by-security-researchers/

Exploit: Hacking

Parler: Social Media Application

Risk to Business: 1.619 = Severe

Now-defunct social media site Parler had a wild ride to the finish, including a hacking incident. Hackers were able to exploit security weaknesses in engineering and security to gain access to the membership-restricted content, scraping at least 70 TB of data. The data scrape also includes deleted posts, meaning that Parler stored user data after users deleted it. The hackers also obtained URLs for over a million video URLs, some deleted and private.

Individual Risk: 1.221 = Extreme

Data was taken from Parler's "Verified Citizens," users of the network who verified their identity by uploading photographs of government-issued IDs, such as a driver's license. The scrape includes user profile data, user information, and which users had administration rights for specific groups within the social network. Data like this could be used to mount spear phishing attacks, or as blackmail material, as it contains details that could connect users to criminal acts or membership in extremist groups.

Customers Impacted: 10 Million

How it Could Affect Your Business: Data like this often makes its way to the Dark Web, enabling it to be used to power cybercrime like phishing and credential compromise.

Taylor Made Diagnostics

https://www.freightwaves.com/news/hackers-leak-trucker-rail-worker-medical-records

Exploit: Ransomware

Taylor Made Diagnostics: Occupational Healthcare Provider

Risk to Business: 2.612 = Moderate

A Conti ransomware attack at this Virginia-based healthcare provider led to some unpleasant consequences for employees of the Norfolk Southern Railroad and UPS after 3K patient records were snatched. The stolen data included health records for employees from both firms, in addition to multiple smaller trucking companies, U.S. government agencies and defense contractors from as recently as December 2020.

Individual Risk: 2.722 = Moderate

The leaked data included completed U.S. Department of Transportation (DOT)-mandated medical exams, as well as drug and alcohol testing reports for truckers and rail workers at multiple companies. Many documents contained detailed personal information such as full names, addresses, social security numbers and scans of driver's licenses. This information could be used for identity theft and spear phishing attacks.

Customers Impacted: Unknown

How it Could Affect Your Business: Ransomware is almost always the result of a successful phishing attack. It's an expensive nightmare for any business, especially one in the healthcare sector.

South Country Health Alliance

https://www.beckershospitalreview.com/cybersecurity/email-phishing-attack-on-minnesota-health-plan-exposes-info-of-66-000-members.html

Exploit: Phishing

South Country Health Alliance: Health Plan Provider

Risk to Business: 1.812 = Severe

South Country Health Alliance, a county-owned health plan based in Owatonna, MN, experienced a data breach after a successful phishing attack let cybercriminals access the protected health data and personal information of more than 60K members. The incident has been under investigation since the attack was first confirmed in September 2020, and the filing made with HIPPA regulators noted that affected patients were informed starting 12/30/20.

Individual Risk: 2.006 = Severe

The exposed information included names, Social Security numbers, addresses, Medicare and Medicaid numbers, health insurance information, diagnostic or treatment information, death dates, provider names and information about treatment costs. The health plan is offering complimentary credit monitoring and identity protection service to impacted members.

Customers Impacted: 66,874

How it Could Affect Your Business: Phishing attacks on healthcare targets have been increasing, as the demand for healthcare information and the opportunity afforded to cybercriminals by an overstressed healthcare system creates fresh opportunities.