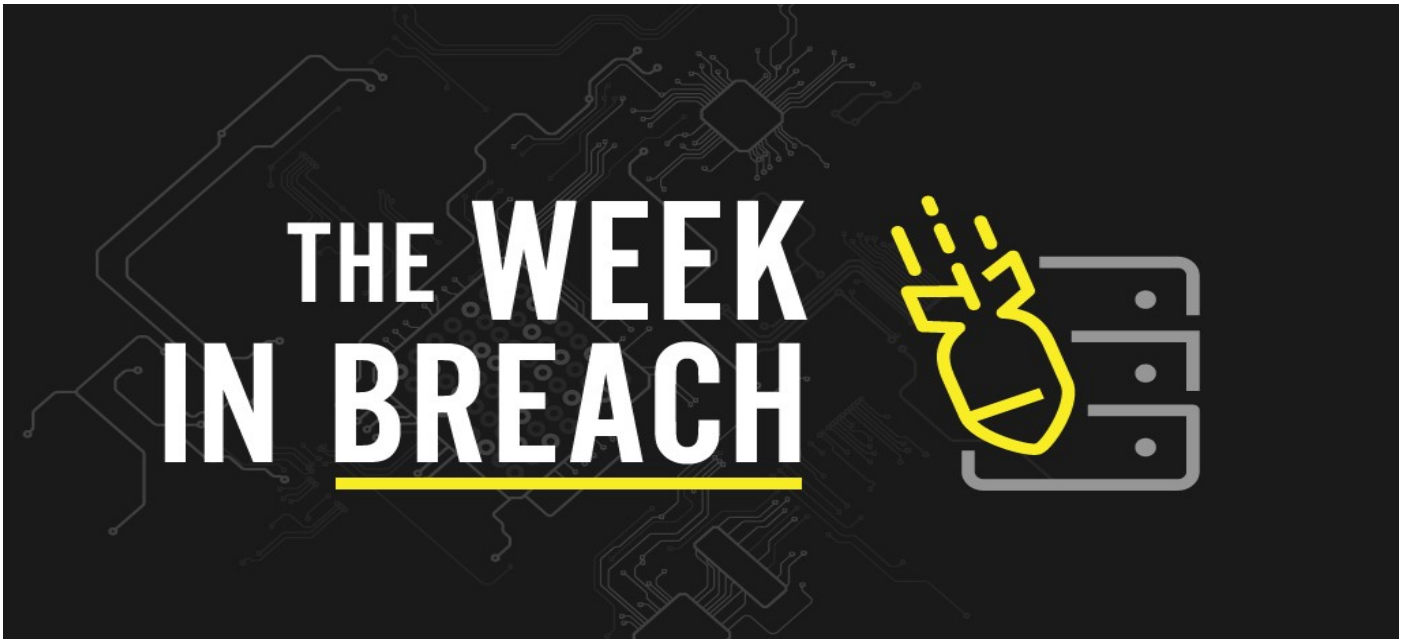
THE WEEK IN BREACH NEWS: 8/18/21— 08/24/21

DenBe Computer Consulting
Connecting Business

August 25, 2021 by Dennis Jock

Fact or Fiction: AT&T had a massive data breach? We'll bring you the latest in the blog. Plus, a crypto incident raises eyebrows, Tokio Marine runs aground in a data breach, ransomware is in fashion in Brazil and why credential compromise is something everyone needs to take seriously right now.



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***

United States: AT&T

https://cybernews.com/news/att-database-of-70-million-users-sold-on-hacker-forum/

Exploit: Hacking

AT&T: Communications Conglomerate

Risk to Business: 1.422 = Extreme

A bit of drama has arisen around what appears to be a data breach at telecom giant AT&T. What's not in dispute is that 70 million records that allegedly belong to AT&T made their debut on the dark web market this week courtesy of ShinyHunters. The hackers contend that this treasure trove is fresh data obtained from AT&T through their ingenuity. AT&T contends that no breach happened and that this data was obtained from an unnamed third-party source. ShinyHunters' reputation precedes them; they are the cybercriminals responsible for well-known data thefts at Microsoft, Tokopedia, Mashable, Pluto TV and a host of other targets, lending credence to their claims. The controversy was not resolved at press time.

Individual Impact: ShinyHunters provided what looks like customer information in the sample posted to their announcement, but the full spectrum of the leaked data is unclear.

Customers Impacted: Unknown

How It Could Affect Your Business: Maintaining strong security in every nook and cranny of your client's business is vital to protecting them from increasingly sophisticated hacking threats.

United States: Indiana Department of Health

https://www.wowo.com/personal-data-of-nearly-750000-hoosiers-accessed-improperly/

Exploit: Misconfiguration

Indiana Department of Health: State Agency

Risk to Business: 1.723 = Severe

The Indiana Department of Health has disclosed that data from the state's COVID-19 online contact tracing survey was improperly accessed in a database misconfiguration incident after a company looking to form a security-based business relationship with the agency accessed it and informed the Department of the mistake. The agency and the company involved signed an agreement noting that the data had not been copied or downloaded. The misconfiguration issue has been corrected according to the agency.

Risk to Individual: 1.571 = Severe

The data included the name, address, email, gender, ethnicity and race, and birthday of nearly 750,000 Hoosiers, according to IDOH. The agency will send letters notifying those affected by the breach and extend an offer for one year of free credit monitoring with Experian.

Customers Impacted: 750,000

How it Could Affect Your Business: Government targets have been especially under the gun recently as cybercriminals seek easy routes to gaining big scores of personal data from targets with historically poor security.

United States: St. Joseph's/Candler Health System

https://portswigger.net/daily-swig/us-healthcare-org-sends-data-breach-warning-to-1-4m-patients-following-ransomware-attack

Exploit: Ransomware

St. Joseph's/Candler(SJ/C): Heath System

Risk to Business: 1.673=Severe

St. Joseph's/Candler, a major Georgia healthcare network, has admitted that it has suffered a data breach as part of a ransomware incident that it just uncovered. The system's IT staff first detected the breach on June 17, but the intrusion occurred as early as December 20, 2020. The cybercriminals launched ransomware from this break-in. The hospital system also disclosed that it had been forced to use pencil and per recordkeeping briefly after it became unable to access its systems or data. That has since been resolved and IT systems restored. The incident is still under investigation.

Individual Risk: 1.811=Severe

The stolen data includes extensive patient records including each patient's name, address, date of birth, Social Security number, driver's license number, patient account number, billing account number and assorted other financial information. It also includes their health insurance plan member ID, medical record number, dates of service, provider names and information about the medical and clinical treatment they've received from SJ/C. Impacted patients will be notified by mail and offered free credit monitoring and identity protection services.

Customers Impacted: 100 million

How it Could Affect Your Business: It shouldn't take that long to detect an intrusion, especially since healthcare targets have been increasingly endangered for the last year. That speaks to poor cybersecurity hygiene.

Japan: Liquid

https://www.newsweek.com/hacker-steals-74-million-cryptocurrencies-including-bitcoin-ethereum-1620892

Exploit: Hacking

Liquid: Cryptocurrency Exchange

Risk to Business: **1.505 = Extreme**

Japanese crypto exchange Liquid was sacked by hackers this week resulting in the theft of a reported $74 million worth of cryptocurrency. The stolen assets include chunks of Bitcoin, Ethereum and others being stolen. The firm said the attack targeted its multiparty computation (MPC) system of custody. Liquid also noted that it is moving assets that were not affected into more secure “cold wallet” storage while suspending deposits and withdrawals.

Customers Impacted: Unknown

How it Could Affect Your Business: Infrastructure targets are increasingly under fire by cybercriminals because of the historically poor security and rich payouts.

Japan: Tokio Marine Holdings

https://www.cyberscoop.com/tokio-marine-ryan-specialty-group-ransomware-cyber-insurance/

Exploit: Ransomware

Toki Maarine Holdngs: Insurer

Risk to Business: 1.721 = Severe

Japan's largest property and casualty company, Tokio Marine Holdings, was struck by ransomware at its Singapore branch. The insurer, which has a U.S. division and offers a cyber insurance product, said it did not have any immediate indication that any customer information was accessed. Tokio Marine was able to isolate the affected network and notified local law enforcement. Investigators from an outside vendor are working to determine the scope of the damage.

Individual Impact: There has not yet been an announcement that employee, customer or consumer personal or financial information was compromised in this incident but the investigation is ongoing.

Customers Impacted: Unknown

How it Could Affect Your Business: Cyberattacks against service providers have been steadily increasing as cybercriminals strike at lynchpins to gain access to even more valuable data.

Brazil: Lojas Renner

https://therecord.media/ransomware-hits-lojas-renner-brazils-largest-clothing-store-chain/

Exploit: Ransomware

Lojas Renner: Fashion Retailer

Risk to Business: 1.663 = Severe

Lojas Renner, Brazilian biggest fashion retail chain, has been struck by a ransomware attack that impacted its IT infrastructure and resulted in the unavailability of some of its systems, including online shopping. Reports claim that the deed was done by RansomExx and it may be related to an incident at a Brazilian IT services provider and that Renner paid the hackers $20 million in ransom.

Individual Impact: There has not yet been an announcement that employee, customer or consumer personal or financial information was compromised in this incident but the investigation is ongoing.

Customers Impacted: Unknown

How it Could Affect Your Business: Ransomware is the weapon of choice for both run-of-the-mill cybercriminals and nation state threat actors. Every business needs to be ready for it.

Brazil: National Treasury (Tesouro Nacial Brasil)

https://www.teiss.co.uk/brazil-national-treasury-ransomware-attack/

Exploit: Hacking

National Treasury (Tesouro Nacional Brasil): National Government Agency

Risk to Business: 1.671 = Severe

The Brazilian government has confirmed that the National Treasury (Tesouro Nacional Brasil) fell victim to a ransomware attack on August 13. The extent of the damage is unclear and operations in the department were quickly restored. Government officials were quick to assure investors that the cyberattack did not affect the operations of Tesouro Direto, which enables the purchase of Brazilian government bonds. The incident is not suspected to be the work of nation-state threat actors.

Customers Impacted: Unknown

How it Could Affect Your Business: Ransomware is a popular tool to use against government targets because it's an easy way for cybercriminals to create disruptions that may produce ransoms more easily.

Indonesia: OT Group

https://www.channelnewsasia.com/business/orangetee-data-security-breach-real-estate-2096391

Exploit: Hacking

OT Group: Real Estate Holding Company

Risk to Business: **1.632 = Severe**

OT Group, a real estate holding company that is part of the OrangeTee & Tie and OrangeTee Advisory family, announced that it had experienced a data breach. The company said it received an email from a third party claiming to have accessed its IT network and reported the incident to the relevant authorities. The incident is under investigation.

Individual Impact: There has not yet been an announcement that employee, customer or consumer personal or financial information was compromised in this incident but the investigation is ongoing.

Customers Impacted: Unknown

How it Could Affect Your Business: Financial companies, financiers and fintech have been catnip for hackers this year, and they're seeking any available route to access information that can lead them to a healthy payday from those firms.