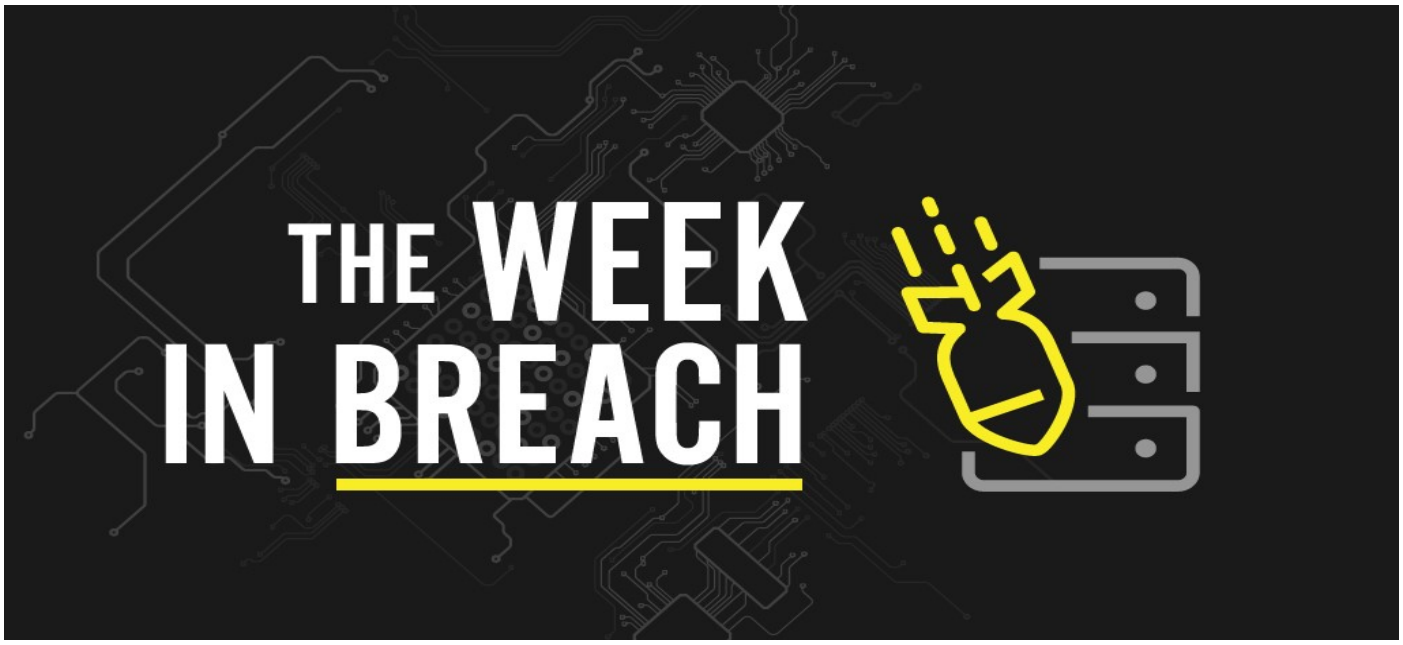
THE WEEK IN BREACH NEWS: 8/11/21— 08/17/21

DenBe Computer Consulting
Connecting Business

August 18, 2021 by Dennis Jock

Get the details of the Accenture breach, the story behind the T-Mobile data being shopped on the dark web, ransomware at Chanel & 3 new dangerous, under-the-radar ransomware risks to secure yourself against.



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: Accenture

https://threatpost.com/accenture-lockbit-ransomware-attack/168594/

Exploit: Ransomware

Accenture: Consulting Firm

Risk to Business: 1.437 = Extreme

The LockBit ransomware gang has hit consulting giant Accenture. In a post on its dark web announcement site, the gang is offering multiple Accenture databases for sale. The LockBit gang also chose to poke fun at Accenture's security. The leak site shows a folder named W1 that contains a collection of PDF documents allegedly stolen from the company. The LockBit ransomware gang reports theft of 6 terabytes worth of Accenture's data. LockBit requested a $50 million ransomware payment. News outlets are reporting that the hack was the result of an insider job.

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 hits against big service providers are attractive for cybercriminals because they often open up fresh avenues of attack, creating third-party risk.

United States: Ford Motor Company

Exploit: Misconfiguration

Ford Motor Company: Automobile Manufacturer

Risk to Business: **2.033 = Severe**

A misconfigured instance of the Pega Infinity customer engagement system running on Ford's servers is the culprit for a data breach this week that exposed client and employee information at Ford. That blunder opened up an opportunity for anyone to access sensitive systems and obtain proprietary data, such as customer databases, employee records, internal tickets, etc. Researchers say that Ford was notified of this massive problem as long as six months ago but failed to take action.

Risk to Individual: **2.371 = Severe**

The investigation is ongoing, but right now we know that some of the exposed assets contained sensitive Personal Identifiable Information (PII), and included customer and employee records, finance account numbers, Database names and tables, OAuth access tokens, Internal support tickets, User profiles within the organization, pulse actions, internal interfaces, search bar history and other details.

Customers Impacted: Unknown

How it Could Affect Your Business: Companies are under the gun for cybersecurity risk often enough without rookie mistakes like failing to secure a database contributing to the danger.

United States: T-Mobile

https://gizmodo.com/hacker-claims-to-have-data-on-more-than-100-million-t-m-1847491056

Exploit: Hacking

T-Mobile: Mobile Phone Company

Risk to Business: 1.673=Severe

Hackers are claiming that they've obtained data related to more than 100 million US T-Mobile customers in a post on a popular dark web forum. They're selling access to part of the information for 6 Bitcoin which translates into roughly $277,000. T-Mobile has confirmed the incident after some back-and-forth.

Risk to Business: 1.737=Severe

The data purportedly stolen is records and information for consumers including social security numbers, phone numbers, names, physical addresses, unique IMEI numbers, and driver licenses information.

Customers Impacted: 100 million

How it Could Affect Your Business: Cybercriminals love personal data, the number one type of data stolen in 2020. Protecting customer data is critical to maintaining good customer relationships.

United States: Maine Department of Environmental Protection

https://bangordailynews.com/2021/08/15/news/in-a-first-for-maine-ransomware-hackers-hit-2-public-wastewater-plants/

Exploit: Ransomware

Main Department of Environmental Protection: State Government Agency

Risk to Business: **1.825 = Severe**

Ransomware attacks endangered operations at two Maine wastewater treatment facilities this week. The attacks occurred in the Aroostook County town of Limestone and the town of Mount Desert on Mount Desert Island. Officials were quick to note that the attacks presented no threat to public health and safety, characterizing them as minor. Operations have been restored.

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.

France: Chanel

https://www.infosecurity-magazine.com/news/chanel-apologizes-for-data-breach/

Exploit: Ransomware

Chanel: Fashion House

Risk to Business: 2.721 = Moderate

French luxury brand Chanel has issued an apology after personal data belonging to its customers was exposed in an incident that impacted customers in Korea. A database belonging to the famed perfume and fashion brand is believed to have been compromised by hackers in a cyberattack at an unnamed cloud-based data storage firm.

Risk to Business: 2.326 = Moderate

The stolen data includes birth dates, customer names, gender details, passwords, phone numbers and shopping or payment history. The incident is still under investigation and complete details have not been released.

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.

Germany: Crytek Studios

https://www.bleepingcomputer.com/news/security/crytek-confirms-egregor-ransomware-attack-customer-data-theft/

Exploit: Ransomware

Crytek Games: Game Studio

Risk to Business: 1.612 = Severe

German game developer Crytek has just disclosed that the Egregor ransomware gang breached its network in late 2020 obtaining client information, stealing proprietary data and encrypting systems. Files related to online FPS hit WarFace, development data on Crytek's canceled Arena of Fate MOBA game, and documents with information on their network operations. The company downplayed the impact in a letter to potentially impacted individuals.

Risk to Business: 1.669 = Severe

The customer information exposed included players' first and last name, job title, company name, email, business address, phone number and country. Impacted players have been sent a notification by mail.

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.

Israel: Bar Ilan University

Exploit: Nation-State Hacking

Bar Ilan University: Institution of Higher Learning

Risk to Business: 1.111 = Severe

A cyberattack that targeted Israel's Bar Ilan University over the weekend was likely launched by Chinese threat actors as part of a massive attack against Israeli targets in varied sectors. In a report released by FireEye, the incident is categorized as part of a large-scale Chinese attack on Israel, in itself part of a broader campaign that targeted Iran, Saudi Arabia, Ukraine, Uzbekistan and Thailand.

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: Nation-state threat actors frequently use ransomware to strike at their targets because it is cheap and effective.

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.