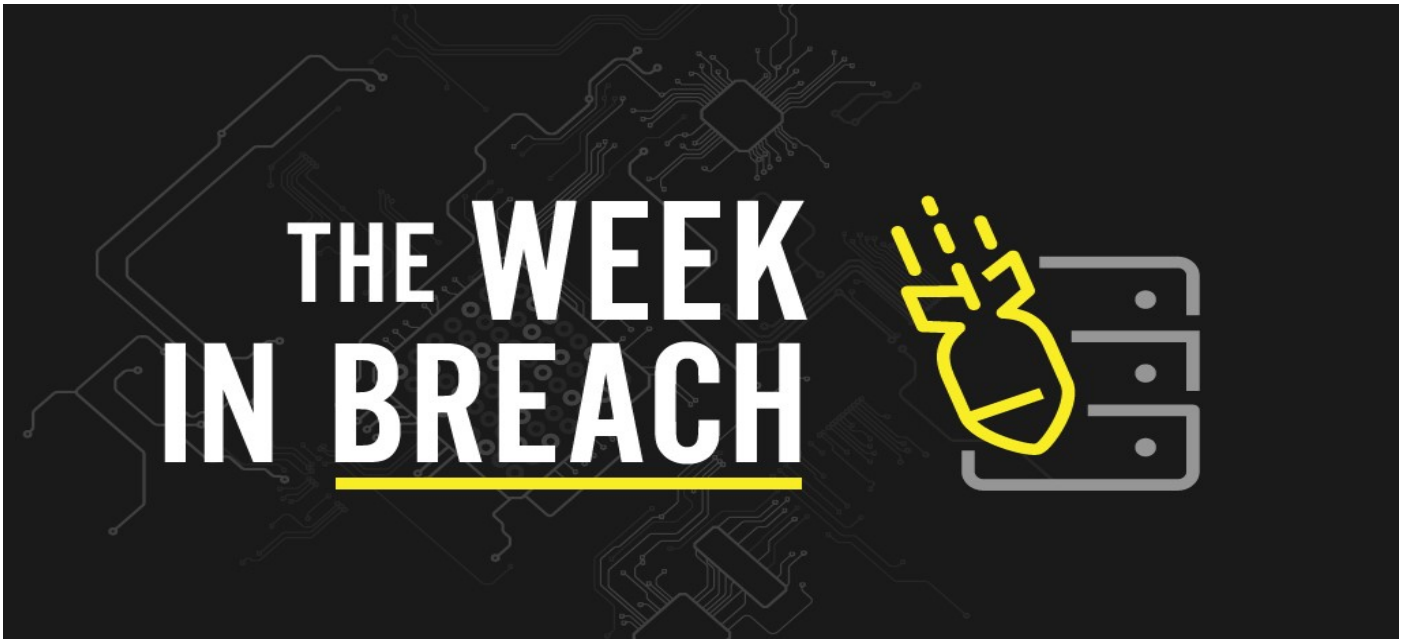
THE WEEK IN BREACH NEWS: 8/25/21— 08/31/21

DenBe Computer Consulting
Connecting Business

September 1, 2021 by Dennis Jock

Ransomware comes calling at a Nokia subsidiary, cyber criminals check data out of the Boston Public Library, personal data is snatched from Bangkok Airlines and 3 easy things to do to improve your clients' security culture (and why that matters now more than ever).



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: SAC Wireless

https://www.bleepingcomputer.com/news/security/nokia-subsidiary-discloses-data-breach-after-conti-ransomware-attack/

Exploit: Ransomware

SAC Wireless: Mobile Network Services

Risk to Business: 1.486 = Extreme

SAC Wireless, a US-based Nokia subsidiary, has disclosed a data breach following a ransomware attack attributed to the Conti ransomware gang. The company disclosed that personal information belonging to current and former employees (and their health plans' dependents or beneficiaries) was also stolen during the ransomware attack. Conti ransomware gang revealed on their leak site that they stole over 250 GB of data. The investigation and remediation is ongoing.

Individual Risk : 1.311 = Extreme

SAC Wireless has announced that they believe that the stolen files contain the following categories of personal info about current and former employees: name, date of birth, contact information (such as home address, email, and phone), government ID numbers (such as driver's license, passport, or military ID), social security number, citizenship status, work information (such as title, salary, and evaluations), medical history, health insurance policy information, license plate numbers, digital signatures, certificates of marriage or birth, tax return information, and dependent/beneficiary names.

Customers Impacted: Unknown

How It Could Affect Your Business: Ransomware gangs are increasingly targeting the partners of major companies to find security flaws that enable them to gain valuable access or information that can then be translated into action against the major target.

United States: Boston Public Library

https://www.bleepingcomputer.com/news/security/boston-public-library-discloses-cyberattack-system-wide-technical-outage/

Exploit: Ransomware

Boston Public Library (BPL): Library System

Risk to Business: **2.336 = Severe**

The Boston Public Library (BPL) has disclosed that its network was hit by a cyberattack leading to a system-wide technical outage. BPL serves almost 4 million visitors per year through its central library and twenty-five neighborhood branches, as well as millions more online. The library experienced a significant system outage and as well as disruption of its online library services. Branch It has been restored and online services are slowly being recovered.

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: 4 million

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: Envision Credit Union

https://www.tallahassee.com/story/money/2021/08/26/envision-credit-union-taking-steps-after-possible-cyber-attack-lockbit/8254377002/

Exploit: Ransomware

Envision Credit Union: Bank

Risk to Business: 1.673=Severe

The LockBit 2.0 ransomware group has threatened to publish stolen data of its newest target, Envision Credit Union in Florida, on August 30. Envision Credit Union disclosed to the media that recently began "experiencing technical difficulties on certain systems" after the LockBit announcement went up on the gang's leak site. An investifation is ongoing and the bank has not yet disclosed exactly what (if any) data was stolen.

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 services and FinTech organizations have been a prime target for hackers recently, and regulators have not been shy about raising the alarm.

United States: Atlanta Allergy and Asthma

Exploit: Hacking

Atlanta Allergy and Asthma: Allergy treatment business

Risk to Business: **1.917 = Severe**

Atlanta Allergy & Asthma (AAA), the largest allergy treatment healthcare business in the region, is notifying 9,800 patients that they experienced a data breach that involved protected health information.
Bloggers spotted the data on the dark web, where it had been posted by the Nefilim ransomware group, also known as Nempty. The gang nabbed 2.5 GB of data consisting of 597 files with PHI.

Individual Risk: **1.835 = Severe**

The data seen by researchers includes what appears to be thousands of records for patients. The files are not just current or recent billing-related files but also included spreadsheets organized by type of health insurance, records on outstanding claims from 2017 and 2018 and more than 100 audits including a multi-page detailed review of a patient's case.

Customers Impacted: 9,800

How it Could Affect Your Business: Medical data is a big revenue driver for cybercriminals but it is an even bigger revenue disaster for the medical practices that lose it to cybercrime.

Germany: Puma

https://securityaffairs.co/wordpress/121617/cyber-crime/puma-available-marketo.html

Exploit: Hacking

Puma: Sportswear Brand

Risk to Business: 1.721 = Severe

Threat actors claim to have stolen data from German sportswear giant Puma. The cybercriminals announced the score in a post on a message board at the rising dark web marketplace Marketo claims to have about 1GB of data stolen from the company. Published samples contain the source code of internal management applications potentially linked to the company's Product Management Portal.

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: Hackers are hungry for data to turn for a quick profit in the booming dark web data markets. Reports note there are more than 150 bids on this little cache already.

Thailand: Bangkok Airways

https://www.zdnet.com/article/bangkok-airways-apologizes-for-passport-info-breach-as-lockbit-ransomware-group-threatens-release-of-more-data/

Exploit: Ransomware

Bangkok Airways: Airline

Risk to Business: 1.802 = Severe

Bangkok Airways has announced that it has experienced a "cybersecurity attack which resulted in unauthorized and unlawful access to its information system". There's no word from the company about how many customers were involved in the breach or what timeframe the data came from, but they were quick to assure customers that no operations or aeronautics systems or data was impacted.

Individual Risk: 1.761 = Severe

The company said in a statement that their initial an investigation revealed that the names, nationalities, genders, phone numbers, emails, addresses, contact information, passport information, historical travel information, partial credit card information and special meal information for passengers of the airline were accessed by the hackers.

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.