DenBe Computer Consulting
Connecting Business

THE WEEK IN BREACH NEWS: 10/07/20 – 10/13/20

This Week in Breach News: medical providers aren't just battling COVID-19, they're also battling cybercrime, malicious insiders cause chaos, studies show how frequently customers break up with businesses that have a data breach.

The Week in Breach News: Top Threats This Week

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

United States – Boom! Mobile

https://securityaffairs.co/wordpress/108925/malware/ajg-ransomware-attack.html

Exploit: Skimming (MageCart)

Boom! Mobile: Telecom

Risk to Business: 1.997 = Severe

Credit card skimming software has landed at Boom! Mobile, courtesy of the cybercriminal skimmers at Fullz House. The card skimmer code settled in, collecting payment card information from input fields every time it detects any changes and immediately exfiltrating the harvested data for a week. The company's mobile payment system is still undergoing repairs.

Individual Risk: 1.517 = Severe

Customers of Boom! Mobile who made electronic payments through the company's website should consider their credit card information compromised and be alert to potential identity theft or fraud using that account.

Customers Impacted: Unknown

How it Could Affect Your Customers' Business: Malware like this runs on a script that's been grafted into the payment system, meaning cybercriminals have access to the nuts and bolts of that business.

United States – Friendemic

https://www.infosecurity-magazine.com/news/marketing-firm-spills-nearly-three/

Exploit: Unsecured Database

Friendemic: Marketing Firm

Risk to Business: 2.227 = Severe

Digital marketing firm Friendemic committed a classic blunder that led to a nasty data breach. An unsecured Amazon S3 bucket resulted in the exposure of 2.7 million records including full names, phone numbers, and email addresses, alongside 16 OAuth tokens stored in plaintext. The company noted that the information was not current customer data and the OAuth tokens were not currently in use.

Individual Risk: No individual information was reported as compromised in this incident, although the potential is there. No details about the uncovered data are available.

Customers Impacted: Unknown

How it Could Affect Your Customers' Business: Failing to secure a database, even an old one, shows a basic lack of attention to cybersecurity best practices, and that doesn't build customer confidence.

United States – AAA Ambulance Service, Inc.

https://www.hattiesburgamerican.com/story/news/local/hattiesburg/2020/10/05/aaa-ambulance-service-hattiesburg-ms-reports-july-data-breach/3625304001/

Exploit: Ransomware

AAA Ambulance Service, Inc.: Ambulance Service

Risk to Business: 1.602 = Severe

Hattiesburg, Mississippi based AAA Ambulance Service, Inc. is just one of several medical sector targets impacted by ransomware this week. A ransomware attack was repelled by the company's security in July, but it was recently discovered that some client data was obtained around August 2020.

Individual Risk: 2.316 = Severe

Personal information about clients of the service was obtained by hackers, including client date of birth, Social Security number, driver's license number, financial account number, diagnosis information, medical treatment information, patient account number, prescription information, medical record number, and health insurance information. Customers who may have been impacted have been contacted by the company and are also being offered complimentary credit monitoring services through TransUnion.

Customers Impacted: Unknown

How it Could Affect Your Customers' Business: Serious personal information deserves serious security – and even a seemingly unsuccessful cyberattack can still result in data loss. Not only will healthcare sector companies have to pay recovery costs, but they'll also be on the hook for regulatory penalties.

United States – Daniel B. Hastings

https://www.freightwaves.com/news/ransomware-hackers-claims-attack-on-texas-customs-broker

Exploit: Ransomware

Daniel B. Hastings: Freight Forwarder

Risk to Business: 2.326 = Moderate

In the latest incident in a spate of recent trucking and freight transport industry cyberattacks, Laredo, Texas-based Daniel B. Hastings was hit with a ransomware attack. the Conti ransomware group posted a selection of the company's files on Saturday, and sources say that they appear authentic. They include completed U.S. Customs and Border Protection documents for shipments involving multiple countries, companies, and modes of transport.

Individual Risk: No personal data has been reported as impacted in this incident.

Customers Impacted: Unknown

How it Could Affect Your Customers' Business: Ransomware is a devastating weapon that bad actors are using to shut down essential services and attacks in the transportation and freight sectors have been increasing, with recent incidents involving several trucking and shipping companies.

United States – Georgia Department of Human Services

https://www.cbs46.com/news/cyber-attack-targets-georgia-department-of-human-services/article_57f9749e-0a72-11eb-a724-3b34ced6f18f.html

Exploit: Employee Email Account Compromise

Georgia Department of Human Services: State Agency

Risk to Business: 1.414 = Extreme

A massive breach at the Georgia Department of Human Services has left the highly sensitive data of adults and children in Child Protective Services (CPS) cases of the DHS Division of Family & Children Services (DFCS). The employee email account compromise occurred in May 2020. Georgia DHS secured the account quickly, but damage included

Individual Risk: 1.202 = Extreme

Extremely sensitive information about parents, children, and families that has contact with DFCS was stolen in this attack, including full names of children involved in those cases and household members, relationship to the child receiving services, county of residence, DFCS case numbers, DFCS identification numbers, date of birth, age, number of times contacted by DFCS, an identifier of whether face-to-face contact was medically appropriate, phone numbers, email addresses, Social Security numbers, Medicaid identification numbers, Medicaid medical insurance identification numbers, medical provider names and appointment dates, plus some psychological reports, counseling notes, medical diagnoses, or substance abuse information and bank information.

Customers Impacted: Unknown

How it Could Affect Your Customers' Business: Not only does a data breach leave a huge mess of expensive cleanup behind, in many industries like healthcare, a data breach can also mean your organization will be paying big regulatory penalties and fines too.