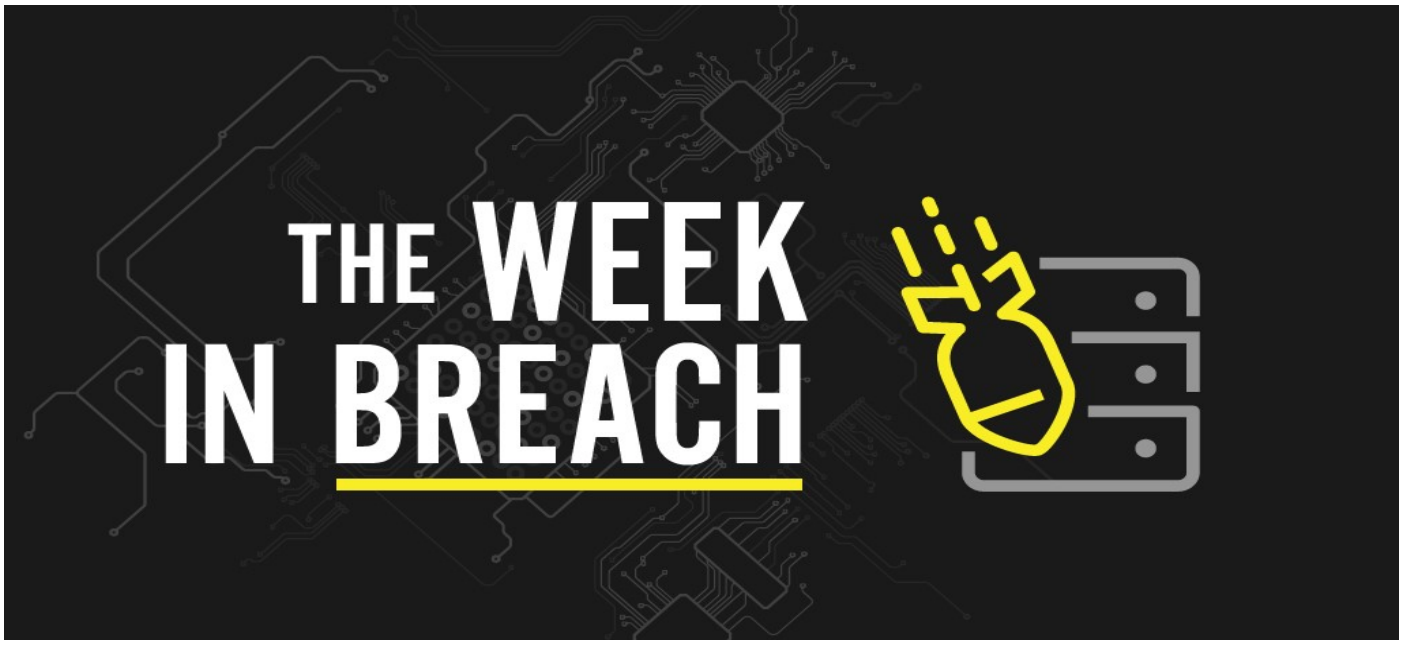
THE WEEK IN BREACH NEWS: 06/09/21— 6/15/21

DenBe Computer Consulting
Connecting Business

June 16, 2021 by Dennis Jock

We're celebrating Flag Day with an All-American Edition of the Week in Breach. This week, REvil takes aim at a US nuclear defense contractor, hackers take a bite out of McDonald's and our new book Ransomware Exposed! tells you behind the scenes to show you the real story of this devastating cybercrime.



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: Electronic Arts

https://www.reuters.com/business/hackers-steal-wealth-data-ea-vice-2021-06-10/

Exploit: Ransomware

Electronic Arts Inc: Game Developer

Risk to Business: **1.355= Extreme**

Electronic Arts (EA) has announced that it is investigating a data breach. Cybercriminals stole valuable corporate data from the company including game source code and related tools. Early reports noted that hackers had stolen source codes for the popular title “FIFA 21” and source code and tools for the Frostbite engine. Researchers estimate that 780 gigabytes of data was snatched then advertised for sale on underground hacking forums.

Customers Impacted: Unknown

How It Could Affect Your Business: Hackers are always interested in proprietary data and corporate secrets, the 3rd most popular category for theft. They’re easy money in the busy dark web data markets.

United States - Edward Don

https://www.bleepingcomputer.com/news/security/foodservice-supplier-edward-don-hit-by-a-ransomware-attack/

Exploit: Ransomware

Edward Don: Foodservice Distributor

Risk to Business: 1.816 = Severe

Foodservice equipment distributor Edward Don has been hit by a ransomware attack. The incident has disrupted their business operations, including their phone systems, network and email. As a result, employees have been driven to using personal Gmail accounts to communicate with customers regarding urgent orders or fulfillment issues. The incident is under investigation and full functionality was quickly restored.

Individual Impact: No sensitive personal or financial information has been declared compromised in this incident and the investigation is ongoing.

Customers Impacted: Unknown

How it Could Affect Your Business: Ransomware attacks against strategic targets like this are becoming all too common as ransomware gangs seek to cause maximum buzz for maximum profit.

United States – McDonald's Corp

https://www.reuters.com/technology/mcdonalds-hit-by-data-breach-south-korea-taiwan-wsj-2021-06-11/

Exploit: Ransomware

McDonald's: Fast Food Chain

Risk to Business: 2.606 = Moderate

McDonald's Corp. said hackers exposed US business information and some customer data in South Korea and Taiwan. The attackers accessed e-mails, phone numbers and delivery addresses. The company reported that it had hired external consultants to investigate unauthorized activity on an internal security system, prompted by a specific incident in which the unauthorized access was cut off a week after it was identified. The announcement noted that the burger chain does not believe any customer payment data was stolen but cautioned that there may be employee data exposed.

Individual Impact: There has not yet been confirmation that sensitive personal or financial information has been compromised in this incident but the investigation is ongoing.

Customers Impacted: Unknown

How it Could Affect Your Business: Cyberattacks that focus on obtaining corporate or business data are increasingly troubling because each one adds more sensitive data to the dark web that can be used against other businesses.

United States - Intuit

https://www.bleepingcomputer.com/news/security/intuit-notifies-customers-of-compromised-turbotax-accounts/

Exploit: Account Takeover (ATO)

Intuit: Financial Software Developer

Risk to Business: **1.612 = Severe**

Accounting software giant Intuit has notified customers that they have suffered a breach. The company warned users of TurboTax that their personal and financial information was accessed by attackers following what looks like a series of account takeover attacks. Intuit announced that the threat actors used credentials (usernames and passwords) obtained from "a non-Intuit source" to gain access to the accounts.

Risk to Business: **1.832= Severe**

Intuit notified potentially impacted clients by mail that information contained in a prior year's tax return or current tax returns in progress including their name, Social Security number, address(es), date of birth, driver's license number and financial information (e.g., salary and deductions) and information of other individuals contained in the tax return may have been exposed.

Customers Impacted: Unknown

How it Could Affect Your Business: Clients expect a high level of information security from companies that they trust with their personal and financial information, and may stop doing business with companies that fail to protect it.

United States - Sol Oriens

https://www.techtimes.com/amp/articles/261472/20210615/revil-hacking-group-s-ransomware-attack-nuclear-weapons-contractor-sol.htm

Exploit: Ransomware

Sol Oriens: Defense Contractor

Risk to Business: 2.337 = Severe

REvil has struck again, this time against a tiny but important target in the defense sector. Sol Oriens, which consults for the US Department of Energy's National Nuclear Safety Administration, is a 50-person firm based in Albuquerque, New Mexico. Researchers noted finding Sol Oriens documents posted on the dark web, told CNBC that they include invoices for NNSA contracts, descriptions of research and development projects managed by defense and energy contractors dated as recently as 2021.

Individual Impact: No sensitive personal or financial information has been confirmed as compromised in this incident although some sources are reporting that human resources data is in the mix.

Customers Impacted: Unknown

How it Could Affect Your Business: This seemingly small attack could pack big consequences. Ransomware gangs have been increasingly focused on hitting strategic targets that service major clients.

United States - Volkswagen Group of America

https://www.reuters.com/business/autos-transportation/vw-says-data-breach-vendor-impacted-33-million-people-north-america-2021-06-11/

Exploit: Third-Party Data Breach

Volkswagen Group of America: Automotive Manufacturer

Risk to Business: 1.825 = Severe

Volkswagen US has announced that it has suffered a data breach impacting millions of US customers and prospective customers. the car company released information saying that a data breach at a vendor has exposed data on more than 3.3 million buyers and prospective buyers in North America. An unauthorized third party obtained limited personal information about customers and interested buyers from a vendor that its Audi Volkswagen brands and some U.S. and Canadian dealers used for digital sales and marketing.

Risk to Business: 2.223 = Severe

The information was gathered for sales and marketing between 2014 and 2019 and was in an electronic file the vendor left unsecured. According to Volkswagen, the majority of people impacted had phone numbers and email addresses exposed, but some clients had their driver's license information stolen as well. In some cases, information about a vehicle purchased, leased, or inquired about was also obtained. VW said 90,000 Audi customers and prospective buyers also had sensitive data impacted relating to purchase or lease eligibility. VW said it will offer free credit protection services to those individuals.

Customers Impacted: 3.3 Million

How it Could Affect Your Business: Attacks on data processors and other essential service providers have escalated as cybercriminals look for big data scores and information that facilitates more cybercrimes.

United States-New York City Law Department

https://www.nytimes.com/2021/06/07/nyregion/cyberattack-law-department-nyc.html

Exploit: Ransomware

New York City Law Department: Municipal Government Agency

Risk to Business: **1.633 = Severe**

The New York City Law Department experienced a cyberattack that impacted its computer systems, forcing it to shut down its technology. The network also had to be disconnected from other city systems for safety. Systems are being restored slowly and the FBI is investigating along with New York police.

.

Individual Impact: No sensitive personal or financial information has been confirmed as compromised in this incident.

Customers Impacted: Unknown

How it Could Affect Your Business: Attacks that strike at government and infrastructure targets frequently use ransomware to get the job done, and no matter how big or small, no organization is safe.

United States: Carter's

https://threatpost.com/baby-clothes-carters-leaks-customer-records/166866/

Exploit: Third Party Data Breach

Carter's: Children's Clothier

Risk to Business: **2.331 = Severe**

In a new disclosure, baby clothing giant Carter's admitted that it had suffered a data breach through a third-party data processor, exposing the personal data of hundreds of thousands of its customers over a multiyear period. The service provider, Linc, handled automation for online purposes. The Linc system was used to send customers shortened URLs containing everything from purchase details to tracking information without basic security protections.

Individual Impact: At this time, no sensitive personal or financial information was announced as compromised in this incident, but the investigation is ongoing.

Customers Impacted: Unknown

How it Could Affect Your Business: Every business has relationships with other businesses, and every relationship they have creates risk. Protecting companies from supply chain risk is imperative.