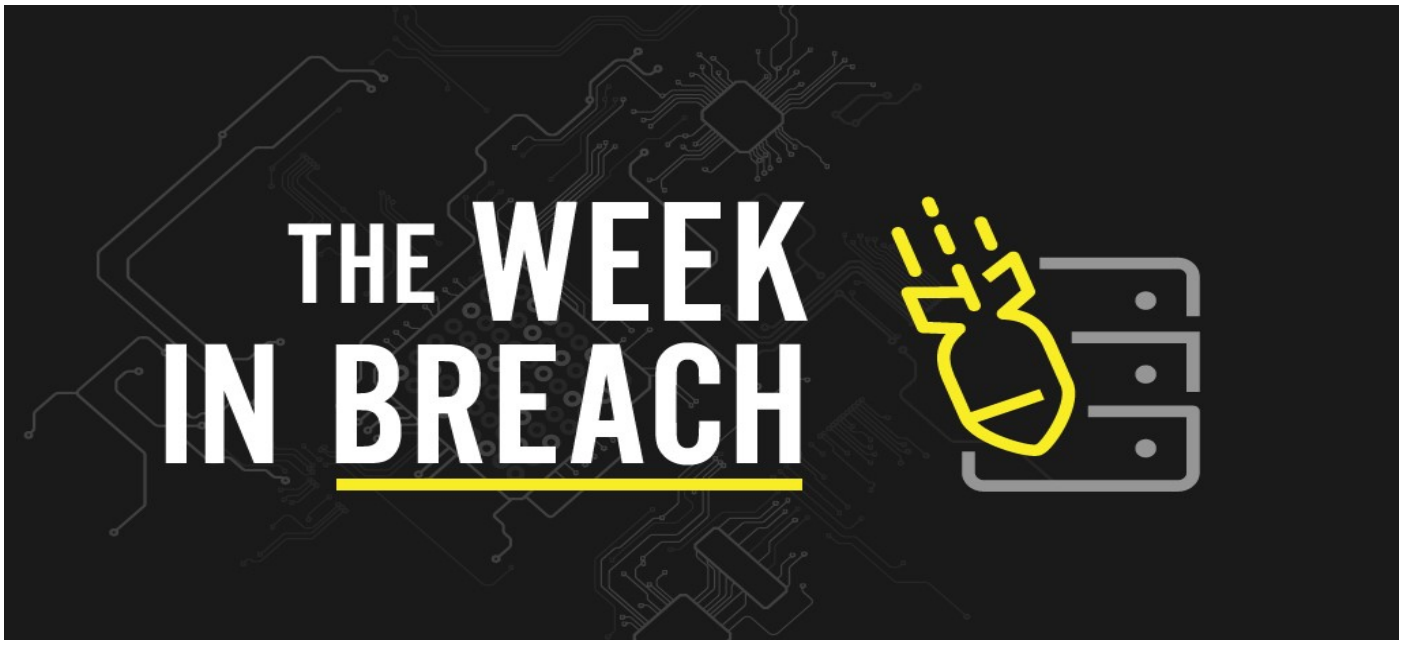
THE WEEK IN BREACH NEWS: 8/04/21— 08/10/21

DenBe Computer Consulting
Connecting Business

August 11, 2021 by Dennis Jock

Ransomware ventures into capital as a funding firm gets hit in California, a penetration test discovers that hackers have already been there at the University of Kentucky, two huge PII exposures and a snapshot of the 3 threats that are topping the charts so far in 2021.



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: Advanced Technology Ventures

https://techcrunch.com/2021/08/03/atv-venture-capital-ransomware/

Exploit: Ransomware

Advanced Technology Ventures: Capital Firm

Risk to Business: 1.207 = Extreme

Advanced Technology Ventures, a Silicon Valley venture capital firm with more than $1.8 billion in assets under its management, has disclosed that it was hit by a ransomware attack. The cybercriminals were able to steal personal information about the company's private investors. ATV said it became aware of the attack on July 9 after its servers storing financial information were encrypted by ransomware. By July 26, the company learned that its investor data had been stolen from the servers before the files were encrypted, a hallmark of the "double extortion" tactic used by ransomware groups.

Individual Risk: 1.326 = Extreme

Investor data was accessed by cybercriminals. ATV believes the names, email addresses, phone numbers and Social Security numbers of the individual investors in ATV's funds were stolen in the attack. Some 300 individuals were affected by the incident.

Customers Impacted: Unknown

How It Could Affect Your Business: Ransomware tactics like double and triple extortion allow cybercriminals to score even bigger paydays, making them very popular techniques.

United States: SeniorAdvisor

https://www.infosecurity-magazine.com/news/senior-citizens-personal-data/

Exploit: Misconfiguration

SeniorAdvisor: Senior Care Review Site

Risk to Business: **1.663 = Severe**

Researchers have discovered a misconfigured Amazon S3 bucket owned by SeniorAdvisor, a site that provides ratings and information for senior care facilities. The bucket in question contained the personal data of more than three million people categorized as “leads”. The team found around 2000 “scrubbed” reviews in the misconfigured bucket, in which the user’s sensitive information was wiped or redacted. In total, it contained more than one million files and 182GB of data, none of which was encrypted and did not require a password or login credentials to access.

Risk to Individual: **1.271 = Severe**

This exposed bucket was full of data including names, emails, phone numbers and dates contacted for every person designated as a lead, comprising an estimated 3 million consumers.

Customers Impacted: 3 million

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: University of Kentucky

https://therecord.media/university-of-kentucky-discovers-data-breach-during-scheduled-pen-test/

Exploit: Hacking

University of Kentucky: Institution of Higher Learning

Risk to Business: 2.223=Severe

In a head-shaking turn of irony, officials at the University of Kentucky discovered that they'd already been breached while conducting a penetration test. The breach affected the university's Digital Driver's License platform, a web-based portal the university developed as a component of its Open-Source Tools for Instructional Support (OTIS) framework. That program provides free online teaching and test-taking capabilities to K-12 schools and colleges in Kentucky and other US states. University officials said that their investigation discovered that an unknown threat actor accessed the system between January 8, 2021, and February 6, 2021, to gain access to the DDL platform and acquire a copy of its internal database.

Risk to Business: 2.223=Severe

The database contained the names and email addresses of students and teachers in Kentucky and in all 50 states and 22 foreign countries, in all more than 355,000 individuals. The university was careful to note that the stolen information included only emails and passwords and no SSNs or financial details were included.

Customers Impacted: Unknown

How it Could Affect Your Business: Cybercriminals have been increasingly setting their sights on education targets since the onset of the global pandemic, and that trend is not stopping in 2021.

United States: Reindeer

https://www.enterprisesecuritytech.com/post/defunct-marketing-company-leaked-the-sensitive-data-of-over-300-000-people

Exploit: Misconfiguration

Reindeer: Digital Marketing Firm

Risk to Business: **1.705 = Severe**

New York-based digital media advertising and marketing company Reindeer left an unpleasant surprise behind when it closed its doors: an Amazon S3 bucket exposed to public access resulting in the irreversible leak of 50,000 files for a total of 32 GB of exposed data. The information exposed included about 1,400 profile photos and the details of approximately 306,000 customers in total. Users in 35 countries were represented with the US, Canada, and Great Britain accounting for almost 280,000 of those users. Nothing can be done to secure this data now.

Individual Risk: **1.622 = Severe**

PII exposed includes customer names, surnames, email addresses, dates of birth, physical addresses, hashed passwords, and Facebook IDs for an estimated 306,000 customers.

Customers Impacted: Unknown

How it Could Affect Your Business: Unexpected risks from sources like zombie accounts are around every corner, so taking that possibility seriously and mitigating risk from nasty surprises is critical.

Canada: School District No. 73 (SD73. Kamloops-Thompson)

https://cfjctoday.com/2021/08/01/sd73s-insurance-provider-for-international-students-suffers-cybersecurity-breach/

Exploit: Nation-State Hacking

School Distrct No. 73 (SD73, Kamloops-Thompson): Education Provider

Risk to Business: 2.911 = Moderate

School District No. 73 (SD73, Kamloops-Thompson) said it was notified that third-party service provider that it uses for travel and medical insurance provider for its international student program, guard.me, experienced a data breach that potentially exposed student information. Guard.me released a statement about the data security incident that spawned this data exposure, noting that the incident occurred during June 2021.

Risk to Business: 2.936 = Moderate

Student personal information that may be impacted by this incident includes identity information, contact information and other information provided to support submitted claims. impacted individuals are encouraged to visit the Canadian Anti-Fraud Centre for further information about how to protect themselves.

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.

Italy: - ERG

https://www.bleepingcomputer.com/news/security/energy-group-erg-reports-minor-disruptions-after-ransomware-attack/

Exploit: Ransomware

ERG: Energy Company

Risk to Business: **1.919 = Severe**

Italian energy company ERG reported minimal impact on infrastructure or consumer-facing services following a LockBit 2.0 ransomware incident. ERG is the leading Italian wind power operator and among the top ten onshore operators on the European market, with a growing presence in France, Germany, Poland, Romania, Bulgaria, and the United Kingdom. ERG was purchased by European power giant Enel earlier this week.

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.

Taiwan: Gigabyte

https://www.bleepingcomputer.com/news/security/computer-hardware-giant-gigabyte-hit-by-ransomexx-ransomware/

Exploit: Misconfiguration

Gigabyte: Motherboard Manufacturer

Risk to Business: 1.602 = Severe

Motherboard manufacturer Gigabyte has been hit by the RansomEXX ransomware gang. The Taiwanese company was forced to shut down systems in Taiwan as well as multiple customer and consumer-facing websites of the company, including its support site and portions of the Taiwanese website. RansomEXX threat actors claimed to have stolen 112GB of data during the attack in an announcement on their leak site.

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: Mistakes like this are only compounded by blunders in the response. It shows clients that you aren't concerned about their security if you aren't concerned about yours.

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.