THE WEEK IN BREACH NEWS: 11/18/20 – 11/24/20

DenBe Computer Consulting
Connecting Business

November 25, 2020 by Dennis Jock

This Week in Breach News: Ransomware scores at Manchester United and chills Americold, Managed.com gets rocked by REvil, Luxottica's data breach nightmare continues, and how social engineering sneaks up on remote workers.

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***

Managed.com

https://securityaffairs.co/wordpress/111154/cyber-crime/managed-com-revil-ransomware.html

Exploit: Ransomware

Managed.com: Web Hosting Provider

Risk to Business: 1.402 = Extreme

REvil has had a nasty impact at this web hosting provider, causing a complete shutdown of company systems. The company says that a "limited number" of customer sites have been affected. Impacted functions included WordPress and DotNetNuke managed hosting platforms, online databases, email servers, DNS servers, RDP access points, and FTP servers.

Individual Risk: Managed.com has not released any information about potential client impact, although the company did note that they'd taken measures to secure client data.

Customers Impacted: Unknown

How it Could Affect Your Customers' Business: Third party risk is a growing problem for every business, especially as cybercriminals target more centralized service and infrastructure companies.

Mercy Iowa City

https://www.kcrg.com/2020/11/18/mercy-iowa-city-reports-data-breach-over-60000-iowans-affected/

Exploit: Unauthorized Access

Mercy Iowa City: Medical Center

Risk to Business: 2.631 = Moderate

An unauthorized user gained access to an employee email account at this Iowa hospital, leading to the potential exposure of sensitive data for thousands of patients. There's no confirmation that data was stolen, but the hospital is warning patients of the possibility The incident was discovered after the compromised account began sending out spam and phishing messages.

Individual Risk: 2.502 = Moderate

The hospital has not yet confirmed that any data was actually accessed or stolen, but they sent out a letter warning patients of the potential breach. Information that may have been compromised includes patient names, Social Security numbers, driver's license numbers, dates of birth, medical treatment information and health insurance information.

Customers Impacted: 60,000

How it Could Affect Your Customers' Business: Password compromise leads to major trouble. Even small incidents like this can quickly turn into huge problems if access to sensitive data isn't carefully controlled.

TronicsXchange

https://www.infosecurity-magazine.com/news/80000-id-cards-fingerprint-exposed/

Exploit: Misconfiguration

TronicsXchange: Used Electronics Dealer

Risk to Business: 1.992 = Severe

A big error at TronicsXchange has led to a big problem, as sensitive customer data was exposed on a misconfigured database. Over 2.6 million files, including ID cards and biometric images, were left open and leaking in a misconfigured AWS S3 bucket. The data appears to be older and is primarily comprised of California residents.

Individual Risk: 1.222 = Extreme

The data that was exposed was seriously sensitive and has the potential for massive troublemaking. Millions of files were leaked including extremely sensitive information like approximately 80,000 images of personal identification cards such as driver's licenses, and 10,000 fingerprint scans. The leaked driver's license photos expose even more information about that individual, including license number, full name, birthdate, home address, gender, hair and eye color, height and weight, and a photo of the individual, among other things.

Customers Impacted: 80,000

How it Could Affect Your Customers' Business: Leaving a database unsecured or misconfigured is a symptom of a lax cybersecurity culture. Leaving a database unsecured that has this kind of incredibly sensitive data inside is a disaster that will send customers running for the exits.

American Bank Systems

https://securityreport.com/american-bank-systems-hit-by-ransomware-attack-full-53-gb-data-dump-leaked/

Exploit: Ransomware

American Bank Systems: Software Services Provider

Risk to Business: 1.864 = Severe

Avaddon ransomware made an unwelcome deposit at American Bank Systems, unleashing a ransomware attack that led to the capture and partial publishing of 53 GB of all sorts of highly confidential data. The banking software services company had data snatched from banks around the world including banking names and mortgage companies, such First Federal Community Bank, Rio Bank, Citizens Bank of Swainsboro, First Bank & Trust, and many more. The leaked data in the dump includes files such as loan documents, business contracts, private emails, invoices, credentials for network shares, and other confidential information.

Individual Risk: 1.516 = Severe

Many of the stolen banking records also contain information about the clients of affected banks including, personally identifying information, loan amounts, and Tax ID or Social Security numbers. Some data on employees of banks was also exposed. Clients of impacted backs should be alert to identity theft and fraud possibilities.

Customers Impacted: Unknown

How it Could Affect Your Customers' Business: Third-party service providers may not have the same commitment to data security as you do. It pays to do your homework to avoid these problems whenever possible.

Americold

https://www.bleepingcomputer.com/news/security/cold-storage-giant-americold-hit-by-cyberattack-services-impacted/

Exploit: Ransomware

Americold: Cold Storage and Logistics

Risk to Business: 2.236 = Severe

Ransomware definitely chilled business at Americold, causing major disruptions to operations. The cyberattack impacted their operations across the board, causing partial or complete shutdowns in phone systems, email, inventory management, and order fulfillment. This attack may be related to a recent spate of attacks against healthcare targets. Cold storage and temperature-controlled transportation will be a huge component in the distribution of any COVID-19 vaccine.

Individual Risk: No personal or consumer information was reported as impacted in this incident.

Customers Impacted: Unknown

How it Could Affect Your Customers' Business: Ransomware isn't just stealing data anymore. Its also being used as a tool to disrupt infrastructure and logistics to devastating effect.

Port of Kennewick

https://www.nbcrightnow.com/news/port-of-kennewick-now-victim-of-cyber-attack/article_2da5b29c-2936-11eb-a2e4-0f3e16c73589.html

Exploit: Ransomware

Port of Kennewick: Municipal Agency

Risk to Business: 2.322 = Severe

Ransomware severely impacted operations at this inland port in Washington. Cybercriminals encrypted the port's systems and demanded $200,000 in ransom to restore access to the port's servers and files. The port authority, FBI, and an outside contractor have been working to restore full operations.

Customers Impacted: Unknown

How it Could Affect Your Customers' Business: Ransomware is a huge threat to infrastructure targets as well as businesses, and nation-state actors are most likely to use ransomware in their attacks.

Kenneth Copeland Ministries

https://www.dailymail.co.uk/news/article-8966623/Russian-hacker-group-REvil-claims-massive-attack-televangelist-Kenneth-Copeland.html

Exploit: Ransomware

Kenneth Copeland Ministries: Televangelism

Risk to Business: **2.306 = Severe**

The REvil ransomware gang strikes again, this time at televangelist Kenneth Copeland's operations. The gang is threatening to release 1.2 terrabytes of sensitive data if he fails to pay their unspecified ransom demands. Evidence of the hack has been displayed on REvil's information website.

Individual Risk: No personal or consumer information was reported as impacted in this incident so far, but it is still being remediated.

Customers Impacted: Unknown

How it Could Affect Your Customers' Business: Ransomware gangs like REvil can see juicy paydays in targeting prominent people in any industry – or releasing potentially embarrassing stolen data if those people decide not o pay the ransom.