THE WEEK IN BREACH NEWS: 01/06/21 – 01/12/21

DenBe Computer Consulting
Connecting Business

February 3, 2021 by Dennis Jock

This Week in Breach News: Ransomware romps through the UK, US Cellular has a CRM disaster that goes from bad to worse, big takedowns of ransomware gangs match the big surge in ransomware but don't fix the problem.

The Week in Breach News: Top Threats This Week

- **Top Source Hits:** ID Theft Forum
- **Top Compromise Type:** Domain
- **Top Industry:** Sales and Retail
- **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!

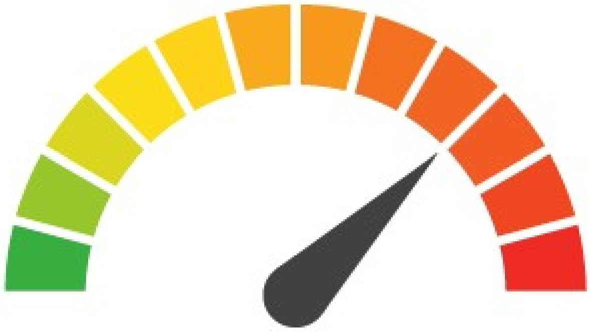
Not ready to talk yet? Visit our website to get your ***FREE Dark Web Scan***. You will get a free, no obligation scan sent to your inbox within 24hrs. ***Visit today: www.denbeconsulting.com***

DSC Logistics

https://www.freightwaves.com/news/ransomware-attack-targets-major-us-logistics-firm-dsc

Exploit: Ransomware

DSC Logistics: Shipping and Freight Logistics



Risk to Business: 1.775 = Severe

DSC logistics received an unwelcome delivery of Egregor ransomware. The attack was announced on the gang’s ransomware site. The company noted that it was successfully able to continue operations without incident. DSC has called in outside experts to investigate, and declined to comment on whether any data was stolen.

Individual Impact: No sensitive personal or financial information was announced as part of this incident, but the investigation is ongoing.

Customers Impacted: Unknown

How it Could Affect Your Business: Ransomware has been a plague on every industry, but freight and logistics companies have been hit especially hard in recent months.

US Cellular

https://www.techtimes.com/articles/256503/20210129/uscellular-data-breach-hackers-gained-access-users-personal-pin-code.htm

Exploit: Credential Compromise

US Cellular: Mobile Phone Company

Risk to Business: 1.379 = Extreme

USCellular, the fourth largest mobile network in the US, has suffered a data breach after a successful malware attack. Hackers used malicious code disguised as a routine software update to gain access to systems including its Customer Relationship Management (CRM) and client records. This is not USCellular's first time at this rodeo – the company has had consistent information security problems.

Individual Risk: 1.321 = Extreme

USCellular advised customers that their account records including name, address, PIN code, and cellular telephone numbers(s) as well as information about the customer's wireless services including service plan, usage and billing statements, personal information, PIN code, service plan, and billing statements might have been compromised. However, data such as social security numbers and credit card information remained inaccessible to the hackers. Clients should be wary of spear phishing, business email compromise and identity theft using this information.

Customers Impacted: 4.9 Million

How it Could Affect Your Business: Data like this is sought-after by cybercriminals to power phishing operations. Unfortunately for these folks, it often hangs around for years on the Dark Web, acting as fuel for future cybercrime.

Nissan North America

https://www.industryweek.com/technology-and-iiot/article/21151660/data-leak-hits-nissan-north-america

Exploit: Misconfiguration

Nissan North America: Automotive Manufacturer

Risk to Business: 2.779 = Moderate

Nissan North America recently suffered a data breach that resulted in source code for its mobile apps and internal tools turning up online. The data leak is reportedly the result of a misconfigured Git server. The source code is reported by a security researcher to pertain to Nissan NA Mobile apps, some parts of the Nissan ASIST diagnostics tool, the Dealer Business Systems and Dealer Portal, Nissan internal core mobile library, Nissan/Infiniti NCAR/ICAR services, client acquisition and retention tools, sale and market research tools and data, various marketing tools, the vehicle logistics portal and vehicle connected services.

Individual Impact: No sensitive personal or financial information was announced as part of this incident, but the investigation is ongoing.

Customers Impacted: Unknown

How it Could Affect Your Business: Keeping data safe from hackers starts with keeping data secure by using strong identity and access management tools across the board and basic security protocols like multifactor authentication.