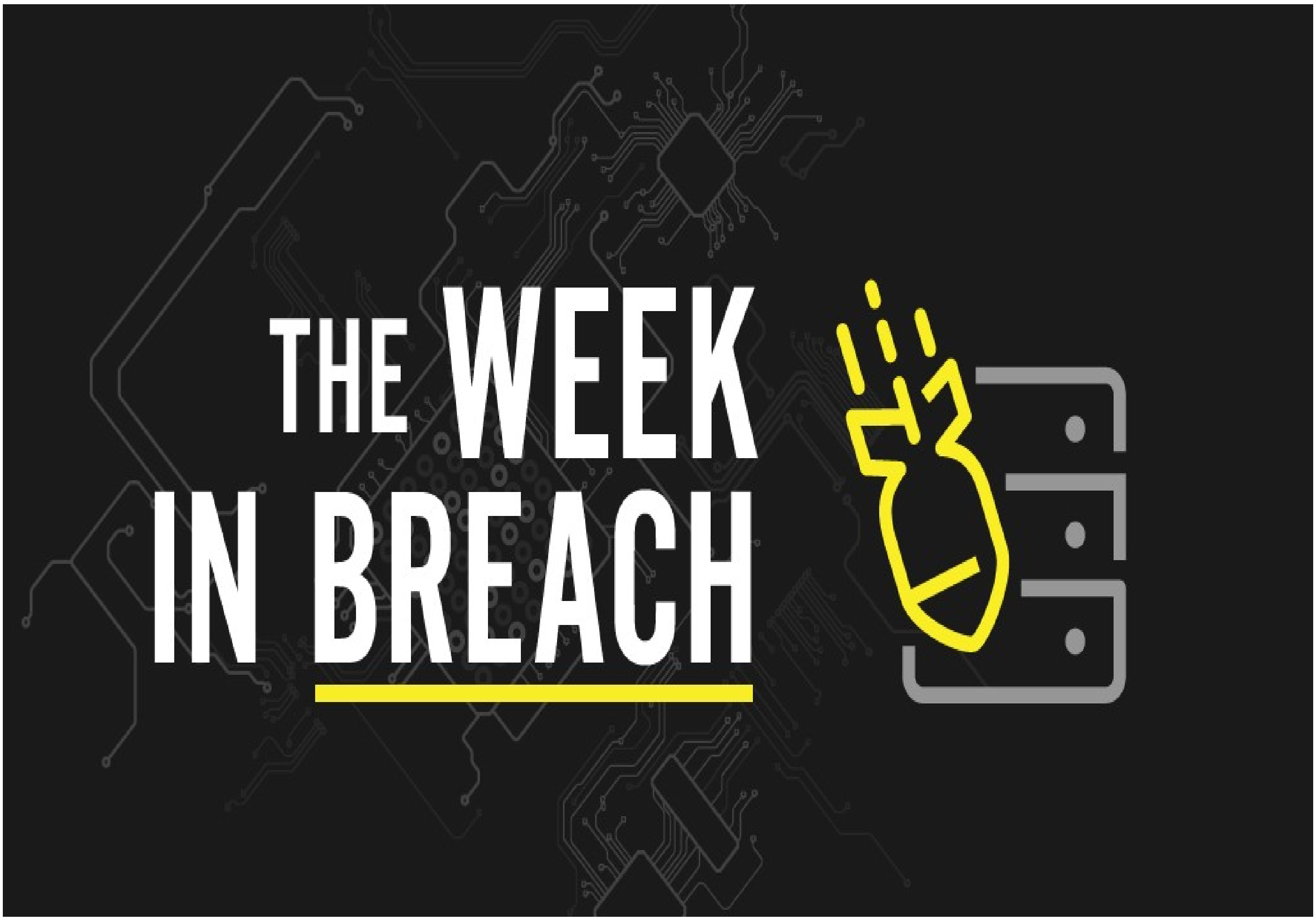
THE WEEK IN BREACH NEWS: 12/21/2022 - 12/27/2022

DenBe Computer Consulting
Connecting Business

December 28th, 2022 by Dennis Jock



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 Federal Bureau of Investigation
https://www.hackread.com/fbi-infragard-hacked-data-sold/

Exploit: Hacking

United States Federal Bureau of Investigation: Federal Government Agency

The U.S. Federal Bureau of Investigation (FBI)'s InfraGard program has experienced a data breach. The program, launched in 1996, encourages physical and cyber threat information-sharing collaborations between the public and private sector. Cybercriminals advertised a database that they purportedly snatched on the dark web containing contact details of over 87,000 members of InfraGard. Initially, the threat actors were asking for $50k for the database. However, Hackread reported that the thieves had a change of heart and decided not to sell or release the database, telling that publication that they'd decided the stolen InfraGard database would no longer be posted for sale as it would "cause more harm to everyone" than benefit for the hackers.

How It Could Affect Your Business: This kind of database is especially sensitive and its exposure could have major national security implications.

Uber
https://www.bleepingcomputer.com/news/security/uber-suffers-new-data-breach-after-attack-on-vendor-info-leaked-online/

Exploit: Supply Chain Attack

Uber: Ride Sharing & Delivery Service

Uber has suffered a new data breach. A threat actor going by the name of "UberLeaks" published a sample of data purportedly snatched from Uber and Uber Eats including employee email addresses, corporate reports and IT asset information stolen from a third-party vendor, thought to be Teqtivity, which it uses for asset management and tracking services, on its dark web leak site. The leaked data also includes files claiming to be source code associated with the mobile device management platforms (MDM) used by Uber and Uber Eats as well as their third-party vendor services. No user data appears to be involved in this breach.

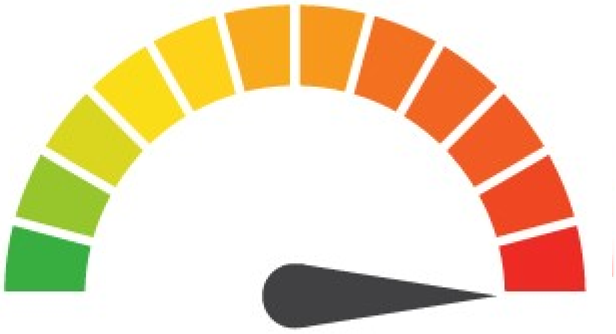
How It Could Affect Your Business: : This isn't the first data breach for Uber, further eroding customer confidence in the company's ability to keep their information safe.

The Centers for Medicare and Medicaid Services (CMS)

https://www.bankinfosecurity.com/subcontractor-breach-affects-245k-medicare-beneficiaries-a-20727

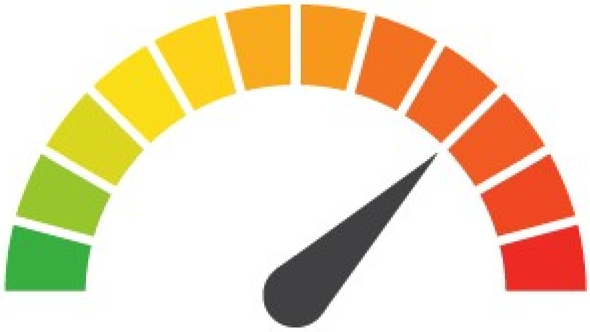
Exploit: Supply Chain Attack

The Centers for Medicare and Medicaid Services (CMS): Federal Government Agency



Risk to Business: 1.211 = Extreme

The Centers for Medicare and Medicaid Services (CMS) has experienced a data breach that impacts 245,000 Medicare beneficiaries. The agency said that the initial security incident that led to the breach was experienced by a subcontractor to another company contracted by Medicare to resolve system errors related to beneficiary entitlement and premium payment records. The subcontractor has been identified as Healthcare Management Solutions and the main contractor is ASRC Federal Data Solutions. CMS explained in its breach notification letter that its initial investigation points to the subcontractor having "acted in violation of its obligations."



Individual Risk: 1.272 = Severe

The incident may have exposed Medicare beneficiaries' sensitive data including names, birthdates, phone numbers, Medicare identifiers, banking information, such as routing and account numbers, Medicare enrollment, entitlement and premium information and Social Security numbers.

How it Could Affect Your Business: This breach can put a lot of very sensitive data at risk for vulnerable people including financial details and will almost certainly incur big regulatory fines

SevenRooms
https://www.bleepingcomputer.com/news/security/restaurant-crm-platform-sevenrooms-confirms-breach-after-data-for-sale/

Exploit: Hacking

SevenRooms: Customer Relationship Platform

Risk to Business: 1.981 = Severe

SevenRooms, a customer relationship management platform used by brands including MGM and Wolfgang Puck, has confirmed it suffered a data breach. A threat actor posted samples of data purportedly stolen from the New York-based company on a dark web forum on December 15. Bad actors claim that they've stolen a 427 GB backup database containing information about SevenRooms customers. The company was quick to reassure the public that guests' credit card information, bank account data, social security numbers, or any other similarly highly sensitive information was not stored on compromised servers or exposed in the attack. The incident is still under investigation.

How It Could Affect Your Business: Service providers of all types have been high on cybercriminals' priority lists as they search for both data and possible backdoors into companies.