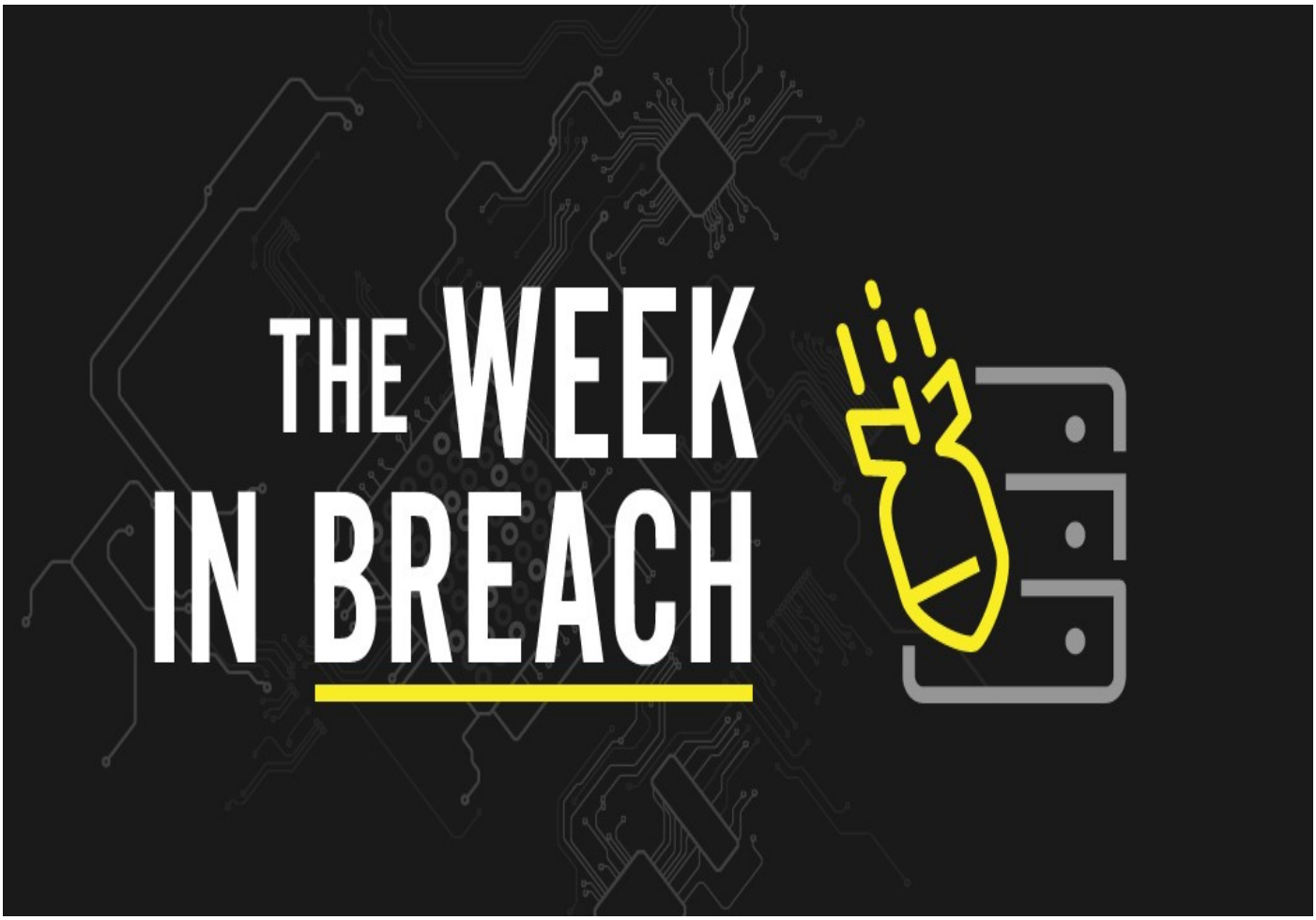
THE WEEK IN BREACH NEWS: BEST OF 2022

DenBe Computer Consulting
Connecting Business

January 4th, 2023 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***

Focus on: Supply Chain Risk

United States – FinalSite

---

https://thejournal.com/articles/2022/01/07/thousands-of-schools-affected-by-ransomware-attack-on-website-provider-finalsite.aspx

Exploit: Ransomware

Risk to Business: 1.106 = Extreme

Users of sports book platform DraftKings took a heavy hit last week with an estimated $300k lost to a credential stuffing attack. A company official confirmed the attack in a statement, saying that they believe that the incident stemmed from customers reusing login credentials that had already been compromised elsewhere. Bad actors gained access to several user accounts that they immediately took over, changing the passwords and enabling 2FA for a phone number they controlled. DraftKings has said that customers who lost money will be made whole but did not offer specifics.

How It Could Affect Your Business: This is not a good look during a busy time f year for sports betting with the World Cup ongoing and the U.S. football playoffs ahead.

Focus on: Employee Errors

United States – U.S. Internal Revenue Service (IRS)

https://news.yahoo.com/irs-inadvertently-publishes-120-000-234841222.html

Exploit: Human Error

U.S. Internal Revenue Service: Federal Government Agency

Risk to Business: 2.843 = Moderate

The Vice Society ransomware group has added Cincinnati State Technical and Community College to its dark web leak site, releasing a trove of purportedly stolen documents ranging across the past two years. The school confirmed that it had experienced a cybersecurity incident that is still under investigation in early November. While class schedules were not impacted, the school is still working to restore functionality in some of its communications systems. Financial aid services, network printing, VPN tools, department share drives, admission application platforms, transcript exchanges, grading tools and more were all still down as of last Friday. The release of the documents may indicate that the school did not pay the ransom that Vice Society demanded.

How It Could Affect Your Business: Educational institutions at every level have been hit hard by bad actors, and they're favored targets for Vice Society.

Focus on: Healthcare Cyberattacks

United States – CommonSpirit Health

https://www.cybersecuritydive.com/news/commonspirit-health-security-incident-cybersecurity-tennessee/633264/

Exploit: Ransomware

CommonSpirit Health: Healthcare System Operator

Risk to Business: 2.771 = Extreme

One of the largest healthcare systems in the US is experiencing outages impacting patient care after a suspected ransomware attack knocked some hospital systems offline. Subsidiaries of CommonSpirit have reported being affected by the attack including CHI Health facilities in Nebraska and Tennessee, Seattle-based Virginia Mason Franciscan Health providers, MercyOne Des Moines Medical Center, Houston-based St. Luke's Health and Michigan-based Trinity Health System. The company disclosed that it has rescheduled some patient procedures because of an inability to access electronic medical records or lab results. Some hospitals are using paper charts. The company says it is working to restore systems and the incident is under investigation.

How It Could Affect Your Customers' Business: Ransomware is an especially devastating prospect for a healthcare organization because it can impact patient care and even mortality rates.