THE WEEK IN BREACH NEWS: 11/04/20 – 11/10/20

DenBe Computer Consulting
Connecting Business

November 11, 2020 by Dennis Jock

This Week in Breach News: This week: Capcom discovers ransomware isn't a game, Magecart hackers strike gold from JM Bullion, and healthcare cyberattack warnings come to fruition.

The Week in Breach News: Top Threats This Week

- **Top Source Hits:** ID Theft Forum
- **Top Compromise Type:** Domain
- **Top Industry:** Finance & Insurance
- **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***

JM Bullion

https://www.bankinfosecurity.com/precious-metal-trader-jm-bullion-admits-to-data-breach-a-15294

Exploit: Skimming (Magecart)

JM Bullion: Precious Metals Dealer

Risk to Business: 1.772 = Severe

This Texas precious metals trader discovered that someone was cashing in on their clients' transactions and it wasn't them. In a recent regulatory filing, the company disclosed that malicious payment skimming code was present and active on their website from February 18, 2020, to July 17, 2020.

Individual Risk: 1.624 = Severe

The information stolen in this attack includes customers' names, addresses, and payment card information, including the account number, expiration date, and security codes. Customers should be alert to potential identity theft and spear phishing attempts.

Customers Impacted: Unknown

How it Could Affect Your Customers' Business: Failing to notice a payment card skimmer operating on your site for 6 months does not speak well to your company's commitment to keeping client data secure.

University of Vermont Medical Center

https://www.idagent.com/passly-digital-risk-protection

Exploit: Ransomware

University of Vermont Medical Center: Hospital System

Risk to Business: **1.402 = Extreme**

In the wake of recent warnings from US government agencies about increased ransomware risk for healthcare targets, University of Vermont Medical Center (UVM) has landed in that trap. A ransomware attack has led to significant, ongoing tech problems for the University of Vermont Health Network, affecting its six hospitals in Vermont and New York. The Vermont National Guard and the FBI have been working with the tech team at UVM to restore service since the attack first began affecting systems on October 30th. Damage assessment and recovery are ongoing, and some systems are still offline. The hospital says that urgent patient care was not impacted.

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

Customers Impacted: Unknown

How it Could Affect Your Customers' Business: Healthcare targets are in increasing danger from money -hungry cybercriminals who know that medical targets don't have time for a long, complex recovery procedure, but they do have money.

GrowDiaries

https://www.zdnet.com/article/configuration-snafu-exposes-passwords-for-two-million-marijuana-growers/

Exploit: Misconfiguration

Grow Diaries: Industry Blogging Platform

Risk to Business: 2.237 = Severe

Leading cannabis industry blogging platform GrowDiaries may need to clear its head after a configuration error in Kibana apps left two Elasticsearch databases unlocked and leaking data. Those open gates allowed attackers to dive into two sets of Elasticsearch databases, with one storing 1.4 million user records and the second holding more than two million user data points.

Individual Risk: 2.612 = Moderate

One open database exposed usernames, email addresses, and IP addresses for platform users, and the other exposed user articles posted on the GrowDiaries site and users' account passwords. Users should be aware of spear phishing and blackmail risks.

Customers Impacted: 1.4 million

How it Could Affect Your Customers' Business: Cyberattacks can have cascading consequences, with information stolen in cyberattacks coming back to haunt businesses months or years later. Data like login credentials can live on in Dark Web data dumps to haunt you later.

Mattel

https://www.bleepingcomputer.com/news/security/leading-toy-maker-mattel-hit-by-ransomware/

Exploit: Ransomware

Mattel: Toymaker

Risk to Business: 2.327 = Severe

In a recent regulatory filing, Mattel told regulators that it suffered a ransomware attack in July 2020 that shut down some systems but did not include a significant data loss. Only business systems were impacted, production and distribution were not affected. Experts believe that TrickBot ransomware was used in the incident.

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

Customers Impacted: Unknown

How it Could Affect Your Customers' Business: Cybersecurity awareness starts with phishing resistance. It's the most likely delivery system for ransomware, but training only sticks if it's refreshed at least every 4 months.

GEO Group

https://www.natlawreview.com/article/geo-group-hit-ransomware-attack

Exploit: Ransomware

GEO Group: Private Prison Developer

Risk to Business: 2.066 = Severe

GEO Group has begun informing impacted individuals and facilities that the Florida-based prison developer was struck by ransomware in July 2020. The company notes that some personally identifiable information and protected health information for some inmates and residents was exposed in the incident. The impacted people connected to the South Bay Correctional and Rehabilitation Facility in Florida, a youth facility in Marienville Pennsylvania, and an unnamed defunct facility in California. Employee data was also obtained in the incident.

Individual Risk: 2.221 = Severe

Residents and former residents of the impacted facilities should be alert to spear phishing, identity theft, or blackmail attempts using the stolen data. Employees of GEO group should also be on the lookout for similar activity.

Customers Impacted: Unknown

How it Could Affect Your Customers' Business: failure to stop ransomware attacks from landing on your business is a fast track to a long, messy, and expensive recovery.