THE WEEK IN BREACH NEWS: 10/28/20 – 11/03/20

DenBe Computer Consulting
Connecting Business

November 4, 2020 by Dennis Jock

This Week in Breach News: Phishing nets cybercriminals more than $2 million from the Republican Party, Google employee information is exposed in a third-party breach, healthcare targets get walloped again, data breach fines pack a punch, and should you just pay the ransom for stolen data?

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:** 1 - 10

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***

Steelcase

https://www.fox17online.com/news/steelcase-experiences-cyberattack

Exploit: Ransomware

Steelcase: Furniture Manufacturer

Risk to Business: 2.311 = Severe

Furniture manufacturing giant Steelcase was hit with a nasty ransomware attack that forced a brief shutdown of all systems. The company was able to quickly contain the suspected Ryuk ransomware incident and says that no data was stolen. Recovery operations were fast and everything is back online.

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

Customers Impacted: Unknown

How it Could Affect Your Customers' Business: These days, ransomware attacks aren't just a threat to data – they're being used to shut down production lines, impact infrastructure, and cause havoc.

Wisconsin Republican Party

https://apnews.com/article/wisconsin-republican-party-hackers-stole-641a8174e51077703888e2fa89070e12

Exploit: Phishing

Wisconsin Republican Party: Political Organization

Risk to Business: **1.337= Extreme**

The Wisconsin Republican Party had a suspected phishing incident that couldn't have come at a worse time. An estimated $2.3 million was stolen by cybercriminals from the party's reelection fund after at least one staffer interacted with a phishing email, impacting operations just as the races were coming down to the wire. The FBI and local officials are investigating 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: Phishing is about more than just credential compromise. Today's most dangerous attack is used to do everything from steal money to deploy malware.

Ledger

https://cryptobriefing.com/bitcoin-wallet-provider-ledger-compromised-again-malicious-phishing-attack/

Exploit: Unsecured Database

Ledger: Cryptocurrency Storage Platform

Risk to Business: 1.667 = Severe

Once again, Ledger is hot water for a cyberattack. This time, Ledger users received a phishing email that directed them to log in at a new address, allowing cybercriminals to steal both the victim's login credentials and cryptocurrency. This is the company's second incident this year, and information from that July 2020 incident is suspected to have played a part in this attack.

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

Customers Impacted: Unknown

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.

Fragomen, Del Rey, Bernsen & Loewy

https://techcrunch.com/2020/10/26/fragomen-data-breach-google-employees/

Exploit: Unauthorized Database Access

Fragomen, Del Rey, Bernsen & Loewy: Law Firm

Risk to Business: 2.801 = Moderate

Data theft at a top law firm that provides employment verification screening services for companies like Google exposed a small amount of sensitive data. An unauthorized intrusion into a database exposed the employment verification information for some current and past Google employees.

Individual Risk: 2.992 = Moderate

The firm has not disclosed exactly what data was stolen although an employment verification or I-9 file can contain very sensitive information. The firm has also not indicated how many employees were affected although they've stated that it is a "limited number".

Customers Impacted: Unknown

How it Could Affect Your Customers' Business: When you're storing sensitive data, that information needs extra protection in order to really serve your clients.

Nitro Software Inc.

https://securityaffairs.co/wordpress/110025/data-breach/nitro-pdf-data-breach.html

Exploit: Unauthorized Database Access

Nitro Software Inc.: Software Developer

Risk to Business: 2.071 = Severe

A massive data breach at Nitro, home of Nitro PDF, may have an impact on some major players. Nitro serves clients including Google, Apple, Microsoft, Chase, and Citibank. The software maker announced that an unauthorized third party gained limited access to a company database. The stolen information has already made its debut on the Dark Web, including about 1TB of documents.

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

Customers Impacted: Unknown

How it Could Affect Your Customers' Business: A data breach at a third-party service provider for your business is just as dangerous as a data breach at your company and smart companies take precautions against supply chain risk.

Gaming Partners International

https://www.forbes.com/sites/leemathews/2020/10/31/ransomware-gang-claims-international-casino-equipment–supplier-as-latest-victim/?sh=7529ed2c68b2

Exploit: Ransomware

Gaming Partners International: Casino Equipment Provider

Risk to Business: 2.211 = Severe

REvil ransomware caused havoc at one of the world's leading casino suppliers, shutting down systems for several days. The hackers also extracted more than 500 gigabytes of data during the breach. Among the files were casino contracts, banking information and technical documents. The company was quickly able to restore operations.

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

Customers Impacted: Unknown

How it Could Affect Your Customers' Business: Every time your employees interact with a phishing email, your business is at risk for ransomware. Security awareness training prevents up to 70% of cybersecurity incidents.