THE WEEK IN BREACH NEWS: 10/14/20 – 10/20/20

DenBe Computer Consulting
Connecting Business

October 21, 2020 by Dennis Jock

This Week in Breach News: Mystery cyberattacks do massive damage to Barnes & Noble, Robinhood, and the Hackney Borough Council, Dickie's Barbecue gets served some skimming trouble, and ransomware puts a beloved Indian snack food brand in danger – plus a deep dive into the Dark Web to jumpstart your 2021 planning.

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:** 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***

Barnes & Noble

https://boston.cbslocal.com/2020/10/15/barnes-noble-cyberattack-hack-data-breach-personal-info/

Exploit: Malware

Barnes & Noble: Bookseller

Risk to Business: 1.411 = Extreme

Barnes & Noble has been starring in its own horror story in the last week, as a massive network outage for its Nook customers rolled into the discovery of a massive cyberattack. The bookseller informed customers on Monday that it had experienced a data breach that exposed customers' transaction histories and PII. Recovery and restoration efforts are underway. It's unknown if the Nook outage was a facet of the data breach or unrelated.

Individual Risk: 2.206 = Severe

Barnes & Noble says that the only data stolen was transaction history information, names, and email addresses. The company doesn't anticipate that any financial information was stolen, but the investigation is ongoing.

Customers Impacted: Unknown

How it Could Affect Your Customers' Business: No one can afford a data breach right now, not even a corporate giant. incidents that impact online sales are especially problematic as online sales remain a focus area during the pandemic.

Intcomex

https://channeldailynews.com/news/miami-based-channel-partner-slammed-by-1tb-customer-and-business-data-leak/72273

Exploit: Ransomware

Intcomex: Managed Services Provider

Risk to Business: 1.772 = Severe

The Miami-based managed services provider suffered a huge data breach, exposing nearly 1Tb of very sensitive data. The leaked data contains a collection called "Internal Audit" at 16.6GB, and "Finance_ER" totaling 18GB. The most recent data was from July 2020. The data included credit cards, license scans, payroll, customer databases, and more. The company serves more than 50,000 resellers in over 41 countries.

Individual Risk: No individual information was reported as compromised in this incident, although the potential is there. No details about the uncovered data are available.

Customers Impacted: up to 50,000

How it Could Affect Your Customers' Business: Third party data breaches are a big risk to every business these days. Even if you're keeping your company's sensitive data secure, your vendors might not be.

Robinhood

https://nypost.com/2020/10/16/hackers-broke-into-nearly-2000-robinhood-trading-accounts/

Exploit: Hacking/Database Intrusion

Robinhood: Investment App

Risk to Business: 1.552 = Extreme

Robinhood informed its users last week that hackers had obtained access to funds and information in some of its accounts. The firm claims that there was no intrusion and that customer email addresses were compromised outside of the app, giving cybercriminals the ability to steal money and data, but investigators and clients say that's not possible, citing the fact that most accounts were protected with MFA.

Individual Risk: 1.412 = Extreme

Personal and financial information about users was accessible and potentially stolen by hackers, and some users had money stolen directly from their accounts. Users should assume that their accounts have been compromised and act accordingly.

Customers Impacted: 2,000

How it Could Affect Your Customers' Business: Providing services that use highly sensitive information implies that you're using the best technology to keep that data safe – especially at a fintech startup.

Dickie's Barbecue Pit

https://www.zdnet.com/article/card-details-for-3-million-dickeys-customers-posted-on-carding-forum/

Exploit: Malware/Skimming

Dickie's Barbecue Pit: Restaurant Chain

Risk to Business: 1.691 = Severe

Dickie's Barbecue Pit has been serving up a side of skimming to every customer. Between August 2019 and July 2020, cybercriminals were operating skimmers at 156 of Dickey's 469 locations in 30 states, with the highest exposure in California and Arizona. The breach was discovered by cybersecurity monitors after hackers began advertising the data stash for sale as "Blazingsun".

Individual Risk: 1.771 = Severe

Customers who made purchases at Dickie's Barbecue Pit during that window have likely experienced a credit card compromise and should contact their card issuer for guidance.

Customers Impacted: 3 million

How it Could Affect Your Customers' Business: The number one cause of a data breach is human error. Failing to keep up with security awareness and phishing resistance training leads to expensive cybersecurity disasters.

Nez Pierce Tribal Casinos

https://lmtribune.com/external-cyber-attack-blamed-for-computer-trouble-at-nez-perce-tribes-casinos/article_091b0264-1000-11eb-a3ed-0f2500bec470.html

Exploit: Ransomware

Nez Pierce Tribal Casinos: Gambling Parlors

Risk to Business: **2.002 = Severe**

Two popular casinos owned and operated by the Nez Peirce Native American tribe were hit with ransomware, resulting in a complete shutdown for at least a week. Systems were frozen at both the tribe's Clearwater River Casino near Lewiston and the Ye-Ye Casino at Kamiah in Idaho. Restoration efforts and investigations are underway, but the casinos are expected to reopen imminently.

Individual Risk: No personal data has been reported as impacted in this incident.

Customers Impacted: Unknown

How it Could Affect Your Customers' Business: Attacks aren't always about stealing data. Ransomware is a devastating weapon that bad actors are using to shut down businesses too., and that can sometimes be even worse.