THE WEEK IN BREACH NEWS: 01/20/21 – 01/26/21

DenBe Computer Consulting
Connecting Business

January 27, 2021 by Dennis Jock

This Week in Breach News: ShinyHunters work overtime at multiple targets including Pixlr, data theft puts a star talent agency in the spotlight,

---

The Week in Breach News: Top Threats This Week

- **Top Source Hits:** ID Theft Forum
- **Top Compromise Type:** Domain
- **Top Industry:** Health & Medical 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***

Teespring

https://cybernews.com/security/8-million-teespring-user-records-leaked-on-hacker-forum/

Exploit: Hacking

Teespring: eCommerce Platform

Risk to Business: 2.129 = Severe

Hackers have dropped a huge trove of user and creator data allegedly from Teespring, an e-commerce platform that specializes in enabling designers to market their wares. The two massive files of stolen data include email addresses and last update dates for 8,242,000 user accounts.

Individual Risk: 1.221 = Extreme

The info dump contains 4,000,000+ user records, including usernames, full names, locations, phone numbers, Creator IDs, referral information, trust score, whitelisted seller campaigns, storefronts, bank check payouts, and other analytics data. This data could be used to conduct business email compromise attacks and spear phishing attempts.

Customers Impacted: 8,242,000

How it Could Affect Your Business: Data like this is sought-after by cybercriminals and often hangs around for years on the Dark Web, acting as fuel for future cybercrime.

Circuit Court of Cook County

https://www.securityweek.com/illinois-court-exposes-more-323000-sensitive-records

Exploit: Unsecured Server

Circuit Court of Cook County: Municipal Court System

Risk to Business: 1.775 = Severe

An unsecured Elasticsearch server is the cause of a huge data exposure containing more than 323,277 Cook County court-related records. Researchers estimate that the database may have belonged to a specialist Cook County department of caseworkers working with people who needed additional help.

Individual Risk: 1.612 = Severe

The records contained PII such as full names, home addresses, email addresses, and court case numbers and notes on the status of both the case and the individuals concerned. Criminal, family and immigration cases are in the mix. This data could be used to mount an array of attacks like blackmail, identity theft and spear phishing attempts.

Customers Impacted: Unknown

How it Could Affect Your Business: Failing to take a simple step to secure a server that contains sensitive information doesn't speak well to an organization's commitment to cybersecurity.

MeetMindful

https://www.zdnet.com/article/sonicwall-says-it-was-hacked-using-zero-days-in-its-own-products/

Exploit: Hacking

MeetMindful: Dating Site

Risk to Business: 1.979 = Severe

Details of an estimated 2.28 million users of dating site MeetMindful was just released online in the latest in a series of stolen data dumps by cybercrime gang ShinyHunters. There's no clear origin of the data, but researchers expect that it may have come from an unsecured AWS S3 bucket

Individual Risk: 1.779 = Severe

The dumped data includes users' real names, email addresses, address information, physical descriptions, dating preferences, marital status, birth data, location data, IP addresses, Bcrypt-hashed passwords, Facebook user IDs and Facebook authentication tokens. This information puts users at risk for spear phishing attacks.

Customers Impacted: 2.28 million

How it Could Affect Your Business: Keeping data safe from hackers starts with keeping data secure using strong access point controls and basic security protocols like multifactor authentication.

Bonobos

https://www.bleepingcomputer.com/news/security/bonobos-clothing-store-suffers-a-data-breach-hacker-leaks-70gb-database/

Exploit: Hacking

Bonobos: Menswear Retailer

Risk to Business: 1.979 = Severe

Men's clothier Bonobos has experienced a huge 70GB data breach exposing millions of customers' personal information after a cloud backup of their database was snatched. ShinyHunters, who had a very busy week, posted the full Bonobos database to a free hacker forum. ShinyHunters was kind enough to transform the stolen password data into a handy list for credential stuffing.

Individual Risk: 2.006 = Severe

The leaked data included customers' addresses, phone numbers, partial credit card numbers (last four digits), order information and password histories. This information can be used in many cyberattacks including spear phishing and credential stuffing.

Customers Impacted: 7 million

How it Could Affect Your Business: Data theft is an increasingly worrisome problem for everyone. Not only is the original business impacted, the addition of such large troves of information to the Dark Web fuels further cybercrime.