Issued 3/16/17

Dun & Bradstreet Database Breached, 33.6M Files Vulnerable

A Dun & Bradstreet 52GB database containing about 33.6 million records with very specific details about each of the people involved from job title to email address has been exposed.

The database was sent to independent cyber researcher Troy Hunt who found the records contained not only dozens of specific details on each person, but is organized in a way indicating the content was not pulled haphazardly from a corporation during a hack, but was instead properly curated and ready for distribution to a customer. ZD Net was able to confirm that the content belonged to NetProspex, a company Dun & Bradstreet purchased in 2015 and is used by marketers looking to sell directly to specific types of people.

Although Dun & Bradstreet is investigating the incident, it is not known at this time how it was exfiltrated, ZD Net reported. Dun & Bradstreet told SC Media in a statement that, "Based on our analysis, it is our determination that there has been no exposure of sensitive personal information from, and no infiltration of our system. The information in question is data typically found on a business card. As general practice, Dun & Bradstreet uses an agile security process and evaluates and evolves security controls to protect the integrity of our data."

Hunt said the files are from a wide spectrum of government and private entities. The Department of Defense is most heavily represented with 101,013 files includes, followed by the U.S. Postal Service, ATT&T and Wal-Mart. The data points are very specific about each individual. Stating the person is a “soldier” with the position “ammunition specialist”, Hunt said. “We've been bombarded by news of state sponsored hacking recently and frankly, if I was a foreign power with a deep interest in infiltrating US military operations, I'd be very interested in a nicely curated list pointing me directly to hundreds of intelligence analysts,” Hunt wrote.

Taking another view on the data loss was Brian Vecci, tech evangelist at Varonis, who noted that with all of the other breaches that have taken place over the last several years it's likely this data is already public.