LexisNexis, Dunn & Bradstreet, Kroll

CYBERTRUTH (//WWW.USATODAY.COM/BLOG/CYBERTRUTH/) Byron Acohido, USA TODAY

Published 4:57 p.m. ET Sept. 26, 2013 | **Updated 6:23 p.m. ET Sept. 26, 2013**

(Photo: USA TODAY)

Three major U.S. data brokerages -- companies that amass and sell sensitive data -- have been hit by a hacking group that specializes in selling stolen social security numbers.

The breaches at LexisNexis, Dun & Bradstreet and Kroll Background America were disclosed by cybersecurity blogger Brian Krebs on KrebsOnSecurity. (http://krebsonsecurity.com/2013/09/data-broker-giants-hacked-by-id-theft-service/)

Krebs reports that a cybercrime ring associated with the cyberunderground website ssndob.ms is responsible. SSNDOB stands for social security number date of birth.

It should come as no surprise that data thieves target data brokers. These companies make big profits by systematically assembling names, addresses, property records and vital statistics. After tapping free public sources for such data, data brokers turn around and sell the data to employers, lawyers, realtors, police, even jealous spouses.

Background: How data brokers' practices spawned data loss disclosure laws (http://usatoday30.usatoday.com/tech/news/computersecurity/infotheft/2007-04-01-choicepoint_N.htm)

An FBI spokeswoman told the Reuters news service that it was investigating but did not elaborate. Krebs reports that the gang snuck malicious software onto servers at LexisNexis as early as April 2013.

Gary Alterson, senior director of Risk and Advisory Services at risk management consultancy Neohapsis, said it is common for large organizations to fail to detect network intruders for months at a time.

"Most security diligence isn't actually that diligent – they're compliance based," Alterson says. "Typically, companies answer a questionnaire or get interviewed. There's no in-depth assessment of the actual effectiveness of security controls which, at the end of the day, is what matters."

Pat Peterson, CEO of messaging security firm Agari, says the cybercriminals most likely stole terabytes of data from D&B, LexisNexis and Kroll Background America, a division of Altegrity.

The SSNDOB gang , Peterson says, is most interested in selling social security numbers, birthdays, mother's maiden names, and similar data to other criminals who specialize in various forms of identity theft.

The gang also likely will sell other miscellaneous data stolen from the data brokers to anyone willing to make a bid. Those include criminals who specialize in targeted attacks that leverage knowledge about a specific victim's acquaintances and preferences.

"While we don't yet know whose data has been compromised, millions of Americans are now at risk as the criminals knit the stolen data together with their attacks to go after identity theft and bank accounts," Peterson says."Think of it as stealing a car and selling the parts. They will find someone to purchase this data. We're talking about names of spouses, children and other family members; information on where they went to school, their hometowns, etc. "

Andreas Baumhof, chief technology officer at ThreatMetrix, observes that breaches on companies that amass sensitive data have become commonplace.

"There are two types of companies. Those that have been hacked and know it and those that have been hacked and don't know it," Baumhof says.

Too many companies still concern themselves with security as an after-thought, he says.

"I know so many chief information security officers who are fighting to get a budget to do the right thing, but it's hard to justify a budget if you haven't had a breach," Baumhof says.

Read or Share this story: http://usat.ly/1asJIU9