

It's Time to Pretend We're Shocked by Yet Another Voter File Data Breach | Gizmodo

By Dell Cameron

July 20, 2018

A security researcher has, yet again, discovered thousands of U.S. voter files with a minimal amount of effort. Given that over the past year virtually [every registered U.S. voter](#) has been [exposed](#) by one [data breach](#) or [another](#), it's becoming increasingly difficult to feign our surprise.

According to the researcher, Kromtech Security's Bob Dianchenko, the files were available online for virtually anyone to download and had long been indexed by [GreyhatWarfare](#), a website that currently lists more than 48,000 Amazon S3 buckets, in which potentially confidential files can be found.

Dianchenko linked the Amazon server containing the voter files to Robocent, a Virginia-based political campaign and robocalling company. More than 2,600 files were exposed, including voter file spreadsheets and audio recordings for several political campaigns. The voter data itself contained names, phones numbers, addresses, political affiliations, age and year of birth, gender, voting district, and other demographic information, such as language and ethnicity.

Source: [It's Time to Pretend We're Shocked by Yet Another Voter File Data Breach | Gizmodo](#)