Election fraud feared as Google and hackers target voter records

By Cory Bennett -

A series of data breaches overseas are spurring concerns that hackers could manipulate elections in the United States.

Since December, hundreds of millions of voters in the U.S., the Philippines, Turkey and Mexico have had their data discovered on the web in unprotected form. In some instances, legitimate security researchers found the information, but in others, malicious hackers are suspected of pilfering the data for criminal purposes.

The data breaches are raising questions as the U.S. considers whether to move toward electronic balloting. More people than ever are using the internet to register to vote and to request mail-in ballots. Some states have even become vote-by-mail only in recent years.

“If you can’t keep the voter registration records safe, what makes you think you can keep the votes safe?” asked Pamela Smith, president of election watchdog Verified Voting.

For a politically inclined hacker, insecure voter data could “very easily” create a pathway to “massive” voter fraud, said Joseph Kiniry, CEO of Free & Fair, which advocates for secure digital election systems.

“If you can go in there and delete rows based on someone’s name or political affiliation, we will have a massively screwed up election process on the day,” he said.

In the U.S., experts say there are few clear standards for locking down voter registration data and hackers have caught on to this fact. Andrew Komarov, chief intelligence officer at identity protection firm InfoArmor, said fraudsters are targeting electoral records at an unprecedented clip.

“They’re looking for something fresh and new they can trade in underground [markets],” he said.

A gargantuan amount of voter data is now for sale, much of it posted in the last six months. In some countries, such as the Philippines and Mexico, every single registered voter has been caught up in voter registration breaches.

In the U.S., an independent security researcher in December said he discovered a database containing 191 million American voters’ information. The dataset — which included names, addresses, birth dates, party affiliations, phone numbers and emails — spanned all 50 states and the District of Columbia.

These details are valuable to cyber criminals, who can bundle the information in batches of 5 to 10 million and flip it on the dark web for between three and five bitcoins a set — or roughly $1,350 to $2,250 — according to Komarov, who tracks such sales.

That's not a ton of money — far less than medical records command, for example — but voter data is easy to obtain. The hackers are taking advantage of disparate and lacking security standards guarding voter registration databases, specialists say.

Congress in 2002 passed the Help America Vote Act, which directed each state to create a computerized statewide voter registration database. The move has many tangible benefits. Registering online enfranchises more people, is more accurate and saves the government money.

But robust digital security guidelines — which are often determined on a state-by-state basis — were not well established when the systems were being developed. Local electoral authorities often didn't have the technical know-how to properly protect the data, and numerous third-party vendors were not held to a high enough standard, several researchers concluded.

U.S. officials also don't always classify electoral records as sensitive data, Kiniry said. In some states, voter registration information is public record. That means federal security standards required for so-called "personally identifiable information" don't necessarily apply to voter records.

But any time several pieces of publicly available data are collected in one location, the dataset becomes desirable to hackers. The more personal details a fraudster has, the easier it is to conduct identity theft.

"It's time to treat such [voter] information as high-security government information," said David Maman, a cloud security expert with database security firm HexaTier.

Until that time comes, identity thieves will likely focus on voter records. The breaches in the past six months are "orders of magnitude larger than anything we've seen previously," Kiniry said.

The sheer scale of the attacks, with hundreds of millions of electoral records exposed, has also brought attention to the vulnerability of the data, a prospect that worries fair voting advocates.

"If you can impersonate a person, you can request a ballot, you could submit changes to a system," said Smith, of Verified Voting. "And that could affect whether a voter gets a ballot or not."

The amount of information in the databases raises the possibility of meddling in elections on a large scale, Kiniry said.

"In the USA, the concern I hold is if our registration systems are easily manipulated, we're not going to see breaches, were going to see voter ID manipulation remotely," he said, meaning hackers could be "removing people who should be there."

"That can have as big an impact on an election as anything else," Kiniry added.

For now, the threat is speculative. But the U.S. not yet had an election in the wake of these massive breaches that revealed the inherent insecurity of voter data.

"This election is going to be very exciting, shall we say," Kiniry said.