



Issued 12/18/17

19 Million California Voter Records Hacked, Held In Bitcoin Ransom

Personal information of at least 19 million California registered voters — pretty much every voter in the state — ended up in the hands of hackers who apparently held it for ransom payable in Bitcoin earlier this year, researchers at a German digital security firm reported Friday. The Secretary of State of California “was aware of the leak” and that it was “looking into it.”

Cyber criminals appeared to have accessed the data of 19,264,123 California registered voters. The type of information stolen included each person’s full name, home address, emails, phone number, gender, date of birth and precinct information. The data was apparently held at ransom for 0.2 Bitcoin, which was valued Friday at roughly \$3,500. Kromtech researchers discovered the breach in early December, it said on its blog post, but the data appear to have been taken some time earlier this year. The exact time frame when the data was taken remains unclear but Kromtech researchers say the “extract date” was 31 MAY.

Unlike the typical targeted breach by hackers, this data appear to have been part of the more than 32,000 MongoDB databases left exposed due to a vulnerability in January. Databases containing California voter information may have belonged to a third party, such as a political action committee or a campaign.

It remains unclear who exactly is behind this breach, but Kromtech identified a hacker group called Harak1r1 as a potential suspect in a mass breach of MongoDB databases. A second group, own3d, was also identified as another suspect.