Report: Ransomware disables Georgia county election database

AP apnews.com/article/virus-outbreak-elections-georgia-voting-2020-voting-c191f128b36d1c0334c9d0b173daa18c

April 20, 2021

By FRANK BAJAKOctober 23, 2020 GMT

A ransomware attack that hobbled a Georgia county government in early October reportedly disabled a database used to verify voter signatures in the authentication of absentee ballots.

It is the first reported case of a ransomware attack affecting an election-related system in the 2020 cycle. Federal officials and cybersecurity experts are especially concerned that ransomware attacks — even ones that don't intentionally target election infrastructure — could disrupt voting and damage confidence in the integrity of the Nov. 3 election.

The Oct. 7 attack on Hall County, in the northern part of the state, hit critical systems and interrupted phone services, the county said in a statement posted on its website. County spokeswoman Katie Crumley did not return multiple requests for comment from The Associated Press.

But according to a report in the Gainesville Times, the attack also disabled the county's voter signature database. Crumley was also quoted in an online CNN story saying that the attack affected both the signature database and a voting precinct map.

Ransomware scrambles affected computer networks with encryption that can only be unlocked with keys provided once the victim has paid up. Deloitte analyst Srini Subramanian said ransoms local governments pay in such cases average about $400,000.

An update Thursday evening on the county website said "the voting process for citizens has not been impacted by the attack." However, a county official quoted by the Times said signature verification was slowed because employees had to manually pull hard copies of voter registration cards in many cases. The official was quoted as saying that most voter signatures could still be verified using a state database unaffected by the attack. The county has 129,000 registered voters.

In most states, signatures are used to validate absentee ballots sent by mail. Written on the envelopes that sheath the ballots, they are matched by election workers against signatures on file with state and local election authorities.

Federal officials recently announced that Russian hackers have infiltrated dozens of state and local government networks and could be poised to launch disruptive attacks.

An international ransomware syndicate known as Doppelpaymer appears to be involved in the Hall County attack. It posted documents purportedly stolen from Hall County on a dark web site as proof of responsibility.

Crumley, the county spokeswoman, did not respond to an email asking how much ransom that attackers had demanded and whether the county had paid a ransom.

Brett Callow, a threat analyst at Emsisoft cybersecurity firm, said the attack could augur other similar actions exploiting the proximity of Election Day.

"The real question is how many local government networks are already compromised? Threat actors frequently delay deploying ransomware on compromised networks until what they consider to be the most opportune moment — and that may well be in the days immediately prior to the election," he said. "What better time to extort money from a government by holding its systems hostage than when those systems are most needed?"

A worsening ransomware plague is afflicting U.S. cities, counties and school districts, exacerbated by the COVID-19 pandemic.

At least 82 government bodies in the U.S. have been hit by ransomware so far this year. Eighteen of those incidents have occurred since the beginning of September, according to Emsisoft.