



FBI says foreign hackers penetrated state election systems



Michael Isikoff, Chief Investigative Correspondent

August 29, 2016

The FBI has uncovered evidence that foreign hackers penetrated two state election databases in recent weeks, prompting the bureau to warn election officials across the country to take new steps to enhance the security of their computer systems, according to federal and state law enforcement officials.

The FBI warning, contained in a “flash” alert from the FBI’s Cyber Division, a copy of which was obtained by Yahoo News, comes amid heightened concerns among U.S. intelligence officials about the possibility of cyberintrusions, potentially by Russian state-sponsored hackers, aimed at disrupting the November elections.

Those concerns prompted Homeland Security Secretary Jeh Johnson to convene a conference call with state election officials on Aug. 15, in which he offered his department’s help to make state voting systems more secure, including providing federal cybersecurity experts to scan for vulnerabilities, according to a “readout” of the call released by the department.

Johnson emphasized in the call that Homeland Security was not aware of “specific or credible cybersecurity threats” to the election, officials said. But three days after that call, the FBI Cyber Division issued a potentially more disturbing warning, titled “Targeting Activity Against State Board of Election Systems.” The alert, labeled as restricted for “NEED TO KNOW recipients,” disclosed that the bureau was investigating cyberintrusions against two state election websites this summer, including one that resulted in the “exfiltration,” or theft, of

voter registration data. “It was an eye opener,” a senior law enforcement official said of the bureau’s discovery of the intrusions. “We believe it’s kind of serious, and we’re investigating.”

The bulletin does not identify the states in question, but sources familiar with the document say it refers to the targeting by suspected foreign hackers of voter registration databases in Arizona and Illinois. In the Illinois case, officials were forced to shut down the state’s voter registration system for 10 days in late July, after the hackers managed to download personal data on up to 200,000 state voters, Ken Menzel, the general counsel of the Illinois Board of Elections, said in an interview. The Arizona attack was more limited, involving malicious software that was introduced into its voter registration system but no successful exfiltration of data, a state official said.

The FBI bulletin listed eight separate IP addresses that were the sources of the two attacks and suggested that the attacks may have been linked, noting that one of the IP addresses was used in both intrusions. The bulletin implied that the bureau was looking for any signs that the attacks may have attempted to target even more than the two states. “The FBI is requesting that states contact their Board of Elections and determine if any similar activity to their logs, both inbound and outbound, has been detected,” the alert reads. “Attempts should not be made to touch or ping the IP addresses directly.”

“This is a big deal,” said Rich Barger, chief intelligence officer for ThreatConnect, a cybersecurity firm, who reviewed the FBI alert at the request of Yahoo News. “Two state election boards have been popped, and data has been taken. This certainly should be concerning to the common American voter.”

Barger noted that one of the IP addresses listed in the FBI alert has surfaced before in Russian criminal underground hacker forums. He also said the method of attack on one of the state election systems — including the types of tools used by the hackers to scan for vulnerabilities and exploit them — appears to resemble methods used in other suspected Russian state-sponsored cyberattacks, including one just this month on the World Anti-Doping Agency.

The FBI did not respond to detailed questions about the alert, saying in a statement only that such bulletins are provided “to help systems administrators guard against the actions of persistent cyber criminals.” Menzel, the Illinois election official, said that in a recent briefing, FBI agents confirmed to him that the perpetrators were believed to be foreign hackers, although they were not identified by country. He said he was told that the bureau was looking at a “possible link” to the recent highly publicized attack on the Democratic National Committee and other political organizations, which U.S. officials suspect was perpetrated by Russian government hackers. But he said agents told him they had reached no conclusions, and other experts say the hackers could also have been common cybercriminals hoping to steal personal data on state voters for fraudulent purposes, such as obtaining bogus tax refunds.

Still, the FBI warning seems likely to ramp up pressure on the Department of Homeland Security to formally designate state election systems as part of the nation’s “critical infrastructure” requiring federal protection — a key step, advocates say, in forestalling the possibility of foreign government meddling in the election.

Such a formal designation, which would allow state election officials to request federal assistance to protect their voting systems, “is under consideration,” a Homeland Security spokesman told Yahoo News.

Federal and state election officials say that the prospect of a full-blown cyberattack that seriously disrupts the November elections is remote, but not out of the question. About 40 states use optical-scan electronic-voting machines, allowing voters to fill out their choices on paper. The results are tabulated by computers.

These are “reasonably safe” because the voting machines are backed up by paper ballots that can be checked, says Andrew W. Appel, a Princeton University computer science professor who has studied election security. But six states and parts of four others (including large swaths of Pennsylvania, a crucial swing state in this year’s race) are more vulnerable because they rely on paperless touchscreen voting, known as DREs or Direct-Recording Electronic voting machines, for which there are no paper ballot backups.

“Then whatever numbers the voting computer says at the close of the polls are completely under the control of the computer program in there,” Appel wrote in a recent blog post titled “Security Against Election Hacking.” “If the computer is hacked, then the hacker gets to decide what numbers are reported. ... All DRE (paperless touchscreen) voting computers are susceptible to this kind of hacking. This is our biggest problem.” Another area of concern cited by Appel and other experts is the growing number of states that allow overseas and military voters to cast their ballots online.

In his conference call this month with state election officials, Johnson urged them to guard against potential intrusions by taking basic precautionary steps, such as ensuring that electronic voting machines are not connected to the Internet while voting is taking place. The FBI bulletin addresses additional potential threats, such as the targeting of state voter registration databases comparable to the attacks in Arizona and Illinois. “This is a wake-up call for other states to look at their systems,” said Tom Hicks, chairman of the federal Election Assistance Commission, an agency created by Congress after the 2000 Florida recount to protect the integrity of elections and which helped distribute the FBI alert to state election officials last week.

Hackers could conceivably use intrusions into voter registration databases to delete names from voter registration lists, although in most states, voters can request provisional ballots at the polls, allowing time for discrepancies to be resolved, an official of the National Association of Secretaries of State told Yahoo News. Still, according to Barger, the cybersecurity expert, such attacks can be used to create havoc and sow doubt over the election results.

As a result, the FBI alert urges state officials to take additional steps to secure their systems, including conducting “vulnerability scans” of their databases. In addition, the bulletin urges officials to sharply restrict access to their databases. “Implement the principle of least privilege for database accounts,” the FBI alert reads. It adds that “any given user should have access to only the bare minimum set of resources required to perform business tasks.”

<https://www.yahoo.com/news/fbi-says-foreign-hackers-penetrated-00000175.html>

FBI Flash PDF: Targeting Activity Against State Board of Election Systems:
https://s.yimg.com/dh/ap/politics/images/boe_flash_aug_2016_final.pdf