The Washington Post

National Security

Russian hackers targeted Arizona election system

By Ellen Nakashima August 29, 2016

Hackers targeted voter registration systems in Illinois and Arizona, and the FBI alerted Arizona officials in June that Russians were behind the assault on the election system in that state.

The bureau described the threat as “credible” and significant, “an eight on a scale of one to 10,” Matt Roberts, a spokesman for Arizona Secretary of State Michele Reagan (R), said Monday. As a result, Reagan shut down the state’s voter registration system for nearly a week.

It turned out that the hackers had not compromised the state system or even any county system. They had, however, stolen the username and password of a single election official in Gila County.

Roberts said FBI investigators did not specify whether the hackers were criminals or employed by the Russian government. Bureau officials on Monday declined to comment, except to say that they routinely advise private industry of cyberthreats detected in investigations.

The Arizona incident is the latest indication of Russian interest in U.S. elections and party operations, and it follows the discovery of a high-profile penetration into Democratic National Committee computers. That hack produced embarrassing emails that led to the resignation of DNC Chairwoman Debbie Wasserman Schultz and sowed dissension on the eve of Hillary Clinton’s nomination as the party’s presidential candidate.

The Russian campaign is also sparking intense anxiety about the security of this year’s elections. Earlier this month, the FBI warned state officials to be on the lookout for intrusions into their election systems. The “flash” alert, which was first reported by Yahoo News, said investigators had detected attempts to penetrate election systems in several states and listed Internet protocol addresses and other technical fingerprints associated with the hacks.

In addition to Arizona, Illinois officials discovered an intrusion into their election system in July. Although the hackers did not alter any data, the intrusion marks the first successful compromise of a state voter registration database, federal officials said.

“This was a highly sophisticated attack most likely from a foreign (international) entity,” said Kyle Thomas, director of voting and registration systems for the Illinois State Board of Elections, in a message that was sent to all election authorities in the state.

The Illinois hackers were able to retrieve voter records, but the number accessed was “a fairly small percentage of the total,” said Ken Menzel, general counsel for the Illinois election board.

State officials alerted the FBI, he said, and the Department of Homeland Security also was involved. The intrusion in Illinois led to a week-long shutdown of the voter registration system.

The FBI has told Illinois officials that it is looking at foreign government agencies and criminal hackers as potential culprits, Menzel said.

At least two other states are looking into possible breaches, officials said. Meanwhile, states across the nation are scrambling to ensure that their systems are secure.

Until now, countries such as Russia and China have shown little interest in voting systems in the United States. But experts said that if a foreign government gained the ability to tamper with voter data — for instance by deleting registration records — such a hack could cast doubt on the legitimacy of U.S. elections.

“I’m less concerned about the attackers getting access to and downloading the information. I’m more concerned about the information being altered, modified or deleted. That’s where the real potential is for any sort of meddling in the election,” said Brian Calkin, vice president of operations for the Center for Internet Security, which operates the MS-ISAC, a multistate - information-sharing center that helps government agencies combat cyberthreats and works closely with federal law enforcement.

James R. Clapper Jr., the director of national intelligence, has told Congress that manipulation or deletion of data is the next big cyberthreat — “the next push on the envelope.”

Tom Hicks, chairman of the federal Election Assistance Commission, an agency set up by Congress after the 2000 Florida recount to maintain election integrity, said he is confident that states have sufficient safeguards in place to ward off attempts to manipulate data.

For example, if a voter’s name were deleted and did not show up on the precinct list, the individual could still cast a provisional ballot, Hicks said. Once the voter’s status was confirmed, the ballot would be counted.

Hicks also said the actual systems used to cast votes "are not hooked up to the Internet" and so "there's not going to be any manipulation of data." However, more than 30 states have some provisions for online voting, primarily for voters living overseas or serving in the military.

This spring, a DHS official cautioned that online voting is not yet secure.

"We believe that online voting, especially online voting in large scale, introduces great risk into the election system by threatening voters' expectations of confidentiality, accountability and security of their votes and provides an avenue for malicious actors to manipulate the voting results," said Neil Jenkins, an official in the department's Office of Cybersecurity and Communications.

Private-sector researchers are also concerned about potential meddling by Russians in the U.S. election system. Rich Barger, chief information officer at ThreatConnect, said that several of the IP addresses listed in the FBI alert trace back to a website-hosting service called King Servers that offers Russia-based technical support. Barger also said that one of the methods used was similar to a tactic employed in other intrusions suspected of being carried out by the Russian government, including one this month on the World Anti-Doping Agency.

"The very fact that [someone] has rattled the doorknobs, the very fact that the state election commissions are in the crosshairs, gives grounds to the average American voter to wonder: Can they really trust the results?" Barger said.

Earlier this month, DHS Secretary Jeh Johnson held a conference call with state elections officials, offering his assistance in protecting against cyberattacks.

Johnson said that DHS was "not aware of any specific or credible cybersecurity threats relating to the upcoming general election systems," according to a readout of the call.

It was not clear whether he was aware at the time of the FBI's investigations in Arizona and Illinois.

Correction: An earlier version of this story misspelled the surname of the vice president of operations for the Center for Internet Security, Brian Calkin.

Ellen Nakashima is a national security reporter for The Washington Post. She focuses on issues relating to intelligence, technology and civil liberties. Follow @nakashimae