

DHS, FBI say election systems in all 50 states were targeted in 2016



Enlarge / Voter registration data was one of the targets of Russian hacking efforts in the run-up to the 2016 presidential election—which DHS and FBI analysts now say went after systems in every state.

Getty Images

reader comments

113 with 56 posters participating

Share this story

A joint intelligence bulletin (JIB) has been issued by the Department of Homeland Security and Federal Bureau of

Investigation to state and local authorities regarding Russian hacking activities during the 2016 presidential election. While the bulletin contains no new technical information, it is the first official report to confirm that the Russian reconnaissance and hacking efforts in advance of the election went well beyond the 21 states confirmed in previous reports.

As reported by the intelligence newsletter OODA Loop, the JIB stated that, while the FBI and DHS “previously observed suspicious or malicious cyber activity against government networks in 21 states that we assessed was a Russian campaign seeking vulnerabilities and access to election infrastructure,” new information obtained by the agencies “indicates that Russian government cyber actors engaged in research on—as well as direct visits to—election websites and networks in the majority of US states.” While not providing specific details, the bulletin continued, “The FBI and DHS assess that Russian government cyber actors probably conducted research and reconnaissance against all US states’ election networks leading up to the 2016 Presidential elections.”

DHS-FBI JIBs are unclassified documents, but they’re usually marked “FOUO” (for official use only) and are shared through the DHS’ state and major metropolitan Fusion Centers with state and local authorities. The details within the report are mostly well-known. “The information contained in this bulletin is consistent with what we have said publicly and what we have briefed to election officials on multiple occasions,” a DHS spokesperson told Ars. “We assume the Russian government researched and in some cases targeted election infrastructure in all 50 states in an attempt to sow discord and influence the 2016 election.”

In fact, DHS Assistant Secretary Jeanette Manfra told the Senate Homeland Security Committee in April of 2018 that Russia had likely at least performed reconnaissance on election infrastructure in all 50 states. The bulletin raises the confidence in that estimate, however, saying:

Russian cyber actors in the summer of 2016 conducted online research and reconnaissance to identify vulnerable databases, usernames, and passwords in webpages of a broader number of state and local websites than previously identified, bringing the number of states known to be researched by Russian actors to greater than 40. Despite gaps in our data where some states appear to be untouched by Russian activities, we have moderate confidence that Russian actors likely conducted at least reconnaissance against all US states based on the methodical nature of their research. This newly available information corroborates our previous assessment and enhances our understanding of the scale and scope of Russian operations to understand and exploit state and local election networks.

Alphabetical recon

The DHS and the FBI have been criticized in the past for the lack of information made publicly available about election-focused hacking and information operations. In December of 2016, the DHS and the FBI released a joint analysis report detailing broad “Russian malicious cyber activity” that the agencies referred to as “Grizzly Steppe,” which largely consisted of restating private sector research findings. An “enhanced analysis” of that activity was released in February of 2017, but it did little to improve on the original other than giving some additional intrusion detection system rules to watch for similar hacking attempts. The second draft reported that the DHS had “observed network scanning activity that is known as reconnaissance” prior to the 2016 election; it also included some generic information about common reconnaissance and malware delivery techniques.

While the latest JIB doesn’t provide any more real technical information about how systems were attacked in 2016, it does go into some detail in describing the methodical

reconnaissance approach “Russian government cyber actors” took in probing for potential vulnerabilities in election systems. Between June and October of 2016, the group associated with the election hacking “researched websites and information related to elections in at least 39 states and territories, according to newly available FBI information,” the bulletin states. “The same actors also directly visited websites in at least 30 states, mostly election-related government sites at both the state and local level—some of which overlap with the 39 researched states.”

The “actors” performed their research “in alphabetical order by state name,” the bulletin states, “suggesting that at least the initial research was not targeted at specific states.” The research focused on Secretary of State voter registration and election results sites, but it also drilled down on some local election officials’ webpages. As they accessed sites, actors “regularly attempted to identify and exploit SQL database vulnerabilities in web servers and databases.”

The FBI and DHS analysts who authored the JIB noted that they had no information on how many of those attempts were successful, aside from two instances when “Russian government operators in June 2016 accessed voter registration files and a sample ballot from a US county website.”

The new information that spurred this JIB did not, however, provide any additional insight into the Russian group’s attempts to scan for vulnerabilities in, and hack into, the networks of government agencies in “at least 21 states,” as the bulletin notes. Some of the details of that effort were provided in the indictment of Main Intelligence Directorate (GRU) officers delivered by Special Counsel Robert Mueller’s probe—at least one state had voter data stolen, though there was no indication that data was tampered with.

Beating the drum

The bulletin included no new technical data for defenders to use. But its purpose is fairly clear—it was meant to get officials in every state on board to prepare for the 2020 presidential elections now. “Since 2016,” the DHS spokesperson said, “we have built relationships and improved threat information sharing at every level—we are working with all 50 states and more than 1,400 local jurisdictions, and are doubling down on these efforts as we work with election officials to protect 2020.”

Much of the responsibility for that coordination is placed on DHS’ Cybersecurity and Infrastructure Security Agency (CISA), which is, according to recent comments by its director, Chris Krebs, ramping up election security efforts in advance of the 2020 presidential election cycle. The agency got an additional budget of \$33 million for Fiscal Year 2019 from Congress specifically for election security efforts. Krebs told reporters in February that the agency is “institutionalizing our election security efforts” and that “as our workforce continues to grow, and it will, our numbers heading up to the 2020 election will only grow,” NextGov’s Frank Konkel reported.

As far as active measures go, the JIB’s authors advised state and local officials to focus on better operational security and basic website security practices. “In anticipation of the 2020 US Presidential Election,” the DHS and FBI bulletin authors warned, “states should limit the availability of information about electoral systems or administrative processes and secure their websites and databases which could be exploited by malicious actors.”

<https://arstechnica.com/?p=1486259>