CYBERSECURITY

Software vendor may have opened a gap for hackers in 2016 swing state

By **KIM ZETTER** | 06/05/2019 01:40 PM EDT | Updated 06/06/2019 12:11 AM EDT

A Florida election software company targeted by Russians in 2016 inadvertently opened a potential pathway for hackers to tamper with voter records in North Carolina on the eve of the presidential election, according to a document reviewed by POLITICO and a person with knowledge of the episode.

VR Systems, based in Tallahassee but with customers in eight states, used what's known as remote-access software to connect for several hours to a central computer in Durham County, N.C., to troubleshoot problems with the company's voter list management tool, the person said. The software distributes voter lists to so-called electronic poll books, which poll workers use to check in voters and verify their eligibility to cast a ballot.

The company did not respond to POLITICO's requests for comment about its practices. But election security experts widely condemn remote connections to election-related computer systems — not only because they can open a door for intruders but because they can also give attackers access to an entire network, depending on how they're configured.

In Durham County's case, the computer in question communicated with North Carolina's State Board of Elections to download the county's voter list before elections, which could have potentially opened a gateway to the state system as well.

That wouldn't have allowed intruders to alter the vote tallies — and no evidence has surfaced that anyone hacked North Carolina's election results. But interference with voter records or electronic poll book software could allow an attacker to alter records in a way that prevents people from voting in crucial swing precincts. Investigations are still ongoing into whether any such tampering might have happened in North Carolina.

Last year, top voting machine maker Election Systems & Software admitted that for years it had installed and used remote access software on election-management systems it sold to counties, after initially denying it. Election-management systems are even more critical to elections because they are used first to program voting machines and then to tally the results. The revelation about VR Systems, however, indicates that the practice of remotely accessing critical election infrastructure is more widespread than previously believed.

“Vulnerabilities in voting machines get most of the attention, but the security and availability of poll books is as critical to the integrity of elections as voting machines themselves,” said Matt Blaze, a professor of law and computer science at Georgetown University and longtime election security expert. “If poll books are compromised, this can selectively disenfranchise voters, create long lines at polling places, and cast doubt on the legitimacy of election results.”

The critical security lapse — previously undisclosed publicly — is the latest cause for concern surrounding VR Systems, a company hit by a malicious email campaign targeting its own employees in August 2016 that was believed to be linked to Russia. VR Systems has long maintained that the so-called spearphishing attempt, which it reported to the FBI at the time, was unsuccessful and that a forensic investigation it commissioned from a top cybersecurity firm proved it was never hacked.

Robert Mueller, and other documents, that Russian hackers successfully compromised a voting technology company — a company that fits VR Systems' description — and installed malware on its network.

Almost three years after the first public revelation of hackers' interference in the 2016 presidential race, the Department of Homeland Security has decided to conduct a forensic analysis of computers used in Durham County during that election, the department confirmed to POLITICO on Wednesday. The DHS move was first reported by The Washington Post.

Even if VR Systems wasn't hacked in 2016, the revelation that it used remote-access software to connect to a critical election system at the height of concerns around Russian hacking alarmed state officials at North Carolina's State Board of Elections when they learned about the incident nearly a year later, according to a person familiar with the matter. The person asked not to be named because of the sensitivity of the case. A document reviewed by POLITICO backs up his assertions.

"Where the vendor would seem to have an interest in making sure customers are secure, they had not thought through [the potential risks] of doing this," the person told POLITICO. This was particularly worrisome, the person said, because the company knew that it had already been targeted by the Russians but apparently hadn't disclosed that information to customers.

What's more, the person said, officials learned it was a common practice for the company to access customer systems remotely if it would take too long to send someone physically to a customer's location to troubleshoot problems, the source said.

The person said the company has since agreed not to do it anymore, at least in North Carolina.

Still, “there was more resistance [to stop] than you would expect,” the person said. The person said VR “cited the need to be able to service customer systems and troubleshoot, and that remote access was part of that process — a feature, not a bug.”

VR Systems has customers in California, Florida, Illinois, Indiana, New York state, North Carolina, Virginia and West Virginia. Sixty-two of Florida’s 67 counties used VR Systems in 2016, including Miami-Dade, the state’s most populous. Twenty-three of North Carolina’s 100 counties, including some of its largest, also used VR Systems’ technology. Both Florida and North Carolina were critical to President Donald Trump’s victory in November 2016: Trump won Florida by 1.2 percentage points, or 119,770 votes, and North Carolina by 3.8 percentage points, or 117,529 votes.

The FBI recently revealed that Russian hackers had successfully infiltrated two counties in Florida before the 2016 election, but details about how the hacks occurred, or the connection if any to VR Systems, are still unclear.

Sen. Ron Wyden (D-Ore.), a leading critic of VR Systems, said the company needs to explain itself.

“Remotely accessing voting systems the day before Election Day is serving up our democracy on a silver platter to foreign hackers,” Wyden told POLITICO. “No company that plays such a critical role in our elections should be taking such a reckless shortcut with the cybersecurity of its state and local customers."

He added: "The fact that we’re just learning about this practice two years after the election, and after any evidence of hacking has likely been destroyed, is inexcusable. Americans need to know if VR Systems still has remote access to election computers in other states, and how often this occurred.”

The remote-access incident occurred in Durham after the county experienced problems loading voter data onto USB sticks used with its electronic poll books.

Before an election, Durham loads a digital file containing each precinct’s voter list onto the USB drives. The sticks, or activators as VR Systems calls them, are inserted into laptops running VR Systems’ electronic poll book software, known as EViD. There’s one activator for each EViD laptop and often multiple laptops in a precinct. When a poll worker types a voter’s name into a laptop, the EViD software checks the registration list on the USB stick to verify that the person is eligible to cast a ballot.

On the Sunday before the 2016 election, and again the next day, it was taking “multiple times longer than normal” to load the voter list to the USB sticks, the person familiar with the episode told POLITICO. Seeking to find out why it was taking so long, VR Systems remotely accessed the county computer used to load the voter lists but never came to a conclusion, the person told POLITICO.

The election night problem with the USB sticks had not been previously reported. But subsequent problems that occurred with the county’s electronic poll books did make headlines.

Electronic poll books at five precincts began having problems almost immediately after polls opened on Election Day. Some crashed, some incorrectly told poll workers they had to ask voters for a photo ID, and others erroneously indicated that at least nine voters had already

that led some voters to leave without casting a ballot.

After the election, Durham County hired an outside cybersecurity firm to investigate the poll book problem. The firm, Protus3, concluded that errors by poll workers were the problem for at least three voters who were told incorrectly they had already voted. The report speculated about the causes of other problems, but ultimately the state determined that the findings were inconclusive.

There was also a problem with the scope of the investigation, which did not appear to focus on whether malicious actors had hacked the electronic poll books or the voter list, according to a copy of the Protus3 report that POLITICO reviewed. Though portions of the report are blacked out, its unredacted summary doesn't mention any attempts to examine the county's network for signs of an intrusion or malware, or to look for malware on the electronic poll books and central computer, though it does say the poll books and central computer were imaged and analyzed.

Although the Russian spearphishing operation against VR Systems was not publicly known when Protus3 conducted its investigation, VR Systems had sent an email to or called all of its customers on Nov. 1, 2016, to warn them about a malicious email campaign sent to some of its customers that was designed to look like an email from the company.

POLITICO asked a Protus3 spokesperson about the scope of its investigation, but she didn't respond.

The North Carolina State Board of Elections sought to obtain an unredacted version of the Protus3 report, but was denied, according to the person familiar with the inquiry. The board considered the Protus3 investigation incomplete but didn't press the matter.

CYBERSECURITY

Russia's manipulation of Twitter was far vaster than believed

By **TIM STARKS**, **LAURENS CERULUS** and MARK SCOTT

That changed in June 2017 when The Intercept published a leaked NSA document that revealed that Russian hackers had sent employees of a voting technology company malicious emails in August 2016 with the intent of hacking into their company email accounts. The document suggested the attackers may have successfully compromised at least one

North Carolina election board officials realized immediately that they had to consider the possibility that Russian intruders could have caused the problems with Durham's electronic poll books on Election Day if they had either breached VR Systems or gained entry through VR Systems' remote-access connection, the person familiar with the incident told POLITICO.

"Until the [NSA] leak … Durham and everybody else thought [the problem] was administrator error, and there was not an overriding need to nail down what happened exactly," the person said.

The state board then launched its own investigation, and from interviews with Durham County workers, learned about the remote-access issue and the USB problem that prompted it.

The person said this wasn't the first time state election officials had developed concerns about VR Systems' security practices. Sometime around March 2016, the person said, officials had uncovered information from counties that appeared to indicate VR Systems software was using an unsecured method to transmit voter data to counties that it had obtained from the state board. (VR Systems insisted to state officials that its file transfer system was secure, the person said.)

Fears of Russian interference hadn't yet surfaced at that time. But officials were worried about identity theft, because the transmitted data included voters' Social Security numbers. So between March and the November election, the state initiated a new process in which sensitive information was removed from versions of the voter data intended for EViD poll books before it was transmitted.

Despite all of these concerns, and lingering questions about what occurred on Election Day with Durham's electronic poll books, the state has never completed its own investigation into what happened, even though it obtained, and still has in its possession, mirror images of the poll books.

Board spokesperson Patrick Gannon told POLITICO last month in an email that state investigators believe that "human error on the part of Durham County election and poll workers likely contributed to the 2016 incident," but the investigation remains open because the agency "does not have the technical expertise to conduct a forensic examination of the

laptops used in Durham County elections in 2016. This support may help to provide a better understanding of previous issues and help to secure the 2020 election."

DHS went on to say that it currently doesn't have "information that there is any previous or ongoing issues regarding election systems in the state of North Carolina and all services are being provided in a proactive manner at the request of the state."